Aficio™ MP 301SP/301SPF

Read This First

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

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.

Printed in China

EN US D127-7504

D1277504

TABLE OF CONTENTS

4. Appendix

Introduction

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.

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.

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

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

In no event will the company be liable for direct, indirect, special, incidental, or consequential damages as a result of handling or operating the machine.

Notes

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.

Machine Types

Check the type of your machine before reading the manuals.

- Type 1: MP 301SP/Aficio MP 301SP
- Type 2: MP 301SPF/Aficio MP 301SPF

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™.

VM Card 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 using Web Image Monitor.

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.

UNIX Supplement

For "UNIX Supplement", please visit our Web site or consult an authorized dealer. This manual includes descriptions of functions and settings that might not be available on this machine.

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.
- 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
Print	No	Yes	No
Scan	No	Yes	No
Connecting the Machine/ System Settings	No	Yes	No
Security Guide	No	No	Yes
PostScript 3	No	Yes	No
VM Card Extended Feature Settings	No	Yes	No
Driver Installation Guide	No	No	Yes
UNIX Supplement	No	No	Yes*1

*1 For "UNIX Supplement", please visit our Web site or consult an authorized dealer.

Note

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

On-screen Operating Instructions

This chapter describes the on-screen operating instructions of this machine. The on-screen operating instructions are included in the supplied manual CD-ROM.

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 p.7 "Manuals for This Machine". The various manuals are available in different formats. For details about availability, see p.10 "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. **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, Windows Server 2003/2003 R2/2008/2008 R2
  - 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 manual CD-ROM.

File path

The manuals are included in the following folder on the CD-ROM:

`MANUAL_PDF\(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].**

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

This chapter describes the safety precautions.

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

- Keep the machine away from salt-bearing air and corrosive gases. Also, do not install the machine in places where chemical reactions are likely (laboratories, etc.), as doing so will cause the machine to malfunction.

⚠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.
  - 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.
  - 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

- If the trays 2 and 3 are 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.

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

- The inside of the machine could be very hot. Do not touch the parts with a label indicating the "hot surface". Otherwise, an injury might occur.

⚠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

- During operation, rollers for transporting the paper and originals revolve. A safety device has been installed so that the machine can be operated safely. But take care not to touch the machine during operation. Otherwise, an injury might occur.

⚠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 the cleaner to suck spilled toner (including used toner). Sucked toner may cause firing or explosion due to electrical contact flickering inside the cleaner. However, it is possible to use the cleaner designed for dust explosion-proof purpose. If toner is spilled over the floor, sweep up spilled toner slowly and clean remainder with wet cloth.

⚠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

- 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.

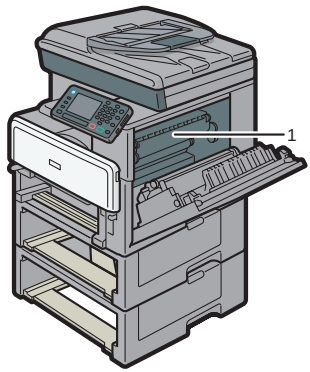
Safety Labels of This Machine

This section explains the machine's safety information labels.

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

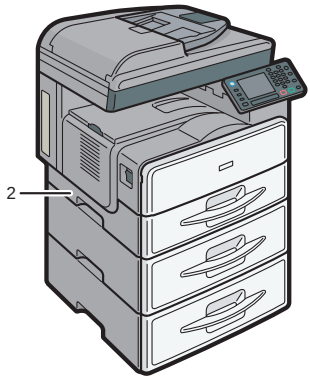


CMV607

1

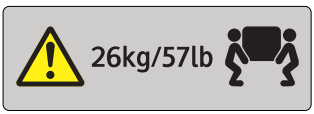
CMV603

High temperature. Be careful of hot parts when clearing paper jams.



CMV608

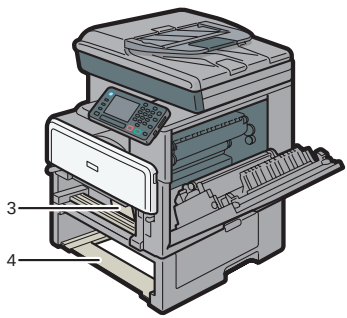
2



CMV604

The machine weighs approximately 26 kg (57.4 lb.). When moving the machine, use the inset grips on both sides, and lift slowly in pairs.

Paper trays (when one paper tray unit are installed)



CMV609

3

CMV610

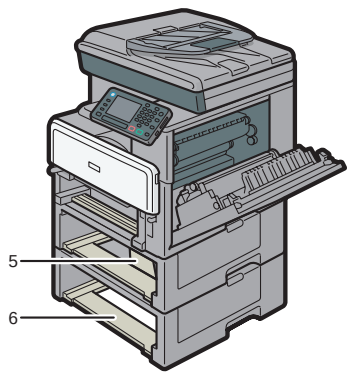
The inside of the machine could be very hot. Do not touch the parts which a label is put on. Otherwise, an injury might occur.

4

CMV611

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.

Paper trays (when two paper tray units are installed)



CMV612

5

CMV610

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.

6

CMV611

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. Information for This Machine

This chapter describes laws and regulations related to this machine.

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 products. This equipment contains AlGaAs laser diode, 12 milliwatts, 775–790 nanometer wavelength for each emitter. The beam divergence angle is 22 degrees (minimum) and 33 degrees (maximum) in the vertical direction, and 6 degrees (minimum) and 12 degrees (maximum) in the horizontal direction, and laser beams are generated in Continuous Wave (CW) mode.

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.

Caution:

When using the optional Gigabit Ethernet board, properly shield twisted pair cable (STP cable) must be used for connections to a host computer (and/or peripheral) in order to meet FCC emission limits.

Caution:

An Modular cable with 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.

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 material 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 manual. 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.

ENERGY STAR Program

ENERGY STAR® Program Requirements for Imaging Equipment

This company is a participant in the ENERGY STAR® Program.

This machine is compliant with the regulations specified by the ENERGY STAR® Program.

The ENERGY STAR® Program Requirements for Imaging Equipment encourage energy conservation by promoting energy efficient computers and other office equipment.

The program backs the development and dissemination of products that feature energy saving functions.

It is an open program in which manufacturers participate voluntarily.

Targeted products are computers, monitors, printers, facsimiles, copiers, scanners, and multi-function devices. Energy Star standards and logos are internationally uniform.

Note

- For details about the "default delay time", see p.37 "Energy Saving Functions".

Energy Saving Functions

To reduce its power consumption, this machine has the following functions:

Sleep mode

- If this machine remains idle for a specified period or when the [Energy Saver] key is pressed, it enters Sleep mode to reduce its electrical consumption.
- The default delay time the machine waits before entering Sleep mode is 1 minute. This default time can be changed.
- The machine can print jobs from computers and receive faxes while in Sleep mode.

Specifications

Items	Type 1	Type 2
Reduced electrical consumption in Sleep mode*1	2.7 W	2.8 W
Time of switch into Sleep mode	1 minute	1 minute
Time of switch out from Sleep mode*1	10 seconds or less	10 seconds or less

*1 The time it takes to switch out from energy saving functions and electrical consumption may differ depending on the conditions and environment of the machine.

Note

- Specifications can vary depending on which options are installed on the machine.
- For details about how to change the default interval, see "Timer Settings", Connecting the Machine/ System Settings.
- Depending on which embedded software application is installed on it, the machine might take longer than indicated to enter Sleep mode.

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 chapter describes trademarks.

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 U.S. and other countries.

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

UNIX is a registered trademark of The Open Group.

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 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

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.

MP 301SP/301SPF

Aficio™ MP 301SP/301SPF

User Guide

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

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 "Read This First" before using the machine.

TABLE OF CONTENTS

3. Copy

4. Fax

5. Print

6. Scan

7. Document Server

8. Web Image Monitor

9. Adding Paper and Toner

10. Troubleshooting

11. Appendix

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.

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

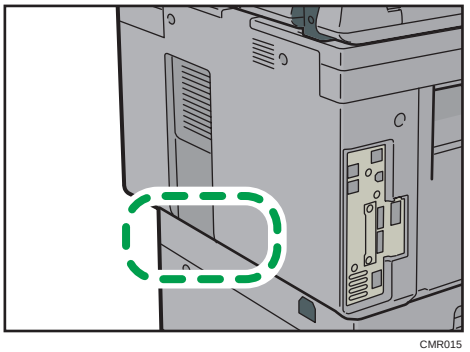
Region B (mainly North America)

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 p.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.



CMR015

The following information is region-specific. Read the information under the symbol that corresponds to the region of your machine.

Region A (mainly Europe and Asia)

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

- CODE XXXX -27, -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
- 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 -27" is printed on the label, see "Region A (mainly Europe)".
- If your machine is a region A model and "CODE XXXX -29" is printed on the label, see "Region A (mainly Asia)".

Names of Major Features

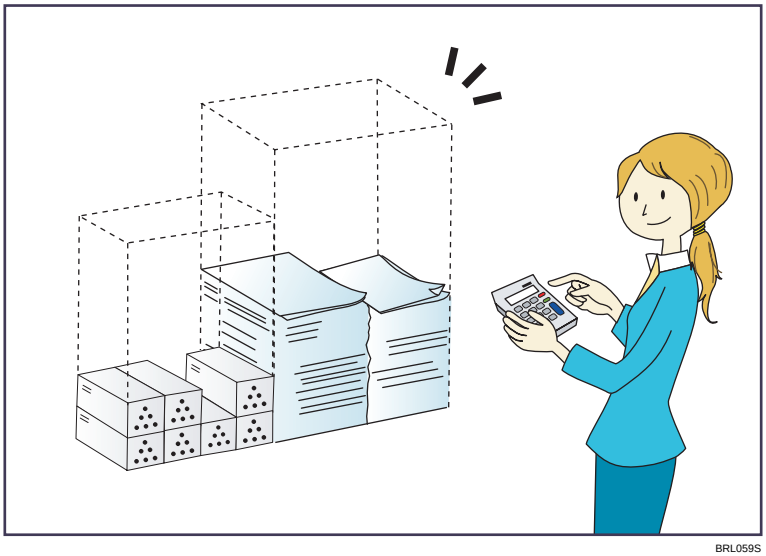
In this manual, major features of the machine are referred to as follows:

- Auto Document Feeder → ADF

1. What You Can Do with This Machine

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

I Want to Save Paper



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.

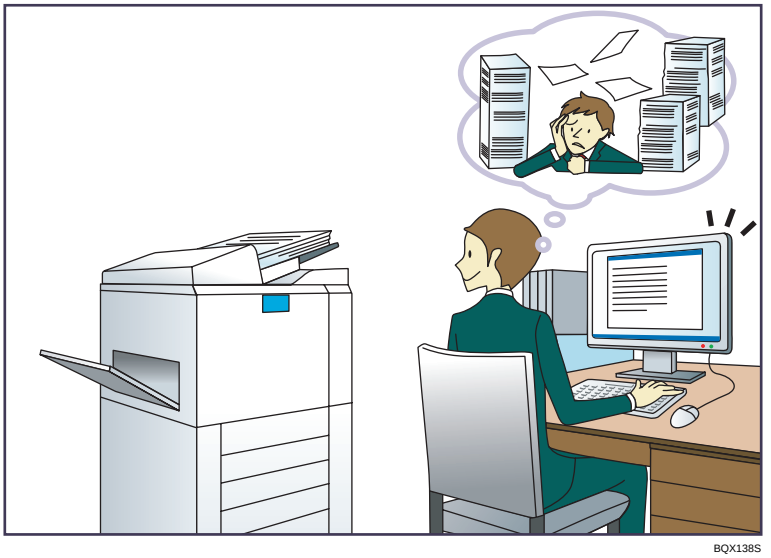
Sending files from the computer without printing them (LAN-Fax)

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

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

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

I Want to Convert Documents to Electronic Formats Easily



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 Removable Memory Device", Scan.

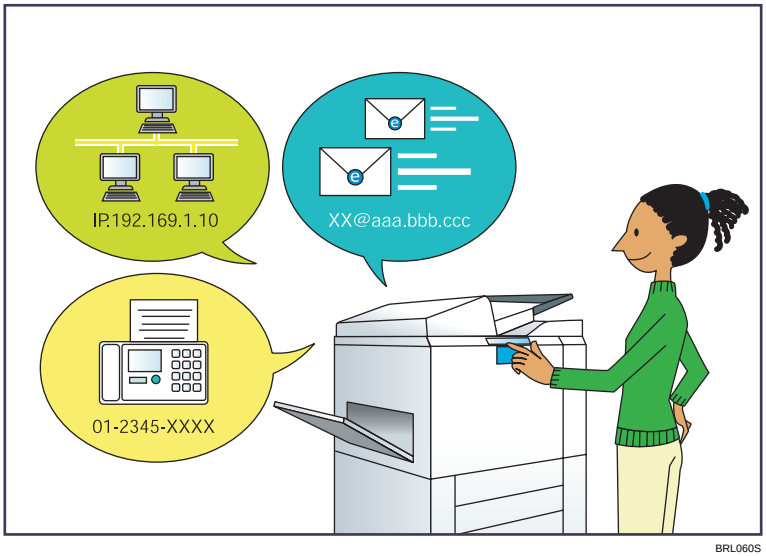
Converting transmitted faxes to electronic formats and sending them to a computer

⇒ 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.

I Want to Register 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.

I Want to Operate the Machine More Effectively

BQX139S

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

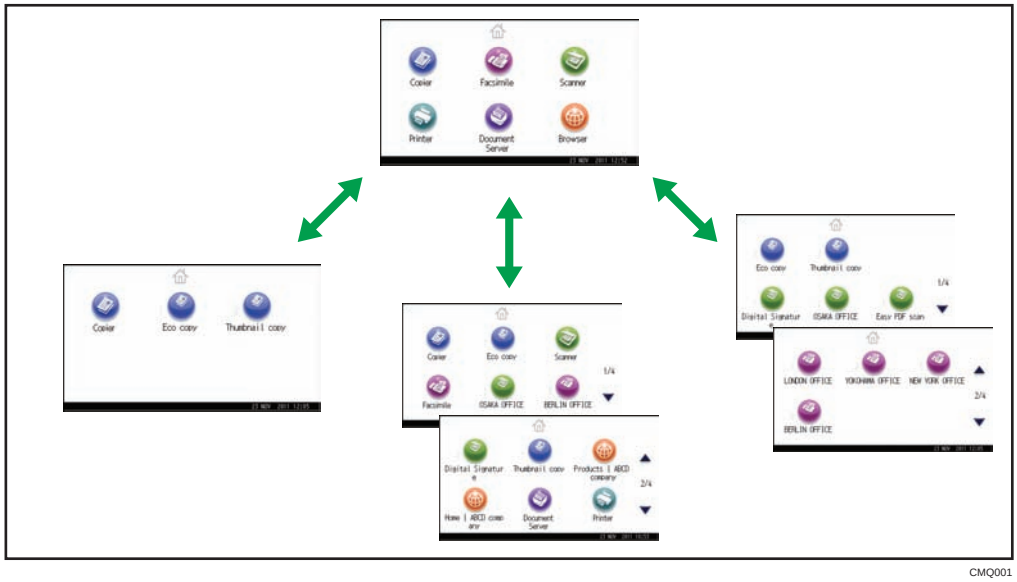
⇒ See "Adding Icons to the [Home] Screen", Convenient Functions.

Changing the order of the function and shortcut icons

⇒ See "Changing the Order of Icons on the [Home] Screen", Convenient Functions.

You Can Customize the [Home] Screen as You Like

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



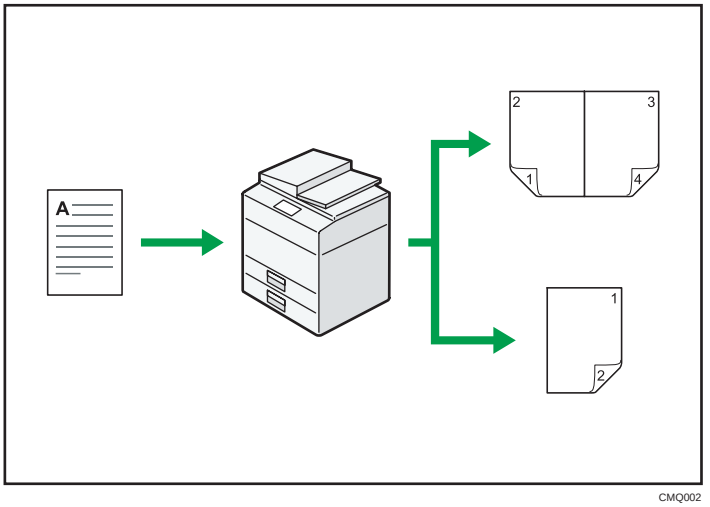
CMQ001

- 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", Getting Started.

You Can Make Copies Using Various Functions



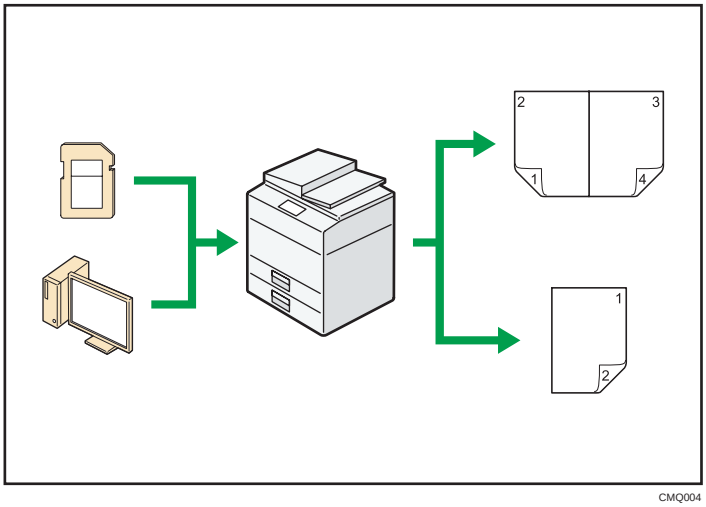
CMQ002

- You can reduce or enlarge the copy image. With the Auto Reduce/Enlarge function, the machine automatically calculates the reproduction ratio based on the sizes of the originals and the paper you have specified.
- Copier functions such as Duplex and Combine allow you to save on paper by copying multiple pages onto single sheets.
- You can copy onto various types of paper such as envelopes and OHP transparencies.
- You can sort copies.

Reference

- See Copy/ Document Server.

You Can Print Data Using Various Functions



CMQ004

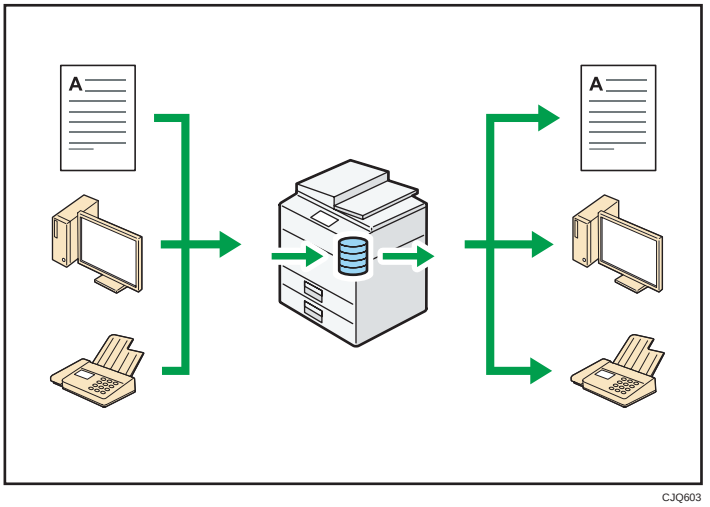
- This machine supports network and local connections.
- You can send PDF files directly to the machine for printing, without having to open a PDF application.
- You can print or delete print jobs stored on the machine's hard disk, which have been previously sent from computers using the printer driver. The following types of print jobs can be selected: Sample Print, Locked Print, Hold Print, and Stored Print.
- You can collate printed paper.
- You can print files stored on a removable memory device and specify print conditions such as print quality and print size.

Reference

- See Print.

You Can Utilize Stored Documents

You can store files scanned in copier, facsimile, printer, or scanner mode on the machine's hard disk. With Web Image Monitor, you can 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.

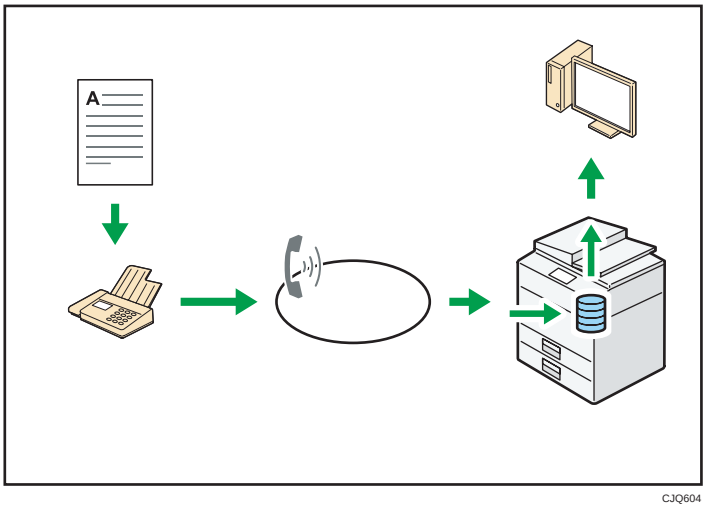
Reference

- For details about the Document Server in copier mode and how to use the Document Server, see "Storing Data in the Document Server" and "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.

You Can Send and Receive Faxes without Paper

Reception

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



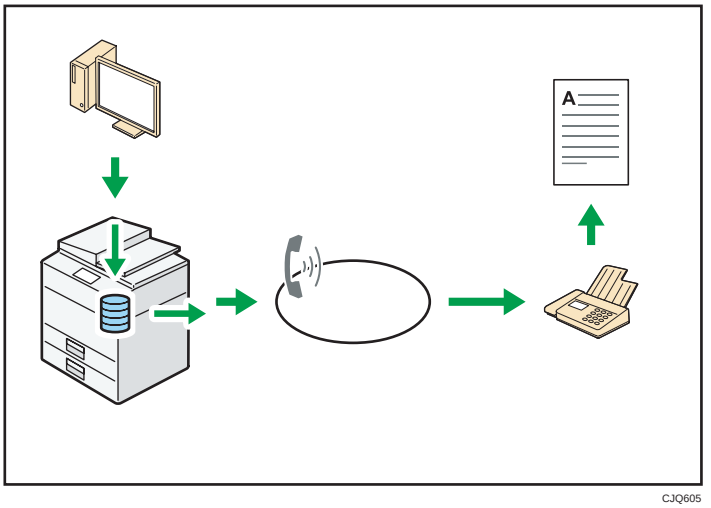
You can use Web Image Monitor to check, print, delete, retrieve, or download documents using your computer (Storing received documents).

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).



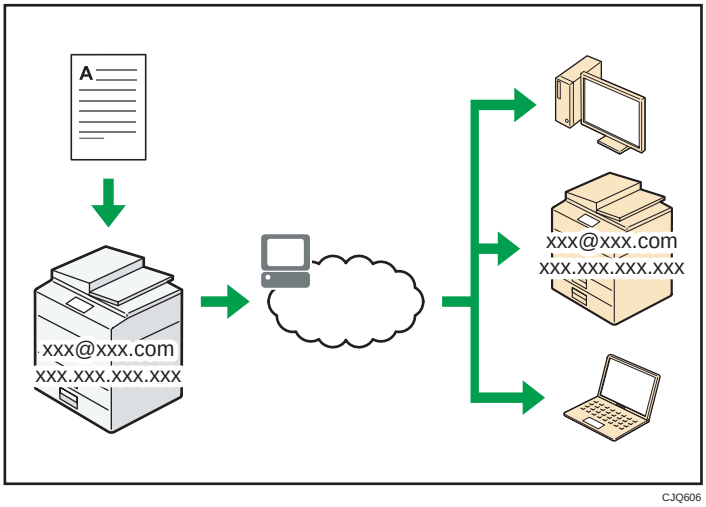
CJQ605

- 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 "Fax via Computer", Fax.

You Can Send and Receive Faxes Using the Internet



CJQ606

E-mail Transmission and Reception

This machine converts scanned document images to e-mail format, and transmits and receives this 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).
- This machine can receive e-mail messages via Internet Fax or from computers (Internet Fax Reception and Mail to Print).
- 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.

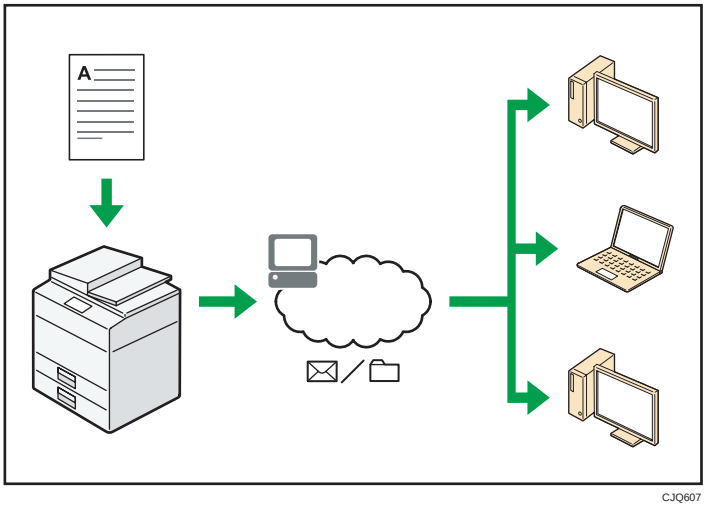
- To send a document, specify an IP address or host name instead of a fax number (IP-Fax Transmission).
- This machine can receive documents sent via Internet Fax (IP-Fax Reception).
- Using a VoIP gateway, this machine can send to G3 facsimiles connected to the public switched telephone network (PSTN).

Reference

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

- For details about how to transmit and receive documents over the Internet, see "Transmission" and "Reception", Fax.

You Can Use the Facsimile and the Scanner in a Network Environment



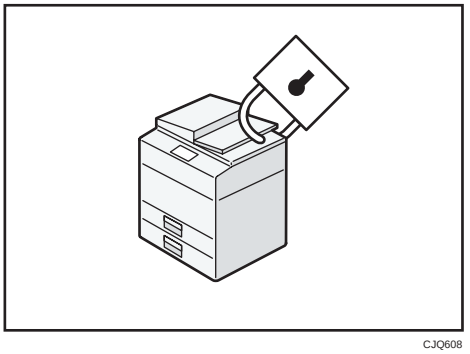
- You can send scan files to a specified destination using e-mail (Sending scan files by e-mail).
- You can send scan files directly to folders (Sending scan files by Scan to Folder).
- You can use this machine as a delivery scanner for the ScanRouter delivery software*1 (Network delivery scanner). You can save scan files in the delivery server or send them to a folder in a computer on the same network.
- You can use Web Services on Devices (WSD) to send scan files to a client computer.

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

Reference

- See Fax, Scan, or Connecting the Machine/ System Settings.

You Can Prevent Information Leakage (Security Functions)



CJQ608

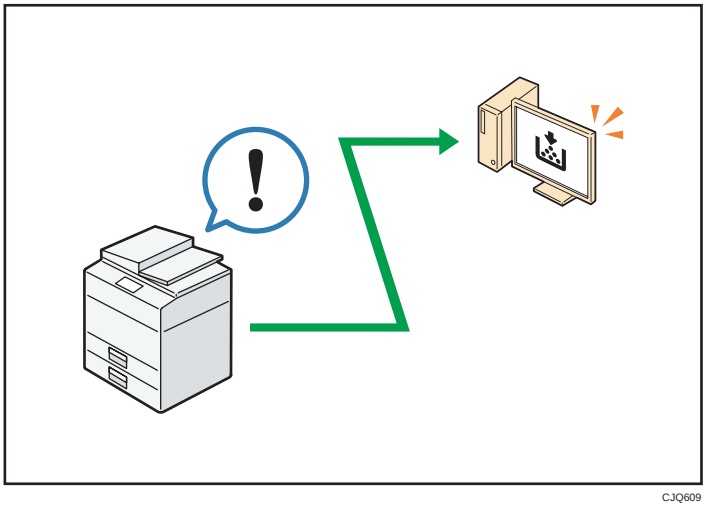
- You can protect documents from unauthorized access and stop them from being copied without permission.
- You can control the use of the machine, as well as prevent machine settings from being changed without authorization.
- By setting passwords, you can prevent unauthorized access via the network.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

Reference

- See Security Guide.

You Can Monitor and Set the Machine Using a Computer

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



CJQ609

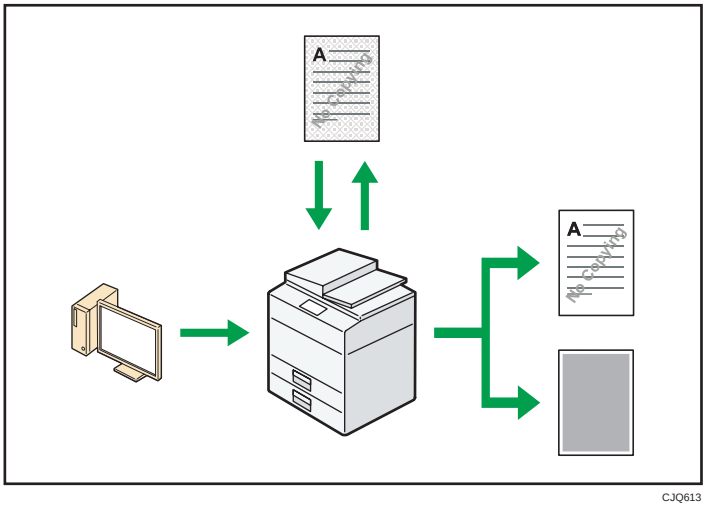
You can check which tray is running out of paper, register information in the Address Book, specify the network settings, configure and change the system settings, manage jobs, print the job history, and configure the authentication settings.

Reference

- See Connecting the Machine/ System Settings or Web Image Monitor Help.

You Can Prevent an Unauthorized Copy

You can print embedded pattern on paper to prevent them from being copied.



CJQ613

- Using 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, preventing confidential information from 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 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, Print, and Security Guide.

2. Getting Started

This chapter describes how to start using this machine.

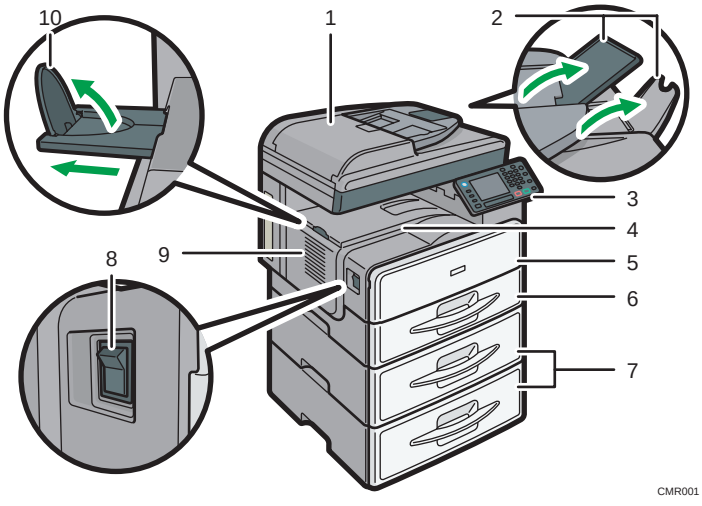
Guide to Names and Functions of Components

Guide to Components Region A (mainly Europe)

Important

- **Do not obstruct the ventilation holes by placing objects near them or leaning things against them. If the machine overheats, a fault might occur.**

Front and left view



1. **Exposure glass cover or ADF**

   (The illustration shows the 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. **Extenders**

   Raise these extenders to support large paper.

3. **Control panel**

   See p.35 "Guide to the Names and Functions of the Machine's Control Panel".

4. **Internal tray**

   Copied/printed paper and fax messages are delivered here.

5. **Front cover**

   Open to access the inside of the machine.

6. **Paper tray**

   Load paper here.

7. **Paper tray unit (Tray 2 and Tray 3)**

   Load paper here.

8. **Main power switch**

   To operate the machine, the main power switch must be on. If it is off, turn the switch on.

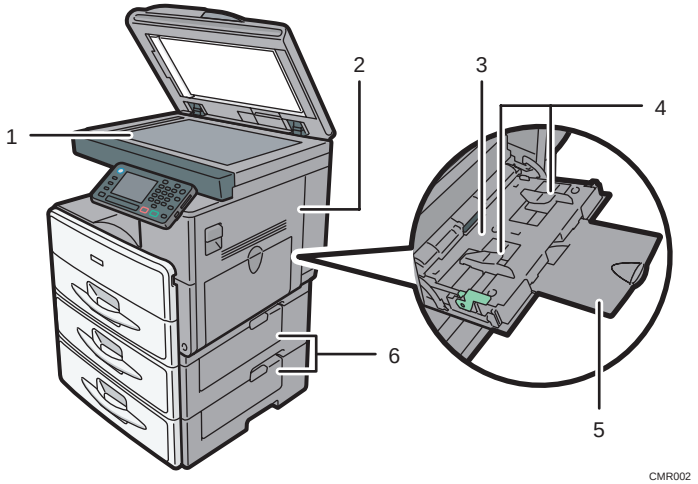
9. **Ventilation holes**

   Prevent overheating.

10. **Internal tray guide**

    Open out and raise the end fence to support large paper.

Front and right view



1. **Exposure glass**

   Place originals face down here.

2. **Right cover**

   Open this cover to remove jammed paper fed from the paper tray.

3. **Bypass tray**

   Use to copy or print on OHP transparencies and label paper (adhesive labels).

4. **Paper guides**

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

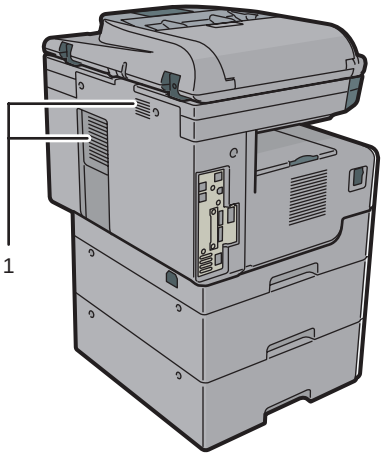
5. **Extender**

   Pull this extender out when loading paper in the bypass tray.

6. **Lower right cover**

   Open this cover when a paper jam occurs.

Rear and left view



CMR016

1. **Ventilation holes**

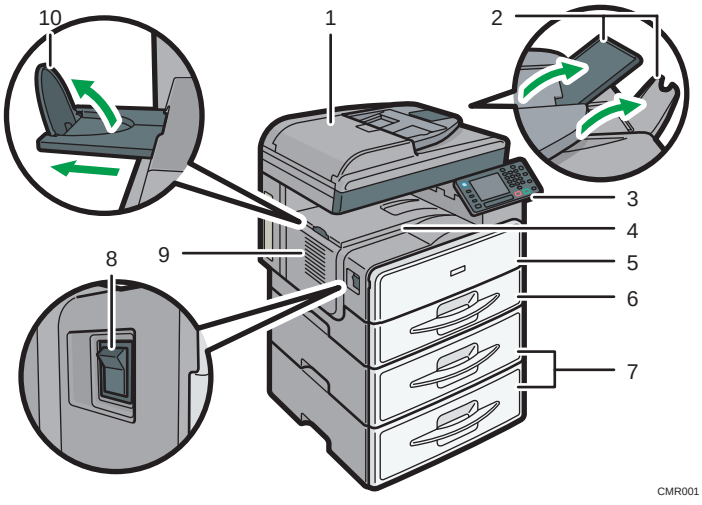
   Prevent overheating.

Guide to Components Region A (mainly Asia)

Important

- Do not obstruct the ventilation holes by placing objects near them or leaning things against them. If the machine overheats, a fault might occur.

Front and left view



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. **Extenders**

   Raise these extenders to support large paper.

3. **Control panel**

   See p.35 "Guide to the Names and Functions of the Machine's Control Panel".

4. **Internal tray**

   Copied/printed paper and fax messages are delivered here.

5. **Front cover**

   Open to access the inside of the machine.

6. **Paper tray**

   Load paper here.

7. **Paper tray unit (Tray 2 and Tray 3)**

   Load paper here.

8. **Main power switch**

   To operate the machine, the main power switch must be on. If it is off, turn the switch on.

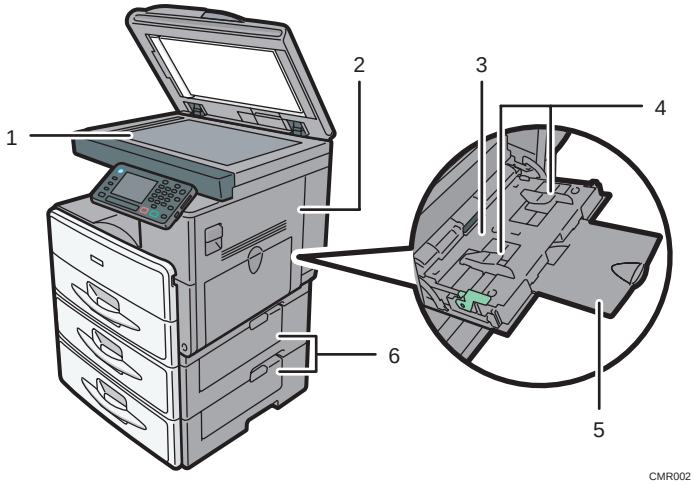
9. **Ventilation holes**

   Prevent overheating.

10. **Internal tray guide**

    Open out and raise the end fence to support large paper.

Front and right view



1. **Exposure glass**

   Place originals face down here.

2. **Right cover**

   Open this cover to remove jammed paper fed from the paper tray.

3. **Bypass tray**

   Use to copy or print on OHP transparencies and label paper (adhesive labels).

4. **Paper guides**

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

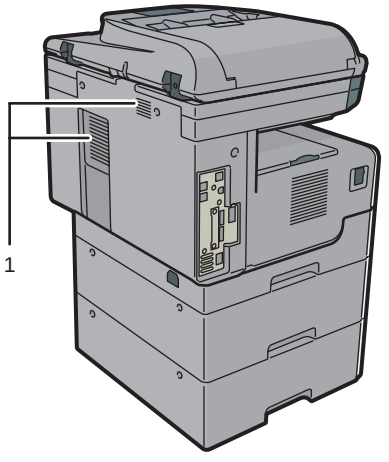
5. **Extender**

   Pull this extender out when loading paper in the bypass tray.

6. **Lower right cover**

   Open this cover when a paper jam occurs.

Rear and left view



CMR016

1. **Ventilation holes**

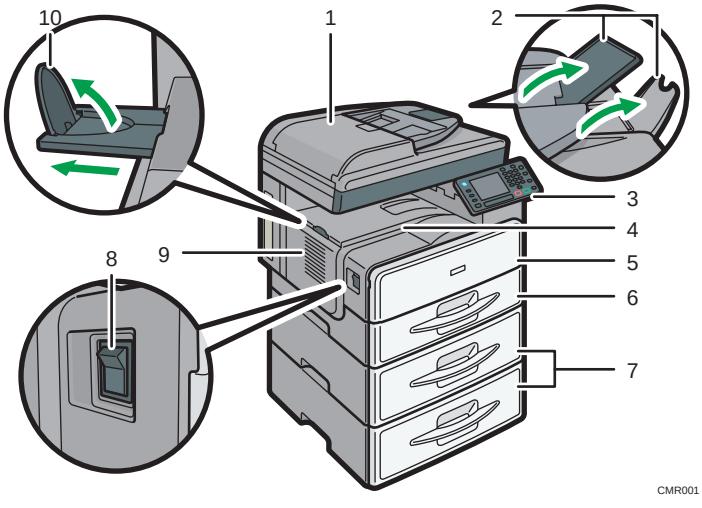
   Prevent overheating.

Guide to Components Region B (mainly North America)

Important

- Do not obstruct the ventilation holes by placing objects near them or leaning things against them. If the machine overheats, a fault might occur.

Front and left view



CMR001

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. **Extenders**

   Raise these extenders to support large paper.

3. **Control panel**

   See p.35 "Guide to the Names and Functions of the Machine's Control Panel".

4. **Internal tray**

   Copied/printed paper and fax messages are delivered here.

5. **Front cover**

   Open to access the inside of the machine.

6. **Paper tray**

   Load paper here.

7. **Paper tray unit (Tray 2 and Tray 3)**

   Load paper here.

8. **Main power switch**

   To operate the machine, the main power switch must be on. If it is off, turn the switch on.

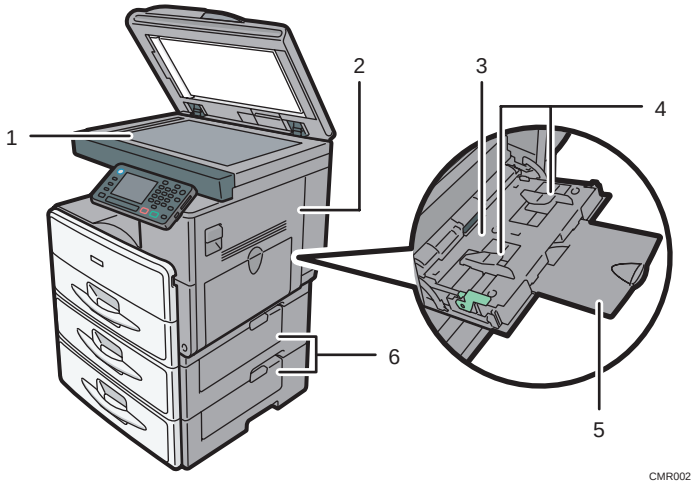
9. **Ventilation holes**

   Prevent overheating.

10. **Internal tray guide**

    Open out and raise the end fence to support large paper.

Front and right view



1. **Exposure glass**

   Place originals face down here.

2. **Right cover**

   Open this cover to remove jammed paper fed from the paper tray.

3. **Bypass tray**

   Use to copy or print on OHP transparencies and label paper (adhesive labels).

4. **Paper guides**

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

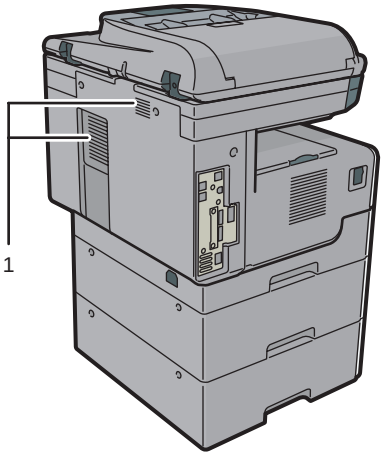
5. **Extender**

   Pull this extender out when loading paper in the bypass tray.

6. **Lower right cover**

   Open this cover when a paper jam occurs.

Rear and left view



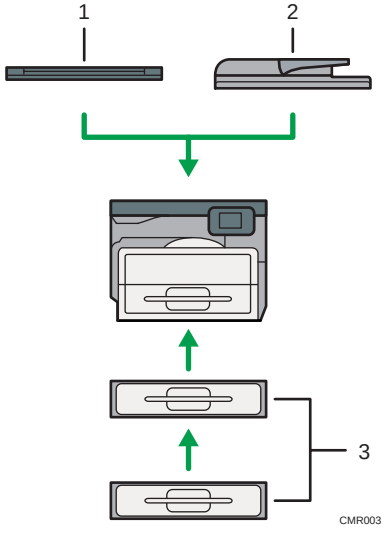
CMR016

1. **Ventilation holes**

   Prevent overheating.

Guide to Functions of the Machine's Options

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



1. **Exposure glass cover**

   Lower this cover over originals.

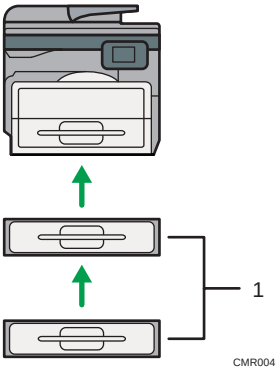
2. **ADF**

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

3. **Paper tray unit (Tray 2 and Tray 3)**

   Holds up to 500 sheets of paper. Up to two trays can be stacked.

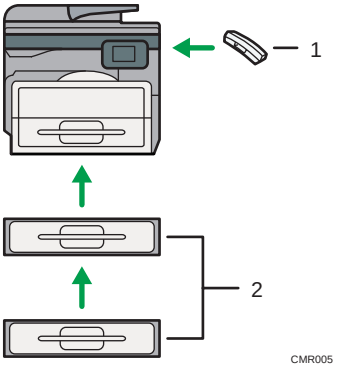
Guide to Functions of the Machine's External Options Region A (mainly Asia)



1. **Paper tray unit (Tray 2 and Tray 3)**

   Holds up to 500 sheets of paper. Up to two trays can be stacked.

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



1. **Handset**

   Used as a receiver when a fax unit is installed.

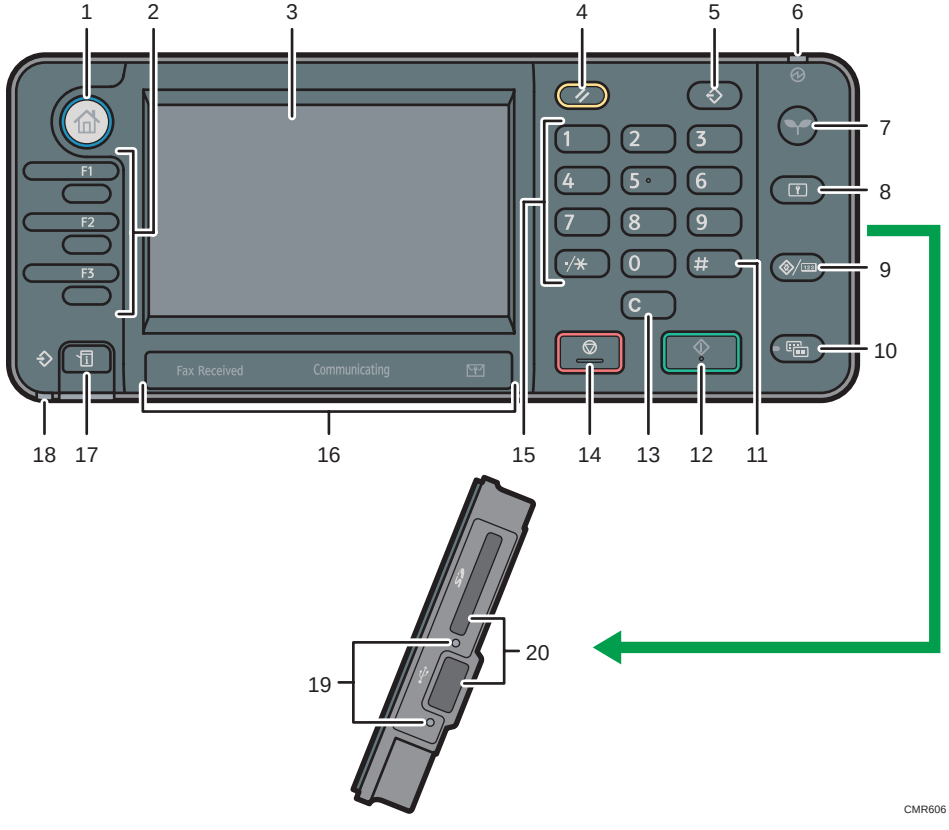
   Allows you to use the On Hook Dial and Manual Dial functions. It also allows you to use the machine as a telephone.

2. **Paper tray unit (Tray 2 and Tray 3)**

   Holds up to 500 sheets of paper. Up to two trays can be stacked.

Guide to the Names and Functions of the Machine's Control Panel

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



1. **[Home] key**

   Press to display the [Home] screen. For details, see p.38 "How to Use the [Home] Screen".

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", Getting Started.

3. **Display panel**

   Displays keys for each function, operation status, or messages. See "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. **Main power indicator**

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

7. **[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.

8. **[Login/Logout] key**

   Press to log in or log out.

9. **[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 Enquiry Using the User Tools", Maintenance and Specifications.

10. **[Simple Screen] key**

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

11. **[#] key (Enter key)**

    Press to confirm values entered or items specified.

12. **[Start] key**

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

13. **[Clear] key**

    Press to delete a number entered.

14. **[Stop] key**

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

15. **Number keys**

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

16. **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.

17. [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.

18. 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.

19. Media access lamp

Lights up when a removable memory device is inserted in the media slot or accessed.

20. Media slots

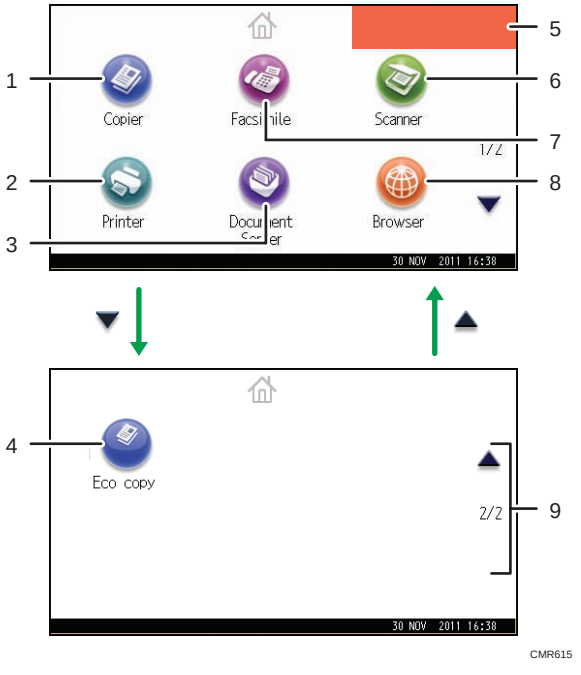
Use to insert an SD card or a USB memory.

How to Use the [Home] Screen

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.



CMR615

1. **[Copier]**

   Press to make copies.

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

2. **[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.

3. **[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.

4. **Shortcut icon**

   You can add shortcuts to programs or Web pages to the [Home] screen. For details about how to register shortcuts, see p.39 "Adding Icons to the [Home] Screen". The program number appears on the lower left of the shortcut icon.

5. **Home screen image**

   You can display an image on the [Home] screen, such as a corporate logo. To change the image, see "Displaying the Image on the [Home] Screen", Convenient Functions.

6. **[Scanner]**

   Press to scan originals and save images as files.

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

7. **[Facsimile]**

   Press to send or receive faxes.

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

8. **[Browser]**

   Press to display Web pages.

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

9. ▲/▼

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

Adding Icons to the [Home] Screen

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 p.44 "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 Favorites by User cannot be registered to the [Home] screen. To register the shortcuts, register Web pages to Common Favorites. For details about kinds of Favorites, see "Specifying the Settings for Favorites", Convenient Functions.
- 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", Convenient Functions.

- You can change the position of icons. For details, see "Changing the Order of Icons on the [Home] Screen", Convenient Functions.

Adding icons to the [Home] screen using Web Image Monitor

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.**

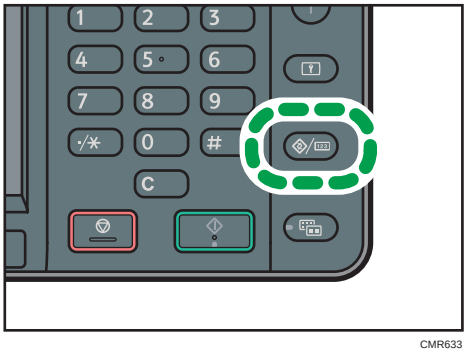
   For details, see Security Guide.

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

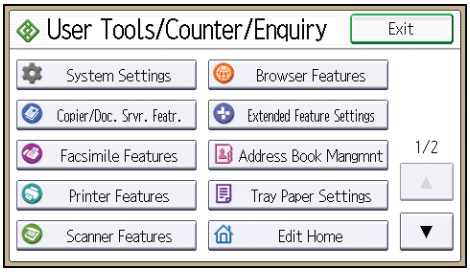
In the following procedure, a shortcut to a copier program is registered to the [Home] screen.

1. **Register a program.**
2. **Press the [User Tools/Counter] key.**

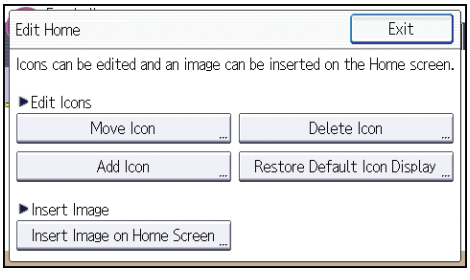


CMR633

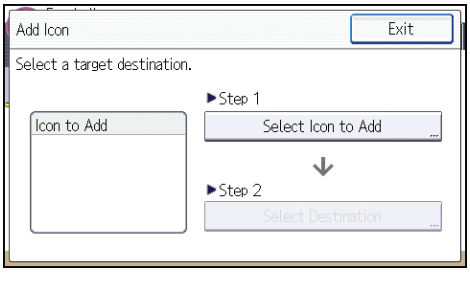
3. **Press [Edit Home].**



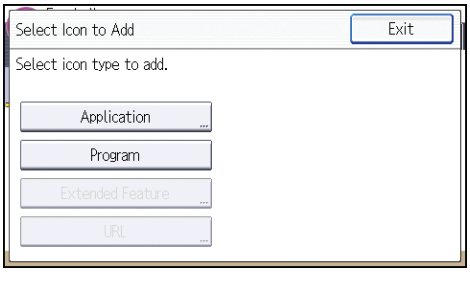
4. **Press [Add Icon].**



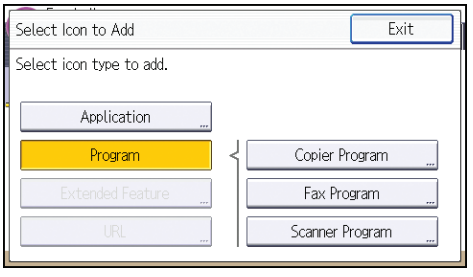
5. **Press [Select Icon to Add].**



6. **Press [Program].**

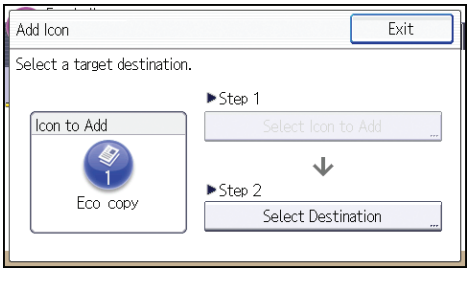


7. **Press [Copier Program].**

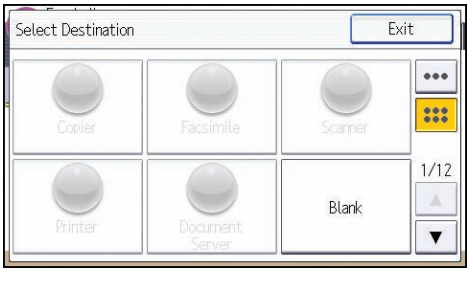


8. **Select the program you want to add.**

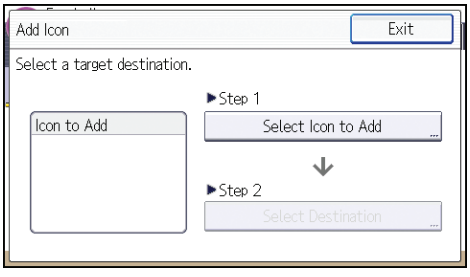
9. **Press [Select Destination].**



10. **Specify the position where [Blank] is displayed.**



11. **Press [Exit].**



12. **Press the [User Tools/Counter] key.**

Note

- Press [•••] on the upper-right corner of the [Select Destination] screen to check the position on the simple screen.

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:

Density, paper tray, Orig. (Settings for Originals), Auto Reduce/Enlarge, Red./Enlg. (Reduce/Enlarge), Other Func. (Other functions), number of copies

Document Server (on the initial document print screen):

2 Sided: Top to Top, 2 Sided: Top to Bottom, Sort, Other Func. (Other functions), number of prints

Facsimile:

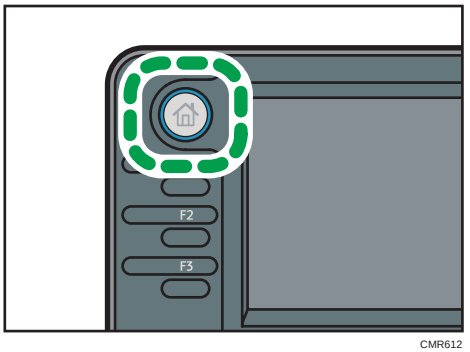
Transmission type, memory transmission/immediate transmission, Select Destination from Address Book (except for folder destinations), Manual Entry, TX Status Report, Send Settings (except for Subject and Sender Name)

Scanner:

Original, Send Settings (except for File Name, Security Settings in File Type, Sender Name, and User Name and Password in Store File)

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

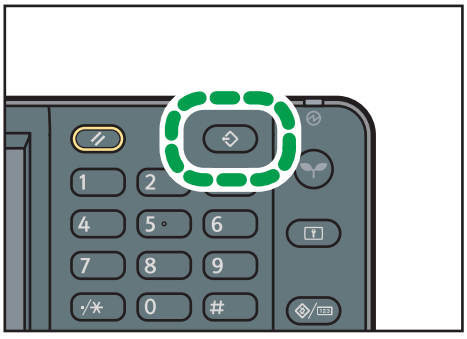
1. **Press the [Home] key on the top left of the control panel, and press the [Copier] icon on the [Home] screen.**



CMR612

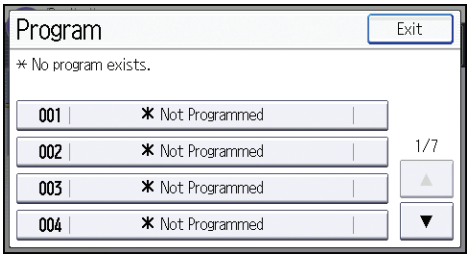
2. **Edit the copy settings so all functions you want to store in a program are selected.**

3. **Press the [Program] key.**



CMT001

4. **Press [Program].**
5. **Press the program number you want to register.**



6. **Enter the program name.**
7. **Press [OK].**
8. **Press [Exit] twice.**

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.

- 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 p.39 "Adding Icons to the [Home] Screen". 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 [Cmb. 2 Sides] under [Combine] in [Other Func.].	You can save paper and toner.
Thumbnail copy	Specify [Cmb. 1 Side] under [Combine] in [Other Func.].	You can copy up to four pages onto one side of a sheet, so that you can save paper.

Scanner mode

Program name	Program description	Effect
Easy PDF scan	In [Send Settings], select [Full Colour] under [Type of Original], and select [PDF] under [File Type]. Then enter the business details such as "London branch: daily report" under [File Name].	You can scan documents efficiently.
High compression PDF scan	In [Send Settings], select [Full Colour] under [Type of Original] and [High Compress. PDF] under [File Type].	You can compress the data size of scanned documents, so that you can send and store them.
Long-term storage scan	Select [PDF/A] under [File Type] in [Send Settings].	You can easily digitize documents to "PDF/A" file format, which is suitable for long-term storage.

Program name	Program description	Effect
Digital signature scan	In [Send Settings], specify [PDF], [High Compress. PDF], or [PDF/A] 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 [Send Settings].	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 under [Resolution] in [Send 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 [Send Settings].	You can apply multiple scans to a large volume of originals and send the scanned originals.

Facsimile mode

Program name	Program description	Effect
Transmission result notification fax	Select [Preview] and specify [Email TX Results] in [Send Settings].	You can check whether the transmission settings are correct before and after transmission.
Specified time fax transmission	Specify [Send Later] in [Send Settings].	You can send a fax at a specified time.
Departmental fax transmission	Specify [Fax Header Print] under [Option Setting] in [Send Settings].	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 left side of the machine. Turning off this switch makes the main power indicator on the right side of the control panel go off. 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.

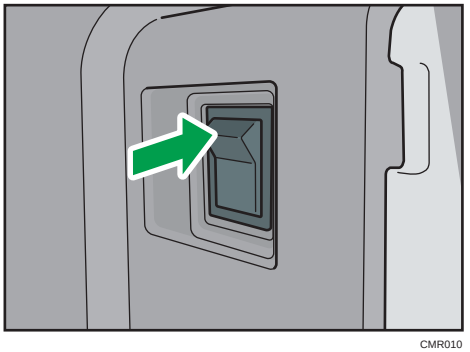
Turning On the Main Power

Important

- **Do not turn off the main power switch immediately after turning it on. Doing so may result in damage to the hard disk or memory, leading to malfunctions.**

1. **Make sure the power cord is firmly plugged into the wall outlet.**
2. **Turn on the main power switch.**

   The main power indicator goes on.



CMR010

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

- **After turning the machine's power off, wait at least a few seconds before turning it back on. If the message "Turn main Power Switch off" appears, turn the machine's power off, wait 10 seconds or more, and then turn it back on again. Never turn the power back on immediately after turning it off.**

- Before unplugging the power cord plug, turn off the main power switch and make sure the main power switch indicator turns off. Not doing so may result in damage to the hard disk or memory, leading to malfunctions.
- Do not turn off the power while the machine is in operation.

1. **Turn off the main power switch.**

   The main power indicator goes out.

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

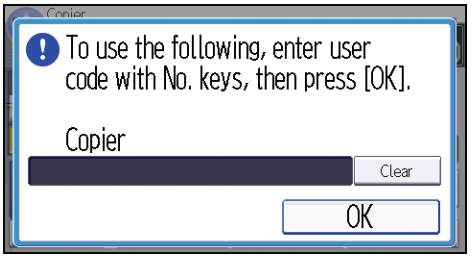
- **Ask the user administrator for the Login User Name, Login Password, and User Code. For details about user authentication, see Security Guide.**
- **User Code to enter on User Code Authentication is the numerical value registered in the Address Book as "User Code".**

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

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.

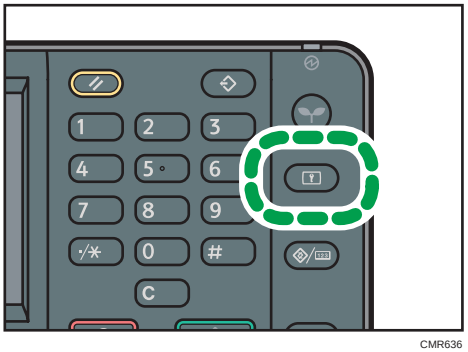
Logging Out Using the Control Panel

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.**



CMR636

2. **Press [Yes].**

Placing Originals

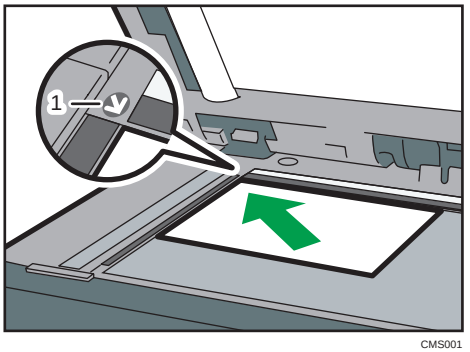
Placing Originals on the Exposure Glass Region A (mainly Europe)

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.
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.



CMS001

1. Positioning mark

3. Lower the ADF or the exposure glass cover.

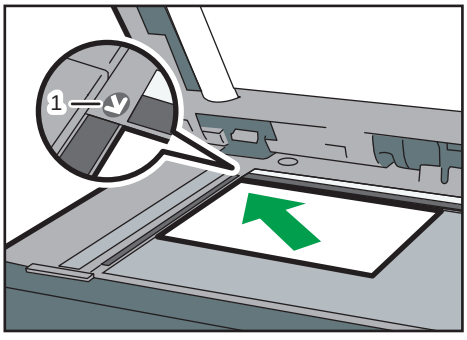
Placing Originals on the Exposure Glass Region A (mainly Asia)

Important

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

1. Lift the ADF.
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.



CMS001

1. **Positioning mark**

3. **Lower the ADF.**

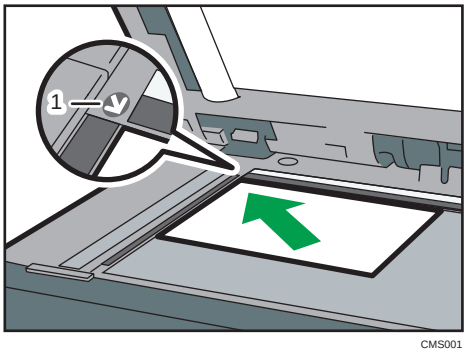
Placing Originals on the Exposure Glass Region B (mainly North America)

Important

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

1. **Lift the ADF.**
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.



CMS001

1. **Positioning mark**

3. **Lower the ADF.**

Placing Originals in the Auto Document Feeder

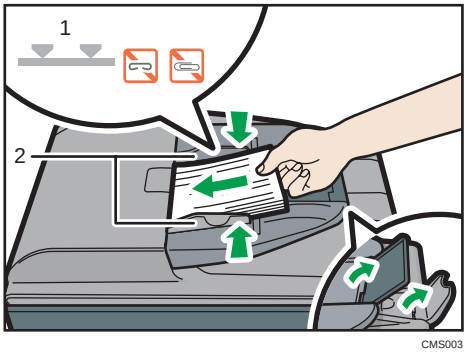
Be sure not to load the original untidily. Doing so may cause the machine to display a paper misfeed message. Also, be sure not to place originals or other objects on the top cover. Doing so may cause a malfunction.

1. **Adjust the original guides 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.

   When placing originals that are longer than A4⬓ or $8^1/_2 \times 11$⬓, open the extenders.



CMS003

1. **Limit mark**
2. **Original guides**

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)

About placing the original on the exposure glass, see p.52 "Placing Originals on the Exposure Glass Region A (mainly Europe)".

Region A (mainly Asia)

About placing the original on the exposure glass, see p.52 "Placing Originals on the Exposure Glass Region A (mainly Asia)".

Region B (mainly North America)

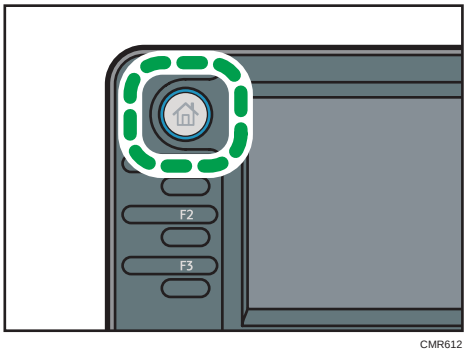
About placing the original on the exposure glass, see p.53 "Placing Originals on the Exposure Glass Region B (mainly North America)".

About placing the original in the ADF, see p.54 "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 "System Settings", Connecting the Machine/ System Settings .

The following procedure explains copying onto paper whose size and orientation matches that of the originals exactly.

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



CMR612

2. **Make sure no previous settings remain.**

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

3. **Select the paper tray containing the paper that is the same size and orientation as the originals.**

4. **Make sure that [Use Paper Tray Settg] is selected.**

   When [Use Paper Tray Settg] is selected, the paper size and orientation of the tray you have selected will appear in [Orig.].

5. **Place the originals.**

6. **Make desired settings.**

7. **Enter the number of copies with the number keys.**

   The maximum copy quantity that can be entered is 99.

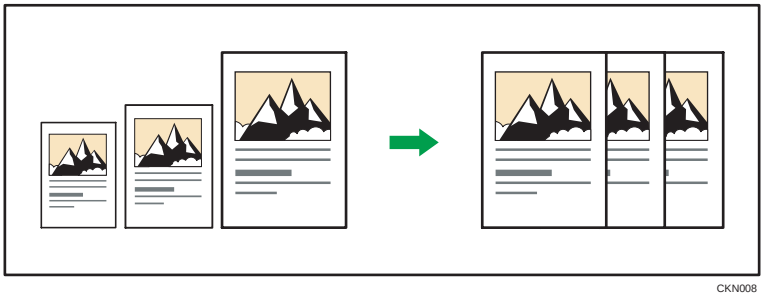
8. **Press the [Start] key.**

   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.

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

Auto Reduce/Enlarge

The machine automatically calculates the reproduction ratio based on the sizes of the originals and the paper you have specified. The machine will rotate, enlarge, or reduce the image of the originals to fit them to the paper.



CKN008

Important

- **You cannot use the bypass tray with this function.**
- **If you select a reproduction ratio after pressing [Auto Reduce/Enlarge], [Auto Reduce/Enlarge] is canceled and the image cannot be rotated automatically.**

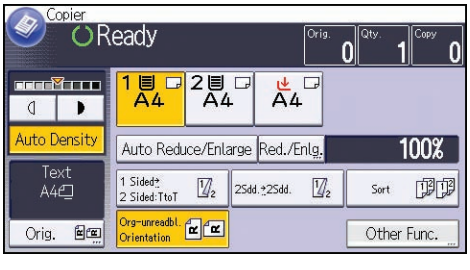
This is useful to copy different size originals to the same size paper.

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 A4 ($8^1/_2 \times 11$)□ originals to fit onto A5 ($5^1/_2 \times 8^1/_2$)□ paper, select a paper tray containing A5 ($5^1/_2 \times 8^1/_2$)□ paper, and then press [Auto Reduce/Enlarge]. The image is automatically rotated.

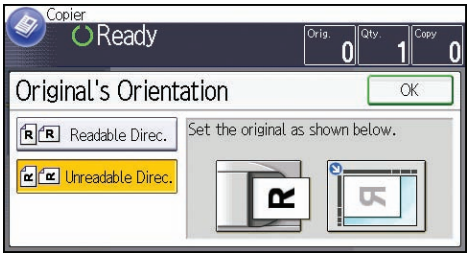
For details about Rotate Copy, see "Rotate Copy", Copy/ Document Server.

1. **Press [Orig.].**



2. **Press [Original's Orientation].**

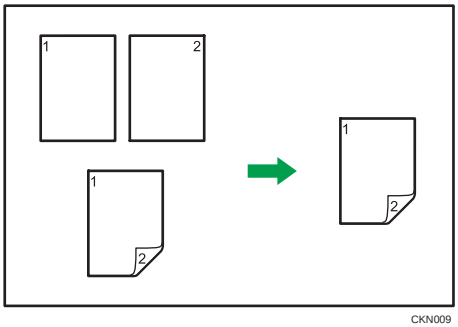
3. Select the original orientation, and then press [OK].



4. Press [Original's Size].
5. Specify the original size, and then press [OK] twice.
6. Press [Auto Reduce/Enlarge].
7. Select the paper tray.
8. 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.



Important

- **You cannot use the bypass tray with this function.**

There are two types of Duplex.

1 Sided → 2 Sided

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

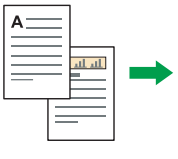
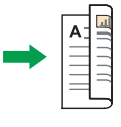
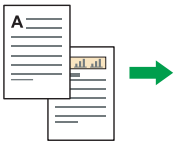
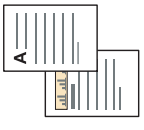
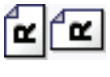
2 Sided → 2 Sided

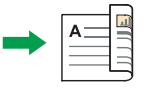
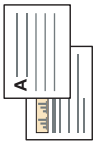
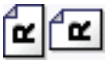
Copies one 2-sided page on one 2-sided page.

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

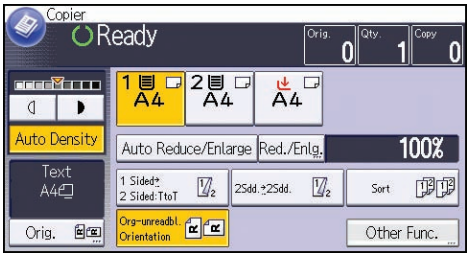
Original orientation and completed copies

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	Orig.'s Orientation	Orientation	Copy
			Top to Top	
			Top to Bottom	

Original	Placing originals	Orig.'s Orientation	Orientation	Copy
			Top to Top	
			Top to Bottom	

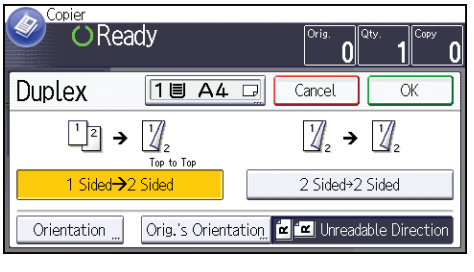
1. **Press [Other Func.].**



2. **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].

   To specify the original orientation is whether readable or unreadable, press [Orig.'s Orientation].

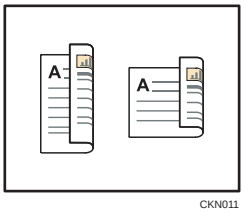


4. **Press [OK] twice.**
5. **Select the paper tray.**
6. **Place the originals, and then press the [Start] key.**

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

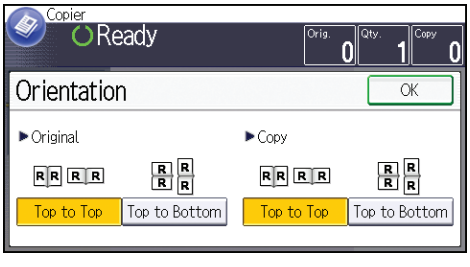


CKN011

- 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

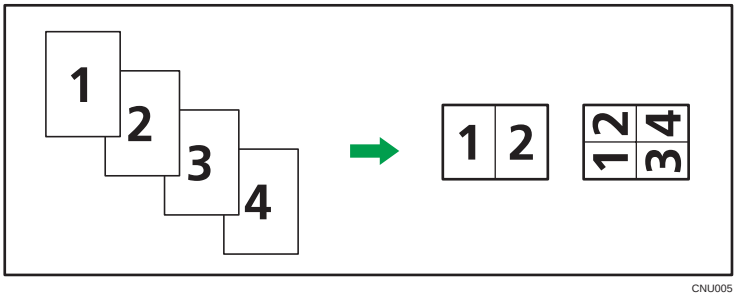
This mode can be used to select a reproduction ratio automatically and copy the originals onto a single sheet of copy paper.

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

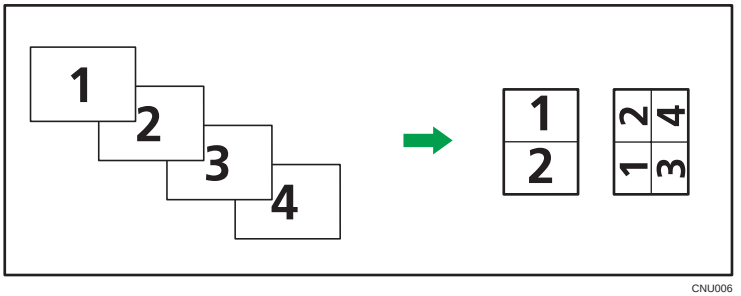
The image position of Combine differs according to original orientation and the number of originals to be combined.

- Portrait (⬓) originals



CNU005

- Landscape (⬓) originals

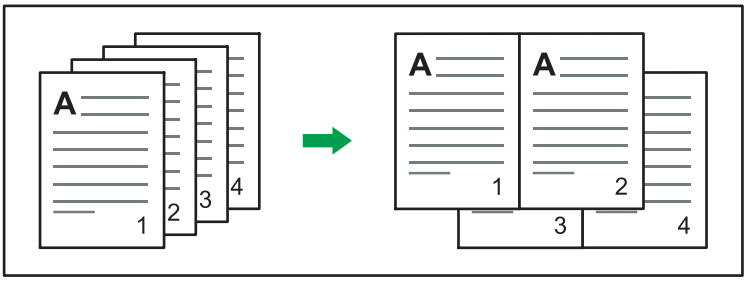


CNU006

Placing originals (originals placed in the ADF)

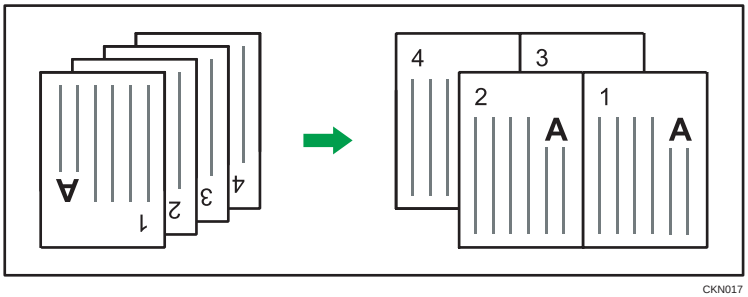
The default value for the copy order in the Combine function is [From Left to Right]. To copy originals from right to left in the ADF, place them upside down.

- 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

Important

- **You cannot use the bypass tray with this function.**

There are four types of One-Sided Combine.

1 Sided 2 Originals → Cmb. 1 Side

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

1 Sided 4 Originals → Cmb. 1 Side

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

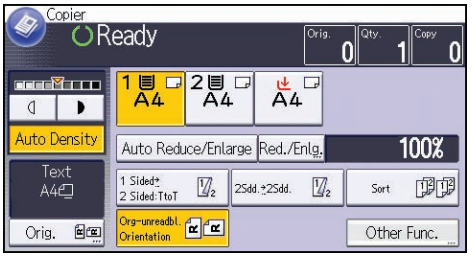
2 Sided 2 Pages → Cmb. 1 Side

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

2 Sided 4 Pages → Cmb. 1 Side

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

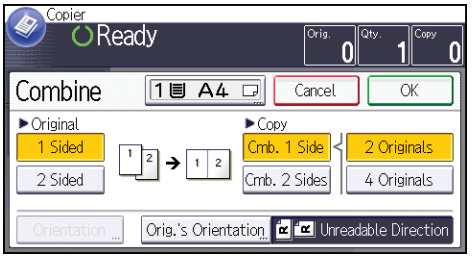
1. **Press [Orig.].**



2. **Press [Original's Size].**
3. **Specify the original size, and then press [OK] twice.**
4. **Press [Other Func.].**
5. **Press [Combine].**
6. **Select [1 Sided] or [2 Sided] for [Original].**

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

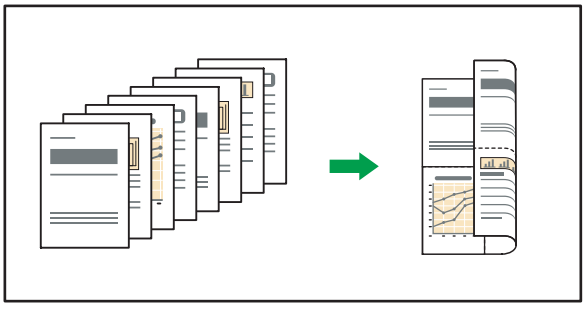
   To specify the original orientation is whether readable or unreadable, press [Orig.'s Orientation].



7. **Press [Cmb. 1 Side].**
8. **Select the number of originals to combine.**
9. **Press [OK] twice.**
10. **Select the paper tray.**
11. **Place the originals, and then press the [Start] key.**

Two-Sided Combine

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



CKN074

Important

- **You cannot use the bypass tray with this function.**

There are four types of Two-Sided Combine.

1 Sided 4 Originals → Cmb. 2 Sides

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

1 Sided 8 Originals → Cmb. 2 Sides

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

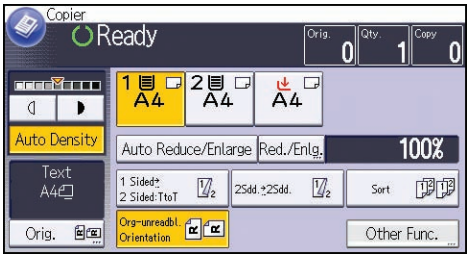
2 Sided 4 Pages → Cmb. 2 Sides

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

2 Sided 8 Pages → Cmb. 2 Sides

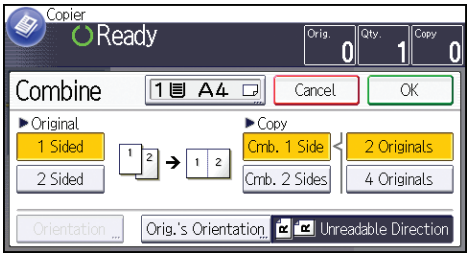
Copies four 2-sided originals to one sheet with four pages per side.

1. **Press [Orig.].**



2. **Press [Original's Size].**
3. **Specify the original size, and then press [OK] twice.**
4. **Press [Other Func.].**
5. **Press [Combine].**
6. **Select [1 Sided] or [2 Sided] for [Original].**

   To specify the original orientation is whether readable or unreadable, press [Orig.'s Orientation].



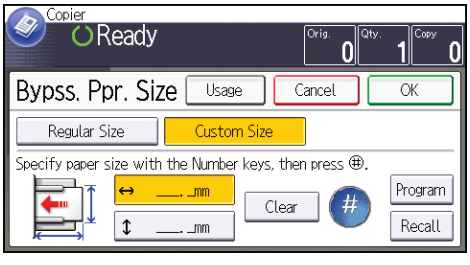
7. Press [Cmb. 2 Sides].
8. Press [Orientation].
9. Select [Top to Top] or [Top to Bottom] for [Original] and/or [Copy], and then press [OK].
10. Select the number of originals to combine.
11. Press [OK] twice.
12. Select the paper tray.
13. Place the originals, and then press the [Start] key.

Copying onto Custom Size Paper from the Bypass Tray

Paper that has a horizontal length of 139.0–600.0 mm (5.48–23.62 inches) and a vertical length of 90.0–216.0 mm (3.55–8.50 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. Envelopes should be fed from the bypass tray.

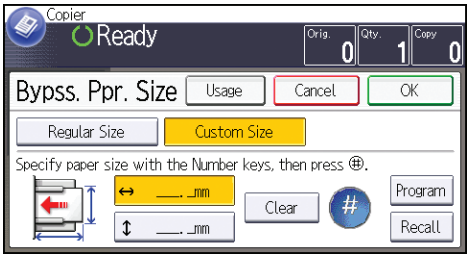
Specify the thickness of the paper according to the weight of the envelopes you are printing on. For details about the relationship between paper weight and paper thickness and the sizes of envelopes that can be used, see p.135 "Recommended Paper Sizes and Types".

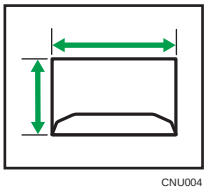
About handling envelopes, supported envelope types, and how to load envelopes, see p.139 "Envelopes".

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.

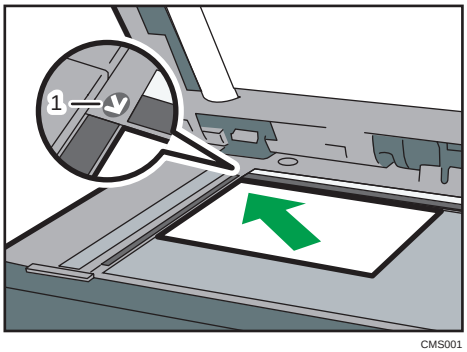




↔: Horizontal

↕: Vertical

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



CMS001

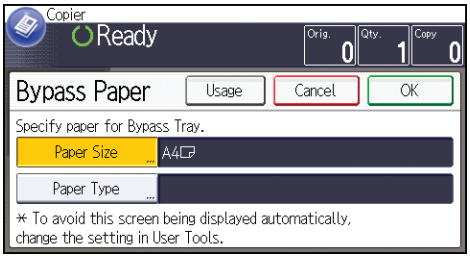
1. **Positioning mark**

2. **Load the envelopes face down in the bypass tray.**

   The bypass tray (⧉) is automatically selected.

3. **Press the [#] key.**

4. **Press [Paper Size].**



5. **Specify the envelope size, and then press [OK].**

6. **Press [Paper Type].**

7. **Press [Thick Paper], and then press [OK].**

8. **Press [OK].**

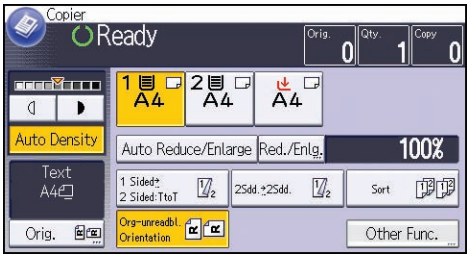
9. **Press the [Start] key.**

Sort

The machine assembles copies as sets in sequential order.

Depending on which options are installed on your machine, this function might not be available. For details, see "Functions Requiring Optional Configurations", Getting Started.

1. **Press [Other Func.].**



2. **Press [Sort], and then press [OK].**
3. **Enter the number of copy sets using the number keys.**
4. **Select the paper tray.**
5. **Place the originals, and then 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.

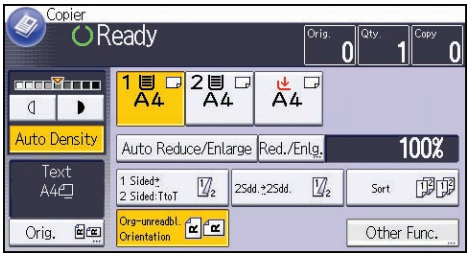
Storing Data in the Document Server

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 from the Document Server screen. For details about the Document Server, see p.115 "Storing Data".

Depending on which options are installed on your machine, this function might not be available. For details, see "Functions Requiring Optional Configurations", Getting Started.

1. **Press [Other Func.].**



2. **Press [▼].**
3. **Press [Store File].**
4. **Enter a file name, user name, or password if necessary.**
5. **Press [OK] twice.**
6. **Select the paper tray.**
7. **Place the originals.**
8. **Make the scanning settings for the original.**
9. **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)

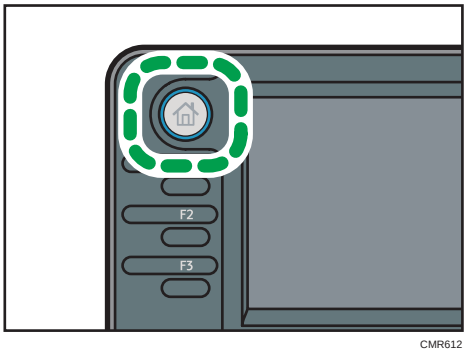
This section describes the basic procedure for transmitting documents using Memory Transmission.

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 12 hours, 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 "Turning Off the Main Power / In the Event of Power Failure", Troubleshooting.

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



CMR612

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

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

4. **Place the original into the ADF.**
5. **Configure the scan and transmission settings in "Send Settings".**
6. **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.
7. **When sending the same original to several destinations (broadcasting), specify the next destination.**
8. **If you send documents to Internet Fax or e-mail destinations or enable the "Email TX Results" function, specify a sender.**
9. **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.**

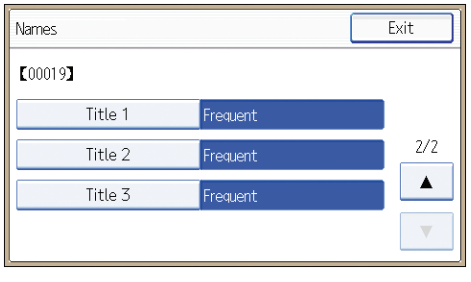
   The machine dials the destination and starts transmission.

Registering a Fax Destination

1. **Press the [User Tools/Counter] key.**
2. **Press [Address Book Mangmnt].**
3. **Press [New Program].**
4. **Press [Names].**
5. **Press [Name].**

   The name entry display appears.

6. **Enter the name, and then press [OK].**
7. **Press [▼] to display [Title 1], [Title 2] and [Title 3].**
8. **Press [Title 1], [Title 2] or [Title 3] to select the key for the classification you want to use.**



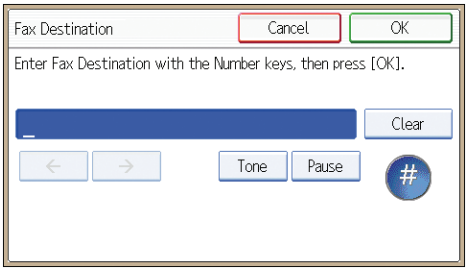
   The keys you can select are as follows:

   - [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 [OK].**
10. **Press [Exit].**
11. **Press [Fax Dest.].**

12. **Press [Fax Destination].**
13. **Enter the fax number using the number keys, and then press [OK].**



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

    To specify [SUB Code], [SEP Code], or [Sub-add./UUI], press [Adv. Features].
15. **Press [OK].**
16. **Press [Exit].**
17. **Press [OK].**
18. **Press the [User Tools/Counter] key.**

Deleting a Fax Destination

Important

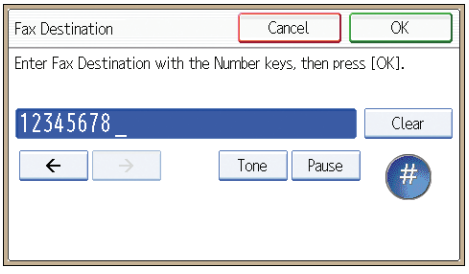
- **If you delete a destination that is a specified delivery destination, messages to its registered Personal Box, for example, cannot be delivered. Be sure to check the settings in the fax function before deleting any destinations.**

1. **Press the [User Tools/Counter] key.**
2. **Press [Address Book Mangmnt].**
3. **Press [Change].**
4. **Press [Fax Dest.].**
5. **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.
6. **Press [Fax Dest.].**
7. **Press [Fax Destination].**

8. **Press [Clear], and then press [OK].**



9. **Press [OK].**
10. **Press [Exit].**
11. **Press [OK].**
12. **Press the [User Tools/Counter] key.**

Transmitting while Checking Connection to Destination (Immediate Transmission)

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

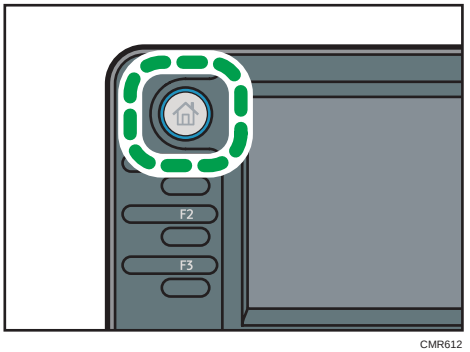
You can specify fax or IP-Fax destinations.

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



CMR612

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.**

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.**

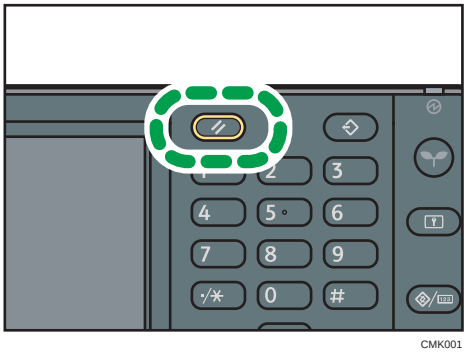
Canceling a Transmission

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. **Press the [Reset] key.**

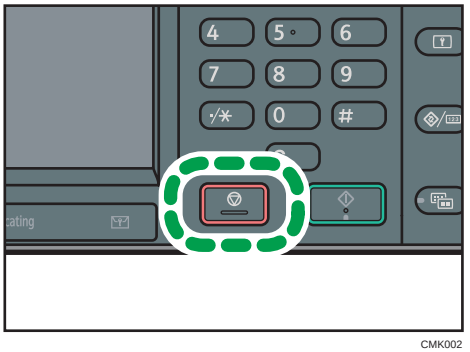


CMK001

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.

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



CMK002

2. **Press [Cancel Scan.] or [Cancel TX].**

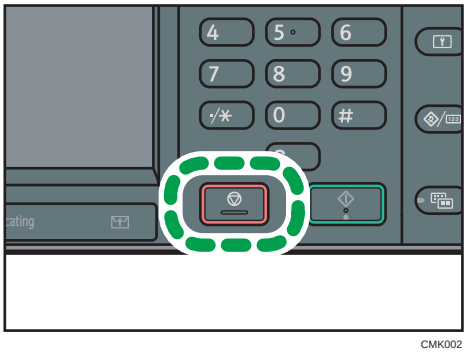
   Depending on the transmission mode and function you use, either [Cancel Scan.] or [Cancel TX] is displayed.

Canceling a Transmission After the Original Is Scanned (While a Transmission Is in Progress)

Use this procedure to delete a file that is being sent after the original is scanned.

All the scanned data is deleted from memory.

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



CMK002

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

2. **Press [Standby File List].**
3. **Select the file you want to cancel.**

   If the desired file is not shown, press [▲] or [▼] to find it.
4. **Press [Cancel TX].**

   To cancel another file, repeat steps 3 through 4.
5. **Press [OK].**
6. **Press [Exit].**

   After pressing [Check/Stop Transmission File] under [Comm. Status/Print] in step 1, press [Exit] twice.

Canceling a Transmission After the Original Is Scanned (Before a Transmission Is Started)

Use this procedure to delete a file stored in memory before its transmission has started.

1. **Press [Comm. Status/Print].**

2. **Press [Check/Stop Transmission File].**
3. **Press [Display File List].**
4. **Select the file you want to cancel.**

   If the desired file is not shown, press [▲] or [▼] to find it.
5. **Press [Cancel TX].**

   To cancel another file, repeat steps 4 through 5.
6. **Press [OK].**
7. **Press [Exit] three times.**

Sending at a Specific Time (Send Later)

Using this function, you can instruct the machine to delay transmission of your fax document until a specified later time.

This allows you to take advantage of off-peak telephone charges without having to be by the machine at the time.

Use Memory Transmission for this function. Immediate Transmission is not possible.

Important

- **If the machine is switched off for about 12 hours, all fax documents stored in memory are lost. If documents are lost for this reason, a Power Failure Report is automatically printed when the main power switch is turned on. Use this report to check the list of lost documents. See "Turning Off the Main Power / In the Event of Power Failure", Troubleshooting.**

1. **Press [Send Settings].**

2. **Press [▼], and then press [Send Later].**
3. **Enter the time, and then press [#].**

   Region A (mainly Europe and Asia)

   Enter the time (24 hour format) using the number keys.

   Region B (mainly North America)

   Enter the time using the number keys, and then select [AM] or [PM].

   When entering numbers smaller than 10, add a zero at the beginning.
4. **Press [OK] 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.

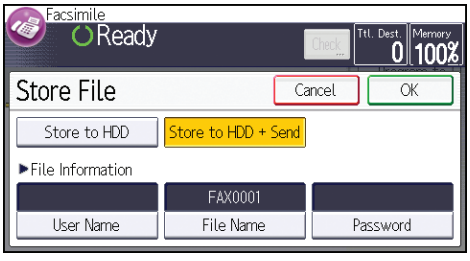
2. **Press [Send Settings].**

3. **Press [▼] three times, and then press [Store File].**
4. **Select [Store to HDD] or [Store to HDD + Send].**

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

   Select [Store to HDD] to store documents.

5. **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].

6. **Press [OK] twice.**
7. **If you have selected [Store to HDD + Send], specify the receiver.**
8. **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 can select the following transmission methods:

Original + Stored File

The machine sends the originals, and then stored files.

Stored file + Original

The machine sends the stored files, and then originals.

This function cannot be used with the following functions:

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

1. **Press [Send Settings].**

2. **Press [▼] four times, and then press [Select Stored File].**
3. **Select the documents to be sent.**

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

   - 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.
4. **If you select a document with a password, enter the password using the number keys, and then press [OK].**
5. **Specify "TX Method" as necessary.**

   Press [TX Method], select [Original + Stored File] or [Stored file + Original], and then press [OK].
6. **Press [OK] twice.**
7. **To add an original to stored documents, place the original, and then select any scan settings you require.**
8. **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.

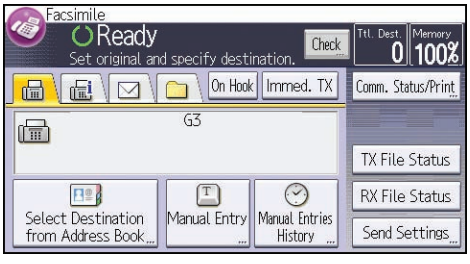
Print per File No.

Prints only the results of communications specified by file number.

Print per User

Prints the results of communications by individual senders.

1. **Press [Comm. 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.

When the machine is connected to a client computer via parallel connection, the printer port is set to [LPT1].

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

   For network connection via TCP/IP, select the machine whose IP address is displayed in [Connect To].

   For parallel connection, select the machine whose printer port is displayed in [Connect To].
7. **Click [Install].**
8. **Configure the user code, default printer, and shared printer as necessary.**
9. **Click [Continue].**

   The installation starts.

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

    When you are prompted to restart your computer, restart it by following the instructions that appear.
11. **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 duplex printing. If you want to print on only one side, select [Off] for the duplex 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. If you want to print multiple copies, specify a number of sets in the "Copies:" box.
10. Click [OK].
11. Start printing from the application's [Print] dialog box.

Locked Print

Sending a Locked Print File

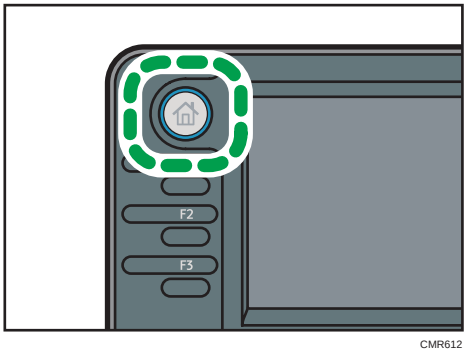
1. Click the WordPad menu button in the upper left corner of the window, and then click [Print].
2. In the "Select Printer" list, select the printer you want to use.
3. Click [Preferences].
4. In the "Job Type:" list, click [Locked Print].
5. Click [Details...].
6. Enter a User ID in the "User ID:" box, and then enter a password in the "Password:" box.
7. Click [OK].
8. Change any other print settings if necessary.
9. Click [OK].
10. Start printing from the application's [Print] dialog box.

Printing a Locked Print File Using the Control Panel

Important

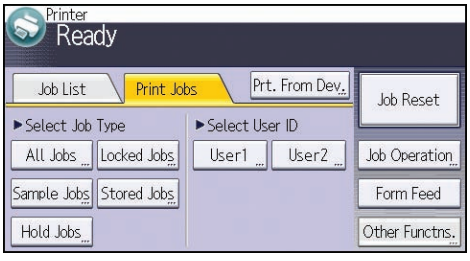
- When printing is completed, the stored file will be deleted.

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



CMR612

2. **Press the [Print Jobs] tab.**



3. **Press [Locked Jobs].**
4. **Select the files you want to print.**

   You can select all the Locked Print files at once by pressing [All Jobs] after selecting a file.
5. **Press [Print].**
6. **Enter the password using the number keys, and then press [OK].**
7. **To change the print settings of the document, press [Det.Settings].**
8. **Enter the number of copies using the number keys if necessary, and then press [Resume Prt.].**

Hold Print

Sending a Hold Print File

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 [Hold Print].
5. Click [Details...].
6. Enter a User ID in the "User ID:" box.

   You can optionally set a file name of a Hold Print file.
7. To specify the print time of the document, select the [Set Print Time] check box, and then specify the time.

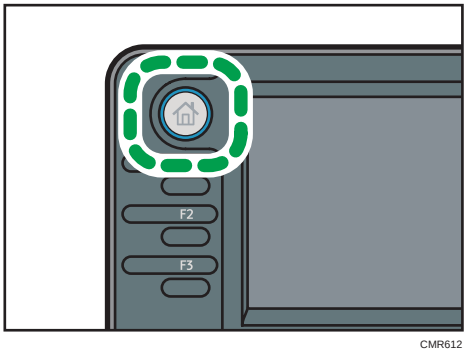
   You can specify the time in 24-hour format.
8. Click [OK].
9. Change any other print settings if necessary.
10. Click [OK].
11. Start printing from the application's [Print] dialog box.

Printing a Hold Print File Using the Control Panel

Important

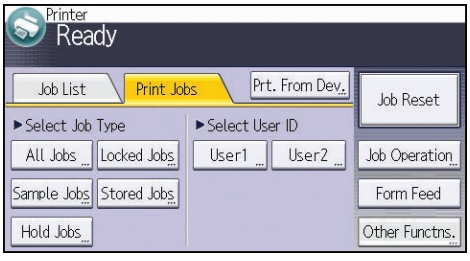
- When printing is completed, the stored file will be deleted.

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



CMR612

2. **Press the [Print Jobs] tab.**



3. **Press [Hold Jobs].**
4. **Select the files you want to print.**

   You can select all the Hold Print files at once by pressing [All Jobs] after selecting a file.
5. **Press [Print].**
6. **To change the print settings of the document, press [Det.Settings].**
7. **Enter the number of copies using the number keys if necessary, and then press [Resume Prt.].**

Stored Print

Sending a Stored Print File

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 the print method to be used for Stored Print files.**

   You can select four methods of Stored Print:

   To use the Stored Print (Shared) and Store and Print (Shared) functions, authentication must be enabled beforehand. For details, see Security Guide.

   - Stored Print

     Stores the file in the machine and prints it later using the control panel.

   - Store and Print

     Prints the file at once and also stores the file in the machine.

   - Stored Print (Shared)

     Stores the file in the machine and allows any user who has print privileges to print the file later using the control panel.

   - Store and Print (Shared)

     Prints the file immediately and also stores the file in the machine. Any user who has print privileges can print any stored file afterward.
5. **Click [Details...].**
6. **Enter a User ID in the "User ID:" box.**

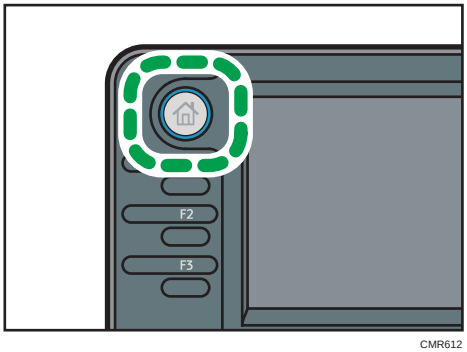
   You can optionally set a file name and a password of a Stored Print file.
7. **Click [OK].**
8. **Change any other print settings if necessary.**
9. **Click [OK].**
10. **Start printing from the application's [Print] dialog box.**

Printing a Stored Print File Using the Control Panel

Important

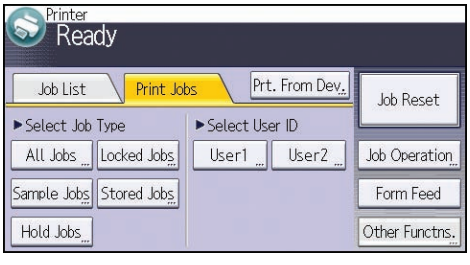
- The stored documents are not deleted even after the printing has been completed. For the procedure to delete the documents, see "Deleting Stored Print files", Print.

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



CMR612

2. **Press the [Print Jobs] tab.**



3. **Press [Stored Jobs].**
4. **Select the files you want to print.**

   You can select all the Stored Print files at once by pressing [All Jobs] after selecting a file.

5. **Press [Print].**

   If you set the password in the printer driver, enter the password.

   If multiple print files are selected, and some of these require a password, the machine prints files that correspond to the entered password and files that do not require a password. The number of files to be printed is displayed on the confirmation screen.

6. **To change the print settings of the document, press [Det.Settings].**
7. **Enter the number of copies using the number keys if necessary, and then press [Resume Prt.].**

Printing Files from an External Memory Device

Direct Printing from a Removable Memory Device

- >>Using the Media Slot
- >>Printable File Formats
- >>Printing from a Removable Memory Device
- >>Screen for Direct Printing

Direct Printing from a Digital Camera (PictBridge)

- >>Using PictBridge
- >>PictBridge Printing
- >>Exiting PictBridge
- >>Supported Functions

Direct Printing from a Removable Memory Device

You can connect removable memory devices (USB flash memory and SD cards) to the machine and directly print the files stored on them.

Files in the following formats can be printed: JPEG, TIFF, and PDF.

This function is useful for printing files without using a computer.

Important

- This feature is available only if the optional hard disk is installed on the machine.

Note

- Large PDF files might not be printable using the PDF direct print function.
- If print jobs through PDF direct printing are being canceled, print using the printer driver from a PDF viewer such as Adobe Reader.

Related Topics

Using the Media Slot
Printable File Formats
Printing from a Removable Memory Device
Screen for Direct Printing

Using the Media Slot

- USB flash memory devices and SD cards are supported for direct printing. However, certain types of USB flash memory devices and SD cards cannot be used. For details, contact your sales or service representative.
- This machine supports SD cards with a maximum capacity of 32 GB.
- USB flash memory devices with password protection or other security features might not be compatible with this machine.
- Connect only USB flash memory to the USB slot; do not connect any other type of USB device.
- Do not use a USB extension cable to connect a USB flash memory to the machine. Insert the USB memory directly into the media slot.
- This machine does not support the use of external USB hubs or SD card readers.
- Do not turn off the machine while a removable memory device is being accessed. Doing so can damage the memory device and corrupt its data.
- If the machine is accidentally turned off while a removable memory device is being accessed, check that the data on the removable memory device has not been corrupted.
- It is possible that any data stored in the removable memory device will be damaged or lost by user error during operation or software error. Be sure to back up of all data beforehand. The manufacturer shall not be liable to you for damages or loss of any data produced by using this function.

Printable File Formats

JPEG files

- Exif version 1.0 or later JPEG files are compatible with this function.

TIFF files

- Following types of TIFF files are compatible with this function: uncompressed TIFF files, or TIFF files compressed using the MH, MR, or MMR method.

PDF files

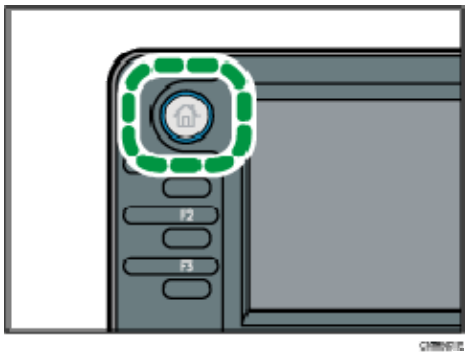
- This function is possible for genuine Adobe PDF files only.
- PDF files whose PDF version is 1.7 (Acrobat 8.0 compatible) or earlier can be printed.
- PDF files created using PDF version 1.5 Crypt Filter functions or more than eight DeviceN Color Space components cannot be printed.
- PDF files created using PDF version 1.6 watermark note functions, or extended optional contents cannot be printed.
- AcroForm is a function specific to PDF version 1.7 and is not supported.

Printing from a Removable Memory Device

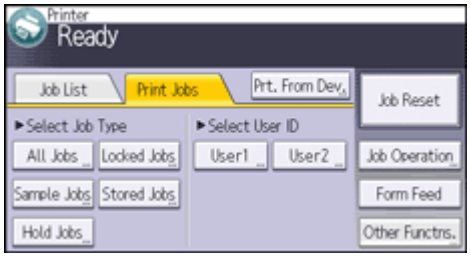
1 Insert a removable memory device into the media slot.

For details about inserting a removable memory device, see "Inserting/Removing a Memory Storage Device", Getting Started.

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



3 Press [Prt. From Dev.].



4 Select the removable memory device that contains the file you want to print.

Only one removable memory device can be selected at a time.

5 Select the file you want to print.

You can simultaneously select multiple files of the same file type in the current folder.

6 If necessary, press [Detailed Sett.] to configure detailed print settings.

Note that certain settings cannot be selected simultaneously.

7 If necessary, press [Preview] to check the print image of the document.

8 Press [Start Printing] or the [Start] key to start printing.

If you start printing a file before the current print job is complete, an error message will appear.

9 When printing is complete, Press [dev. slct.].

10 Remove the removable memory device.

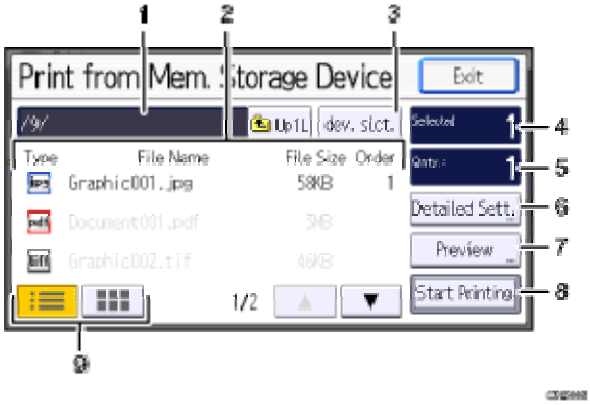
For details about removing a removable memory device, see "Inserting/Removing a Memory Storage Device", Getting Started.

Note

- Depending on the security setting, [Prt. From Dev.] may not appear. For details, see Security Guide
- You cannot select multiple files of different formats at the same time.
- Files or groups of files larger than 1 GB cannot be printed.
- You can select up to 999 JPEG files at once, as long as the total size of the files you select does not exceed 1 GB.
- The machine might print data that appears to be black-and-white in color printing mode. If you need to make sure that the data is printed in black-and-white, specify black-and-white for the print job.
- Paper size is not automatically selected when a JPEG file is selected.
- If you insert another removable memory device while following the procedure above, a list of files and folders in the root directory on that removable memory device will appear.
- If the removable memory device is partitioned, only the files stored on the first partition can be printed.
- If a USB flash memory device is inserted in the media slot, the LED on the slot will light up and remain lit.
- If an SD card is inserted in the media slot, the LED on the slot will light up and remain lit.

Screen for Direct Printing

To display this screen, press the [Home] key on the top left of the control panel, and press the [Printer] icon on the [Home] screen, and then press [Prt. From Dev.]. You can view files either as a list or as thumbnails.



1. **Current folder**

   Displays the name and path of the current folder. To display the contents of the parent folder, press [Up1L].

2. **File/Folder list**

   Press to select the file you want to print or the folder you want to open. Press [▲] or [▼] to scroll through the list if necessary. Depending on the number of files, up to 999 pages might be shown.

   The formats, names, and sizes of files are displayed. If multiple files are selected, the order in which the files were selected will also be displayed.

3. **[dev. slct.]**

   Press to display the removable memory device selection screen.

4. **Selected**

   Displays the number of selected documents (1-999).

5. **Qnty.:**

   Use the number keys to specify the number of the copies (1-999) that you want to print.

6. **[Detailed Sett.]**

   Press to configure detailed print settings.

7. **[Preview]**

Press to display the print image of the 1st page of the selected document. You can change the scale factor and display position of the print image.

8. [Start Printing]

Press to print the selected file.

9. List/Thumbnail

Press to switch between list view and thumbnail view.

Note

- The machine can recognize up to a total of 5990 files and folders in a removable memory device.
- File names must not exceed 255 bytes (including the path name). Also, file names must not contain any character that the machine cannot display correctly.
- JPEG format files can be displayed as thumbnails when they are in Exif or DCF format. An icon will be shown for any other type of file.
- Following sizes of JPEG files can be printed:
  - Standard sizes: 8 × 10", Letter ($8^1/_2$ × 11"), A4, A5, A6, B5, B6
  - Custom sizes: 2L (5 × 7"), Postcard, 100 mm × 150 mm, 4 × 6"
- Custom size PDF files may not be printed using this function.
- Print settings are effective for the format of the currently selected file, and will remain effective as long as the file of that format stays selected.
- The machine will remember an entered PDF password until you switch out of the printer function.
- If you try to select a removable memory device that the machine has not recognized correctly, an error message will appear.

Direct Printing from a Digital Camera (PictBridge)

You can connect a PictBridge-compatible digital camera to this machine using a USB cable. This allows you to print photographs taken using the digital camera directly by operating the digital camera.

Related topics

Using PictBridge
PictBridge Printing
Exiting PictBridge
Supported Functions

Using PictBridge

- Check your digital camera is PictBridge-compatible.
- To use this function, the optional Camera Direct Print Card must be installed on the machine.
- Use the USB cable bundled to your digital camera.
- Do not disconnect the USB cable while data is being sent. If you do, printing will fail.
- Up to 999 images can be sent from the digital camera to the machine during one print transaction. If an attempt is made to send more images, an error message is sent to the camera and printing fails.
- The number of copies that can be printed at one time depends on the digital camera that you are using. For details, see the manual provided with the digital camera.
- Since printing conditions are specified on the digital camera, specifiable parameters depend on the particular digital camera. For details, see your digital camera's manual.

PictBridge Printing

1 Check the machine and the digital camera are both switched on.

2 Using a USB cable, connect the digital camera to the machine's USB host interface or the media slot.

For details about connecting the digital camera to the machine's USB host interface, see "Connecting a Device to the Machine's USB Host Interface", Connecting the Machine/ System Settings. For details about connecting the device via the media slot, see "Inserting/Removing a Memory Storage Device", Getting Started.

3 On your digital camera, select the images you want to print, and specify the printing conditions.

4 The machine receives settings from the digital camera and starts printing.

Note

- Since printing conditions are specified on the digital camera, specifiable meters depend on the particular digital camera. For details, see your digital camera's manual.

- Some digital cameras require settings for manual PictBridge operation. For details, see your digital camera's manual.

Exiting PictBridge

Important

- Do not disconnect the USB cable while data is being sent to the machine. If you do, printing will fail.

1. **Check the control panel of this machine is displaying the "Ready" state.**
2. **Disconnect the USB cable from the machine.**

Supported Functions

This machine can perform the following functions using its PictBridge feature.

The settings available for these functions are as follows:

- Single image printing
- Selected image printing
- All image printing
- Index printing
- Trimming
- Date and file name printing
- Paper size
- Image print size
- Multi-Image-Layout
- Duplex printing
- Printing quality
- Color matching
- Paper type specification
- Form printing
- Toner saving
- Camera memo printing

Note

- This machine does not support the following settings:
  - DPOF printing
  - Margin-less printing
- The setting parameters and their names may vary depending on the digital camera. For details, see your digital camera's manual.

6. Scan

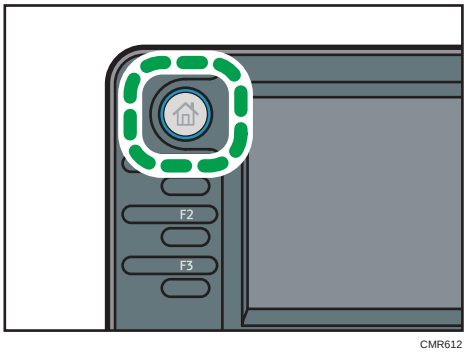
This chapter describes frequently used scanner functions and operations. For the information not included in this chapter, see Scan on the supplied CD-ROM.

Basic Procedure When Using Scan to Folder

Important

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

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

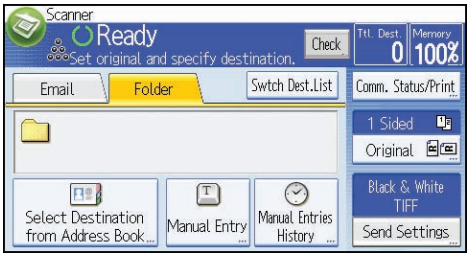


CMR612

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, select [Send Settings] or [Original], and specify scan settings according to the original you want to scan.**

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

- Press [Original], and then press [2 Sided].
- Press [Send Settings]. Select [Type of Original], and then press [Full Colour].
- Press [Send Settings]. Select [File Type], and then press [PDF].

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

1. **Confirm the user name and the name of the computer you will send scanned documents to.**
2. **On the [Start] menu, point to [All Programs], then [Accessories], and then click on [Command Prompt].**
3. **Enter the command "ipconfig/all", and then press the [Enter] key.**
4. **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.

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

   The user name is displayed under [USERNAME].

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

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:

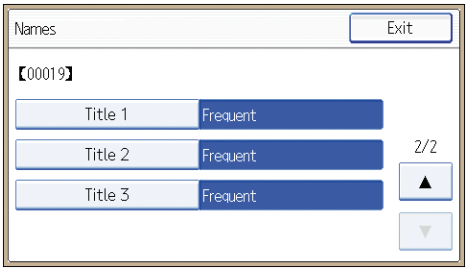
1. **Right-click the folder created in step 2, and then click [Properties].**
2. **On the [Security] tab, select [Edit...].**
3. **Click [Add...].**
4. **In the [Select Users or Groups] window, click [Advanced...].**
5. **Specify one or more object types, select a location, and then click [Find Now].**
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. **Press [OK] twice.**

Registering an SMB Folder

1. **Press the [User Tools/Counter] key.**
2. **Press [Address Book Mangmnt].**
3. **Press [New Program].**
4. **Press [Names].**
5. **Press [Name].**

   The name entry display appears.
6. **Enter the name, and then press [OK].**
7. **Press [▼] to display [Title 1], [Title 2] and [Title 3].**
8. **Press [Title 1], [Title 2] or [Title 3] to select the key for the classification you want to use.**

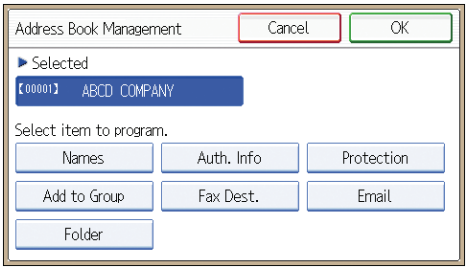


   The keys you can select are as follows:

   - [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.

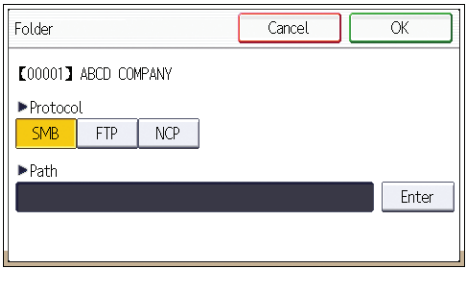
   You can select [Frequent] and one more key for each title.
9. **Press [OK].**
10. **Press [Exit].**

11. **Press [Auth. Info].**



12. **Press [Folder Authentication].**
13. **Press [Specify Other Auth. Info].**

    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.
14. **Press [Change] under "Login User Name".**
15. **Enter the login user name of the destination computer, and then press [OK].**
16. **Press [Change] under "Login Password".**
17. **Enter the password of the destination computer, and then press [OK].**
18. **Enter the password again to confirm, and then press [OK].**
19. **Press [OK].**
20. **Press [Exit].**
21. **Press [Folder].**
22. **Check that [SMB] is selected.**



23. **Press [Enter] under "Path".**
24. **Press [Enter] 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.
25. **Press [Connection Test] to check the path is set correctly.**
26. **Press [Exit].**

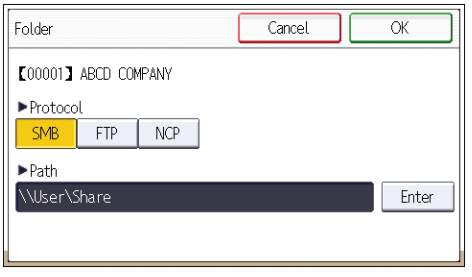
    If the connection test fails, check the settings, and then try again.

27. **Press [OK] three times.**
28. **Press the [User Tools/Counter] key.**

Locating the SMB folder manually

1. **Press [Enter] 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] four times.**

   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

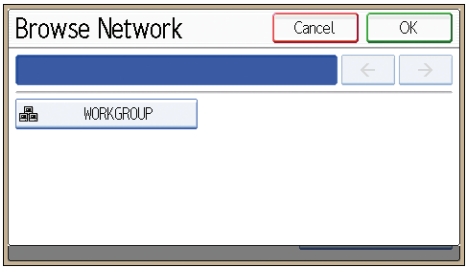
1. **Press [Browse Network].**

   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] four times.**

Deleting an SMB Registered Folder

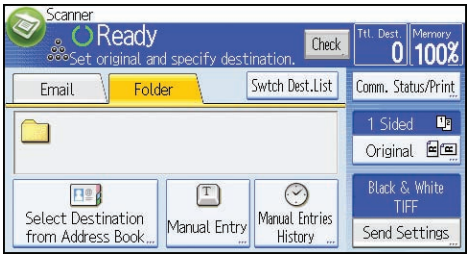
1. **Press the [User Tools/Counter] key.**
2. **Press [Address Book Mangmnt].**
3. **Press [Change].**
4. **Press [Folder].**
5. **Select the name whose folder you want to delete.**

   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.
6. **Press [Folder].**
7. **Press the protocol which is not currently selected.**
8. **Press [OK] twice.**
9. **Press the [User Tools/Counter] key.**

Entering the Path to the Destination Manually

1. **Press [Manual Entry].**



2. **Press [SMB].**
3. **Press [Enter] in [Destination].**
4. **Press [Enter] on the right side of the path field.**
5. **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`
6. **Press [OK].**
7. **Depending on the destination setting, enter the user name for logging in to the computer.**

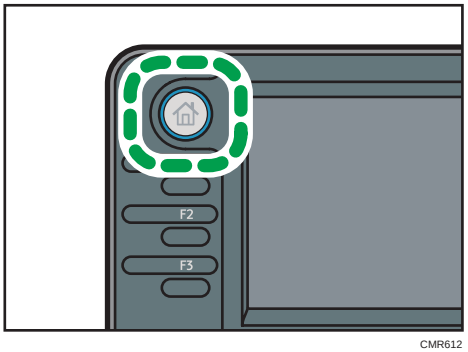
   Press [Enter] to the right of the user name field to display the soft keyboard.
8. **Depending on the destination setting, enter the password for logging in to the computer.**

   Press [Password] for the password to display the soft keyboard.
9. **Press [Connection Test].**

   A connection test is performed to check whether the specified shared folder exists.
10. **Check the connection test result, and then press [Exit].**
11. **Press [OK].**

Basic Procedure for Sending Scan Files by E-mail

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

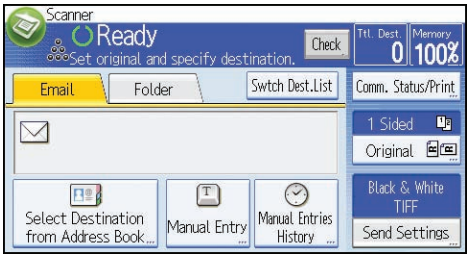


CMR612

2. **Make sure that no previous settings remain.**

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

3. **Press the [Email] tab.**



4. **Place originals.**
5. **If necessary, select [Send Settings] or [Original], and specify scan settings according to the original you want to scan.**

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

   - Press [Original], and then press [2 Sided].
   - Press [Send Settings]. Select [Type of Original], and then press [Full Colour].
   - Press [Send Settings]. Select [File Type], and then press [PDF].

6. **Specify the destination.**

   You can specify multiple destinations.

7. **Press [▼] in [Send Settings] twice, select [Sender Name], and then specify the e-mail sender (originator).**

8. **To use the Message Disposition Notification function, select [Send Settings], press [▼] four times, and then press [Reception Notice].**

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

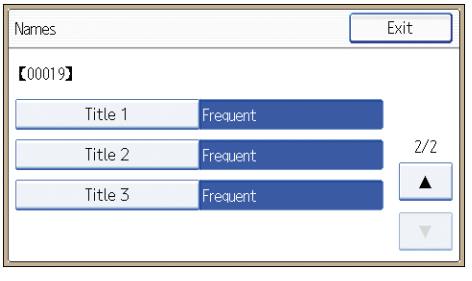
9. **Press the [Start] key.**

Registering an E-mail Destination

1. **Press the [User Tools/Counter] key.**
2. **Press [Address Book Mangmnt].**
3. **Press [New Program].**
4. **Press [Names].**
5. **Press [Name].**

   The name entry display appears.

6. **Enter the name, and then press [OK].**
7. **Press [▼] to display [Title 1], [Title 2] and [Title 3].**
8. **Press [Title 1], [Title 2] or [Title 3] to select the key for the classification you want to use.**



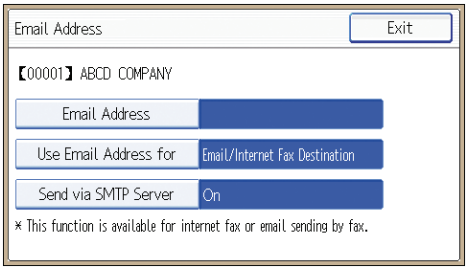
   The keys you can select are as follows:

   - [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 [OK].**
10. **Press [Exit].**
11. **Press [Email].**

12. **Press [Email Address].**



13. **Enter the e-mail address.**

14. **Press [OK].**
15. **Press [Use Email Address for], and then select [Email/Internet Fax Dest.] or [Internet Fax Destination Only].**

    If [Email/Internet Fax Dest.] is specified, registered e-mail addresses appear in both the 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 the internet fax display on the fax function screen.

16. **Press [OK].**
17. **If you want to use Internet fax, press [Send via SMTP Server], and set to [On].**
18. **Press [OK].**
19. **Press [Exit].**
20. **Press [OK].**
21. **Press the [User Tools/Counter] key.**

Deleting an E-mail Destination

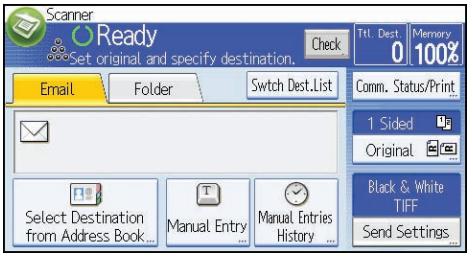
1. **Press the [User Tools/Counter] key.**
2. **Press [Address Book Mangmnt].**
3. **Press [Change].**

4. **Press [Email].**
5. **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.
6. **Press [Email].**
7. **Press [Email Address].**
8. **Press [Delete All], and then press [OK].**
9. **Press [Exit].**
10. **Press [OK].**
11. **Press the [User Tools/Counter] key.**

Entering an E-mail Address Manually

1. **Press [Manual Entry].**



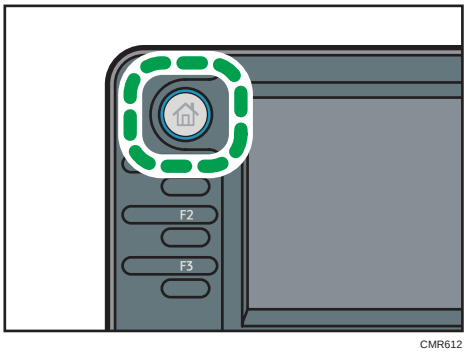
2. **Press [Enter] under [Destination].**
3. **Enter the e-mail address.**
4. **Press [OK].**

Basic Procedure for Storing Scan Files

Important

- You can specify a password for each stored file. Files that are not password-protected can be accessed by other users on the same local area network using DeskTopBinder. 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. For long-term storage of files, we recommend the use of DeskTopBinder. For details, contact your local dealer, or see the documentation for DeskTopBinder.

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



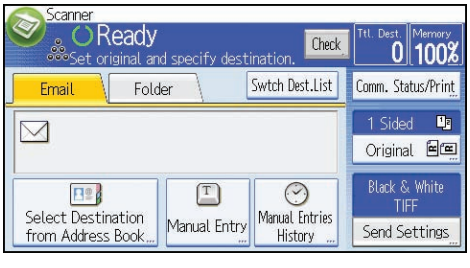
CMR612

2. **Make sure that no previous settings remain.**

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

3. **Place originals.**

4. **Press [Send Settings].**



5. **Press [▼] four times, and then press [Store File].**

6. **Press [Store to HDD].**

7. **If necessary, specify file information, such as [User Name], [File Name], and [Password].**

   - 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

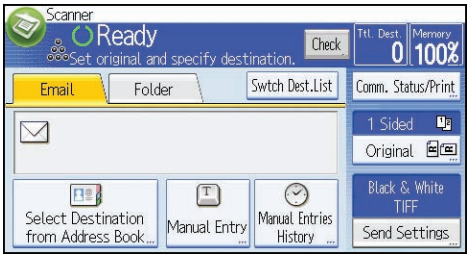
  Press [Password], enter a password, and then press [OK]. Re-enter the password for confirmation, and then press [OK].

8. **Press [OK] twice.**
9. **If necessary, press [Send Settings] or [Original] to configure settings for resolution and scan size.**
10. **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 [Send Settings].**



2. **Press [▼] four times, and then press [Select/Manage Stored File].**
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 removable memory device.

You can select one of the following file types:

- Single Page: [PDF], [High Compress. PDF], [PDF/A], [TIFF/JPEG]

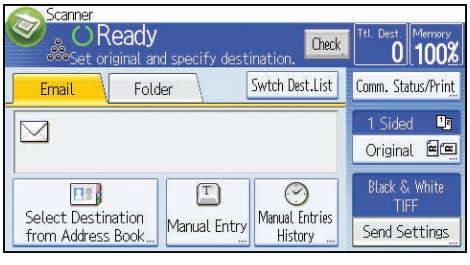
  If you select a single-page file type when scanning multiple originals, one file is created for each single page and the number of files sent is the same as the number of pages scanned.

- Multi-page: [PDF], [High Compress. PDF], [PDF/A], [TIFF]

  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.

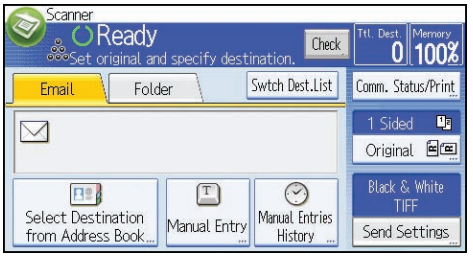
1. **Press [Send Settings].**



2. **Press [File Type].**
3. **Select a file type.**
4. **Press [OK] twice.**

Specifying Send Settings

1. **Press [Send Settings].**



2. **Specify resolution, scan size, and other settings, as required.**
3. **Press [OK].**

Storing the Scanned Documents to a USB Flash Memory or SD Card

This section explains how to save data on external media using the scanner function.

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.

Important

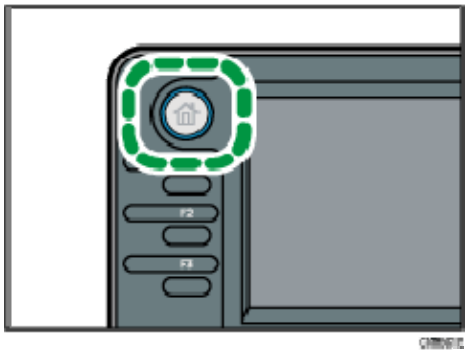
- For details about the optional units required for this function, see "Functions Requiring Optional Configurations", Getting Started.

Basic Procedure for Saving Scan Files on a Removable Memory Device

Important

- This machine supports FAT16 or FAT32 format USB flash memory and SD cards. Other forms of removable memory device are not compatible.
- SD cards with storage capacity up to 32GB can be used.
- Make sure that the format of the removable memory device is FAT16 or FAT32.
- Saving might fail if the USB flash memory features password protection or other security features.
- Connect only USB flash memory to the USB slot, not any other form of USB device.
- Do not use a USB extension cable to connect a USB memory to the machine. Insert the USB memory directly into the media slot.
- Do not remove the media while data is being written. Doing so will result in corrupted data.
- Do not turn the machine's main power switch to off while data is being written. Doing so will result in corrupted data.
- If the machine's main power is accidentally switched off while data is being written, you must check the data on your media for corruption when you switch the machine back on.
- USB flash memory devices and SD cards are supported for direct printing. However, certain types of USB flash memory devices and SD cards cannot be used. For details, contact your sales or service representative.

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



2 Insert a removable memory device in the media slot.

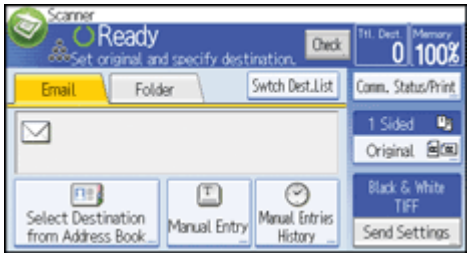
You can connect only one removable memory device at a time. The media slot cannot be used if both an SD card and a USB flash memory are inserted into it at the same time.

3 Make sure that no previous settings remain.

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

4 Place originals.

5 Press [Send Settings].



6

6 Press [▼] three times, and then press [Store File].

7 Press [Store to Memory Device].

8 Press [OK] twice.

9 If necessary, select [Send Settings] or [Original], and 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 [Original], and then press [2 Sided].
- Press [Send Settings]. Select [Type of Original], and then press [Full Colour].
- Press [Send Settings]. Select [File Type], and then press [PDF].

For information about other settings, see Various Scan Settings.

10 Press the [Start] key.

When scanning batches, place subsequent originals after the scan files have been sent.

When writing is complete, a confirmation message appears.

11 Press [Exit].

12 Remove the memory device from the media slot.

Remove the media from the media slot only after data has been written completely. Removing the media while data is being written will result in corrupted data.

Note

- The amount of time required to save files to a USB flash memory device or SD card will vary according to the device's specifications.
- The documents stored on the removable media device can be printed from the machine's control panel. For details, see "Printing Files from an External Memory Device", Print.
- The documents stored on the removable media device cannot be sent from the machine's control panel.
- Depending on the security settings, [Store to Memory Device] may not be displayed. Consult your administrator.
- You cannot specify where the data is saved. Files are saved in the root directory of the removable memory device.
- If the removable memory device is partitioned, files are saved on the first partition.
- You cannot configure file information such as [User Name], [File Name], and [Password].
- The amount of free space on the memory device is displayed. Note that if the amount of free space exceeds 10 GB, "9999.99 MB" will be displayed.
- To cancel writing, press the [Stop] key. If files are being written when writing is cancelled, any partially written files are deleted. Only complete files are stored on the removable memory device.

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.

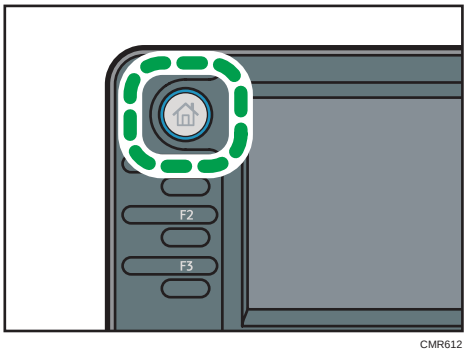
User Name

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 key 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 [Home] screen.**



2. **Press [To Scanning Scrn.].**
3. **Press [User Name].**
4. **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.
5. **Press [File Name].**
6. **Enter a file name, and then press [OK].**
7. **Press [Password].**
8. **Enter a password with the number keys, and then press [OK].**

   You can use four to eight digits for the password.
9. **For double-check, enter the password again, and then press [OK].**
10. **Select the paper tray.**
11. **Place the original.**
12. **Specify the original scanning conditions.**
13. **Press the [Start] key.**

    The original is scanned. The document is saved in the Document Server.

    After scanning, a list of stored documents will be displayed. If the list does not appear, press [Finish Scanning].

Printing Stored Documents

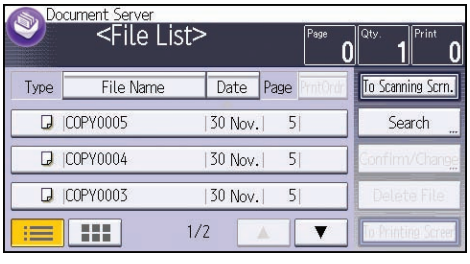
Prints stored documents on the Document Server.

The items you can specify on the printing screen are as follows:

- Paper tray
- The number of prints
- [2 Sided: Top to Top], [2 Sided: Top to Bottom]
- [Sort]
- [Margin Adjustment]

For details about each function, see Copy/ Document Server.

1. **Select a document to be printed.**



2. **When printing two or more documents at a time, repeat step 1.**

   Up to 30 documents can be printed.

3. **When specifying printing conditions, press [To Printing Screen], and then configure print settings.**
4. **Enter the number of print copies with the number keys.**

   The maximum quantity that can be entered is 99.

5. **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".**

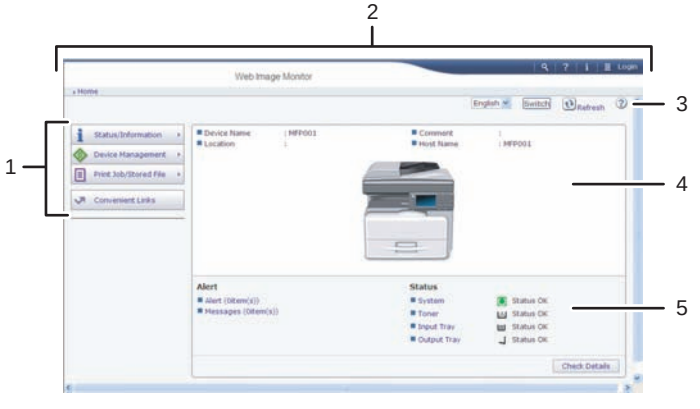
1. **Start your Web browser.**
2. **Enter "http://(machine's IP address or host name)/" in your Web browser's URL bar.**

   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:



CMM004

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.

Viewing Received Fax Documents Using Web Image Monitor

1. **Start Web Image Monitor.**
2. **Click [Fax Received File] on the [Print Job/Stored File] menu in the left pane.**
3. **If you have programmed a user code for the stored reception file, enter the code, and then press [OK].**

   If the programmed user code was deleted from the Address Book, a message indicating incorrect user code entry appears. If this is the case, reprogram a user code.
4. **Click the property icon of the desired fax document.**
5. **View the content of the fax document.**
6. **To download the received fax document, select [PDF], [PDF/A], or [Multi-page: TIFF], and then click [Download].**

   When you select [PDF], make the necessary "PDF File Security Settings" before clicking [Download]. Adobe Acrobat Reader/Adobe Reader starts and the selected document is displayed.
7. **Quit Web Image Monitor.**

9. Adding Paper and Toner

This chapter describes how to load paper into the paper tray and recommended paper sizes and types.

Loading Paper into Paper Trays

Important

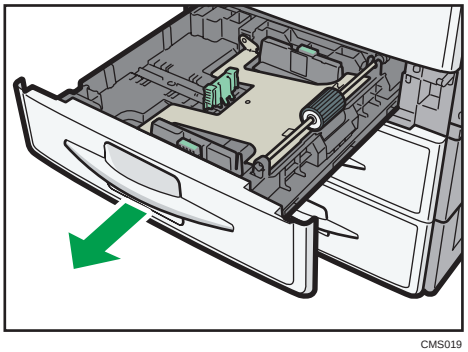
- If a paper tray is pushed vigorously when putting it back into place, the position of the tray's side fences may slip out of place.
- Check the paper edges are aligned at the right side.
- When loading a low number of sheets, be sure not to squeeze the side fences in too tightly. If the side fences are squeezed too tightly against the paper, the edges may crease or the paper may be misfed.

Note

- Various sizes of paper can be loaded in the paper trays by adjusting the positions of side fences and end fence. For details, see "Changing the Paper Size in the Paper Trays", Paper Specifications and Adding Paper.

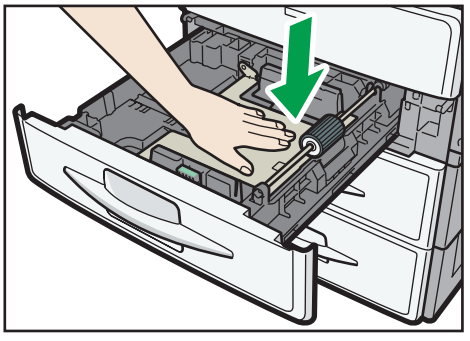
Loading Paper into Tray 1

1. Carefully pull out the paper tray until it stops.



CMS019

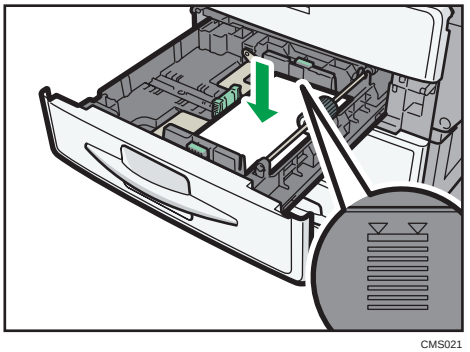
2. **Press the metal plate down until it clicks.**



CMS020

3. **Square the paper and load it print side up.**

   Do not stack paper over the limit mark.



CMS021

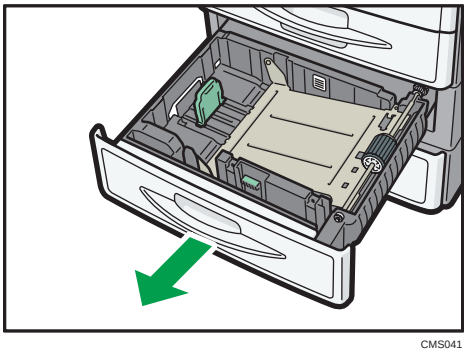
4. **Carefully slide the paper tray fully in.**

Loading Paper into Trays 2 and 3

Each paper tray is loaded in the same way.

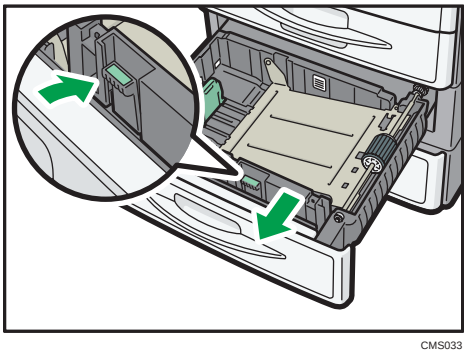
In the following example procedure, paper is loaded into tray 2.

1. **Carefully pull out the paper tray until it stops.**



CMS041

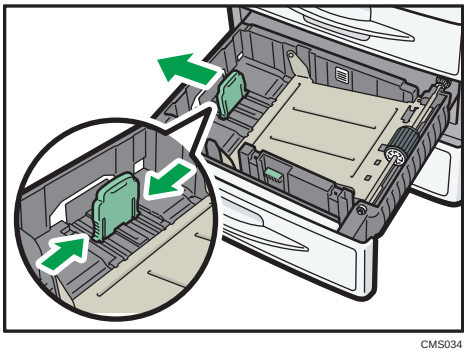
2. **While pressing down the release lever of the side fence, slide the side fence outward.**



CMS033

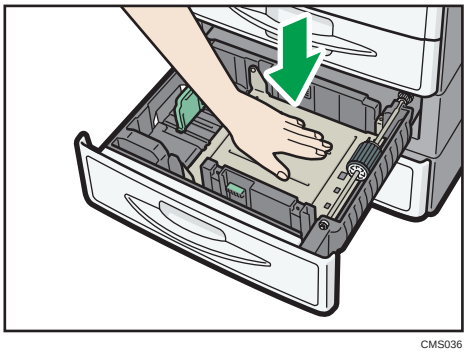
If the paper size that is loaded is $8\frac{1}{4} \times 14$ or $8\frac{1}{2} \times 14$, proceed to step 4.

3. **While pinching the release levers of the end fence, slide the end fence outward.**



CMS034

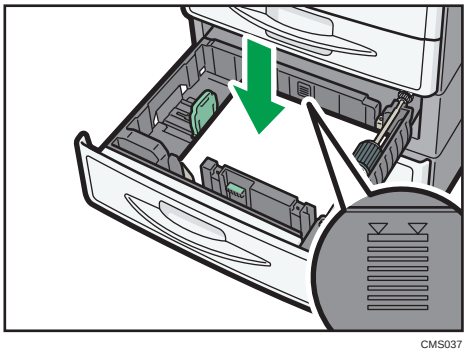
4. **Press the metal plate down until it clicks.**



CMS036

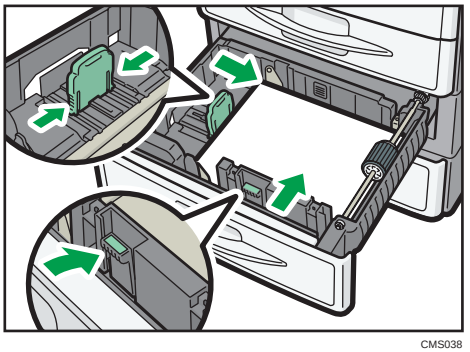
5. **Square the paper and load it print side up.**

   Do not stack paper over the limit mark.



CMS037

6. **Align the back and side fences gently against the paper you loaded.**



CMS038

7. **Carefully slide the paper tray fully in.**

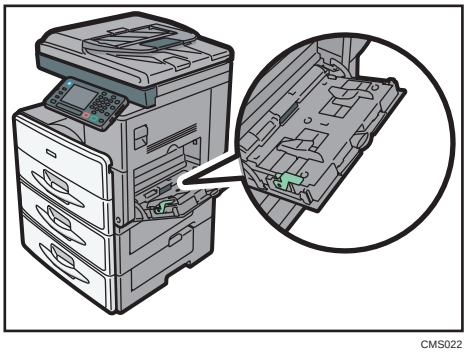
Loading Paper into the Bypass Tray

Use the bypass tray to use OHP transparencies, adhesive labels, translucent paper, and paper that cannot be loaded in the paper trays.

Important

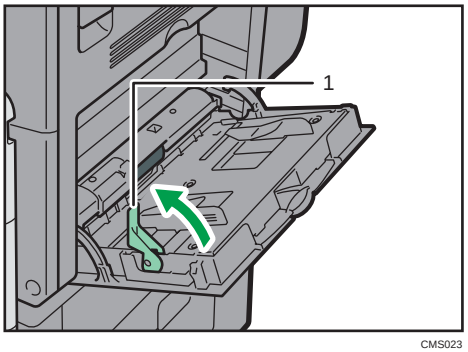
- **The maximum number of sheets you can load at the same time depends on paper type. Do not load paper over the limit mark. For the maximum number of sheets you can load, see p.135 "Recommended Paper Sizes and Types".**

1. **Open the bypass tray.**



CMS022

2. **Push up the release lever.**

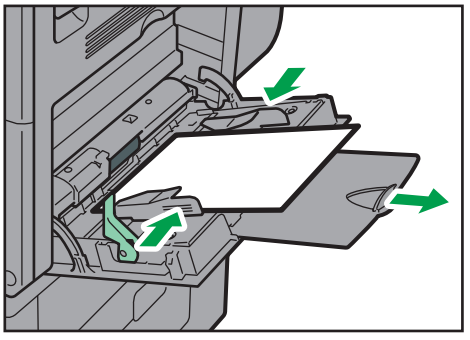


CMS023

1. **Release lever**

3. **Insert the paper face down.**
4. **Align the paper guides to the paper size.**

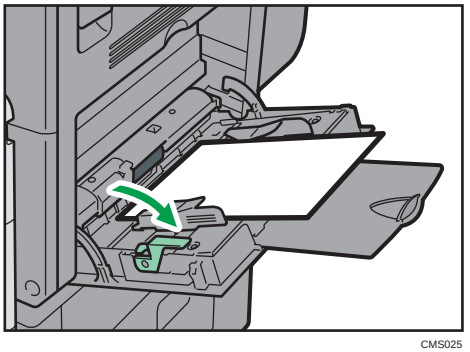
   If the guides are not flush against the paper, images might be skewed or paper misfeeds might occur.



CMS024

5. **Push down the release lever.**

A beeping sound will occur after the paper is inserted and the release lever is pushed down.



CMS025

Note

- When you use the bypass tray, it is recommended to load the paper in ▭ orientation.
- When copying from the bypass tray, see "Copying from the Bypass Tray", Copy/ Document Server. When printing from a computer, see p.129 "Settings to Use the Bypass Tray under the Printer Function".
- 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 paper in the bypass tray.
- When the [Panel Key Sound] is turned off, it will not sound if you load paper into the bypass tray. For details about [Panel Key Sound], see "System Settings", Connecting the Machine/ System Settings.
- When loading thick paper or OHP transparencies, specify the paper size and the paper type.
- Letterhead paper must be loaded in a specific orientation. For details, see, p.132 "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 p.139 "Envelopes".

Settings to Use the Bypass Tray under the Printer Function

Important

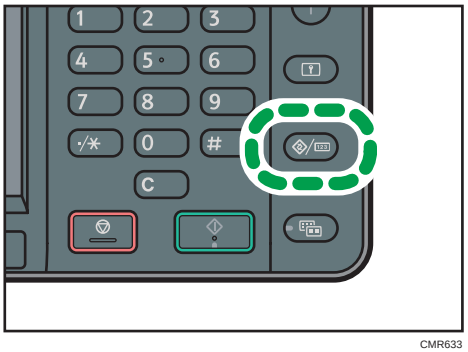
- **If you select [Machine Setting(s)] in [Bypass Tray] under [Tray Setting Priority] in [System] of the Printer Features menu, the settings made using the control panel have priority over the printer driver settings. For details, see "System", Print.**
- **The default setting of [Bypass Tray] is [Driver/Command].**

Note

- Settings remain valid until they are changed. After printing, be sure to clear settings for the next user.
- For details about setting printer drivers, see "Printing Documents", Print.
- Region A (mainly Europe and Asia)
  - [A4] is the default setting for [Printer Bypass Paper Size].
- Region B (mainly North America)
  - [$8\frac{1}{2} \times 11$] is the default setting for [Printer Bypass Paper Size].

Setting the paper size using the control panel

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



CMR633

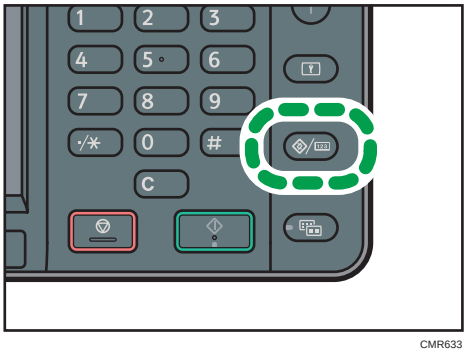
2. **Press [Tray Paper Settings].**
3. **Press [▼].**
4. **Press [Printer Bypass Paper Size].**
5. **Select the paper size.**
6. **Press [OK].**
7. **Press the [User Tools/Counter] key.**

Note

- When loading thick paper or OHP transparencies, specify the paper size and the paper type.

Setting custom size paper using the control panel

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



CMR633

2. Press [Tray Paper Settings].
3. Press [▼].
4. Press [Printer Bypass Paper Size].
5. Press [Custom Size].

   If a custom size is already specified, press [Change].
6. Press [Vertical].
7. Enter the size of the paper using the number keys, and then press the [#] key.
8. Press [Horizontal].
9. Enter the size of the paper using the number keys, and then press the [#] key.
10. Press [OK] twice.
11. Press the [User Tools/Counter] key.

Note

- When loading thick paper, specify the paper size and the paper type.

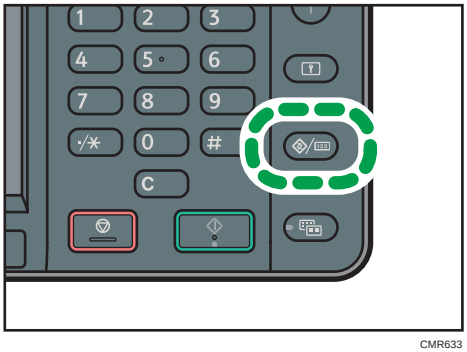
Setting thick paper or OHP transparencies using the control panel

Important

- Use A4 or $8\frac{1}{2} \times 11$ size OHP transparencies, and specify their size.
- When you load OHP transparencies, check the front and back of the sheets, and place them correctly.

- When printing onto OHP transparencies, remove printed sheets one by one.

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

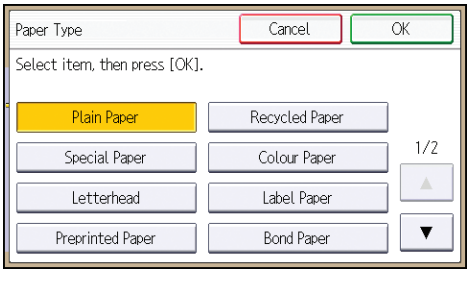


CMR633

2. Press [Tray Paper Settings].
3. Press [▼].
4. Press [Printer Bypass Paper Size], and then specify the paper size.
5. Press [OK].
6. Press [Paper Type: Bypass Tray].
7. Press [Paper Type].
8. Select the paper type, and then press [OK].

   To load thick paper, make sure that [Plain Paper] is selected.

   Press [OHP (Transparency)] when loading OHP transparencies.



9. When printing onto thick paper, press [Paper Thickness]. When printing onto OHP transparencies, proceed to step 11.
10. Press [Thick Paper], and then press [OK].
11. Press the [User Tools/Counter] key.

Note

- We recommend that you use specified OHP transparencies.
- For details about paper thickness, see "System 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 print correctly, depending on how the originals and paper are placed.

Settings for the User Tools

- Copier mode

  Specify [On] for [Letterhead Setting] in [Input/Output] under the Copier/Docu. Server Features menu, and then place the original and paper as shown below.

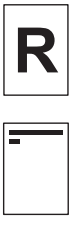
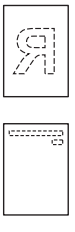
- Printer mode

  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 "Copier/Document Server Features", Copy/Document Server, or "Printer Features", Print.

Original orientation and paper orientation

The meanings of the icons are as follows:

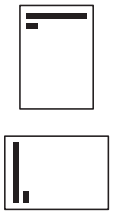
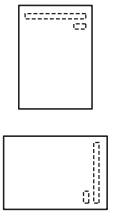
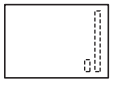
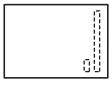
Icon	Meaning
	Place or load paper scanned or printed side face up.
	Place or load paper scanned or printed side face down.

- Original orientation

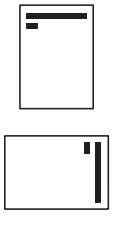
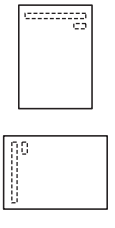
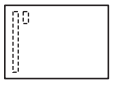
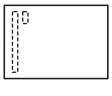
Original orientation	Exposure glass	ADF
Portrait (↓)		

Original orientation	Exposure glass	ADF
Landscape (⧉)	• Copy  • Scanner 	

- Paper orientation
  - Copier mode

Copy side	Tray 1	Trays 2 and 3	Bypass tray
One-sided			
Two-sided			Unavailable

  - Printer mode

Print side	Tray 1	Trays 2 and 3	Bypass tray
One-sided			
Two-sided			Unavailable

Note

- 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 "Printing on Both Sides of Sheets", Print  .

- In copier mode:
  - For details about how to make two-sided copies, see p.59 "Duplex Copying".

Recommended Paper Sizes and Types

This section describes recommended paper sizes and types.

Important

- If you use damp or curled paper, a 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.
- For details about and recommendations concerning thick paper, see p.138 "Thick Paper".
- For details about various details about and recommendations concerning envelopes, see p.139 "Envelopes".

Tray 1

Paper type and weight	Paper size	Paper capacity
60–90 g/m^2 (16–24 lb. Bond) Plain Paper 1–Plain Paper 2	Select the paper size using the System Settings menu: A4⬓, A5⬒, B5 JIS⬓, $8^1/_2 \times 11$⬓, $5^1/_2 \times 8^1/_2$⬒, 16K⬓	250 sheets

Trays 2 and 3

Paper type and weight	Paper size	Paper capacity
60–90 g/m^2 (16–24 lb. Bond) Plain Paper 1–Plain Paper 2	Select the paper size using the System Settings menu: A4⬓, $8^1/_2 \times 14$⬓, $8^1/_2 \times 13$⬓, $8^1/_2 \times 11$⬓, $8^1/_4 \times 14$⬓, $8^1/_4 \times 13$⬓	500 sheets

Bypass tray

Paper type and weight	Paper size	Paper capacity
60–157 g/m^2 (16–40 lb. Bond) Plain Paper 1–Thick Paper	Select the paper size *1: A4, A5, A6, B5 JIS, B6 JIS, $8^1/_2 \times 14$, $8^1/_2 \times 13$, $8^1/_2 \times 11$, $8^1/_4 \times 14$, $8^1/_4 \times 13$, 8×13, $7^1/_4 \times 10^1/_2$, $5^1/_2 \times 8^1/_2$, 16K	• Plain Paper 1–Plain Paper 2: 100 sheets • Middle Thick–Thick Paper: *3
60–157 g/m^2 (16–40 lb. Bond) Plain Paper 1–Thick Paper	Custom size *2: Region A Vertical: 90.0–216.0 mm Horizontal: 139.0–600.0 mm Region B Vertical: 3.55–8.50 inches Horizontal: 5.48–23.62 inches	• Plain Paper 1–Plain Paper 2: 100 sheets • Middle Thick–Thick Paper: *3
Translucent paper	A4	10 sheets
OHP transparencies	A4, $8^1/_2 \times 11$	10 sheets
Label paper (adhesive labels)	A4, $8^1/_2 \times 11$	1 sheet
Envelopes	Select the paper size *1: $4^1/_8 \times 9^1/_2$, $3^7/_8 \times 7^1/_2$, C5 Env, C6 Env, DL Env	*3

*1 For copier mode, see "Copying onto Regular Size Paper from the Bypass Tray", Copy/ Document Server. For printer mode, see p.129 "Setting the paper size 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 p.130 "Setting custom size paper using the control panel".

*3 Do not stack over the limit mark. The number of sheets you can load in the paper tray varies depending on the weight and condition of the paper.

Paper Thickness

Paper Thickness *1	Paper weight
Plain Paper 1	60–80 g/m^2 (16–20 lb. Bond)

Paper Thickness *1	Paper weight
Plain Paper 2	81–90 g/m^2 (20–24 lb. Bond)
Middle Thick	91–105 g/m^2 (24–28 lb. Bond)
Thick Paper	106–157 g/m^2 (28–40 lb. Bond)

*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.

Note

- Certain types of paper produce noise when delivered. This noise does not indicate a problem and print quality is unaffected. (Translucent paper and OHP transparencies can produce noise when delivered.)
- 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.
- When loading envelopes, see p.139 "Envelopes".
- When loading thick paper of 106–157 g/m^2 (28–40 lb. Bond), see p.138 "Thick Paper".
- When copying or printing onto letterhead paper, the paper placing orientation is different depending on which function you are using. For details, see p.132 "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 shifts to the other tray when the first tray in use runs out of paper. This function is called Auto Tray Switching. (However, if the paper type of one tray is recycled or special paper, the settings of the other trays must be the same for the Auto Tray Switching function to work.) 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: Tray 1]–[Paper Type: Tray 3]. For details, see "System Settings", Connecting the Machine/ System Settings. For the setting procedure of the Auto Tray Switching function, see "Copier/Document Server Features", Copy/ Document Server.
- When loading label paper:
  - We recommend that you use specified label paper.
  - Place one sheet at a time.
  - After pressing [≡], press [Paper Type], and then press [Thick Paper].
- When loading OHP transparencies:

- When copying onto OHP transparencies, see "Copying onto OHP Transparencies", Copy/ Document Server.
- When printing on OHP transparencies from the computer, see p.130 "Setting thick paper or OHP transparencies 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.

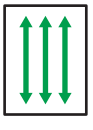
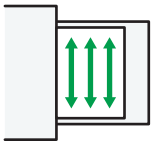
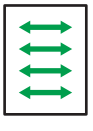
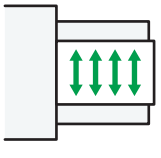
- When loading translucent paper:
  - Remove copied or printed sheets one by one.
  - When loading translucent paper, always use long grain paper, and set the paper direction according to the grain.
  - Translucent paper easily absorbs humidity and becomes curled. Remove curl in the translucent paper before loading.

Thick Paper

This section gives you various details about and recommendations concerning thick paper.

When loading thick paper of 106–157 g/m^2 (28–40 lb. Bond) in the bypass tray, 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 thick paper, set the paper direction according to its grain, as shown in the following diagram:

Direction of paper grain	Bypass tray
	
	

Note

- Select [Thick Paper] for [Paper Type] of the bypass tray.

- 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.

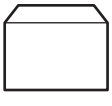
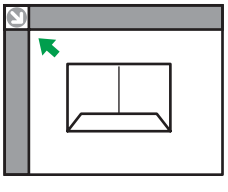
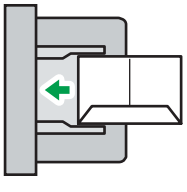
Important

- **Do not use window envelopes.**
- **Fan the envelopes before loading them to separate them and prevent the glue on them from causing them to stick together. If fanning does not prevent them sticking together, load them one by one. Note that some types of envelopes cannot be used with this machine.**
- **Misfeeds might occur depending on the length and shape of the flaps.**
- **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

When copying onto envelopes, load them according to the applicable orientation shown below. Load the envelopes in the same direction as the original.

How to load envelopes

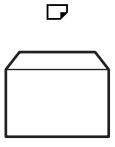
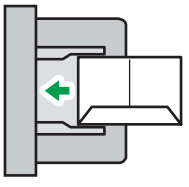
Orientation of envelopes	Exposure glass	Bypass tray
Side-opening envelopes 	 • Flaps: closed • Bottom side of envelopes: toward the back of the machine • Side to be scanned: face down	 • Flaps: closed • Bottom side of envelopes: toward the back of the machine • Side to be printed: face down

When loading envelopes, specify the envelope type and thickness. For details, see p.68 "Copying onto Envelopes".

In printer mode

When printing onto envelopes, load them according to the applicable orientation shown below:

How to load envelopes

Types of envelopes	Bypass tray
Side-opening envelopes 	 • Flaps: closed • Bottom side of envelopes: toward the back of the machine • Side to be printed: face down

When loading envelopes, select "Thick Paper" as the paper thickness and "Plain Paper" as the paper type using both the User Tools and printer driver. For details, see "Printing on Envelopes", Print.

To print on envelopes that are loaded with their bottom edge pointing toward the back of the machine, 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 p.135 "Recommended Paper Sizes and Types".

Note

- Load only one size and type of envelope at a time.
- To get better output quality, it is recommended that you set the right, left, top, and bottom print margin, to at least 10 mm (0.4 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.
- 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 the cleaner to suck spilled toner (including used toner). Sucked toner may cause firing or explosion due to electrical contact flickering inside the cleaner. However, it is possible to use the cleaner designed for dust explosion-proof purpose. If toner is spilled over the floor, sweep up spilled toner slowly and clean remainder with wet cloth.

⚠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.

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 on a flat surface.**
- **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 still toner in the cartridge, hold the cartridge with the opening upward, shake it well, and then reinstall it.
- You can make about 50 copies even after appears, but replace the toner early to prevent poor copy quality.
- 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 "Enquiry", 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. **Make sure the machine is in facsimile or scanner mode.**
2. **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.

Indicators

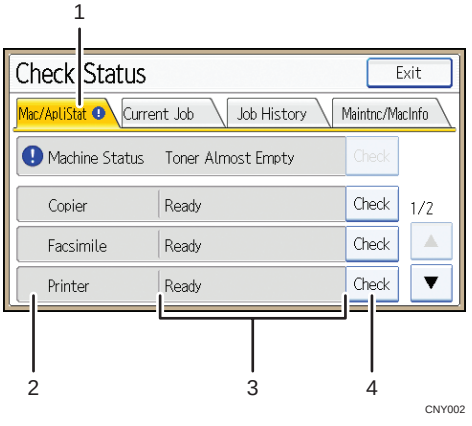
This section describes the indicators displayed when the machine requires the user to remove misfed paper, to add paper, or to perform other procedures.

Indicator	Status
: Paper Misfeed indicator	Appears when a paper misfeed occurs. For details about removing jammed paper, see "Removing Jammed Paper", Troubleshooting.
: Original Misfeed indicator	Appears when an original misfeed occurs. For details about removing jammed paper, see "Removing Jammed Paper", Troubleshooting.
: Load Paper indicator	Appears when paper runs out. For details about loading paper, see "Loading Paper", Paper Specifications and Adding Paper.
: Add Toner indicator	Appears when toner runs out. For details about adding toner, see "Adding Toner", Maintenance and Specifications.
: Waste Toner Full indicator	Appears when the waste toner bottle is full. Contact your sales or service representative.
: Service Call indicator	Appears when the machine is malfunctioning or requires maintenance.
: Open Cover indicator	Appears when one or more covers of the machine are open.

When an Indicator for the [Check Status] Key Is Lit

If an indicator for the [Check Status] key lights up, 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



1. **[Mac/ApliStat] tab**

   Indicates the status of the machine and each function.

2. **Status icons**

   Each icon that can be displayed is described below:

   : The function is performing a job.

   : An error has occurred on the machine.

   : An error has occurred in the function being used. Or, the function cannot be used because an error has occurred on the machine.

3. **Messages**

   Displays a message that indicates the status of the machine and each function.

4. **[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.

   - p.154 "Messages Displayed When Using the Copy/Document Server Function"
   - p.156 "Messages Displayed When Using the Facsimile Function"
   - p.169 "Messages Displayed When Using the Printer Function"
   - p.182 "Messages Displayed When Using the Scanner Function"

The following table explains problems that cause the indicator to light:

Problem	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 p.154 "When Messages Are Displayed on the Control Panel". You can use other functions normally.
The machine is unable to connect to the network.	A network error has occurred.	• Press [Check] in the function which error is occurred. And then check the displayed message, and take appropriate action. For details about error messages and their solutions, see p.154 "When Messages Are Displayed on the Control Panel". • 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 is still lit even after trying to solve the problem as described here, contact your service representative.

Panel Tone

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 pattern	Meaning	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 Copy/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 Copy/ 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

This section describes common problems and messages. If other messages appear, follow the instructions displayed.

Problem	Causes	Solutions
The [Facsimile] or [Scanner] icon does not appear on the [Home] screen even though the copier screen appears when the machine is turned on using the main power switch.	Functions other than the copier function are not yet ready.	Functions appear on the [Home] screen when they become ready for use. Time required varies by function. 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.	Functions appear in the User Tools menu when they become ready for use. Time required varies by function. Wait a little longer.
The lamp remains lit and the machine does not enter Sleep mode even though the [Energy Saver] key was pressed.	• The ADF is open. • The machine is communicating with external equipment. • The hard disk is active.	• Close the ADF. • Check if the machine is communicating with external equipment. • Wait a little longer.
The display is off.	The machine is in Sleep mode.	Press the [Energy Saver] key or the [Check Status] key to cancel Sleep mode.
Nothing happens when the [Check Status] key or the [Energy Saver] key is pressed.	The main power switch is turned off.	Turn on the main power switch.
"Please wait." appears.	This message appears when you press the [Energy Saver] key.	Wait for a while. If the machine does not get ready in five minutes, contact your service representative.

Problem	Causes	Solutions
"Please wait." appears.	This message appears when the machine is warming up.	• Wait until the message disappears. Do not turn off the main power switch while the message is displayed. • If the machine does not get ready in five minutes, contact your service representative.
"Please wait." appears.	This message appears when you change the toner cartridge.	• Wait until the message disappears. Do not turn off the main power switch while the message is displayed. • If the message does not disappear in five minutes, contact your service representative.
"Memory is full. Do you want to store scanned file?" appears.	The scanned originals exceed the number of sheets/pages that can be stored on the hard disk.	• Press [Yes] to store pages that have been scanned. Delete unnecessary files by pressing [Delete File]. • Press [No] if you are not storing pages that have been scanned. Delete unnecessary files by pressing [Delete File].
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 Login Password. For details about the Authentication screen, see "When the Authentication Screen is Displayed", Getting Started.
"Authentication has failed." appears.	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." appears.	The machine cannot perform authentication.	For details about authentication, see Security Guide.

Problem	Causes	Solutions
"You do not have the privileges to use this function." continues to be displayed even though you have entered a valid user name.	The logged in user name does not have permission for the selected function.	For details about how to set permissions, see Security Guide.
An error message remains, even if misfed paper is removed.	• When a misfeed message appears, it remains until you open and close the cover as required. • Paper is still jammed in the tray.	Remove misfed paper, and then open and close the cover. For details about removing jammed paper, see "Removing Jammed Paper", Troubleshooting.
An error message remains, even if consumables are replaced and/or misfed paper is removed.	This may occur if the HDD is not installed.	Press the [Start] key.
Original images are printed on the reverse side of the paper.	You may have loaded the paper incorrectly.	• Load paper into the paper tray with the print side up. • Load paper into the bypass tray with the print side down.
Misfeeds occur frequently.	The tray's side or end fences may not be set properly.	• Remove misfed paper. For details about removing jammed paper, see "Removing Jammed Paper", Troubleshooting. • Check that the side or end fences are set properly. Also, check that the side fences are locked. For details about setting the side and end fences, see "Changing the Paper Size", Paper Specifications and Adding Paper.

Problem	Causes	Solutions
Misfeeds occur frequently.	Copy paper size setting is not correct.	• Remove misfed paper. For details about removing jammed paper, see "Removing Jammed Paper", Troubleshooting. • Set the proper paper size. For details about specifying paper size with the control panel, see "Changing Paper Size Settings", Paper Specifications and Adding Paper.
Cannot print in duplex mode.	You have selected a paper tray that is not set for duplex printing.	Change the setting for "Apply 2-sided" in [System Settings] to enable duplex printing for the paper tray. For details about setting "Apply 2-sided", see "Tray Paper Settings", Connecting the Machine/ System Settings.
Cannot print in duplex mode.	Duplex printing cannot be done with paper set in the bypass tray.	When using duplex printing, make settings to use paper from a tray other than the bypass tray.
"Turn main Power Switch off" appears.	The machine does not shut down normally when the main power switch is turned off, and then immediately turned on.	Turn off the main power switch. Wait for ten seconds or more after the machine shuts down, and then turn it on again.
"Shutting down... Please wait. Main power will be turned off automatically. Maximum waiting time: 2 minute(s)" appears.	The shut down procedure has begun because the main power switch was turned off while the machine was in standby mode or performing an operation.	Follow the message that appears and wait until the machine has shut down. Do not turn on the main power switch while this message is displayed. If the main power switch has been turned on, follow the message that appears. For details about turning the main power switch on and off, see "Turning On/Off the Power", Getting Started.

Problem	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.
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.	• 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".
"Home is in use by another function." appears.	The [Home] screen is being edited by another function.	Wait for a while, and then try to create the shortcut on the [Home] screen again.
"The image data size is not valid. See the manual for required data." appears.	The image data size is not valid.	For details about file size for shortcut image, see "Customizing the [Home] Screen", Convenient Functions .
"The format of the image data is not valid." appears.	The file format of the shortcut image to be added is not supported.	The file format of shortcut images to be added must be JPEG. Specify the image again.

Note

- If you cannot make copies as you want because of paper type, paper size, or paper capacity problems, use recommended paper. For details about recommended paper, see p.135 "Recommended Paper Sizes and Types".
- Using curled paper often causes misfeeds, soiled paper edges, or slipped positions while performing stack printing. When using curled paper, take the stiffness out of the paper with your hands to straighten out the curl, or load the paper up side down. Also, lay paper on a flat surface to prevent paper from curling, and do not lean it against the wall.

When Messages Are Displayed on the Control Panel

Messages Displayed When Using the Copy/Document Server Function

This section describes the machine's main messages. If other messages appear, follow their instructions.

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 p.135 "Recommended Paper Sizes and Types".**
- **For messages that are not listed here, see p.149 "When You Have Problems Operating the Machine".**

Message	Causes	Solutions
"Check paper size."	An irregular paper size is set.	If you press the [Start] key, the copy will start using the selected paper.
"2 Sided Copy is not available with this paper size. Select another paper size or cancel 2 Sided Copy."	A paper size not available in Duplex mode has been selected.	Select a proper paper size. For details about Duplex mode, see "Duplex Copying", Copy/ Document Server.
"Exceeded max. number of pages per file. Do you want to store the scanned pages as 1 file?"	The number of scanned pages exceeds the capacity per file of the Document Server.	• If you want to store the scanned pages as a file in the Document Server, press [Yes]. • If you do not want to store scanned pages, press [No]. Scanned data is deleted.
"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.

Message	Causes	Solutions
"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/ Doc. Srvr. Featr.]. For details about Max. Copy Quantity, see "General Features", Copy/ Document Server.
"Orig. scanned for diffrnt fnctn."	A function of the machine other than the Copier function is being used such as the Document Server function.	Cancel the job that is being processed. For example, press [Exit], and then press the [Home] key. Next, press the [Document Server] icon on the [Home] screen, and then press the [Stop] key. When the message appears on the screen, follow the instructions to cancel the job.
"Please wait."	The destination list is being updated from the network using Web Image Monitor.	Wait until the message disappears. Do not turn off the main power switch while this message is displayed. Depending on the number of destinations to be updated, there may be some delay before you can resume operation. Operations are not possible while this message is displayed.
"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.	Files can be deleted by the person who created the file. To delete a file which you are not authorized to delete, contact the person who created the file.
"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.

When the memory becomes full while using the copy/document server function

Message	Causes	Solutions
"Memory is full. nn originals have been scanned. Press [Print] to copy scanned originals." "nn" 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.

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

This section describes the machine's main messages. If other messages appear, follow their instructions.

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.

Message	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.

Message	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.	• 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.	• Check that the correct gate keeper 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.
"Check whether there are any network problems." [13-17]	Registering of user name is rejected by SIP server.	• Check 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.	• 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.

Message	Causes	Solutions
"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.	• 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.
"Check whether there are any network problems." [13-26]	The "Effective Protocol" and "SIP Server IP Address" settings are different, or an incorrect IP address has been registered.	• 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.

Message	Causes	Solutions

"Check whether there are any network problems."
[14-01]
	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.	• Check that the following settings in [System Settings] are listed correctly.
		  • DNS server
		  • Server name and IP address for the SMTP Server
		For details about these settings, see "Interface Settings" or "File Transfer", Connecting the Machine/ System Settings.
		• 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 network problems of the destinations, contact the administrator of the destinations.
		• For details about network problems, contact your administrator.

Message	Causes	Solutions

"Check whether there are any network problems."
[14-09]
	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.	• Check that User Name and Password for the following settings in [System Settings] are listed correctly.
		  • SMTP Authentication
		  • POP before SMTP
		  • Fax Email Account
		For details about these settings, see "File Transfer", Connecting the Machine/ System Settings.
		• 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.

"Check whether there are any network problems." [14-33]	E-mail addresses for the machine and the administrator are not registered.	• Check that the correct Email Address is listed in [Fax Email Account] of [System Settings]. For details about Fax Email Account, see "File Transfer", Connecting the Machine/ System Settings. • For details about network problems, contact your administrator.

Message	Causes	Solutions
"Check whether there are any network problems." [15-01]	No POP3/IMAP4 server address is registered.	• 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.	• Check that the correct User Name and Password are listed in [Fax Email Account] of [System Settings]. For details about Fax Email 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.	• 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.

Message	Causes	Solutions

"Check whether there are any network problems."
[15-11]
	Cannot find the DNS server or POP3/IMAP4 server.	• Check that the following settings in [System Settings] are listed correctly.
		  • 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
		For details about these settings, see "Interface Settings" or "File Transfer", Connecting the Machine/ System Settings.
		• Check that the LAN cable is correctly connected to the machine.
		• For details about network problems, contact your administrator.

"Check whether there are any network problems."
[15-12]
	Cannot log in to the POP3/ IMAP4 server.	• Check that the following settings in [System Settings] are listed correctly.
		  • the user name and password for [Fax Email Account]
		  • the user name and password for POP before SMTP authentication
		For details about these settings, see "File Transfer", Connecting the Machine/ System Settings.
		• For details about network problems, contact your administrator.

Message	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.
"Error occurred, and transmission was cancelled."	• 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.
"Exceeded max. number to display. Max. No.: n" (A figure is placed at n.)	The number of search results has exceeded the maximum number of items that can be displayed.	Search again after changing the search conditions.
"Exceeded time limit for LDAP server search. 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 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.

Message	Causes	Solutions
"Functional problem occurred. Stopped processing."	The main power switch was turned off while the machine was receiving a document by Internet Fax.	Even if you turn the main power switch back on 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.
"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.
"Orig. scanned for diffrnt fnctn."	A function of the machine other than the Facsimile function is being used such as the Document Server function.	Before sending a file by fax, cancel the job in progress. For example, press [Exit], and then press the [Home] key. Press the [Document Server] icon on the [Home] screen. Next, press the [Stop] key. When the message appears on the screen, follow the instructions to cancel the job.
"Put original back, check it and press the Start key."	Original jammed during Memory Transmission.	Press [Exit], and then send the documents again.
"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].

Message	Causes	Solutions
"Some page(s) are almost blank. To cancel press the Stop key."	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.
"The selected file(s) contained file(s) without access privileges. Only file(s) with access privileges will be deleted."	You tried to delete a document for which you do not have permission to delete.	To check your access permission for stored documents, or to delete a document you do not have permission to delete, see Security Guide.
"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 main power switch 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.
"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 destination cannot be selected because its 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 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 certificate used for the S/MIME signature is not currently valid."	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.

Message	Causes	Solutions
"The program contains a destination(s) with a certificate that is not currently valid. The destination(s) cannot be recalled."	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 specified destination for Email TX Result, which is registered to the program, has a certificate that is not currently valid. The destination cannot be recalled."	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 specified dest. for Email TX Result, which is registered to program, contains a dest. that has a certificate that is not currently valid. The dest. cannot be recalled."	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 certificate for encryption 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.
"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.
"Email TX Result cannot be set because the specified destination's certificate is not currently valid."	The user certificate (destination certificate) has expired.	For details about the user certificate (destination certificate), see Security Guide.

Message	Causes	Solutions
"The program contains a destination(s) that does not have a certificate."	There is no user certificate (destination certificate).	For details about the user certificate (destination certificate), see Security Guide.
"The specified destination for Email TX Result, which is registered to the program, has no certificate for encryption."	There is no user certificate (destination certificate).	For details about the user certificate (destination certificate), see Security Guide.
"The specified destinations for Email TX Result, which is registered to the program, contain a destination(s) that has no certificate for encryption."	There is no user certificate (destination certificate).	For details about the user certificate (destination certificate), see Security Guide.
"The device certificate used for the S/MIME signature is not currently valid. XXX which is registered to the program cannot be recalled." (XXX indicates the e-mail destination(s) or destination(s) for [Email TX Results].)	The device certificate (S/MIME) has expired.	For details about the 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.

Message	Causes	Solutions
"XXX cannot be recalled because there is a problem with the device certificate used for the S/MIME signature." (XXX indicates the e-mail destination(s) or destination(s) for [Email TX Results].)	There is no device certificate (S/MIME), or the certificate is invalid.	For details about the device certificate (S/MIME), see Security Guide.
"The PDF Digital Signature's device certificate is not currently valid. The email destination(s) which is registered to the program cannot be recalled."	The device certificate (PDF with digital signature) has expired.	A new device certificate (PDF with digital signature) must be installed. For details about how to install a device certificate (PDF with digital signature), see Security Guide.
"XXX cannot be YYY because the PDF Digital Signature's device certificate is not currently valid." (XXX and YYY indicate the user action.)	The device certificate (PDF with digital signature) has expired.	A new device certificate (PDF with digital signature) must be installed. For details about how to install a device certificate (PDF with digital signature), see Security Guide.
"XXX cannot be YYY because there is a problem with the PDF 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 the certificate is invalid.	A new device certificate (PDF with digital signature) must be installed. For details about how to install a device certificate (PDF with digital signature), see Security Guide.
"The email destination(s) which is registered to the program cannot be recalled because there is a problem with the PDF Digital Signature's device certificate."	There is no device certificate (PDF with digital signature), or the certificate is invalid.	A new device certificate (PDF with digital signature) must be installed. For details about how to install a device certificate (PDF with digital signature), see Security Guide.

Note

- 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.
- If the paper tray runs out of paper, "Cannot print fax message. 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 the memory becomes full while using the facsimile function

Message	Causes	Solutions
"Memory is full. Cannot scan more. Transmission will be stopped."	The memory is full.	If you press [Exit], the machine returns to standby mode and starts transmitting the stored pages. Check the pages that have not been sent using the Communication Result Report, and then resend those pages.

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.

Status messages

Message	Status
"Hex Dump Mode"	In Hex Dump mode, the machine receives data in hexadecimal format. Press [Job Reset] to cancel Hex Dump mode.
"Suspended job exists."	Printing was temporarily stopped by SmartDeviceMonitor for Client. You can resume printing via [My Job List] in SmartDeviceMonitor for Client, or via the Web Image Monitor. To resume printing via Web Image Monitor, ask your system administrator first.

Message	Status
"Offline"	The machine is offline.
"Please wait."	This message might appear for a second or two while the machine is preparing, performing initial adjustments, or adding toner. Wait a while.
"Printing..."	The machine is printing. Wait a while.
"Ready"	This is the default ready message. The machine is ready for use. No action is required.
"Resetting job..."	The machine is resetting the print job. Wait until "Ready" appears on the display panel.
"Setting change..."	The machine is changing settings. You cannot use the control panel while this message is displayed. Wait a while.
"Waitg. for prt.data"	The machine is waiting for the next data to print. Wait a while.
"Job suspended."	Printing was temporarily suspended because [Job Operation] or the [Stop] key was pressed.
"Updating certif..."	The @Remote certificate is being updated. Wait a while.

Messages displayed on the control panel when using the printer function

Note

- Before turning the main power switch off, see p.48 "Turning On/Off the Power".

Message	Causes	Solutions
"Cannot connect with the wireless card. Turn the main power switch off, then check the card."	• 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.	Turn off the main power switch, and then confirm the wireless LAN board is inserted correctly. And then, turn on the main power switch again. If the message appears again, contact your service representative.

Message	Causes	Solutions
"Cannot connect with the Bluetooth interface. Check the Bluetooth interface."	• The Bluetooth interface unit was installed while the machine was turned on. • The Bluetooth interface unit was removed while the machine was turned on.	Turn off the main power switch, and then confirm that the Bluetooth interface unit was installed correctly. And then, turn on the main power switch again. If the message appears again, contact your service representative.
"Hardware Problem: Ethernet"	An error has occurred in the Ethernet interface.	Turn off the main power switch, 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 main power switch, and then back on again. If the message appears again, contact your service representative.
"Hardware Problem: Parallel I/F"	An error has occurred in the IEEE 1284 interface board.	Turn off the main power switch, 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 main power switch, 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 main power switch, and then confirm the wireless LAN board is inserted correctly. And then, turn on the main power switch again. If the message appears again, contact your service representative.

Message	Causes	Solutions
"Hardware Problem: Wireless Card" (A "wireless LAN board" or "Bluetooth interface unit" is referred to as a "wireless card".)	• 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 main power switch, and then confirm the Bluetooth interface unit is inserted correctly. And then, turn on the main power switch again. If the message appears again, contact your service representative.
"Out of paper in n. Load paper of the following size and type. To cancel the current 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.
"Tray setg. do not match spcfd siz&yp. Select new tray or use sz&typ below."	The printer driver settings are incorrect or the tray does not contain paper of the size or type 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. • 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.
"n ppr siz msmtch Select new tray or use ppr size below." (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.
"Problem: Printer Font Error"	An error has occurred in the font settings.	Contact your service representative.

Message	Causes	Solutions
"Problems with the wireless board. Please call service." (A "wireless LAN board" or "Bluetooth unit" is referred to as a "wireless board".)	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.
"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.
"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 main power switch while this message is displayed. Depending on the number of destinations to be updated, there may be some delay before you can resume operation. Operations are not possible while this message is displayed.
"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.

Messages during Direct print from a removable memory device

Message	Causes	Solutions
"Unable to access the specified memory storage device."	The memory device used cannot be recognized.	For details about the recommended memory devices for the Direct printing function from removable memory devices, contact your service representative. The USB flash memory that features password protection or other security features may not work normally.

Message	Causes	Solutions
"Exceeded the limit value for total data size of the selected files. Cannot select more files."	• The size of the selected file exceeds 1 GB. • The total size of the selected files exceeds 1 GB.	Files or groups of files larger than 1 GB cannot be printed. • When the total size of the multiple files that are selected exceeds 1 GB, select files separately. • When the size of selected file exceeds 1 GB, print by using a function other than the Direct printing function from removable memory devices. You cannot select files of different formats at the same time.

Other messages

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

Message	Causes	Solutions
"86: Error"	Parameters of the control code are invalid.	Check the print settings.
"91: Error"	Printing was canceled by the auto job cancel function due to a command error.	Check that the data is valid.
"92: Error"	Printing was canceled because [Job Reset] or the [Stop] key was selected on the machine's control panel.	Perform the print operation again if necessary.
"98: Error"	The machine could not access the hard disk correctly.	Turn off the main power switch, and then back on again. If the message appears frequently, contact your service representative.

Message	Causes	Solutions
"Address Book is currently in use by another function. Authentication has failed."	The machine currently cannot perform authentication because the Address Book is being used by another function.	Wait a while, and then retry the operation.
"Unauthorized Copy Prevention error occurred. Job cancelled."	You tried to store a file in the Document Server when [Unauthorized Copy Prevention] was specified.	**Only when using PCL 6 / PostScript 3** On the printer driver, select a job type other than [Document Server] in "Job Type:" or deselect [Unauthorized Copy Prevention].
"Unauthorized Copy Prevention error occurred. Job cancelled."	The [Enter User Text:] field on the [Unauthorized Copy Prevention for Pattern Details] screen is blank.	**Only when using PCL 6 / PostScript 3** 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:].
"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.
"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.
"Classification Code is incorrect."	The classification code has not been entered, or the classification code has been entered incorrectly.	Enter the correct classification code.

Message	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.
"Collate has been cancelled."	Collate was canceled.	Turn off the main power switch, and then back on again. If the message appears again, contact your service representative.
"Command Error"	An RPCS command error occurred.	• 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.
"Compressed Data Error."	The printer detected corrupt compressed data.	• 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.

Message	Causes	Solutions
"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.
"Duplex has been cancelled."	Duplex printing was canceled.	• Select the proper paper size for the duplex function. For details about paper, see "Specifications for the Main Unit", Maintenance and Specifications. • Change the setting for "Apply 2-sided" in [System Settings] to enable duplex printing for the paper tray. For details about setting "Apply 2-sided", see "Tray Paper Settings", Connecting the Machine/ System Settings.
"Error has occurred."	A syntax error, etc., occurred.	Check that the PDF file is valid.
"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.
"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.

Message	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 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.	• Delete unneeded files stored in the machine. • Reduce the number of pages to print.
"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.
"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.
"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 Volum. Use Limit., see Security Guide.
"Failed to obtain file system."	PDF direct printing could not be performed because the file system could not be obtained.	Turn off the main power switch, 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.

Message	Causes	Solutions
"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. • Reduce the data size of the Sample Print, Locked Print, Hold Print, or Stored Print file.
"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. (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. • Reduce the data size of the Temporary Print file and/or the Stored Print file.
"I/O buffer overflow."	An input buffer overflow occurred.	• In [Printer Features], under [System], set [Memory Usage] to [Font Priority]. • 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.
"Information for user authentication is already registered for another user."	The user name for LDAP Authentication 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.

Message	Causes	Solutions
"Insufficient Memory"	A memory allocation error occurred.	**PCL 5e** Select a lower resolution on the printer driver. For details about how to change the resolution setting, see the printer driver Help. **PCL 6** 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.
"Memory Retrieval Error"	A memory allocation error occurred.	Turn off the main power switch, and then back on again. If the message appears again, replace the RAM. For details about replacing the RAM, contact your service representative.
"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.
"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.	**PCL 5e** Select a lower resolution on the printer driver. For details about how to change the resolution setting, see the printer driver Help.
"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.
"Receiving data failed."	Data reception was aborted.	Resend the data.

Message	Causes	Solutions
"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.
"Sending data failed."	The machine received a command to stop transmission from the printer driver.	Check if the computer is working correctly.
"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. No. 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 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.
"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 Login User Name and Login 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.

Messages during Direct print from a removable memory device

Message	Causes	Solutions
"99: Error"	This data cannot be printed. The specified data is either corrupt or not supported by the Direct printing function from removable memory devices.	Check that the data is valid. For details about the kinds of data supported by the Direct printing function from removable memory devices, see "Direct Printing from a Removable Memory Device", Print.

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

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.

Message	Causes	Solutions
"Authentication with the destination has failed. Check settings. To check the current status, press [Comm. Status/ Print]."	The entered user name or password was invalid.	• 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.
"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.

Message	Causes	Solutions
"Connection with the destination has failed. Check the settings. Entered path name might be incorrect, or firewall and security settings might be blocking network connectivity."	The destination computer name or folder name is invalid.	Check whether the computer name and the folder name for the destination are correct.
"Connection with the destination has failed. Check the settings. Entered path name might be incorrect, or firewall and security settings might be blocking network connectivity."	An antivirus program or a firewall is preventing the machine connecting to your computer.	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 firewall's Help.
"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 "Changing a Scan Profile", Scan.
"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.

Message	Causes	Solutions
"Cannot write on the memory storage device. Check the memory storage device and machine settings."	The memory device is faulty, or the file name contains a character that cannot be used.	• Check to see if the memory device is defective. • Check the memory 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 "Available Characters and How to Enter Them", Getting Started.
"Cannot write on the memory storage device because remaining free space is insufficient."	• The memory device is full and scan data cannot be saved. • Even if the memory device appears to have sufficient free space, data might not be saved if the maximum number of files that can be saved is exceeded.	• Replace the memory device. • If the document is scanned as single-page or divided multiple pages, data already written to the memory device is saved as is. Replace the memory device, and then press [Retry] to save the remaining data, or press [Cancel] to redo the scan.
"Cannot write on the memory storage device because the device is write-protected."	The memory device is write-protected.	Unlock the write-protection on the memory device.
"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 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.

Message	Causes	Solutions
"The data could not be sent 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: • Too many originals per set. • Misfed originals. • Transmission of other jobs.	• 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.
"Entered protection code for destination is incorrect. Please re-enter."	The correct protection code was not entered.	Make sure the protection code is correct, and then enter it again. For details about a protection code, see "Registering a Protection Code", Connecting the Machine/ System Settings.
"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. email size. Sending email has been cancelled. Check [Max. Email Size] in Scanner Features."	The file size per page has reached the maximum e-mail size specified in [Scanner Features].	Change the [Scanner Features] settings as follows: • Increase the e-mail size limit in [Max. Email Size]. • Change the [Divide & Send Email] setting to [Yes (per Page)] or [Yes (per Max. Size)]. For details about these settings, see "Send Settings", Scan.
"Exceeded max. number to display. Max. No.: n" (A figure is placed at n.)	Search results have exceeded the max. displayable number.	Search again after changing the search conditions.

Message	Causes	Solutions
"Exceeded max. data capacity. Check the scanning resolution, then press the 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 scan function, see "Relationship between Resolution and Scan Size", Scan.
"Exceeded max. data capacity. Check resolution, then reset n orig." (A figure is placed at n.)	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 scan function, see "Relationship between Resolution and Scan Size", Scan.
"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.
"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.
"Exceeded max. number of files which can be sent at the same time. Reduce the number of the selected files."	The number of files exceeded the maximum number possible.	Reduce the number of files, and then send them 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.

Message	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 standby files. Try again after the current file is sent."	The maximum number of standby files was exceeded.	There are 100 files waiting in the sending queue for e-mail, Scan to Folder, or delivery functions. Wait until files have been sent.
"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 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 device.	Reduce the number of documents to be written to the memory device, and then try again.
"Exceeded maximum number of files to store. Delete all unnecessary files."	Too many files are waiting to be delivered.	Try again after they have been delivered.

Message	Causes	Solutions
"Exceeded time limit for LDAP server search. 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 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."	The user name and password differ from those set for LDAP Authentication.	For details about LDAP Authentication, see Security Guide.
"Memory device error occurred. Check the memory device."	A non-writable medium is being used.	Use a different medium.
"Memory is full. Cannot scan. The scanned data will be deleted."	Because of insufficient hard disk space, the first page could not be scanned.	• 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 "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.

Message	Causes	Solutions
"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 device.	Select whether or not to save the scanned document to the memory device.
"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.
"Memory storage device not detected. Insert the device."	There is no memory device inserted.	Insert a memory device, or check to see whether the memory device is properly inserted in the media slot.
"No paper. Load paper of one of the following sizes."	No paper is set in the specified paper tray.	Load paper of the sizes listed in the message. For details about loading paper, see "Loading Paper", Paper Specifications and Adding Paper.
"Orig. scanned for diffrnt fnctn."	A function of the machine other than the Scanner function is being used such as the Copier function.	Cancel the job that is being processed. For example, press [Exit], and then press the [Home] key. Next, press the [Copier] icon on the [Home] screen, and then press the [Stop] key. When the message appears on the screen, follow the instructions to cancel the job.
"Output buffer is full. Sending the data has been cancelled. Please try again later."	Too many jobs are in standby state, and sending was canceled.	Retry sending after sending jobs in standby state completes.
"SMTP authentication email address and administrator email 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.

Message	Causes	Solutions
"Scanner journal full. Cannot send data. Delete scan.journals in Scan.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 printing or deleting Scanner Journal, see "General Settings", Scan.
"Selected file is currently in use. File name cannot be changed."	You cannot change the name of a file whose status is "Waiting to send data..." or that is being edited with DeskTopBinder.	Cancel transmission ("Waiting to send data..." status cleared) or the DeskTopBinder setting, 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 to send data..." or that is being edited with DeskTopBinder.	Cancel transmission ("Waiting to send data..." status cleared) or the DeskTopBinder setting, 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 to send data..." or that is being edited with DeskTopBinder.	Cancel transmission ("Waiting to send data..." status cleared) or the DeskTopBinder setting, and then change the user name.
"Some destinations cannot receive encrypted files. Sending to these destinations may be unsafe."	If you have selected multiple destinations including destinations for which encryption has not been configured, e-mail sent to those destinations will not be encrypted even if you specify encryption.	Using Web Image Monitor, check the file encryption settings for all destinations.
"Some destinations will receive automatically encrypted files. All files sent to these destinations will be encrypted."	If you have selected multiple destinations including destinations for which encryption has been configured, e-mail sent to such destinations will be automatically encrypted.	Using Web Image Monitor, check the file encryption settings for all destinations.

Message	Causes	Solutions
"Some invalid destination(s) contained. Do you want to select only valid destination(s)?"	The specified group contains e-mail destinations and Scan to Folder destinations, either of which are incompatible with the specified transmission method.	In the message that appears at each transmission, press [Select].
"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 to send data..." status displayed) or whose information is being changed with DeskTopBinder.	Cancel transmission ("Waiting to send data..." status cleared) or the DeskTopBinder setting, and then delete the file.
"Some page(s) are almost blank. To cancel press the Stop key."	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.
"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. For details about characters that can be used in file names, see "Available Characters and How to Enter Them", Getting Started. • 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 ".".
"The number of destinations that can be entered manually at the same time is as shown above."	The e-mail has too many destinations.	Split the destinations into two or more groups.

Message	Causes	Solutions
"The number of destinations that can be specified at the same time is as shown above."	The e-mail has too many destinations.	Split the destinations into two or more groups.
"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.
"Transmission has failed. Insufficient memory in the destination hard disk. To check the current status, press [Comm. Status/Print]."	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 [Comm. Status/Print]."	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.

Message	Causes	Solutions

"Updating the destination list has failed. Try again?"	A network error has occurred.	• 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 firewall's Help.

"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.
"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 main power switch while this message is displayed. Depending on the number of destinations to be updated, there may be some delay before you can resume operation. Operations are not possible while this message is displayed.

Message	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.
"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.
"The size of the scanned data is too small. Check the scanning resolution, 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.
"Not all of the image will be scanned."	If the scaling factor specified in "Reproduction Ratio" is too large, part of the image may be lost.	• Reduce the scaling factor in "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.
"Not all of the image will be scanned."	Using "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.
"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.
"The Digital Signature's device certificate has expired. The file cannot be sent."	The device certificate (PDF with digital signature) has expired.	A new device certificate (PDF with digital signature) must be installed. For details about how to install a device certificate (PDF with digital signature), see Security Guide.

Message	Causes	Solutions
"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) has expired.	A new device certificate (PDF with digital signature) must be installed. For details about how to install a device certificate (PDF with digital signature), see Security Guide.
"The Digital Signature's device certificate is invalid. The file cannot be sent."	There is no device certificate (PDF with digital signature), or the certificate is invalid.	A new device certificate (PDF with digital signature) must be installed. For details about how to install a device certificate (PDF 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 the certificate is invalid.	A new device certificate (PDF with digital signature) must be installed. For details about how to install a device certificate (PDF with digital signature), 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.	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 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.

Message	Causes	Solutions
"Transmission cannot be performed because the certificate used for the S/MIME signature is not currently valid."	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.
"The destination cannot be selected because its 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 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 certificate for encryption 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.

When Messages Are Displayed on Your Computer Screen

Messages Displayed When Using the Scanner Function

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.

Message	Causes	Solutions
"Any of Login User Name, Login Password or Driver Encryption Key is incorrect."	The entered Login User Name, Login Password, or DriverEncryp.Key was invalid.	Check your Login User Name, Login Password, or DriverEncryp.Key, and then enter them correctly. For details about Login User Name, Login Password, and DriverEncryp.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.
"Call Service" "Please call your service representative."	An unrecoverable error has occurred in the machine.	Contact your service representative.
"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 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 switch of the previously used scanner is not set to "On".	Check whether the main power switch of the scanner used for the previous scan is turned on.

Message	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.	• 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.
"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.	• Remove jammed originals, and then insert them again. For details about how to remove 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.
"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.

Message	Causes	Solutions
"Error has occurred in the scanner driver."	An error has occurred in the driver.	• 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.	• Close all the unnecessary applications running on the client computer. • Uninstall the TWAIN driver, and then reinstall it after restarting the computer.

Message	Causes	Solutions
"Insufficient memory. Reduce the scanning area."	Scanner memory is insufficient.	• Reset the scan size. • Lower the resolution. • Set with no compression. For details about the settings, see TWAIN driver Help. The problem may also be due to the following causes: • 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 User Code is registered. Consult your system administrator."	Access is restricted with user codes.	For details about User Code Authentication, see Security Guide.
"No response from the scanner."	The machine or client computer is not connected to the network correctly.	• 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.

Message	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.	• Wait for a while, and then reconnect. • Cancel the job that is being processed. For example, press [Exit], and then press the [Home] key. Next, press the [Copier] icon on the [Home] screen, and then press the [Stop] key. When the message appears on the screen, follow the instructions to cancel the job.
"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 available. Check the scanner connection status."	The machine's main power switch is off.	Turn on the main power switch.
"Scanner is not available. Check the scanner connection status."	The machine is not connected to the network correctly.	• 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.

Message	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.	• 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 addresses cannot be obtained from the host name. Specify the machine's IPv6 address in the Network Connection Tool.
"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.

11. Appendix

This chapter describes the trademarks.

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.

The Bluetooth® word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. and any use of such marks by Ricoh Company, Ltd. is under license.

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

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

UNIX is a registered trademark of The Open Group.

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 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

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.

INDEX

M

N

O

P

Q

R

S

T

U

V

W

MEMO

Operating Instructions

Driver Installation Guide

For safe and correct use, be sure to read the Safety Information in "Read This First" before using the machine.

TABLE OF CONTENTS

1. Introduction

2. Installing the Printer Driver

3. Installing the Scanner Driver

4. Installing the Facsimile Driver

5. Troubleshooting

6. Installing the Printer Driver Under Mac OS X

7. Appendix

1. Introduction

This chapter explains the software included on the supplied CD-ROM.

Start Installer

To connect this machine to a client computer and use its printer, scanner, and fax functions, the software included on the provided CD-ROM must be installed on the client computer.

The installer starts automatically when you insert the provided CD-ROM into the CD-ROM drive of a client computer running under Windows or Windows Server. You can then install the various software included on the CD-ROM.

The contents (display item) of the installer are as follows:

Quick Install

Install the PCL 6 printer driver, and configure the Standard TCP/IP port to establish a connection with a network printer. Quick Install is also available when the machine is connected with a client computer via parallel connection.

For details, see p.13 "Quick Install".

PCL Printer Drivers

Installs the PCL 6 and/or PCL 5e printer drivers.

For details about installing the driver, see p.14 "Installing the Printer Driver for a Network Connection" or p.27 "Installing the Printer Driver for a Local Connection".

PostScript 3 Printer Driver

Install the PostScript 3 printer driver.

For details about installing the driver, see p.14 "Installing the Printer Driver for a Network Connection" or p.27 "Installing the Printer Driver for a Local Connection".

LAN-Fax Driver

This software enables you to fax documents directly from your computer. Address Book and LAN-Fax Cover Sheet Editor will also be installed.

For details about installing the driver, see p.41 "Installing the LAN-Fax Driver".

TWAIN Driver

This software enables you to utilize image data from other TWAIN compliant applications.

For details about installing the driver, see p.39 "Installing the TWAIN Driver".

Font Manager

This software enables you to use screen fonts.

For details about installing the software, see p.37 "Installing Font Manager".

Select Language

Change the interface language.

Browse This CD-ROM

Browse the contents of this CD-ROM.

Exit

Quit Installer.

Note

- Manage Printers permission is required to install the driver. Log on as an Administrators group member.
- Auto Run might not work automatically with certain OS settings. If this is the case, double-click "SETUP.EXE", located on the CD-ROM root directory, or click [Run SETUP.EXE] in the [AutoPlay] dialog box.
- If you want to cancel Auto Run, hold down the left [Shift] key while inserting the CD-ROM. Keep the [Shift] key held down until the computer stops reading the CD-ROM.

Software and Utilities Included on the CD-ROM

This section explains the software and utilities CD-ROM provided with this machine.

Note

- For the latest information on the corresponding operating system, see "Readme.txt" file in the DRIVERS folder.
- For the latest information on Windows terminal service, Citrix Presentation Server, and Citrix Xen App, see the manufacturer's Web site.

Printer Drivers

Printing requires installation of a printer driver for your operating system. The following drivers are included on the CD-ROM.

Operating System	Printer Language		
	PCL 5e	PCL 6	PostScript 3
Windows XP *1 *6	OK	OK	OK
Windows Vista *2 *6	OK	OK	OK
Windows 7 *3 *6	OK	OK	OK
Windows Server 2003 *4 *6	OK	OK	OK
Windows Server 2008 *5 *6	OK	OK	OK
Mac OS X *7	–	–	OK

*1 Microsoft Windows XP Professional Edition/Microsoft Windows XP Home Edition/Microsoft Windows XP Media Center Edition/Microsoft Windows XP Tablet PC Edition

*2 Microsoft Windows Vista Ultimate/Microsoft Windows Vista Enterprise/Microsoft Windows Vista Business/Microsoft Windows Vista Home Premium/Microsoft Windows Vista Home Basic

*3 Microsoft Windows 7 Home Premium/Microsoft Windows 7 Professional/Microsoft Windows 7 Ultimate/Microsoft Windows 7 Enterprise

*4 Microsoft Windows Server 2003 Standard Edition/Microsoft Windows Server 2003 Enterprise Edition/Microsoft Windows Server 2003 R2 Standard Edition/Microsoft Windows Server 2003 R2 Enterprise Edition

*5 Microsoft Windows Server 2008 Standard/Microsoft Windows Server 2008 Enterprise/Microsoft Windows Server 2008 R2 Standard/Microsoft Windows Server 2008 R2 Enterprise

*6 Supports both versions (32/64 bit)

*7 Mac OS X 10.2 or later (native mode). Any versions higher than Mac OS X 10.6 are not supported.

PCL printer drivers

Two kinds of PCL printer driver (PCL 5e and PCL 6) are included. These drivers allow your computer to communicate with this machine via a printer language.

Adobe® PostScript® printer driver and PPD files

Adobe PostScript printer driver allows the computer to communicate with the printer using a printer language. PPD files allow the printer driver to enable specific printer functions.

Depending on the machine you are using, PostScript 3 unit must be installed.

Note

- Some applications may require installation of the PCL 5e printer driver. In this case, you can install PCL 5e without having to install PCL 6.
- For details about installing the driver, see p.14 "Installing the Printer Driver for a Network Connection" or p.27 "Installing the Printer Driver for a Local Connection".

Supported languages

The languages supported in each printer driver are as follow:

Supported languages	Printer Language			
	PCL 5e *1	PCL 6 *2	PostScript 3 *2	PPD (Mac OS X)
English	○	○	○	○
German	○	○	○	○
French	○	○	○	○
Italian	○	○	○	○
Spanish	○	○	○	○
Dutch	○	○	○	○
Swedish	○	○	○	○
Norwegian	○	○	○	○
Danish	○	○	○	○
Finnish	○	○	△	△
Hungarian	○	○	△	△

Supported languages	Printer Language			
	PCL 5e *1	PCL 6 *2	PostScript 3 *2	PPD (Mac OS X)
Czech	○	○	△	△
Polish	○	○	△	△
Portuguese	○	○	△	△
Russian	○	○	△	△
Catalan	○	○	△	△
Turkish	○	○	△	△
Brazilian Portuguese	△	○	△	△
Greek	△	○	△	△

○: Supported

△: Supported, but the printer language is displayed in English

*1 The PCL 5e printer driver does not support Brazilian Portuguese and Greek. Use the English version of the driver.

*2 The PCL 6 and PostScript 3 printer drivers use the same interface language as the one specified by your operating system. However, the PostScript 3 printer will be displayed in English if your operating system uses one of the following languages: Finnish, Hungarian, Czech, Polish, Portuguese, Russian, Catalan, Turkish, Brazilian Portuguese, Greek.

TWAIN Driver

This driver is required to scan an original using a scanner. To use the machine as a network TWAIN scanner, this driver must be installed.

File path

The driver is included in the following folder on the CD-ROM:

`\X86\DRIVERS\TWAIN`

System requirements

- Hardware

  PC/AT-compatible machines that support the following operating system properly

- Operating system *1

  Windows XP/Vista/7

  Windows Server 2003/2003 R2/2008/2008 R2

*1 Operates in 32-bit compatibility mode on 64-bit operating systems

- Display resolution

  800 × 600 pixels, 256 colors or higher

1

Supported languages

The TWAIN driver uses the same interface language as the one specified by your operating system.

Note

- For details about installing the driver, see p.39 "Installing the TWAIN Driver".

LAN-Fax Driver

This driver is required to use LAN-Fax functions.

File path

The driver is included in the following folder on the CD-ROM:

- 32-bit driver

  `\X86\DRIVERS\LAN-FAX\XP_VISTA`

- 64-bit driver

  `\X64\DRIVERS\LAN-FAX\X64`

System requirements

- Hardware

  PC/AT-compatible machines that support the following operating system properly

- Operating systems

  Windows XP/Vista/7

  Windows Server 2003/2003 R2/2008/2008 R2

- Display

  VGA 640 × 480 pixels or more

Supported languages

The interface language is supported in the language specified when installing driver.

Note

- For details about installing the driver, see p.41 "Installing the LAN-Fax Driver".

Font Manager

For installing new screen fonts, or organizing and managing fonts already in the system. For details about Font Manager, see the manual on the CD-ROM.

File path

The software is included in the following folder on the CD-ROM:

\FONTMAN\DISK1

Note

- For details about installing the software, see p.37 "Installing Font Manager".

For Mac OS X Users

If you are using Mac OS X, the following limitations apply to each function:

- When using the scanner function, the TWAIN driver cannot be used.
- When using the fax function, the LAN-Fax driver cannot be used.
- When using the printer function, use the printer driver for Mac OS X.

  For details, see p.53 "Installing the Printer Driver Under Mac OS X".

2. Installing the Printer Driver

This chapter explains how to install and configure the printer drivers for use on the Windows operating system.

Confirming the Connection Method

This machine supports network and local connection.

Before installing the printer driver, check how the machine is connected. Follow the driver installation procedure that is appropriate to the connection method.

Network Connection

This machine can be used as a Windows printing port or network printer.

Using the Windows printing port

Network connections can be established through Ethernet and Wireless LAN.

Available ports are determined based on the combination of Windows operating system version and connection method used.

Windows XP, Windows Server 2003/2003 R2

Connection Method	Available Ports
• Ethernet • Wireless LAN	• Standard TCP/IP port • IPP port • LPR port • SmartDeviceMonitor for Client port

Windows Vista/7, Windows Server 2008/2008 R2

Connection Method	Available Ports
• Ethernet • Wireless LAN	• Standard TCP/IP port • IPP port • LPR port • WSD port • SmartDeviceMonitor for Client port

Note

- For details about how to install the printer driver for each type of port, see p.14 "Installing the Printer Driver for the Selected Port".

Using as a network printer

This machine can be used as a remote printer using the Windows or NetWare print server function.

Client OS	Using Server
• Windows XP • Windows Server 2003/2003 R2	• Windows XP print server • Windows Vista print server • Windows 7 print server • Windows Server 2003/2003 R2 print server • Windows Server 2008/2008 R2 print server • NetWare print server (using IPv4 only) • NetWare file server (using IPv4 only)
• Windows Vista • Windows 7 • Windows Server 2008/2008 R2	• Windows 2000 print server • Windows XP print server • Windows Vista print server • Windows 7 print server • Windows Server 2003/2003 R2 print server • Windows Server 2008/2008 R2 print server

Note

- For details about how to install the printer driver to print server, see p.22 "Using as a Network Printer".

Local Connection

Local connections can be established via USB, parallel and Bluetooth connections.

Note

- For details about how to install the printer driver for each method of connections, see p.27 "Installing the Printer Driver for a Local Connection".

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.

When the machine is connected to a client computer via parallel connection, the printer port is set to [LPT1].

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

   For details about the languages supported in the printer drivers, see p.6 "Supported languages".
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. **Select the machine model you want to use in the [Select Printer] dialog box.**

   For network connection via TCP/IP, select the machine whose IP address is displayed in [Connect To].

   For parallel connection, select the machine whose printer port is displayed in [Connect To].
7. **Click [Install].**
8. **Configure the user code, default printer, and shared printer as necessary.**
9. **Click [Continue].**

   The installation starts.

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

    When you are prompted to restart your computer, restart it by following the instructions that appear.
11. **Click [Exit] in the first window of the installer, and then take out the CD-ROM.**

Note

- Quick Install is not available unless bidirectional communication between the machine and computer is enabled via parallel connection. For details about meeting the bidirectional communication conditions, see p.35 " Configuring Option Settings for the Printer".

Installing the Printer Driver for a Network Connection

This section describes the installation procedure of the printer drivers for network connection.

Important

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

Note

- If the [User Account Control] dialog box appears during the driver installation procedure, click [Yes] or [Continue].
- If the [Windows Security] dialog box appears during the driver installation procedure, click [Install this driver software anyway].
- A message appears if there is a newer version of the printer driver already installed. If there is, you cannot install the printer driver using Auto Run. If you still want to install the printer driver, use [Add Printer]. See p.49 "Messages Displayed When Installing the Printer Driver".

Installing the Printer Driver for the Selected Port

Describes the driver installation procedure for each printer port. See the installation procedure for the printer port you are using.

Important

- **To use the SmartDeviceMonitor for Client port, you must first download SmartDeviceMonitor for Client from the manufacturer's Web site and install it on your computer. Contact your local dealer for information on downloading SmartDeviceMonitor for Client. For details about SmartDeviceMonitor for Client, see "Software that You Can Download", Getting Started.**

Port Type	Printer Driver Type	Reference
Standard TCP/IP port	PCL PS3	p.15 "Using the Standard TCP/IP port"
IPP port	PCL PS3	p.15 "Using the IPP port"
LPR port	PCL PS3	p.17 "Using the LPR port"
WSD port	PCL PS3	p.18 "Using the WSD port"
SmartDeviceMonitor for Client port	PCL PS3	p.20 "Using the SmartDeviceMonitor for Client port"

Using the Standard TCP/IP port

PCL PS3

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

   For details about the languages supported in the printer drivers, see p.6 "Supported languages".
4. **Click [PCL Printer Drivers] or [PostScript 3 Printer Driver].**
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].**

   If installing the PostScript 3 printer driver, proceed to step 7.
6. **Select a printer driver you want to use, and then click [Next].**
7. **Select the check box of the manufacturer and machine model you want to use.**
8. **Double-click the machine name to display the printer settings.**
9. **Click [Port :], and then click [Add] in the [Change settings for 'Port'] box.**
10. **Click [Standard TCP/IP Port], and then click [OK].**

    If [Standard TCP/IP Port] does not appear, see Windows Help, and then configure the settings.
11. **Click [Next].**
12. **Enter the machine name or IP address, and then click [Next].**

    When the device type selection appears, select "RICOH Network Printer C model".
13. **Click [Finish].**
14. **Check that the port of the selected printer is displayed in [Port :].**
15. **Configure the user code, default printer, and shared printer as necessary.**
16. **Click [Continue].**

    The installation starts.
17. **Click [Finish].**

    Select one of the options to restart the computer either now or later, and then click [Finish].

Using the IPP port

PCL PS3

Important

- To print via IPP-SSL, use the SmartDeviceMonitor for Client port.

- Installation of the certificate is especially necessary for users who want to print via IPP-SSL from Windows Vista/7 or Windows Server 2008/2008 R2. For details, consult your administrator.
- If a certificate authority issues a certificate that must be authenticated by an intermediate certificate authority, and the certificate is installed on this machine, an intermediate certificate must be installed on the client computer. Otherwise, validation by the certificate authority will not be performed correctly.
- If validation cannot be performed properly, a warning message informing you that installation is not possible might appear when you try to add a printer using IPP-SSL under Windows Vista/7 or Windows Server 2008/2008 R2. To enable authentication from the client computer, install the intermediate certificate on the client computer, and then reestablish connection.
- Intermediate certificates cannot be installed on this machine.

1. **Quit all applications. (Do not close this manual.)**
2. **On the [Start] menu, click [Devices and Printers].**
3. **Click [Add a printer].**
4. **Click [Add a network, wireless or Bluetooth printer].**
5. **Click [The printer that I want isn't listed].**
6. **In the [Select a shared printer by name] box, enter "http://(machine's IP address or host name)/printer (or ipp)" as the printer's address, and then click [Next].**
7. **Click [Have Disk...].**
8. **Insert the provided CD-ROM into the computer's CD-ROM drive.**

   If the [AutoPlay] dialog box appears, click [Close].
9. **Click [Browse...], and then specify a location for the INF file.**

   If the CD-ROM drive is D, the source files of the printer driver are stored in the following locations:

   - PCL 5e

     32-bit driver D:\X86\DRIVERS\PCL5E\XP_VISTA\(Language)\DISK1

     64-bit driver D:\X64\DRIVERS\PCL5E\X64\(Language)\DISK1
   - PCL 6

     32-bit driver D:\X86\DRIVERS\PCL6\XP_VISTA\MUI\DISK1

     64-bit driver D:\X64\DRIVERS\PCL6\X64\MUI\DISK1
   - PostScript 3

     32-bit driver D:\X86\DRIVERS\PS\XP_VISTA\MUI\DISK1

     64-bit driver D:\X64\DRIVERS\PS\X64\MUI\DISK1

   For details about the languages supported in the printer drivers, see p.6 "Supported languages".
10. **Click [Open].**
11. **Click [OK] to close the [Install From Disk] window.**

12. **Select the manufacturer and model name of the machine you want to use, and then click [Next].**

    The installation starts.

13. **Follow the instructions that appear. Modify settings such as printer name and default printer configuration, as necessary. You can also print a test page.**

14. **Click [Finish].**

    If a check box for setting the machine as a default printer appears, configure as necessary.

Using the LPR port

PCL PS3

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 AUTORUN.EXE].

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

    For details about the languages supported in the printer drivers, see p.6 "Supported languages".

4. **Click [PCL Printer Drivers] or [PostScript 3 Printer Driver].**
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].**

    If installing the PostScript 3 printer driver, proceed to step 7.

6. **Select a printer driver you want to use, and then click [Next].**
7. **Select the check box of the machine model you want to use.**
8. **Double-click the machine name to display the printer settings.**
9. **Click [Port :], and then click [Add] in the [Change settings for 'Port'] box.**
10. **Click [LPR Port], and then click [OK].**

    If [LPR Port] does not appear, see Windows Help and install it.

11. **Enter the machine name or IP address in the [Name or address of server providing lpd:] box.**
12. **Enter "lp" in the [Name of printer or print queue on that server:] box, and then click [OK].**
13. **Check that the port of the selected printer is displayed in [Port :].**
14. **Configure the user code, default printer, and shared printer as necessary.**
15. **Click [Continue].**

    The installation starts.

16. **Click [Finish].**

    Select one of the options to restart the computer either now or later, and then click [Finish].

Using the WSD port

PCL PS3

Important

- The WSD port can be used under Windows Vista/7, or Windows Server 2008/2008 R2.
- You can connect to the printer only if both the printer and computer are on the same network segment, or "Network discovery" is enabled. For details, see Windows Help.

Windows Vista, Windows Server 2008

1. Quit all applications. (Do not close this manual.)
2. On the [Start] menu, click [Network].
3. Right-click the machine's icon, and then click [Install].
4. Click [Locate and install driver software (recommended)].
5. Click [Browse my computer for driver software (advanced)].
6. Insert the provided CD-ROM into the computer's CD-ROM drive.

   If the [AutoPlay] dialog box appears, click [Close].
7. Click [Browse...], and then specify the location of the INF file.

   If the CD-ROM drive is D, the source files of the printer driver are stored in the following locations:

   - PCL 5e

     32-bit driver D:\X86\DRIVERS\PCL5E\XP_VISTA\(Language)\DISK1

     64-bit driver D:\X64\DRIVERS\PCL5E\X64\(Language)\DISK1
   - PCL 6

     32-bit driver D:\X86\DRIVERS\PCL6\XP_VISTA\MUI\DISK1

     64-bit driver D:\X64\DRIVERS\PCL6\X64\MUI\DISK1
   - PostScript 3

     32-bit driver D:\X86\DRIVERS\PS\XP_VISTA\MUI\DISK1

     64-bit driver D:\X64\DRIVERS\PS\X64\MUI\DISK1

   For details about the languages supported in the printer drivers, see p.6 "Supported languages".
8. Click [Next].
9. Click [Close].

   If installation is successful, the icon of the printer connected to the WSD port will appear in the window for configuring printers.

Note

- The port name that follows "WSD" uses random character strings. It cannot be changed freely.

- To stop the installation, click [Cancel] before the installation is complete. When re-installing the WSD Port, right-click the printer's icon in the [Network] window, and then click [Uninstall].

Windows 7, Windows Server 2008 R2

1. **Quit all applications. (Do not close this manual.)**
2. **On the [Start] menu, click [Computer].**
3. **Click [Network].**
4. **Right-click the machine's icon, and then click [Install].**
5. **On the [Start] menu, click [Devices and Printers].**
6. **Click [Add a printer].**
7. **Click [Add a local printer].**
8. **Check the [Use an existing port:] check box, and select WSD port.**
9. **Click [Next].**
10. **Click [Have Disk...].**
11. **Insert the provided CD-ROM into the computer's CD-ROM drive.**

    If the [AutoPlay] dialog box appears, click [Close].
12. **Click [Browse...], and then specify the location of the INF file.**

    If the CD-ROM drive is D, the source files of the printer driver are stored in the following locations:

    - PCL 5e

      32-bit driver D:\X86\DRIVERS\PCL5E\XP_VISTA\(Language)\DISK1

      64-bit driver D:\X64\DRIVERS\PCL5E\X64\(Language)\DISK1
    - PCL 6

      32-bit driver D:\X86\DRIVERS\PCL6\XP_VISTA\MUI\DISK1

      64-bit driver D:\X64\DRIVERS\PCL6\X64\MUI\DISK1
    - PostScript 3

      32-bit driver D:\X86\DRIVERS\PS\XP_VISTA\MUI\DISK1

      64-bit driver D:\X64\DRIVERS\PS\X64\MUI\DISK1

    For details about the languages supported in the printer drivers, see p.6 "Supported languages".
13. **Click [Open].**
14. **Click [OK] to close the [Install From Disk] window.**
15. **Select the manufacturer and model name of the machine you want to use, and then click [Next].**
16. **Follow the instructions that appear. Modify settings such as printer name, default printer, and printer sharing configuration, as necessary. You can also print a test page.**

17. **Click [Finish].**

    If installation is successful, the icon of the printer connected to the WSD port will appear in the window for configuring printers.

Note

- To stop installation of the selected driver, click [Cancel] before the installation is complete. When re-installing the WSD Port, right-click the machine's icon in the [Network] window, and then click [Uninstall].

Using the SmartDeviceMonitor for Client port

PCL PS3

To use this function, you must first download SmartDeviceMonitor for Client from the manufacturer's Web site and install it on your computer. Contact your local dealer for information on downloading SmartDeviceMonitor for Client.

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

   For details about the languages supported in the printer drivers, see p.6 "Supported languages".
4. **Click [PCL Printer Drivers] or [PostScript 3 Printer Driver].**
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].**

   If installing the PostScript 3 printer driver, proceed to step 7.
6. **Select a printer driver you want to use, and then click [Next].**
7. **Select the check box of the machine model you want to use.**
8. **Double-click the machine name to display the printer settings.**
9. **Click [Port :], and then click [Add] in the [Change settings for 'Port'] box.**
10. **Click [SmartDeviceMonitor], and then click [OK].**
11. **To configure port settings using TCP/IP, click [TCP/IP], and then click [Search].**

    To configure port settings using IPP, proceed to step 13.
12. **Select the machine you want to use, and then click [OK].**

    Only machines that respond to a broadcast from the computer appear. To use a machine not listed here, click [Specify Address], and then enter the IP address or host name of the machine.

    Proceed to step 18.
13. **To configure port settings using IPP, click [IPP].**

14. **In the [Printer URL] box, enter "http://machine's IP address/printer" as the machine's address.**

    If the server authentication is issued, enter "https://machine's IP address/printer" to enable SSL (a protocol for encrypted communication). Example IP address: 192.168.15.16

    http://192.168.15.16/printer

    https://192.168.15.16/printer

    You can enter "http://machine's IP address/ipp" as the machine's address.

15. **Enter a name for identifying the machine in the [IPP Port Name] box. Use a name different from the one of any existing ports.**

    If a name is not specified here, the address entered in the [Printer URL] box becomes the IPP port name.

16. **Click [Detailed Settings] Settings to make necessary settings.**

    For details about the settings, see SmartDeviceMonitor for Client Help.

17. **Click [OK].**
18. **Check that the port of the selected printer is displayed in [Port :].**
19. **Configure the user code, default printer, and shared printer as necessary.**
20. **Click [Continue].**

    The installation starts.

21. **Click [Finish].**

    Select one of the options to restart the computer either now or later, and then click [Finish].

Changing the port settings for SmartDeviceMonitor for Client

Follow the procedure below to change the SmartDeviceMonitor for Client settings, such as TCP/IP protocol.

Windows XP, Windows Server 2003/2003 R2

1. **On the [Start] menu, click [Printers and Faxes].**
2. **Click the icon of the machine you want to use. On the [File] menu, click [Properties].**
3. **Click the [Ports] tab, and then click [Configure Port].**

    The [Port Configuration:] window appears.

Windows Vista, Windows Server 2008:

1. **On the [Start] menu, click [Control Panel].**
2. **Click [Printer].**
3. **Right-click the icon of the machine you want to use, and then click [Properties].**

4. **Click the [Ports] tab, and then click [Configure Port].**

   The [Port Configuration:] window appears.

Windows 7, Windows Server 2008 R2:

1. **On the [Start] menu, click [Devices and Printers].**
2. **Right-click the icon of the machine you want to use, and then click [Printer Properties].**
3. **Click the [Ports] tab, and then click [Configure Port].**

   The [Port Configuration:] window appears.

Note

- User, proxy, and timeout settings can be configured for IPP.
- For details about these settings, see SmartDeviceMonitor for Client Help.

Using as a Network Printer

Describes the driver installation procedure for each print server. See the installation procedure for the print server you are using.

Important

- **When using NetWare, an optional NetWare unit is required.**

Server OS	Client OS	Printer Driver Type	Reference
Windows Server	Windows	PCL PS3	p.22 "Using Windows print server"
NetWare	Windows	PCL PS3	p.23 "Using NetWare print server"

Using Windows print server

PCL PS3

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

   For details about the languages supported in the printer drivers, see p.6 "Supported languages".
4. **Click [PCL Printer Drivers] or [PostScript 3 Printer Driver].**

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].**

   If installing the PostScript 3 printer driver, proceed to step 7.

6. **Select a printer driver you want to use, and then click [Next].**
7. **Select the check box of the machine model you want to use.**
8. **Double-click the machine name to display the machine settings.**
9. **Click [Port :], and then click [Add] in the [Change settings for 'Port'] box.**
10. **Click [Network Printer], and then click [OK].**
11. **Double-click the computer name you want to use as a print server in the [Browse for Printer] window.**
12. **Select the machine you want to use, and then click [OK].**
13. **Check that the port of the selected printer is displayed in [Port :].**
14. **Configure the user code, default printer, and shared printer as necessary.**
15. **Click [Continue].**

    The installation starts.

16. **Click [Finish].**

    Select one of the options to restart the computer either now or later, and then click [Finish].

Note

- If you print with a print server connected to the machine using the SmartDeviceMonitor for Client port, Recovery Printing and Parallel Printing cannot be used from the client computer.
- If you print under Windows Vista/7 or Windows Server 2008 print server, notification functions of SmartDeviceMonitor may not be used with the client computer.

Using NetWare print server

PCL PS3

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 AUTORUN.EXE].

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

   For details about the languages supported in the printer drivers, see p.6 "Supported languages".

4. **Click [PCL Printer Drivers] or [PostScript 3 Printer Driver].**
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].**

   If installing the PostScript 3 printer driver, proceed to step 7.

6. **Select a printer driver you want to use, and then click [Next].**
7. **Select the check box of the machine model you want to use.**
8. **Double-click the machine name to display the printer settings.**
9. **Click [Port :], and then click [Add] in the [Change settings for 'Port'] box.**
10. **Click [Network Printer], and then click [OK].**
11. **Double-click the name of the NetWare file server on the network tree.**

    The created queue is displayed.
12. **Select the print queue, and then click [OK].**
13. **Check that the port of the selected printer is displayed in [Port :].**
14. **Click [Continue].**

    The installation starts.
15. **Click [Finish] in the [Select Program] dialog box.**
16. **After the installation is completed, select one of the options to restart the computer either now or later, and then click [Finish].**

    Restart the computer to complete installation.
17. **After restarting the computer, open the printer window.**
    - Windows XP, Windows Server 2003/2003 R2:

      On the [Start] menu, select [Printers and Faxes].
    - Windows Vista, Windows Server 2008:

      On the [Start] menu, select [Control Panel], and then click [Printers] in [Hardware and Sound] category.
    - Windows 7, Windows Server 2008 R2:

      On the [Start] menu, select [Devices and Printers].
18. **Open the printer properties dialog box.**
    - Windows XP/Vista, Windows Server 2003/2008:

      Right-click the machine's icon, and then click [Properties].
    - Windows 7, Windows Server 2008 R2:

      Right-click the machine's icon, and then click [Printer properties].
19. **Click the [NetWare Settings] tab.**
20. **Clear the [Form Feed] and [Enable Banner] check boxes.**

    Do not select these check boxes since they are automatically selected by the printer driver. If you select the check boxes, the printer may not print correctly.
21. **Click [OK].**

Note

- The protocol is set to inactive as default. Enable the protocol on the control panel, using Web Image Monitor, SmartDeviceMonitor or telnet.

Notes when using NetWare

Form Feed

Do not use NetWare to configure form feed. Form feed is controlled by the printer driver on Windows. If NetWare form feed is configured, the printer may not print properly.

Follow the procedure below to disable form feed according to the operating system used:

- Clear the [Form feed] check box on the [NetWare Settings] tab in the printer properties dialog box.

Banner Page

Do not use NetWare to configure banner page.

Follow the procedure below to disable banner page according to the operating system used:

- Clear the [Enable banner] check box on the [NetWare Settings] tab in the printer properties dialog box.

When using the PostScript 3 Printer Driver

Follow the procedure below to set up the PostScript 3 printer driver.

1. Open the printer window.
   - Windows XP, Windows Server 2003/2003 R2:

     On the [Start] menu, select [Printers and Faxes].
   - Windows Vista, Windows Server 2008:

     On the [Start] menu, select [Control Panel], and then click [Printers] in [Hardware and Sound] category.
   - Windows 7, Windows Server 2008 R2:

     On the [Start] menu, select [Devices and Printers].
2. Open the printer properties dialog box.
   - Windows XP/Vista, Windows Server 2003/2008:

     Right-click the machine's icon, and then click [Properties].
   - Windows 7, Windows Server 2008 R2:

     Right-click the machine's icon, and then click [Printer properties].
3. Click the [Device Settings] tab.
4. Select [No] on the [Send CTRL-D Before Each Job:] and [Send CTRL-D After Each Job:], and then click [Apply].

5. Click [OK].

Printing after Resetting the Printer

Printer to print server connection requires 30 - 40 seconds to resume after the printer is reset. During this period, jobs may be accepted (depending on NetWare specifications) but not printed.

To print after resetting the printer as the remote printer, check on the print server that the remote printer is disconnected, or wait for two minutes before trying to print.

Installing the Printer Driver for a Local Connection

This section describes the installation procedure of the printer drivers for USB, parallel, or Bluetooth connection.

Important

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

Note

- If the [User Account Control] dialog box appears in driver installation procedure, click [Yes] or [Continue].
- If the [Windows Security] dialog box appears in driver installation procedure, click [Install this driver software anyway].
- A message appears if there is a newer version of the printer driver already installed. If there is, you cannot install the printer driver using Auto Run. If you still want to install the printer driver, use [Add Printer]. See p.49 "Messages Displayed When Installing the Printer Driver".

USB Connection

This section explains how to install the printer drivers using USB.

Before installing, check that only the operating system is running on the computer and no print jobs are in progress.

If the printer driver has already been installed, and plug and play is enabled, the icon of the printer connected to the "USB" port is added to the [Printers], [Printers and Faxes], or [Devices and Printers] window.

If the printer driver is not installed, follow the plug-and-play instructions of the machine to install it from the CD-ROM provided with this machine.

Note

- To disable Auto Run, press the left Shift key when inserting the CD-ROM into the drive and keep it pressed until the computer finishes reading from the CD-ROM.

Windows XP, Windows Server 2003/2003 R2

1. **Quit all applications. (Do not close this manual.)**
2. **Check that the power of the machine is off.**

3. **Connect the machine and computer using the USB cable.**

   Connect the USB cable firmly.

4. **Turn on the power of the machine.**

   Found New Hardware Wizard starts, and USB Printing Support is installed automatically.

5. **Select [No, not this time], and then click [Next].**
6. **Click [Install from a list or specific location [Advanced]], and then click [Next].**
7. **Insert the provided CD-ROM into the computer's CD-ROM drive.**

   If Auto Run starts, click [Cancel] and then [Exit].

8. **Select the [Search removable media (floppy, CD-ROM...)] check box under [Search for the best driver in these locations.], and then click [Next].**
9. **Select the name of the machine whose driver you want to install.**

   Check the location where the source files of the printer driver is stored.

   If the CD-ROM drive is D, the source files are stored in the following locations:

   - PCL 5e

     32-bit driver D:\X86\DRIVERS\PCL5E\XP_VISTA\(Language)\DISK1

     64-bit driver D:\X64\DRIVERS\PCL5E\X64\(Language)\DISK1

   - PCL 6

     32-bit driver D:\X86\DRIVERS\PCL6\XP_VISTA\MUI\DISK1

     64-bit driver D:\X64\DRIVERS\PCL6\X64\MUI\DISK1

   - PostScript 3

     32-bit driver D:\X86\DRIVERS\PS\XP_VISTA\MUI\DISK1

     64-bit driver D:\X64\DRIVERS\PS\X64\MUI\DISK1

   For details about the languages supported in the printer drivers, see p.6 "Supported languages".

10. **Click [Next].**

    The installation starts.

11. **Click [Finish].**

    If the printer driver has already been installed and plug and play is enabled, the icon of the printer connected to the "USB001" port is added to the [Printers], [Printers and Faxes], or [Devices and Printers] window.

    The number after "USB" varies depending on the number of printers connected.

Windows Vista, Windows Server 2008

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

2. **Check that the power of the machine is off.**
3. **Connect the machine and computer using a USB cable.**

   Connect the USB cable firmly.
4. **Turn on the power of the machine.**

   Found New Hardware Wizard starts, and USB Printing Support is installed automatically.
5. **In the [Found New Hardware] window, click [Locate and install driver software (recommended)].**
6. **Insert the provided CD-ROM into the computer's CD-ROM drive.**

   If the [AutoPlay] dialog box appears, click [Close].
7. **Select the name of the machine whose driver you want to install.**

   Check the location where the source files of the printer driver is stored.

   If the CD-ROM drive is D, the source files are stored in the following locations:

   - PCL 5e

     32-bit driver D:\X86\DRIVERS\PCL5E\XP_VISTA\(Language)\DISK1

     64-bit driver D:\X64\DRIVERS\PCL5E\X64\(Language)\DISK1
   - PCL 6

     32-bit driver D:\X86\DRIVERS\PCL6\XP_VISTA\MUI\DISK1

     64-bit driver D:\X64\DRIVERS\PCL6\X64\MUI\DISK1
   - PostScript 3

     32-bit driver D:\X86\DRIVERS\PS\XP_VISTA\MUI\DISK1

     64-bit driver D:\X64\DRIVERS\PS\X64\MUI\DISK1

   For details about the languages supported in the printer drivers, see p.6 "Supported languages".
8. **Click [Next].**

   The installation starts.
9. **Click [Close].**

   If the printer driver has already been installed and plug and play is enabled, the icon of the printer connected to the "USB001" port is added to the [Printers], [Printers and Faxes], or [Devices and Printers] window.

   The number after "USB" varies depending on the number of printers connected.

Windows 7, Windows Server 2008 R2

1. **Quit all applications. (Do not close this manual.)**
2. **Check that the power of the machine is off.**

3. **Connect the machine and computer using a USB cable.**

   Connect the USB cable firmly.

4. **Turn on the power of the machine.**

   Found New Hardware Wizard starts, and USB Printing Support is installed automatically.

5. **Click [Devices and Printers] from the [Start] menu.**
6. **Double-Click the icon of machine you want to use in the [Unspecified] category.**
7. **Click the [Hardware] tab.**
8. **Click [Properties].**
9. **Click the [General] tab.**
10. **Click [Change settings].**
11. **Click [Driver] tab.**
12. **Click [Update Driver...].**
13. **Click [Browse my computer for driver software].**
14. **Insert the provided CD-ROM into the computer's CD-ROM drive.**

    If the [AutoPlay] dialog box appears, click [Close].

15. **Click [Browse], and then select the printer driver location.**

    If the CD-ROM drive is D, the source files of the printer driver are stored in the following locations:

    - PCL 5e

      32-bit driver D:\X86\DRIVERS\PCL5E\XP_VISTA\(Language)\DISK1

      64-bit driver D:\X64\DRIVERS\PCL5E\X64\(Language)\DISK1

    - PCL 6

      32-bit driver D:\X86\DRIVERS\PCL6\XP_VISTA\MUI\DISK1

      64-bit driver D:\X64\DRIVERS\PCL6\X64\MUI\DISK1

    - PostScript 3

      32-bit driver D:\X86\DRIVERS\PS\XP_VISTA\MUI\DISK1

      64-bit driver D:\X64\DRIVERS\PS\X64\MUI\DISK1

    For details about the languages supported in the printer drivers, see p.6 "Supported languages".

16. **Click [Next].**

    The installation starts.

17. **Click [Close].**

    If the printer driver has already been installed and plug and play is enabled, the icon of the printer connected to the "USB001" port is added to the [Printers], [Printers and Faxes], or [Devices and Printers] window.

    The number after "USB" varies depending on the number of printers connected.

Parallel Connection

To use a printer connected using a parallel interface, click [LPT1] when installing the printer driver.

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

   For details about the languages supported in the printer drivers, see p.6 "Supported languages".
4. **Click [PCL Printer Drivers] or [PostScript 3 Printer Driver].**
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].**

   If installing the PostScript 3 printer driver, proceed to step 7.
6. **Select a printer driver you want to use, and then click [Next].**
7. **Select the check box of the machine model you want to use.**
8. **Double-click the machine name to display the printer settings.**
9. **Click [Port :].**
10. **Select [LPT1:] in the [Change settings for 'Port'] drop-down list.**
11. **Configure the user code, default printer, and shared printer as necessary.**
12. **Click [Continue].**

    The installation starts.
13. **Click [Finish].**

    Select one of the options to restart the computer either now or later, and then click [Finish].

Bluetooth Connection

Important

- **The Bluetooth unit and the optional wireless LAN unit cannot be used simultaneously.**

Supported profiles and restrictions

Supported Profiles

- SPP (Serial Port Profile)
- HCRP (Hardcopy Cable Replacement Profile)
- BIP (Basic Imaging Profile)

Restrictions on SPP, HCRP

- A maximum of two Bluetooth adaptor or Bluetooth-equipped computers can be connected at the same time using the Bluetooth interface: one by SPP, one by HCRP.
- When connecting more than one Bluetooth adaptor or Bluetooth-equipped computer at the same time, the first device that establishes connection is selected. When selecting the connection between the other devices, cancel the first established connection.
- SPP connection does not support bidirectional communications.
- HCRP connection supports bidirectional communications.
- Depending on the machine, additional printer option may be required to use SPP, HCRP. To see if your machine requires additional printer option, see the manual provided with the machine.

Restrictions on BIP

- PostScript 3 must be installed on the printer to connect via BIP. For information about PostScript 3, see the manual provided with the printer.
- Only one Bluetooth adaptor or Bluetooth-equipped computer can be connected via BIP.
- Only JPEG images can be printed using BIP.
- User codes are disabled for BIP.
- You cannot print if print functions are restricted.
- Some printers do not support BIP.

Instructions in this manual relate to printing via HCRP. To print using SPP or BIP, see the Help supplied with the Bluetooth adapter you want to use, or the Microsoft Web site.

Adding a Bluetooth printer

If your computer is running SP1 or an earlier version of Windows XP, there are additional applications that you must install. For details about these, see the Help supplied with your Bluetooth device.

Important

- **To connect to a Bluetooth printer, your computer must have a Bluetooth device installed. Make sure a Bluetooth device is installed on your computer.**

Windows XP, Windows Server 2003/2003 R2

1. **Quit all applications. (Do not close this manual.)**
2. **On the [Start] menu, click [Printers and Faxes].**
3. **Click [Add a printer].**
4. **Click [Next].**

5. **Click [Bluetooth Printer], and then click [Next].**

   The computer begins searching for available Bluetooth printers.

   If a new printer is discovered, the [Found New Hardware Wizard] window appears. To ignore a discovered device and continue searching, click [Cancel]. The computer resumes searching for other available Bluetooth printers.

6. **Click [No, I will not connect], and then click [Next].**
7. **Click [Install from a list or specific location (Advanced)], and then click [Next].**
8. **Insert the CD-ROM provided with this machine into your computer's CD-ROM drive, select the [Search removable media (floppy, CD-ROM...)] check box, and then click [Next].**
9. **If the [Hardware Installation] window appears, click [Continue].**
10. **If the installation was successful, click [Finish].**
11. **Select [Test Print], and then click [Next].**
12. **Click [Finish].**

Note

- Actual Bluetooth printer operations will vary according to your Bluetooth device and/or Bluetooth-installed computer. For details, see the Help supplied with your Bluetooth device and/or Bluetooth-equipped computer.
- After printing the test page, check it, and then click [Close] to close the window.
- If there is a problem with the test page, click [Troubleshooting] in the test print window.

Windows Vista, Windows Server 2008

1. **Quit all applications. (Do not close this manual.)**
2. **On the [Start] menu, click [Control Panel].**
3. **In the "Hardware and Sound" area, click [Printers].**
4. **In the top part of the window, click [Add a printer].**
5. **In the [Add Printer] window, select [Add a network, wireless or Bluetooth printer], and then click [Next].**

   The computer begins searching for available Bluetooth devices.

6. **From the list of discovered devices, select the machine you want to use, and then click [Next].**

   All discovered wireless printers appear in the list of discovered printers, not only Bluetooth printers.

   Make sure the machine you select is a Bluetooth printer.

7. **Insert the CD-ROM provided with this machine into your computer's CD-ROM drive, and then click [Browse my computer for driver software (advanced)] on the [Found New Hardware] display.**

8. **In the [Found New Hardware] window, select the printer driver you want to use, and then click [Next].**

   The installation starts.

9. **If the [Windows Security] window appears, click [Install this driver software anyway].**
10. **Click [Close].**
11. **If you want to change the printer name, enter the new name in the [Printer Name Settings] window.**
12. **If you want to print a test page, click [Printing Test Page] on the "Test Print" page.**

    Otherwise, click [Finish].

Note

- If you print the test page, after checking it, click [Close] to close the test print window.
- If there is a problem with the test page, click [Troubleshooting Printer Problems] in the test print window.

Windows 7, Windows Server 2008 R2

1. **Quit all applications. (Do not close this manual.)**
2. **On the [Start] menu, click [Devices and Printers].**
3. **Click [Add a printer].**
4. **Click [Add a network, wireless or Bluetooth printer].**

   The computer begins searching for available Bluetooth devices.

5. **From the list of discovered devices, select the machine you want to use, and then click [Next].**
6. **If you want to change the printer name, enter the new name in the [Printer Name:], and then click [Next].**
7. **To share the printer, configure the necessary settings, and then click [Next].**
8. **If you want to print a test page, click [Print a test page] on the "Test Print" page.**

   Otherwise, click [Finish].

Note

- If you print the test page, after checking it, click [Close] to close the test print window.
- If there is a problem with the test page, click [Get help with printing] in the test print window.

Configuring Option Settings for the Printer

When bidirectional communication works correctly, your computer obtains information about option, paper size and paper feed direction settings from the machine automatically. Bidirectional communication also allows you to monitor machine status.

When bidirectional communication is disabled, you have to set up option, paper size and paper feed direction settings on your computer manually.

Conditions for Bidirectional Communication

To support bidirectional communication, the following conditions must be met:

When connected with parallel cables

- The computer must support bidirectional communication.
- The interface cable must support bidirectional communication.
- The machine must be connected to the computer using the standard parallel cables and parallel connectors.

When connected with the network

- The Standard TCP/IP port must be used.
- In addition to the above, one of the following conditions must also be met:
  - The TCP/IP protocol or the IPP protocol is used. (When using the IPP protocol, the IPP port name must include the IP address.)

When connected with USB

- The machine must be connected to the computer's USB port using the USB interface cable.
- The computer must support bidirectional communication.
- [Enable bidirectional support] must be selected, and [Enable printer pooling] must not be selected on the [Ports] tab with the printer driver.

Note

- The PCL 6 and PostScript 3 printer drivers support bidirectional communication and automatic printer status updates.
- To obtain printer information automatically using the bidirectional communication function of the PCL 6 or PostScript 3 printer driver, you must select the [Automatically Update Printer Information] check box on the [Accessories] tab in the printer driver's properties window.
- The PCL 5e printer driver supports bidirectional communication. You can update the printer status manually.

If Bidirectional Communication is Disabled

This section describes how to set up option, paper size and paper feed direction settings on your computer manually.

Important

- **Manage Printers permission is required to change the printer properties. Log on as an Administrators group member.**

1. **Open the printer window.**
   - Windows XP, Windows Server 2003:

     On the [Start] menu, select [Printers and Faxes].
   - Windows Vista, Windows Server 2008:

     On the [Start] menu, select [Control Panel], and then click [Printers] in [Hardware and Sound] category.
   - Windows 7, Windows Server 2008 R2:

     On the [Start] menu, select [Devices and Printers].
2. **Open the printer properties dialog box.**
   - Windows XP/Vista, Windows Server 2003/2008:

     Right-click the machine's icon, and then click [Properties].
   - Windows 7, Windows Server 2008 R2:

     Right-click the machine's icon, and then click [Printer properties].
3. **Click the [Accessories] tab.**

   If options in the [Accessories] tab are disabled, bidirectional connection is enabled. In this case, no change is necessary for option settings.
4. **Select options installed from the [Options] area, and then make the necessary settings.**
5. **Click [Change Input Tray Settings...].**
6. **In [Input Tray:] select which trays to use, and then, in [Paper Size:] select the size of the paper that you want to load in each tray.**

   Click [Modify Input Tray/Paper Size] to apply the setting for each tray.
7. **Click [OK].**
8. **Click [OK] to close the printer properties window.**

Note

- For details about making option settings for the machine using a Mac OS X, see p.57 "Configuring Option Settings for the Printer Under Mac OS X".

Installing Font Manager

Important

- Manage Printers permission is required to install Font Manager. Log on as an Administrators group member.
- The operating systems compatible with Font Manager are Windows XP/Vista.

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 AUTORUN.EXE].
3. Select an interface language, and then click [OK].
4. Click [Font Manager].
5. Follow the instructions on the display.

3. Installing the Scanner Driver

This chapter explains how to install the TWAIN driver on a client computer.

Installing the TWAIN Driver

To use the network TWAIN scanner, you must install the TWAIN driver on a client computer.

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

   For details about the languages supported in the TWAIN driver, see p.7 "TWAIN Driver".
4. **Click [TWAIN Driver].**
5. **The installer of the TWAIN driver starts. Follow the instructions.**

Note

- Before you start the installation, check the system requirements for the TWAIN driver. For details about the system requirements, see p.5 "Software and Utilities Included on the CD-ROM".
- When the installation is complete, a message about restarting the client computer may appear. In this case, restart the client computer.
- After the installation is complete, a folder with the name of the machine in use is added in [Programs] or [All Programs] on the [Start] menu. Help can be displayed from here.
- Notes on using the network TWAIN scanner are provided in "Readme.txt". Be sure to read them before use.

Installing a TWAIN-Compliant Application on the Same Client Computer

To use this machine as a network TWAIN scanner, a TWAIN-compliant application, such as DeskTopBinder, must be installed on the client computer.

You can download DeskTopBinder from the manufacturer's Web site and then install it on the client computer. For details about DeskTopBinder, see "Software that You Can Download", Getting Started.

4. Installing the Facsimile Driver

This chapter explains how to install and configure the LAN-Fax driver on a client computer.

Installing the LAN-Fax Driver

Address Book and LAN-Fax Cover Sheet Editor are installed with the LAN-Fax Driver. Address Book helps you edit LAN-Fax transmission destinations. LAN-Fax Cover Sheet Editor helps you edit LAN-Fax cover sheets.

Important

- **Manage Printers permission is required to install the drivers. Log on as an Administrators group member.**
- **In an IPv6 environment, you cannot use the Standard TCP/IP port. Use the SmartDeviceMonitor for Client port.**

Enabling the function to prevent transmission to the wrong destination

The following function is available to prevent a document from being transmitted to the wrong destination even if the incorrect destination was entered. To enable this function, edit the configuration file before you install the driver.

- Prompt user to reenter the destination number multiple times.
- Prompt user to confirm that the destination number is correct.
- Allow user to select the destination from the destination list only, and prohibit the destination from being manually entered.

For details, see p.44 "Enabling the Function to Prevent Transmission to the Wrong Destination".

Specifying the same port as the printer driver

If a port name that is the same as one that is already in use by the existing driver is specified, the LAN-FAX driver installation may fail. If the printer driver is already installed, make sure that the port numbers of the LAN-FAX driver and the printer driver match.

For details, see p.41 "Specifying the Same Port as the Printer Driver".

Specifying the Same Port as the Printer Driver

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

   For details about the languages supported in the LAN-Fax driver, see p.8 "LAN-Fax Driver".

4. **Click [LAN-Fax Driver].**
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. **Double-click [Printer Name : <LAN-Fax M(number)>].**
8. **Click [Port:].**
9. **Select the same port as the one selected in the printer driver from the ['Change settings for 'Port'] drop-down list.**
10. **Click [Continue].**

    The installation starts.
11. **Click [Finish].**

    Select one of the options to restart the computer either now or later, and then click [Finish].

Specifying the Port When Installing the LAN-FAX Driver

To specify a port that is different from the printer driver when installing the LAN-FAX driver, see the installation procedure of the printer driver.

If places where the procedure or description differs depending on the driver to be installed, replace the corresponding procedure or description accordingly, and install the driver.

Installation procedures	Corresponding items to replace
p.15 "Using the Standard TCP/IP port"	1, 2, 4
p.15 "Using the IPP port"	3
p.17 "Using the LPR port"	1, 2, 4
p.18 "Using the WSD port"	3
p.20 "Using the SmartDeviceMonitor for Client port"	1, 2, 4

List of Items to Replace

No.	Items to be replaced	Procedure/description in the printer driver	Procedure/description in the LAN-Fax driver
1	The name of the button that starts the installation procedure	Click [PCL Printer Drivers] or [PostScript 3 Printer Driver].	Click [LAN-Fax Driver].

No.	Items to be replaced	Procedure/description in the printer driver	Procedure/description in the LAN-Fax driver
2	The procedures in the [Install Printer Driver] dialog box	• Select the check box of the machine model you want to use. • Double-click the machine name to display the printer settings.	Double-click [Printer Name : <LAN-Fax M(number)>].
3	The destination folder in which the driver files are stored	The destination folder is written in the description.	The LAN-FAX driver is installed in the following folder: • 32-bit driver X86\DRIVERS\LAN-FAX\XP_VISTA\DISK1 • 64-bit driver X64\DRIVERS\LAN-FAX\X64\DISK1
4	Availability of the User Code setting	Can be specified.	Cannot be specified.

Enabling the Function to Prevent Transmission to the Wrong Destination

To enable the function to prevent transmission to the wrong destination, edit the configuration file before you install the driver. This section explains how to edit the configuration file and install the LAN-Fax driver using the edited configuration file.

Editing the Configuration File

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 [Close].
3. **Copy the LAN-FAX driver in the provided CD-ROM to the hard disk of your computer.**

   If the drive letter of the CD-ROM drive is "D:", copy one of the following folders. Select either 32-bit or 64-bit version according to the environment you are using. Do not copy the files to the desktop or a directory whose path name contains multi-byte characters.

   - 32-bit driver D:\X86\DRIVERS\LAN-FAX
   - 64-bit driver D:\X64\DRIVERS\LAN-FAX
4. **Open the file "IfxShLnk.ini" that has been copied to your computer using a text editor.**
5. **Edit the items that are related to the prevention function.**

   Edit the following three items:

   - ConfirmFAXNo

     Syntax: ConfirmFAXNo=0/1/2/3/4/5/6/7/8/9/10

     Description: Specify the number of times the confirmation dialog box for reentering the destination number appears. Enter the number of times to prompt the user to reenter the destination from 0 to 10.

     Example: ConfirmFAXNo=1
   - ConfirmAddress

     Syntax: ConfirmAddress=ON/OFF

     Description: When set to "ON", the destination confirmation dialog appears.

     Example: ConfirmAddress=ON
   - ProhibitDirectAddress

     Syntax: ProhibitDirectAddress=ON/OFF

     Description: When set to "ON", the destination cannot be entered manually.

     Example: ProhibitDirectAddress=ON

6. **Save the configuration file that has been edited.**

Installing the LAN-FAX driver in "Add Printer"

Install the LAN-FAX driver after the configuration file has been edited.

1. **Open the printer window.**
   - Windows XP, Windows Server 2003:

     On the [Start] menu, select [Printers and Faxes].
   - Windows Vista, Windows Server 2008:

     On the [Start] menu, select [Control Panel], and then click [Printers] in [Hardware and Sound] category.
   - Windows 7, Windows Server 2008 R2:

     On the [Start] menu, select [Devices and Printers].
2. **Click [Add Printer] or [Add a printer].**
3. **Click [Add a local printer].**
4. **Select the port.**
   - To use the same port as the printer drive:
     1. Click [Use an existing port:].
     2. Select the same port as the one selected in the printer driver from the [Use an existing port:] list.
     3. Click [Next].
   - To use another Standard TCP/IP port:
     1. Click [Create a new port:].
     2. Select [Standard TCP/IP Port] in the [Type of port:] list.
     3. Click [Next].
     4. Enter the machine name or IP address in the [Hostname or IP address:] box.
     5. Click [Next].
5. **Select the manufacturer and model name of the machine you want to use, and then click [Next].**
6. **Change the machine name if you want, and then click [Next].**

   The installation starts.
7. **Follow the instructions that appear. Modify settings such as the default printer and printer sharing configuration, as necessary. You can also print a test page.**

8. **Click [Finish].**

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

Setting LAN-Fax Driver Properties

Note

- Manage Printers permission is required to set the properties for the LAN-Fax driver. Log on as an Administrators group member.
- The method for selecting the LAN-Fax driver will vary according to your operating system. For details, see Windows Help.

Setting Print Properties

This section explains how to make settings such as paper size or resolution.

1. **Open the printer window.**
   - Windows XP, Windows Server 2003/2003 R2:

     On the [Start] menu, select [Printers and Faxes].
   - Windows Vista, Windows Server 2008:

     On the [Start] menu, select [Control Panel], and then click [Printers] in [Hardware and Sound] category.
   - Windows 7, Windows Server 2008 R2:

     On the [Start] menu, select [Devices and Printers].
2. **Open the printer properties dialog box.**
   - Windows XP/Vista, Windows Server 2003/2003 R2/2008:

     Right-click the [LAN-Fax M(number)] icon, and then click [Properties].
   - Windows 7, Windows Server 2008 R2:

     Right-click the [LAN-Fax M(number)] icon, and then click [Printer properties].
3. **To set the following properties.**
   - Paper Size
   - Orientation
   - Tray
   - Resolution
4. **Click [OK].**

Configuring Option Settings for the Facsimile

1. **Open the printer windows.**
   - Windows XP, Windows Server 2003/2003 R2:

     On the [Start] menu, select [Printers and Faxes].
   - Windows Vista, Windows Server 2008:

     On the [Start] menu, select [Control Panel], and then click [Printers] in [Hardware and Sound] category.
   - Windows 7, Windows Server 2008 R2:

     On the [Start] menu, select [Devices and Printers].
2. **Open the printer properties dialog box.**
   - Windows XP/Vista, Windows Server 2003/2003 R2/2008:

     Right-click the [LAN-Fax M(number)] icon, and then click [Properties].
   - Windows 7, Windows Server 2008 R2:

     Right-click the [LAN-Fax M(number)] icon, and then click [Printer properties].
3. **Click the [Accessories] tab, and then make the settings for the option configuration.**
4. **Select the check boxes for the installed optional units.**
5. **Click [Apply].**

   Option configuration settings are complete.
6. **Click [OK].**

[Accessories] tab

The [Accessories] tab contains the following items besides option configuration items.

- Enable E-mail

  Check this when using Internet Fax with the LAN-Fax function.
- IP-Fax

  Check this option when using IP-Fax.

  After checking this option, select a protocol by clicking an appropriate radio button.

Note

- If the options on this machine are not configured as instructed, LAN-Fax functions may fail.
- If this machine is connected to a network and SmartDeviceMonitor for Client is installed on your computer, configuration of each option installed on the machine will be performed automatically. If the settings do not match the installed optional units, click [Load from Device].

5. Troubleshooting

This chapter provides solutions for driver installation and USB connection problems.

Messages Displayed When Installing the Printer Driver

This section describes what to do if a message appears when installing the printer driver.

Message number 58 or 34 indicates that the printer driver cannot be installed using Auto Run. Install the printer driver using Add Printer Wizard.

Message number 58 appears if there is a newer version of the printer driver already installed.

1. **Open the printer window.**
   - Windows XP, Windows Server 2003/2003 R2:

     On the [Start] menu, select [Printers and Faxes].
   - Windows Vista, Windows Server 2008:

     On the [Start] menu, select [Control Panel], and then click [Printers] in [Hardware and Sound] category.
   - Windows 7, Windows Server 2008 R2:

     On the [Start] menu, select [Devices and Printers].
2. **Click [Add a printer].**
3. **Follow the instructions in Add Printer Wizard.**

   If the CD-ROM drive is D, the source files of the printer driver are stored in the following locations:
   - PCL 5e

     32-bit driver D:\X86\DRIVERS\PCL5E\XP_VISTA\(Language)\DISK1

     64-bit driver D:\X64\DRIVERS\PCL5E\X64\(Language)\DISK1
   - PCL 6

     32-bit driver D:\X86\DRIVERS\PCL6\XP_VISTA\MUI\DISK1

     64-bit driver D:\X64\DRIVERS\PCL6\X64\MUI\DISK1
   - PostScript 3

     32-bit driver D:\X86\DRIVERS\PS\XP_VISTA\MUI\DISK1

     64-bit driver D:\X64\DRIVERS\PS\X64\MUI\DISK1

   For details about the languages supported in the printer drivers, see p.6 "Supported languages".
4. **Specify a port.**

Note

- Available ports vary according to your Windows operating system or the type of interface. For details, see p.11 "Confirming the Connection Method".

If USB Connection Fails

This section describes how to troubleshoot a problem related to USB connections.

Problem	Causes	Solutions
The machine is not automatically recognized.	The USB cable is not connected properly.	Disconnect the USB cable, and then turn off the main power switch. Turn on the main power switch again. When the machine has fully booted up, reconnect the USB cable.
Windows has already configured the USB settings.	Check whether the computer has identified the machine as an unsupported device.	Open Windows' Device Manager, and then, under [Universal Serial Bus controllers], remove any conflicting devices. Conflicting devices have a [!] or [?] icon by them. Take care not to accidentally remove required devices. For details, see Windows Help.
The machine does not recognize the USB connection even when a USB cable is inserted.	If the USB cable is connected while the machine is off, the machine might not recognize the USB connection.	Press the operation switch, and then disconnect the USB cable. When the machine has returned to the ready condition, reconnect the USB cable.

6. Installing the Printer Driver Under Mac OS X

This chapter explains how to install and configure the printer drivers for use on the Mac OS X operating system.

Installing the PPD Files

To print using the printer specific features under Mac OS X, install the PPD files.

Important

- Mac OS X 10.2 or higher is required.
- You need an administrator name and a password (phrase). For details, consult your network administrator.
- For the latest information on the corresponding operating system, see the "Readme.txt" file in the DRIVERS folder.

1. Quit all applications. (Do not close this manual.)
2. Insert the provided CD-ROM into the computer's CD-ROM drive.
3. Double-click the CD-ROM drive icon.
4. Double-click the [Mac OS X] folder.
5. Double-click the [(brand name)] folder.
6. Double-click the [Mac OS X 10.2 or later] or [Mac OS X 10.5 or later] folder, depending on your operating system.
7. Double-click the [MacOSX PPD Installer] folder.
8. Double-click the package file icon.
9. Follow the instructions on the screen.

Note

- The PPD files will be automatically installed in the following location:
  - Mac OS X 10.2 - 10.4:

    \Library\Printers\PPDs\Contents\Resources\(language code *1).lproj

    *1 da=Danish, de=German, en=English, es=Spanish, fr=French, it=Italian, nl=Dutch, no=Norwegian, sv=Swedish
  - Mac OS X 10.5 - 10.6:

    \Library\Printers\PPDs\Contents\Resources\

Registering the Printer

To use the machine, the printer must be registered in the printer list.

Make sure the machine and computer are connected and turned on, and perform the following procedure.

For how to connect the machine to the computer, see "Connecting the Machine", Connecting the Machine/ System Settings.

Important

- **Depending on the machine you are using, PostScript 3 unit must be installed.**

Note

- When printing with a USB connection to a Macintosh computer, the printer language does not change automatically. Use the control panel on this machine to change the printer language to [Auto Detect] or [PS] before printing.
- The operating procedure under Mac OS X differs depending on the version of the operating system. Consult the procedure described in this manual, and make the necessary settings according to the manual of each version.

USB Connection

Important

- **Make sure the computer and the machine are connected using the USB cable, and the power of the devices are turned on beforehand.**
- **USB2.0 can be used only with Mac OS X 10.3.3 or higher.**

Mac OS X 10.2 - 10.3

1. **Start Print Center or Printer Setup Utility in Applications\Utilities.**
2. **Click [Set Up Printers].**

   Depending on your computer's operating system, [Set Up Printers] may not appear.
3. **Click [Add].**
4. **Select [USB] on the pop-up menu.**
5. **Select the machine.**
6. **Select the machine you are using from the [Printer Model:] pop-up menu.**

   If the machine you are using is not selected in [Printer Model:], select its manufacturer or [Other...] in the pop-up menu, and then select the PPD file of the machine. For the location of the PPD files, see p.53 "Installing the PPD Files".

7. **Click [Choose].**
8. **Click [Add].**

   If the option settings need to be configured, see p.57 "Configuring Option Settings for the Printer Under Mac OS X".
9. **Quit Print Center or Printer Setup Utility.**

Mac OS X 10.4 - 10.6

1. **Start System Preferences.**
2. **Click [Print & Fax].**
3. **Click the [+] button.**
4. **Click [Default Browser] or [Default].**
5. **Select the machine that has "USB" indicated in the [Connection] or [Kind] column.**
6. **Select the machine you are using from the [Print Using:] pop-up menu.**

   If the machine you are using is not selected in [Print Using:], select its manufacturer, [Select a driver to use...], or [Select Printer Software...] in the pop-up menu, and then select the PPD file of the machine. For the location of the PPD files, see p.53 "Installing the PPD Files".
7. **Click [Add].**

   If the option settings need to be configured, click [Configure...] in the dialog box that appears, and then configure the option settings.
8. **Quit System Preferences.**

Network Connection

Mac OS X 10.2 - 10.3

1. **Start Print Center or Printer Setup Utility in Applications\Utilities.**
2. **Click [Set Up Printers].**

   Depending on your computer's operating system, [Set Up Printers] may not appear.
3. **Click [Add].**
4. **Select [Directory Services] on the pop-up menu, and then select [Rendezvous].**
5. **Select the machine.**

   If the machine name is not displayed, select the icon that corresponds to your network environment (TCP/IP, etc.).

6. **Select the machine you are using from the [Printer Model:] pop-up menu.**

   If the machine you are using is not selected in [Printer Model:], select its manufacturer or [Other...] in the pop-up menu, and then select the PPD file of the machine. For the location of the PPD files, see p.53 "Installing the PPD Files".

7. **Click [Choose].**
8. **Click [Add].**

   If the option settings need to be configured, see p.57 "Configuring Option Settings for the Printer Under Mac OS X".

9. **Quit Print Center or Printer Setup Utility.**

Mac OS X 10.4 - 10.6

1. **Start System Preferences.**
2. **Click [Print & Fax].**
3. **Click the [+] button.**
4. **Click [Default Browser] or [Default].**
5. **Select the machine that has "Bonjour" indicated in the [Connection] or [Kind] column.**

   If the machine name is not displayed, select the icon that corresponds to your network environment (TCP/IP, etc.).

6. **Select the machine you are using from the [Print Using:] pop-up menu.**

   If the machine you are using is not selected in [Print Using:], select its manufacturer, [Select a driver to use...], or [Select Printer Software...] in the pop-up menu, and then select the PPD file of the machine. For the location of the PPD files, see p.53 "Installing the PPD Files".

7. **Click [Add].**

   If the option settings need to be configured, click [Configure...] in the dialog box that appears, and then configure the option settings.

8. **Quit System Preferences.**

Configuring Option Settings for the Printer Under Mac OS X

This section explains how to configure the printer driver.

Mac OS X 10.2 - 10.3

1. **Start Print Center or Printer Setup Utility in Applications\Utilities.**
2. **Click [Set Up Printers...].**

   Depending on your computer's operating system, [Set Up Printers...] may not appear.
3. **Select the machine you are using, and then click [Show Info] on the [Printers] menu.**
4. **Select [Installable Options] in the pop-up menu, and then configure settings needed.**
5. **Click [Apply Changes], and then close the [Printer Info] dialog box.**
6. **Quit Print Center or Printer Setup.**

Mac OS X 10.4

1. **Start System Preferences.**
2. **Click [Print & Fax].**
3. **Select the machine you are using, and then click [Printer Setup...].**
4. **Select [Installable Options] in the pop-up menu, and then configure settings as needed.**
5. **Click [Apply Changes], and then close the [Printer Info] dialog box.**
6. **Quit System Preferences.**

Mac OS X 10.5 - 10.6

1. **Start System Preferences.**
2. **Click [Print & Fax].**
3. **Select the machine you are using, and then click [Options & Supplies...].**
4. **Click [Driver], and then configure settings as needed.**
5. **Click [OK].**
6. **Quit System Preferences.**

Note

- If the option you want to select is not displayed, PPD files may not be set up correctly. To complete the setup, check the name of the PPD file displayed in the dialog box.

7. Appendix

Updating or Deleting the Driver

Important

- **Administrator permission is required to update or delete the driver in use. Log on as an Administrators group member.**

Note

- If the [User Account Control] dialog box appears, click [Yes] or [Continue].
- If the [Windows Security] dialog box appears, click [Install this driver software anyway].

Updating the Driver

Printer driver / LAN-Fax driver

You can download the most recent version of the driver from the manufacturer's Web site. Download the latest driver, and then perform the following procedure.

1. **Open the printer window.**
   - Windows XP, Windows Server 2003:

     On the [Start] menu, select [Printers and Faxes].
   - Windows Vista, Windows Server 2008:

     On the [Start] menu, select [Control Panel], and then click [Printers] in [Hardware and Sound] category.
   - Windows 7, Windows Server 2008 R2:

     On the [Start] menu, select [Devices and Printers].
2. **Open the printer properties dialog box.**
   - Windows XP/Vista, Windows Server 2003/2008:

     Right-click the machine's icon, and then click [Properties].
   - Windows 7, Windows Server 2008 R2:

     Right-click the machine's icon, and then click [Printer properties].
3. **Click the [Advanced] tab.**
4. **Click [New Driver...], and then click [Next].**
5. **Click [Have Disk...].**
6. **Click [Browse...], and then select the driver location.**

7. **Click [OK].**
8. **Select the machine model, and then click [Next].**

   The driver update starts.
9. **Click [Finish].**
10. **Click [OK] to close the printer properties window.**
11. **Restart the computer.**

TWAIN driver

You can download the most recent version of the TWAIN driver from the manufacturer's Web site.

Delete the old version of the TWAIN driver first, and then install the new TWAIN driver. For details about how to delete the driver, see p.60 "Deleting the Driver".

Deleting the Driver

Printer driver / LAN-Fax driver

Windows XP, Windows Server 2003/2003 R2

1. **On the [Start] menu, click [Printers and Faxes].**
2. **Right-click the icon of the machine you want to delete, and then click [Delete].**
3. **Click [Server Properties] on the [File] menu.**
4. **Click the [Drivers] tab.**
5. **Select the driver you want to delete, and then click [Remove].**
6. **Click [Yes].**
7. **Click [Close] to close the print server properties window.**

Windows Vista, Windows Server 2008

1. **On the [Start] menu, select [Control Panel], and then click [Printers] in [Hardware and Sound] category.**
2. **Right-click the icon of the machine you want to delete, and then click [Delete].**
3. **On the [File] menu, point to [Run as administrator], and then click [Server Properties...].**
4. **Click the [Drivers] tab.**
5. **Select the driver you want to delete, and then click [Remove...].**
6. **Select [Remove driver and driver package.], and then click [OK].**
7. **Click [Yes].**

8. Click [Delete].
9. Click [OK].
10. Click [Close] to close the print server properties window.

Windows 7, Windows Server 2008 R2

1. On the [Start] menu, click [Devices and Printers].
2. Right-click the icon of the machine you want to delete, and then click [Remove Device].
3. Click [Yes].
4. Click any machine icon, and then click [Print server properties].
5. Click the [Drivers] tab.
6. Click the [Change Driver Settings] button if it is displayed.
7. Select the driver you want to delete, and then click [Remove...].
8. Select [Remove driver and driver package.], and then click [OK].
9. Click [Yes].
10. Click [Delete].
11. Click [OK].
12. Click [Close] to close the print server properties window.

TWAIN driver

1. Start uninstaller.
   - Windows XP, Windows Server 2003/2003 R2:

     On the [Start] menu, select [Control Panel], and then click [Add or Remove Programs].
   - Windows Vista/7, Windows Server 2008 R2:

     On the [Start] menu, select [Control Panel], and then click [Uninstall a program].
   - Windows Server 2008:

     On the [Start] menu, select [Control Panel], and then double-click [Programs and Features].
2. Remove the TWAIN driver.
   - Windows XP, Windows Server 2003/2003 R2:
     1. Select [(model type) TWAIN Driver Ver.4].
     2. Click [Change/Remove].
   - Windows Vista/7, Windows Server 2008/2008 R2:
     1. Select [(model type) TWAIN Driver Ver.4].
     2. Click [Uninstall/Change].

3. **Quit uninstaller.**

Trademarks

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

Macintosh, and Mac OS are registered trademarks of Apple Inc, registered in the U.S. and other countries.

IPS is a trademark or registered trademark of Zoran Corporation and/or its subsidiaries in the United States or other countries.

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

Monotype is a registered trademark of Monotype Imaging, Inc.

NetWare, IPX, IPX/SPX are either registered trademarks or trademarks of Novell, Inc.

PCL® is a registered trademark of Hewlett-Packard Company.

Other product names used herein are for identification purposes only and might be trademarks of their respective companies. We disclaim any and all right to those marks.

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

- The product names of Windows 2000 are as follows:

  Microsoft® Windows® 2000 Professional

  Microsoft® Windows® 2000 Server

  Microsoft® Windows® 2000 Advanced Server
- The product names of Windows XP are as follows:

  Microsoft® Windows® XP Professional Edition

  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 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

INDEX

MEMO

MEMO

MEMO

EN GB EN US EN AU D127-7518

Operating Instructions

Security Guide

For safe and correct use, be sure to read the Safety Information in "Read This First" before using the machine.

TABLE OF CONTENTS

3. Restricting Machine Usage

4. Preventing Leakage of Information from Machines

5. Enhanced Network Security

6. Preventing the Leaking of Documents

7. Managing the Machine

8. Troubleshooting

9. Checking Operation Privileges

Functions That Require Options

The following functions require certain options and additional functions.

- Data security for copying function

  Copy Data Security Unit

Main Software Products

Product name	Names in the text
DeskTopBinder Lite and DeskTopBinder Professional *1	DeskTopBinder
ScanRouter EX Professional *1 and ScanRouter EX Enterprise *1	the ScanRouter delivery software
Remote Communication Gate S Pro for @Remote Enterprise *2 and Remote Communication Gate S *2	Remote Communication Gate S

*1 This product is no longer sold.

*2 Sold separately.

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

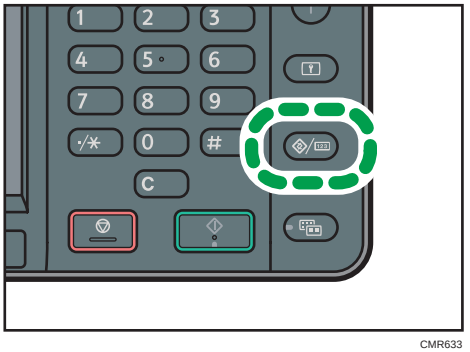
- **If the security settings are not configured, the data in the machine is vulnerable to attack.**

1. To prevent this machine being stolen or willfully damaged, etc., install it in a secure location.
2. 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.
3. 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 Using the Security Functions".
4. Administrators must inform users regarding proper usage of the security functions.
5. Administrators should routinely examine the machine's logs to check for irregular and unusual events.
6. If this machine is connected to a network, its environment must be protected by a firewall or similar.
7. 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.

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



CMR633

3. **Press [System Settings].**
4. **Press [Interface Settings].**
5. **Press [Network].**
6. **Specify IPv4 Address.**

   For details on how to specify the IPv4 address, see "Interface Settings", Connecting the Machine/ System Settings.

7. **Be sure to connect this machine to a network that only administrators can access.**
8. **Start Web Image Monitor, and then log in to the machine as the administrator.**

   For details about logging in to Web Image Monitor as an administrator, see p.22 "Administrator Login Method".

9. **Point to [Device Management], and then click [Configuration].**
10. **Click [Email] under "Device Settings".**
11. **Enter the e-mail address of the administrator of this machine in "Administrator Email Address" and click [OK].**
12. **Install the device certificate.**

    For information on how to install the device certificate, see p.127 "Protecting the Communication Path via a Device Certificate".

    The settings for device certificate creation can be configured only if an administrator e-mail address is specified.

13. **Enable SSL/TLS.**

    For details about enabling SSL/TLS, see p.132 "Configuring SSL/TLS".

14. **Change the administrator's user name and password.**

    For details about specifying administrators' user names and passwords, see p.21 "Using Web Image Monitor to Configure Administrator Authentication".

15. **Log out and then close Web Image Monitor.**

16. **Disconnect this machine from the administrator-only access network, and then connect it to the general usage network environment.**

Note

- To enable higher security, see p.270 "Additional Information for Enhanced Security"

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 p.18 "Registering and Changing Administrators", and for instructions on changing the administrator's password, see p.25 "Supervisor". For details on Users, see p.29 "Users".

Important

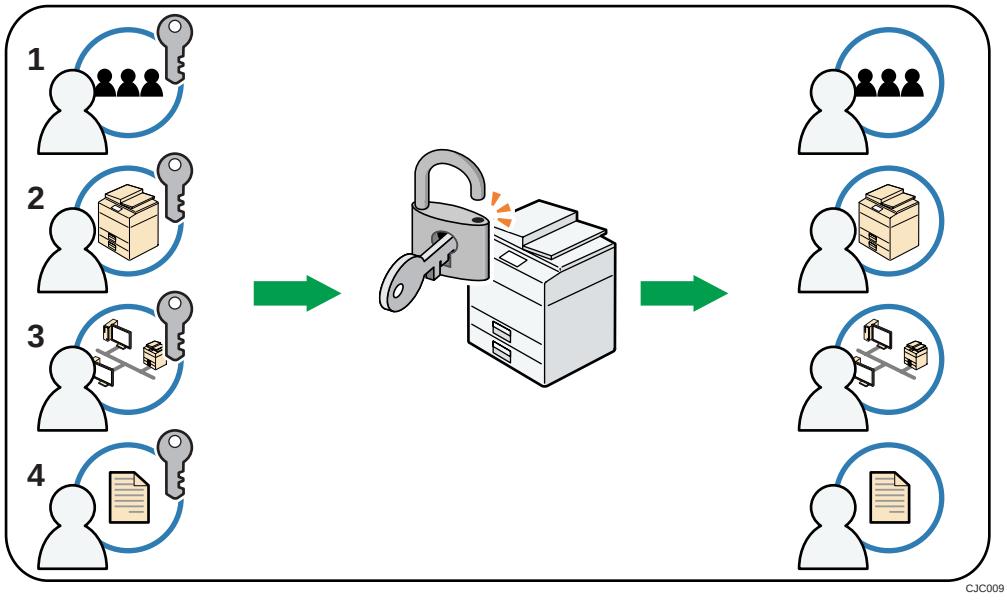
- **If user authentication is not possible because of a problem with the hard disk or network, you can use the machine by accessing it using administrator authentication and disabling user authentication. Do this if, for instance, you need to use the machine urgently.**

Configuring Administrator Authentication

Administrator authentication is a mechanism by which an administrator ID is confirmed via a login user name and password when an administrator starts to make the various settings of this machine or when accessing the machine 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 p.18 "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 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 p.31 "Configuring User Authentication".

Roles of each administrator



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]. Once settings are activated, the default setting items allocated to each administrator become controlled items.

To log in as an administrator, use the default login user name and login password.

The default login user name is "admin". No login password is configured.

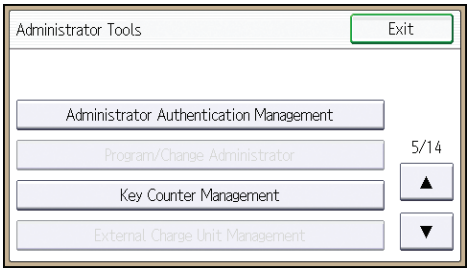
For details about logging in and logging out with administrator authentication, see p.22 "Administrator Login Method" and p.24 "Administrator Logout Method".

Important

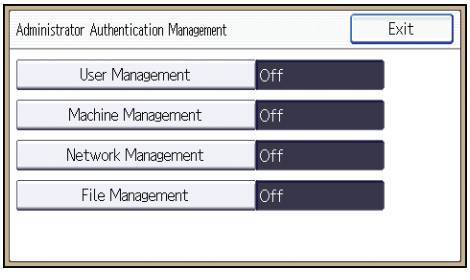
- **If you have enabled "Administrator Authentication Management", make sure not to forget the administrator login user name and login password. If an administrator login user name or login password is forgotten, a new password must be specified using the supervisor's privilege. For details on supervisor privileges, see p.25 "Supervisor".**

- 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 all data in the machine being lost. Charges may also apply to the service call.

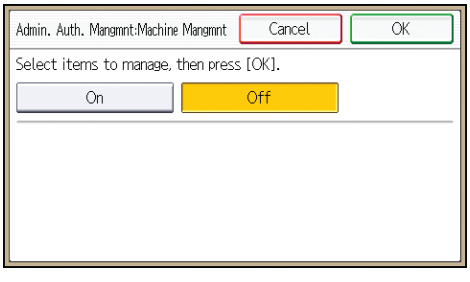
1. Press the [User Tools/Counter] key.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [▼] four times.
5. Press [Administrator Authentication Management].



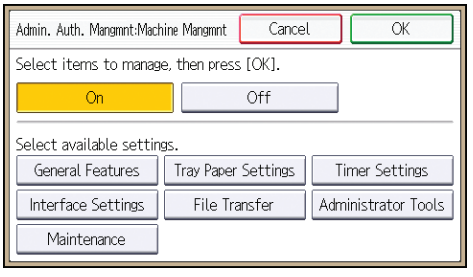
6. Press [User Management], [Machine Management], [Network Management], or [File Management] to select which settings to manage.



7. Press [On].



8. **Select the settings to manage.**



The selected settings will be unavailable to users.

The available settings (settings that can be made) differ for each administrator.

To specify administrator authentication for more than one category, repeat steps 6 to 8.

9. **Press [OK].**
10. **Press the [User Tools/Counter] key.**

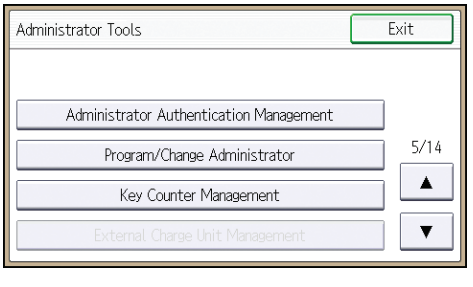
Registering and Changing Administrators

If administrator authentication has been specified, we recommend only one person take each administrator role.

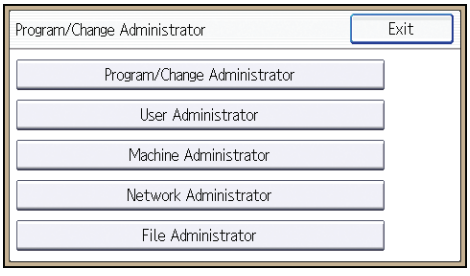
The sharing of administrator tasks eases the burden on individual administrators while also limiting unauthorized operation by a single administrator. You can register up to four login user names (Administrators 1-4) to which you can grant administrator privileges.

For details about logging in and logging out with administrator authentication, see p.22 "Administrator Login Method" and p.24 "Administrator Logout Method".

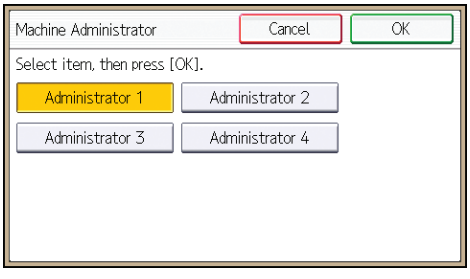
1. **The administrator logs in from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼] four times.**
5. **Press [Program/Change Administrator].**



6. **Select a category so that administrator settings can be specified from User Administrator, Machine Administrator, Network Administrator and File Administrator.**



7. **Select the number of the administrator and press [OK].**

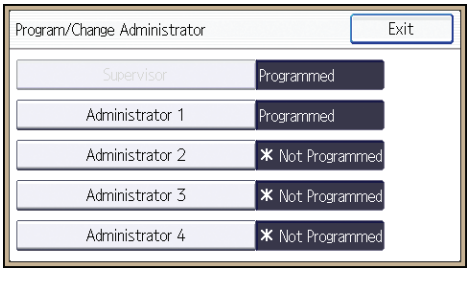


When assigning privileges to each administrator individually, specify administrator numbers in each category separately. For example, if you specify [Administrator 1] for [User Administrator], then specify [Administrator 2] for [Machine Administrator].

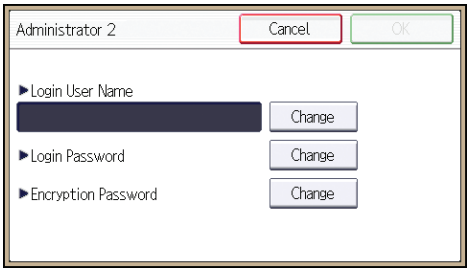
To combine the privileges of multiple administrators, assign multiple privileges to a single administrator number.

For example, if you want to combine user and machine administrator privileges for [Administrator 1], specify [Administrator 1] for both [User Administrator] and [Machine Administrator].

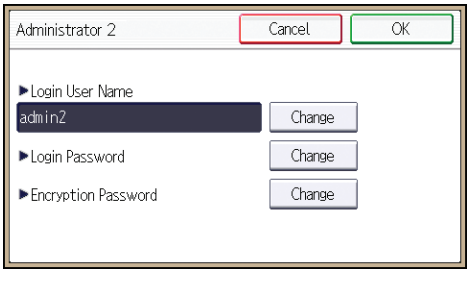
8. **Press [Program/Change Administrator].**
9. **Select the number of the administrator whose user name and password you want to change, and then press [OK].**



10. **Press [Change] for "Login User Name".**



11. **Enter the login user name, and then press [OK].**
12. **Press [Change] for "Login Password".**



13. **Enter the login password, and then press [OK].**

    Follow the password policy to make the login password more secure.

    For details about the password policy and how to specify it, see p.259 "Specifying the Extended Security Functions".

14. **Re-enter the login password for confirmation, and then press [OK].**
15. **Press [Change] for "Encryption Password".**
16. **Enter the encryption password, and then press [OK].**
17. **Re-enter the encryption password for confirmation, and then press [OK].**
18. **Press the [Login/Logout] key.**

    A confirmation message appears.

    If you press [Yes], you will be automatically logged out.

Note

- For the characters that can be used for login user names and passwords, see p.21 "Usable characters for user names and passwords".
- An administrator's privileges can only be changed by an administrator with the relevant privileges.
- Administrator privileges cannot be revoked by any single administrator.

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

- Spaces, colons, and quotation marks cannot be used.
- Cannot have blanks or only numbers.
- May 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.
- A password can be set up if it fulfill the conditions for complexity and minimum length, as per [Password Policy] in [Extended Security]. For how to set up passwords according to the password policy, see "Password Policy" in p.259 "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 p.22 "Administrator Login Method" and p.24 "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

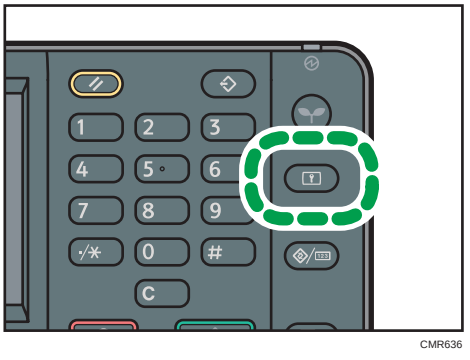
- For details about Web Image Monitor, see Web Image Monitor Help.

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.

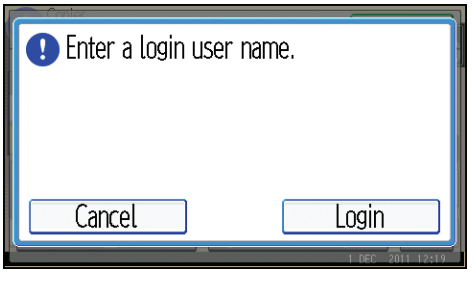
Logging in Using the Control Panel

1. **Press the [User Tools/Counter] key.**
2. **Press the [Login/Logout] key.**



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. Because of this, do not enter anything for the password and simply 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.

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].
3. **Click [Login].**
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.

Logging out Using the Control Panel

1. **Press the [Login/Logout] key.**
2. **Press [Yes].**

Note

- You can log out using the following procedures also.
  - Press the [Energy Saver] key.

Logging out Using Web Image Monitor

1. **Click [Logout] to log out.**

Note

- Delete the cache memory in Web Image Monitor after logging out.

Supervisor

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 logged in using the supervisor's user name and password, you cannot use normal functions or specify defaults. The methods for logging in and out are the same as for administrators.

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 p.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 all data in the machine being lost and the service call may not be free of charge.**

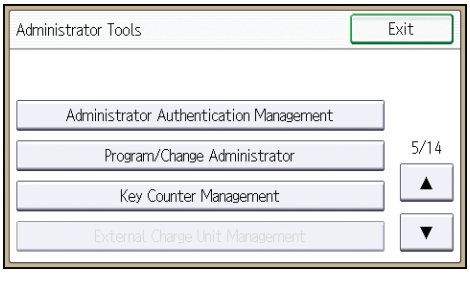
Note

- 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.

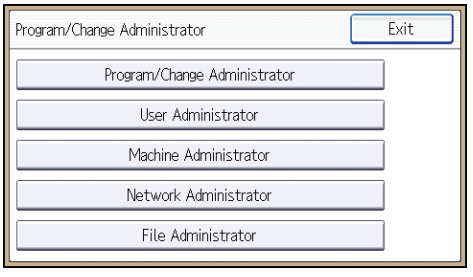
Resetting the Administrator's Password

1. **The supervisor logs in from the control panel.**

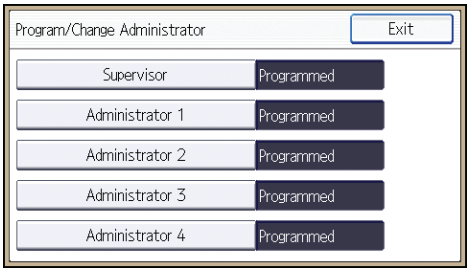
   For details on how to log in, see p.22 "Administrator Login Method".
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼] four times.**
5. **Press [Program/Change Administrator].**



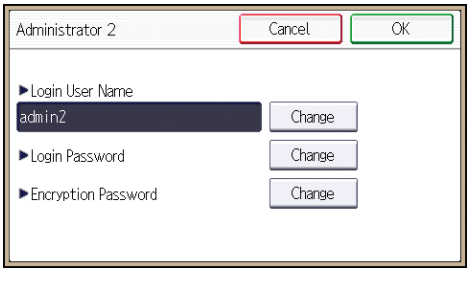
6. **Press [Program/Change Administrator].**



7. **Select the administrator number you want to reset.**



8. **Press [Change] for "Login Password".**



9. **Enter the login password, and then press [OK].**
10. **Re-enter the login password for confirmation, and then press [OK].**
11. **Press [Change] for "Encryption Password".**
12. **Re-enter the encryption password for confirmation, and then press [OK].**
13. **Press the [Login/Logout] key.**

    A confirmation message appears.

    If you press [Yes], you will be automatically logged out.

Note

- Log in as the supervisor only to change an administrator's password. Administrator's login names cannot be changed.

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 p.16 "Specifying Administrator Privileges".

1. **The supervisor logs in from the control panel.**

   For details on how to log in, see p.22 "Administrator Login Method".
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼] four times.**
5. **Press [Program/Change Administrator].**
6. **Press [Program/Change Administrator].**
7. **Press [Supervisor].**
8. **Press [Change] for "Login User Name".**
9. **Enter the login user name, and then press [OK].**
10. **Press [Change] for "Login Password".**
11. **Enter the login password, and then press [OK].**
12. **Re-enter the login password for confirmation, and then press [OK].**
13. **Press the [Login/Logout] key.**

    A confirmation message appears.

    If you press [Yes], you will be automatically logged out.

2. Configuring User Authentication

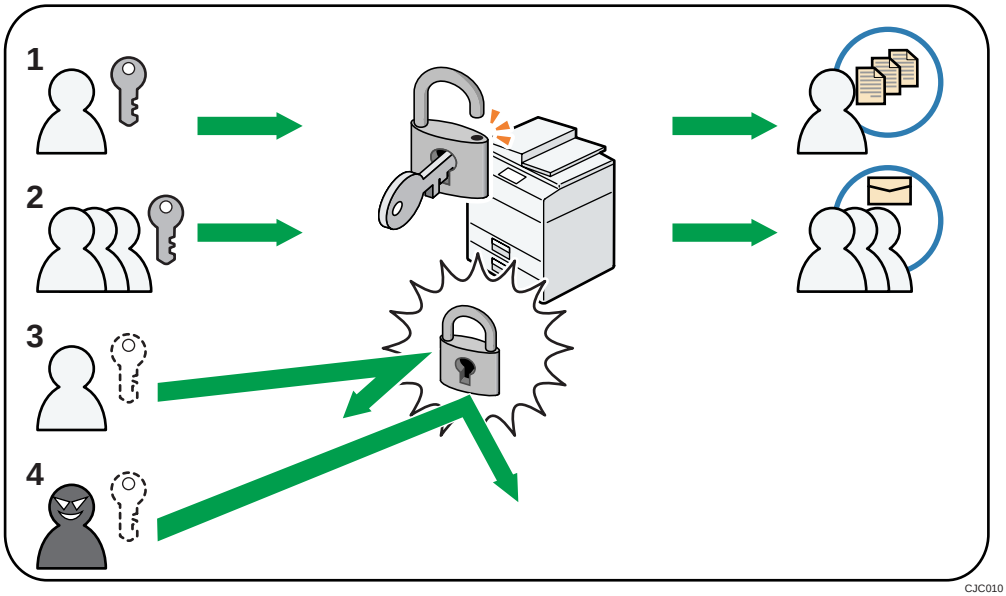
This chapter describes how to specify user authentication and explains the functions that are enabled by user authentication.

Users

A user performs normal operations on the machine, such as copying and printing. Users are managed using the personal information in the machine's Address Book, and can use only 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 p.14 "Administrators". For details about user registration, see "Registering User Information", Connecting the Machine/ System Settings or Web Image Monitor Help.

About User Authentication

User authentication is a process by which the user's ID is confirmed via a login user name and password when the user starts to use this machine or when accessing the machine from a network.



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

To control users' access to the machine, perform user authentication using login user names and passwords. 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.**

User authentication configuration flow

Configuration procedure	Details
Configuring administrator authentication	p.16 "Specifying Administrator Privileges" p.18 "Registering and Changing Administrators"
Configuring user authentication	Specify user authentication. Five types of user authentication are available: • p.33 "User Code Authentication" • p.36 "Basic Authentication" • p.42 "Windows Authentication" • p.51 "LDAP Authentication" • p.57 "Integration Server Authentication"

Note

- To specify Basic authentication, Windows authentication, LDAP authentication, or Integration Server authentication, you must first enable user administrator privileges in "Administrator Authentication Management".
- You can specify User Code authentication without specifying administrator authentication.
- User Code authentication is used for authenticating on the basis of a user code, and Basic authentication, Windows authentication, LDAP authentication, and Integration Server authentication are used for authenticating individual users.
- 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 p.39 "Specifying Login User Names and Passwords".
- You cannot use more than one authentication method at the same time.
- If a user's e-mail address has been obtained via Windows authentication, LDAP authentication or Integration Server authentication, when e-mail from the scanner is sent, or a received fax is forwarded by e-mail, the sender's address (From) is fixed, allowing ID fraud to be prevented.
- 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 "Authentication Information", Connecting the Machine/ System Settings.

For details about specifying the user code for the printer driver, see Print or the printer driver Help.

For details about specifying the LAN-Fax driver user code, see the LAN-Fax driver Help.

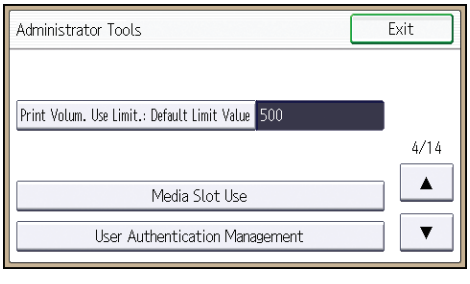
For details about specifying the TWAIN driver user code, see the TWAIN driver Help.

Important

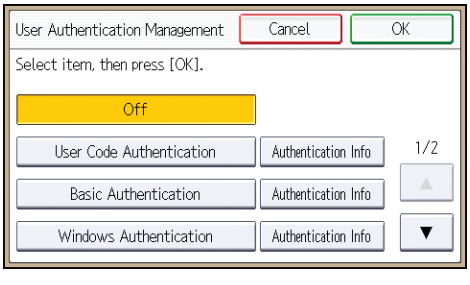
- **To control the use of DeskTopBinder for the delivery of files stored in the machine, select Basic authentication, Windows authentication, LDAP authentication, or Integration Server authentication.**

Specifying User Code Authentication

1. **The machine administrator logs in from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼] three times.**
5. **Press [User Authentication Management].**

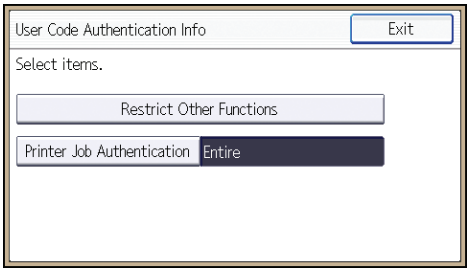


6. **Select [User Code Authentication], and then press [Authentication Info] next to it.**

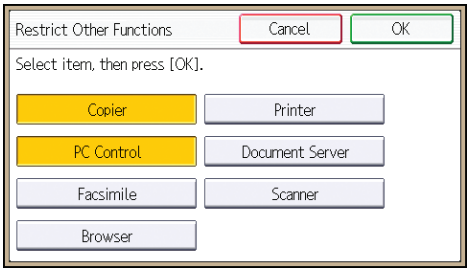


If you do not want to use user authentication management, select [Off].

7. **Press [Restrict Other Functions].**



8. **Select which of the machine's functions you want to limit.**



If the function you want to select is not displayed, press [▼].

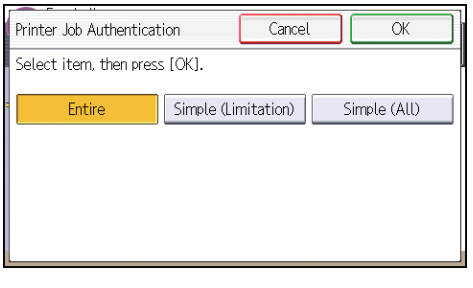
The selected functions are subject to User Code authentication. User Code authentication is not applied to the functions not selected.

For details about limiting available functions for individuals or groups, see p.80 "Limiting Available Functions".

To enable printer job authentication, either deselect [PC Control] for "Restrict Other Functions" or select [Restrict Printer Functions].

If you do not want to specify printer job authentication, proceed to step 15.

9. **Press [OK].**
10. **Press [Printer Job Authentication].**
11. **Select the printer job authentication level.**

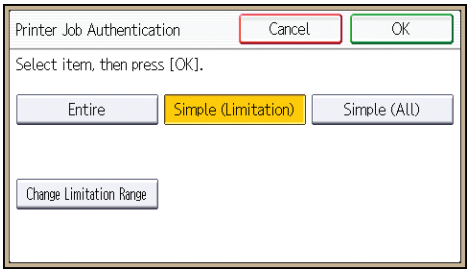


For a description of the printer job authentication levels, see p.63 "Printer Job Authentication".

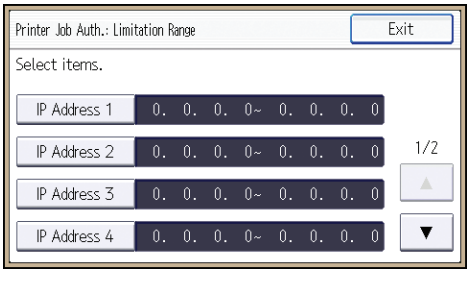
If you select [Entire] or [Simple (All)], proceed to step 16.

If you select [Simple (Limitation)], proceed to step 13.

12. **Press [Change Limitation Range].**



13. **Specify the range in which [Simple (Limitation)] is applied to "Printer Job Authentication".**



Pressing [▼] allows you to display all items.

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 [OK].**
16. **Press [Exit], and then press [OK].**
17. **Press the [Login/Logout] key.**

A confirmation message appears.

If you press [Yes], you will be automatically logged out.

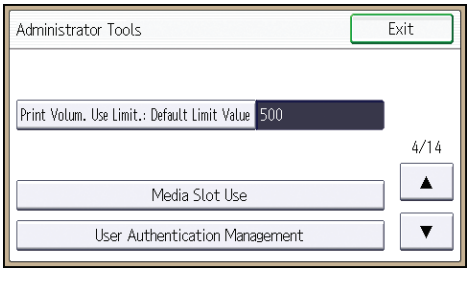
Basic Authentication

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 personal data in 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 p.38 "Authentication Information Stored in the Address Book".

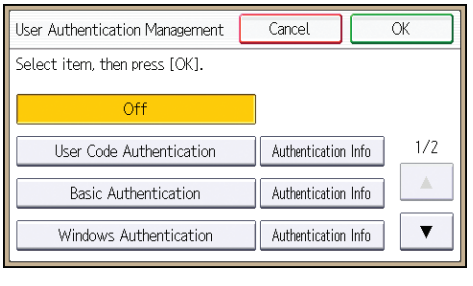
Specifying Basic Authentication

Before beginning to configure the machine, make sure that administrator authentication is properly configured under "Administrator Authentication Management".

1. **The machine administrator logs in from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼] three times.**
5. **Press [User Authentication Management].**

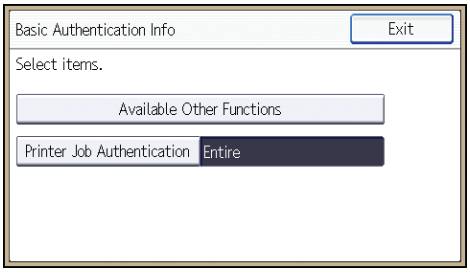


6. **Select [Basic Authentication], and then press [Authentication Info] next to it.**

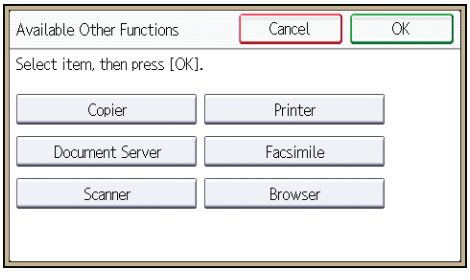


If you do not want to use user authentication management, select [Off].

7. **Press [Available Other Functions].**



8. **Select which of the machine's functions you want to permit.**

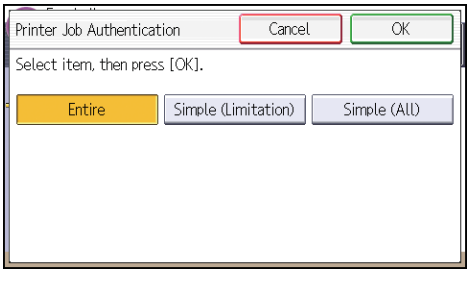


If the function you want to select is not displayed, press [▼].

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 p.80 "Limiting Available Functions".

9. **Press [OK].**
10. **Press [Printer Job Authentication].**
11. **Select the printer job authentication level.**

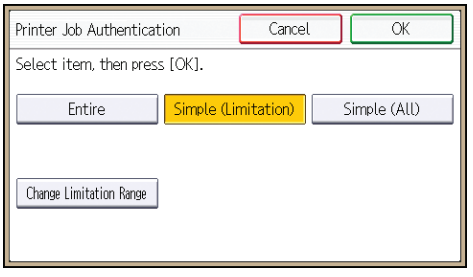


For a description of the printer job authentication levels, see p.63 "Printer Job Authentication".

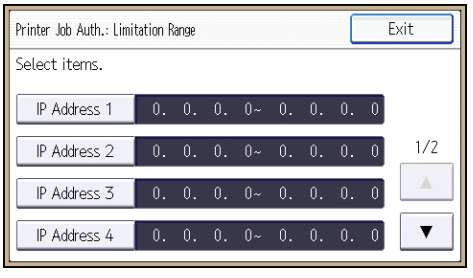
If you select [Entire] or [Simple (All)], proceed to step 16.

If you select [Simple (Limitation)], proceed to step 13.

12. **Press [Change Limitation Range].**



13. **Specify the range in which [Simple (Limitation)] is applied to "Printer Job Authentication".**



Pressing [▼] allows you to display all items.

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 [OK].**
16. **Press the [Login/Logout] key.**

A confirmation message appears.

If you press [Yes], 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 p.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, see "Registering Names", Connecting the Machine/ System Settings.

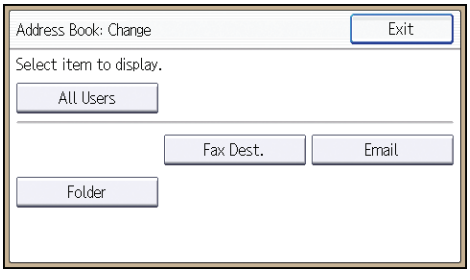
User authentication can also be specified via Web Image Monitor. For details, see Web Image Monitor Help.

Specifying Login User Names and Passwords

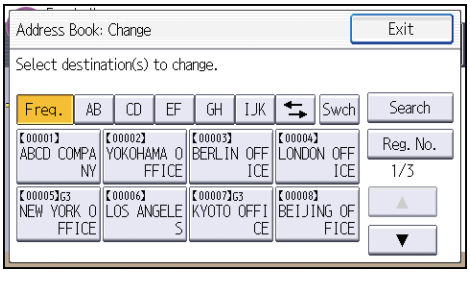
In "Address Book Management", specify the login user name and login password to be used for "User Authentication Management".

For the characters that can be used for login user names and passwords, see p.21 "Usable characters for user names and passwords".

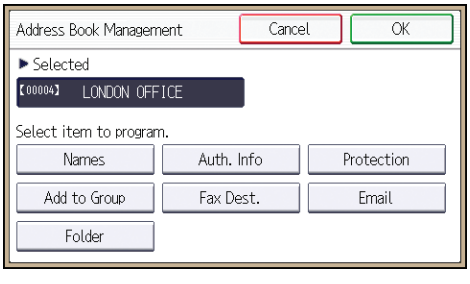
1. **The user administrator logs in from the control panel.**
2. **Press [Address Book Mangmnt].**
3. **Press [Change].**
4. **Select the conditions for displaying the address book.**



5. **Select the user.**

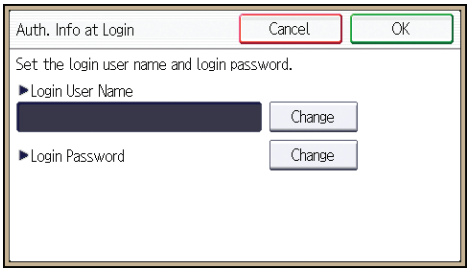


6. **Press [Auth. Info].**



7. **Press [Auth. Info at Login].**

8. Press [Change] for "Login User Name".



9. Enter a login user name, and then press [OK].
10. Press [Change] for "Login Password".
11. Enter a login password, and then press [OK].
12. Re-enter the login password for confirmation, and then press [OK].
13. Press [OK].
14. Press [Exit].
15. Press [OK].
16. Log out.

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".

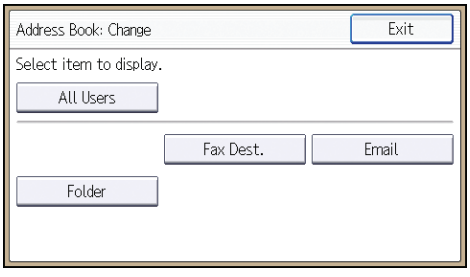
If you do not want to use the login user name and password specified in "Address Book Management" for "SMTP Authentication", "Folder Authentication", or "LDAP Authentication", see "Registering Folders" and "Registering SMTP and LDAP Authentication", Connecting the Machine/ System Settings.

Important

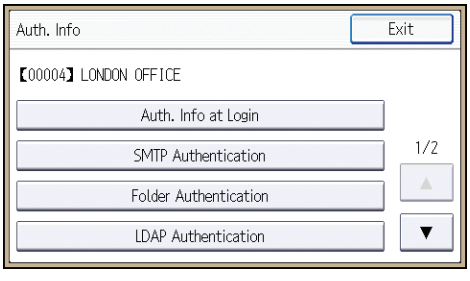
- When using "Use Auth. Info at Login" for "SMTP Authentication", "Folder Authentication", or "LDAP Authentication", a user name other than "other", "admin", "supervisor" or "HIDE***" must be specified. The symbol "****" represents any character.

1. The user administrator logs in from the control panel.
2. Press [Address Book Mangmnt].
3. Press [Change].

4. **Select the conditions for displaying the address book.**



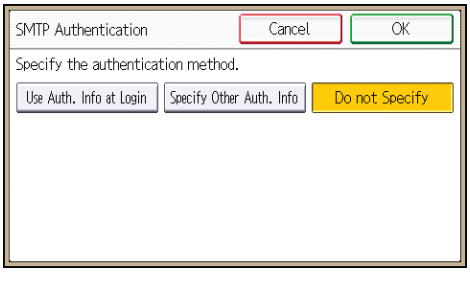
5. **Select the user.**
6. **Press [Auth. Info].**
7. **Press [SMTP Authentication].**



For folder authentication, press [Folder Authentication].

For LDAP authentication, press [LDAP Authentication].

8. **Select [Use Auth. Info at Login].**



9. **Press [OK].**
10. **Press [Exit].**
11. **Press [OK].**
12. **Log out.**

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.

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, SSLv2, or SSLv3.
    - Windows Server 2003/2003 R2
    - Windows Server 2008/2008 R2

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, SSLv2, or SSLv3. Compatible operating systems are listed below.
    - Windows Server 2003/2003 R2
    - Windows Server 2008/2008 R2

  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 p.179 "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.**

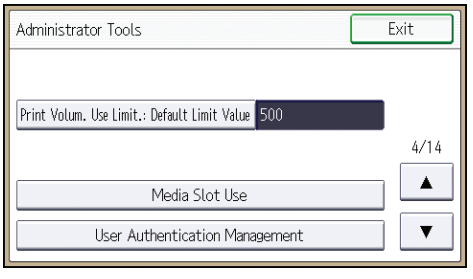
Note

- For the characters that can be used for login user names and passwords, see p.21 "Usable characters for user names and passwords".
- 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.
- 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.
- 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".
- Under Windows Authentication, you can select whether or not to use secure sockets layer (SSL) authentication.
- 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 p.49 "Creating the Server Certificate".
- 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 p.50 "If the Fax Number Cannot be Obtained".

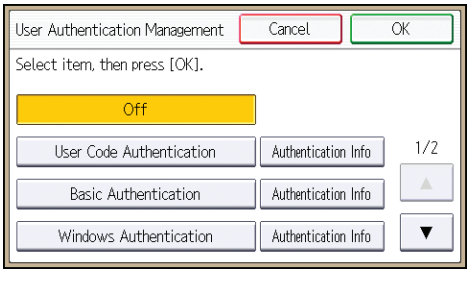
Specifying Windows Authentication

Before beginning to configure the machine, make sure that administrator authentication is properly configured under "Administrator Authentication Management".

1. **The machine administrator logs in from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼] three times.**
5. **Press [User Authentication Management].**

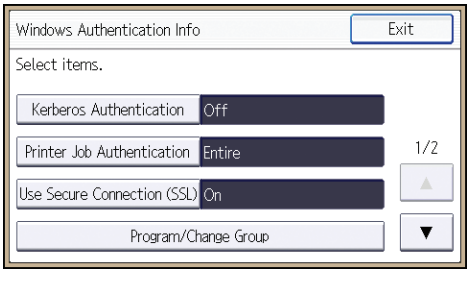


6. **Select [Windows Authentication], and then press [Authentication Info] next to it.**

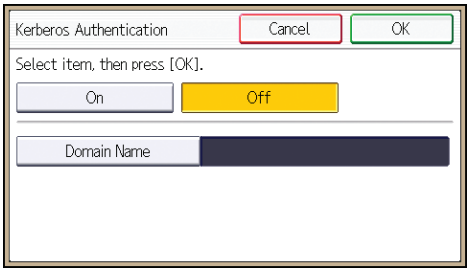


If you do not want to use user authentication management, select [Off].

7. **Press [Kerberos Authentication].**

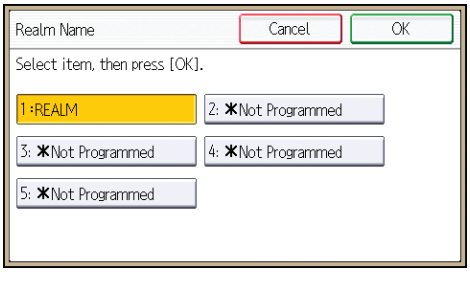


8. **Select [On], and then press [Realm Name].**



If you want to use NTLM authentication, proceed to step 11.

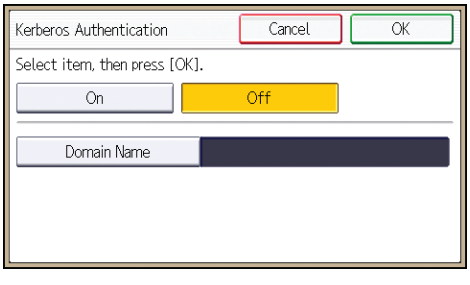
9. **Select Kerberos authentication realm.**



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.

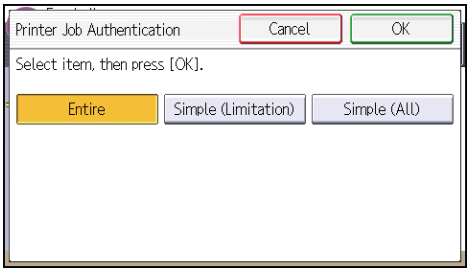
Up to 5 realms can be registered.

10. **Press [OK], and then proceed to step 12.**
11. **Press [Domain Name], enter the name of the domain controller to be authenticated, and then press [OK].**



12. **Press [OK].**
13. **Press [Printer Job Authentication].**

14. **Select the printer job authentication level.**

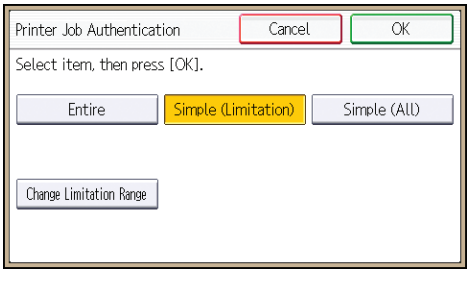


For a description of the printer job authentication levels, see p.63 "Printer Job Authentication".

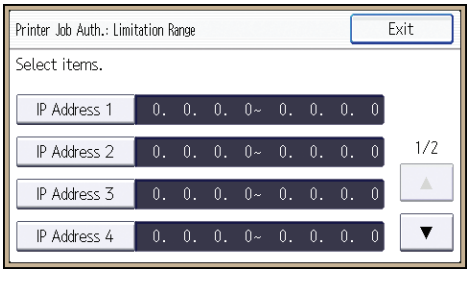
If you select [Entire] or [Simple (All)], proceed to step 18.

If you select [Simple (Limitation)], proceed to step 15.

15. **Press [Change Limitation Range].**



16. **Specify the range in which [Simple (Limitation)] is applied to "Printer Job Authentication".**



Pressing [▼] allows you to display all items.

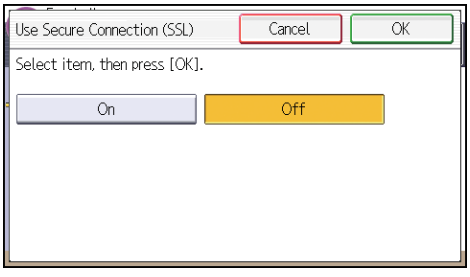
You can specify the IPv4 address range to which this setting is applied, and whether or not to apply the setting to the parallel and USB interfaces.

17. **Press [Exit].**

18. **Press [OK].**

19. **Press [Use Secure Connection (SSL)].**

20. **Press [On], and then press [OK].**



If you are not using secure sockets layer (SSL) for authentication, press [Off].

If you have not registered a global group, proceed to step 29.

If you have registered a global group, proceed to step 21.

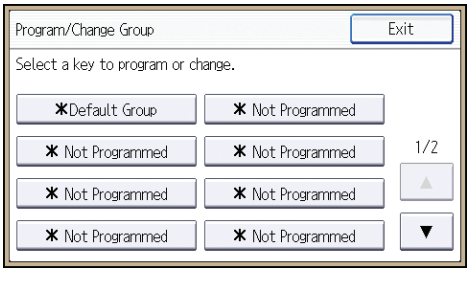
If global groups have been registered under Windows server, you can limit the use of functions for each global group.

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.

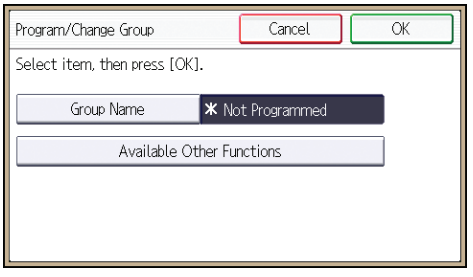
If global groups are not specified, users can use the available functions specified in [*Default Group]. If global groups are specified, users not registered in global groups can use the available functions specified in [*Default Group]. By default, all functions are available to *Default Group members. Specify the limitation on available functions according to user needs.

21. **Press [Program/Change Group].**

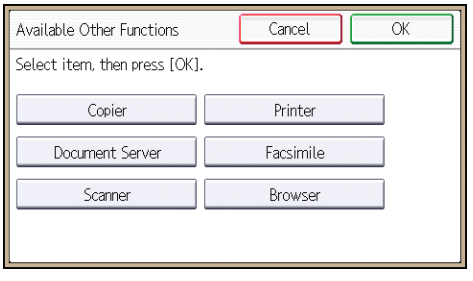
22. **Press [* Not Programmed].**



23. **Press [Group Name], and then enter the group name.**



24. **Press [OK].**
25. **Press [Available Other Functions].**
26. **Select which of the machine's functions you want to permit.**



If the function you want to select is not displayed, press [▼].

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 p.80 "Limiting Available Functions".

27. **Press [OK].**
28. **Press [OK].**
29. **Press the [Login/Logout] key.**

A confirmation message appears.

If you press [Yes], 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:

Windows Server 2008 R2 is used to illustrate the procedure.

1. **On the [Start] menu, point to [Administrator 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>].**
5. **Read the content information, and then click [Next>].**
6. **Confirm 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].**

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 [Administrator Tools], and then click [Internet Information Services (IIS) Manager].**
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. Open the command prompt window, enter "regsvr32 schmmgmt.dll", and then press the [Enter] key.
2. Click [OK], and then close the command prompt window.
3. On the [Start] menu, click [Run...].
4. Enter "mmc", and then click [OK].
5. On the [File] menu, click [Add/Remove Snap-in...].
6. Select [Active Directory Scheme], and then click [Add>].
7. Click [OK].
8. Click [Active Directory Scheme] in the left column, and then open the [Attributes] folder.
9. Right-click [facsimileTelephoneNumber], and then click [Properties].
10. Select the "Replicate this attribute to the Global Catalog" check box, and then click [Apply].
11. Click [OK].
12. On the [File] menu, click [Save].
13. Specify a file name and a location in which to store the file, and then click [Save].
14. 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 p.49 "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.

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.**

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, SSLv2, 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.

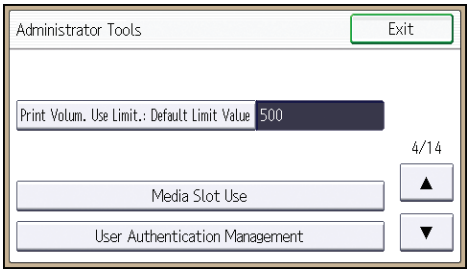
Note

- For the characters that can be used for login user names and passwords, see p.21 "Usable characters for user names and passwords".
- 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.
- In LDAP simple authentication mode, authentication will fail if the password is left blank. To allow blank passwords, contact your service representative.
- 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.
- 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 the available functions during LDAP authentication. To limit the available functions for each user, register each user and corresponding the available functions setting in the Address Book, or specify the available functions for each registered user. The available functions setting becomes effective when the user accesses the machine subsequently.
- 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.
- Transmission between the machine and the KDC server is encrypted if Kerberos authentication is enabled. For details about specifying encrypted transmission, see p.179 "Kerberos Authentication Encryption Setting".

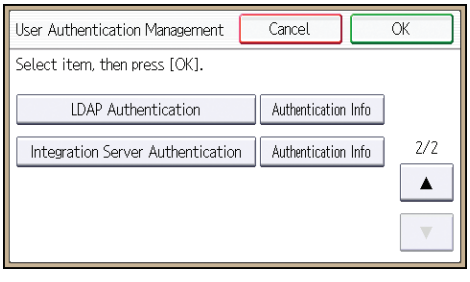
Specifying LDAP Authentication

Before beginning to configure the machine, make sure that administrator authentication is properly configured under "Administrator Authentication Management".

1. **The machine administrator logs in from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼] three times.**
5. **Press [User Authentication Management].**

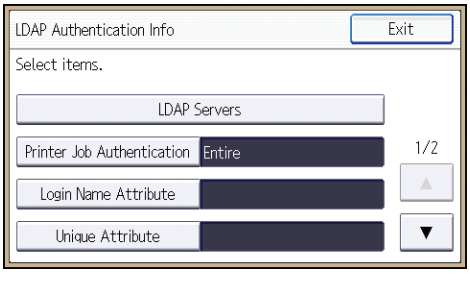


6. **Press [▼].**
7. **Select [LDAP Authentication], and then press [Authentication Info] next to it.**

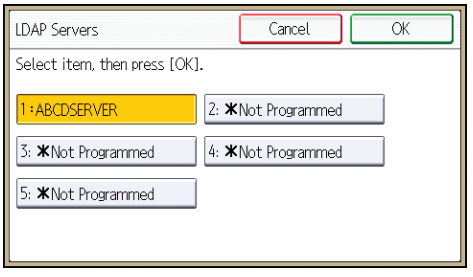


If you do not want to use user authentication management, select [Off].

8. **Press [LDAP Servers].**

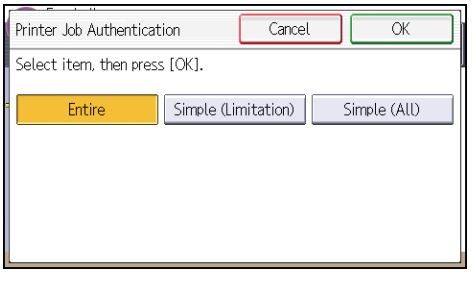


9. **Select the LDAP server to be used for LDAP authentication, and then press [OK].**



10. **Press [Printer Job Authentication].**

11. **Select the printer job authentication level.**

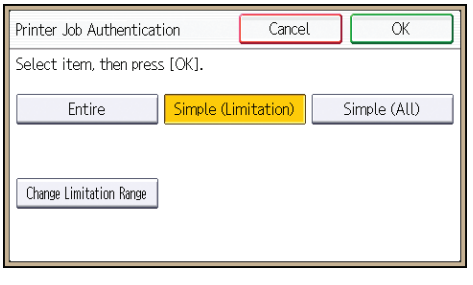


For a description of the printer job authentication levels, see p.63 "Printer Job Authentication".

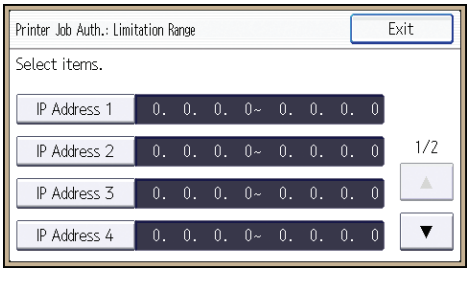
If you select [Entire] or [Simple (All)], proceed to step 15.

If you select [Simple (Limitation)], proceed to step 12.

12. **Press [Change Limitation Range].**



13. **Specify the range in which [Simple (Limitation)] is applied to "Printer Job Authentication".**



Pressing [▼] allows you to display all items.

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 [OK].**
16. **Press [Login Name Attribute].**
17. **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.

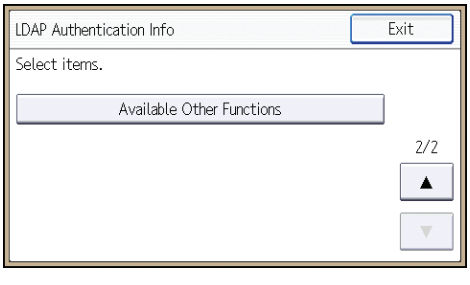
    When authenticating using the DN format, login attributes do not need to be registered.

    The method for selecting the user name depends on the server environment. Check the server environment and enter the user name accordingly.

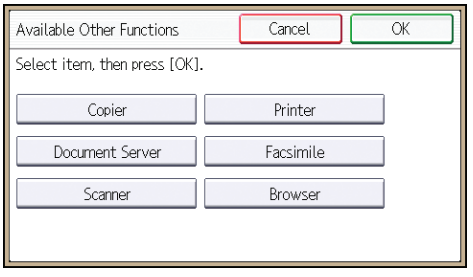
18. **Press [Unique Attribute].**
19. **Enter the unique attribute and then press [OK].**

    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.

20. **Press [▼].**
21. **Press [Available Other Functions].**



22. Select which of the machine's functions you want to permit.



If the function you want to select is not displayed, press [▼].

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 p.80 "Limiting Available Functions".

23. Press [OK].

24. Press the [Login/Logout] key.

A confirmation message appears.

If you press [Yes], 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.

For example, if the delivery server and the machine share the same Integration Server authentication, single sign-on is possible using DeskTopBinder.

To use Integration Server authentication, access to a server on which ScanRouter System or Remote Communication Gate S and Authentication Manager are installed, other than the machine, is required. For details about the 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.

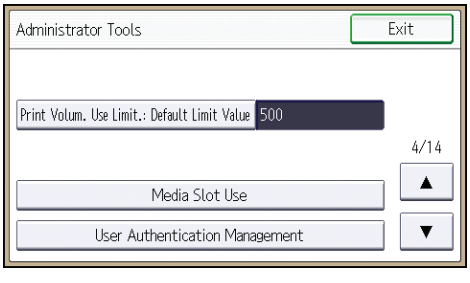
Important

- **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".**

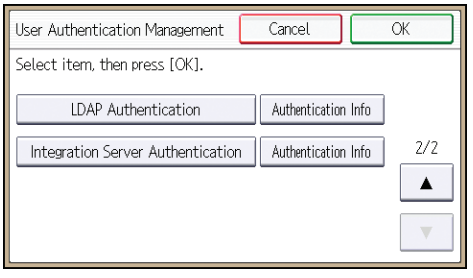
Specifying Integration Server Authentication

Before beginning to configure the machine, make sure that administrator authentication is properly configured under "Administrator Authentication Management".

1. **The machine administrator logs in from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼] three times.**
5. **Press [User Authentication Management].**

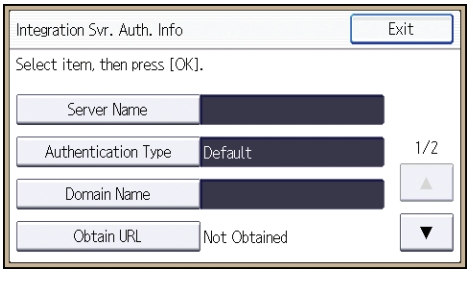


6. **Press [▼].**
7. **Select [Integration Server Authentication], and then press [Authentication Info] next to it.**



If you do not want to use user authentication management, select [Off].

8. **Press [Server Name].**

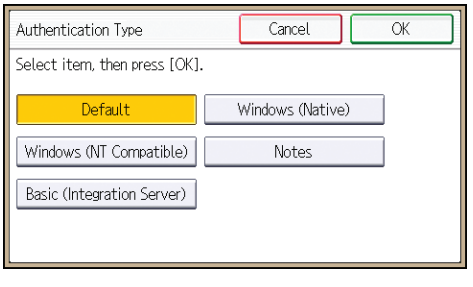


Specify the name of the server for external authentication.

9. **Enter the server name, and then press [OK].**

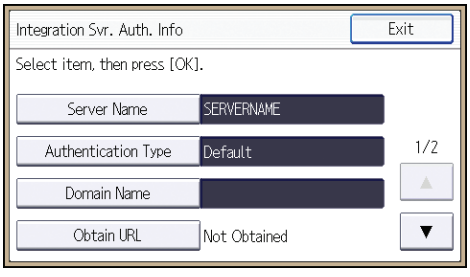
Enter the IPv4 address or host name.

10. **Press [Authentication Type].**
11. **Select the authentication system for external authentication, and then press [OK].**



Select an available authentication system. For general usage, select [Default].

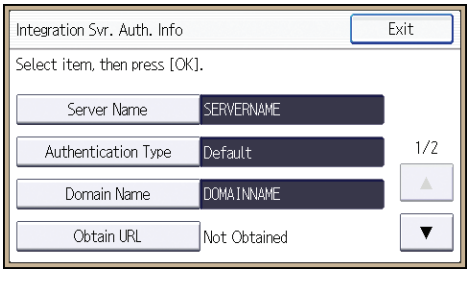
12. **Press [Domain Name].**



13. **Enter the domain name, and then press [OK].**

    You cannot specify a domain name under an authentication system that does not support domain login.

14. **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".

15. **Press [Exit].**

16. **Press [▼].**

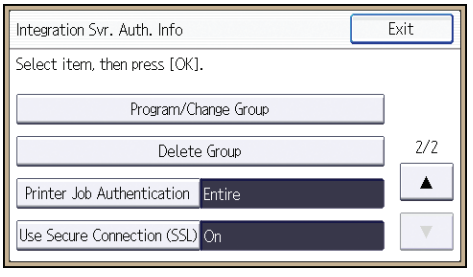
    In the "Authentication Type", if you have not registered a group, proceed to step 25.

    If you have registered a group, proceed to step 17.

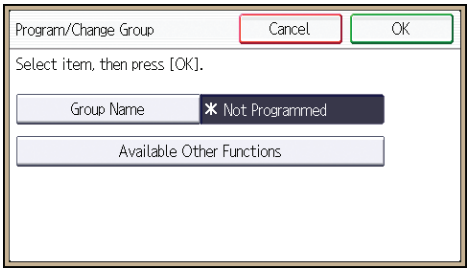
    If you set "Authentication Type" to [Windows (Native)] or [Windows (NT Compatible)], you can use the global group.

    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.

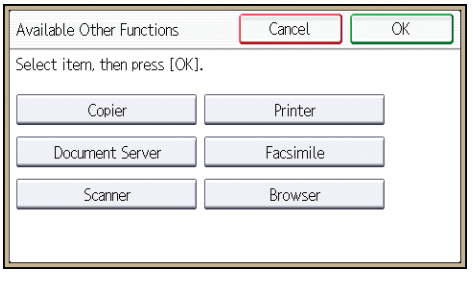
17. **Press [Program/Change Group], and then press [* Not Programmed].**



18. **Press [Group Name].**



19. **Enter the group name, and then press [OK].**
20. **Press [Available Other Functions].**
21. **Select which of the machine's functions you want to permit.**



If the function you want to select is not displayed, press [▼].

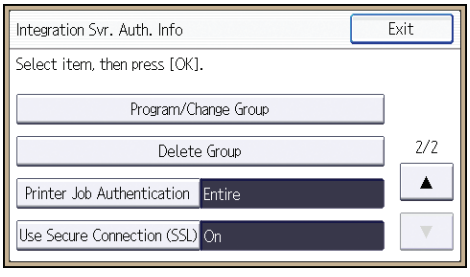
Authentication will be applied to the selected functions.

Users can use the selected functions only.

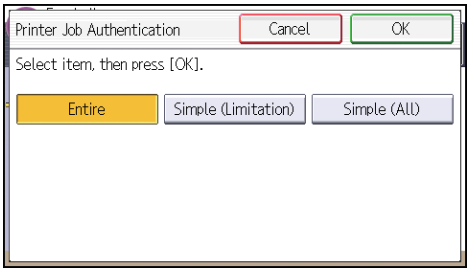
For details about specifying available functions for individuals or groups, see p.80 "Limiting Available Functions".

22. **Press [OK] twice.**
23. **Press [Exit].**

24. Press [Printer Job Authentication].



25. Select the printer job authentication level.

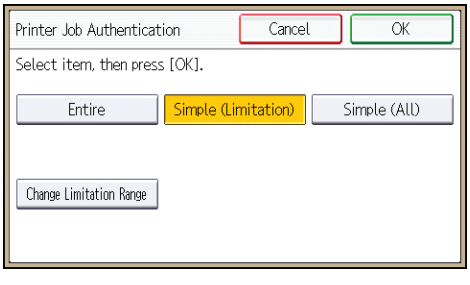


For a description of the printer job authentication levels, see p.63 "Printer Job Authentication".

If you select [Entire] or [Simple (All)], proceed to step 30.

If you select [Simple (Limitation)], proceed to step 27.

26. Press [Change Limitation Range].

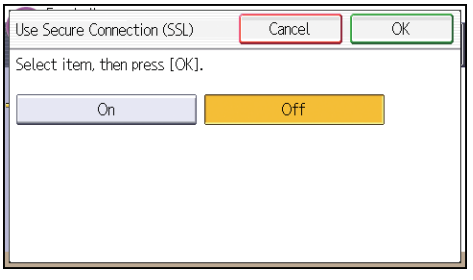


27. Specify the range in which [Simple (Limitation)] is applied to "Printer Job Authentication".

Pressing [▼] allows you to display all items.

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.

28. **Press [Exit].**
29. **Press [OK].**
30. **Press [Use Secure Connection (SSL)].**
31. **Press [On], and then press [OK].**



To not use secure sockets layer (SSL) for authentication, press [Off].

32. **Press [Exit].**
33. **Press the [Login/Logout] key.**

A confirmation message appears.

If you press [Yes], you will be automatically logged out.

Printer Job Authentication

Printer job authentication refers to the function of authenticating the user for printer jobs.

The drivers that handle user authentication are PCL or PostScript3. PostScript3 only handles User Code authentication.

Printer Job Authentication Levels

- Entire

  Select this setting when you want to authenticate all printer jobs and remote settings.

  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 (All)

  Select this setting when you want to print with a printer driver or device that cannot be identified by the machine or when you do not require authentication 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.

- Simple (Limitation)

  Select this setting when you want to restrict the range of [Simple (All)].

  You can specify the range to apply [Simple (All)] by specifying a parallel connection or USB connection and the user's IPv4 address. Also note that the range of the IPv6 address can be configured from Web Image Monitor.

  The specified range can be printed regardless of the authentication function. Any address outside this range must be specified using the authentication function.

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 without a printer driver and is printed via LPR. 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 p.259 "Specifying the Extended Security Functions".

"authfree" Command

When [Simple (Limitation)] is selected under printer job authentication, the telnet authfree command makes it possible to specify objects to be excluded from printer job authentication.

The default user name for logging in to telnet is "admin". No password is configured. For details on how to login to and use telnet, see "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_addr1 range_addr2
```

IPv6 address settings

```
msh> authfree "ID" range6_addr1 range6_addr2
```

IPv6 address mask settings

```
msh> authfree "ID" mask6_addr1 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

If a user logs in via Windows, LDAP or Integration Server authentication, their personal information is automatically registered in the Address Book. Any other information may be specified by copying from other registered users.

Automatically registered Address Book items

- Login User Name
- Login Password
- Registration No.
- Name*1
- Key Display*1
- Email Address*2
- Protect File(s)

  Permissions for Users/Groups*3

*1 When information cannot be obtained, the login user name is registered.

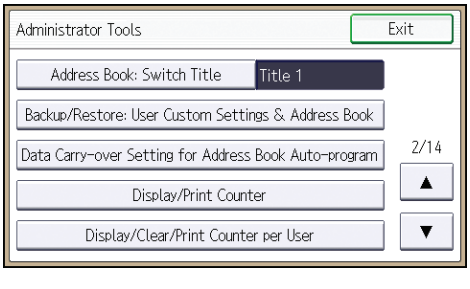
*2 When information cannot be obtained, auto registration does not work.

*3 When [Carry-over Data] on [Data Carry-over Setting for Address Book Auto-program] is specified, it has priority.

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. **The user administrator logs in from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼].**
5. **Press [Data Carry-over Setting for Address Book Auto-program].**



6. **Press [Carry-over Data].**
7. **Press [Change].**
8. **Use the number keys to enter the registration number of the Address Book that will use the setting content and press [#].**
9. **Press [OK].**
10. **Press the [Login/Logout] key.**

    A confirmation message appears.

    If you press [Yes], 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.	• Active • Inactive	• 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.	• Active • Inactive	• 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

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 [Manual Input], and then click [Change].**
5. **Set "Lockout" to [Inactive] under "Authentication Information".**
6. **Click [OK].**
7. **Log out.**

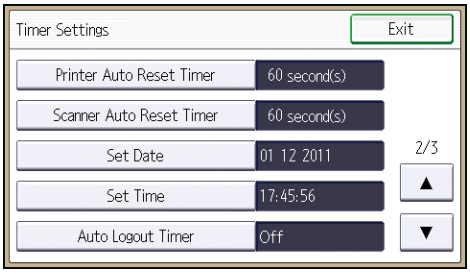
Note

- 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

When using Basic authentication, Windows authentication, LDAP authentication or Integration Server authentication, the machine automatically logs you off 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.

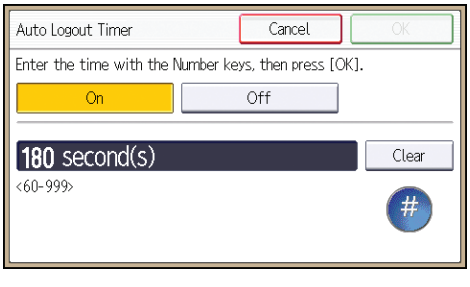
1. **The machine administrator logs in from the control panel.**
2. **Press [System Settings].**
3. **Press [Timer Settings].**
4. **Press [▼].**
5. **Press [Auto Logout Timer].**



6. **Select [On].**

   If you do not want to specify [Auto Logout Timer], select [Off].

7. **Press [Change].**
8. **Enter "60" to "999" (seconds) using the number keys, and then press [#].**



   If you make a mistake, press [Clear].

9. **Press [OK].**
10. **Press the [Login/Logout] key.**

    A confirmation message appears.

    If you press [Yes], 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.

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 destination of faxes and scanned documents can be restricted to addresses that are registered in the Address Book. Similarly, registering a destination in the Address Book is prohibited if the destination is input manually.

Restrict Use of Destinations / Restrict Adding of User Destinations

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)

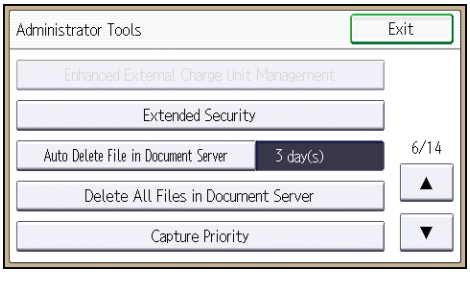
Destinations for faxes or scanned documents are restricted to addresses registered in the Address Book.

When a user is sending a document, it becomes impossible to enter the other party's fax number, e-mail address or folder destination.

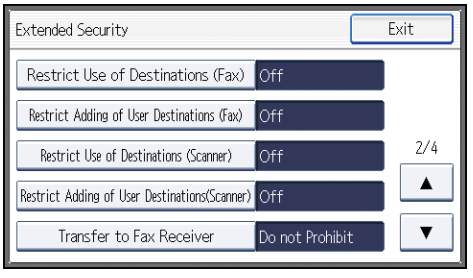
Restrict Adding of User Destinations (Fax), Restrict Adding of User Destinations (Scanner)

This setting prevents the registration of addresses into the Address Book using [Program to Address Book] when a fax or scanned document is being sent if the address was input directly. 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. **The user administrator logs in from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼]five times.**
5. **Press [Extended Security].**



6. **Press [▼].**
7. **Press [Restrict Use of Destinations (Fax)] or [Restrict Use of Destinations (Scanner)].**



8. **Press [On].**
9. **Press [OK].**
10. **Press [Exit].**
11. **Log out.**

Note

- 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.

Preventing Changes to Administrator Settings

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 p.301 "List of Operation Privileges for Settings".

Register the administrators before using the machine. For instructions on registering the administrator, see p.18 "Registering and Changing Administrators".

Prohibiting Users from Making Changes to Settings

Makes it possible to prohibit users from changing administrator settings.

Select the available settings in "Administrator Authentication Management" to prevent such changes.

For details on selections in the available settings, see p.15 "Configuring Administrator Authentication".

Menu Protect

In addition to the System Settings, Menu Protect limits user permission to access the initial settings menu for each function. This function is also effective when management is not based on user authentication. To change the menu protect setting, first enable administrator authentication. For details on how to set administrator authentication, see p.15 "Configuring Administrator Authentication". For a list of settings that users can specify according to the menu protect level, see p.301 "List of Operation Privileges for Settings".

Specifying Menu Protect

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].

Note

- When menu protect is set to [Level 1] or [Level 2], it eliminates the ability of users to register programs.

Copy Function

1. **The machine administrator logs in from the control panel.**
2. **Press [Copier/Doc. Srvr. Featr.].**
3. **Press [Administrator Tools].**
4. **Press [Menu Protect].**
5. **Select the menu protect level, and then press [OK].**
6. **Log out.**

Fax Function

1. **The machine administrator logs in 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. The machine administrator logs in from the control panel.
2. Press [Printer Features].
3. Press [Maintenance].
4. Press [Menu Protect].
5. Select the menu protect level, and then press [OK].
6. Log out.

Scanner Function

1. The machine administrator logs in 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.

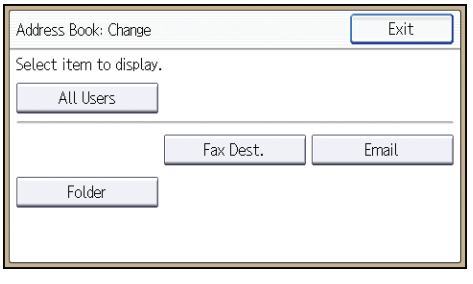
Available functions

Specify the available functions from the copier, Document Server, fax, scanner, printer, and browser functions.

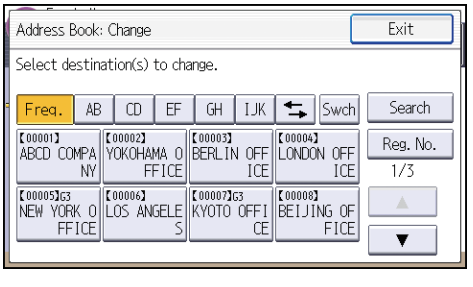
Specifying Which Functions are Available

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

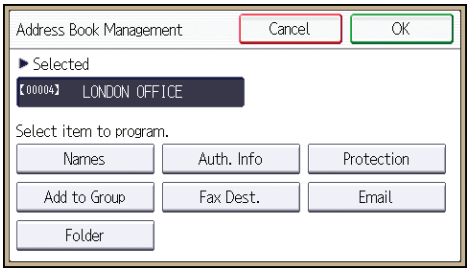
1. **The user administrator logs in from the control panel.**
2. **Press [Address Book Mangmnt].**
3. **Press [Change].**
4. **Select the conditions for displaying the address book.**



5. **Select the user.**

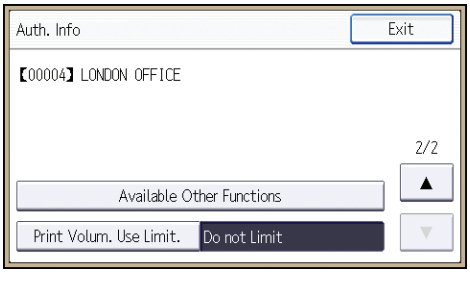


6. Press [Auth. Info].

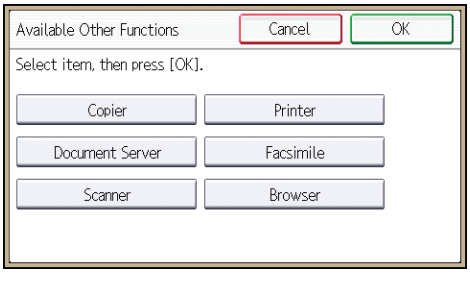


7. Press [▼].

8. Press [Available Other Functions].



9. Select the functions you want to specify.



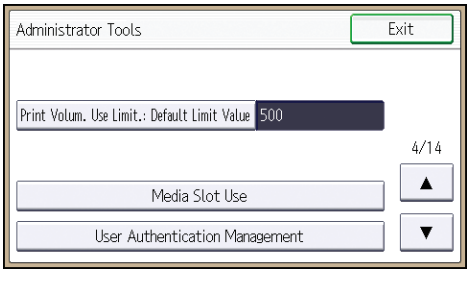
10. Press [OK].

11. Log out.

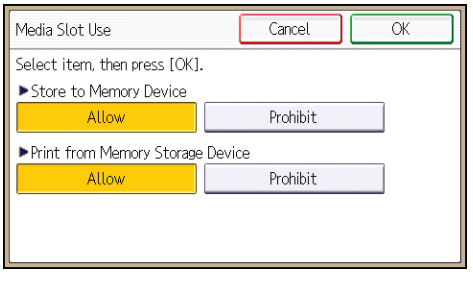
Restricting Media Slot Access

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. **The machine administrator logs in from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼] three times.**
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. When a user reaches their printing limit, their print job is canceled and/or a message indicating so is displayed.

Either the user administrator or the machine administrator can specify the print volume available to a user.

Print volume

The print volume is calculated by multiplying the number of pages by a unit count.

The unit count can be weighted according to the printing conditions. For example, with a unit count weight of 10, if one page is printed, then the print volume would be 10.

The print volume is tracked for each user.

Setting Items

Item	Explanation	Setting
Machine action when limit is reached	Specify whether to limit print volume and the method for limiting prints. • 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.	• Stop Job • Finish Job and Limit • **Allow Continue Use** (Default setting)
Print Volume Use Limitation: Unit Count Setting	For each of the two print conditions, specify a per-page unit count between 0 and 200. The default per-page unit count for every print condition is 1.	• Copier • Printer

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:

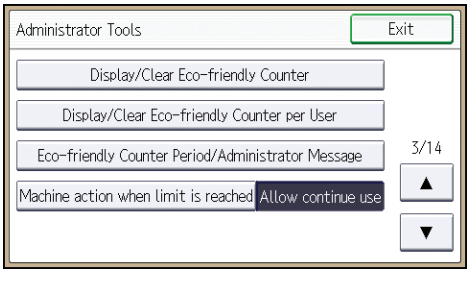
- Under Windows or LDAP authentication, a user logs in to the same user account by using multiple login user names, and these multiple login names are registered in the Address Book as separate users.

The following operations are exempt from print volume limitation:

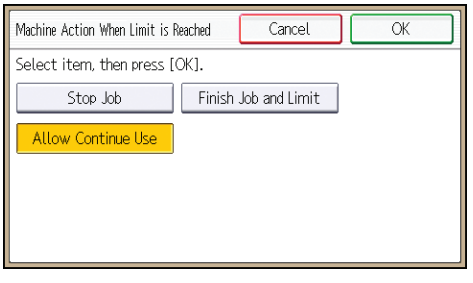
- Printing from an operating system that does not support the current authentication method
- Printing data using the Mail to Print function, received faxes, LAN-Fax data, and files stored using the fax function

Specifying Limitations for Print Volume

1. **The machine administrator logs in from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼] twice.**
5. **Press [Machine action when limit is reached].**

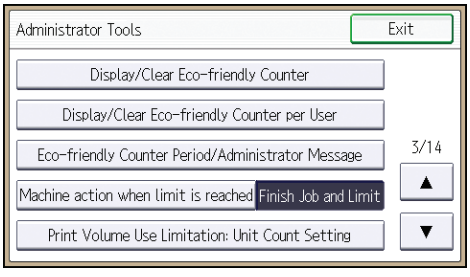


6. **Select [Stop Job] or [Finish Job and Limit], and then press [OK].**

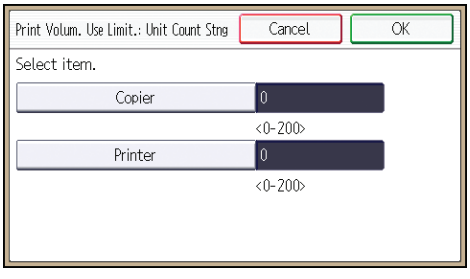


If you do not want to limit print volume, select [Allow Continue Use].

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

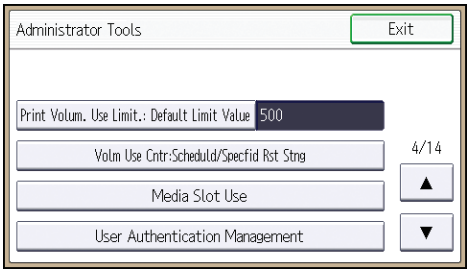
When User Code authentication is enabled, the following restrictions apply to the print volume limitation settings:

- 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 in [User Code Authentication] in [User Authentication Management].

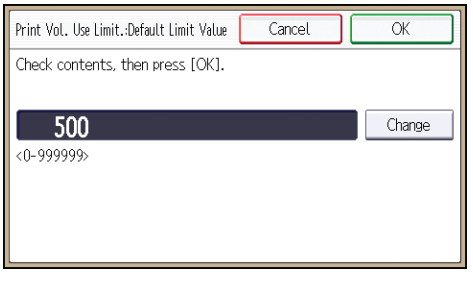
Specifying the Default Maximum Use Count

1. **The machine administrator logs in from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼] three times.**
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 [#].**

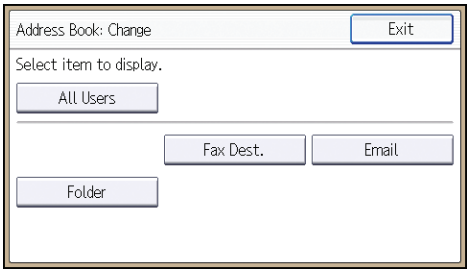


7. **Press [OK].**
8. **Log out.**

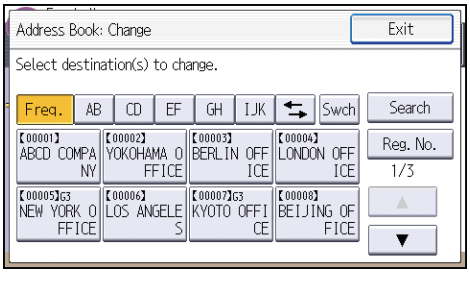
Specifying the Maximum Use Count per User

1. **The machine administrator logs in from the control panel.**
2. **Press [Address Book Mangmnt].**

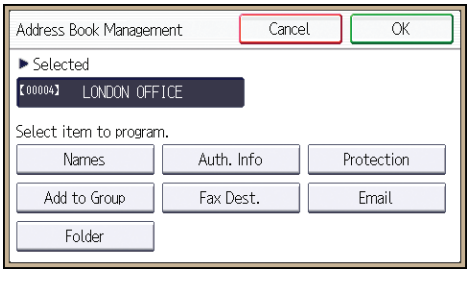
3. **Press [Change].**
4. **Select the conditions for displaying the address book.**



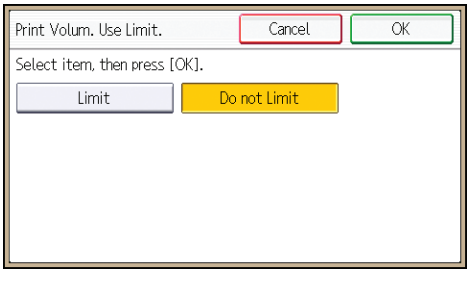
5. **Select the user whose maximum available print volume you want to specify.**



6. **Press [Auth. Info].**



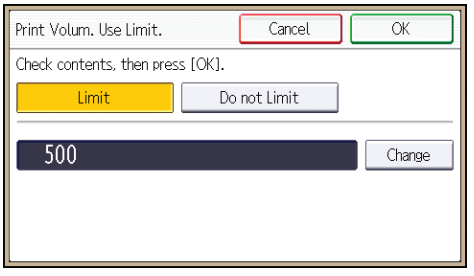
7. **Press [Print Volum. Use Limit.].**
8. **Press [Limit].**



"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].

9. **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".

10. **Press [OK].**
11. **Press [Exit].**
12. **Press [OK].**
13. **Log out.**

Note

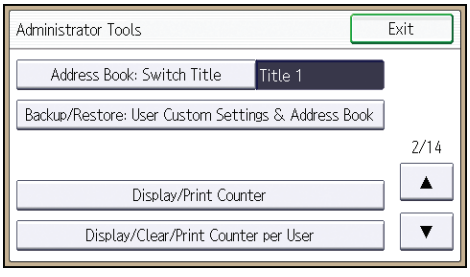
- The maximum print volume for an individual user can also be specified in [Address Book] in Web Image Monitor.
- You can search for users by entering a name in the text box at the top of the control panel, and then pressing [Search].
- You can specify a maximum print volume for up to 500 users.

Checking Print Volume per User

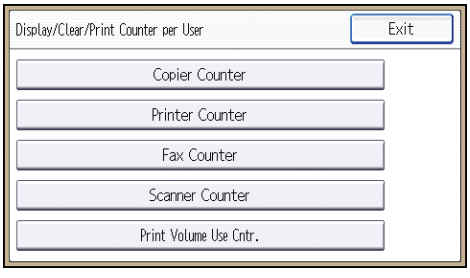
This procedure can be done by any administrator.

1. **The administrator logs in from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼].**

5. **Press [Display/Clear/Print Counter per User].**



6. **Press [Print Volume Use Cntr.].**



Each user's print volume limit and print volume used to date are displayed.

7. **After confirming the settings, log out.**

Note

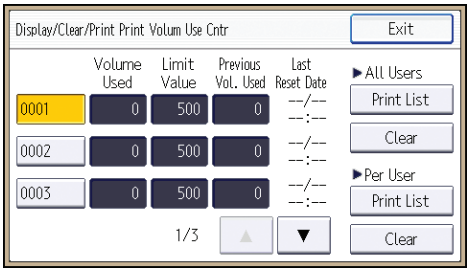
- Authorized users and the user administrator can also use [Address Book] in Web Image Monitor to check users' print volume use counters.

Printing a List of Print Volume Use Counters

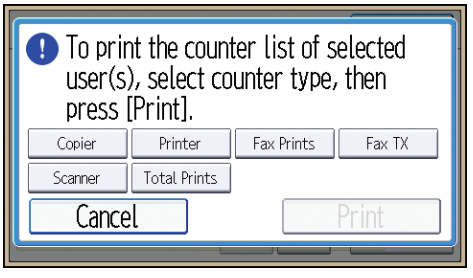
1. **The machine administrator logs in from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼].**
5. **Press [Display/Clear/Print Counter per User].**
6. **Press [Print Volume Use Cntr.].**

   A list of users' print volume use counters is displayed.

7. **To print a list of the volume use counters of every user, press [Print 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 List] under "Per User".**



8. **Select the counter you want to print in the list, and then press [Print].**



9. **Log out.**

Note

- Print volume use counter lists can be printed only if the following paper sizes is loaded in the paper tray: A4 or $8\frac{1}{2} \times 11$ inches.

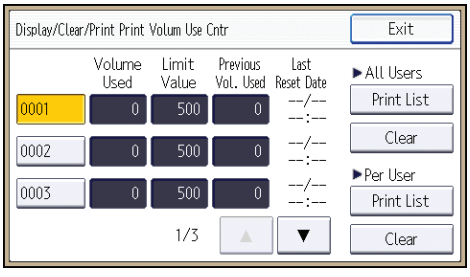
Clearing Print Volume Use Counters

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.

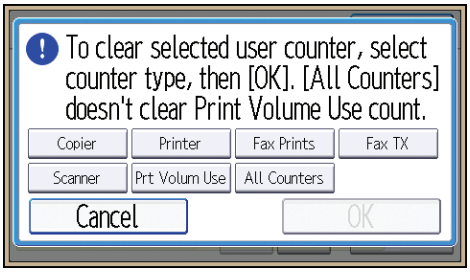
1. **The user administrator logs in from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼].**
5. **Press [Display/Clear/Print Counter per User].**
6. **Press [Print Volume Use Cntr.].**

   A list of users' print volume use counters is displayed.

7. **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".**



8. **Select [Prt Volum Use], and then press [OK].**



9. **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.

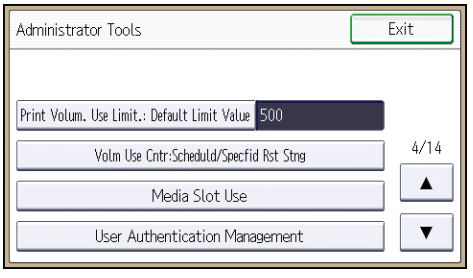
Configuring the Auto-Reset Function

The print volume counter can be reset at a specified time.

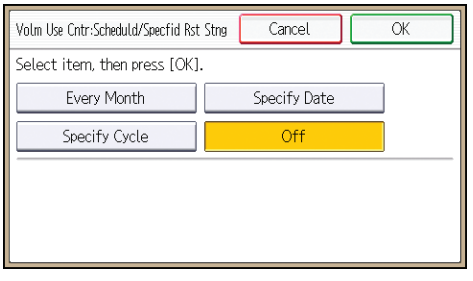
Options	Details
Every Month	Resets the print volume at the specified time/date each month.
Specify Date	Resets the volume at the specified time/date. Only resets one time.
Specify Cycle	Resets after the specified interval from a reference date, then resets thereafter after the same interval.

1. **The machine administrator logs in from the control panel.**
2. **Press [System Settings].**

3. Press [Administrator Tools].
4. Press [▼] three times.
5. Press [Volm Use Cntr:Scheduld/Specfid Rst Stng].



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 off at the specified time, the volume is reset when the power is turned on.
- If a date such as the 31st does not appear in the calendar under [Every Month], the volume is reset at 0:00 on 1st of the following 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.

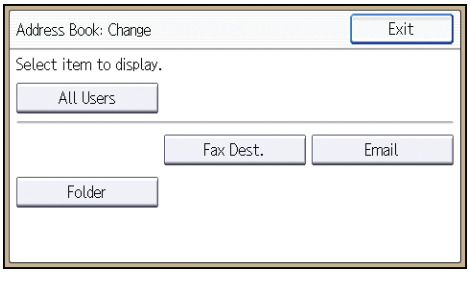
Protecting the Address Book

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.

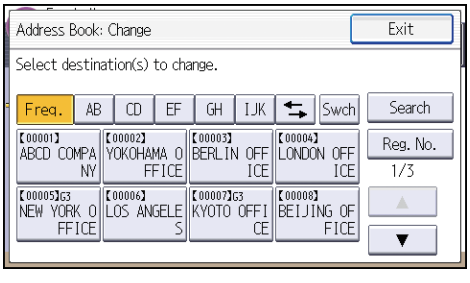
Specifying Address Book Access Permissions

These access permissions can be specified by the users registered in the Address Book or with full control, or the user administrator.

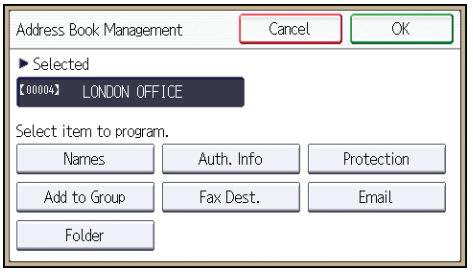
1. **The user administrator logs in from the control panel.**
2. **Press [Address Book Mangmnt].**
3. **Press [Change].**
4. **Select the conditions for displaying the address book.**



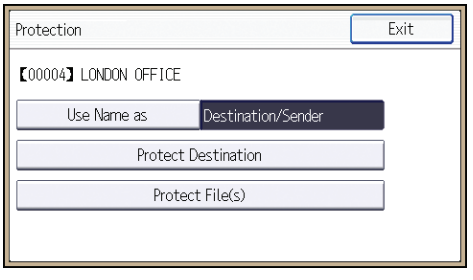
5. **Select the user.**



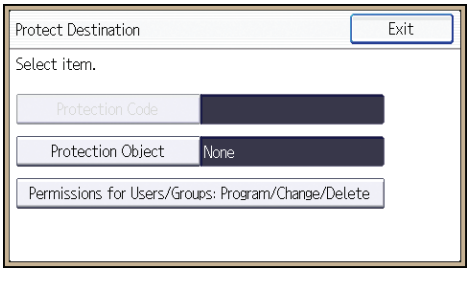
6. **Press [Protection].**



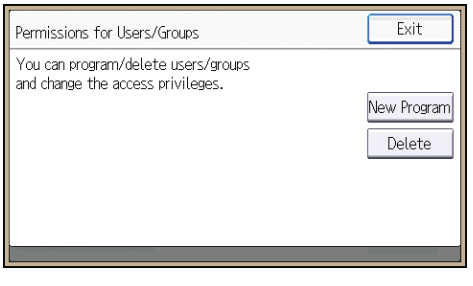
7. **Press [Protect Destination].**



8. **Press [Permissions for Users/Groups: Program/Change/Delete].**



9. **Press [New Program].**



10. **Select the users or groups to register.**

    You can select more than one user.

    By pressing [All Users], you can select all the users.

11. **Press [OK].**

12. **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].

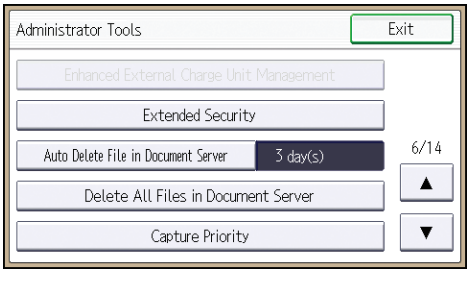
13. **Press [OK].**
14. **Press [Exit] twice.**
15. **Log out.**

Note

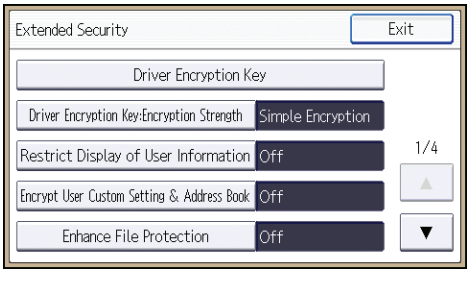
- The "Edit", "Edit/Delete", and "Full Control" access permissions allow a user to perform high level operations that could result in loss of or changes to sensitive information. We recommend you grant only the "Read-only" permission to general users.

Encrypting Data in the Address Book

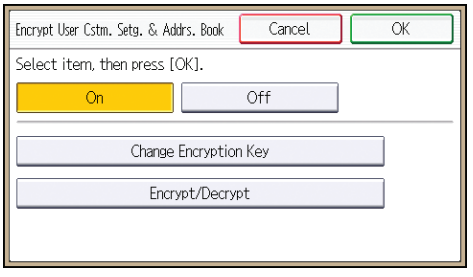
1. **The user administrator logs in from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼] five times.**
5. **Press [Extended Security].**



6. **Press [Encrypt User Custom Setting & Address Book].**



7. **Press [On], and then press [Change Encryption Key].**

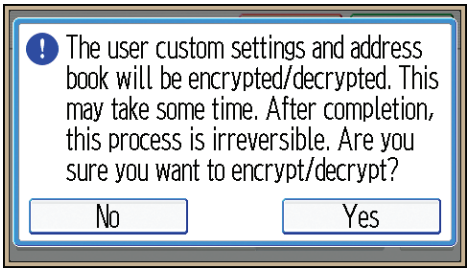


8. **Enter the encryption key, and then press [OK].**

   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.

   Encrypting the data in the Address Book may take a long time.

   The time it takes to encrypt the data in the Address Book depends on the number of registered users.

   The machine cannot be used during encryption.

   Normally, once encryption is complete, "Encryption / Decryption is successfully complete. Press [Exit]." appears.

   If you press [Stop] during encryption, the data is not encrypted.

   If you press [Stop] during decryption, the data stays encrypted.

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 out of reach of children. If a child accidentally swallows an SD card, 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 malfunctions or 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.

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.

The amount of time it takes set up encryption depends on the machine type being used. For information on machine types, see "Machine Types", Read This First.

Setting	Data to be kept	Data to be initialized	Required time
File System Data Only	• 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	• 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)	Approximately 2 hours
All Data	All Data: Both the data to be kept and data not kept when [File System Data Only] is specified	None	Approx. 7 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.

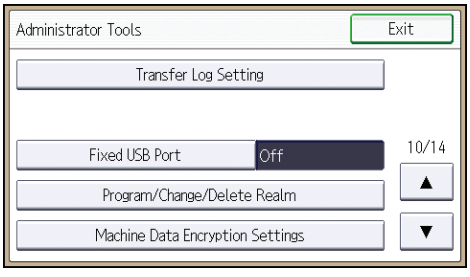
Enabling the Encryption Settings

Important

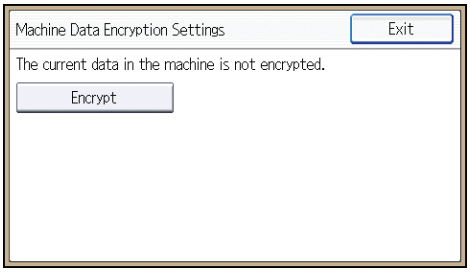
- The machine cannot be operated while data is being encrypted.
- Once the encryption process begins, it cannot be stopped. Make sure that the machine's main power is not turned off while the encryption process is in progress. If the machine's main power is turned off while the encryption process is 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 you select overwrite three times for "Random Numbers", the maximum time to complete the operations will be 10 hours, 45 minutes. Re-encrypting from an already encrypted state takes 11 hours, 45 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.
- 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. The machine administrator logs in from the control panel.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [▼] nine times.

5. **Press [Machine Data Encryption Settings].**

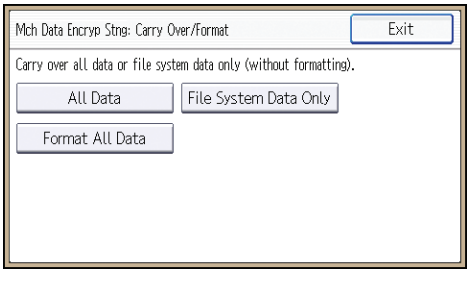


6. **Press [Encrypt].**

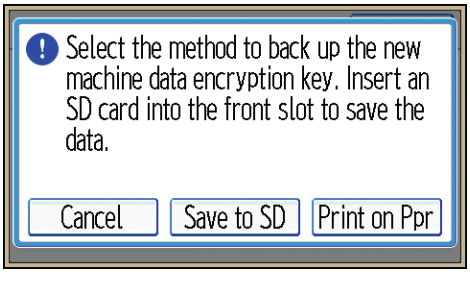


7. **Select the data to be carried over to the hard disk and not be reset.**

   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], load an SD card into the media slot on the front of the control panel and press [OK] to back up the machine's data encryption key.

If you have selected [Print on Ppr], 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 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. **The machine administrator logs in from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼] nine 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], load an SD card into the media slot on the front of the control panel and press [OK]; once the machine's data encryption key is backed up, press [Exit].

   If you have selected [Print on Ppr], 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 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. **The machine administrator logs in from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼] nine 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], load an SD card into the media slot on the front of the control panel and press [OK] to back up the machine's data encryption key.

   If you have selected [Print on Ppr], 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 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 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 p.105 "Deleting Data on the Hard Disk".

1. **The machine administrator logs in from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼] nine 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 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

- Fax transmission data, fax numbers and network TWAIN scanner data are recorded in the memory installed on this machine. This information is not overwritten with the hard disk data.

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.

Note

- Customer engineers dispatched from the manufacturer and its affiliated companies are trained in the maintenance of this machine.

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 Energy Saver mode when overwriting is in progress, press the [Energy Saver] key to revive the display in order to check the icon.
- The machine will not enter Off mode (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.

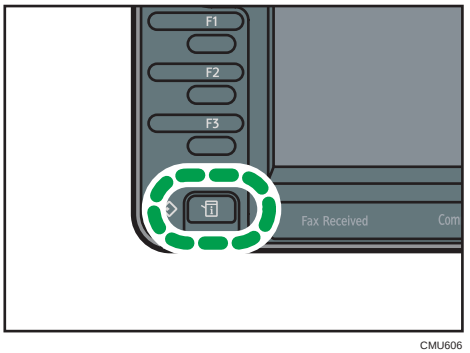
Overwriting starts automatically once the job is completed.

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.

Checking the Auto Erase Memory status

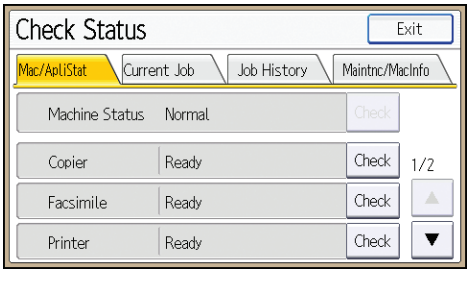
If Auto Erase Memory is enabled, you can use the "Check Status" screen to find out whether there is any data to be erased in the memory.

1. **Press [Check Status] key.**

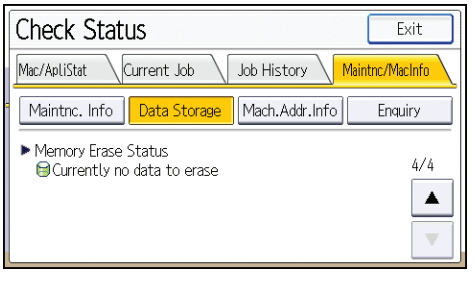


CMU606

2. **Press [Maintnc/MacInfo].**



3. **Press [Data Storage].**
4. **Press [▼] three times.**
5. **Check "Memory Erase Status".**



If Auto Erase Memory is disabled, "Memory Erase Status" does not appear.

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

  Temporary data is overwritten with a fixed value, the fixed value's complement, and random numbers. When completed, the overwriting 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

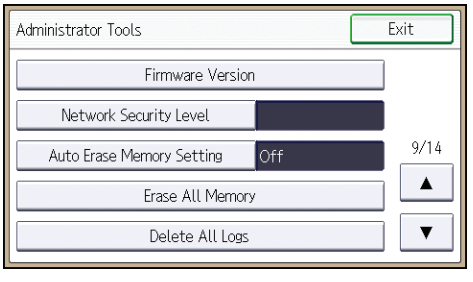
- The default method for overwriting is "Random Numbers", and the default number of overwrites is 3.
- NSA stands for "National Security Agency", U.S.A.
- DoD stands for "Department of Defense", U.S.A.

Using Auto Erase Memory

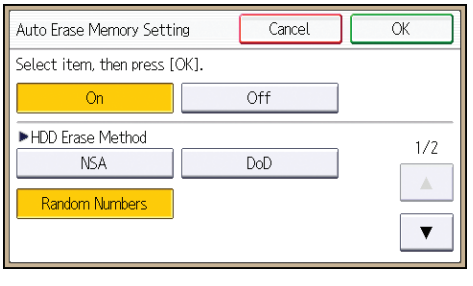
Important

- 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. The machine administrator logs in from the control panel.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [▼] eight 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 11.

If you select [Random Numbers], proceed to step 8.

8. Press [▼].

9. **Press [Change].**
10. **Enter the number of times that you want to overwrite using the number keys, and then press [#].**
11. **Press [OK].**

    Auto Erase Memory is set.
12. **Log out.**

Note

- If you specify to both overwrite and encrypt the data, the data will all be encrypted.

Canceling Auto Erase Memory

1. **Follow steps 1 to 5 in "Using Auto Erase Memory".**
2. **Press [Off].**
3. **Press [OK].**

    Auto Erase Memory is disabled.

Note

- To set Auto Erase Memory to [On] again, repeat the procedure in "Using Auto Erase Memory".

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

  Data sent or received 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 DeskTopBinder, the ScanRouter delivery software or Web Image Monitor
- Network TWAIN scanner

  Data scanned with network TWAIN scanner will not be overwritten by Auto Erase Memory.

  However, If the "ADF(Read-ahead)" function is specified, data scanned with the network TWAIN scanner will be stored on the hard disk, so will be overwritten by Auto Erase Memory.

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 p.93 "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 amount of time it takes to completely erase the memory depends on the machine type being used. For information on machine types, see "Machine Types", Read This First.

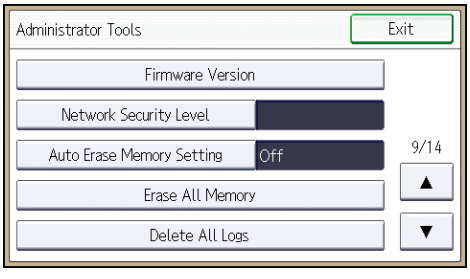
Important

- **If you select "Erase All Memory", the following are also deleted: user codes, counters under each user code, data stored in the Address Book, printer fonts downloaded by users, applications using Embedded Software Architecture, SSL server certificates, and the machine's network settings.**
- **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 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 Help or Web Image Monitor Help.**
- **Other than pausing, no operations are possible during the "Erase All Memory" process. When "Random Numbers" is selected and it is set to overwrite three times, take a maximum of 3 hours, 30 minutes.**

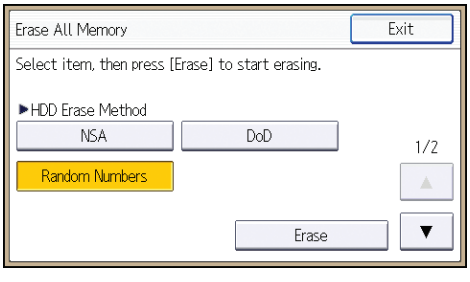
- The "Erase All Memory" function also clears the machine's security settings, with the result that afterward, neither machine nor user administration will be effective. Ensure that users do not save any data on the machine after "Erase All Memory" has completed.

Using Erase All Memory

1. Disconnect communication cables connected to the machine.
2. The machine administrator logs in from the control panel.
3. Press [System Settings].
4. Press [Administrator Tools].
5. Press [▼] eight times.
6. Press [Erase All Memory].



7. Select the method of overwriting.

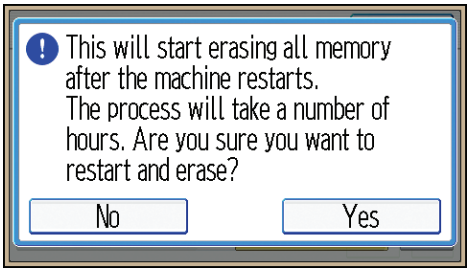


If you select [NSA] or [DoD], proceed to step 11.

If you select [Random Numbers], proceed to step 8.

8. Press [▼].
9. Press [Change].
10. Enter the number of times that you want to overwrite using the number keys, and then press [#].
11. Press [Erase].

12. **Press [Yes].**



13. **When overwriting is completed, press [Exit], and then turn off the main power.**

    Before turning the power off, 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 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 again, and then repeat from step 2.
- If you specify to both overwrite and encrypt the data, the data will all be encrypted.

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.**

   Before turning the power off, 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), IPP, DIPRINT, RHPP, Web Image Monitor, SmartDeviceMonitor for Client, or DeskTopBinder. You cannot limit the monitoring of SmartDeviceMonitor for Client. You cannot limit access involving telnet, or SmartDeviceMonitor for Admin, 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].**

   Access control is set.
6. **Click [OK].**
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 using Web Image Monitor, telnet, SmartDeviceMonitor for Admin or Remote Communication Gate S. If you use SmartDeviceMonitor for Admin, start Web Image Monitor from SmartDeviceMonitor for Admin and configure the settings from there.

Protocol	Port	Setting method	When disabled
IPv4	-	• Control panel • Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Remote Communication Gate S	All applications that operate over IPv4 cannot be used. IPv4 cannot be disabled from Web Image Monitor when using IPv4 transmission.
IPv6	-	• Control panel • Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Remote Communication Gate S	All applications that operate over IPv6 cannot be used.
IPsec	-	• Control panel • Web Image Monitor • telnet • SmartDeviceMonitor for Admin	Encrypted transmission using IPsec is disabled.

Protocol	Port	Setting method	When disabled
FTP	TCP:21	• Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Remote Communication Gate S	Functions that require FTP cannot be used. You can restrict personal information from being displayed by making settings on the control panel using "Restrict Display of User Information".
ssh/sftp	TCP:22	• Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Remote Communication Gate S	Functions that require sftp cannot be used. You can restrict personal information from being displayed by making settings on the control panel using "Restrict Display of User Information".
telnet	TCP:23	• Web Image Monitor • SmartDeviceMonitor for Admin	Commands using telnet are disabled.
SMTP	TCP:25 (variable)	• Control panel • Web Image Monitor • SmartDeviceMonitor for Admin • Remote Communication Gate S	Internet Fax or e-mail notification functions that require SMTP reception cannot be used.
HTTP	TCP:80	• Web Image Monitor • telnet • SmartDeviceMonitor for Admin	Functions that require HTTP cannot be used. Cannot print using IPP on port 80.

Protocol	Port	Setting method	When disabled
HTTPS	TCP:443	• Web Image Monitor • telnet • SmartDeviceMonitor for Admin	Functions that require HTTPS cannot be used. @Remote cannot be used. You can also make settings to require SSL transmission using the control panel or Web Image Monitor.
SMB	TCP:139	• Control panel • Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Remote Communication Gate S	SMB printing functions cannot be used.
NBT	UDP:137 UDP:138	• telnet	SMB printing functions via TCP/IP, as well as NetBIOS designated functions on the WINS server cannot be used.
SNMPv1,v2	UDP:161	• Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Remote Communication Gate S	Functions that require SNMPv1, v2 cannot be used. Using the control panel, Web Image Monitor or telnet, you can specify that SNMPv1, v2 settings are read-only, and cannot be edited.

Protocol	Port	Setting method	When disabled
SNMPv3	UDP:161	• Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Remote Communication Gate S	Functions that require SNMPv3 cannot be used. 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.
RSH/RCP	TCP:514	• Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Remote Communication Gate S	Functions that require RSH and network TWAIN functions cannot be used. You can restrict personal information from being displayed by making settings on the control panel using "Restrict Display of User Information".
LPR	TCP:515	• Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Remote Communication Gate S	LPR functions cannot be used. You can restrict personal information from being displayed by making settings on the control panel using "Restrict Display of User Information".

Protocol	Port	Setting method	When disabled
IPP	TCP:631	• Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Remote Communication Gate S	IPP functions cannot be used.
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)	• Control panel • Web Image Monitor • SmartDeviceMonitor for Admin • Remote Communication Gate S	IP-Fax connecting functions using H.323, SIP and T.38 cannot be used.
SSDP	UDP:1900	• Web Image Monitor • telnet • SmartDeviceMonitor for Admin	Device discovery using UPnP from Windows cannot be used.
Bonjour	UDP:5353	• Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Remote Communication Gate S	Bonjour functions cannot be used.
@Remote	TCP:7443 TCP:7444	• Control panel • telnet	@Remote cannot be used.

Protocol	Port	Setting method	When disabled
DIPRINT	TCP:9100	• Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Remote Communication Gate S	DIPRINT functions cannot be used.
RFU	TCP:10021	• Control panel • telnet	You can attempt to update firmware via FTP.
NetWare	(IPX/SPX)	• Control panel • Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Remote Communication Gate S	Cannot print with NetWare. SNMP over IPX cannot be used.
WSD (Device)	TCP:53000 (variable)	• Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Remote Communication Gate S	WSD (Device) functions cannot be used.
WSD (Printer)	TCP:53001 (variable)	• Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Remote Communication Gate S	WSD (Printer) functions cannot be used.

Protocol	Port	Setting method	When disabled
WSD (Scanner)	TCP-53002 (variable)	• Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Remote Communication Gate S	WSD (Scanner) functions cannot be used.
WS-Discovery	UDP/TCP:3702	• telnet • Remote Communication Gate S	WSD (Device, Printer, Scanner) search function cannot be used.
RHPP	TCP:59100	• Web Image Monitor • telnet • SmartDeviceMonitor for Admin	Cannot print with RHPP.
LLTD	-	• telnet	Device search function using LLTD cannot be used.
LLMNR	UDP:5355	• Web Image Monitor • telnet	Name resolution requests using LLMNR cannot be respond.

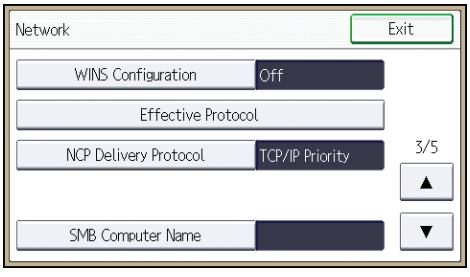
Note

- "Restrict Display of User Information" is one of the Extended Security features. For details about making this setting, see p.259 "Specifying the Extended Security Functions".

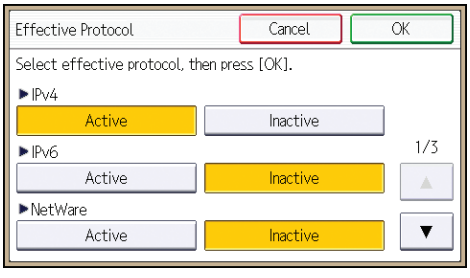
Enabling and Disabling Protocols Using the Control Panel

1. **The network administrator logs in from the control panel.**
2. **Press [System Settings].**
3. **Press [Interface Settings].**
4. **Press [Network].**
5. **Press [▼] twice.**

6. **Press [Effective Protocol].**



7. **Set the desired protocols to active/inactive.**



If the protocol you want to select is not displayed, press [▼].

8. **Press [OK].**
9. **Press [Exit].**
10. **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], click the web browser's [Reload] 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.**

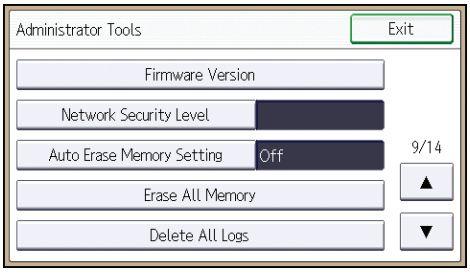
Network Security Levels

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]	Has a security strength intermediate between [Level 1] and [Level 2]. It only uses a password as 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.

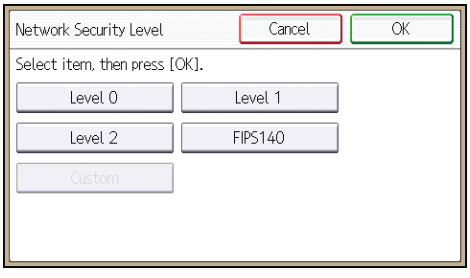
Specifying Network Security Level Using the Control Panel

1. **The network administrator logs in from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼] eight 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.**

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], click the web browser's [Reload] 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
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

Function	Level 0	Level 1	FIPS 140	Level 2
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
WSD (Scanner)	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
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.

To use these protocols, it is necessary to create and install a device certificate for the machine in advance.

The following two kinds of device certificates are possible.

- Create a self-signed certificate via the machine itself
- Request a certificate from a certificate authority

Important

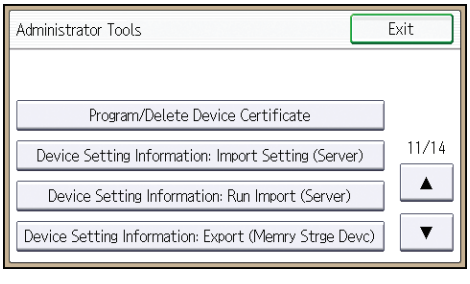
- **The administrator is required to manage the expiration of certificates and renew the certificates before they expire.**
- **The administrator is required to check that the issuer of the certificate is valid.**
- **When SHA256 or SHA512 is set for the "Algorithm Signature" on the device certificate, 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. **The network administrator logs in from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼] ten times.**
5. **Press [Program/Delete Device Certificate].**



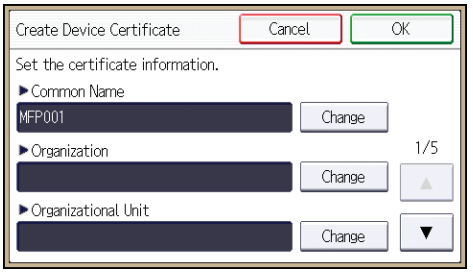
6. **Press [Program].**

   Select [Delete] to delete the device certificate from the machine.

7. **Press [Certificate 1].**

   Only [Certificate 1] can be created from the control panel.

8. **Make the necessary settings.**



   Press [▼] to flip through pages.

   To use S/MIME, specify the e-mail address of the administrator of the machine in the mail address setting.

9. **Press [OK].**

   "Installed" appears to the right of "Certificate Stat." to show that a device certificate for the machine has been installed.

10. **Log out.**

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].**

6. **Make the necessary settings.**

   To use S/MIME, set up the e-mail address of the administrator of the machine in the mail address setting.

7. **Click [OK].**

   The setting is changed.

8. **Click [OK].**

9. **If a security warning dialog box appears, check the details, and then click [OK].**

   "Installed" appears under "Certificate Status" to show that a device certificate for the machine has been installed.

10. **Log out.**

Note

- Click [Delete] to delete the device certificate from the machine.

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.
- Using Web Image Monitor, you can create the contents of the device certificate but you cannot send the certificate application.
- Click [Cancel Request] to cancel the request for the device certificate.

Installing the Device Certificate (Issued by a Certificate Authority)

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 a moment for the device to restart, 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 a moment for the device to restart, and then click [OK].**

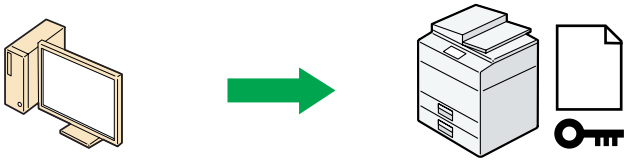
   The intermediate certificate will be installed on the device. The "Certificate Details" screen will inform you whether or not the installation of the intermediate certificate was successful. For details about the "Certificate Details" screen, see Web Image Monitor Help.
9. **Log out.**

Configuring SSL/TLS

Configuring the machine to use SSL/TLS enables encrypted communication. Doing so makes it possible to prevent data from being intercepted during transmission, and its content from being analyzed or tampered with.

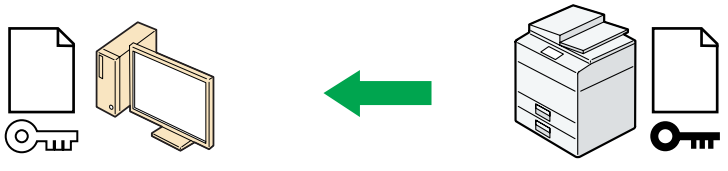
Flow of SSL/TLS encrypted communications

1. To access the machine from a user's computer, request the SSL/TLS device certificate and public key.



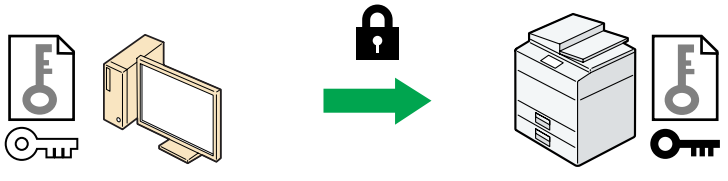
CJC002

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.

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. **Click [Active] for the protocol version used in "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], click the web browser's [Reload] button.

10. **Log out.**

Note

- If you set "Permit SSL/TLS Communication" to [Ciphertext Only], enter " https://(the machine's IP address or host name)/" to access the machine.
- 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, Windows Server 2008/2008 R2. The network administrator must instruct each user to install the certificate.

Note

- Take the appropriate steps when you receive a user's inquiry concerning problems such as an expired certificate.

- Select [Trusted Root Certification Authorities] for the certificate store location when accessing the machine by IPP.
- If a certificate issued by a certificate authority is installed in the machine, confirm the certificate store location with the certificate authority.
- When the operating system's standard IPP port is used with Windows Vista/7 or Windows Server 2008/2008 R2, if the host name or IP address of the [Common Name] of the device certificate is changed, delete any previously configured PC printer(s) and re-install the printers after changing the [Common Name]. Also, if a user's authentication information (login user name and password) is to be changed, the printer must be deleted and after the user's information authentication settings are changed, the printer must then be reinstalled.

Setting the SSL/TLS Encryption Mode

By specifying the SSL/TLS encrypted communication mode, you can change the security level.

Encrypted communication mode

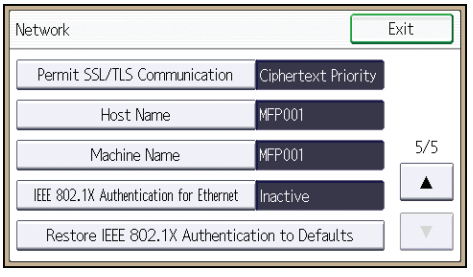
Using the encrypted communication mode, you can specify encrypted communication.

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. **The network administrator logs in from the control panel.**
2. **Press [System Settings].**
3. **Press [Interface Settings].**
4. **Press [Network].**
5. **Press [▼] four times.**

6. **Press [Permit SSL/TLS Communication].**



7. **Select the encrypted communication mode.**

   Select [Ciphertext Only], [Ciphertext Priority], or [Ciphertext/Cleartext] as the encrypted communication mode.

8. **Press [OK].**
9. **Log out.**

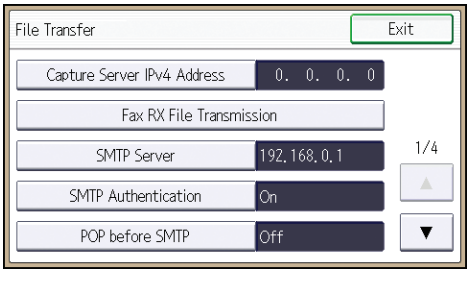
Note

- 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

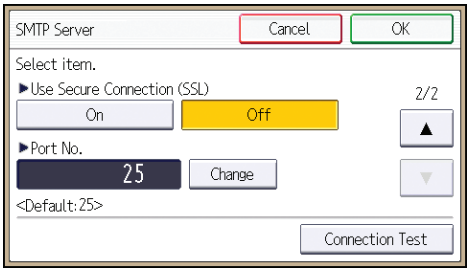
Use the following procedure to enable SSL encryption for SMTP connections.

1. **The network administrator logs in from the control panel.**
2. **Press [System Settings].**
3. **Press [File Transfer].**
4. **Press [SMTP Server].**



5. **Press [▼].**

6. **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.

7. **Press [OK].**
8. **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 98 and later
- Microsoft Outlook Express 5.5 and later
- Thunderbird 3.1.7 and later
- Lotus Notes R5 and later
- Windows Live Mail 2009 and later

Important

- **To use S/MIME, you must first specify [Administrator's Email 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 sending e-mail to users that support S/MIME and users that do not support S/MIME at the same time, the e-mail is separated into encrypted and unencrypted groups and then sent.
- When using S/MIME, the e-mail size is larger than normal.
- For details about using S/MIME with the scanner function, see "Security Settings to E-mails", Scan.
- 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.

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 [Manual 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], click the web browser's [Reload] 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.

It is possible to use either a self-signed certificate created by the machine, or a certificate issued by a certificate authority. For details on creating and installing a device certificate, see p.127 "Protecting the Communication Path via a Device Certificate".

Important

- **To install an S/MIME device certificate, you must first register "Administrator's Email 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.

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], click the web browser's [Reload] 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 this machine, configure the conditions for signatures for S/MIME. 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	The validity period is verified at the following timings. **User Certificate** (a). When the address is selected (b). When the [Start] key is pressed **Device certificate** (c). When the first address is selected (d). When the [Start] key is pressed

Operation mode	Description
Performance Priority	Performing (c) and (d) are omitted. If it takes a long time to verify the validity period when the address is selected or when the [Start] key is pressed, operation can be completed quicker by selecting "Performance Priority".

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 Operation Mode.**
5. **Click [OK].**
6. **Log out.**

Note

- If the validity period of a certificate is valid, but expires before an e-mail is retrieved from the mail server by a client computer, the e-mail cannot be retrieved from the server.
- If an error occurs outside the validity period of the certificate when S/MIME e-mail is sent automatically, such as when sending e-mail at a specified time, notification is sent in plain text to the sender's or administrator's e-mail address. The error content can be viewed in the job log. When using S/MIME, be sure to enable the job log collection function. For details about how to view the logs, see p.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.

The configuration procedure is the same regardless of whether you are using a self-signed certificate or a certificate issued by a certificate authority.

Selecting the Device Certificate

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], click the web browser's [Reload] 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.
- To provide an electronic signature for a PDF/A file, select "SHA1withRSA1024" as the device certificate's algorithm signature.

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 has two methods that you can use to specify the shared encryption key for both parties: encryption key auto exchange and encryption key manual settings. 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 "System 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 and Windows Server 2003/2003 R2. IPsec for both IPv4 and IPv6 is supported by Windows Vista/7, Windows Server 2008/2008 R2, 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 and Encryption Key Manual Settings

This machine provides two key setting methods: manual and auto exchange. Using either of these methods, agreements such as the IPsec algorithm and key must be specified 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.

If you specify the encryption key manually, the SA settings must be shared and specified identically by both parties. To preserve the security of your SA settings, we recommend that they are not exchanged over a network.

Note that for both the manual and auto method of encryption key specification, multiple settings can be configured in the SA.

Settings 1-4 and default setting

Using either the manual or 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.

Encryption key auto exchange / manual settings - shared settings

Setting	Description	Setting value
IPsec	Specify whether to enable or disable IPsec.	• Active • Inactive
Exclude HTTPS Communication	Specify whether to enable IPsec for HTTPS transmission.	• Active • Inactive Specify "Active" if you do not want to use IPsec for HTTPS transmission.
Encryption Key Manual Settings	Specify whether to enable Encryption Key Manual Settings, or use Encryption Key Auto Exchange Settings only.	• Active • Inactive Specify "Active" if you want to use "Encryption Key Manual Settings".

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.
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

Setting	Authentication Only	Authentication and Low Level Encryption	Authentication and High Level Encryption
Phase 1 Diffie-Hellman Group	2	2	2
Phase 2 Security Protocol	AH	ESP	ESP
Phase 2 Authentication Algorithm	HMAC-SHA512-256/ HMAC-SHA384-192/ HMAC-SHA256-128/ HMAC-SHA1-96	HMAC-SHA512-256/ HMAC-SHA384-192/ HMAC-SHA256-128/ HMAC-SHA1-96	HMAC-SHA512-256/ HMAC-SHA384-192/ HMAC-SHA256-128
Phase 2 Encryption Algorithm	Cleartext (NULL encryption)	3DES/AES-128/ AES-192/AES-256	AES-128/AES-192/ AES-256
Phase 2 PFS	Inactive	Inactive	2

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.	• 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.	• Apply • Bypass • Discard
Encapsulation Mode	Specify the encapsulation mode. (auto setting)	• Transport • Tunnel (Tunnel beginning address - Tunnel ending address) Select the transport mode (this has no bearing on the security level). 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".
IPsec Requirement Level	Specify whether to only transmit using IPsec, or to allow cleartext transmission when IPsec cannot be established. (auto setting)	• Use When Possible • Always Require

Setting	Description	Setting value
Authentication Method	Specify the method for authenticating transmission partners. (auto setting)	• PSK • Certificate If you specify "PSK", you must then set the PSK text (using ASCII characters). If you are using "PSK", specify a PSK password using up to 32 ASCII characters. If you specify "Certificate", the certificate for IPsec must be installed and specified before it can be used.
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)	• MD5 • SHA1 • SHA256 • SHA384 • SHA512
Phase 1 Encryption Algorithm	Specify the encryption algorithm to be used in phase 1. (auto setting)	• 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)	• 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)	• ESP • AH • ESP+AH
Phase 2 Authentication Algorithm	Specify the authentication algorithm to be used in phase 2. (auto setting)	• 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)	• 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)	• 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.).

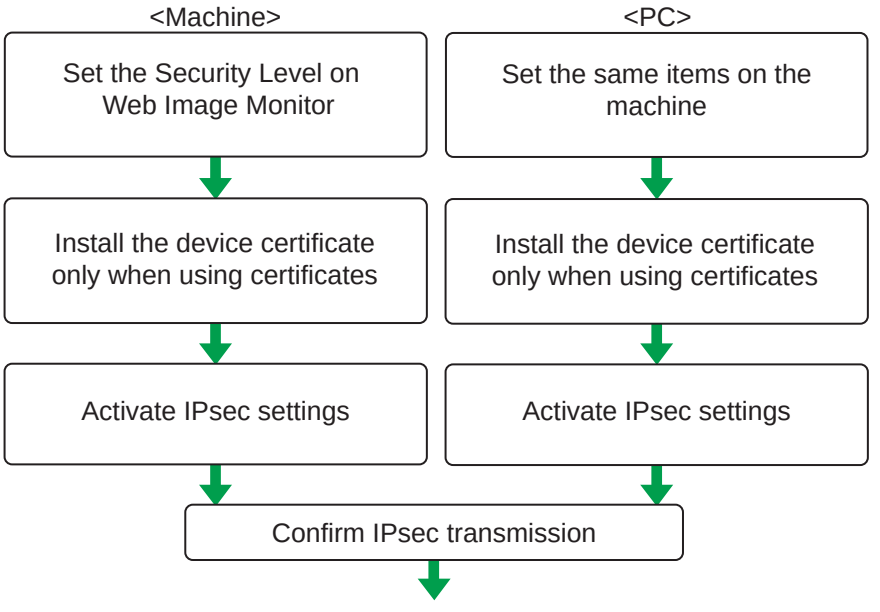
Encryption key manual settings items

Setting	Description	Setting value
Address Type	Specify the address type for which IPsec transmission is used.	• Inactive • IPv4 • IPv6 • IPv4/IPv6 (Default Settings only)
Local Address	Specify the machine's address. If you are using multiple IPv6 addresses, 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.
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.
Encapsulation Mode	Select the encapsulation mode.	• Transport • Tunnel (Tunnel beginning address - Tunnel ending address) If you select "Tunnel", set the "Tunnel End Point", the beginning and ending IP addresses. In "Tunnel End Point", set the same address for the beginning point as you set in "Local Address".
SPI (Output)	Specify the same value as your transmission partner's SPI input value.	Any number between 256 and 4095
SPI (Input)	Specify the same value as your transmission partner's SPI output value.	Any number between 256 and 4095

Setting	Description	Setting value
Security Protocol	To apply both encryption and authentication to sent data, specify "ESP" or "ESP+AH". To apply authentication data only, specify "AH".	• ESP • AH • ESP+AH
Authentication Algorithm	Specify the authentication algorithm.	• HMAC-MD5-96 • HMAC-SHA1-96 • HMAC-SHA256-128 • HMAC-SHA384-192 • HMAC-SHA512-256
Authentication Key	Specify the key for the authentication algorithm.	Specify a value within the ranges shown below, according to the encryption algorithm. Hexadecimal value 0-9, a-f, A-F • If HMAC-MD5-96, set 32 digits • If HMAC-SHA1-96, set 40 digits • If HMAC-SHA256-128, set 64 digits • If HMAC-SHA384-192, set 96 digits • If HMAC-SHA512-256, set 128 digits ASCII • IF HMAC-MD5-96, set 16 characters • If HMAC-SHA1-96, set 20 characters • If HMAC-SHA256-128, set 32 characters • If HMAC-SHA384-192, set 48 characters • If HMAC-SHA512-256, set 64 characters

Setting	Description	Setting value
Encryption Algorithm	Specify the encryption algorithm.	• Cleartext (NULL encryption) • DES • 3DES • AES-128 • AES-192 • AES-256
Encryption Key	Specify the key for the encryption algorithm.	Specify a value within the ranges shown below, according to the encryption algorithm. hexadecimal value 0-9, a-f, A-F • DES, set 16 digits • 3DES, set 48 digits • AES-128, set 32 digits • AES-192, set 48 digits • AES-256, set 64 digits ASCII • DES, set 8 characters • 3DES, set 24 characters • AES-128, set 16 characters • AES-192, set 24 characters • AES-256, set 32 characters

Encryption Key Auto Exchange Settings Configuration Flow



Note

- 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

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], click the web browser's [Reload] button.
11. **Log out.**

Note

- 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 p.127 "Protecting the Communication Path via a Device Certificate". For the method of assigning installed certificates to IPsec, see "Selecting the Certificate for IPsec".

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 p.127 "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], click the web browser's [Reload] button.
7. **Log out.**

Specifying IPsec settings on the computer

Specify exactly the same settings for IPsec SA settings on your computer as are specified by 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].**

   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. **Confirm 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. **Click [Add] in the IP Filter List.**
18. **In [Name], enter an IP Filter name, and then click [Add].**

    The IP Filter Wizard appears.

19. **Click [Next].**
20. **If required, enter a description of the IP filter, and then click [Next].**
21. **Select "My IP Address" in "Source address", and then click [Next].**

22. **Select "A specific IP Address or Subnet" in "Destination address", enter the machine's IP address, and then click [Next].**
23. **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.
24. **Click [Finish].**
25. **Click [OK].**
26. **Select the IP filter that was just created, and then click [Next].**
27. **Click [Add].**

    Filter action wizard appears.
28. **Click [Next].**
29. **In [Name], enter an IP Filter action name, and then click [Next].**
30. **Select "Negotiate security", and then click [Next].**
31. **Select "Allow unsecured communication if a secure connection connect be established.", and then [Next].**
32. **Select "Custom" and click [Settings].**
33. **In "Integrity algorithm", select the authentication algorithm that was specified on the machine in "Encryption Key Auto Exchange Settings Phase 2".**
34. **In "Encryption algorithm", select the encryption algorithm that specified on the machine in "Encryption Key Auto Exchange Settings Phase 2".**
35. **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".**
36. **Click [OK].**
37. **Click [Next].**
38. **Click [Finish].**
39. **Select the filter action that was just created, and then click [Next].**
40. **Select the authentication method, and then click [Next].**

    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.
41. **Click [Finish].**
42. **Click [OK].**

    The new IP security policy (IPsec settings) is specified.

43. Select the security policy that was just created, right click, and then click [Assign].

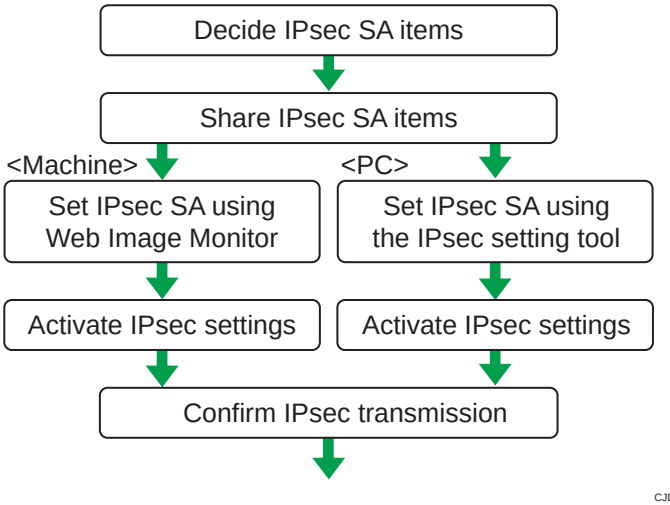
IPsec settings on the computer are enabled.

Note

- To disable the computer's IPsec settings, select the security policy, right click, and then click [Unassign].
- If you specify the "Authentication and High Level Encryption" security level in "Encryption Key Auto Exchange Settings", also select the "Use session key perfect forward secrecy (PFS)" check box in the filter action properties screen. 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.

5

Encryption Key Manual Settings Configuration Flow



Note

- Before transmission, SA information is shared and specified by the sender and receiver. To prevent SA information leakage, we recommend that this exchange is not performed over the network.
- 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. 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 Manual Settings

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. **Select [Active] for "Encryption Key Manual Settings".**
5. **Click [Edit] under "Encryption Key Manual Settings".**
6. **Set items for encryption key manual settings in [Settings 1].**

   If you want to make multiple settings, select the settings number and add settings.
7. **Click [OK].**
8. **Select [Active] for "IPsec" in "IPsec".**
9. **Set "Exclude HTTPS Communication" to [Active] if you do not want to use IPsec for HTTPS communication.**
10. **Click [OK].**
11. **"Updating..." appears. Wait for about one or two minutes, and then click [OK].**

    If the previous screen does not reappear after you click [OK], click the web browser's [Reload] button.
12. **Log out.**

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 in to telnet is "admin". No password is configured. For details about logging in to telnet and telnet operations, see "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 shared settings values

- Encryption key manual settings, SA setting 1-4 values
- Encryption key manual settings, default setting 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 manual mode

To display or specify encryption key manual settings, use the "ipsec manual_mode" command.

Display current settings

```
msh> ipsec manual_mode
```

- Displays the current encryption key manual settings.

Specify encryption key manual settings

```
msh> ipsec manual_mode {on|off}
```

- To enable encryption key manual settings, set to [on]. To disable settings, set to [off].

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 manual

To display or specify the encryption key manual settings, use the "ipsec manual" command.

Display current settings

```
msh> ipsec manual {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 manual {1|2|3|4|default} disable
```

- To disable the settings 1-4, specify the setting number [1-4].
- To disable the default settings, specify [default].

Specify the local/remote address for settings 1-4

```
msh> ipsec manual {1|2|3|4} {ipv4|ipv6} "local address" "remote address"
```

- Enter the separate setting number [1-4] and specify the local address and remote address.
- To specify the local or remote address value, specify masklen by entering [/] and an integer 0-32 if you are specifying an IPv4 address. If you are specifying 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 manual default {ipv4|ipv6|any}
```

- Specify the address type for the default setting.
- To specify both IPv4 and IPv6, enter [any].

Security protocol setting

```
msh> ipsec manual {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.

SPI value setting

```
msh> ipsec manual {1|2|3|4|default} spi "SPI input value" "SPI output value"
```

- Enter the separate setting number [1-4] or [default] and specify the SPI input and output values.
- Specify a decimal number between 256-4095, for both the SPI input and output values.
- Not specifying a SPI value displays the current setting.

Encapsulation mode setting

```
msh> ipsec manual {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 manual {1|2|3|4|default} tunneladdar "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 settings.

Authentication algorithm and authentication key settings

```
msh> ipsec manual {1|2|3|4|default} auth {hmac-md5|hmac-sha1|hmac-sha256|hmac-
sha384|hmac-sha512} "authentication key"
```

- Enter the separate setting number [1-4] or [default] and specify the authentication algorithm, and then set the authentication key.
- If you are setting a hexadecimal number, attach 0x at the beginning.
- If you are setting an ASCII character string, enter it as is.
- Not specifying either the authentication algorithm or key displays the current setting. (The authentication key is not displayed.)

Encryption algorithm and encryption key setting

```
msh> ipsec manual {1|2|3|4|default} encrypt {null|des|3des|aes128|aes192|
aes256} "encryption key"
```

- Enter the separate setting number [1-4] or [default], specify the encryption algorithm, and then set the encryption key.
- If you are setting a hexadecimal number, attach 0x at the beginning. If you have set the encryption algorithm to [null], enter an encryption key of arbitrary numbers 2-64 digits long.
- If you are setting an ASCII character string, enter it as is. If you have set the encryption algorithm to [null], enter an encryption key of arbitrary numbers 1-32 digits long.
- Not specifying an encryption algorithm or key displays the current setting. (The encryption key is not displayed.)

Reset setting values

```
msh> ipsec manual {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.

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 manual {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 local/remote address for settings 1-4

```
msh> ipsec manual {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 manual 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)

Installing a Site Certificate

Install a site certificate (root CA certificate), which checks the reliability of the authentication server. You need to have at least a certificate that is signed by a certificate authority who signed the server certificate or a certificate from an upper level certificate authority.

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] on the "Site Certificate to Import" window, 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 p.127 "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], click the web browser's [Reload] button.
7. **Log out.**

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], click the web browser's [Reload] 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], click the web browser's [Reload] button.
13. **Log out.**

Note

- If there is a problem with settings, you might not be able to communicate with the machine. To identify the problem, print a network summary.
- If you cannot identify the problem, reset the machine interface to normal, and then repeat the procedure from the beginning.

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".

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], click the web browser's [Reload] 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 [WPA] in "Security Method".**
14. **Select [WPA] or [WPA2] in "WPA 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], click the web browser's [Reload] button.
17. **Log out.**

Note

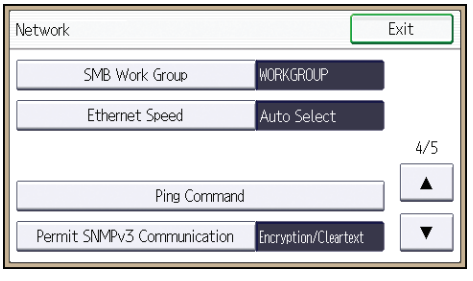
- If there is a problem with settings, you might not be able to communicate with the machine. To identify the problem, print a network summary.
- If you cannot identify the problem, reset the machine interface to normal, and then repeat the procedure from the beginning.

SNMPv3 Encryption

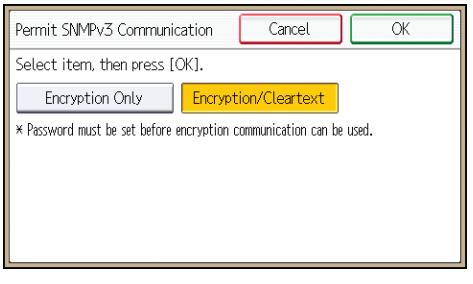
When using SmartDeviceMonitor for Admin or another application to make various settings, you can encrypt the data transmitted.

By making this setting, you can protect data from being tampered with.

1. **The network administrator logs in from the control panel.**
2. **Press [System Settings].**
3. **Press [Interface Settings].**
4. **Press [Network].**
5. **Press [▼] three times.**
6. **Press [Permit SNMPv3 Communication].**



7. **Press [Encryption Only].**



8. **Press [OK].**
9. **Log out.**

Note

- To use SmartDeviceMonitor for Admin 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, in addition to specifying [Permit SNMPv3 Communication] on the machine. For details about specifying [Encryption Password] in SmartDeviceMonitor for Admin, see SmartDeviceMonitor for Admin 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 p.18 "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 of passwords against analysis. 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

When user authentication is ON, this key is a character string used for encrypting the login passwords or document passwords that are sent from each kind of driver.

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 p.18 "Registering and Changing Administrators".

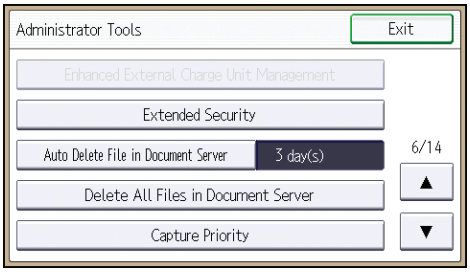
Specifying a Driver Encryption Key

Specify the driver encryption key on the machine.

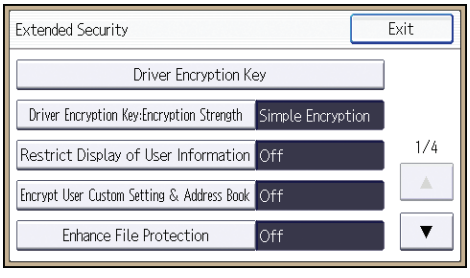
This setting enables encrypted transmission of login passwords and strengthens the security against password analysis.

1. **The network administrator logs in from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼] five times.**

5. **Press [Extended Security].**



6. **Press [Driver Encryption Key].**



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. **Re-enter the driver encryption key for confirmation, and then press [OK].**
9. **Press [Exit].**
10. **Log out.**

Note

- For details about specifying the encryption key on the printer driver, see the printer driver Help.
- For details about specifying the encryption key on the LAN-FAX driver, see the LAN-FAX driver Help.
- For details about specifying the encryption key on the TWAIN driver, see the TWAIN 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 analysis.

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], click the web browser's [Reload] button.
9. **Log out.**

Note

- When using the IPP port under Windows XP/Vista/7, Windows Server 2003/2003 R2/2008/2008 R2, you can use the operating system's standard IPP port.

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	• RC4-HMAC (ARCFOUR-HMAC-MD5)
Windows Server 2008	• AES256-CTS-HMAC-SHA1-96 • AES128-CTS-HMAC-SHA1-96 • RC4-HMAC (ARCFOUR-HMAC-MD5)
Windows Server 2008 R2	• AES256-CTS-HMAC-SHA1-96 • AES128-CTS-HMAC-SHA1-96 • RC4-HMAC (ARCFOUR-HMAC-MD5)*
Heimdal	• 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.

Configuring Access Permissions for 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 the file administrator or file creator (owner). You can obtain greater protection against the unauthorized use of files. For details about assigning a password to a stored file, see p.188 "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 file creator (owner) is "Read-only". You can also specify the access permission.
- The document 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 file creator (owner).

Specify the users and their access permissions for each stored file.

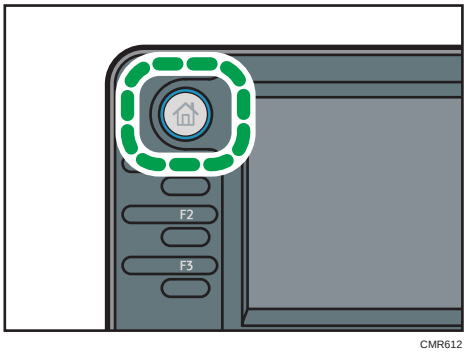
Important

- **If files become inaccessible, reset their access permission as the file creator (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 file creator (owner).**
- **The file administrator can change the owner of a document using the document's [Change Access Privilege] 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 Privilege] setting.**

1. **The file administrator or the file creator (owner) logs in from the control panel.**
2. **Press the [User Tools/Counter] key to switch to the normal screen.**

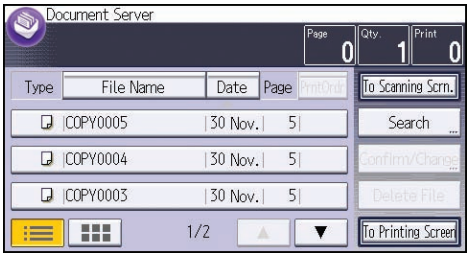
   If the message "You do not have the privileges to use this function." appears, press [Exit].
3. **Press the [Home] key on the top left of the control panel, and press the [Document Server] icon on the [Home] screen.**

   If the message "You do not have the privileges to use this function." appears, press [Exit].

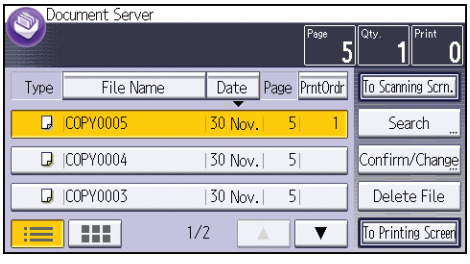


CMR612

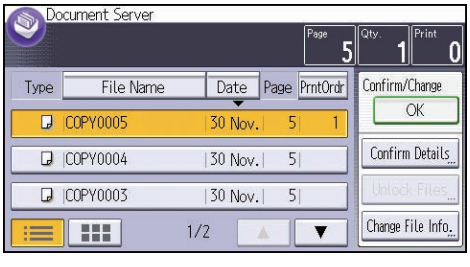
4. **Select the file.**



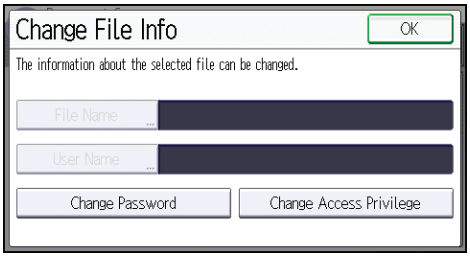
5. **Press [Confirm/Change].**



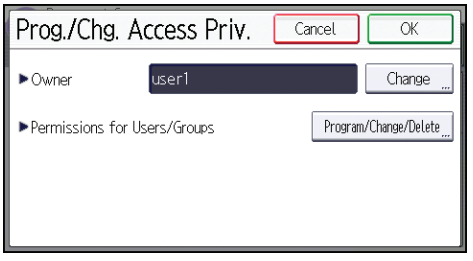
6. **Press [Change File Info.].**



7. **Press [Change Access Privilege].**

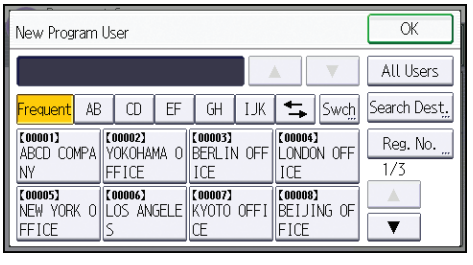


8. **Press [Program/Change/Delete] for "Permissions for Users/Groups".**



9. **Press [New Program].**

10. **Select the users or groups to whom you want to assign access permission.**

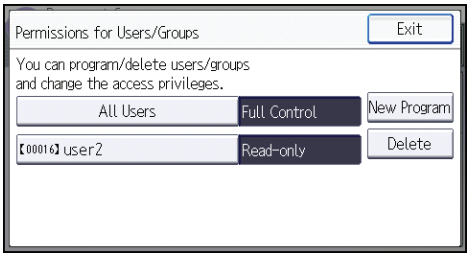


You can select more than one user.

By pressing [All Users], you can select all the users.

11. **Press [OK].**

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 [OK].**

14. **Press [Exit].**
15. **Press [OK].**
16. **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. **The file administrator logs in from the control panel.**
2. **Press the [User Tools/Counter] key to switch to the normal screen.**

   If the message "You do not have the privileges to use this function." appears, press [Exit].
3. **Press the [Home] key on the top left of the control panel, and press the [Document Server] icon on the [Home] screen.**

   If the message "You do not have the privileges to use this function." appears, press [Exit].
4. **Select the file.**
5. **Press [Confirm/Change].**
6. **Press [Change File Info.].**
7. **Press [Change Access Privilege].**
8. **Press [Change] for "Owner".**
9. **Select the user you want to register.**
10. **Press [OK] three times.**
11. **Log out.**

Configuring Access Permission for Each User for Stored Files

This can be specified by the user administrator or file creator (owner).

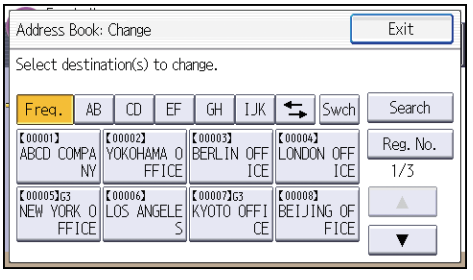
Specify the users and their access permission to files stored by a particular user.

This makes managing access permission easier than specifying and managing access permissions for each stored file.

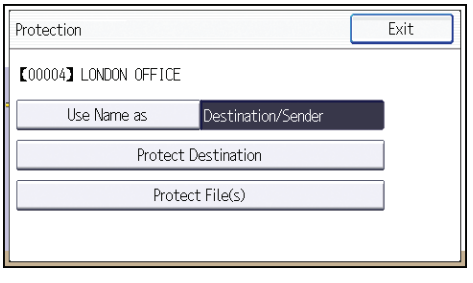
Important

- 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.

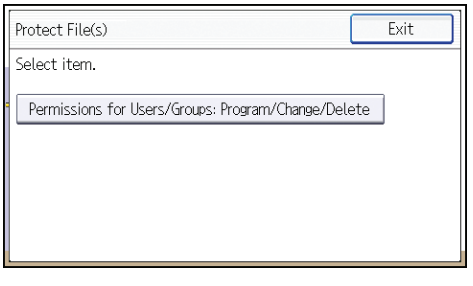
1. The user administrator or the file creator (owner) logs in from the control panel.
2. Press [Address Book Mangmnt].
3. Press [Change].
4. Select the conditions for displaying the address book.



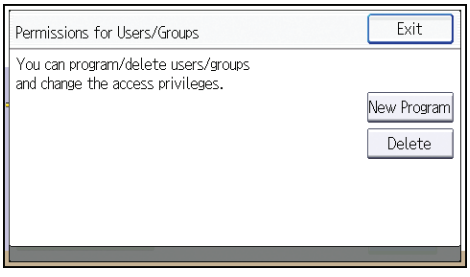
5. Select the user.
6. Press [Protection].
7. Press [Protect File(s)].



8. Press [Permissions for Users/Groups: Program/Change/Delete].



9. **Press [New Program].**



10. **Select the users or groups to register.**

    You can select more than one user.

    By pressing [All Users], you can select all the users.

11. **Press [OK].**

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 [OK].**

14. **Press [Exit] twice.**

15. **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.

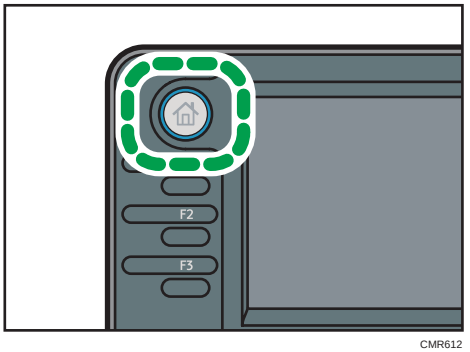
Specifying Passwords for Stored Files

This can be specified by the file administrator or file creator (owner).

1. **The file administrator or the file creator (owner) logs in from the control panel.**
2. **Press the [User Tools/Counter] key to switch to the normal screen.**

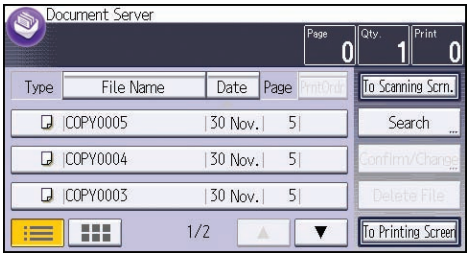
   If the message "You do not have the privileges to use this function." appears, press [Exit].
3. **Press the [Home] key on the top left of the control panel, and press the [Document Server] icon on the [Home] screen.**

   If the message "You do not have the privileges to use this function." appears, press [Exit].

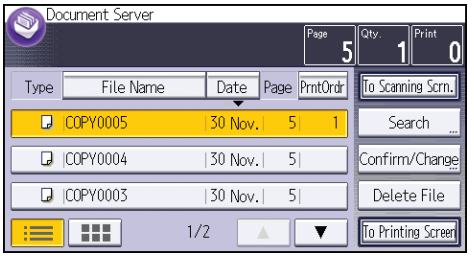


CMR612

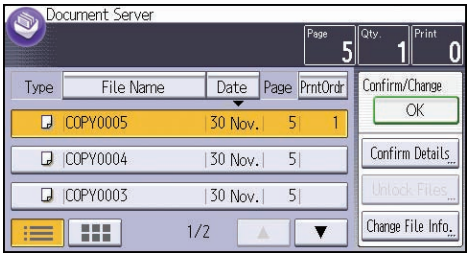
4. **Select the file.**



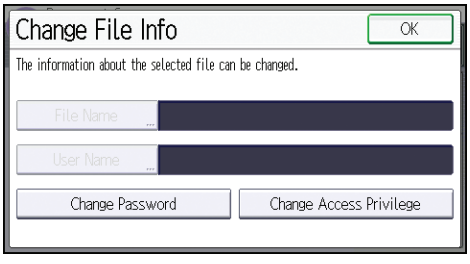
5. **Press [Confirm/Change].**



6. **Press [Change File Info.].**



7. **Press [Change Password].**



8. **Enter the password using the number keys.**

   You can use 4 to 8 numbers as the password for the stored file.

9. **Press [OK].**
10. **Confirm the password by re-entering it using the number keys.**
11. **Press [OK] twice.**

    The icon appears next to a stored file protected by password.

12. **Press [OK].**
13. **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 p.259 "Specifying the Extended Security Functions".

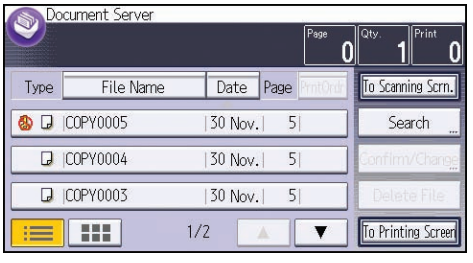
1. **The file administrator logs in from the control panel.**
2. **Press the [User Tools/Counter] key to switch to the normal screen.**

   If the message "You do not have the privileges to use this function." appears, press [Exit].

3. **Press the [Home] key on the top left of the control panel, and press the [Document Server] icon on the [Home] screen.**

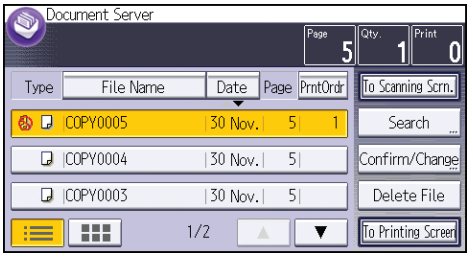
   If the message ""You do not have the privileges to use this function."" appears, press [Exit].

4. **Select the file.**

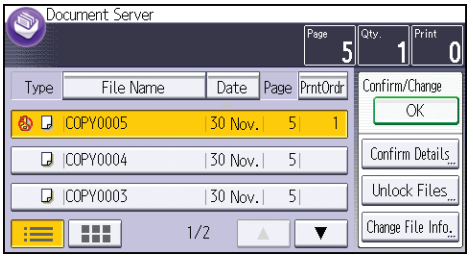


   The icon appears next to a file locked by the Enhance File Protection function.

5. **Press [Confirm/Change].**



6. **Press [Unlock Files].**



7. **Press [Yes].**

   The icon changes to the icon.

8. **Press [OK].**

9. **Log out.**

Unauthorized Copy Prevention / Data Security for Copying

In Printer Features, using the printer driver, you can embed a pattern in the printed copy to discourage or prevent unauthorized copying.

The unauthorized copy prevention function prevents unauthorized copies of documents by embedding a text pattern (for instance, a warning such as "No Copying") that you can set on the print driver (which will appear on printed copies).

Data security for copying prevents document information leaks by graying out copies of documents that were printed with the data security for copying pattern enabled in the printer driver.

However, in order to gray out the security pattern, the Copy Data Security Unit is required for the copier or multi-function printer.

For more information, see the information below.

Unauthorized Copy Prevention

1. Using the machine, specify the settings to print the pattern. The settings must be specified by the machine administrator.
2. Using the printer driver, specify the printer settings for unauthorized copy prevention. The settings must be specified by the printer user. For details on how to specify settings for unauthorized copy prevention, see "Printing Documents that are not Allowed to Duplicate", Print.

Data Security for Copying

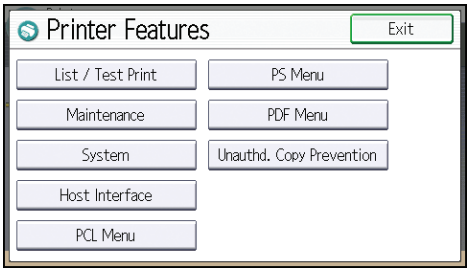
1. Using the machine, specify the settings to print the pattern. The settings must be specified by the machine administrator.
2. Using the printer driver, specify the printer settings for data security for copying. The settings must be specified by the printer user. For details on how to specify settings on the printer driver, see "Printing Documents that are not Allowed to Duplicate", Print.
3. Set the data security for copying function to appear gray when documents with the function are copied, scanned, or stored on the machine. The settings must be specified by the machine administrator. For details on how to specify settings on the machine, see p.193 "Enabling Data Security for Copying".

Enabling Pattern Printing

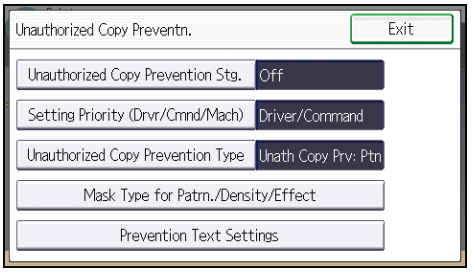
Enable pattern printing to discourage or prevent unauthorized copying.

1. **The machine administrator logs in from the control panel.**
2. **Press [Printer Features].**

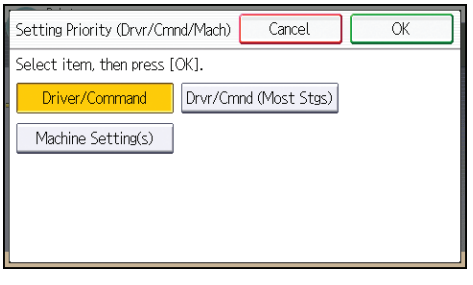
3. **Press [Unauthd. Copy Prevention].**



4. **Press [Unauthorized Copy Prevention Stg.].**



5. **Press [On], and then press [OK].**
6. **Press [Setting Priority (Drvr/Cmnd/Mach)].**
7. **Select the range within which the user can specify the pattern to be printed using the printer driver.**



- [Driver/Command]

  Specifies all the content of the pattern to be printed using the printer driver.
- [Drvr/Cmnd (Most Stgs)]

  Specifies the settings other than pattern type and density using the printer driver.
- [Machine Setting(s)]

  The pattern cannot be specified using the printer driver. The pattern specified using the machine is printed.

8. **Press [OK].**
9. **Log out.**

Note

- For details of the settings when specifying the pattern using the machine, see "Printer Features", Print.

Enabling Data Security for Copying

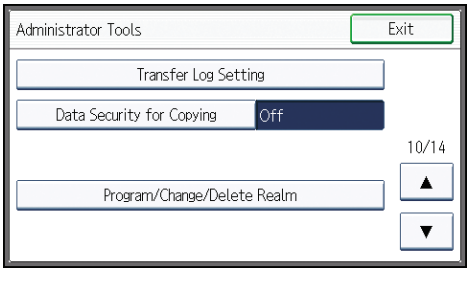
To use this function, the Copy Data Security Unit must be installed.

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. **The machine administrator logs in from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼] nine times.**
5. **Press [Data Security for Copying].**



6. **Press [On].**

   If you do not want to specify "Data Security for Copying", select [Off].

7. **Press [OK].**
8. **Log out.**

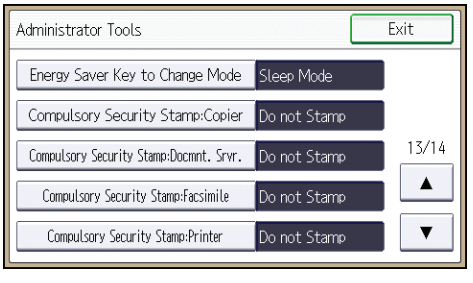
Printing User Information on Paper

Information such as the start time of a job, information on the person who outputs it (name or login user name), machine number or IP address of the machine can be forced to be printed on paper. This function is called Compulsory Security Stamp.

Always printing out information on the person who outputs a job has the effect of suppressing leaks of information. It can also be used in identifying the source of an information leak.

Compulsory Security Stamp can be used with each function, copying, Document Server, faxing and printing.

1. **The machine administrator logs in from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼] twelve times.**
5. **Select the function(s) for Compulsory Security Stamp.**



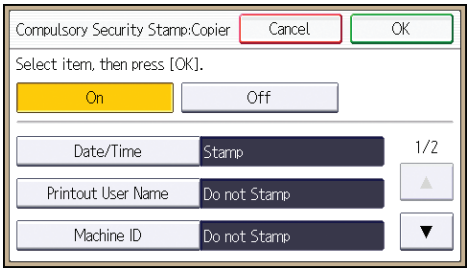
- To set the copy function to be stamped, press [Compulsory Security Stamp:Copier].
- To set the Document Server to be stamped, press [Compulsory Security Stamp:Docmnt. Srvr.].
- To set the fax function to be stamped, press [Compulsory Security Stamp:Facsimile].
- To set the printer function to be stamped, press [Compulsory Security Stamp:Printer].

6. **Press [On].**

   To turn Compulsory Security Stamp off, press [Off].

7. **Select the data you want to use for a stamp, and then press [Stamp]. After this, press [OK].**

   Any items that [Do not Stamp] is specified for will not be printed.



- Date/Time

  The time a job starts is printed.

- Printout User Name

  If "Stamp User Name" is selected, the "Name" in the "Names" in the Address Book is printed. If "Stamp Login User Name" is selected, the "Login User Name" in the "Auth. Info" in the Address Book is printed. When user authentication is not set up, or when User Code authentication is not set up, the name of the person who outputs a job is not printed.

- Machine ID

  The same number as the "Serial No. of Machine" in the [Enquiry] is printed.

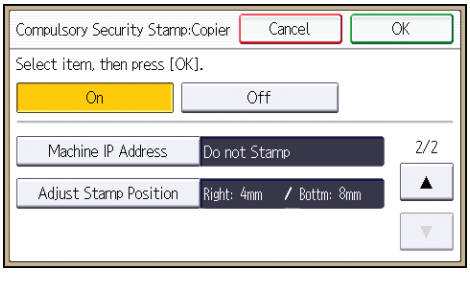
- Machine IP Address

  The IP address of the machine is printed. If both an IPv4 address and an IPv6 address exist, the IPv4 address is printed. If there is no IP address configured, then it does not stamp anything.

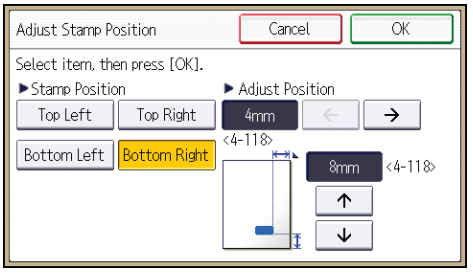
Pressing [▼] allows you to display all items.

8. **Press [Adjust Stamp Position].**

If it is not displayed, press [▼].



9. **Set the stamp position.**



10. **Press [OK] twice.**

11. **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.

Deleting Locked Print Files

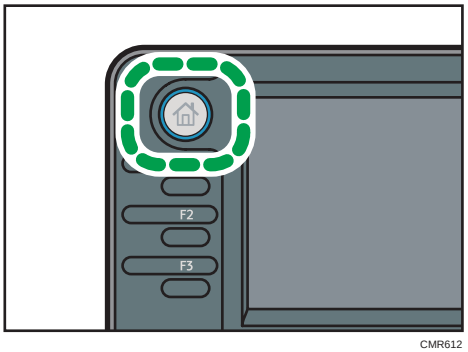
This can be specified by the file administrator or file creator (owner).

To delete Locked Print files, you must enter the password for the files. If the password has been forgotten, the file administrator changes the password to restore access.

1. **The file administrator or the file creator (owner) logs in from the control panel.**
2. **Press the [User Tools/Counter] key to switch to the normal screen.**

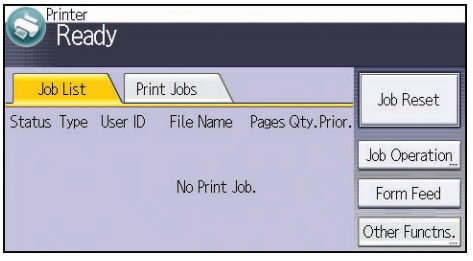
   If the message "You do not have the privileges to use this function." appears, press [Exit].
3. **Press the [Home] key on the top left of the control panel, and press the [Printer] icon on the [Home] screen.**

   If the message "You do not have the privileges to use this function." appears, press [Exit].

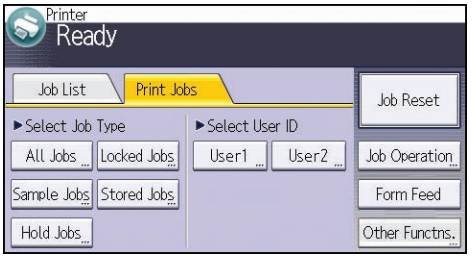


CMR612

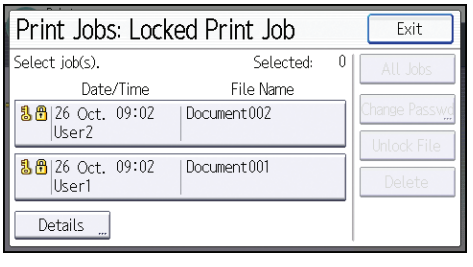
4. **Press [Print Jobs].**



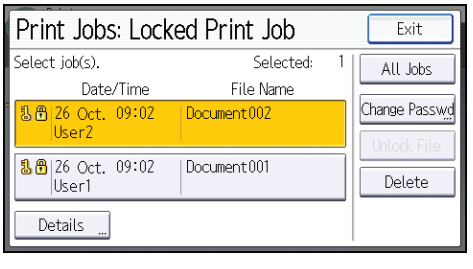
5. **Press [Locked Jobs].**



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 "Maintenance", 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

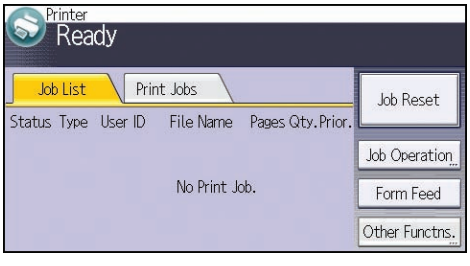
This can be specified by the file administrator or file creator (owner).

If the password has been forgotten, the file administrator changes the password to restore access.

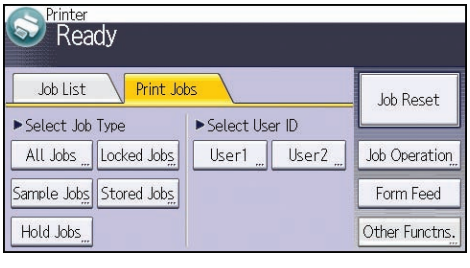
1. **The file administrator or the file creator (owner) logs in from the control panel.**
2. **Press the [User Tools/Counter] key to switch to the normal screen.**

   If the message "You do not have the privileges to use this function." appears, press [Exit].
3. **Press the [Home] key on the top left of the control panel, and press the [Printer] icon on the [Home] screen.**

   If the message "You do not have the privileges to use this function." appears, press [Exit].
4. **Press [Print Jobs].**

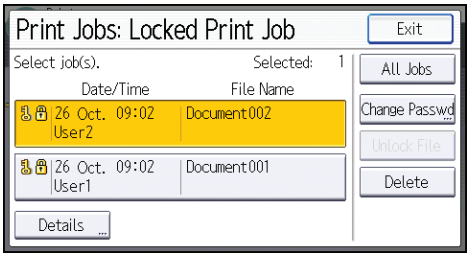


5. **Press [Locked Jobs].**



6. **Select the file.**

7. **Press [Change Passwd].**



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 p.259 "Specifying the Extended Security Functions".

1. **The file administrator logs in from the control panel.**
2. **Press the [User Tools/Counter] key to switch to the normal screen.**

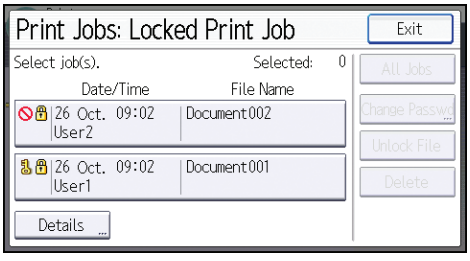
   If the message "You do not have the privileges to use this function." appears, press [Exit].

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

   If the message "You do not have the privileges to use this function." appears, press [Exit].

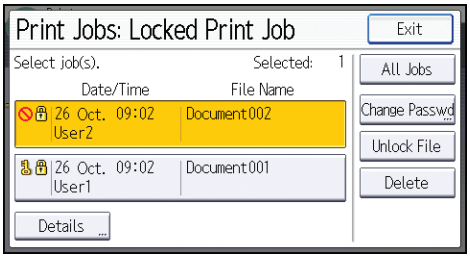
4. **Press [Print Jobs].**
5. **Press [Locked Jobs].**

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.

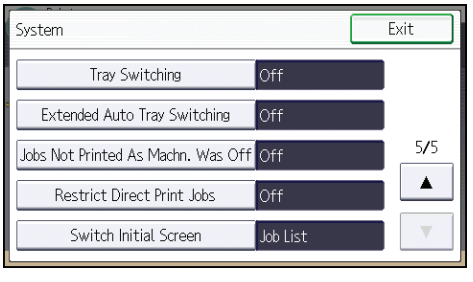
Enforced Storage of Documents to be Printed on a Printer

Enforced storage of documents to be printed on a printer prevents information leakage due to users failing to collect prints or leaving prints unattended.

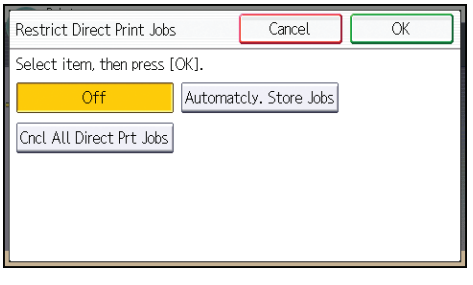
With respect to printer output, the following print jobs are subject to compulsory storage.

- Normal Print
- Sample Print
- Store and Print

1. **The machine administrator logs in from the control panel.**
2. **Press [Printer Features].**
3. **Press [System].**
4. **Press [▼] four times.**
5. **Press [Restrict Direct Print Jobs].**



6. **Press [Automatcly. Store Jobs].**



7. **Press [OK].**
8. **Log out.**

- If you select [Cncl All Direct Prt Jobs], the print jobs associated with printer output are cancelled and no data is stored.
- For information on how to print stored documents, see "Printing Stored Documents", Printer.

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, service 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 further details, refer to 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.

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.

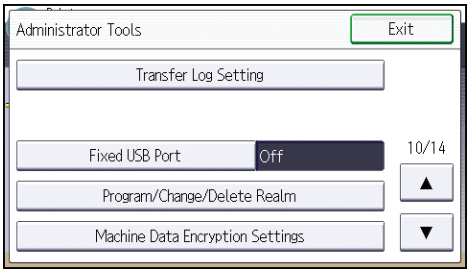
Disabling log transfer to the log collection server

Use the following procedure to disable log transfer from the machine to the log collection server. Note that you can change 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.

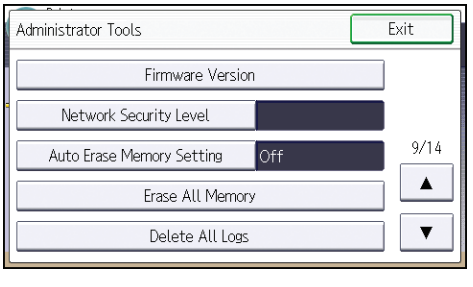
1. **The machine administrator logs in from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼] nine times.**
5. **Press [Transfer Log Setting].**



6. **Press [Off].**
7. **Press [OK].**
8. **Log out.**

Specifying Delete All Logs

1. **The machine administrator logs in from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼] eight times.**
5. **Press [Delete All Logs].**



6. **Press [Yes].**
7. **Press [Exit].**
8. **Log out.**

Note

- Deleting all logs from the machine as a batch can be achieved by either using the log collection server or via Web Image Monitor if the collection setting of one of the logs — job log, access log or eco-friendly log is enabled.

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.

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.

Specifying log collect settings

Enable the collection settings for each kind of log and configure the collection level.

Job Log Collect Level

Level 1

User Settings

Access Log Collect Level

Level 1

Level 2

User Settings

Eco-friendly Log Collect Level

Level 1

Level 2

User Settings

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. If the collection level selected is [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], click the web browser's [Reload] button.
8. **Log out.**

Note

- The greater "Access Log Collect Level" setting value, the more logs are collected.

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 change 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] under "Transfer Logs".**
5. **Click [OK].**
6. **Log out.**

Specifying log encryption

Use the following procedure to enable/disable log encryption.

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] under "Encrypt Logs".**

   To disable log encryption, select [Inactive].

5. **Click [OK].**

   A confirmation message appears.

6. **Click [OK].**
7. **Log out.**

Note

- To encrypt the logs, it is necessary to make the collection setting active for each of the job logs, access logs, and/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.

Deleting all logs

Use the following procedure to delete all logs stored in the machine.

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.**

Note

- When reading the log settings screen, "Delete All Logs" does not appear if the job log, access log, or eco-friendly log is not set to [Active].

Downloading logs

Use the following procedure to convert the logs stored in the machine into a CSV file for simultaneous batch download.

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 the two kinds of logs: job logs and access logs.

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.
- 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.
- For details about the items contained in the logs, see p.218 "Attributes of logs you can download".

Number of logs that can be kept on the machine

When the maximum number of job logs, access logs or eco-friendly logs that can be kept on the machine is exceeded and new logs are generated, the old logs are overwritten by the 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.

Maximum number of logs that can be stored in the machine

Job logs	Access logs	Eco-friendly logs
2,000	6,000	2,000

If the optional hard disk is not installed, the maximum number of job logs, access logs and eco-friendly logs that can be stored in the machine is 500 per log.

Estimated number of logs created per day

Job logs	Access logs	Eco-friendly logs
100 (per day)	300 This figure is based on 100 operations such as initialization and access operations over the Web and 200 access log entries (two entries per job: one login and one logout).	100 (per day)

According to these conditions, the machine can maintain logs for 20 days without overwriting, but to be cautious, we recommend downloading after half that time, 10 days, to leave room for error.

It is the responsibility of the machine administrator to deal downloaded log files appropriately.

Note

- If you change the [Collect] / [Do not Collect] setting for log collection, you must perform a batch deletion of the logs.
- After downloading the logs, perform a batch deletion of the logs.
- 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 value, the oldest logs are deleted and overwritten by newer logs. Whether or not the maximum number of logs that can be stored exceeds the maximum depends on the types of logs, which are job logs, access logs and eco-friendly logs.

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.

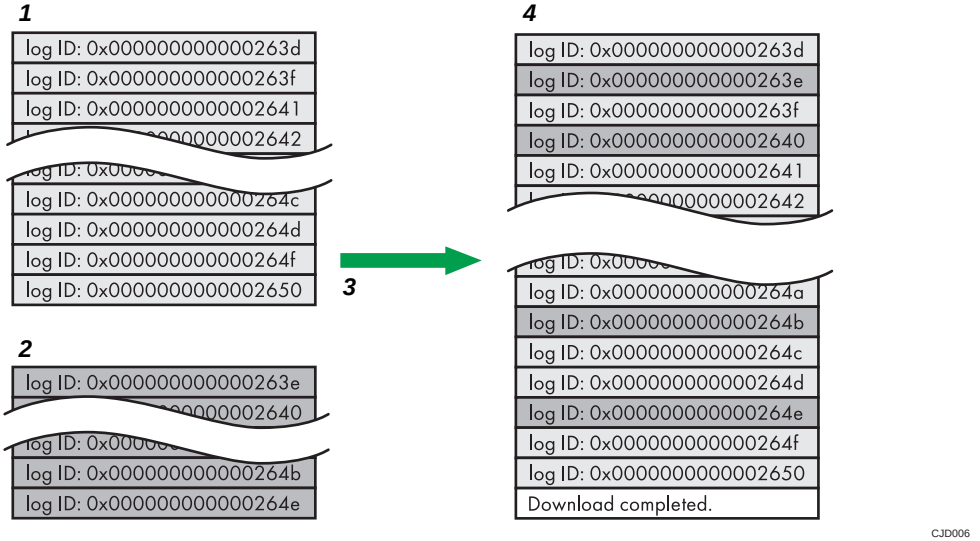
"If logs are downloaded during overwriting" below indicates that part of the access log is overwritten.

In this example, part of the access log was overwritten by a downloaded log and deleted.

The eco-friendly log is downloaded as an independent file.

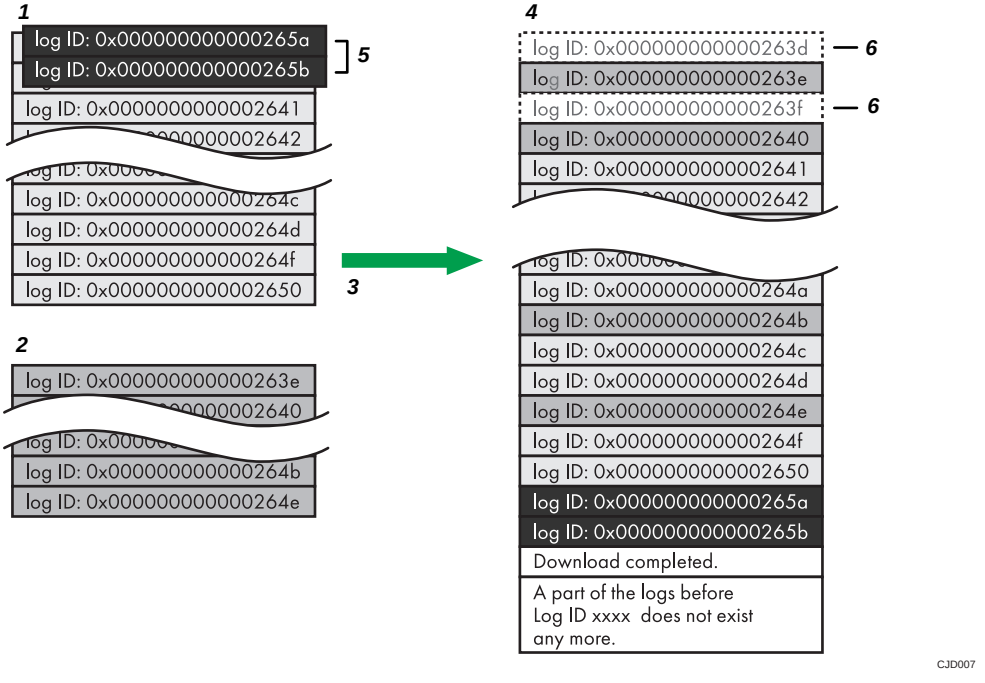
When logs are overwritten, it depends on the priority order and the logs with higher priority will not be overwritten or deleted.

If logs are downloaded without overwriting



1. **Access log**
2. **Job log**
3. **Download**
4. **Downloaded logs**

If logs are downloaded during overwriting



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

- Examine logs following "Log ID xxxx".

Printer Job Logs

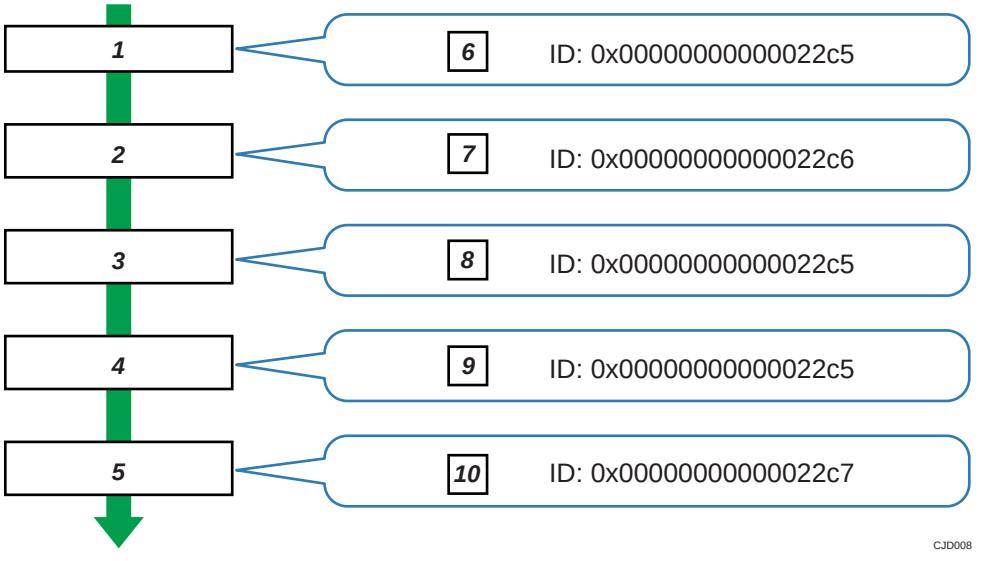
Print Log entries are made before the login entry is made in the Access Log.

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



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.

Logs That Can Be Managed Using Web Image Monitor

Logs that can be collected

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 or DeskTopBinder.
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.
Scanner: Stored File Downloading	Scanner: Stored File Downloading	Details of scan files stored in Document Server and downloaded using Web Image Monitor, DeskTopBinder 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.

Job Log Item	Log Type Attribute	Content
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.
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.

Job Log Item	Log Type Attribute	Content
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 or DeskTopBinder.
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.
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.

Access Log Item	Log Type Attribute	Content
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.
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.

Access Log Item	Log Type Attribute	Content
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.
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.

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.

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.

Note

- If "Job Log Collect Level" is set to [Level 1], all job logs are collected.
- 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.
- The first log made following power on is the "Firmware: Structure" log.
- 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.

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

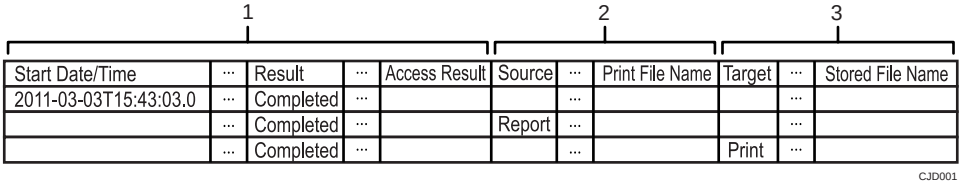
  Multiple lines appear in the order of All, Source (job input data), and Target (job output data). The same log ID is assigned to all lines corresponding to a single job log entry.

- Access log

  Items in the list and access log entries appear on separate lines.

- Eco-friendly log

  Items in the list and eco-friendly log entries appear on separate lines.



1. **All**

   Each item in the list is displayed on a separate line.

2. **Source**

   Displays details of the job log entry and the "Result" and "Status" of each item.

   If there are multiple sources, multiple lines are displayed.

3. **Target**

   Displays details of the job log entry and the "Result" and "Status" of each item.

   If there are multiple targets, multiple lines are displayed.

Job and access log information items

Item	Content
Start Date/Time	For a job log entry, indicates the start date and time of the operation. If the job has not been completed, this is blank. For an access log entry, indicates the same date and time as shown by "End Date/Time". This is in Item 1 of the CSV file.
End Date/Time	For a job log entry, indicates the end date and time of the operation. If the operation is still in progress, this will be blank. For an access log entry, indicates the same date and time as shown by "Result". This is Item 2 of the CSV file.
Log Type	Details of the log type. Access logs are classified under "Access Log Type". For details about the information items contained in each type of log, see p.212 "Logs that can be collected". This is Item 3 of the CSV file.
Result*1	Indicates the result of an operation or event: • If "Succeeded" is displayed for a job log entry, the operation completed successfully; "Failed" indicates the operation was unsuccessful. If the operation is still in progress, this will be blank. • If "Succeeded" is displayed for an access log entry, the event completed successfully; "Failed" indicates the event was unsuccessful.
Operation Method	Operation procedures are recorded.

Item	Content
Status	Indicates the status of an operation or event: • If "Completed" is displayed for a job log entry, the operation completed successfully; "Failed" indicates the operation was unsuccessful; "Processing" indicates the operation is still in progress. • If "Completed" is displayed for "Source" or "Target" in a job log entry, the operation completed successfully; "Failed" indicates the operation was unsuccessful; "Processing" indicates the operation is still in progress; "Error" indicates an error occurred; "Suspended" indicates the operation is currently suspended. • If "Succeeded" is displayed for an access log entry, the operation completed successfully; if any of the following are displayed, the operation was unsuccessful: "Password Mismatch", "User Not Programmed", "Other Failures", "User Locked Out", "File Password Mismatch", "No Privileges", "Failed to Access File", "File Limit Exceeded", "Transfer Cancelled", "Power Failure", "Lost File", "Functional Problem", "Communication Failure", or "Communication Result Unknown".
Status (For results of clearing user-specific counter, for results of clearing all-user counter)	If clearing user-specific counter or all-user counter fails, "Failure in some or all parts" is recorrded.

Item	Content
Status (For importing and exporting device information)	The status of an operation or event is recorded. If importing or exporting is executed by another user, "Importing/Exporting by Other User" is recorded. If a connection to an output destination fails, "Connection Failed with Remote Machine" is recorded. If an error occurs in writing to an output destination, "Write Error to Remote Machine" is recorded. If the specified file is incompatible, "Specified File: Incompatible" is recorded. If a format error occurs with the specified file, "Specified File: Format Error" is recorded. If the specified file cannot be found, "Specified File: Not Exist" is recorded. If there are no privileges for operating the specified file, "Specified File: No Privileges" is recorded. If an error occurs in accessing the specified file, "Specified File: Access Error" is recorded. If the external media is full, "Memory Storage Device Full" is recorded. If an abnormality is found in the external media, "Memory Storage Device Error" is recorded. If encryption fails, "Encryption Failed" is recorded. If decoding fails, "Decoding Failed" is recorded. If there are no common keys, "Common Key Not Exist" is recorded. If a communication error occurs, "Connection Error" is recorded.

Item	Content
Status Supplement	If the status of a log is abnormal termination (Failed), the status is recorded. If it does not terminate abnormally, nothing is recorded. If a user cancels an operation, "Cancelled by User" is recorded. If it terminates abnormally during input, "Input Failure" is recorded. For the reason it failed, refer to the input information (Source) noted below it. If it terminates abnormally during output, "Output Failure" is recorded. For the reason it failed, refer to the output information (Target) noted below it. If an error is detected prior to execution of a job, "Other Error" is recorded. If power is lost, "Power Failure" is recorded.
Status Supplement (If the Source is a Scan File)	If the accounting device is unplugged during operation, "External Charge Unit Disconnected" is recorded. If pages are missing from a manuscript during execution of the overlaid copying, "Insufficient No. of Original for Overlay" is recorded. If the storage capacity of pages on Document Server is exceeded, "Exceed Max. Stored Page (File Storage)" is recorded. If the storage capacity of documents on Document Server is exceeded, "Exceed Max. Stored File (File Storage)" is recorded. If the hard disk capacity on Document Server is exceeded, "Hard Disk Full (File Storage Memory)" is recorded. If the limit to e-mail size is exceeded, "Exceeded Max. Email Size" is recorded. If the size limit for one document is exceeded, "Exceeded Max. File Size" is recorded. If a read error occurs with the automatic document feed, "Scanner Error" is recorded. If a time-out occurs, "Timeout" is recorded. If any other error occurs, "Other Error" is recorded.

Item	Content
Status Supplement (If the Source is a Stored File)	If the number of pages that can be captured is exceeded, "Exceed Max. Stored Page (Image Area)" is recorded. If the hard disk capacity for capture is exceeded, "Hard Disk Full (Image Area)" is recorded. If the memory range for processing data becomes full, "Memory Full" is recorded. If an attempt to use a PDL or port not installed on the machine is made, "Print Data Error" is recorded. If the wrong type of driver is used, a network malfunction occurs, a job is cancelled by the PC fax driver or a fax communication failure occurs, "Data Transfer Interrupted" is recorded. If any other error occurs, "Other Error" is recorded.
Status Supplement (If the Source is a Received File)	If a fax fails to be received, "Reception Error" is recorded.

Item	Content
Status Supplement (If the Source is a Printer)	If the number of jobs that can be received is exceeded, "Over Job Limit" is recorded. If an illegal address or an address with 41 or more digits is specified, "Specifying Destination Error" is recorded. If an error occurs in the line specified, "Specifying Line Error" is recorded. If the memory range for processing data becomes full, "Memory Full" is recorded. If device authentication fails, "Authentication Failed (Access Restricted)" is recorded. If the wrong type of driver is used, a network malfunction occurs, a job is cancelled by the PC fax driver or a fax communication failure occurs, "Data Transfer Interrupted" is recorded. If an attempt to use a PDL or port not installed on the machine is made, "Print Data Error" is recorded. If the storage capacity of pages on Document Server is exceeded, "Exceed Max. Stored Page (File Storage)" is recorded. If the storage capacity of documents on Document Server is exceeded, "Exceed Max. Stored File (File Storage)" is recorded. If any other error occurs, "Other Error" is recorded.
Status Supplement (If the Source is a Report)	If a system error is detected on the machine, "Other Error" is recorded.

Item	Content
Status Supplement (If the Target is Store)	If the accounting device is unplugged during operation, "External Charge Unit Disconnected" is recorded. If the logged in user exceeds their paper usage limit, "Exceeded Print Volume Use Limitation" is recorded. If a time-out occurs, "Timeout" is recorded. If the user does not have permission to use a document or function, "No Privilege" is recorded. If the storage capacity of pages on Document Server is exceeded, "Exceed Max. Stored Page (File Storage)" is recorded. If the storage capacity of documents on Document Server is exceeded, "Exceed Max. Stored File (File Storage)" is recorded. If the hard disk capacity on Document Server is exceeded, "Hard Disk Full (File Storage Memory)" is recorded. If the size of paper specified (including irregular sizes) is of a size that cannot be stored, "Unavailable Size to Store" is recorded. If the number of pages that can be captured is exceeded, "Exceed Max. Stored Page (Image Area)" is recorded. If the hard disk capacity for capture is exceeded, "Hard Disk Full (Image Area)" is recorded. If any other error occurs, "Other Error" is recorded.

Item	Content
Status Supplement (If the Target is Send 1)	If a time-out occurs, "Timeout" is recorded. If a document is deleted or an undelivered document exceeds its wait time and is deleted, "Transmission Failed (Data Deleted)" is recorded. If the user does not have permission to use a document or function, "No Privilege" is recorded. If the password for a document is not input, "Not Entered Document Password" is recorded. If the specified server or folder is not found, "Connection Failed with Destination" is recorded. If authentication with the destination fails, "Authentication Failed with Destination" is recorded. If the destination memory is full, "Transmission Failed with Memory Full" is recorded. If the memory range for processing data becomes full, "Memory Full" is recorded.
Status Supplement (If the Target is Send 2)	If the wrong type of driver is used, a network malfunction occurs, a job is cancelled by the PC fax driver or a fax communication failure occurs, "Data Transfer Interrupted" is recorded. If the destination is busy, "Line Busy" is recorded. If there is not response from the destination, "No Response" is recorded. If the destination is not a fax machine, "Not Facsimile Destination" is recorded. If the limit to e-mail size is exceeded, "Exceeded Max. Email Size" is recorded. If any other error occurs, "Other Error" is recorded. If there is no device certificate, its valid period is elapsed, or if the e-mail address of the administrator and that of the certificate do not match, "Invalid Device Certificate" is recorded. If the valid period of the destination certificate is expired, "Invalid Expiration Date: Destination's Certificate" is recorded. If both the destination certificate and the device certificate are invalid, "Invalid Device/Destination's Certificate" is recorded.

Item	Content
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: For supervisors, only 0xffffff86 is available; for administrators, 0xffffff87, 0xffffff88, 0xffffff89, and 0xffffff8a are available. For general users, any value between 0x00000001 and 0xfffffeff is available. "0x00000000", "0xffffff80", and "0xffffff81" indicate system operations related to user authentication. IDs "0xffffff80" and "0xffffff81" indicate system operations related to stored files and the address book; "0x00000000" indicates other operations. "0xffffff80" indicates operations related to deleting Hold Print, Locked Print, and Stored Print jobs (such as when the [Auto Delete Temporary Print Jobs] setting is enabled), and operations related to changing the access permissions of such jobs. Displays Address Book updates when Auto registration of users is enabled through Windows, LDAP, or another authentication system. ID "0xffffff81" indicates only operations related to the creation of stored files when it is assumed such files will be deleted through system operations. "0x00000000" and "0xffffff81" indicate operations that do not require user authentication (such as copying and scanning) and that were performed by non-authenticated users. ID "0xffffff81" indicates operations related to stored files, the address book and job logs; "0x00000000" indicates other operations.
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.

*1 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).

Access log information items

Item	Content
Access Log Type	Indicates the type of access: "Authentication" indicates a user authentication access. "System" indicates a system access. "Stored File" indicates a stored file access. "Network Attack Detection/Encrypted Communication" indicates a network attack or encrypted communication access. "Firmware" indicates a firmware verification access. "Address Book" indicates an address book access.
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 determine whether or not authentication server availability is detected. The number of server switches is indicated as 0 to 4. A value of 0 indicates the authentication server is available.
Logout Mode	Mode of logout. The remark "by User's Operation" indicates manual logout by the user; "by Auto Logout Timer" indicates automatic logout following a timeout.
Login Method	The route by which the authentication request is received is recorded. "Control Panel" indicates the login was performed through the control panel; "via Network" indicates the login was performed remotely through a network computer; and "Others" indicates the login was performed through another method.

Item	Content
Login User Type	Indicates the type of login user: "User" indicates the logged in user was a registered general user. "Guest" indicates the logged in user was a guest user. "File Administrator" indicates the logged in user was a registered file administrator. "Machine Administrator" indicates the logged in user was a registered machine administrator. "Network Administrator" indicates the logged in user was a registered network administrator. "Supervisor" indicates the logged in user was a registered supervisor. "Custom Engineer (Service Mode)" indicates the logged in user was a customer engineer. "Others" indicates the logged in user did not belong to any of the above types of user.
Target User Entry ID	Indicates the entry ID of the target user is. 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.	The registration number of the user who performs the operation is recorded.
Address Book Operation Mode	The method of how the Address Book is changed is recorded.
Address Book Change Item	Which content of the Address Book is changed is recorded.
Address Book Change Request IP Address	The IP address information (IPv4/IPv6) of the user who operated the Address Book is recorded.

Item	Content
Lockout/Release	The mode of operation access. "Lockout" indicates activation of password lockout; "Release" indicates deactivation of password lockout.
Lockout Release Method	"Manual" is recorded if the machine is unlocked manually. "Auto" is recorded if the machine is unlocked by the lockout release timer.
Lockout Release Target Administrator	If a lockout is deactivated, the target administrator is recorded.
Counter to Clear	Which counter is reset for each user is recorded.
Export Target	The setting information that is the target of device information exporting is recorded. The recorded information is specified below: • System Settings, Copier Features, Facsimile Features, Printer Features, Scanner Features, Program (Copier), Program (Scanner), Program (Document Server), Browser Features, Web Image Monitor Setting, Web Service Settings, System/Copier SP, Scanner SP, Printer SP, Facsimile SP
Target File Name	The file name that is the target of device information importing or exporting is recorded.
Stored File ID	Identifies a created or deleted file. This is a hexadecimal ID that indicates created or deleted stored files.
Stored File Name	Name of a created or deleted file.
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: "Active" indicates job log collection is enabled. "Inactive" indicates job log collection is disabled. "Not Changed" indicates no changes have been made to the job log collection setting.

Item	Content
Collect Access Logs	Indicates the status of the access log collection setting: "Active" indicates access log collection is enabled. "Inactive" indicates access log collection is disabled. "Not Changed" indicates 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: "Active" indicates eco-friendly log collection is enabled. "Inactive" indicates eco-friendly log collection is disabled. "Not Changed" indicates no changes have been made to the eco-friendly log collection setting.
Transfer Logs	Indicates the status of the log transfer setting: "Active" indicates log transfer is enabled. "Inactive" indicates log transfer is disabled. "Not Changed" indicates no changes have been made to the log transfer setting.
Encrypt Logs	Indicates the status of the log encryption setting: "Active" indicates log encryption is enabled. "Inactive" indicates log encryption is disabled. "Not Changed" indicates no changes have been made to the log encryption setting.
Log Type	If a log's collection level setting has been changed, this function indicates details of the change: "Job Log" indicates the job log's collection level has been changed. "Access Log" indicates the access log's collection level has been changed. "Eco-friendly Log" indicates the eco-friendly log's collection level has been changed. "Level 1" indicates a level 1 collection setting. "Level 2" indicates a level 2 collection setting. "User Settings" indicates a user-specified collection level setting.

Item	Content
Log Collect Level	Indicates the level of log collection: "Level 1", "Level 2", or "User Settings".
Encryption/Cleartext	Indicates whether communication encryption is enabled or disabled: "Encryption Communication" indicates encryption is enabled; "Cleartext Communication" indicates encryption is not disabled.
Machine Port No.	Indicates the machine's port number.
Protocol	Destination protocol. "TCP" indicates the destination's protocol is TCP; "UDP" indicates the destination's protocol is UDP; "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: "Communication Start Request Receiver (In)" indicates the machine received a request to start communication; "Communication Start Request Sender (Out)" indicates 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.

Item	Content
Network Attack Status	Indicates the attack status of the network: "Violation Detected" indicates an attack on the network was detected. "Recovered from Violation" indicates the network recovered from an attack. "Max. Host Capacity Reached" indicates the machine became inoperable due to the volume of incoming data reaching the maximum host capacity. "Recovered from Max. Host Capacity" indicates that the machine became operable again following reduction of the volume of incoming data.
Network Attack Type	Identifies the type of network attack as either "Password Entry Violation" or "Device Access Violation".
Network Attack Type Details	Indicates details about the type of network attack: "Authentication Error" or "Encryption Error".
Network Attack Route	Identifies the route of the network attack as either "Attack from Control Panel" or "Attack from Other than Control Panel".
Login User Name used for Network Attack	Identifies the login user name that the network attack was performed under.
Add/Update/Delete Firmware	Indicates the method used to add, update, or delete the machine's firmware: "Updated with SD Card" indicates an SD card was used to perform the firmware update. "Added with SD Card" indicates an SD card was used to add the firmware update. "Deleted with SD Card" indicates an SD card was used to delete the firmware update. "Moved to Another SD Card" indicates the firmware update was moved to another SD card. "Updated via Remote" indicates the firmware update was updated remotely from a computer. "Updated for Other Reasons" indicates the firmware updated was performed using a method other than any of the above.
Module Name	Firmware module name.

Item	Content
Parts Number	Firmware module part number.
Version	Firmware version.
Machine Data Encryption Key Operation	Indicates the type of encryption key operation performed: "Back Up Machine Data Encryption Key" indicates an encryption key backup was performed. "Restore Machine Data Encryption Key" indicates an encryption key was restored. "Clear NVRAM" indicates the NVRAM was cleared. "Start Updating Machine Data Encryption Key" indicates an encryption key update was started. "Finish Updating Machine Data Encryption Key" indicates an encryption key update was finished.
Machine Data Encryption Key Type	Identifies the type of the encryption key as "Encryption Key for Hard Disk", "Encryption Key for NVRAM", or "Device Certificate".
Validity Error File Name	Indicates the name of the file in which a validity error was detected.
Configuration Category	The category whose settings were changed is recorded. For details, see "Category/Attribute List".
Configuration name	The attributes of the categories are recorded. For details, see "Category/Attribute List".
Configuration value	The values of the attributes are recorded. For details, see "Category/Attribute List".
Destination Server Name	If the log type is "SDK Tracking", the name of the destination server that tracking information failed to be sent is recorded. If the log type is import or export of preference information, the name of the server that a data export or import request is issued from is recorded.
Hdd Init Partition No.	The initial status of each hard disk partition is recorded.

Item	Content
Access Result	Indicates the results of logged operations: "Completed" indicates an operation completed successfully; "Failed" indicates an operation completed unsuccessfully.

Job log information items

Input information

Item	Content
Source	Indicates the source of the job file: "Scan File" indicates the job file was scanned in; "Stored File" indicates the job file was stored on the hard disk; "Printer" indicates the job file was sent from the printer driver; "Received File" indicates the job file was received over the network; "Report" indicates 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.
Print File Name	Name of "Printer" files.

Output information

Item	Content
Target	Type of the job target. "Print" indicates a print file; "Store" indicates a stored file; "Send" indicates a sent file.
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.

Item	Content
Stored File ID*1	Indicates the ID of data that is output as a store file. This is a decimal ID that identifies the stored file.
Stored File Name*2	If the Target Type is "Store", the file name of the stored file is recorded.

Printing stored faxes from the Fax screen before transmission will not be recorded in the job log.

*1 Stored File ID logs are not logged for documents processed using fax functions.

*2 Stored File Name logs are not logged for documents processed using fax functions.

Eco-friendly log information items

Item	Content
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. Power ON, Power OFF, Status of Power, Job Information or Consumption of Paper is recorded.
Log Result	Whether the event has ended or not is displayed. When the event ends normally, "Completed" is recorded. When the event does not end normally, "Failed" is recorded.
Result	The result of the event is recorded. When the event is successful, "Succeeded" is recorded. When the event fails, "Failed" is recorded.
Log ID	Identifies the ID that is assigned to the log. This is a hexadecimal ID that identifies the log.

Item	Content
Power Mode (After)	The power status of the machine (after state transition) is logged. When in standby, "Standby" is recorded. When in a silent state, "Silent" is recorded. When the hard disk is running, "HDD On" is recorded. When the engine is stopped, "Engine Off" is recorded. When the controller is stopped, "Controller Off" is recorded. When in the STR state (Suspend to RAM), "STR" is recorded. When in a silent print state, "Silent Print" is recorded. When in a low-noise print state, "Low Power Print" is recorded.
Job Interval (seconds)	The elapsed time from the start of the previous job until the start of the job is recorded.
Job Duration (seconds)	The elapsed time from the start of a job until its end is recorded.
Paper Usage (Large Size)	The amount of large, one-sided paper used each hour is recorded. Large size means A3 (11 × 17 inches) or larger.
Paper Usage (Small Size)	The amount of small, one-sided paper used each hour is recorded. Small size means A3 (11 × 17 inches) or smaller.
Paper Usage (2 Sided: Large Size)	The amount of large, two-sided paper used each hour is recorded. Large size means A3 (11 × 17 inches) or larger.
Paper Usage (2 Sided: Small Size)	The amount of small, two-sided paper used each hour is recorded. Small size means A3 (11 × 17 inches) or smaller.

Item	Content
Detected Power	The power consumption status of the machine is measured and registered in the log while the machine is being used. "Controller Standby" indicates controller standby mode. "STR" indicates Suspend to RAM (STR) mode. "Main Power Off" indicates the main power is turned off. "Scanning/Printing" indicates simultaneous scanning and printing. "Printing" indicates the machine's printing status. "Scanning" indicates the machine's scanning status. "Engine Standby" indicates the engine's standby status. "Engine Low" indicates the engine's low-power status. "Engine Night" indicates the engine's the silent status. "Engine Total" indicates the machine's total electricity consumption.
Power Consumption(Wh)	The power consumption in each power state is recorded.

Category/Attribute List

Category	Attribute	Description
User Lockout Policy	1. Lockout 2. Number of Attempts before Lockout 3. Lockout Release Timer 4. Lock Out User for	1. Whether the lockout is active (Active) or inactive (Inactive) is recorded. 2. The number of times a user may enter a login password is recorded. 3. Whether the lockout release timer is active (Active) or inactive (Inactive) is recorded. 4. The time until lockout release is recorded.
Auto Logout Timer	1. Auto Logout Timer 2. Auto Logout Timer(seconds)	1. Whether an auto logout time is set to (On) or (Off) is recorded. 2. The time until the auto logout operates is recorded.

Category	Attribute	Description
Device Certificate	1. Operation Mode 2. Certificate No. 3. Certificate No. (XXX) (XXX) is replaced by one of the following: • SSL/TLS • IEEE 802.1X • S/MIME • IPsec • PDF Digital Signature • PDF/A Digital Signature	1. The type of operation is recorded. "Create" is recorded when a certificate is created. "Delete" is recorded when a certificate is deleted. "Install" is recorded when a certificate is installed. When the certificate to be used is changed, "Change Application to Use Certificate" is recorded. When an intermediate certificate is installed, "Install Intermediate Certificate" is recorded. When an intermediate certificate is deleted, "Delete Intermediate Certificate" is recorded. 2. The number of the certificate to be used is recorded. 3. The number of the certificate for applications is recorded. When a certificate is not used, "Do not Use" is recorded.

Category	Attribute	Description
IPsec	1. IPsec 2. Encryption Key Auto Exchange / Encryption Key Manual Exchange: Setting1-4: Remote Address 3. Encryption Key Auto Exchange: Setting1-4, Default: Security Level 4. Encryption Key Auto Exchange: Setting1-4, Default: Authentication Method	1. Whether IPsec is active (Active) or inactive (Inactive) is recorded. 2. The remote address is recorded. 3. 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. 4. The authentication method used for the auto key exchange format is recorded. Either "PSK" or "Certificate" is recorded.
Compulsory Security Stamp	Compulsory Security Stamp	Whether [Compulsory Security Stamp] is set to (On) or (Off) is recorded.

Category	Attribute	Description
S/MIME	1. Operation Mode 2. When Sending E-mail by Scanner 3. When Transferring by Fax 4. When Sending E-mail by Fax 5. When E-mailing TX Results by Fax 6. When Transferring Files Stored in Document Server (Utility)	1. The mode of operation is recorded. 2. The signature is recorded when the scanner is used for sending e-mail. 3. The signature is recorded when transferring by fax. 4. The signature is recorded when the fax is used for sending e-mail. 5. The signature is recorded when the fax is used for sending e-mail notification. 6. The signature is recorded when Document Server (utility) is used for transferring documents stored on it.

Customizing the Control Panel

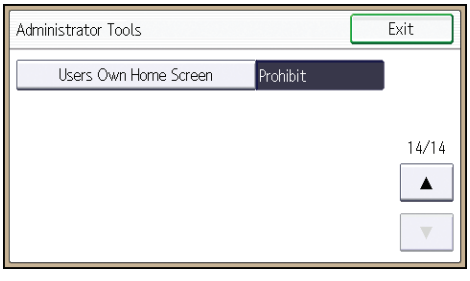
Configurations of settings such as arrangement of icons on the home screen or allocation of function keys to functions can be made to suit the user.

Configuring the Home Screen for Individual Users

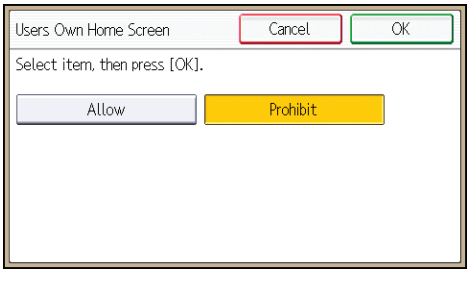
This allows each user to use their own home screen.

When a user logs in, their personalized home screen is displayed.

1. **The machine administrator logs in from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼] 13 times.**
5. **Press [Users Own Home Screen].**



6. **Press [Allow].**



7. **Press [OK].**
8. **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 Users Own Home Screen 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.
- The icons of functions that an administrator has restricted are not displayed on the home screen of users whose use of the function(s) has been restricted.
- 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 p.132 "Configuring SSL/TLS".

For details about installing site certificates, see p.169 "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 p.248 "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.

Changing the Browser Settings

You can change the default settings for the browser functions.

1. **The machine administrator logs in from the control panel.**
2. **Press [Browser Features].**

3. **Press [Browser Default Setting].**
4. **Press the setting you want to change, and change the setting.**
5. **Press [OK].**
6. **Press [Exit] twice.**
7. **Log out.**

Browser default settings

Home Screen

Specify the URL of your home screen.

Cache File

Specify whether or not to enable cache files.

When using cache files, specify a size within a range between 1024 and 10240 KB.

To clear cache files, press [Clear Caches].

Default: [**Do not use**]

Keep the History

Specify whether or not to keep the history.

When keeping the history, specify a duration between 1 and 30 days.

Default: [**Off**]

JavaScript

Specify whether or not to activate JavaScript and its extended function.

When JavaScript is inactive, the JavaScript extensions are also inactive.

- JavaScript

  Default: [**Active**]

- Extended JavaScript

  Default: [**Inactive**]

Use Cookies

Up to 20 cookies are stored for access by any user.

The cookie created when the machine administrator uses the browser is automatically deleted when the machine administrator logs out.

Default: [**On**]

Use Proxy Server

Specify whether or not to use a proxy server.

When using a proxy server, specify "Proxy Server Name", "Proxy Port", "Proxy User Name", "Proxy Password", and "Exceptional Addresses".

Default: [Off]

User Agent

Specify the user agent.

Enter the user agent's name using the keyboard.

Default HTTP Request Method

Specify the type of HTTP request method.

Default: [GET]

Screen Settings

Specify whether or not to display the URL bar and the horizontal scroll bar.

- URL Bar

  Default: [Display]

- Horizontal Scroll Bar

  Default: [Display]

Bookmark

You can register and manage bookmarks, including changing, deleting, importing and exporting.

Restricting User Browser Functions

You can restrict the user functions when using the browser.

1. **The machine administrator logs in from the control panel.**
2. **Press [Browser Features].**
3. **Press [Settings per Users].**
4. **Press the setting you want to change, and change the setting.**
5. **Press [OK].**
6. **Press [Exit] twice.**
7. **Log out.**

Screen settings by user settings

Home Screen

Specify whether or not to enable the home screen to be displayed.

Default: [Allow]

Bookmark

Specify whether or not to enable the use of bookmarks.

Default: [Allow]

Use Proxy Server

Specify whether or not to enable a proxy server.

Default: [Allow]

Keep the History

Specify whether or not to enable the history to be kept.

Default: [Allow]

Screen Settings

Specify whether or not to enable the size of the window displayed on the control panel.

Default: [Allow]

Checking the Usage Status of the Browser Functions

The following logs can be used to check how the browser functions has been used.

- View Send Log
- View Download Log
- View Print Log

1. **The machine administrator logs in from the control panel.**
2. **Press [Browser Features].**
3. **Press [View Logs].**
4. **Press [View Send Log], [View Download Log], or [View Print Log].**
5. **Press [Exit] three times.**
6. **Log out.**

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 out of reach of children. If a child accidentally swallows an SD card, consult a doctor immediately.

This can be set by an administrator with privileges to manage everything — devices, users, networks and files.

The device information of a machine can be exported to an outside device as a device setting information file. If an exported device setting information file is imported to the machine, the file can be used for backups since any changed settings will return to their default settings.

Also, managing device setting information file with the device management server, allows device setting information file to be imported periodically at a specified time or at device startup.

Data that can be imported and exported

- Copier / Document Server Features
- Printer Features
- Scanner Features
- Facsimile Features
- Extended Feature Settings
- Program (Document Server)
- Program (Copier)
- Program (Scanner)
- Web Image Monitor Setting
- Web Service Settings
- System Settings

Data that cannot be imported or exported

- Address book
- Programs (fax function)
- Programs (printer function)
- Scanner function programs that include password settings
- Settings for configuring from telnet

Note

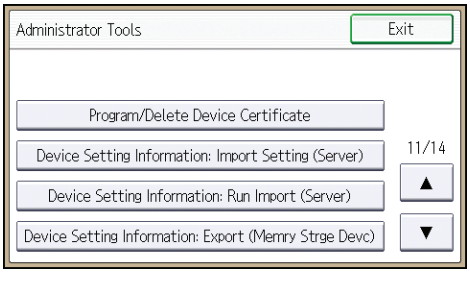
- The file format for exports is CSV.

- The device configurations of the device setting information file to be imported from the control panel must be the same as those of the device setting information file that is exported. If not, the device setting information file cannot be imported.
- If the device configurations of the device setting information file are changed, update the file.
- If multiple devices have the same device configuration, import the device setting file so that the device settings are the same.
- When images are inserted into a home screen, JPG image files are also 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.

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.**
2. **Log in from the control panel as an administrator with all privileges.**
3. **Press [System Settings].**
4. **Press [Administrator Tools].**
5. **Press [▼] ten times.**
6. **Press [Device Setting Information: Export (Memry Strge Devc)].**



7. **Press [Device Unique Information].**

   Device unique information includes the IP address, host name, fax number, etc.
8. **Press [Enter Encryption Key].**
9. **Enter an encryption key, and then press [OK].**
10. **Press [Run Export].**
11. **Press [OK].**
12. **Press [Exit].**
13. **Log out.**

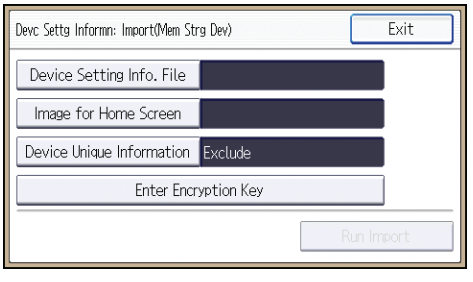
Note

- If data export fails, the details of the error can be viewed in the log.

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.**
2. **Log in from the control panel as an administrator with all privileges.**
3. **Press [System Settings].**
4. **Press [Administrator Tools].**
5. **Press [▼] eleven times.**
6. **Press [Device Setting Information: Import (Memry Strge Devc)].**
7. **Press [Device Setting Info. File].**



8. **Select the file(s), and then press [OK].**
9. **Press [Image for Home Screen].**
10. **Select the file, and then press [OK].**
11. **Press [Device Unique Information].**

    Device unique information includes the IP address, host name, fax number, etc.
12. **Select [Include] or [Exclude], and then press [OK].**
13. **Press [Enter Encryption Key].**
14. **Specify the encryption key that was created when the file was exported, and then press [OK].**
15. **Press [Run Import].**
16. **Press [OK].**
17. **Press [Exit].**

    The machine restarts.

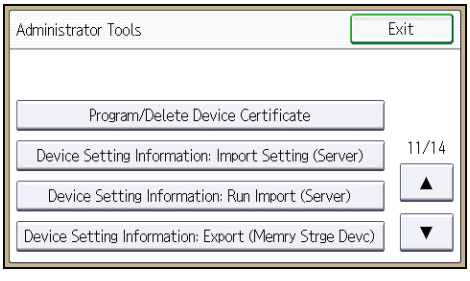
Note

- If data import fails, the details of the error can be viewed in the log.

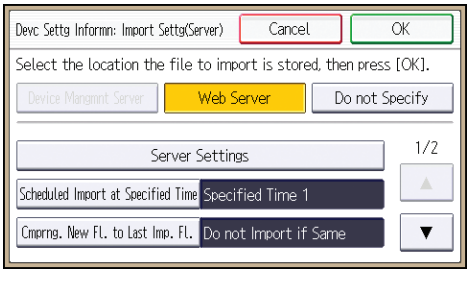
Periodically Importing Device Information

This setting enables automatic importing of device information stored on a server.

1. **Log in from the control panel as an administrator with all privileges.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼] ten times.**
5. **Press [Device Setting Information: Import Setting (Server)].**



6. **Configure the import conditions.**



   - Select the source for importing files. Configure settings such as the URL, user name, password, etc., using the detail settings of the server.
   - Select the frequency for importing device setting information files and set the time used for a periodic import at the specified time.
   - Specify whether or not to import a device setting information file if it is identical as compared to the last imported file.
   - Specify an encryption key.
   - Select whether or not to send e-mail notification to the machine administrator when importing fails.
7. **Press [OK].**

8. **Log out.**

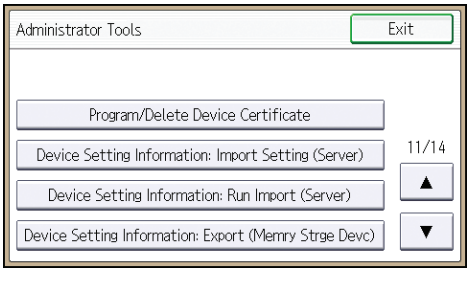
Note

- If data import fails, the details of the error can be viewed in the log.

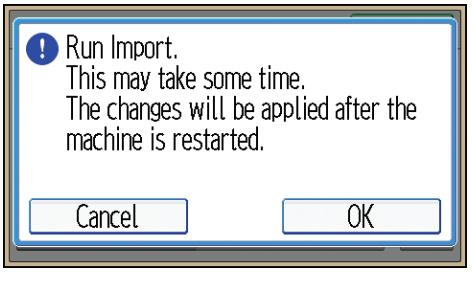
Manually Importing the Device Setting Information File of a Server

Manually import the device setting information file specified with [Device Setting Information: Import Setting (Server)].

1. **Log in from the control panel as an administrator with all privileges.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼] ten times.**
5. **Press [Device Setting Information: Run Import (Server)].**



6. **Press [OK].**



7. **Press [Exit].**

   The machine restarts.

Note

- If data import fails, the details of the error can be viewed in the log.

Managing Eco-friendly Counter

When user authentication is being used, information on the eco-friendly counter is displayed at login.

The eco-friendly counter is the ratio of use of two-sided and multi-page printing to the total number of output pages.

How much toner and paper are being saved is indicated by the eco-friendly index.

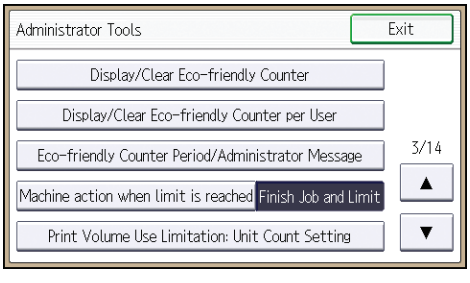
Note

- When Basic, Windows, LDAP or Integration Server authentication is used for user authentication, it collects and displays an eco-friendly counter for each user.
- When user code authentication is used for user authentication, or when user authentication is not in use, it collects and displays an overall eco-friendly counter for the machine.

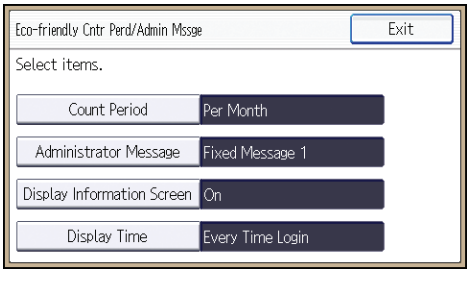
Configuring the Display of Eco-friendly Counters

Set up the period for collecting data for the eco-friendly counter and an administrator's message.

1. **The machine administrator logs in from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼] twice.**
5. **Press [Eco-friendly Counter Period/Administrator Message].**



6. **Press the setting item you want to change.**



7. **Change the settings.**
8. **Press [OK].**
9. **Press [Exit].**
10. **Log out.**

Eco-friendly counter settings

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 collected for the number of days specified.

Default: [**Do not Count**]

Administrator Message

Select a message type.

If you select "Fixed Message", a preset message is displayed.

If you select "User Message", the machine administrator can enter a free message to be displayed.

Default: [**Fixed Message**]

Display Information Screen

Set up whether or not to display the eco-friendly index with information at login.

Default: [**Off**]

Display Time

Set up the timing for displaying information.

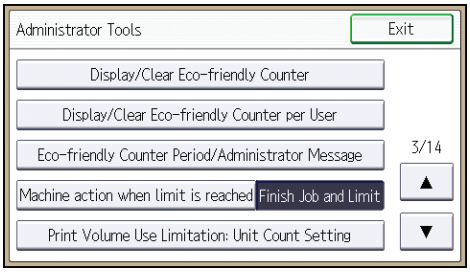
Default: [**Every Time Login**]

Clearing a Machine's Eco-friendly Counter

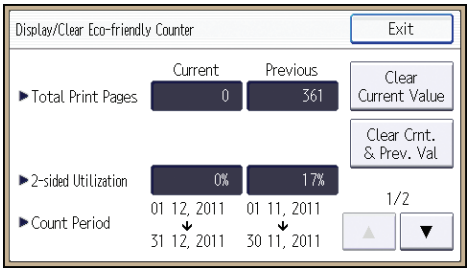
A machine's eco-friendly counter can be cleared.

1. **The machine administrator logs in from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼] twice.**

5. **Press [Display/Clear Eco-friendly Counter].**



6. **Press [Clear Current Value] or [Clear Crnt. & Prev. Val.].**

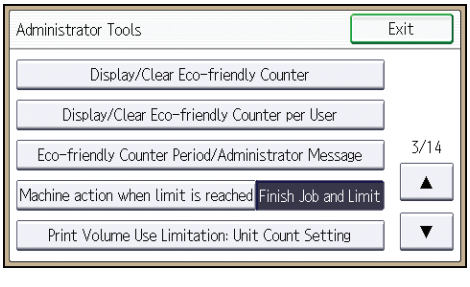


7. **Press [OK].**
8. **Press [Exit].**
9. **Log out.**

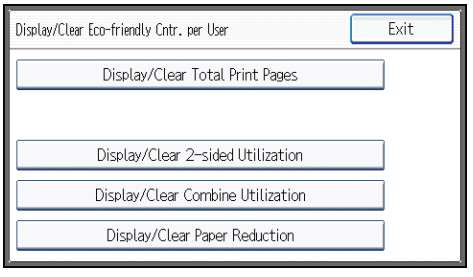
Clearing the Eco-friendly Counter by User

The eco-friendly counter can be cleared according to the user.

1. **The machine administrator logs in from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼] twice.**
5. **Press [Display/Clear Eco-friendly Counter per User].**



6. **Press the counter item to clear.**



7. **Press [Clear Current Value] or [Clear Crnt. & Prev. Val.].**
8. **Press [OK].**
9. **Press [Exit].**
10. **Log out.**

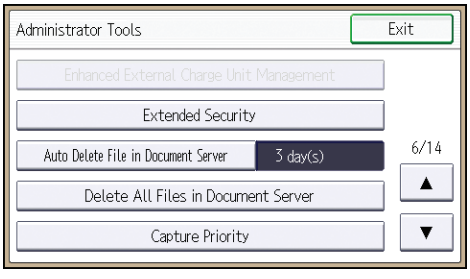
Note

- The eco-friendly counter for all users is cleared. The eco-friendly counter for individual users cannot be cleared.

Specifying the Extended Security Functions

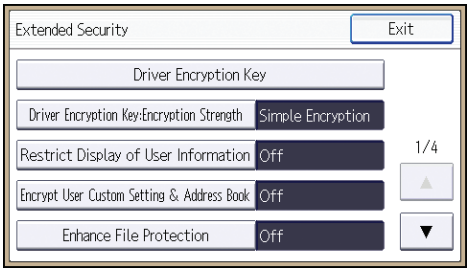
In addition to providing basic security through user authentication and administrator specified access limits on the machine, security can also be increased by encrypting transmitted data and data in the Address Book.

1. **Log in from the control panel as an administrator with privileges.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼] five times**
5. **Press [Extended Security].**



6. **Press the setting item you want to change.**

   If the setting you want to change is not displayed, press [▼] to move to another page.



7. **Change the settings.**
8. **Press [OK].**
9. **Press [Exit].**
10. **Log out.**

Note

- The operation privileges of an administrator differs depending on the setting.

Extended Security Function Settings

Driver Encryption Key

This can be specified by the network administrator.

When user authentication is ON, specify the string of text for the key used for encrypting the login passwords or document passwords that are sent from each kind of driver.

To specify the driver encryption key, register the encryption key specified using the machine in the driver.

For details, see p.176 "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 support 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, 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 p.93 "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.

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 p.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 [Program to Address Book]. If you set these functions to [On], the [Program to Address Book] 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 [Program to Address Book].

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.

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 the 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 "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 "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 [Facsimile Features], set "Switch 03, Bit 7" in [Parameter Setting] under [Initial Settings] to change the setting for automatically printing the Journal.
- In [Facsimile Features], set "Switch 21, Bit 4" in [Parameter Setting] under [Initial Settings] 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, click [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

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, [Mach.Addr.Info] is displayed in [Maintnc/MacInfo] 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.

Limiting Machine Operations to Customers Only

The machine can be set so that operation is impossible without administrator authentication.

The machine can be set to prohibit operation without administrator authentication and also prohibit remote registration in the Address Book by a service representative.

We maintain strict security when handling customers' data. Administrator authentication prevents us from operating the machine without administrator permission.

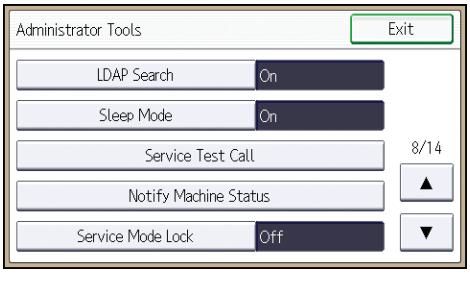
Settings

Service Mode Lock

This can be specified by the machine administrator. Service mode is used by a service representative 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 the service representative to operate the machine for inspection and repair. This ensures that the inspection and repair are done under the supervision of the machine administrator.

Specifying Service Mode Lock

1. **The machine administrator logs in from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼] seven times.**
5. **Press [Service Mode Lock].**



6. **Press [On], and then press [OK].**
7. **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 p.71 "Auto Logout".
Administrator Tools	User Authentication Management	Select [Basic Authentication], and then set "Printer Job Authentication" to [Entire]. See p.36 "Basic Authentication".
Administrator Tools	Administrator Authentication Management→User Management	Select [On], and then select [Administrator Tools] for the available settings. See p.15 "Configuring Administrator Authentication".
Administrator Tools	Administrator Authentication Management→Machine Management	Select [On], and then select each of the available settings. See p.15 "Configuring Administrator Authentication".
Administrator Tools	Administrator Authentication Management→Network Management	Select [On], and then select [Interface Settings], [File Transfer], and [Administrator Tools] for the available settings. See p.15 "Configuring Administrator Authentication".
Administrator Tools	Administrator Authentication Management→File Management	Select [On], and then select [Administrator Tools] for the available settings. See p.15 "Configuring Administrator Authentication".

Tab	Item	Setting
Administrator Tools	Extended Security→ Settings by SNMPv1, v2	Prohibit See p.259 "Specifying the Extended Security Functions".
Administrator Tools	Extended Security→Driver Encryption Key:Encryption Strength	AES See p.259 "Specifying the Extended Security Functions".
Administrator Tools	Extended Security→ Authenticate Current Job	Access Privilege See p.259 "Specifying the Extended Security Functions".
Administrator Tools	Extended Security→ Password Policy	"Complexity Setting": Level 1 or higher, "Minimum Character No.": 8 or higher See p.259 "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 p.122 "Specifying Network Security Level".
Administrator Tools	Service Mode Lock	On See p.269 "Limiting Machine Operations to Customers Only".
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).". If [Encrypt] is already selected, further encryption settings are not necessary. See p.98 "Encrypting Data on the Hard Disk".

Scanner Features

Tab	Item	Setting
Initial Settings	Menu Protect	Level 2 See p.78 "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 p.267 "Other Security Functions".
Initial Settings	Menu Protect	Level 2 See p.78 "Menu Protect".

Note

- The SNMP setting can be specified in [SNMP] under [Configuration] in Web Image Monitor.
- For details about the stored reception file user setting, see p.267 "Other Security Functions" or "Stored Reception File User Setting", Fax.

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 p.69 "User Lockout Function".
Security→User Lockout Policy	Number of Attempts before Lockout	5 times or less. For details, see p.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 p.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 p.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→ 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 p.138 "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 Manual Settings	Inactive
Security→IPsec	Encryption Key Auto Exchange Settings→ 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 p.132 "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 "Basic Procedure for Sending Scan Files by E-mail", Scan.

Note

- For details about enabling and disabling IPsec using the control panel, see "System Settings", Connecting the Machine/ System Settings.
- For details about specifying the IPsec setting via Web Image Monitor, see p.145 "Configuring IPsec".

8. Troubleshooting

This chapter describes what to do if the machine does not function properly.

If Authentication Fails

This section explains what to do if a user cannot operate the machine because of a problem related to user authentication. Refer to this section if a user comes to you with such a problem.

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.

Messages	Cause	Solutions
"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 default setting: • The administrator differs depending on the default 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.

Messages	Cause	Solutions
"Authentication has failed."	The entered login user name or login password is incorrect.	Ask the user administrator for the correct login user name and login password. See the error codes below for possible solutions: B, W, L, I 0104-000 B, W, L, I 0206-003 W, L, I 0406-003
"Authentication has failed."	Authentication failed because no more users can be registered. (The number of users registered in the Address Book has reached capacity.)	Delete unnecessary user addresses. See the error codes below for possible solutions: W, L, I 0612-005
"Authentication has failed."	Cannot access the authentication server when using Windows authentication, LDAP authentication, or Integration Server authentication.	A network or server error may have occurred. Confirm the network in use with the LAN administrator. If an error code appears, follow the instructions next to the error code in the table below.
"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 p.15 "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.

Messages	Cause	Solutions
"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 file creator (owner) or file administrator. To delete a file which you are not privileged to delete, contact the file creator (owner).

If an Error Code is Displayed

When authentication fails, the message "Authentication has failed." appears with an error code. The following lists explain the different methods for resolving each error code. If the error code that appears is not on this table, write down the error code and contact your service representative.

Error code display position

CJD017

1. **Error code**

   An error code appears.

Basic authentication

Error Code	Cause	Solution
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.	1. A password error occurred. Make sure the password is entered correctly. 2. Either [DES] or [AES] is selected for "Driver Encryption Key:Encryption Strength". The administrator has restricted use of simple encryption. You can use the encryption key if it has been specified in the driver. 3. A driver encryption key error occurred. Make sure that the encryption key is correctly specified on the driver.
B0105-000	A login user name was not specified but a DeskTopBinder operation was performed.	Specify the DeskTopBinder login user name correctly.
B0206-002	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	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.

Error Code	Cause	Solution
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	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

Error Code	Cause	Solution
W0103-000	A TWAIN operation occurred during authentication.	Make sure no other user is logged in to the machine, and then try again.
W0107-000	Failed to encrypt password.	1. A password error occurred. Make sure the password is entered correctly. 2. Either [DES] or [AES] is selected for "Driver Encryption Key:Encryption Strength". The administrator has restricted use of simple encryption. You can use the encryption key if it has been specified in the driver. 3. A driver encryption key error occurred. Make sure that the encryption key is correctly specified on the driver.
W0107-000	A login user name was not specified but a DeskTopBinder operation was performed.	Set the DeskTopBinder login user name correctly.
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.

Error Code	Cause	Solution
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.
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.
W0400-102	Kerberos authentication failed because the server or security module is not functioning correctly.	1. Make sure that the server is functioning properly. 2. Make sure that the security module is installed.
W0406-104	1. Cannot connect to the authentication server.	Make sure that connection to the authentication server is possible. Use the "Ping Command" to check the connection.
W0406-104	2. 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.
W0406-104	3. A domain name error occurred.	Make sure that the Windows authentication domain name is specified correctly.

Error Code	Cause	Solution
W0406-104	4. Cannot resolve the domain name.	Specify the IP address in the domain name and confirm that authentication is successful. If authentication was successful: 1. 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". 2. If a NetBIOS domain name is specified in domain name (such as DOMAINNAME), make sure that WINS is specified in "Interface Settings".
W0406-104	4. Cannot resolve the domain name.	Specify the IP address in the domain name and confirm that authentication is successful. If authentication was unsuccessful: 1. Make sure that Restrict LM/NTLM is not set in either "Domain Controller Security Policy" or "Domain Security Policy". 2. Make sure that the ports for the domain control firewall and the firewall on the machine to the domain control connection path are open.

Error Code	Cause	Solution
W0406-104	4. Cannot resolve the domain name.	Under Windows 7, if the Windows firewall is activated, create a firewall rule in the "Advanced settings" on the "System and security" control panel, and then 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".

Error Code	Cause	Solution
W0406-104	5. Kerberos authentication failed.	1. Kerberos authentication settings are not correctly configured. Make sure the realm name, KDC (Key Distribution Center) name and corresponding domain name are specified correctly. 2. 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. 3. Kerberos authentication will fail if the realm name is specified in lower-case letters. Make sure the realm name is specified in capital letters. 4. 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.
W0400-105	1. The UserPrincipleName (user@domainname.xxx.com) form is being used for the login user name.	The user group cannot be obtained if the UserPrincipleName (user@domainname.xxx.com) form is used. Use "sAMAccountName(user)" to log in, because this account allows you to obtain the user group.

Error Code	Cause	Solution
W0400-105	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.
W0400-106	The domain name cannot be resolved.	Make sure that DNS/WINS is specified in the domain name in "Interface Settings".
W0400-200	Due to the high number of authentication attempts, all resources are busy.	Wait a few minutes and then try again.
W0400-202	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	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 UserPrincipleName for the login name instead.

Error Code	Cause	Solution
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.
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.)	1. Delete the old, duplicated name or change the login name. 2. If the authentication server has just been changed, delete the old name on the server.
W0607-001	An authentication error occurred because the Address Book is being used at another location.	Wait a few minutes and then try again.
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.
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

Error Code	Cause	Solution
L0103-000	A TWAIN operation occurred during authentication.	Make sure no other user is logged in to the machine, and then try again.

Error Code	Cause	Solution
L0104-000	Failed to encrypt password.	1. A password error occurred. Make sure the password is entered correctly. 2. Either [DES] or [AES] is selected for "Driver Encryption Key:Encryption Strength". The administrator has restricted use of simple encryption. You can use the encryption key if it has been specified in the driver. 3. A driver encryption key error occurred. Make sure that the encryption key is correctly specified on the driver.
L0105-000	A login user name was not specified but a DeskTopBinder operation was performed.	Set the DeskTopBinder login user name correctly.
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.
L0306-018	The LDAP server is not correctly configured.	Make sure that a connection test is successful with the current LDAP server configuration.

Error Code	Cause	Solution
L0307-001	An authentication error occurred because the Address Book is being used at another location.	Wait a few minutes and then try 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	1. There is an error in the LDAP authentication settings, LDAP server, or network configuration.	1. 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". 2. Make sure the LDAP server is specified correctly in the LDAP authentication settings. 3. Make sure the login name attribute is entered correctly in the LDAP authentication settings. 4. Make sure the SSL settings are supported by the LDAP server.

Error Code	Cause	Solution
L0406-202 L0406-203	2. A login user name or password error occurred.	1. Make sure the login user name and password are entered correctly. 2. 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	3. There is an error in the simple encryption method.	1. Authentication will fail if the password is left blank in simple authentication mode. To allow blank passwords, contact your service representative. 2. 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.

Error Code	Cause	Solution
L0406-204	Kerberos authentication failed.	1. Kerberos authentication settings are not correctly configured. Make sure the realm name, KDC (Key Distribution Center) name, and supporting domain name are specified correctly. 2. 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. 3. Kerberos authentication will fail if the realm name is specified in lower-case letters. Make sure the realm name is specified in capital letters.
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.
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.

Error Code	Cause	Solution
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.)	1. Delete the old, duplicated name or change the login name. 2. If the authentication server has just been changed, delete the old name on the server.
L0607-001	An authentication error occurred because the Address Book is being used at another location.	Wait a few minutes and then try again.
L606-004	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.
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

Error Code	Cause	Solution
I0103-000	A TWAIN operation occurred during authentication.	Make sure no other user is logged in to the machine, and then try again.

Error Code	Cause	Solution
I0104-000	Failed to decrypt password.	1. A password error occurred. Make sure the password is entered correctly. 2. Either [DES] or [AES] is selected for "Driver Encryption Key:Encryption Strength". The administrator has restricted use of simple encryption. You can use the encryption key if it has been specified in the driver. 3. A driver encryption key error occurred. Make sure that the encryption key is correctly specified on the driver.
I0105-000	A login user name was not specified but a DeskTopBinder operation was performed.	Set the DeskTopBinder login user name correctly.
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.

Error Code	Cause	Solution
I0406-003	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 account name was entered incorrectly, enter it correctly and log in again.
I0406-301	1. The URL could not be obtained.	Obtain the URL using Obtain URL in Integration Server authentication.
I0406-301	2. A login user name or password error occurred.	1. Make sure the login user name and password are entered correctly. 2. 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, colon (:), 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.)	1. Delete the old, duplicated name or change the login name. 2. If the authentication server has just been changed, delete the old name on the server.
I0607-001	An authentication error occurred because the Address Book is being used at another location.	Wait a few minutes and then try again.

Error Code	Cause	Solution
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.
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: • 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: • 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 p.176 "Specifying a Driver Encryption Key".

Condition	Cause	Solution
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.
After starting "User Management Tool" or "Address Management Tool" in SmartDeviceMonitor for Admin and entering the correct login user name and password, a message that an incorrect password has been entered appears.	"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.	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. For details, see p.259 "Specifying the Extended Security Functions" and p.132 "Configuring SSL/TLS".
Cannot log in to the machine using [Document Server (MFP): Authentication/Encryption] in DeskTopBinder.	"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.	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. For details, see p.259 "Specifying the Extended Security Functions" and p.132 "Configuring SSL/TLS".

Condition	Cause	Solution
Cannot access the machine using ScanRouter EX Professional V3 / ScanRouter EX Enterprise V2.	"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.	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. For details, see p.259 "Specifying the Extended Security Functions" and p.132 "Configuring SSL/TLS".
Cannot connect to the ScanRouter delivery software.	The ScanRouter delivery software may not be supported by the machine.	Update to the latest version of the ScanRouter delivery software.
Cannot access the machine using ScanRouter EX Professional V2.	ScanRouter EX Professional V2 does not support user authentication.	ScanRouter EX Professional V2 does not support user authentication.
Cannot log out when using the copying or scanner functions.	The original has not been scanned completely.	When the original has been scanned completely, press [#], remove the original, and then log out.
"Program to Address Book" does not appear on the fax or scanner screen for specifying destinations.	"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.	Registration must be done by the user administrator.

Condition	Cause	Solution
Cannot send e-mail from the scanner. Similarly: • Cannot select an address. • Cannot specify a signature. • Cannot store data in a media.	The following are possible causes: • 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.	• 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 p.127 "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
Cannot transfer faxed documents. Similarly: • Cannot select an address. • Cannot specify a signature.	The following are possible causes: • 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.	• 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 p.127 "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.
User authentication is disabled, yet stored files do not appear.	User authentication might have been disabled without "All Users" being selected for user access to stored files.	Re-enable user authentication, and select [All Users] as the access permission setting of the files you want to display. For details, see p.181 "Configuring Access Permissions for Stored Files".

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 p.93 "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 about clearing print volume counters, ask the user administrator.
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 consult an administrator or the user who executed the job.
After you execute "Encpt User Cstm Setg & Add Bk", the "Exit" message does not appear.	The hard disk may be faulty. The file may be corrupt.	Contact your service representative.

9. Checking Operation Privileges

This chapter specifies a list of the administrator and user operation privileges for the machine settings when administrator authentication or user authentication is enabled.

List of Operation Privileges for Settings

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 the available settings of [Administrator Authentication Management].

- Set

  The logged in user has privileges for this operation.

  Status when settings are selected in the 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.

Note

- When user authentication is active, users who have not been authenticated or do not have login data cannot operate the machine.

- When [Menu Protect] is set to [Off], users can execute, change and read all of the settings of each function.

System Settings

When administrator authentication is set, the restrictions to user operations differ depending on the configurations of the available settings in [Administrator Authentication Management].

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	R	R/W	R	R	R/W	R
Screen Colour 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
Key Repeat	R	R/W	R	R	R/W	R
Measurement Unit	R	R/W	R	R	R/W	R
Check 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

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 1-3	R	R/W	R	R	R/W	R

Settings	User	Mach	N/W	File	Unset	Set
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 1-3	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
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
Weekly Timer Code	R	R/W	R	R	R/W	R
Weekly Timer	R	R/W	R	R	R/W	R

Interface Settings

Network

Settings	User	Mach	N/W	File	Unset	Set
Machine IPv4 Address*1	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

Settings	User	Mach	N/W	File	Unset	Set
DHCPv6 Configuration	R	R	R/W	R	R/W	R
DNS Configuration*2	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*1	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
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	–

*1 When auto-obtain is set, the data is read-only.

*2 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 Signal	R	R	R/W	R	R/W	R
Restore Factory Defaults	–	–	R/W	–	R/W	–

File Transfer

Settings	User	Mach	N/W	File	Unset	Set
Delivery Option*3	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*4	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

Settings	User	Mach	N/W	File	Unset	Set
POP3/IMAP4 Settings	R	R/W	R	R	R/W	R
Administrator's Email Address	R	R/W	R	R	R/W	R
Email Communication Port	R	R	R/W	R	R/W	R
Email Reception Interval	R	R	R/W	R	R/W	R
Max. Reception Email Size	R	R	R/W	R	R/W	R
Email Storage in Server	R	R	R/W	R	R/W	R
Default User Name/Password (Send)*4	R	R/W	R	R	R/W	R
Program/Change/Delete Email Message	R	R/W	R	R	R/W	R/W
Auto Specify Sender Name	R	R	R/W	R	R/W	R
Fax Email 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

*3 The primary and secondary distribution server addresses are read-only.

*4 Passwords cannot be read.

Administrator Tools

Settings	User	Mach	N/W	File	Unset	Set
Address Book Management	R/W	R/W *5	R/W *5	R/W *5	R/W *6	R*6
Address Book: Program/Change/Delete Group	R/W	R/W *5	R/W *5	R/W *5	R/W *6	R*6
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	–

Settings	User	Mach	N/W	File	Unset	Set
Data Carry-over Setting for Address Book Auto-program	R/W	R	R	R	R/W	R
Display/Print Counter	R	R/W	R	R	R/W	R/W
Display/Clear/Print Counter per User	R/W *7	R/W *8	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
Print Volum. Use Limit.: Default Limit Value	R/W	R	R	R	R	R
Volm Use Cntr:Scheduld/Specfid Rst Stng	R	R/W	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 *9*10	R/W *10	R/W *10	R/W *10	R/W	–
Program/Change Administrator	R/W *11	R/W *11	R/W *11	R/W *11	–	–
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
Driver Encryption Key*12	–	–	R/W	–	R/W	–
Driver Encryption Key:Encryption Strength*12	R	R	R/W	R	R/W	R
Restrict Display of User Information*12	R	R/W	R	R	R/W	R

Settings	User	Mach	N/W	File	Unset	Set
Encrypt User Cstm. Setg. & Addrs. Book*12	R/W	R	R	R	R	R
Enhance File Protection*12	R	R	R	R/W	R	R
Restrict Use of Destinations (Fax)*12	R/W	R	R	R	R	R
Restrict Adding of User Destinations (Fax)*12	R/W	R	R	R	R	R
Restrict Use of Destinations (Scanner)*12	R/W	R	R	R	R	R
Restrict Adding of User Destin.(Scanner)*12	R/W	R	R	R	R	R
Transfer to Fax Receiver*12	R	R/W	R	R	R	R
Remote Diagnostics (Facsimile)	–	–	–	–	R/W	–
Authenticate Current Job*12	R	R/W	R	R	R/W	R
@Remote Service*12	R	R/W	R	R	R/W	R
Update Firmware*12	R	R/W	R	R	–	–
Change Firmware Structure*12	R	R/W	R	R	–	–
Password Policy*12	R/W	–	–	–	–	–
Settings by SNMPv1, v2*12	R	R	R/W	R	R/W	R
Security Setting for Access Violation*12	R	R/W	R	R	–	–
Password Entry Violation*12	–	R/W	–	–	–	–
Device Access Violation*12	–	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*4	–	R/W	–	–	R/W	R

Settings	User	Mach	N/W	File	Unset	Set
LDAP Search	R	R/W	R	R	R/W	R
Sleep Mode	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
Erase All Memory	–	R/W	–	–	–	–
Delete All Logs	–	R/W	–	–	R/W	–
Transfer Log Setting*13	R	R/W	R	R	R/W	R
Data Security for Copying	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	–	–	–	–
Machine Data Encryption Settings	–	R/W	–	–	–	–
Program/Delete Device Certificate	R	R	R/W	R	–	–
Device Setting Information: Import Setting (Server)*14	–	–	–	–	–	–
Device Setting Information: Run Import (Server)*14	–	–	–	–	–	–
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	R
Stop Key to Suspend Print Job	R	R/W	R	R	R/W	R

Settings	User	Mach	N/W	File	Unset	Set
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
Users Own Home Screen	R	R/W	R	R	R/W	R

*4 Passwords cannot be read.

*5 Only changing headings and user searches are possible.

*6 The items that can be executed, changed and read differ according is set to access privilege.

*7 Can only be cleared.

*8 Can only be printed.

*9 Cannot be changed when using the individual authentication function.

*10 Only the administrator privilege settings can be changed.

*11 Administrators can only change their own accounts.

*12 [Extended Security] settings.

*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.

Print List

Settings	User	Mach	N/W	File	Unset	Set
Print List	–	–	R/W	–	R/W	–

Edit Home

When administrator authentication is set, the restrictions to user operations differ depending on the configurations of the available settings in [Administrator Authentication Management].

Edit Home

Settings	User	Mach	N/W	File	Unset	Set
Edit Icons	–	R/W	–	–	R/W	–
Insert Image	–	R/W	–	–	R/W	–

Maintenance

When administrator authentication is set, the restrictions to user operations differ depending on the configurations of the available settings in [Administrator Authentication Management].

Maintenance

Settings	User	Mach	N/W	File	Unset	Set
Plain Paper Setting	–	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
Orig.'s Photo Type Prio. (Txt./Photo)	R	R/W	R	R	R	R
Original's Photo Type Priority (Photo)	R	R/W	R	R	R	R
Original's Type Display	R	R/W	R	R	R	R
Paper Display (Stored File Print)	R	R/W	R	R	R	R
Original's 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: Orig. left on Exp. 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

Reproduction Ratio

Settings	User	Mach	N/W	File	Lv.1	Lv.2
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
Combine: Type of Separation Line	R	R/W	R	R	R/W	R
Copy Order in Combine	R	R/W	R	R	R/W	R

Input/Output

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

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	–
Delete Box	–	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
Delete Box	–	R/W	–	–	R	–

Send Settings

Settings	User	Mach	N/W	File	Lv.1	Lv.2
Max. Email Size	R	R	R/W	R	R	R
Program/Change Standard Message	R	R/W	R	R	R	R
Delete Standard Message	R	R/W	R	R	R	R

Settings	User	Mach	N/W	File	Lv.1	Lv.2
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
Centre 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

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	–

Settings	User	Mach	N/W	File	Lv.1	Lv.2
Internet Fax Setting	R	R/W	R	R	R	R
Select Dial/Push Phone	R	R/W	R	R	R	R
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 Gateway	R	R	R/W	R	R	R
Delete Gateway	R	R	R/W	R	R	R
Menu Protect	R	R/W	R	R	R	R
Email 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 Email 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	– *1	R	– *1	– *1	R	R
Print Jobs	–	–	–	R/W	R/W	R/W
Prt. From Dev.	–	–	–	–	R/W	R/W
Job Reset	–	R/W	–	–	R/W	R/W
Job Operation	R	R/W	R	R	R/W	R/W
Form Feed	–	R/W	–	–	R/W	R/W
Spooling Job List	–	R/W	–	–	R/W	R/W
Error Log	–	R/W	–	–	R/W	R/W

*1 Can be viewed if [Authenticate Current Job] is set to [Off] in [Extended Security].

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
Menu List	–	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

Maintenance

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	–
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

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
Rotate by 180 Degrees	R	R/W	R	R	R	R
Print Compressed Data	R	R/W	R/W	R	R	R
Memory Usage	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
Edge Smoothing	R	R/W	R	R	R	R
Toner Saving	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
Switching btwn. 1&2 Sided Print	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
Orientation Auto Detect	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
Orientation Auto Detect	R	R/W	R	R	R	R

Unauthorized Copy Preventn.

Settings	User	Mach	N/W	File	Lv.1	Lv.2
Unauthorized Copy Prevention Stg.	R	R/W	R	R	R	R
Setting Priority (Drvr/Cmnd/Mach)	R	R/W	R	R	R	R
Unauthorized Copy Prevention Type	R	R/W	R	R	R	R
Mask Type for Patrn./Density/Effect	R	R/W	R	R	R	R
Prevention Text Settings	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 Set.	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/W	–	–	–	–
Delete Scanner Journal	–	R/W	–	–	–	–
Delete Recent Destinations	–	R/W	–	–	–	–

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
Background Density of ADS (Full Colour)	R	R/W	R	R	R	R
Blank Page Detect	R	R/W	R	R	R	R
Reproduction Ratio	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 (Grey Scale/Full Colour)	R	R/W	R	R	R/W	R
Compression Method for High Compress. PDF	R	R/W	R	R	R/W	R
High Compression PDF Level	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

Browser Features

Settings	User	Mach	N/W	File	Unset	Set
Browser Default Settings	–	R/W	–	–	R	R
Settings per Users	–	R/W	–	–	R	R
View Logs	–	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	R	R	R	R

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
Device Total Counter	–	R	–	–	–	–
Counter per User	–	R	–	–	R	R
Download	–	R/W	–	–	–	–

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 if user code authentication is used for the user authentication method.

Printer

Settings	User	Mach	N/W	File	Unset	Set
Spool Printing: Delete	–	R/W	–	–	–	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 of the available settings in [Administrator Authentication Management].

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
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	–	–
Function Reset Timer	R	R/W	R	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
Paper Tray Priority	R	R/W	R	R	R/W	R

Function Key Allocation/Function Priority

Settings	User	Mach	N/W	File	Unset	Set
Function Key Allocation	R	R/W	R	R	R/W	R
Function Priority	R	R/W	R	R	R/W	R

Paper

Settings	User	Mach	N/W	File	Unset	Set
Tray 1-3	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
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
Weekly Timer Code	R	R/W	R	R	R/W	R
Weekly Timer: Monday-Sunday	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*1	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	–

*1 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
SMTP Authentication	–	R/W	–	–	R/W	R

Settings	User	Mach	N/W	File	Unset	Set
SMTP Auth. Email Address	–	R/W	–	–	R/W	R
SMTP Auth. User Name	–	R/W	–	–	R/W	–
SMTP Auth. Password*2	–	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*2	–	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
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*2	–	R/W	–	–	R/W	–

*2 Passwords cannot be read.

Auto Email Notification

Settings	User	Mach	N/W	File	Unset	Set
Notification Message	R	R/W	R	R	R	R
Groups to Notify	R	R/W	R	R	R	R
Select Groups/Items to Notify	R	R/W	R	R	R	R
Detailed Settings of Each Item	R	R/W	R	R	R	R

On-demand Email Notification

Settings	User	Mach	N/W	File	Unset	Set
Notification Subject	R	R/W	R	R	R	R
Notification Message	R	R/W	R	R	R	R
Access Restriction to Information	R	R/W	R	R	R	R
Receivable Email Address/Domain Name Settings	R	R/W	R	R	R	R

File Transfer

Settings	User	Mach	N/W	File	Unset	Set
SMB User Name	–	R/W	–	–	R/W	–
SMB Password*2	–	R/W	–	–	R/W	–
FTP User Name	–	R/W	–	–	R/W	–
FTP Password*2	–	R/W	–	–	R/W	–
NCP User Name	–	R/W	–	–	R/W	–
NCP Password*2	–	R/W	–	–	R/W	–

*2 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

Settings	User	Mach	N/W	File	Unset	Set
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
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	–	–

Settings	User	Mach	N/W	File	Unset	Set
File Administrator	R	R	R	R/W	–	–
Login User Name*1	R/W	R/W	R/W	R/W	–	–
Login Password*1	R/W	R/W	R/W	R/W	–	–
Encryption Password*1	R/W	R/W	R/W	R/W	–	–

*1 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	–
Program	–	R/W	–	–	R/W	–
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	–	–	–	–

Device Setting Information: Import Setting (Server)

Settings	User	Mach	N/W	File	Unset	Set
Import File From*1	–	–	–	–	–	–
Scheduled Import at Specified Time*1	–	–	–	–	–	–
Comparing New File to Last Import File*1	–	–	–	–	–	–
Email Failure Notification*1	–	–	–	–	–	–
Number of Retries*1	–	–	–	–	–	–
Retry Interval*1	–	–	–	–	–	–
Encryption Key*1	–	–	–	–	–	–

*1 R/W is the administrator with all privileges that include user administrator, machine administrator, network administrator, and file administrator privileges.

Import Test

Settings	User	Mach	N/W	File	Unset	Set
Start*1	–	–	–	–	–	–

*1 R/W is the administrator with all privileges that include user administrator, machine administrator, network administrator, and file administrator privileges.

Import/Export Device Setting Information

Settings	User	Mach	N/W	File	Unset	Set
Export Device Setting Information*1	–	–	–	–	–	–
Import Device Setting Information*1	–	–	–	–	–	–
Export Image File for Home Screen*1	–	–	–	–	–	–

*1 R/W is the administrator with all privileges that include user administrator, machine administrator, network administrator, and file administrator privileges.

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
Administrator Message	R	R/W	R	R	R/W	R

Compulsory Security Stamp

Settings	User	Mach	N/W	File	Unset	Set
Compulsory Security Stamp	R	R/W	R	R	R	R
Adjust Stamp Position	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 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
Memory Usage	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
Edge Smoothing	R	R/W	R	R	R	R
Toner Saving	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
Tray Setting Priority	R	R/W	R	R	R	R

Settings	User	Mach	N/W	File	Lv.1	Lv.2
Paper Confirmation for Bypass Tray	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

Unauthorized Copy Prevention

Settings	User	Mach	N/W	File	Lv.1	Lv.2
Unauthorized Copy Prevention Setting	R	R/W	R	R	R	R
Setting Priority (Driver/Command/Machine)	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

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	–	–	–	–

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
Rotate by 180 Degrees	R	R/W	R	R	R	R
Memory Usage	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
Edge Smoothing	R	R/W	R	R	R	R
Toner Saving	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
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
PDF Menu	R	R/W	R	R	R	R
RHPP Settings	R	R/W	R	R	R/W	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	–	–	–	–

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
High Compression PDF Level	R	R/W	R	R	R/W	R

Settings	User	Mach	N/W	File	Lv.1	Lv.2
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	–
Display WSD Destination List	R	R/W	R	R	R	R
Prohibit WSD Scan Command	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

Settings	User	Mach	N/W	File	Lv.1	Lv.2
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 of the available settings in [Administrator Authentication Management].

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

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	–
Security Method	R	R	R/W	R	R/W	R

Settings	User	Mach	N/W	File	Unset	Set
WEP Authentication	–	–	R/W	–	R/W	–
WEP Key Number	R	R	R/W	R	R/W	R
WEP Key	R	R	R/W	R	R/W	R
WPA Authentication Method	R	R	R/W	R	R/W	R
WPA-PSK/WPA2-PSK	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 of the available settings in [Administrator Authentication Management].

IPv4

Settings	User	Mach	N/W	File	Unset	Set
IPv4	R	R	R	R	R	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

IPv6

Settings	User	Mach	N/W	File	Unset	Set
IPv6	R	R	R/W	R	R/W	R
Host Name	R	R	R/W	R	R/W	R
Domain Name	R	R	R/W	R	R/W	R
Link-local Address	R	R	R	R	R	R

Settings	User	Mach	N/W	File	Unset	Set
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

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 of the available settings in [Administrator Authentication Management].

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 of the available settings in [Administrator Authentication Management].

Settings	User	Mach	N/W	File	Unset	Set
Reset the Machine	–	R/W	–	–	R/W	–

Web Image Monitor: Device Home Management

These settings are in [Device Management].

When administrator authentication is set, the restrictions to user operations differ depending on the configurations of the available settings in [Administrator Authentication Management].

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: Customize Screen per User

Users can change only their own settings.

Settings	User	Mach	N/W	File	Unset	Set
Edit Icons	–	–	–	–	–	R/W
Restore Default Icon Display	–	–	–	–	–	R/W
Function Priority per User	–	–	–	–	–	R/W

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 p.367 "List of Operation Privileges for Stored Files".

Settings	User	Mach	N/W	File	Unset	Set
Print	–	–	–	–	R/W	R/W
Send	–	–	–	–	R/W	R/W
Delete	–	–	–	R/W	R/W	R/W
Edit detailed information (Detailed information icon)	–	–	–	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 (Detailed information icon)	–	–	–	–	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 (Detailed information icon)	–	–	–	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 Privilege: Owner	–	–	–	–	–	R/W
Change Access Privilege: Permissions for Users/Groups	–	–	–	R/W	R/W*1	R/W
Change User Name	–	–	–	–	–	R/W
Change File Name	–	R/W	R/W	R/W	R/W*1	–
Change Password	–	–	–	–	R/W	R/W
Unlock Files	–	–	–	–	–	R/W
Combine Files	–	–	R/W	R/W	R/W*1	–

Settings	Read	Edit	E/D	Full	Owner	File
Insert File	–	–	R/W	R/W	R/W*1	–
Delete Pages	–	–	R/W	R/W	R/W*1	–
Print specified page	R/W	R/W	R/W	R/W	R/W	–
Duplicate File	R/W	R/W	R/W	R/W	R/W	–
Delete File	–	–	R/W	R/W	R/W*1	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
Registration No.	R	R/W	R/W	R/W	R/W	R/W
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
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
Login User Name	–	–	–	–	R	R/W

Settings	Read	Edit	E/D	Full	Entry	User
Login Password	–	–	–	–	R/W *1	R/W *1
SMTP Authentication	–	–	–	–	R/W *1	R/W *1
Folder Authentication	–	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
Protection Code	–	–	–	R/W *2	R/W *2	R/W *2
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.

Add to Group

Settings	Read	Edit	E/D	Full	Entry	User
Registration No.	R	R/W	R/W	R/W	R/W	R/W
Search	–	R/W	R/W	R/W	R/W	R/W
Switch Title	R/W	R/W	R/W	R/W	R/W	R/W

Fax Dest.

Settings	Read	Edit	E/D	Full	Entry	User
Fax Destination	R	R/W	R/W	R/W	R/W	R/W
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

Email

Settings	Read	Edit	E/D	Full	Entry	User
Email Address	R	R/W	R/W	R/W	R/W	R/W
Use Email 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/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 may 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.

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 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

INDEX

EN GB EN US EN AU D127-7519

User Information on Electrical & Electronic Equipment

Users in the countries where this symbol shown in this section has been specified in national law on collection and treatment of E-waste

Our Products contain high quality components and are designed to facilitate recycling.

Our products or product packaging are marked with the symbol below.

The symbol indicates that the product must not be treated as municipal waste. It must be disposed of separately via the appropriate return and collection systems available. By following these instructions you ensure that this product is treated correctly and help to reduce potential impacts on the environment and human health, which could otherwise result from inappropriate handling. Recycling of products helps to conserve natural resources and protect the environment.

For more detailed information on collection and recycling systems for this product, please contact the shop where you purchased it, your local dealer or sales/service representatives.

All Other Users

If you wish to discard this product, please contact your local authorities, the shop where you bought this product, your local dealer or sales/service representatives.

For Users in India

This product complies with the “India E-waste Rule 2011” and prohibits use of lead, mercury, hexavalent chromium, polybrominated biphenyls or polybrominated diphenyl ethers in concentrations exceeding 0.1 weight % and 0.01 weight % for cadmium, except for the exemptions set in Schedule 2 of the Rule.

Printed in Japan
EN (AU)
D127-6602

D1276602