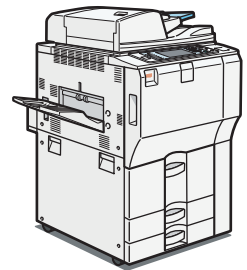




9060/9070/9080/9090
MP 6001/MP 7001/MP 8001/MP 9001
LD360/LD370/LD380/LD390
Aficio™ MP 6001/7001/8001/9001

Operating Instructions Scanner Reference



-
- 1** Sending Scan Files by E-mail
 - 2** Sending Scan Files to Folders
 - 3** Sending Scan Files Using WSD
 - 4** Storing Files Using the Scanner Function
 - 5** Saving Scan Files on a Removable Memory Device
 - 6** Delivering Scan Files
 - 7** Scanning Originals with the Network TWAIN Scanner
 - 8** Various Scan Settings
 - 9** Scanner Features
 - 10** Appendix

TABLE OF CONTENTS

- Manuals for This Machine.....6
- Notice.....8
 - Important.....8
- How to Read This Manual.....9
 - Symbols.....9
 - Notes.....9
- Laws and Regulations.....10
 - Legal Prohibition.....10
- About the Scanner Functions.....11
- Display Panel.....13
 - Simplified Display.....13
 - Confirmation Displays.....14
- 1. Sending Scan Files by E-mail**

- Before Sending Scan Files by E-mail.....19
 - Overview of Sending Scan Files by E-mail.....19
 - Preparation for Sending by E-mail.....20
 - Registering E-mail Addresses in the Address Book.....22
 - E-mail Screen.....23
- Basic Procedure for Sending Scan Files by E-mail.....25
- Switching to the E-mail Screen.....28
- Specifying E-mail Destinations.....29
 - Selecting the Destination from the Machine's Address Book.....29
 - Entering an E-mail Address Manually.....32
 - Selecting Destinations by Searching an LDAP Server.....33
 - Registering a Directly-Entered Destination in the Address Book.....36
- Specifying the E-mail Sender.....38
 - Selecting a Sender from the List.....38
 - Using a Registration Number to Specify a Sender Name.....39
 - Selecting the Sender by Searching the Machine's Address Book.....39
- Entering the E-mail Subject.....42
- Entering the E-mail Message.....43
 - Selecting a Message from the List.....43
 - Manual Entry of a Message.....44

Simultaneous Storage and Sending by E-mail.....	45
Security Settings to E-mails.....	46
Sending Encrypted E-mail.....	46
Sending E-mail with a Signature.....	47
Sending the URL by E-mail.....	48

2. Sending Scan Files to Folders

Before Sending Files by Scan to Folder.....	51
Overview of Sending Scan Files by Scan to Folder.....	51
Preparation for Sending by Scan to Folder.....	53
Registering Destination Folders in the Address Book.....	55
Scan to Folder Screen.....	56
Basic Procedure When Using Scan to Folder.....	58
Switching to the Scan to Folder Screen.....	60
Specifying Scan to Folder Destinations.....	61
Selecting the Destination from the Machine's Address Book.....	61
Sending Files to a Shared Network Folder.....	64
Sending Files to an FTP Server.....	68
Sending Files to NetWare Server.....	69
Registering the Path to the Selected Destination in the Address Book.....	73
Simultaneous Storage and Sending by Scan to Folder.....	74

3. Sending Scan Files Using WSD

Before Sending Scan Files Using WSD.....	75
Overview of Sending Scan Files Using WSD.....	75
Preparation for Sending Files Using WSD.....	76
WSD Scanner Screen.....	79
Basic Procedure for Sending Scan Files Using WSD.....	80
Switching to the WSD Scanner Screen.....	82
Specifying the Destination Client Computer.....	83
Selecting a Destination Client Computer from the Destination List.....	83
Searching for a Destination Client Computer.....	84
Changing a Scan Profile.....	86
Creating a New Scan Profile.....	87

4. Storing Files Using the Scanner Function

Before Storing Files.....	89
Overview of File Storage under the Scanner Function.....	89
Basic Procedure for Storing Scan Files.....	91
Specifying File Information for a Stored File.....	93
Specifying a User Name.....	93
Specifying a File Name.....	93
Specifying a Password.....	94
Displaying the List of Stored Files.....	96
List of Stored Files.....	96
Searching the List of Stored Files.....	97
Checking Stored Files.....	99
Checking a Stored File Selected from the List.....	99
Checking Stored Files from a Client Computer.....	100
Sending a Stored File.....	102
Sending Stored Files.....	102
Managing Stored Files.....	104
Deleting a Stored File.....	104
Changing Information for a Stored File.....	105

5. Saving Scan Files on a Removable Memory Device

Before Saving Files on a Removable Memory Device.....	109
Overview of Saving Files on a Removable Memory Device.....	109
Basic Procedure for Saving Scan Files on a Removable Memory Device.....	111

6. Delivering Scan Files

Before Delivering Files.....	113
Overview of Scan File Delivery.....	113
Preparing to Deliver Files.....	114
Installing DeskTopBinder Lite from the Supplied CD-ROM.....	117
Network Delivery Scanner Screen.....	117
Basic Procedure for Delivering Files.....	119
Switching to the Network Delivery Scanner Screen.....	122
Specifying Delivery Destinations.....	123
Selecting Destinations Registered in the Delivery Server's Address Book.....	123

Specifying the Sender.....	127
Selecting a Sender from the Sender List.....	127
Selecting the Sender by Entering the Registration Number.....	127
Selecting a Sender by Searching the Delivery Server's Destination List.....	128
Entering the Subject of the E-mail to Be Transmitted via the Delivery Server.....	131
Simultaneous Storage and Delivery.....	132

7. Scanning Originals with the Network TWAIN Scanner

Before Using the Network TWAIN Scanner.....	133
Overview of the Network TWAIN Scanner.....	133
Preparing to Use the Network TWAIN Scanner.....	134
Installing the TWAIN Driver from the Supplied CD-ROM.....	136
Basic Network TWAIN Scanner Procedure.....	138
Scan Settings When Using TWAIN Scanner.....	140
Setting Original Orientation on the TWAIN Scanner.....	140
When Scanning Originals of Mixed Sizes Using TWAIN Scanner.....	142

8. Various Scan Settings

Specifying Scan Settings.....	143
Scan Settings.....	144
Scan Type.....	144
Resolution.....	145
Scan Size.....	145
Edit.....	150
Adjusting Image Density.....	151
Setting of Original Feed Type.....	152
Original Orientation.....	152
Original Settings.....	154
Batch, SADF.....	155
Divide.....	156
Scanning Multiple Pages of Originals as One File.....	158
Specifying the File Type and File Name.....	160
Specifying the File Type.....	160
Notes About and Limitations of File Types.....	161
Specifying the File Name.....	162

Security Settings for PDF Files.....	164
Programs.....	169
Registering Frequently Used Settings.....	169
Recalling a Registered Content.....	170
Changing a Registered Program.....	170
Deleting a Program.....	171
Changing the Registered Program Name.....	171
Changing the Default Functions of the Scanner's Initial Display.....	173

9. Scanner Features

Accessing User Tools.....	175
Changing User Tools.....	175
Closing User Tools.....	176
General Settings.....	177
Scan Settings.....	179
Send Settings.....	181
Initial Settings.....	184

10. Appendix

Relationship between Resolution and Scan Size.....	185
When Using the E-mail, Folder Sending, WSD Scanner, Storing, or Network Delivery Functions.....	185
When Using as a TWAIN Scanner.....	186
Software Supplied on CD-ROM.....	188
Auto-Run Program.....	188
TWAIN Driver.....	188
DeskTopBinder Lite.....	189
Values of Various Set Items for Transmission/Storage/Delivery Function.....	191
Transmission Function.....	191
Storage Function.....	193
Network Delivery Function.....	194
About WIA Scanning.....	196
Specifications.....	199
Trademarks.....	202
INDEX	205

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.
- The printed and electronic versions of a manual have the same contents.
- 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.

About This Machine

Before using the machine, be sure to read the section of this manual entitled Safety Information.

This manual introduces the machine's various functions. It also explains the control panel, preparation procedures for using the machine, how to enter text, how to install the CD-ROMs provided, and how to replace paper, toner, staples, and other consumables.

Troubleshooting

Provides a guide for resolving common usage-related problems.

Copy and Document Server Reference

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

Facsimile Reference

Explains Facsimile functions and operations.

Printer Reference

Explains Printer functions and operations.

Scanner Reference

Explains Scanner functions and operations.

Network and System Settings Guide

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

Security Reference

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 "Setting Up the Machine", Security Reference.

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

PostScript 3 Supplement

Explains how to set up and use PostScript 3.

Other manuals

- UNIX Supplement
- Quick Reference Copy Guide
- Quick Reference Printer Guide
- Quick Reference Fax Guide
- Quick Reference Scanner Guide
- Manuals for DeskTopBinder Lite
 - DeskTopBinder Lite Setup Guide
 - DeskTopBinder Introduction Guide
 - Auto Document Link Guide

↓ Note

- Manuals provided are specific to machine types.
- 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.
- The following software products are referred to using general names:

Product name	General name
DeskTopBinder Lite and DeskTopBinder Professional *1	DeskTopBinder
ScanRouter EX Professional *1 and ScanRouter EX Enterprise *1	The ScanRouter delivery software

*1 Optional

Notice

Important

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.

For good copy quality, the supplier recommends that you use genuine toner from the supplier.

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

How to Read This Manual

Symbols

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 that appear on the machine's display panel.

[]

Indicates the names of keys on the machine's control panel.

Notes

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

Two kinds of size notation are employed in this manual.

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

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.

Laws and Regulations

Legal Prohibition

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.

About the Scanner Functions

This section describes functions you can use in the scanner mode.

You can use the scanner functions to send scan files to computers, scan originals from a computer using the TWAIN driver, or store scan files on the machine's hard disk.

For details about each function, see respective chapters.

Sending scanned files (Network Scanner)

Scan files can be sent to or stored on a computer, and you can specify the format of a scan file according to how the file will be used.

- Sending by e-mail

You can send scan files to specified e-mail addresses.

For details, see chapter 1 "Sending Scan Files by E-mail".

- Sending to folders

Scan files can be stored in shared network folders, or on FTP or Netware servers.

For details, see chapter 2 "Sending Scan Files to Folders".

- Sending using WSD

You can use Web Services on Devices (WSD) to send scan files to a client computer.

For details, see chapter 3 "Sending Scan Files Using WSD".

- Delivering

You can deliver scan files using a delivery server.

For details, see chapter 6 "Delivering Scan Files".

Scanning originals from a client computer (TWAIN Scanner)

You can use the TWAIN driver to scan originals from networked client computers.

For details, see chapter 7 "Scanning Originals with the Network TWAIN Scanner".

Storing files

Scan files can be stored on the machine's hard disk or saved on a removable memory device.

- Storing files on the machine's hard disk

You can do various things with files that are stored on the hard disk, such as save them in shared folders or send them by e-mail.

For details, see chapter 4 "Storing Files Using the Scanner Function".

- Saving files on a removable memory device

You can save scan files on a removable memory device such as a USB memory stick or an SD card.

For details, see chapter 5 "Saving Scan Files on a Removable Memory Device".

Note

- When the Copy Data Security Unit is installed, if you scan an original that was printed using the data security for copying function, the machine beeps and an entirely gray page is sent or stored. You can use the log file to check who scanned the confidential original. For details about the data security for copying function, consult the administrator.
- This machine's scanner functions are only available as network functions. They are not available through direct (USB) connection.

Reference

- p.19 "Sending Scan Files by E-mail"
- p.51 "Sending Scan Files to Folders"
- p.75 "Sending Scan Files Using WSD"
- p.113 "Delivering Scan Files"
- p.133 "Scanning Originals with the Network TWAIN Scanner"
- p.89 "Storing Files Using the Scanner Function"
- p.109 "Saving Scan Files on a Removable Memory Device"

Display Panel

This section explains the simplified display and three confirmation screens: Check Modes, Preview, and Scanned Files Status.

In this manual you can find explanations about the E-mail screen, Scan to Folder screen, WSD scanner screen, list of stored files screen, and the network delivery scanner screen. For details about each of these screens, see "E-mail Screen", "Scan to Folder Screen", "WSD Scanner Screen", "List of Stored Files", and "Network Delivery Scanner Screen" respectively.

Reference

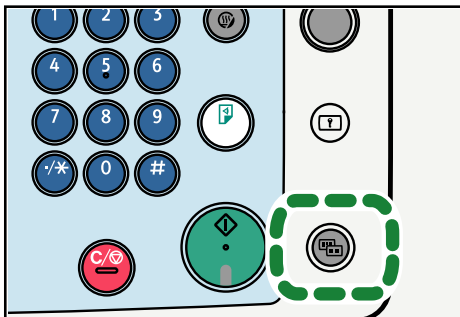
- p.23 "E-mail Screen"
- p.56 "Scan to Folder Screen"
- p.79 "WSD Scanner Screen"
- p.96 "List of Stored Files"
- p.117 "Network Delivery Scanner Screen"

Simplified Display

This section explains how to switch to the simplified display.

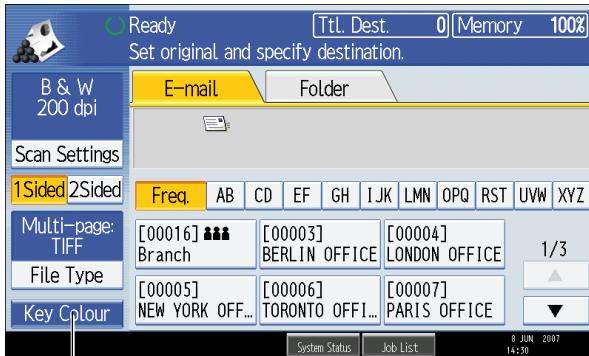
When you press the [Simplified Display] key, the screen changes from the initial display to the simplified display.

Letters and keys are displayed at a larger size, making operations easier.



BQC002S

Example of Simplified Display



1

BAP001S

1. [Key Colour]

Press to increase screen contrast by changing the color of the keys.

This is available only for the simplified display.

↓ Note

- To return to the initial screen, press the [Simplified Display] key again.
- Certain keys do not appear on the simplified display.

Confirmation Displays

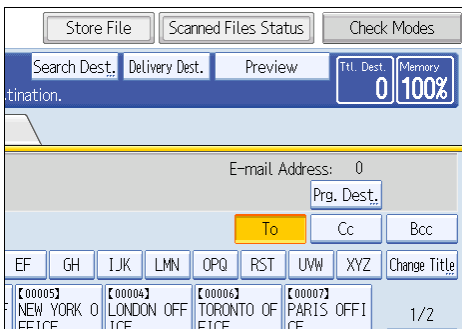
This section explains three confirmation displays: Check Modes, Preview, and Scanned Files Status.

Check Modes

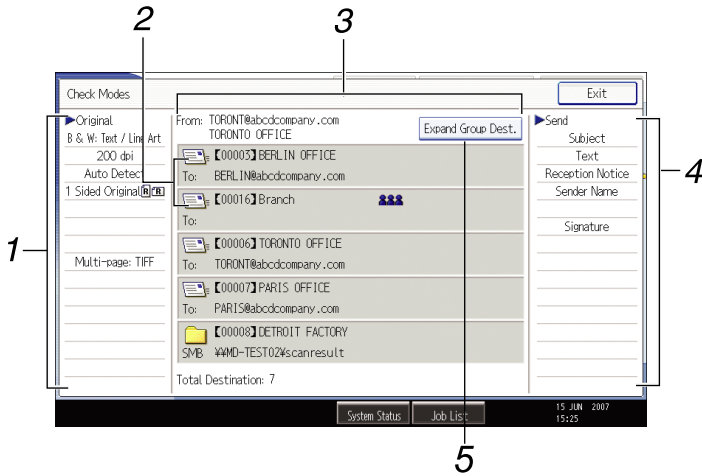
This section explains items that are displayed and how to display the Check Modes screen.

Use the Check Modes screen to check scanning and transmission settings.

Pressing [Check Modes] switches the screen from the initial scanner screen to the Check Modes screen.



Check Modes



BAP002S

1. Original

Displays Scan Settings, Original Feed Type, and other scanning settings.

2. Transmission function icon

Displays the icon of the transmission function in use.

3. Sender and Destination

Displays the sender and transmission or delivery destinations.

The (👤👤👤) symbol indicates a group destination.

The (🔒) symbol indicates a destination that can receive encrypted e-mail.

4. Send

Displays transmission settings such as Sender and Subject.

5. [Expand Group Dest.]

Press to display the members of the group, when a group is specified as the destination.

Note

- While this machine is being used as a WSD scanner, only the settings specified directly on the machine can be displayed.

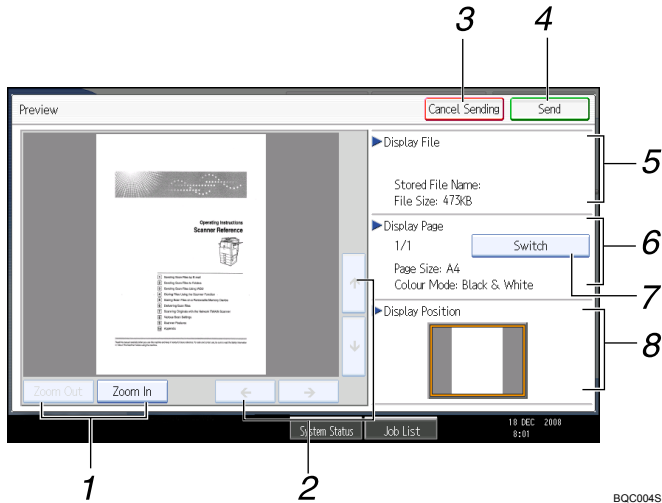
Preview

Use the Preview screen to check that originals have been scanned correctly.

This section explains about the Preview screen that can be used before sending files by e-mail or Scan to Folder, or delivering files.

Before you start scanning, press [Preview]. If you scan originals while [Preview] is selected, the Preview screen appears. You can start or cancel sending the files after checking the preview and the scan settings used for scanning.

Preview



1. [Zoom Out] and [Zoom In]

Press to reduce or enlarge the displayed preview.

2. [←][→][↑][↓]

Press to shift the displayed area.

3. [Cancel Sending]

Press to close a preview and interrupt a transmission.

4. [Send]

Press to close a preview and continue a transmission.

5. Display File

Displays a file's name and size.

6. Display Page

Displays the number of the currently displayed page, total number of pages, page size, and color mode.

7. [Switch]

Press to change the page of the selected file that is displayed.

8. Display Position

Displays the position of an image when enlarged.

↓ Note

- Preview is not available if you are scanning by WSD. View the scanned images on the destination computer instead.
- Preview is not available if a file is scanned using [Store to HDD].
- You can view a stored file using the Preview screen displayed from the list of stored files. For details about viewing a stored file, see "Checking a Stored File Selected from the List".

- Preview is not available if you select High Compression PDF as the file type.
- Preview might not be displayed if scanning failed or the image file is corrupted. If this is the case, scan the original again.

Reference

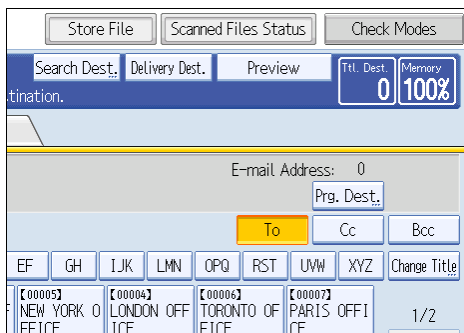
- p.99 "Checking a Stored File Selected from the List"

Scanned Files Status

This section explains items that are displayed and how to display the Scanned Files Status screen.

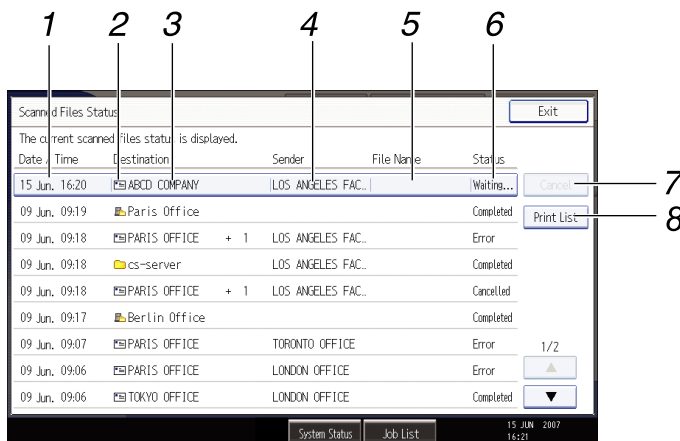
Use the Scanned Files Status screen to check e-mail transmission, Scan to Folder, and delivery results.

Press [Scanned Files Status] to display the Scanned Files Status screen.



Up to 9 transmission or delivery results are displayed at the same time. Press [▲] or [▼] to switch between results.

Scanned Files Status



BAP004S

1. Date / Time

Displays the time and date transmission was specified by this machine or the time and date when Completed, Error, or Cancelled was confirmed.

2. Transmission function icon

Displays the icon of the transmission function used.

The  symbol indicates a destination that can receive encrypted e-mail.

3. Destination

Displays the transmission destination.

If you have selected multiple destinations, the first selected destination is displayed.

Other destinations appear as "+ X" (X indicates the number of destinations.) when sending files by e-mail or delivering them.

4. Sender

Displays the sender name.

5. File Name

Displays the stored file name of files that are simultaneously sent and stored, or of stored files that are sent.

6. Status

Displays one of the following transmission statuses: Completed, Trnsmtg., Waiting..., Error, or Cancelled.

7. [Cancel]

To cancel transmission, select a file whose status is "Waiting...", and then press [Cancel].

8. [Print List]

Press to print transmission results.

Note

- You cannot check scanner function transmission results by pressing [Job List] at the bottom of the screen. To check transmission results, press [Scanned Files Status], and then display the Scanned Files Status screen.
- Depending on security settings, some transmission results might not be displayed.

1. Sending Scan Files by E-mail

You can attach scan files to e-mails and send them via connections such as LAN and the Internet.

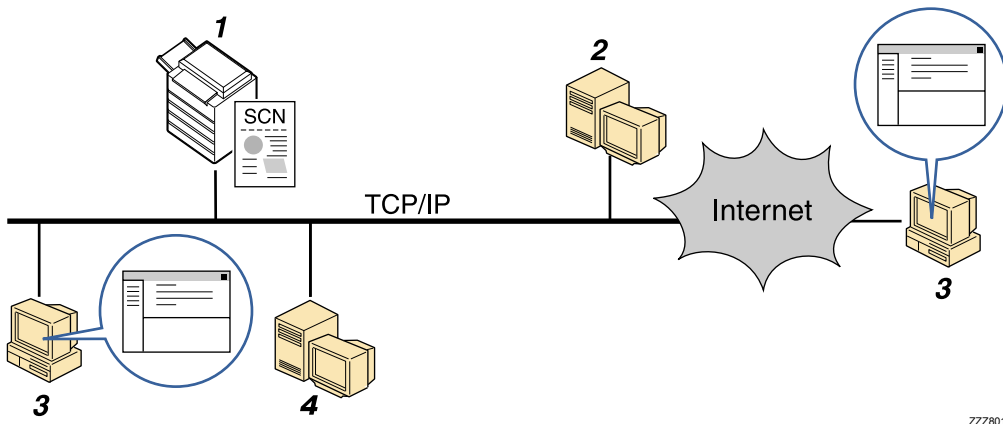
1

Before Sending Scan Files by E-mail

This section explains the necessary preparations and the procedure for sending scan files by e-mail.

Overview of Sending Scan Files by E-mail

This section describes the process for sending scan files by e-mail.



ZZZ801S

1. This machine

You can attach scan files to e-mail and send them to a mail server. You can also encrypt and/or attach a signature to the scan files you send by e-mail.

2. SMTP server

You need to have an access to an e-mail server that supports SMTP (Simple Mail Transfer Protocol), to send scan files by e-mail. However, it is not essential to have an e-mail server inside the LAN where this machine belongs. It transfers a received e-mail to a specified destination through a LAN or the Internet.

3. Client computer

Use e-mail client software to receive e-mail messages and scan file attachments that are generated by this machine.

4. LDAP Server

Use this server for administering e-mail accounts, searching the network, and authenticating the computers that access the machine. Using the LDAP server, you can search for destinations from the machine.

↓ Note

- This machine does not support SMTPS (SMTP over SSL).

Preparation for Sending by E-mail

1

To send scanned files by e-mail, you must first perform the following:

- Check the machine is properly connected to the network
- Configure the network settings in [System Settings]
- Configure the necessary settings in [Scanner Features]

Checking the machine is properly connected to the network

Check that this machine is properly connected to the network.

For details about how to connect this machine to a network, see "Connecting to the Interface", Network and System Settings Guide.

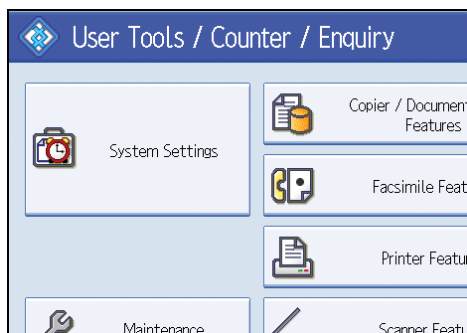
Configuring the network settings in [System Settings]

Configure the network settings in [System Settings] according to your environment and how you will be using the machine.

The following procedure explains connecting this machine to an IPv4 network using Ethernet cable.

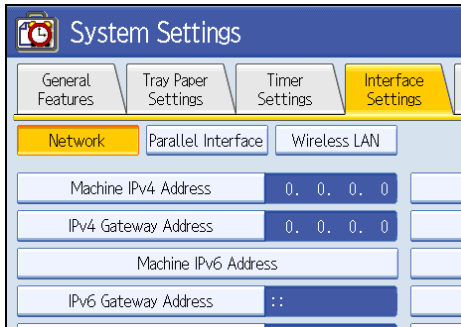
Note that the settings you must configure will vary depending on your operating environment. For details about network settings and configuration procedures, see "Network Settings Required to Use E-mail Function", Network and System Settings Guide.

1. Press the [User Tools/Counter] key, and then press [System Settings].



The System Settings screen appears.

2. Press the [Interface Settings] tab.



3. Press [Machine IPv4 Address] to specify the machine's IPv4 address.

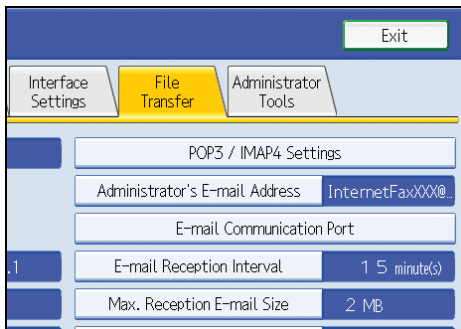
To specify a static IPv4 address for this machine, press [Specify], and then enter the IPv4 address and subnet mask.

To obtain an IPv4 address from a DHCP server automatically, press [Auto-Obtain (DHCP)].

4. Press [IPv4 Gateway Address], and then enter the IPv4 gateway address.

5. Press [Effective Protocol], and then make [IPv4] active.

6. Press the [File Transfer] tab, and then press [SMTP Server].



7. Press [Change], which is to the right of [Server Name], then enter the SMTP server host name or IPv4 address, and then press [OK].

If necessary, you can change the port number by pressing [Change], which is to the right of the port number.

8. Press [Exit] twice.

↓ Note

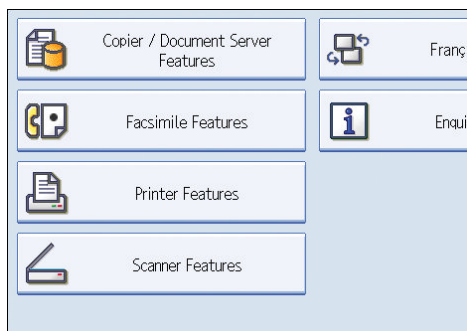
- If an extended wireless LAN board (optional) is installed, press [LAN Type] on the [Interface Settings] tab, then press [Ethernet], and then configure the network settings.

Configuring the necessary settings in [Scanner Features]

Using [Scanner Features], you can make or change various settings related to the scanner function, such as compressing scan data or printing the scanner journal. Configure the scanner settings according to your environment and how you will be using the machine.

This section explains how to display the Scanner Features screen. For details about the settings on this screen, see "Scanner Features".

1. Press the [User Tools/Counter] key, and then press [Scanner Features].



The Scanner Features screen appears.

2. Press the [General Settings], [Scan Settings], [Send Settings], or [Initial Settings] tabs and configure the relevant settings on those tabs.

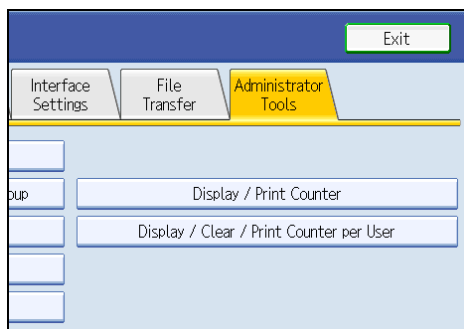
Reference

- p.175 "Scanner Features"

Registering E-mail Addresses in the Address Book

You can register frequently used e-mail addresses in the address book. This section explains how to register e-mail addresses in the address book.

1. Press the [User Tools/Counter] key, and then press [System Settings].
2. Press the [Administrator Tools] tab.



3. Press [Address Book Management].

4. Press [New Program], and then enter necessary information.

You can register the e-mail address in groups.

5. Press [Exit] twice.

↓ Note

- For details about registering e-mail addresses in the address book, see "Registering Addresses and Users for Facsimile/Scanner Functions", Network and System Settings Guide.
- You can also register e-mail addresses in the address book using Web Image Monitor or SmartDeviceMonitor for Admin. For details about how to display Web Image Monitor or install SmartDeviceMonitor for Admin, see "Monitoring and Configuring the Printer", Network and System Settings Guide. For details about registering addresses in the address book, see Web Image Monitor or SmartDeviceMonitor Help.
- Depending on the machine type, you may not be able to use the machine when it is updating the address book using CSV files (retrieved using SmartDeviceMonitor for Admin) that contain user codes.
- Encrypted files can be sent by e-mail only to destinations for which decryption is set. For details about sending encrypted files by e-mail, see "Security Settings to E-mails".

📖 Reference

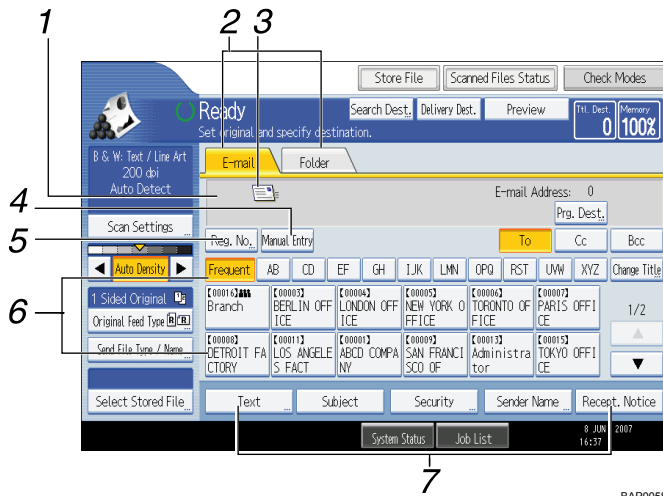
- p.46 "Security Settings to E-mails"

E-mail Screen

This section explains the screen layout when sending scan files by e-mail.

The function items displayed serve as selector keys. You can select or specify an item by pressing it.

When you select or specify an item on the display panel, it is highlighted like []. Keys that cannot be selected appear like [].



1. Destination field

The specified destination appears. If more than one destination has been specified, press [▲] or [▼] to scroll through the destinations.

2. E-mail / Folder

Press these tabs to switch between the E-mail screen and Scan to Folder screen.

Switch the screen also when sending the same files by both e-mail and Scan to Folder.

3. E-mail icon

Indicates that the E-mail screen is displayed.

4. [Manual Entry]

To specify destinations not registered in the address book, press this key, and then enter the e-mail addresses using the soft keyboard that appears.

5. [Reg. No.]

Press this key to specify the destination using a 5-digit registration number.

6. Destination List

The list of destinations registered in the machine appears. If all of the destinations cannot be displayed, press [▲] or [▼] to switch the screen.

The (👤👤👤) symbol indicates a group destination.

The (🔒 or 👤👤) symbol indicates a destination that can receive encrypted e-mail.

7. [Text] [Subject] [Security] [Sender Name] [Recept. Notice]

Enter the message and specify the subject, security (encryption and a signature), sender, and whether or not to use Message Disposition Notification.

Basic Procedure for Sending Scan Files by E-mail

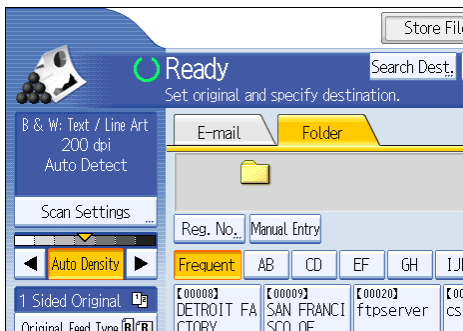
This section explains the basic procedure for sending scan files by e-mail.

1. Make sure that no previous settings remain.

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

2. If the network delivery scanner screen or Scan to Folder screen appears, switch to the E-mail screen.

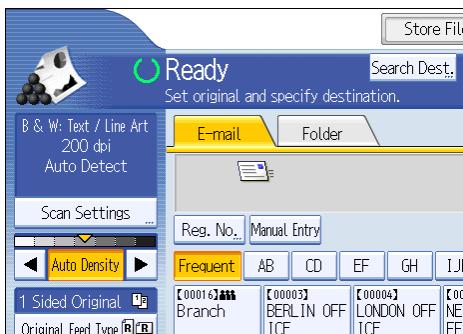
For details, see "Switching to the E-mail Screen".



3. Place originals.

4. If necessary, press [Scan Settings] to specify scanner settings such as resolution and scan size.

For details, see "Various Scan Settings".



5. If necessary, specify the scanning density.

For details, see "Adjusting Image Density".

6. If necessary, press [Original Feed Type] to specify settings such as original orientation.

For details, see "Setting of Original Feed Type".

7. If necessary, press [Send File Type / Name] to specify settings such as file format and file name.

For details, see "Specifying the File Type and File Name".

8. Specify the destination.

You can specify multiple destinations.

For details, see "Specifying E-mail Destinations".

9. If necessary, press [Text] to enter the e-mail message.

For details, see "Entering the E-mail Message".

10. If necessary, press [Subject] to specify the e-mail subject.

For details, see "Entering the E-mail Subject".

11. To specify the e-mail sender, press [Sender Name].

For details, see "Specifying the E-mail Sender".

12. If necessary, press [Security] to specify [Encryption] or [Signature].

For details, see "Security Settings to E-mails".

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

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

14. Press the [Start] key.

If you are scanning batches, place the next originals.

Note

- If you have selected two or more destinations, the destinations can be made to appear one by one by pressing [▲] or [▼] next to the destination field.
- To cancel a selected destination, press [▲] or [▼] to display the destination in the destination field, and then press the [Clear/Stop] key. You can cancel a destination selected from the destination list by pressing the selected destination again.
- In [System Settings], you can specify the administrator's e-mail address as the default sender name. This lets you send e-mail without entering anything for [Sender Name]. For details, see "File Transfer", Network and System Settings Guide.
- Depending on the security setting, the logged-on user may be specified as [Sender Name].
- To use Message Disposition Notification, log on to the machine as a user and specify the sender. Note, however, that the [Recept. Notice] notification e-mail may not be transmitted if the e-mail software of the recipient does not support Message Disposition Notification.
- If you press [Check Modes] before pressing the [Start] key, the initial scanner screen switches to the Check Modes screen. You can use the Check Modes screen to check the settings such as destinations. For details, see "Check Modes".
- If you press [Preview] and then start scanning while [Preview] is selected, the Preview screen appears. You can use this screen to check how the originals are scanned and the scan setting used for scanning. After checking the preview, you can specify whether to send the file or not. For details, see "Preview".
- To cancel scanning, press the [Clear/Stop] key.

- You can also store a scan file and simultaneously send it by e-mail. For details, see "Simultaneous Storage and Sending by E-mail".
- When [Security] is set to [Encryption], if you specify multiple destinations, a delivery failure message will appear each time a scan file is sent to a destination where decryption settings have not been configured.
- After an e-mail is sent, the destination, sender, subject, text, and file name fields will be automatically cleared. If you want to preserve the information in these fields, contact your local dealer.

Reference

- p.28 "Switching to the E-mail Screen"
- p.143 "Various Scan Settings"
- p.151 "Adjusting Image Density"
- p.152 "Setting of Original Feed Type"
- p.160 "Specifying the File Type and File Name"
- p.29 "Specifying E-mail Destinations"
- p.43 "Entering the E-mail Message"
- p.42 "Entering the E-mail Subject"
- p.38 "Specifying the E-mail Sender"
- p.46 "Security Settings to E-mails"
- p.14 "Check Modes"
- p.15 "Preview"
- p.45 "Simultaneous Storage and Sending by E-mail"

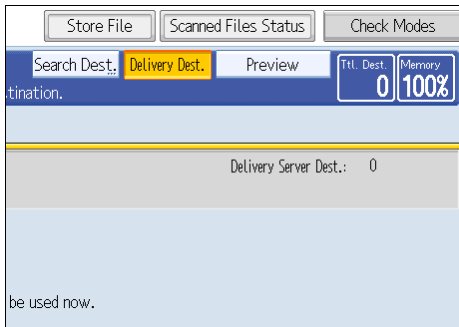
Switching to the E-mail Screen

This section explains how to switch the screen to the E-mail screen.

If the Scan to Folder screen is being displayed, press [E-mail] to switch to the E-mail screen.

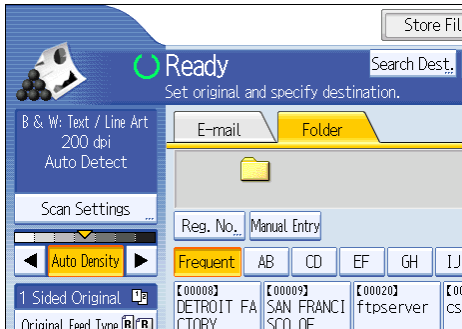
If the network delivery scanner screen is being displayed, switch to the E-mail screen as follows:

1. Press [Delivery Dest.].



The E-mail screen or Scan to Folder screen appears.

2. If the Scan to Folder screen appears, press [E-mail].



The E-mail screen appears.

Note

- You cannot switch from the network delivery scanner screen or other screens while destinations are being specified. To clear the specified destination, display the destination in the destination field, and then press the [Clear/Stop] key.
- If you are scanning files using WSD, [Swch Dest.List] or [WSD Dest.] appears instead of [Delivery Dest.]. To switch to the E-mail screen, press [Swch Dest.List], and then, on the screen that appears, press [E-mail / Folder], or press [WSD Dest.].

Specifying E-mail Destinations

This section explains how to specify e-mail destinations.

You can specify e-mail destinations by any of the following methods:

- Select the destination from the machine's address book
- Enter the e-mail address directly
- Search the LDAP server for the destination and select it

Before you select destinations, make sure you have selected [To]. If necessary, press [Cc] or [Bcc], and then select destinations.

↓ Note

- You can specify multiple destinations.

Selecting the Destination from the Machine's Address Book

This section explains how to select the destination from the machine's address book.

★ Important

- **To use this function, you must register the destinations in [System Settings] in advance. For details, see "Registering Addresses and Users for Facsimile/Scanner Functions", Network and System Settings Guide.**

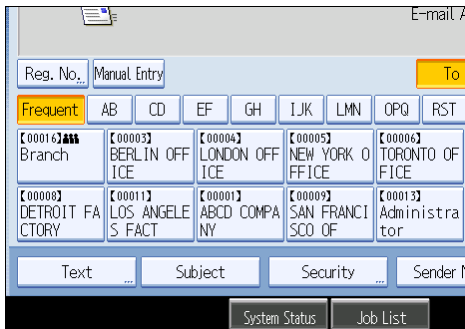
You can use the following methods to select destinations registered in the machine's address book:

- Select a destination from the list
- Select a destination by entering the registration number
- Select a destination by searching the machine's address book

Selecting a destination from the list

Select the destination from the destination list.

1. In the destination list, press the key including the destination name.



The key of the selected destination is highlighted, and the destination appears in the destination field at the top of the screen.

If the target destination does not appear, take one of the following steps:

- Display the destination by selecting its initial letter from the title
- Display the destination by pressing [▲] or [▼]

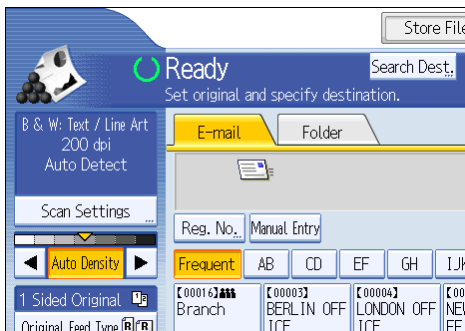
Note

- Depending on the security setting, some destinations may not appear in the destination list.

Selecting destinations by entering the registration numbers

Select the destination from the machine's address book using its registration number.

1. Press [Reg. No.].



2. Using the number keys, enter the five-digit registration number assigned to the required destination.

If the entered number is less than five digits, press the [#] key after the last number.

Example: To enter 00003

Press the [3] key, and then press the [#] key.

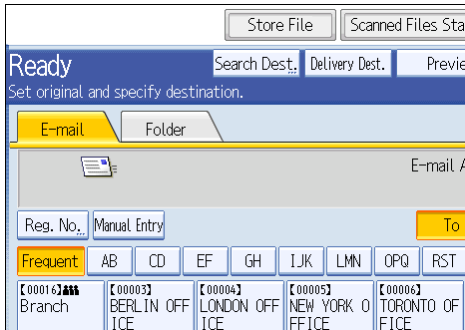
By pressing [Change], you can change the selected destination.

3. Press [OK].

Searching the machine's address book for the destination and selecting it

This section explains how to search the machine's address book for the destination and select it.

1. Press [Search Dest.].



2. To search by destination name, press [Name].

To search by e-mail address, press [E-mail Address].

The soft keyboard appears.

You can also search by combining [Name] and [E-mail Address].

3. Enter the beginning of the destination name.

To search by e-mail address, enter the beginning of the address.

4. Press [OK].

5. If necessary, press [Advanced Search] to specify the detailed search criteria, and then press [OK].

By pressing [Advanced Search], you can search using criteria such as [Name], [Fax Destination], [E-mail Address], and [Folder Name]. You can specify search criteria such as [Beginning Word] or [End Word]. You can refine your search using multiple criteria.



The illustrated screen is an example. The items that actually appear on the screen may differ.

6. Press [Start Search].

Destinations that match the search criteria are displayed.

7. Select a destination.

8. Select [To], [Cc], or [Bcc].

9. Press [OK].

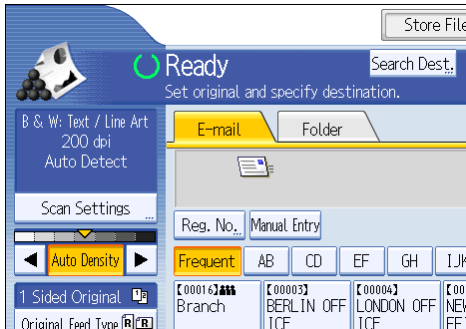
↓ Note

- If [LDAP Search] is set to [On] in [System Settings], check that [Address Book] has been selected before executing the search.
- Search criteria that appear in [Advanced Search], such as [Name], [Fax Destination], [E-mail Address], and [Folder Name], are registered in the machine's address book. For details, see "Registering Addresses and Users for Facsimile/Scanner Functions", Network and System Settings Guide.
- By pressing [Details], you can view details about the selected destinations.
- Up to 100 destinations can be displayed as search results.
- By pressing [Advanced Search], the following criteria appear:
 - [Beginning Word]: The names which start with the entered character or characters are targeted. For example, to search for "ABC", enter "A".
 - [End Word]: The names which end with the entered character or characters are targeted. For example, to search for "ABC", enter "C".
 - [Exact Match]: The names which correspond to an entered character or characters are targeted. For example, to search for "ABC", enter "ABC".
 - [Include one Word]: The names which contain an entered character or characters are targeted. For example, to search for "ABC", enter "A", "B", or "C".
 - [Exclude Words]: The names which do not contain an entered character or characters are targeted. For example, to search for "ABC", enter "D".

Entering an E-mail Address Manually

This section explains how to enter an e-mail address manually.

1. Press [Manual Entry].



The soft keyboard appears.

2. Enter the e-mail address.

3. Press [OK].

Note

- Depending on the security settings, [Manual Entry] may not be displayed.
- To change a registered destination e-mail address, press [Edit] to the left of the destination field to display the soft keyboard, use the soft keyboard to enter the new address, and then click [OK].
- The e-mail address that is entered directly can be registered in the machine's address book. For details, see "Registering a Directly-Entered Destination in the Address Book".

Reference

- p.36 "Registering a Directly-Entered Destination in the Address Book"

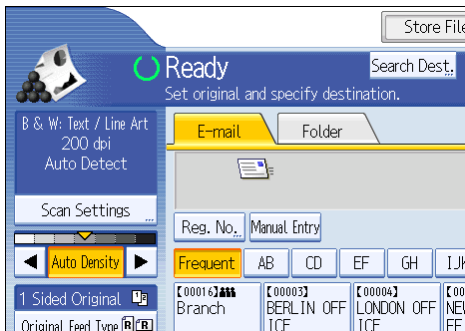
Selecting Destinations by Searching an LDAP Server

This section explains how to search for an address registered in an LDAP server and specify it as an e-mail destination.

Important

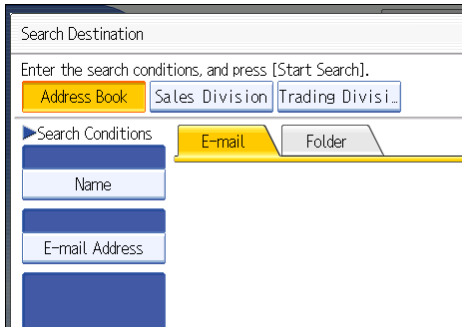
- To use this function, an LDAP server must be connected to the network.
- Under [System Settings], the LDAP server must be registered and [LDAP Search] must be set to [On]. For details, see "System Settings", Network and System Settings Guide.

1. Press [Search Dest.].



2. Select the LDAP server that appears next to [Address Book].

Register the LDAP server in advance in [System Settings].



If authentication is required to access the selected server, the authentication screen appears. To authenticate, enter the user name and password.

3. To search by destination name, press [Name].

To search by e-mail address, press [E-mail Address].

The soft keyboard appears.

You can also search by combining [Name] and [E-mail Address]. If you search by [Name], LDAP server's settings determine whether the search is based on surname or first name. Consult your administrator.

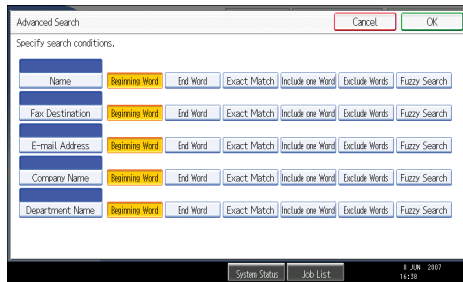
4. Enter the beginning of the destination name.

To search by e-mail address, enter the beginning of the destination address.

5. Press [OK].

6. If necessary, press [Advanced Search] to specify the detailed search criteria, and then press [OK].

By pressing [Advanced Search], you can search using criteria such as [Name], [Fax Destination], [E-mail Address], [Company Name], and [Department Name]. You can specify search criteria such as [Beginning Word] or [End Word]. You can refine your search using multiple criteria.



The illustrated screen is an example. The items that actually appear on the screen may differ.

7. Press [Start Search].

Destinations that match the search criteria are displayed.

8. Select the destination.

9. Select [To], [Cc], or [Bcc].

10. Press [OK].

↓ Note

- Search criteria that appear in [Advanced Search], such as [Name], [Fax Destination], [E-mail Address], [Company Name], and [Department Name], are registered in the LDAP server.
- If you specified [Search Options] on [Program / Change / Delete LDAP Server] under [System Settings], you can add a search condition for LDAP search on the [Advanced Search] screen. For details, see "System Settings", Network and System Settings Guide.
- By pressing [Details], you can view details about the selected destinations.
- Up to 100 destinations can be displayed as search results.
- If an e-mail address returned by the LDAP server is too long, it will be impossible to specify it as the destination. For details about the number of characters that can be specified, see "Sending e-mail".
- You can register multiple e-mail addresses in individual LDAP server accounts. However, only one e-mail address will be displayed as the search result. Usually, the address that was registered first on the LDAP server is the address that is displayed.
- By pressing [Advanced Search], the following criteria appear:
 - [Beginning Word]: The names which start with the entered character or characters are targeted. For example, to search for "ABC", enter "A".
 - [End Word]: The names which end with the entered character or characters are targeted. For example, to search for "ABC", enter "C".
 - [Exact Match]: The names which correspond to an entered character or characters are targeted. For example, to search for "ABC", enter "ABC".
 - [Include one Word]: The names which contain an entered character or characters are targeted. For example, to search for "ABC", enter "A", "B", or "C".

- [Exclude Words]: The names which do not contain an entered character or characters are targeted.

For example, to search for "ABC", enter "D".

- [Fuzzy Search]: a vague search (The function of this vague search depends on the system supported by the LDAP server.)

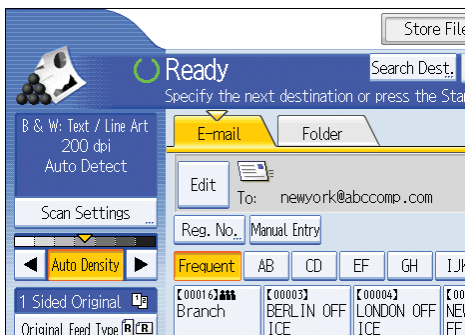
Reference

- p.191 "Sending e-mail"

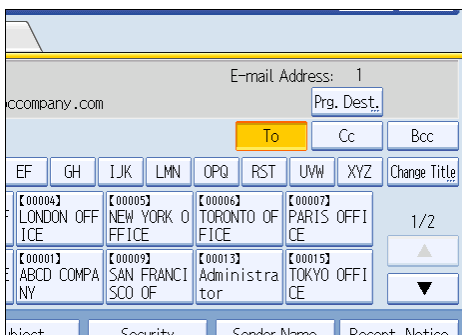
Registering a Directly-Entered Destination in the Address Book

This section explains how to register a directly-entered destination in the machine's address book. You can also register a destination selected from the LDAP server.

1. In the destination field, display the destination you want to register.



2. Press [Prg. Dest.].



3. Press [Names], and then specify the name and other information to be registered.

For details about specifying the information to be registered, see "Registering Addresses and Users for Facsimile/Scanner Functions", Network and System Settings Guide.

4. Press [OK].

Note

- Depending on the security setting, [Prg. Dest.] may not appear. In such case, you cannot complete the registration.
- To register in the machine's address book a destination searched for and selected from the LDAP server, display the destination, and then press [Prg. Dest.].

Specifying the E-mail Sender

This section explains how to specify the e-mail sender.

To send e-mail, you must specify the name of the sender.

You can specify the e-mail sender by any of the following methods:

- Select the sender from the sender list
- Select the sender by entering the registration number
- Select the sender by searching the machine's address book

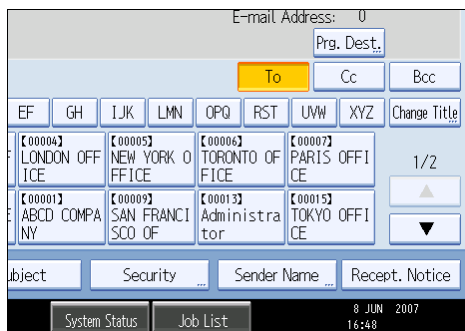
Note

- Senders must be registered in advance under [System Settings]. For details, see "Registering Addresses and Users for Facsimile/Scanner Functions", Network and System Settings Guide.
- In [System Settings], you can specify the administrator's e-mail address as the default sender name. This lets you send e-mail without entering anything for [Sender Name]. For detail, see "File Transfer", Network and System Settings Guide.
- Depending on the security setting, the logged-on user may be specified as [Sender Name].
- When a protection code has been set, a screen for entering the protection code appears after selecting the sender. Enter the protection code, and then press [OK]. If the protection code you entered is correct, the sender name is displayed.

Selecting a Sender from the List

This section explains how to select the sender from the machine's sender list.

1. Press [Sender Name].



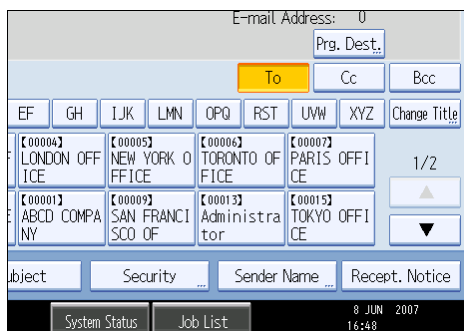
2. Select the sender.

3. Press [OK].

Using a Registration Number to Specify a Sender Name

Select the sender using the registration numbers specified by users in the machine's address book.

1. Press [Sender Name].



2. Press [Registration No.].

3. Using the number keys, enter the five-digit registration number assigned to the required destination.

If the entered number is less than five digits, press the [#] key after the last number.

Example: To enter 00006

Press the [6] key, and then press the [#] key.

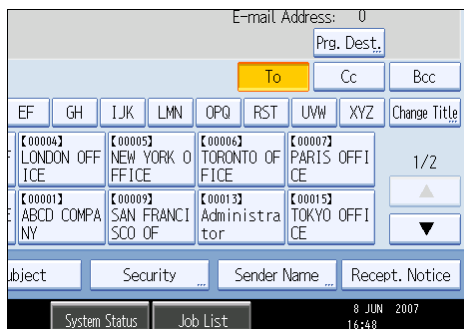
By pressing [Change], you can change the selected destination.

4. Press [OK] twice.

Selecting the Sender by Searching the Machine's Address Book

This section explains how to select the sender by searching the machine's address book.

1. Press [Sender Name].



2. Press [Search].

3. To search by user name, press [Name].

To search by e-mail address, press [E-mail Address].

The soft keyboard appears.

You can also search by combining [Name] and [E-mail Address].

4. Enter the beginning of the sender's name you want to search for.

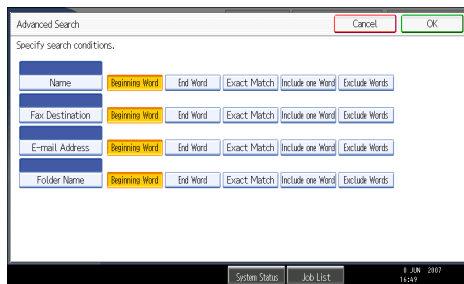
To search by e-mail address, enter the beginning of the address.

5. Press [OK].

6. If necessary, press [Advanced Search] to specify the detailed search criteria, and then press [OK].

By pressing [Advanced Search], you can search using criteria such as [Name], [Fax Destination], [E-mail Address], and [Folder Name].

You can specify search criteria such as [Beginning Word] or [End Word]. You can refine your search using multiple criteria.



The illustrated screen is an example. The items that actually appear on the screen may differ.

7. Press [Start Search].

Destinations that match the search criteria are displayed.

8. Select the sender.

9. Press [OK] twice.

Note

- Search criteria that appear in [Advanced Search], such as [Name], [Fax Destination], [E-mail Address], and [Folder Name], are registered in the machine's address book. For details, see "Registering Addresses and Users for Facsimile/Scanner Functions", Network and System Settings Guide.
- By pressing [Details], you can view details about the selected sender.
- By pressing [Advanced Search], the following criteria appear:
 - [Beginning Word]: The names which start with the entered character or characters are targeted. For example, to search for "ABC", enter "A".
 - [End Word]: The names which end with the entered character or characters are targeted.

For example, to search for "ABC", enter "C".

- [Exact Match]: The names which correspond to an entered character or characters are targeted.

For example, to search for "ABC", enter "ABC".

- [Include one Word]: The names which contain an entered character or characters are targeted.

For example, to search for "ABC", enter "A", "B", or "C".

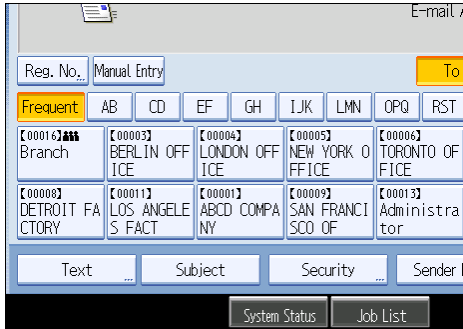
- [Exclude Words]: The names which do not contain an entered character or characters are targeted.

For example, to search for "ABC", enter "D".

Entering the E-mail Subject

When sending a scan file by e-mail, you can enter a subject line for the e-mail.

1. Press [Subject].



2. Enter the subject.

To enter characters, press [Text Entry].

To enter symbols, press [Symbol Entry].

To add predefined User Text registered on this machine, press [User Text].

For details about entering the text, see "Entering Text", About This Machine.

3. Press [OK].

Note

- If you do not specify the e-mail subject, the settings specified in [Default E-mail Subject] on the [Send Settings] tab under [Scanner Features] will be applied. For details, see "Send Settings".

Reference

- p.181 "Send Settings"

Entering the E-mail Message

This section explains how to enter the e-mail message.

The message can be created in the following ways:

- Select the registered e-mail message from the list
- Enter the message directly

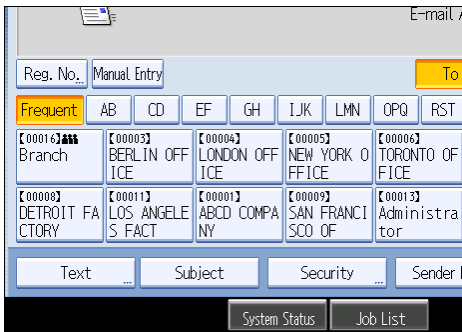
★ Important

- The messages that can be selected from the list must be registered in [System Settings] in advance. For details, see "File Transfer", Network and System Settings Guide.

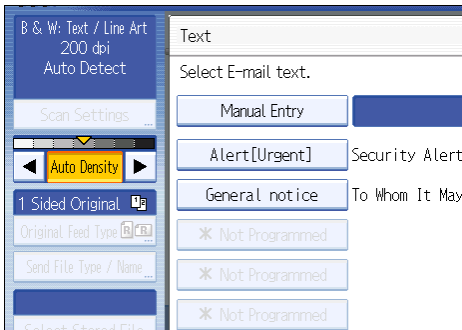
Selecting a Message from the List

You can select a message from the list.

1. Press [Text].



2. Select a message.



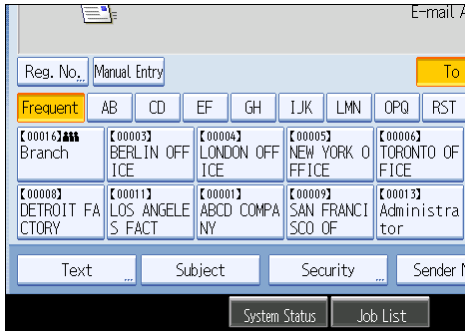
3. Press [OK].

Manual Entry of a Message

You can enter the message manually.

1

1. Press [Text].



2. Press [Manual Entry].

The soft keyboard appears.

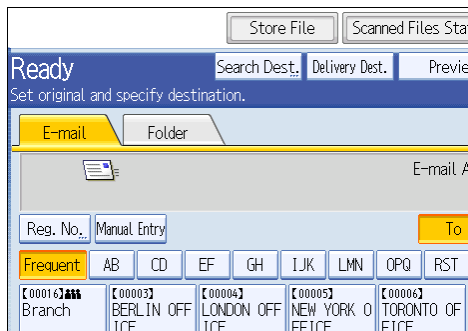
3. Enter the message.

4. Press [OK] twice.

Simultaneous Storage and Sending by E-mail

This section explains how to store a file and simultaneously send it by e-mail.

1. Press [Store File].



2. Select [Store to HDD + Send].

3. If necessary, specify the stored file's information, such as [User Name], [File Name], and [Password].

For details, see "Specifying File Information for a Stored File".

4. Press [OK].

5. Specify the destination, make any other necessary settings, and then send the e-mail.

For details about sending a file by e-mail, see "Basic Procedure for Sending Scan Files by E-mail".

6. Press the [Start] key.

Note

- Depending on the security setting, [Access Privileges] may appear instead of [User Name]. For details about specifying [Access Privileges], consult the administrator.
- You can resend stored files by e-mail. To resend stored files, select the files on the Select Stored File screen, and then send them. For details, see "Sending a Stored File".
- If a file is sent and stored simultaneously with [Security] set, the e-mail will be encrypted and the signature applied, but the stored file will not be changed.

Reference

- p.93 "Specifying File Information for a Stored File"
- p.25 "Basic Procedure for Sending Scan Files by E-mail"
- p.102 "Sending a Stored File"

Security Settings to E-mails

This section explains the procedure for applying security (encryption and a signature) to e-mail.


Applying security (encryption and a signature) to e-mail helps prevent spoofing and information leakage.

↓ Note

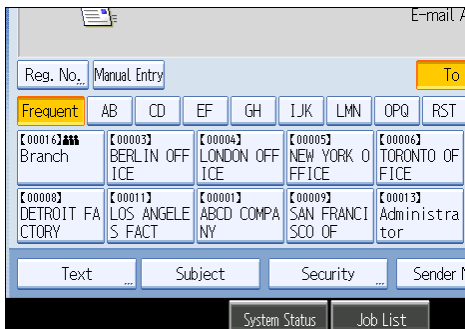
- The S/MIME is used to set security. For details about security settings, consult your network administrator.
- Applying security to e-mail can reduce transmission speed.

Sending Encrypted E-mail

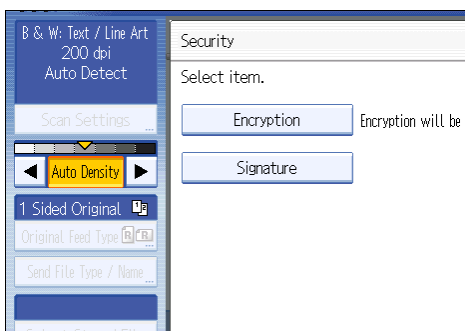
Use the following procedure to specify a destination for which encryption is configured, and encrypt and send an e-mail.

Destinations for which encryption can be configured for each transmission are indicated by this symbol .

1. Press [Security].




2. Select [Encryption].



3. Press [OK].

↓ Note

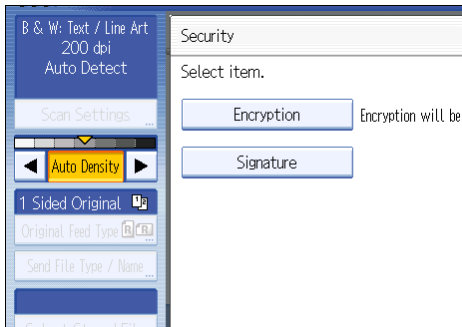
- Encrypting e-mail will increase its size.
- When you specify a destination denoted by the symbol  (which indicates that e-mail sent to this destination is always encrypted) encrypted e-mail will be sent regardless of the setting specified in [Security].
- If you have selected multiple destinations including destinations for which encryption has not been configured, e-mail sent to such destinations will not be encrypted even if you specify encryption.
- If you selected [Store to HDD + Send], the e-mail will be encrypted, but the stored file will not be encrypted.

1

Sending E-mail with a Signature

Use the following procedure to apply a signature to an e-mail that has scan file attachments.

1. Press [Security].
2. Select [Signature].



3. Press [OK].

↓ Note

- The certificate (device certificate) installed on this machine is used to attach signatures.
- Note that the following can result if certain signature settings are specified by the administrator:
 - [Signature] does not appear. This is because you cannot apply signatures to scan files that are sent by e-mail.
 - You cannot change the [Signature] settings. This is because a signature is always applied to scan files that are sent by e-mail.

Sending the URL by E-mail

This section explains how to send the URL of a scanned file by e-mail.

Use this function if network restrictions prevent you sending attachments by email.

★ Important

- Depending on your e-mail application, a phishing warning might appear after you receive an e-mail message. To prevent phishing warnings appearing after you receive e-mail from a specified sender, you must add the sender to your e-mail application's exclusion list. For details about how to do this, see your e-mail application's Help.

1. In [Scanner Features], on the [Send Settings] tab, press [Stored File E-mail Method], and then select [Send URL Link].

For details about specifying the setting, see "Send Settings".

2. Return to the initial scanner screen, and then press [Store File] to select [Store to HDD + Send].

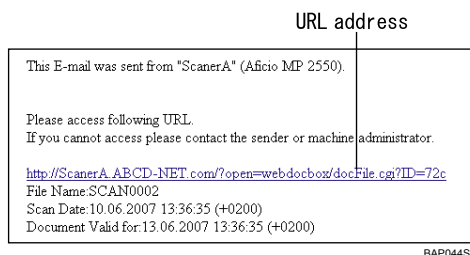
To send the URL by e-mail, you must select [Store to HDD + Send]. For details, see "Simultaneous Storage and Sending by E-mail".

3. Press [OK].

4. Specify the e-mail destination, make any other necessary settings, and then send the e-mail.

For details about sending e-mail, see "Basic Procedure for Sending Scan Files by E-mail".

An e-mail similar to the following will be sent to the destination:



5. In the e-mail destination, click the URL.

Web Image Monitor starts.

6. View, delete, send, or download the file over the network using Web Image Monitor.

↓ Note

- For details about Web Image Monitor functions and their settings, see "Monitoring and Configuring the Printer", Network and System Settings Guide.
- It is recommended that you use Web Image Monitor on the same network environment.

- Depending on the environment, even if you click the URL in the file sent by e-mail, the browser may not start and you may not be able to view the file. If this happens, click the same URL again, or manually enter the URL in the browser's address bar.
- To display details about the functions for managing stored files using Web Image Monitor, click [Help] on the upper right of each Web browser's window.
- You can send the URL by e-mail and simultaneously send it by Scan to Folder. In this case, the file is sent to the Scan to Folder destination, not the URL.
- To send a stored file, see "Sending a Stored File".

Reference

- p.181 "Send Settings"
- p.45 "Simultaneous Storage and Sending by E-mail"
- p.25 "Basic Procedure for Sending Scan Files by E-mail"
- p.102 "Sending a Stored File"

2. Sending Scan Files to Folders

Using the Scan to Folder function, you can send scan files over the network to shared folders, FTP server folders, or NetWare folders.

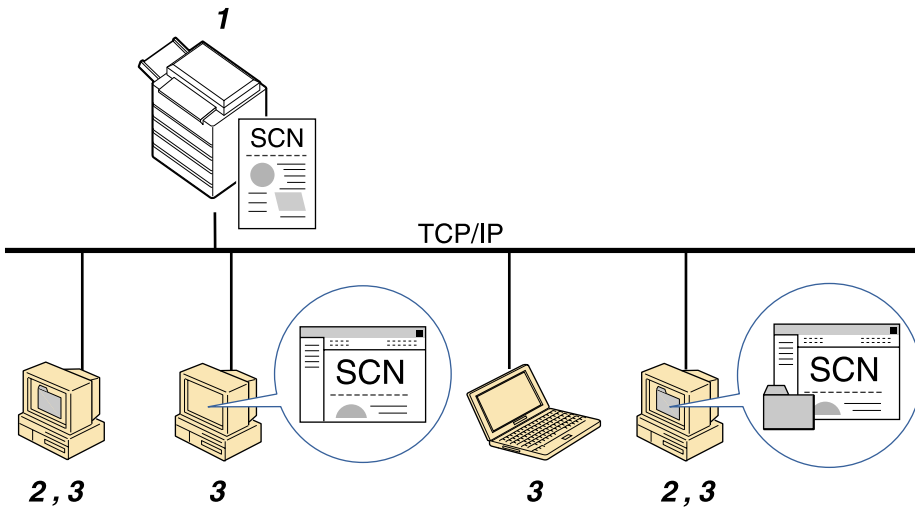
Before Sending Files by Scan to Folder

This section describes the preparations and procedure for sending files by Scan to Folder.

Overview of Sending Scan Files by Scan to Folder

This section describes the process for sending scan files by Scan to Folder.

Sending files to shared folders



ZZZ802S

1. This machine

You can send scan files to shared network folders. To send scan files to shared network folders, use the SMB protocol.

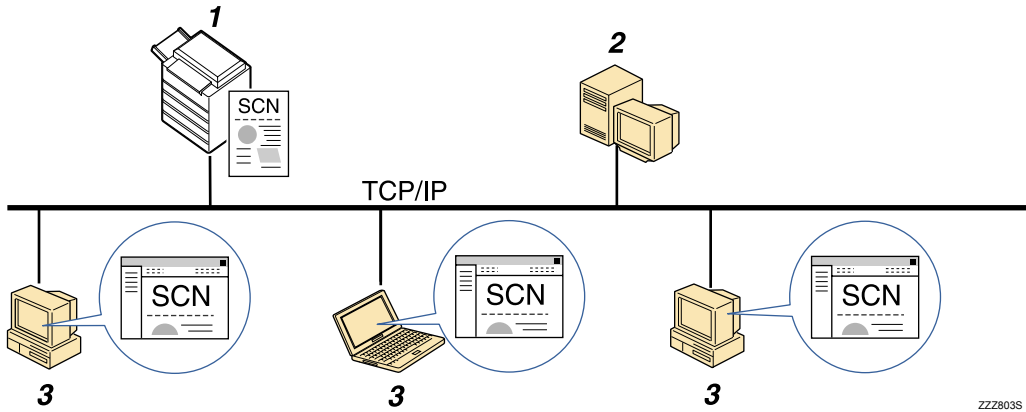
2. Computer with a shared folder

To use this function, it is necessary to create a shared folder in advance. You can specify a shared folder to save scan files.

3. Client computer

You can also browse scanned files saved to a shared folder from a client computer.

Sending files to an FTP server



ZZZ803S

1. This machine

You can send scan files to FTP server folders. To send scan files to FTP server folders, use the FTP protocol.

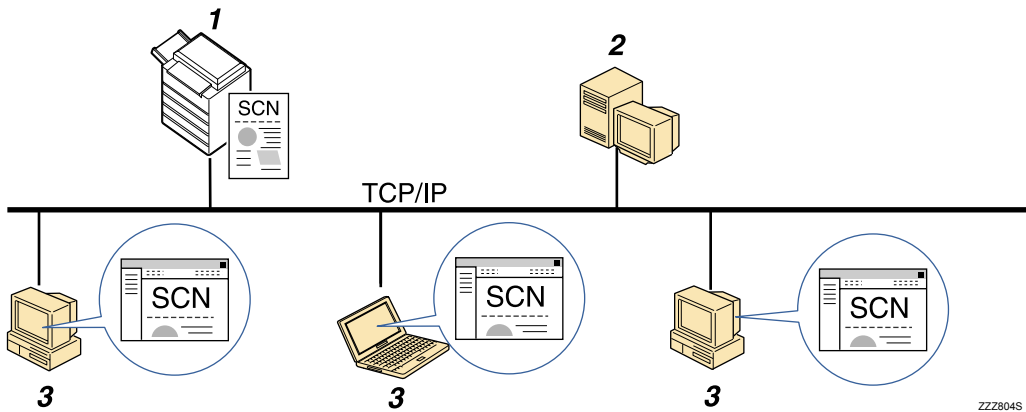
2. FTP server

The FTP server is a server that provides file transfer services among computers on the same network. Transferred files are stored on this server. It is essential to have the FTP server inside the LAN/WAN where this machine belongs. It is not possible to access an FTP server via a proxy server.

3. Client computer

You can browse scanned files saved to an FTP server from a client computer. You need to have an FTP client program on the computer to connect to an FTP server.

Sending files to a NetWare server



ZZZ804S

1. This machine

You can send scan files to NetWare folders. To send scan files to NetWare folders, use the NCP protocol.

2. NetWare server

You can use this server to share files over the network via NetWare. By sending image data to the server, files can be stored on the server.

3. Client computer

To download files, a computer must be running the NetWare client and be logged onto the server.

Preparation for Sending by Scan to Folder

To send scanned files by Scan to Folder, you must first perform the following:

- Check the machine is properly connected to the network
- Configure the network settings in [System Settings]
- Configure the necessary settings in [Scanner Features]

↓ Note

- If necessary, configure the shared folders, FTP server, and Netware server on the network in advance.
- Files can be sent by SMB in NetBIOS over TCP/IP environments only. Files cannot be sent by SMB in NetBEUI environments.
- Scan to Folder is still possible even if sending by SMB or FTP is disabled from the control panel, Web Image Monitor, or Telnet etc.

Checking the machine is properly connected to the network

Check that this machine is properly connected to the network.

For details about how to connect this machine to a network, see "Connecting to the Interface", Network and System Settings Guide.

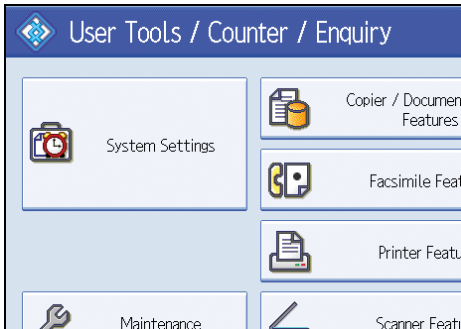
Configuring the network settings in [System Settings]

Configure the network settings in [System Settings] according to your environment and how you will be using the machine.

The following procedure explains connecting this machine to an IPv4 network using Ethernet cable.

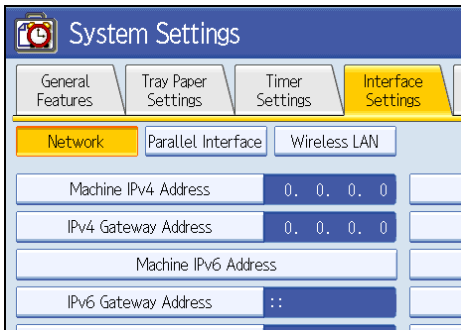
Note that the settings you must configure will vary depending on your operating environment. For details about network settings and configuration procedures, see "Network Settings Required to Use Scan to Folder Function", Network and System Settings Guide.

1. Press the [User Tools/Counter] key, and then press [System Settings].



The System Settings screen appears.

2. Press the [Interface Settings] tab.



3. Press [Machine IPv4 Address] to specify the machine's IPv4 address.

To specify a static IPv4 address for this machine, press [Specify], and then enter the IPv4 address and subnet mask.

To obtain an IPv4 address from a DHCP server automatically, press [Auto-Obtain (DHCP)].

4. Press [IPv4 Gateway Address], and then enter the IPv4 gateway address.
5. Press [Effective Protocol], and then make [IPv4] active.

To send files to shared folders, make [SMB] active.

To send files to Netware folders, make [NetWare] active.

6. Press [Exit] twice.

Note

- If an extended wireless LAN board (optional) is installed, press [LAN Type] on the [Interface Settings] tab, then press [Ethernet], and then configure the network settings.

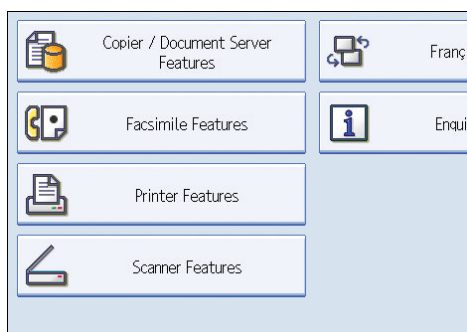
Configure the necessary settings in [Scanner Features]

Using [Scanner Features], you can make or change various settings related to the scanner function, such as compressing scan data or printing the scanner journal. Configure the scanner settings according to your environment and how you will be using the machine.

This section explains how to display the Scanner Features screen. For details about the settings on this screen, see "Scanner Features".

2

1. Press the [User Tools/Counter] key, and then press [Scanner Features].



The Scanner Features screen appears.

2. Press the [General Settings], [Scan Settings], [Send Settings], or [Initial Settings] tabs and configure the relevant settings on those tabs.

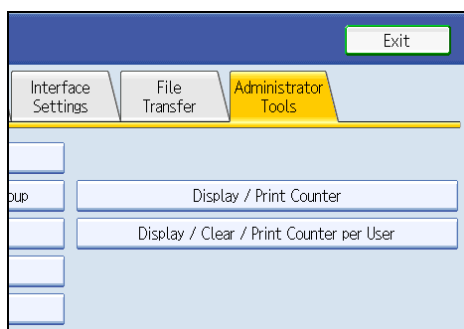
Reference

- p.175 "Scanner Features"

Registering Destination Folders in the Address Book

You can register the addresses of frequently-used destination folders in the address book. This section explains how to register destination folders in the address book.

1. Press the [User Tools/Counter] key, and then press [System Settings].
2. Press the [Administrator Tools] tab.



3. Press [Address Book Management].

4. Press [New Program], and then enter necessary information.

You can register the e-mail address in groups.

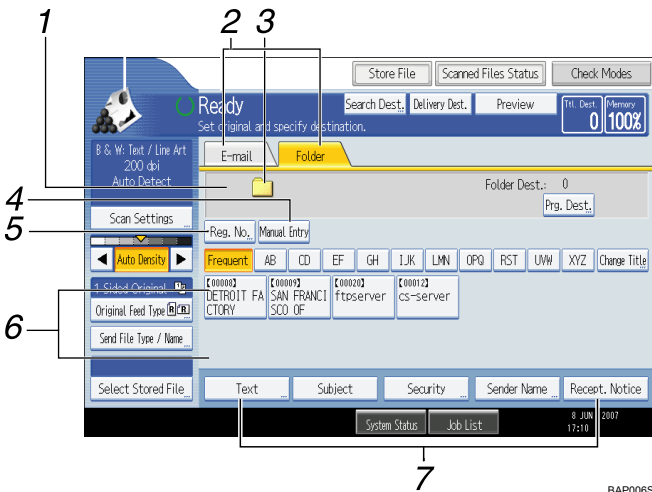
Note

- For details about registering the address of a destination folder in the address book, see "Registering Addresses and Users for Facsimile/Scanner Functions", Network and System Settings Guide.
- You can register entries in the address book using Web Image Monitor or SmartDeviceMonitor for Admin. For details about how to display Web Image Monitor or install SmartDeviceMonitor for Admin, see "Monitoring and Configuring the Printer", Network and System Settings Guide. For details about registering addresses in the address book, see Web Image Monitor or SmartDeviceMonitor Help.
- Depending on the machine type, you may not be able to use the machine when it is updating the address book using CSV files (retrieved using SmartDeviceMonitor for Admin) that contain user codes.

Scan to Folder Screen

This section describes the screen layout when sending scan files by Scan to Folder.

The function items displayed serve as selector keys. You can select or specify an item by pressing it. When you select or specify an item on the display panel, it is highlighted like [**Set**]. Keys that cannot be selected appear like [**OK**].



1. Destination field

The specified destination appears. If more than one destination has been specified, press [▲] or [▼] to scroll through the destinations.

2. E-mail / Folder

Press to switch between the Scan to Folder screen and E-mail screen.

Also switch the screen when sending a file simultaneously by both Scan to Folder and e-mail.

3. Scan to Folder icon

Shows that the Scan to Folder screen is displayed.

4. [Manual Entry]

To specify destinations not registered in the address book, press this button to display the soft keyboard, and then enter the address of the destination folder.

5. [Reg. No.]

Press to specify a destination using a five-digit registration number.

6. Destination List

The list of destinations registered in the machine appears.

If all of the destinations cannot be displayed, press [▲] or [▼] to switch the screen.

The (👤) symbol indicates a group destination.

7. [Text] [Subject] [Security] [Sender Name] [Receipt Notice]

Enter the message and specify the subject, e-mail security (encryption and a signature), sender, and whether or not to use Message Disposition Notification. The entries will be used for e-mail transmission when sending files simultaneously by Scan to Folder and e-mail. For details, see "Sending Scan Files by E-mail".

Reference

- p.19 "Sending Scan Files by E-mail"

Basic Procedure When Using Scan to Folder

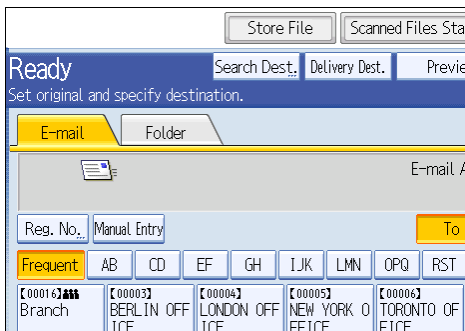
This section describes the basic procedure involved in using Scan to Folder.

1. Make sure that no previous settings remain.

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

2. If the network delivery scanner screen or E-mail screen appears, switch to the Scan to Folder screen.

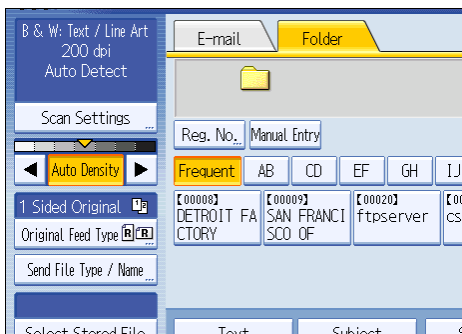
For details, see "Switching to the Scan to Folder Screen".



3. Place originals.

4. If necessary, press [Scan Settings] to specify scanner settings such as resolution and scan size.

For details, see "Various Scan Settings".



5. If necessary, specify the scanning density.

For details, see "Adjusting Image Density".

6. If necessary, press [Original Feed Type] to specify settings such as original orientation.

For details, see "Setting of Original Feed Type".

7. If necessary, press [Send File Type / Name] to specify settings such as file format and file name.

For details, see "Specifying the File Type and File Name".

8. Specify the destination.

You can specify multiple destinations.

For details, see "Specifying Scan to Folder Destinations".

9. Press the [Start] key.

If you are scanning batches, place the next originals.

↓ Note

- If you have selected more than one destination, you can press [▲] or [▼] next to the destination field to scroll through the destinations.
- To cancel a selected destination, press [▲] or [▼] to display the destination in the destination field, and then press the [Clear/Stop] key. You can cancel a destination selected from the destination list by pressing the selected destination again.
- If you press [Check Modes] before pressing the [Start] key, the initial scanner screen switches to the Check Modes screen. You can use the Check Modes screen to check the settings such as destinations. For details, see "Check Modes".
- If you press [Preview], and then start scanning while [Preview] is highlighted, the Preview screen appears. You can use this screen to check how the originals are scanned and the scan settings used for scanning. After checking the preview, you can specify whether to send the file or not. For details, see "Preview".
- To cancel scanning, press the [Clear/Stop] key.
- You can also store a file and simultaneously send it by Scan to Folder. For details, see "Simultaneous Storage and Sending by Scan to Folder".
- After scan files are sent, the destination and file name fields will be automatically cleared. If you want to preserve the information in these fields, contact your local dealer.

📖 Reference

- p.60 "Switching to the Scan to Folder Screen"
- p.143 "Various Scan Settings"
- p.151 "Adjusting Image Density"
- p.152 "Setting of Original Feed Type"
- p.160 "Specifying the File Type and File Name"
- p.61 "Specifying Scan to Folder Destinations"
- p.14 "Check Modes"
- p.15 "Preview"
- p.74 "Simultaneous Storage and Sending by Scan to Folder"

Switching to the Scan to Folder Screen

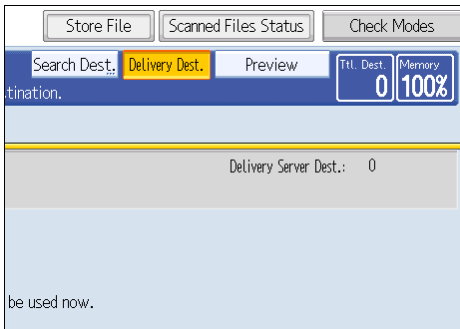
This section explains how to switch to the Scan to Folder screen.

If the E-mail screen is being displayed, press the [Folder] tab to switch to the Scan to Folder screen.

If the network delivery scanner screen is being displayed, switch to the Scan to Folder screen as follows:

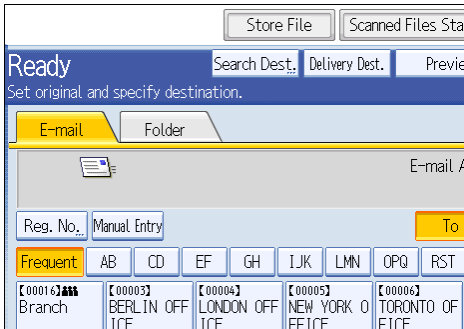
2

1. Press [Delivery Dest.].



The E-mail screen or Scan to Folder screen appears.

2. If the E-mail screen appears, press the [Folder] tab.



The Scan to Folder screen appears.

↓ Note

- You cannot switch from the network delivery scanner screen or other screens while destinations are being specified. To clear the specified destination, display the destination in the destination field, and then press the [Clear/Stop] key.
- If you are scanning files using WSD, [Swch Dest.List] or [WSD Dest.] appears instead of [Delivery Dest.]. To switch to the Scan to Folder screen, press [Swch Dest.List], and then, on the screen that appears, press [E-mail / Folder], or press [WSD Dest.].

Specifying Scan to Folder Destinations

This section explains how to specify Scan to Folder destinations.

You can send a file by Scan to Folder by any of the following methods:

- Select a destination registered in the machine's address book
- Send a file to a shared network folder
- Send a file to an FTP server
- Send a file to a NetWare server

↓ Note

- You can specify multiple destinations.

Selecting the Destination from the Machine's Address Book

This section explains how to select the destination from the machine's address book.

★ Important

- **To use this function, you must register the destinations in [System Settings] in advance.**

You can select a destination registered in the machine's address book by any of the following methods:

- Select the destination from the destination list
- Select the destination by entering its registration number
- Select the destination by searching the machine's address book

↓ Note

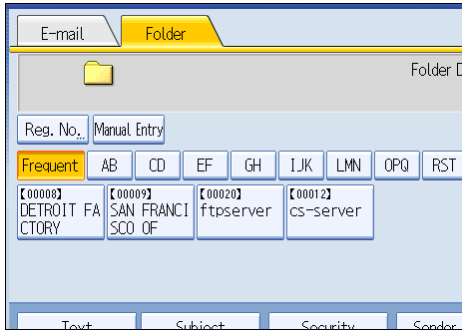
- If you have specified the address protection code for accessing the address book, the screen for entering the address protection code appears. Enter the protection code, and then press [OK]. If the protection code you entered is correct, you can specify Scan to Folder destinations from the address book.
- Depending on the security setting, some destinations may not appear in the destination list.

Selecting a destination registered in the destination list

Select the destination from the destination list.

1. **In the destination list, press the key including the destination name.**

The key of the selected destination is highlighted, and the destination appears in the destination field at the top of the screen.



If the target destination does not appear, take one of the following steps:

- Display the destination by selecting its initial letter from the title
- Display the destination by pressing [▲] or [▼]

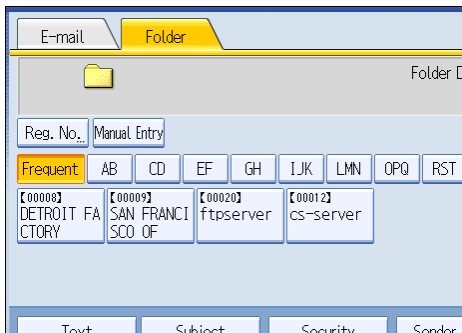
↓ Note

- Depending on the security setting, some destinations may not appear in the destination list.

Selecting destinations by entering the registration numbers

Select the destination from the machine's address book using its registration number.

1. Press [Reg. No.].



2. Enter the five-digit registration number that has been assigned to a destination folder using the number keys.

If the entered number is less than five digits, press the [#] key after the last number.

Example: To enter 00004

Press the [4] key, and then press the [#] key.

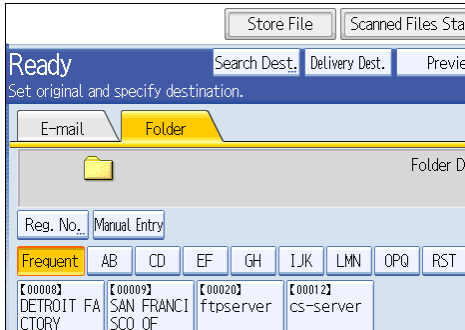
By pressing [Change], you can change the selected destination.

3. Press [OK].

Searching the machine's address book for the destination and selecting it

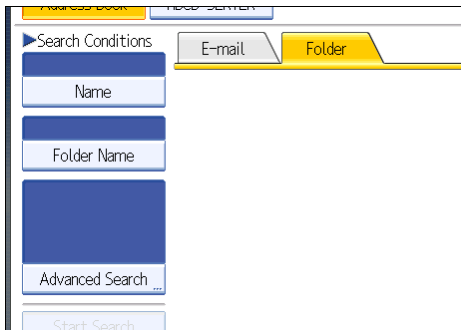
This section explains how to search the machine's address book for the destination and select it.

1. Press [Search Dest.].



2. To search by destination name, press [Name].

To search by path, press [Folder Name].



The soft keyboard appears.

You can also search by combining [Name] and [Folder Name].

3. Enter the beginning of the destination name.

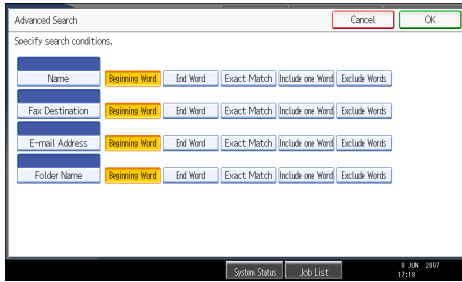
To search by path, enter the beginning of the path.

4. Press [OK].

5. If necessary, press [Advanced Search] to specify the detailed search criteria, and then press [OK].

By pressing [Advanced Search], you can search using criteria such as [Name], [Fax Destination], [E-mail Address], and [Folder Name].

You can specify search criteria such as [Beginning Word] or [End Word]. You can refine your search using multiple criteria.



The illustrated screen is an example. The items that actually appear on the screen may differ.

6. Press [Start Search].

Destinations that match the search criterion are displayed.

7. Select the destination folder.

8. Press [OK].

Note

- Search criteria that appear in [Advanced Search], such as [Name], [Fax Destination], [E-mail Address], and [Folder Name], are registered in the machine's address book. For details, see "Registering Addresses and Users for Facsimile/Scanner Functions", Network and System Settings Guide.
- By pressing [Details], you can view details about the selected destinations.
- Up to 100 destinations can be displayed as search results.
- By pressing [Advanced Search], the following criteria appear:
 - [Beginning Word]: The names which start with the entered character or characters are targeted. For example, to search for "ABC", enter "A".
 - [End Word]: The names which end with the entered character or characters are targeted. For example, to search for "ABC", enter "C".
 - [Exact Match]: The names which correspond to an entered character or characters are targeted. For example, to search for "ABC", enter "ABC".
 - [Include one Word]: The names which contain an entered character or characters are targeted. For example, to search for "ABC", enter "A", "B", or "C".
 - [Exclude Words]: The names which do not contain an entered character or characters are targeted. For example, to search for "ABC", enter "D".

Sending Files to a Shared Network Folder

This section explains how to specify the destination when sending files to a shared network folder.

★ Important

- The shared folder must have been created on the client computer in advance. For details about creating shared folders, see Windows Help.
- You can create the shared folder under Windows 98/Me/2000/XP/Vista, Windows NT 4.0, Windows Server 2003/2003 R2/2008, and Mac OS X 10.2 or later.
- Depending on the operating system of the client computer, access to the shared folder may require authentication.
- This machine does not support DFS (Distributed File System).

2

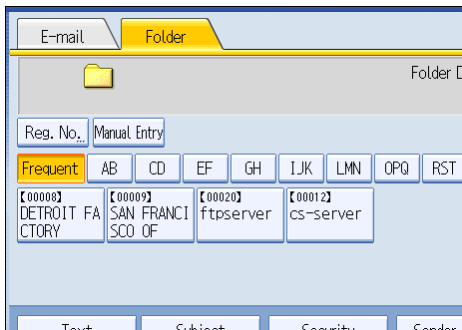
You can send a file to a shared folder over the network by any of the following methods:

- Enter the path to the destination directly
- Specify the path by browsing the network for the destination

Entering the path to the destination manually

You can enter the path to the destination folder manually.

1. Press [Manual Entry].



2. Press [SMB].

3. Press [Manual Entry] on the right side of the path field.

The soft keyboard appears.

4. Enter the path for the folder.

The following is an example of a path where the folder name is "user" and the computer name is "desk01": \\desk01\user.

Instead of the computer name, you can also use its IPv4 address.

5. Press [OK].

6. Depending on the destination setting, enter the user name for logging on to the computer.

Press [Manual Entry] to the right of the user name field to display the soft keyboard.

7. Depending on the destination setting, enter the password for logging on to the computer.

Press [Manual Entry] for the password to display the soft keyboard.

8. Press [Connection Test].

A connection test is performed to check whether the specified shared folder exists.

If the message "Connection with PC has failed. Check the settings." appears, see "Troubleshooting When Using the Scanner Function", Troubleshooting.

9. Check the connection test result, and then press [Exit].

10. Press [OK].

Note

- If authentication is required to access the folder, the login screen appears. Enter the user name and password.
- If you change the protocol after entering the path name, user name, or password, a confirmation message appears.
- To change the path for the folder that has been entered, press [Edit] on the left side of the destination field. Enter the correct path for the folder, and then press [OK].
- The connection test may take time.
- You may not be able to press [Connection Test] right after pressing [Cancel] during a connection test.
- Even if the connection test was successful, the machine may fail to transfer the file if you do not have write privileges for the file or there is not enough free hard disk space.
- You can register the path to the destination in the machine's address book. For details, see "Registering the Path to the Selected Destination in the Address Book".

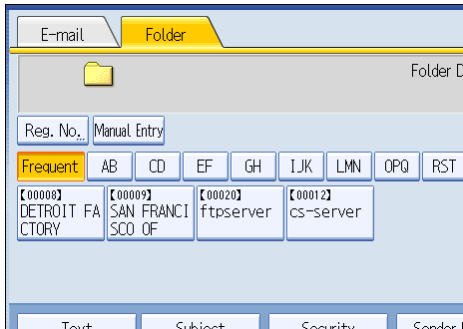
Reference

- p.73 "Registering the Path to the Selected Destination in the Address Book"

Specifying the path by browsing the network for destinations

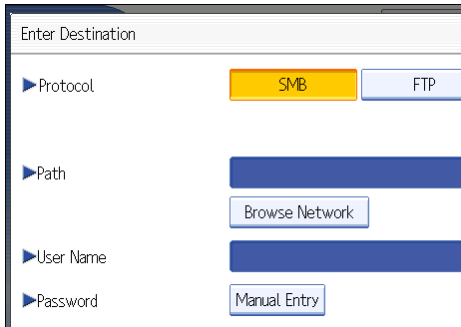
You can browse computers on the network for the destination folder, and then specify the path.

1. Press [Manual Entry].



2. Press [SMB].

3. Press [Browse Network] under the path name field.



Domains or workgroups on the network appear.

If the message "Cannot find the specified path. Please check the settings." appears, see "Troubleshooting When Using the Scanner Function", Troubleshooting.

4. Select the domain or workgroup in which the destination folder is located.

5. Select the client computer that has the destination folder.

If you cannot find the computer you are looking for, press [Up One Level] and browse that level.

If authentication is required to access the selected computer, the authentication screen appears. To authenticate, enter the user name and password.

6. Select the destination folder.

When the selected folder has sub-folders, the sub-folders list appears.

If you cannot find the destination folder, press [Up One Level], and then search for the folder at that level.

7. Press [OK] twice.

↓ Note

- If authentication is required to access the folder, the login screen appears. Enter the user name and password.

- If you change the protocol after entering the path name, user name, or password, a confirmation message appears.
- Up to 100 computers or shared folders can be displayed.
- The machine may fail to transfer the file if you do not have the write privileges for the shared folder or there is not enough free hard disk space.
- You can register the path to the destination in the machine's address book. For details, see "Registering the Path to the Selected Destination in the Address Book".

Reference

- p.73 "Registering the Path to the Selected Destination in the Address Book"

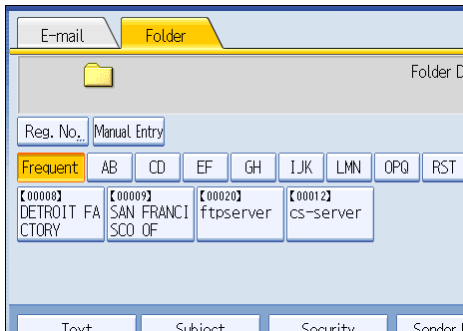
Sending Files to an FTP Server

This section explains how to specify destinations when sending files to an FTP server.

Entering the path to an FTP server manually

You can enter the path to an FTP server manually.

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



2. Press **[FTP]**.
3. Press **[Manual Entry]** on the right side of the server name field.
The soft keyboard appears.
4. Enter a server name.
Instead of the server name, you can also use its IPv4 address.
5. Press **[OK]**.
6. Press **[Manual Entry]** on the right side of the path field.

7. Enter the path for the folder.

The following is an example of a path where the folder name is "user" and the subfolder name is "lib":
user\lib.

8. Press [OK].**9. Enter the user name according to the setting at the destination.**

Press [Manual Entry] to the right of the user name field to display the soft keyboard.

10. Enter the password according to the setting at the destination.

Press [Manual Entry] next to the password field to make the soft keyboard appear.

11. To change the port number which is set in [System Settings], press [Change] on the right side of the port number field. Enter a port number using the number keys, and then press the [#] key.**12. Press [Connection Test].**

A connection test is performed to check whether the specified folder exists.

If the message "Connection with PC has failed. Check the settings." appears, see "Troubleshooting When Using the Scanner Function", Troubleshooting.

13. Check the connection test result, and then press [Exit].**14. Press [OK].****Note**

- If you change the protocol after entering the path name, user name, or password, a confirmation message appears.
- The connection test may take time.
- You may not be able to press [Connection Test] right after pressing [Cancel] during a connection test.
- To change the registered path to a destination folder, press [Edit] to the left of the destination field to display the soft keyboard, enter the new path, and then click [OK].
- You can register the path to the destination in the machine's address book. For details, see "Registering the Path to the Selected Destination in the Address Book".
- The machine may fail to transfer the file if you do not have write privileges for the folder or there is not enough free hard disk space.

Reference

- p.73 "Registering the Path to the Selected Destination in the Address Book"

Sending Files to NetWare Server

This section explains how to specify destinations when sending files to a NetWare server.

The NetWare folder of the destination can be specified in an NDS tree or on a NetWare Bindery server, depending on the NetWare environment. Consult your administrator.

You can send a file to NetWare server by any of the following methods:

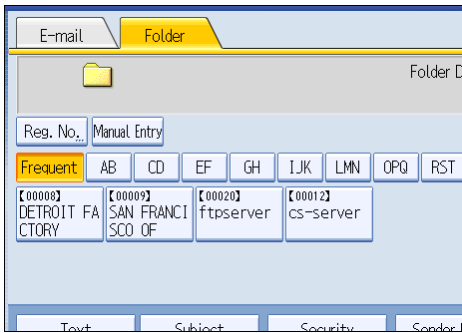
- Enter the destination path of the Netware server directly
- Specify the path by browsing to the destination on the Netware server

2

Entering the path of the NetWare server directly

You can enter the path of the NetWare server.

1. Press [Manual Entry].



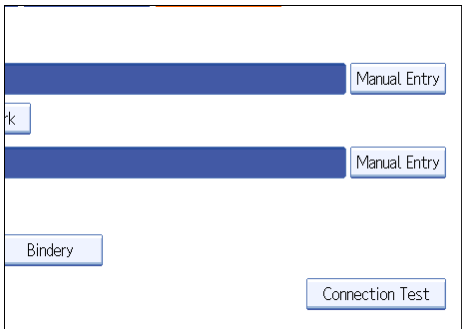
2. Press [NCP].

3. Select the connection type.

Press [NDS] to specify the folder in the NDS tree.

Press [Bindery] to specify the folder on the NetWare Bindery server.

4. Press [Manual Entry] on the right side of the path field.



The soft keyboard appears.

5. Enter the path for the folder.

If you set the connection type to [NDS], and when the NDS tree name is "tree", the name of the context including the volume is "context", the volume name is "volume", and the folder name is "folder", the path will be "\\tree\volume.context\folder".

If you set the connection type to [Bindery], and when the NetWare server name is "server", the volume name is "volume", and the folder name is "folder", the path will be "\\server\volume\folder".

6. Press [OK].**7. Enter the user name for logging on to the NDS tree or NetWare Bindery server.**

Press [Manual Entry] to the right of the user name field. The soft keyboard appears.

If you press [NDS] for [Connection Type], enter the user name, and then enter the name of the context containing the user object. If the user name is "user" and the name of the Context is "context", the user name will be "user.context".

8. If a password is specified for the log on user, enter it.

Press [Manual Entry] to the right of the password field. The soft keyboard appears.

9. Press [Connection Test].

A connection test is performed to check whether the specified folder exists.

If the message "Connection with PC has failed. Check the settings." appears, see "Troubleshooting When Using the Scanner Function", Troubleshooting.

10. Check the connection test result, and then press [Exit].**11. Press [OK].****Note**

- If you change the protocol after entering the path name, user name, or password, a confirmation message appears.
- To change a registered path to a destination folder, press [Edit] to the left of the destination field to display the soft keyboard, enter the correct path to the folder, and then press [OK].
- You can connect only to folders that you have the read privileges for.
- The connection test may take time.
- You may not be able to press [Connection Test] right after pressing [Cancel] during a connection test.
- Even if the connection test was successful, the machine may fail to transfer the file if you do not have write privileges for the file or there is not enough free hard disk space.
- You can register the path to the destination in the machine's address book. For details, see "Registering the Path to the Selected Destination in the Address Book".

Reference

- p.73 "Registering the Path to the Selected Destination in the Address Book"

Specify the path by browsing to the destination on the Netware server

Specify the path by browsing to the destination folder in an NDS tree or on a NetWare Bindery server.

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

2. Press **[NCP]**.

3. Select the connection type.

Press **[NDS]** to specify a folder in the NDS tree.

Press **[Bindery]** to specify a folder on the NetWare Bindery server.

4. Press **[Browse Network]** under the path name field.

The screenshot shows a dialog box with the following fields and buttons:

- Path:** A text input field with a blue bar above it and a "Browse Network" button below it.
- User Name:** A text input field with a blue bar above it.
- Password:** A text input field with a "Manual Entry" button below it.
- Connection Type:** Two buttons, "NDS" (highlighted in yellow) and "Bindery" (light blue).

If you selected **[NDS]** under **[Connection Type]**, the NDS tree list appears.

If you selected **[Bindery]** under **[Connection Type]**, the NetWare Bindery server list appears.

5. Search for the destination folder in the NDS tree or NetWare Bindery server.

If you cannot find the destination folder, press **[Up One Level]**, and then search for the folder at that level.

6. Select the destination folder.

7. Press **[OK]** twice.

↓ Note

- If you change the protocol after entering the path name, user name, or password, a confirmation message appears.
- Only folders that you have the read privileges for are displayed.
- If the language used for the NDS tree or by the NetWare Bindery server differs from that used by the machine, file names in the NDS tree or on the NetWare Bindery server might appear garbled.
- Up to 100 items can be displayed.
- If the selected NDS tree or NetWare Bindery server requires authentication, a login screen appears. Enter a user name and password for logging on to the NDS tree or NetWare Bindery server. If you log on to the NDS tree, enter a user name, and then enter the name of the context containing the user object. If the user name is "user" and the name of the Context is "context", the user name will be "user.context".

- The machine may fail to transfer the file if you do not have write privileges for the folder or there is not enough free hard disk space.
- You can register the path to the destination in the machine's address book. For details, see "Registering the Path to the Selected Destination in the Address Book".

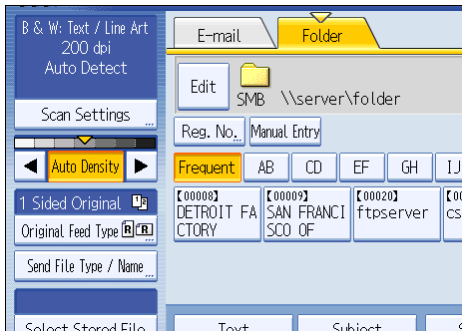
Reference

- p.73 "Registering the Path to the Selected Destination in the Address Book"

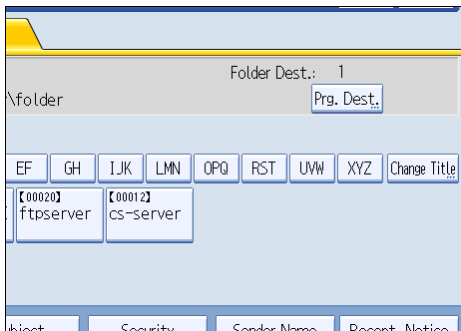
Registering the Path to the Selected Destination in the Address Book

This section explains how to register folder paths you have entered manually or specified by browsing the network to the machine's address book.

1. In the destination field, display the destination you want to register.



2. Press [Prg. Dest.].



3. Press [Names], and then specify the name and other information to be registered.

For details about specifying the information to be registered, see "Registering Addresses and Users for Facsimile/Scanner Functions", Network and System Settings Guide.

4. Press [OK].

Note

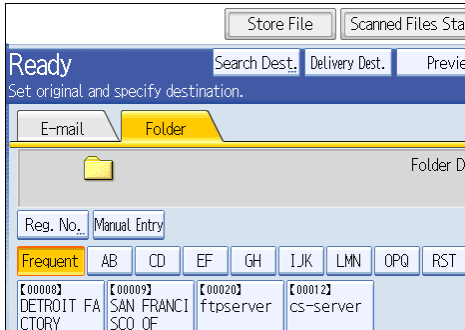
- Depending on the security setting, [Prg. Dest.] may not appear.

Simultaneous Storage and Sending by Scan to Folder

This section explains how to store a file and simultaneously send it by Scan to Folder.

2

1. Press [Store File].



2. Make sure that [Store to HDD + Send] is selected.

3. If necessary, specify the stored file's information, such as [User Name], [File Name], and [Password].

For details, see "Specifying File Information for a Stored File".

4. Press [OK].

5. Specify the setting for sending the file by Scan to Folder, and then send the file.

For details about sending a file by Scan to Folder, see "Basic Procedure When Using Scan to Folder".

6. Press the [Start] key.

Note

- Depending on the security setting, [Access Privileges] may appear instead of [User Name]. For details about specifying [Access Privileges], consult the administrator.
- You can resend stored files by Scan to Folder. To resend stored files, select the files on the Select Stored File screen, and then send them. For details, see "Sending a Stored File".

Reference

- p.93 "Specifying File Information for a Stored File"
- p.58 "Basic Procedure When Using Scan to Folder"
- p.102 "Sending a Stored File"

3. Sending Scan Files Using WSD

If your computer has a WSD-compliant operating system such as Windows Vista, it can receive scan files sent using WSD. After you have configured the necessary settings, you can send scan files simply by connecting your computer to the network.

Before Sending Scan Files Using WSD

This section explains the preparation and procedure for sending scan files using Web Services on Devices (WSD).

★ Important

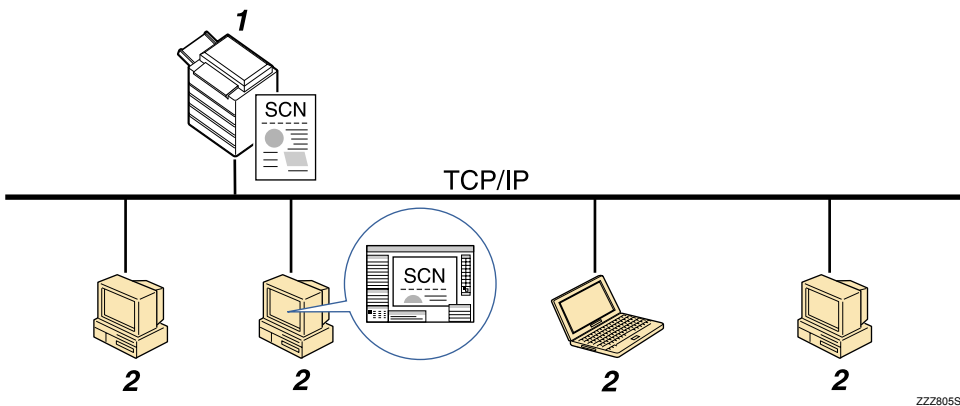
- This function is available only if your computer has a WSD-compliant operating system such as Windows Vista. Check your computer's settings before using the WSD scanner.
- The example explanations shown in this manual are based on Windows Vista Ultimate.
- To begin a scan job, press the [Start] key on the machine. Note that you cannot scan documents from client computers.
- If a personal authentication function is configured, the WSD scanner function will be automatically disabled. To perform WSD scanning again, you must enable the WSD scanner function. For details about making this setting, see "Enabling WSD using Web Image Monitor".

📖 Reference

- p.77 "Enabling WSD using Web Image Monitor"

Overview of Sending Scan Files Using WSD

This section describes the process of sending scan files using WSD.



ZZZ805S

1. This machine

From this machine you can send scan files to WSD-compliant client computers.

2. Client computers (WSD-compliant)

WSD-compliant computers receive the sent scan files via the network.

Preparation for Sending Files Using WSD

To send scanned files using WSD, you must first perform the following:

- Check the machine is properly connected to the network
- Configure the network settings in [System Settings]
- Enable WSD using Web Image Monitor
- Register the machine to a client computer

3

Checking the machine is properly connected to the network

Check that this machine is properly connected to the network.

For details about how to connect this machine to a network, see "Connecting to the Interface", Network and System Settings Guide.

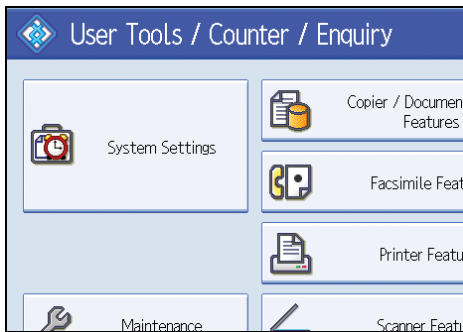
Configuring the network settings in [System Settings]

Configure the network settings in [System Settings] according to your environment and how you will be using the machine.

The following procedure explains connecting this machine to an IPv4 network using Ethernet cable.

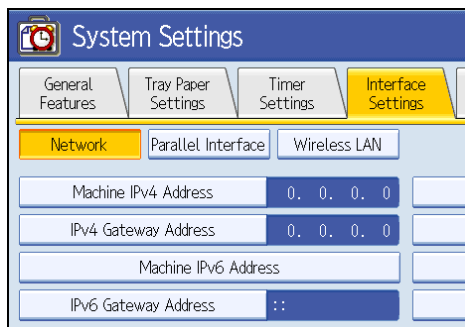
Note that the settings you must configure will vary depending on your operating environment. For details about network settings and configuration procedures, see "Network Settings Required to Use WSD Scanner", Network and System Settings Guide.

1. Press the [User Tools/Counter] key, and then press [System Settings].



The System Settings screen appears.

2. Press the [Interface Settings] tab.



3. Press [Machine IPv4 Address] to specify the machine's IPv4 address.

To specify a static IPv4 address for this machine, press [Specify], and then enter the IPv4 address and subnet mask.

To obtain an IPv4 address from a DHCP server automatically, press [Auto-Obtain (DHCP)].

4. Press [IPv4 Gateway Address], and then enter the IPv4 gateway address.

5. Press [Effective Protocol], and then make [IPv4] active.

6. Press [Exit] twice.

↓ Note

- If an extended wireless LAN board (optional) is installed, press [LAN Type] on the [Interface Settings] tab, then press [Ethernet], and then configure the network settings.

Enabling WSD using Web Image Monitor

To use this machine as a WSD scanner, you must first configure the following settings using Web Image Monitor on a client computer:

- WSD scanner function (default setting: [Off])
Click [Configuration], click [Initial Settings] under [Scanner], and then set [WSD (Scanner)] to [On].
- WSD protocol (default setting: [Active])
Click [Configuration], click [IPv4] or [IPv6] under [Network], and then enable [WSD (Scanner)].

Use the following procedure to set the WSD scanner function to [On].

1. On the [Start] menu, click [Network].

2. Double-click the icon for this machine.

3. Click [Login].

The Web Image Monitor login page appears.

4. Enter your login user name and password in the [Login User Name] and [Login Password] boxes respectively, and then click [Login].

Consult your administrator if you require a login user name and password.

5. On the menu in the left frame, click [Configuration].

6. Under [Scanner], click [Initial Settings].

The [Initial Settings] page appears.

7. Set [WSD (Scanner)] to [On].

8. Click [OK].

↓ Note

- For details about displaying Web Image Monitor, see "Monitoring and Configuring the Printer", Network and System Settings Guide. For details about using Web Image Monitor, see Web Image Monitor Help.

Registering the machine to a client computer

Use the following procedure to register this machine to a client computer.

★ Important

- You must log on as an Administrators group member to register the machine.
- The client computer cannot detect the machine if they are on different network segments or if the Windows Vista's Network Search setting is disabled. For details, see Windows Help.

1. On the [Start] menu, click [Network].

The [Network] window appears and the device search starts automatically.

2. Right-click the icon for this machine, and then click [Install].

The [User Account Control] dialog box appears.

3. Click [Continue].

↓ Note

- If the message "Found New Hardware" appears, install the printer driver using the procedure shown under "Installing the Printer Driver", Printer Reference.
- When registration is complete, the scan profile is created automatically. To change the scan profile, see "Changing a Scan Profile".

📖 Reference

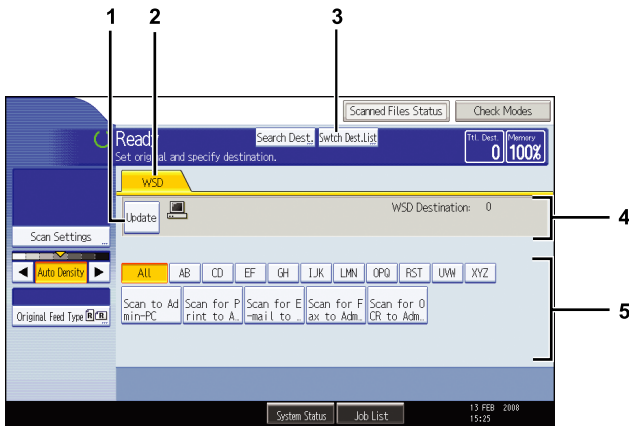
- p.86 "Changing a Scan Profile"

WSD Scanner Screen

This section explains the layout of the screen that allows you to send scan files using WSD.

The function items displayed serve as selector keys. You can select or specify an item by pressing it.

When you select or specify an item on the display panel, it is highlighted like [**Set**]. Keys that cannot be selected appear like [**OK**].



BHF001S

1. [Update]

Press this key to update the destination list.

2. WSD

This tab is highlighted whenever the machine is used as a WSD scanner.

3. [Swch Dest.List]

Press this key to switch from the screen that is currently displayed to the WSD scanner screen.

If you are not using the network delivery function, [WSD Dest.] appears instead of [Swch Dest.List].

4. Destination field

The specified destination is displayed here. You can specify only one destination.

5. Destination List

The list of available destinations is displayed here.

If all of the destinations cannot be displayed, press [▲] or [▼] to move through the list.

Basic Procedure for Sending Scan Files Using WSD

This section explains the basic procedure for sending scan files using WSD.

★ Important

- If the message "Updating the destination list has failed. Try again?" appears, press [OK]. The destination list will then be updated.

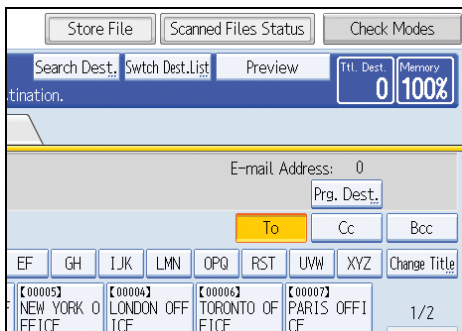
3

1. Make sure that no previous settings remain.

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

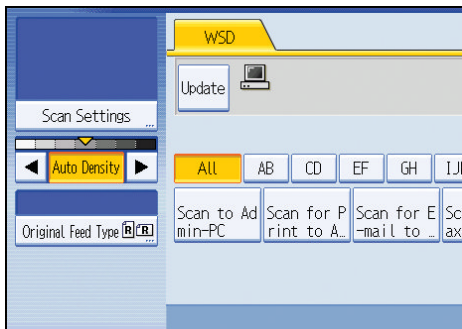
2. If the E-mail screen, Scan to Folder screen, or network delivery scanner screen is displayed, switch to the WSD scanner screen.

For details, see "Switching to the WSD Scanner Screen".



3. Place originals.

4. If necessary, press [Scan Settings] to configure the scan settings.



Note that only [Erase Border] can be specified directly from this machine. Use the client computer to configure the other scan settings. For details, see "Changing a Scan Profile".

5. If necessary, specify the scanning density.

For details, see "Adjusting Image Density".

6. If necessary, press [Original Feed Type] to configure the original orientation settings.

For details, see "Setting of Original Feed Type".

7. Specify the destination.

For details, see "Specifying the Destination Client Computer".

8. Press the [Start] key.

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

Note

- If you are using this machine as a WSD scanner, you can specify only one destination per scan job.
- You cannot preview scanned images. After pressing the [Start] key, you can view the scanned images on your computer.
- To cancel a specified destination, press the destination again, or press the [Clear/Stop] key.
- To cancel scanning, press the [Clear/Stop] key.
- You cannot store files scanned using WSD on the machine.
- You cannot use WSD to send files stored on the machine.
- You cannot scan originals while other originals are being scanned.
- Two-sided originals are scanned for sideways opening (top-to-top orientation).
- If scanning takes too long, the client computer might time out, causing the error message "Automatic Scanning could not be completed" to appear. If this happens, the scan files are sent again. Depending on the settings of the client computer, you might have to perform a procedure on the client computer directly. To check the files have been sent successfully, use the machine's Scanned Files Status screen or a client computer. For details, see "Scanned Files Status".
- If scanning does not begin after you press the [Start] key, the machine might not be registered to the computer or the profile might be incorrectly configured. For details, see "Registering the machine to a client computer" or "Creating a New Scan Profile".
- After scan files are sent, their destination settings are automatically cleared. If you want to preserve this information, contact your local dealer for details.

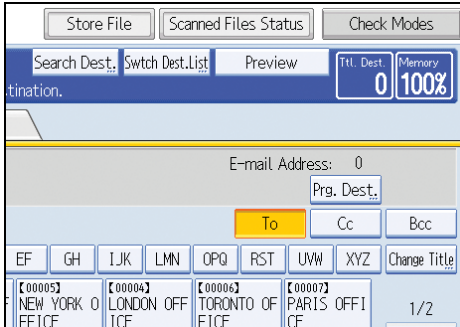
Reference

- p.82 "Switching to the WSD Scanner Screen"
- p.86 "Changing a Scan Profile"
- p.151 "Adjusting Image Density"
- p.152 "Setting of Original Feed Type"
- p.83 "Specifying the Destination Client Computer"
- p.17 "Scanned Files Status"
- p.78 "Registering the machine to a client computer"
- p.87 "Creating a New Scan Profile"

Switching to the WSD Scanner Screen

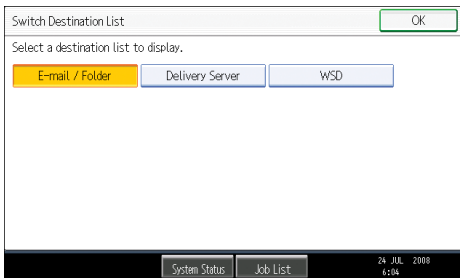
This section explains how to switch from the screen that is currently displayed to the WSD scanner screen. When the E-mail screen, Scan to Folder screen, or network delivery screen is displayed, you can use the following procedure to switch to the WSD scanner screen.

1. Press [Swch Dest.List].



The [Switch Destination List] screen appears.

2. Press [WSD], and then press [OK].



The WSD scanner screen appears.

↓ Note

- You cannot switch the screen while e-mail or other destinations are being specified. To clear a specified destination, display the destination in the destination field of each screen, and then press the [Clear/Stop] key.
- If you are not using the network delivery function, [WSD Dest.] is displayed instead of [Swch Dest.List]. Press [WSD Dest.] to switch to the WSD scanner screen.
- [Swch Dest.List] or [WSD Dest.] is displayed only when the WSD scanner function is set to [On] using Web Image Monitor. For details about making this setting, see "Preparation for Sending Files Using WSD".

📖 Reference

- p.76 "Preparation for Sending Files Using WSD"

Specifying the Destination Client Computer

This section explains how to specify a destination client computer for the scan files you are sending by WSD.

You can specify the destination computer using either of the following methods:

- Selecting a destination computer from the destination list
- Searching for a destination computer and then selecting it

★ Important

- If you are using this machine as a WSD scanner, you can specify only one destination per scan job.

3

Selecting a Destination Client Computer from the Destination List

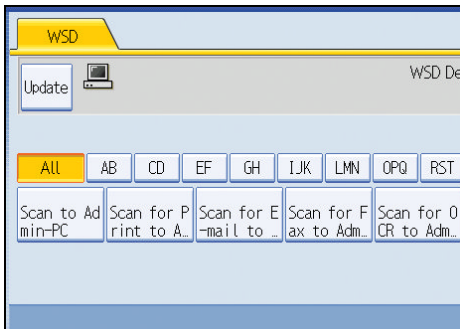
Use the following procedure to select a destination client computer from the destination list.

Destinations appear in the destination list after you log on to your computer.

★ Important

- If the destination computer does not appear but the machine is already registered to the destination computer, press [Update]. This will update the destination list with the latest information.

1. In the destination list, press the destination computer that you want to send to.



The key of the selected destination client computer is highlighted, and the destination appears in the destination field at the top of the screen.

↓ Note

- In the destination list, each destination client computer is displayed using up to 20 characters.
- We recommend you register easily recognizable computer names.
- If a WSD-compatible computer is connected to the network, the following five destinations appear on the display panel automatically. For details about the saving location of files in each destination, see the relevant computer's settings.

3

- Scan to "Computer Name"
- Scan for Print to "Computer Name"
- Scan for E-mail to "Computer Name"
- Scan for Fax to "Computer Name"
- Scan for OCR to "Computer Name" (Scan for OCR to "Computer Name" might not be available depending on the destination client computer.)
- If the target destination does not appear, take one of the following steps:
 - Display the destination by selecting the initial letter of its title
 - Display the destination by pressing [▲] or [▼]
- You can also search for the destination by pressing [Search Dest.]. For details, see "Searching for a Destination Client Computer".
- The destination list can display up to 250 client computer destinations.

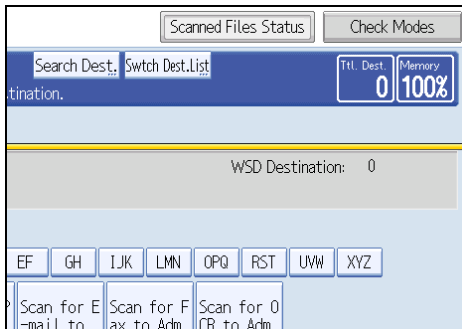
Reference

- p.84 "Searching for a Destination Client Computer"

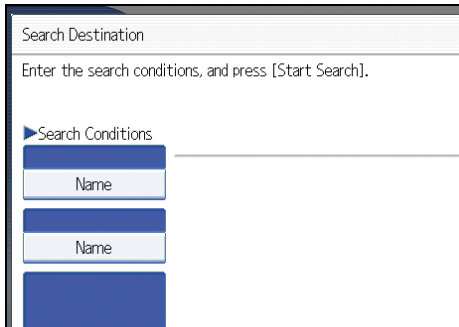
Searching for a Destination Client Computer

Use the following procedure to search for a destination client computer and select it.

1. Press [Search Dest.].



2. Press [Name].



The soft keyboard appears.

3. Enter the search characters, and then press [OK].

4. If necessary, press [Advanced Search] to specify the detailed search criteria.

You can specify up to three search criteria. You can specify [Beginning Word] or [End Word] as the matching criterion. You can refine your search using multiple criteria.

5. Press [OK].

6. Press [Start Search].

Destinations that match the search criteria are displayed.

7. Select a destination, and then press [OK].

↓ Note

- Search targets are computer names.
- By pressing [Details], you can view details about the selected destinations.
- Up to 100 destinations can be displayed as search results.
- By pressing [Advanced Search], the following criteria appear:
 - [Beginning Word]: The names which start with the entered character or characters are targeted. For example, to search for "ABC", enter "A".
 - [End Word]: The names which end with the entered character or characters are targeted. For example, to search for "ABC", enter "C".
 - [Exact Match]: The names which correspond to an entered character or characters are targeted. For example, to search for "ABC", enter "ABC".
 - [Include one Word]: The names which contain an entered character or characters are targeted. For example, to search for "ABC", enter "A", "B", or "C".
 - [Exclude Words]: The names which do not contain an entered character or characters are targeted. For example, to search for "ABC", enter "D".

Changing a Scan Profile

This section explains how to change a scan profile. A scan profile contains scan settings specified on a client computer.

Whenever the machine is first registered to a computer, a profile is created automatically. Using the following procedure, you can change this profile on the computer.

1. On the [Start] menu, click [Control Panel].

Control Panel opens.

2. Click [Hardware and Sound].

You do not have to perform this step depending on the Control Panel settings.

3. Click [Scanners and Cameras].

The [Scanners and Cameras] dialog box appears.

4. Select this machine, and then click [Scan Profiles].

The [Scan Profiles] dialog box appears.

5. Select a profile, and then click [Edit].

The [Edit Profile] dialog box appears.

6. Configure the necessary settings.

7. Click [Save Profile].

The changed scan settings are saved as a profile.

The following table tells you the scan profile settings that you can configure.

Scan Profile Items and Settings

Item	Scan settings
Profile name:	Enter the profile name.
Source:	Select one of the following: Flatbed Feeder (Scan one side) Feeder (Scan both sides)
Paper size:	If you select [Feeder (Scan one side)] or [Feeder (Scan both sides)] in [Source], you must specify the paper size.

Item	Scan settings
Color format:	Select one of the following: Color Grayscale Black and white
File type:	Select one of the following: BMP (Bitmap Image) JPG (JPEG Image) PNG (PNG Image) TIF (TIFF Image)
Resolution (DPI):	Specify the resolution.
Brightness:	The setting you specify here will not be applied for scanning.
Contrast:	The setting you specify here will not be applied for scanning.

↓ Note

- If a profile does not appear in the [Scanners and Cameras] dialog box, the associated machine might be turned off, or the required WSD scanner settings might not have been specified. For details about WSD scanner settings, see "Preparation for Sending Files Using WSD".
- If a profile does not appear in the [Scan Profiles] dialog box, recreate it as a new profile. For details, see "Creating a New Scan Profile".
- You can create multiple profiles.
- You cannot use [Preview] in the [Edit Profile] dialog box.

📖 Reference

- p.76 "Preparation for Sending Files Using WSD"
- p.87 "Creating a New Scan Profile"

Creating a New Scan Profile

Use the following procedure to create a new profile.

1. On the [Start] menu, click [Control Panel].

Control Panel opens.

2. Click [Hardware and Sound].

You do not have to perform this step depending on the Control Panel settings.

3. Click [Scanners and Cameras].

The [Scanners and Cameras] dialog box appears.

4. Select this machine, and then click [Scan Profiles].

The [Scan Profiles] dialog box appears.

5. Click [Add].

The [Add New Profile] dialog box appears.

6. Configure the necessary settings for the profile.

7. Click [Save Profile].

The scan settings are saved as a new profile.

Note

- You can register multiple profiles. If multiple profiles are registered, the profile specified as default in the [Scan Profiles] dialog box is applied.
- To specify a scan profile as the default profile, perform one of the following procedures:
 - In the [Scan Profiles] dialog box, click the scan profile, and then click [Set as Default].
 - After you create a new scan profile, in the [Add New Profile] dialog box, select the [Set this profile as default] check box.

4. Storing Files Using the Scanner Function

Using the scanner function, you can store scan files in the machine and then send the stored files by e-mail or Scan to Folder.

Before Storing Files

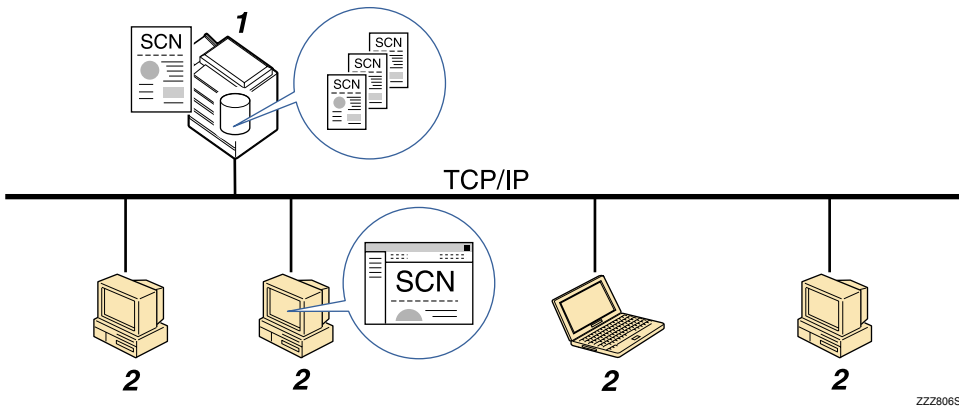
This section outlines file storage under the scanner function and provides related cautions.

Overview of File Storage under the Scanner Function

This section describes the process of storing files under the scanner function.

★ 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.



ZZZ806S

1. This Machine

You can store scan files on the machine's hard disk. The stored files can be sent by e-mail, Scan to Folder, or the network delivery scanner.

2. Client Computer

Using DeskTopBinder, you can, over the network, view, copy, or delete files stored in the machine. Using Web Image Monitor, you can, over the network, view, download, send, or delete files stored in the machine. For

details about DeskTopBinder Lite, see DeskTopBinder Lite-related manuals. For details about Web Image Monitor, Web Image Monitor Help.

Note

- Stored files will be deleted after a set period. For details about specifying the period, see "Administrator Tools", Network and System Settings Guide.
- Files stored under the scanner function cannot be printed from the machine's control panel. Print the files from a client computer after receiving them on the computer.
- You can also store a file and simultaneously send it. For details, see "Simultaneous Storage and Sending by E-mail", "Simultaneous Storage and Sending by Scan to Folder", and "Simultaneous Storage and Delivery".
- If a media slot (optional) is installed on the machine, you can save scan files on a removable memory device. For details, see "Basic Procedure for Saving Scan Files on a Removable Memory Device".

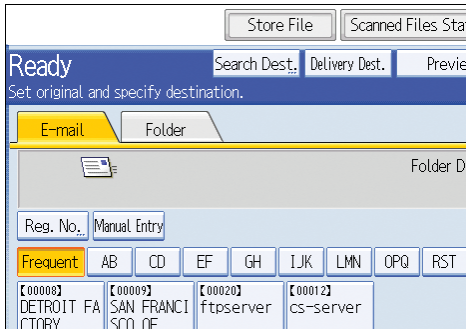
Reference

- p.45 "Simultaneous Storage and Sending by E-mail"
- p.74 "Simultaneous Storage and Sending by Scan to Folder"
- p.132 "Simultaneous Storage and Delivery"
- p.111 "Basic Procedure for Saving Scan Files on a Removable Memory Device"

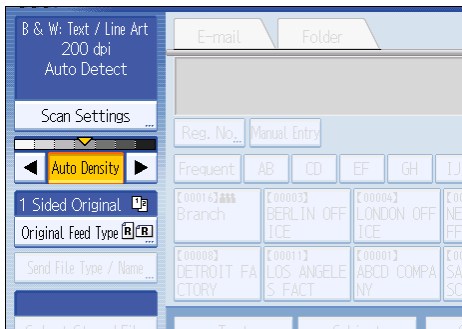
Basic Procedure for Storing Scan Files

This section explains the basic procedure for storing scan files.

1. **Make sure that no previous settings remain.**
If a previous setting remains, press the [Clear Modes] key.
2. **Place originals.**
3. **Press [Store File].**



4. **Press [Store to HDD].**
5. **If necessary, specify file information, such as [User Name], [File Name], and [Password].**
For details, see "Specifying File Information for a Stored File".
6. **Press [OK].**
7. **If necessary, press [Scan Settings] to specify scanner settings such as resolution and scan size.**
For details, see "Various Scan Settings".



8. **If necessary, specify the scanning density.**
For details, see "Adjusting Image Density".
9. **If necessary, press [Original Feed Type] to specify settings such as original orientation.**
For details, see "Setting of Original Feed Type".

10. Press the [Start] key.

If you are scanning batches, place the next originals.

↓ Note

- Depending on the security setting, [Access Privileges] may appear instead of [User Name]. For details about specifying [Access Privileges], consult the administrator.
- By pressing [Store to HDD + Send], you can simultaneously store scan files and send them. For details, see "Simultaneous Storage and Sending by E-mail", "Simultaneous Storage and Sending by Scan to Folder", and "Simultaneous Storage and Delivery".
- You cannot press [Store File] if:
 - "PDF" is selected as the file type and security is applied
 - High Compression PDF is selected as the file type
- You cannot specify [Store to HDD] if:
 - a destination is specified
 - [Preview] is selected
- To cancel scanning, press the [Clear/Stop] key.
- After scan files are stored, the file information fields will be automatically cleared. If you want to preserve the information in these fields, contact your local dealer.

📖 Reference

- p.93 "Specifying File Information for a Stored File"
- p.143 "Various Scan Settings"
- p.151 "Adjusting Image Density"
- p.152 "Setting of Original Feed Type"
- p.45 "Simultaneous Storage and Sending by E-mail"
- p.74 "Simultaneous Storage and Sending by Scan to Folder"
- p.132 "Simultaneous Storage and Delivery"

Specifying File Information for a Stored File

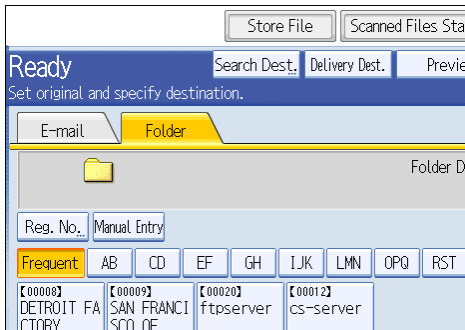
You can specify information for a stored file, such as user name, file name, and password.

By specifying information for a stored file, you can search for the file by user name or file name, or protect the file with a password to prevent other people from accessing the file.

Specifying a User Name

You can specify a user name for the stored file.

1. Press [Store File].



The Store File screen appears.

2. Press [User Name].

A list of user names appears.

3. Press the user name you want to specify.

The user names shown here are names that were registered on the [Administrator Tools] tab in [System Settings]. To specify a name not shown here, press [Manual Entry], and then enter the user name.

4. Press [OK] twice.

Note

- Depending on the security setting, [Access Privileges] may appear instead of [User Name]. For details about specifying [Access Privileges], consult the administrator.

Specifying a File Name

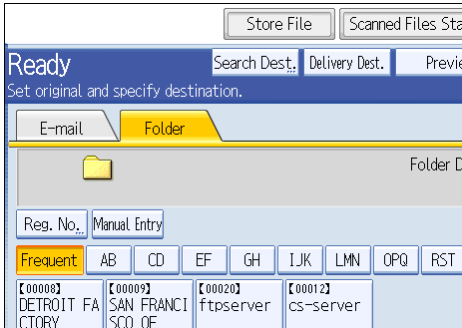
This section explains how to change the name of a stored file.

A stored file is allocated a name starting with "SCAN" followed by a 4-digit number.

- Example: SCAN0001

You can change this file name.

1. Press [Store File].



The Store File screen appears.

2. Press [File Name].

The soft keyboard appears.

3. Change the file name.

4. Press [OK] twice.

Note

- For details about entering the text, see "Entering Text", About This Machine.

Specifying a Password

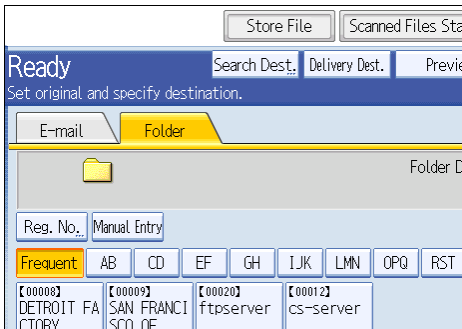
You can specify a password for the stored file.

Important

- **Do not forget the password. If you forget it, consult the system administrator of the machine.**

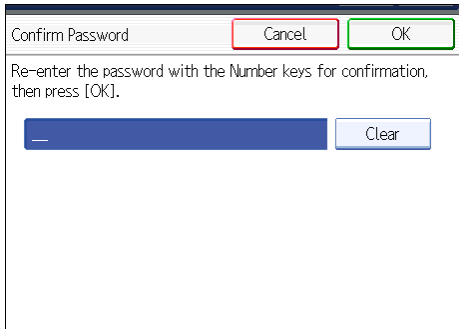
By specifying a password, you can ensure that only the people who know the password can view the file.

1. Press [Store File].



The Store File screen appears.

2. Press [Password].
3. Using the number keys, enter a four to eight-digit number.
4. Press [OK].
5. Enter the same number again using the number keys.



The screenshot shows a dialog box titled "Confirm Password". At the top right, there are two buttons: "Cancel" (with a red border) and "OK" (with a green border). Below the title bar, the text reads: "Re-enter the password with the Number keys for confirmation, then press [OK].". Underneath this text is a dark blue rectangular input field with a white cursor line on the left. To the right of the input field is a "Clear" button.

6. Press [OK] twice.

Displaying the List of Stored Files

This section describes the list of stored files. Using the list of stored files, you can delete stored files or change the file's information.

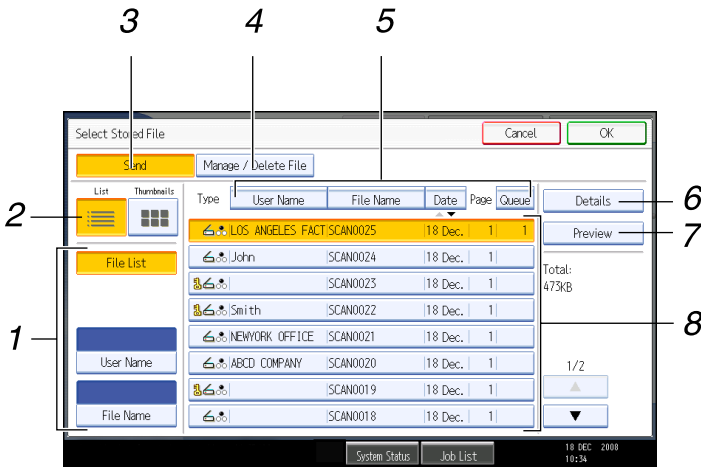
List of Stored Files

This section describes how the list of stored files is displayed.

To display the list of stored files, press [Select Stored File] on the initial scanner screen.

The function items displayed serve as selector keys. You can select or specify an item by pressing it. When you select or specify an item on the display panel, it is highlighted like [Set]. Keys that cannot be selected appear like [OK].

4



BQC006S

1. Keys for searching for files

Press to switch to the screens for searching for a file by user name or file name, or to the screen for displaying all files.

2. List / Thumbnails

You can select whether to display stored files as a list or as thumbnails.

3. [Send]

Press this to deliver or send a stored file by e-mail or Scan to Folder.

4. [Manage / Delete File]

Press this to delete stored files or change the file data.

5. Keys for sorting files

Press to sort the files using the selected item. Select the same item once more for a reverse sort. However, the files cannot be sorted in reverse delivery.

6. [Details]

Press this to display details about the selected file.

7. [Preview]

Press this to display a preview of the selected file. For details, see "Checking a Stored File Selected from the List".

8. List of stored files

Displays the list of stored files.

If the file you want to select is not displayed in the list, press [▲] or [▼] to scroll the screen. If a password has been specified for a file, a key icon appears to the left of the user name for the file.

Note

- Depending on the security setting, some files may not appear in the list.
- Files stored under functions other than the scanner function do not appear on this screen.

Reference

- p.99 "Checking a Stored File Selected from the List"

Searching the List of Stored Files

You can search for files from the stored files using the user name or file name.

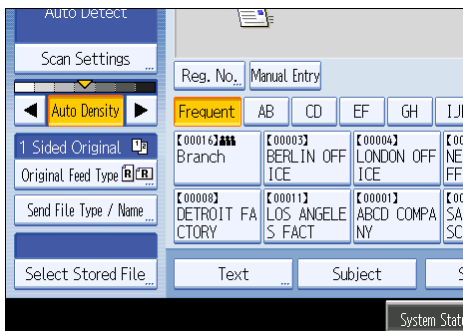
You can search the list of stored files by either of the following methods:

- Search by user name
- Search by file name

Searching by user name

You can search for a stored file by its user name.

1. Press [Select Stored File].



2. Press [User Name].

3. Select the user name to be used for the search.

The user names shown here are names that were registered on the [Administrator Tools] tab in [System Settings]. To change a user name not shown here, press [Manual Entry], and then enter the user name.

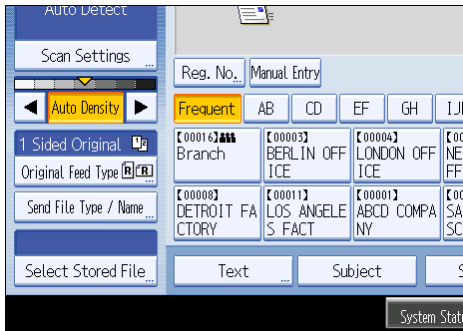
4. Press [OK].

The search begins, and then files belonging to the specified user appear.

Searching by file name

You can search for a stored file by its file name.

1. Press [Select Stored File].



2. Press [File Name].

The soft keyboard appears.

3. Enter the file name.

For information about how to enter characters, see "Entering Text", About This Machine.

4. Press [OK].

The search starts, and files whose name starts with the entered string appear.

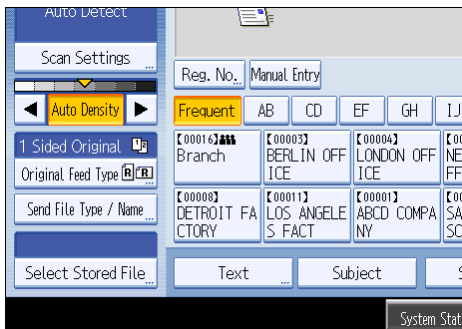
Checking Stored Files

You can display the Preview screen and check a stored file on the machine or from the client computer.

Checking a Stored File Selected from the List

This section explains how to preview a file selected from the list of stored files.

1. Press [Select Stored File].



The list of stored files appears.

For details about the list of stored files, see "List of Stored Files".

2. From the list of stored files, select the file you want to check.

You can select more than one file.

3. Press [Preview].

A preview of the selected stored file appears.

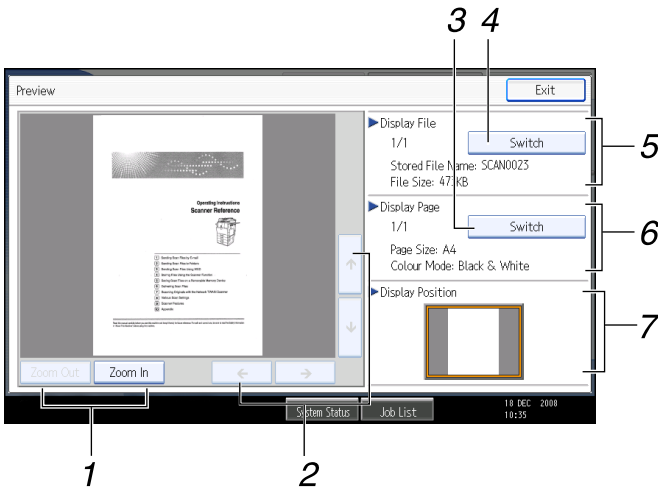
Note

- If you select a password-protected stored file, a screen for entering the password appears. To select the file, enter the correct password, and then press [OK].

Reference

- p.96 "List of Stored Files"

Stored File Preview Screen



BQC007S

1. [Zoom Out], [Zoom In]

In previewing, you can reduce or enlarge the file image.

2. [←] [→] [↑] [↓]

Press to shift the displayed area.

3. [Switch]

You can switch to a preview of another page.

4. [Switch]

You can switch to a preview of another file.

5. Display File

The name and size of the selected file appear.

6. Display Page

The page number of the previewed page, total number of pages, page size, and color mode appear.

7. Display Position

When the preview is enlarged, the location of the part of the page displayed on the preview screen is indicated.

Checking Stored Files from a Client Computer

Using DeskTopBinder Lite or Web Image Monitor, you can also display the files stored in the machine on a client computer.

★ Important

- To view stored files from a client computer, you must first make the required IPv4 or IPv6 address settings using DeskTopBinder or Web Image Monitor.

You can also check files stored under the copier, Document Server, and printer functions.

Using DeskTopBinder Lite to display stored files

The stored files are displayed and can be checked on a client computer using DeskTopBinder Lite.

↓ Note

- You can also transfer the stored files to the client computer.
- For details about DeskTopBinder, see the DeskTopBinder-related manuals.
- For details about installing DeskTopBinder Lite, see "Installing DeskTopBinder Lite from the Supplied CD-ROM".

📖 Reference

- p.117 "Installing DeskTopBinder Lite from the Supplied CD-ROM"

Using Web Image Monitor to display stored files

The stored files are displayed and can be checked also on a client computer using Web Image Monitor.

If you enter "http:// (machine IPv4 or IPv6 address, or host name)/" in the address bar of the client computer's Web browser, the top page of Web Image Monitor appears.

★ Important

- **Do not begin IPv4 segments with zeros. For example: if the address is "192.168.001.010", enter it as "192.168.1.10".**

↓ Note

- You can also download the stored files.
- It is recommended that you use Web Image Monitor only within your local area network.
- For details about displaying or downloading stored files using Web Image Monitor, see "Displaying Stored Documents with Web Image Monitor", "Downloading Stored Documents with Web Image Monitor", Copy and Document Server Reference.
- For details about making settings for using Web Image Monitor, see "Monitoring and Configuring the Printer", Network and System Settings Guide.
- For details about functions for managing stored files using Web Image Monitor, click [Help] on the upper-right corner of the displayed screen.

Sending a Stored File

This section explains how to send a stored file.

Stored files can be sent by e-mail, Scan to Folder, or the network delivery scanner.

There are two methods of sending stored files by e-mail. Settings made under [Scanner Features] determine which method is used. For details, see "Send Settings".

- To send the URL by e-mail:

Under [Scanner Features], [Stored File E-mail Method], select [Send URL Link]. This method is useful when network restrictions prevent you sending attachments.

- To send an attached file by e-mail:

Under [Scanner Features], [Stored File E-mail Method], select [Send File].

★ Important

- Depending on your e-mail application, a phishing warning might appear after you receive an e-mail message. To prevent phishing warnings appearing after you receive e-mail from a specified sender, you must add the sender to your e-mail application's exclusion list. For details about how to do this, see your e-mail application's Help.

📖 Reference

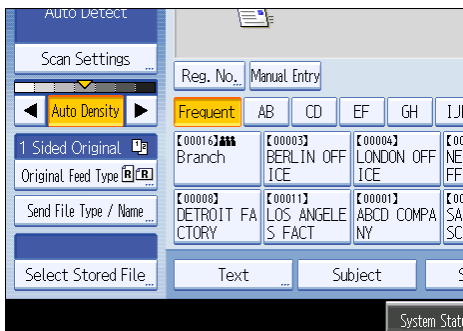
- p.181 "Send Settings"

Sending Stored Files

This section mainly explains how to select the files you want to send.

For details about how to select stored files and make settings for sending those files, see respective pages.

1. Press [Select Stored File].



The list of stored files appears.

2. Select the file you want to send.

You can select multiple files.

The selected files are sent in the order they were selected.

If you press [Queue], only the files you have selected are displayed in the order they will be sent.

For details about selecting the stored files, see "Displaying the List of Stored Files".

3. Press [OK].

4. If necessary, switch to the E-mail, Scan to Folder, or network delivery scanner screen.

For details about switching the screen, see "Switching to the E-mail Screen", "Switching to the Scan to Folder Screen", or "Switching to the Network Delivery Scanner Screen".

5. Specify the destination, make any other necessary settings.

For details about how to send a file by e-mail or Scan to Folder, or how to deliver a file, see "Basic Procedure for Sending Scan Files by E-mail", "Basic Procedure When Using Scan to Folder", or "Basic Procedure for Delivering Files".

6. Press the [Start] key.

The stored file will be sent.

Note

- If you select a password-protected stored file, a screen for entering the password appears. To select the file, enter the correct password, and then press [OK].
- When the URL has been sent by e-mail, the recipient can check the stored file by clicking that URL. For details, see "Sending the URL by E-mail".
- You can encrypt e-mail or attach a signature to it. For details, see "Security Settings to E-mails".

Reference

- p.28 "Switching to the E-mail Screen"
- p.60 "Switching to the Scan to Folder Screen"
- p.122 "Switching to the Network Delivery Scanner Screen"
- p.25 "Basic Procedure for Sending Scan Files by E-mail"
- p.58 "Basic Procedure When Using Scan to Folder"
- p.119 "Basic Procedure for Delivering Files"
- p.48 "Sending the URL by E-mail"
- p.46 "Security Settings to E-mails"

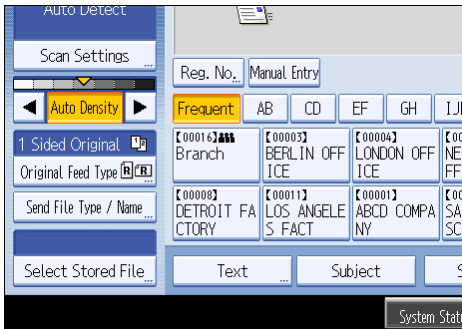
Managing Stored Files

This section explains how to delete stored files and how to change the data for stored files.

Deleting a Stored File

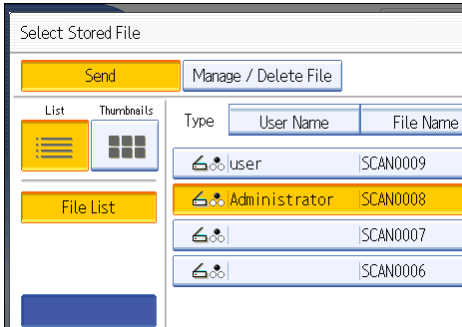
This section explains how to delete a stored file.

1. Press [Select Stored File].



The list of stored files appears.

2. Press [Manage / Delete File].



3. Select the file you want to delete.

If you select a password-protected stored file, a screen for entering the password appears. To select the file, enter the correct password, and then press [OK].

4. Press [Delete File].

A confirmation message about deleting the file appears.

5. Press [Yes].

Note

- Files waiting for sending cannot be deleted.

- You can also delete files stored in the machine by accessing the machine from a client computer using Web Image Monitor or DeskTopBinder. For detail about Web Image Monitor, see Web Image Monitor Help. For details about DeskTopBinder, see the manuals supplied with DeskTopBinder.

Changing Information for a Stored File

You can change information for a stored file, such as [User Name], [File Name], and [Password].

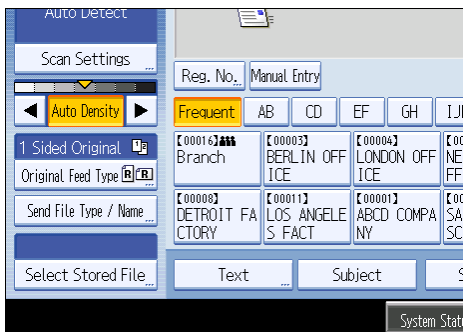
Note

- Information for files waiting for being sent cannot be changed.

Changing a user name

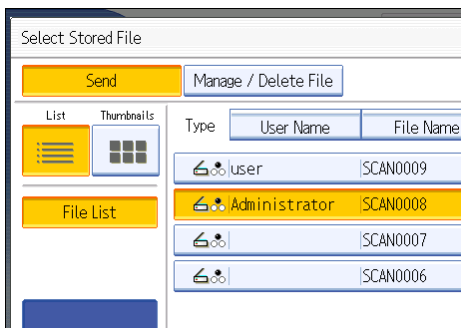
You can change the user name for a stored file.

1. Press [Select Stored File].



The list of stored files appears.

2. Press [Manage / Delete File].



3. Select the file containing the information you want to change.

If you select a password-protected stored file, a screen for entering the password appears. Enter the password, and then press [OK].

4. Press [Change User Name].

5. Enter a new user name.

The user names shown here are names that were registered on the [Administrator Tools] tab in [System Settings]. To change a user name not shown here, press [Manual Entry], and then enter the user name.

6. Press [OK].

7. Make sure that the user name was changed as necessary, and press [Exit].

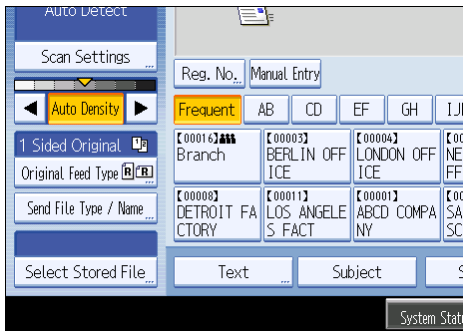
Note

- Using Web Image Monitor or DeskTopBinder you can also change the user name of a file stored in the machine from the client computer. For details about Web Image Monitor, see Web Image Monitor Help. For details about DeskTopBinder, see the manuals supplied with DeskTopBinder.
- Depending on the security setting, [Change Access Priv.] may appear instead of [Change User Name]. For details about specifying [Change Access Priv.] consult the administrator.

Changing a file name

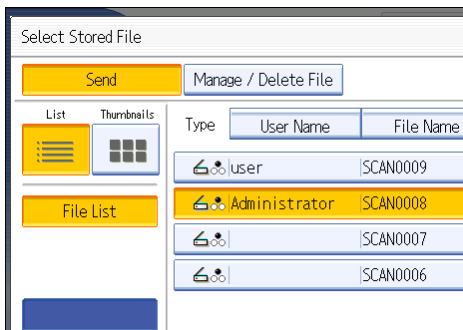
You can change the file name of a stored file.

1. Press [Select Stored File].



The list of stored files appears.

2. Press [Manage / Delete File].



3. Select the file containing the file information you want to change.

If you select a password-protected stored file, a screen for entering the password appears. Enter the password, and then press [OK].

4. Press [Change File Name].

5. Change the file name.

6. Press [OK].

7. Make sure that the file information was changed as necessary, and press [Exit].

↓ Note

- For information about how to enter characters, see "Entering Text", About This Machine.
- Using Web Image Monitor or DeskTopBinder, you can also change the name of a file stored in the machine from the client computer. For details about Web Image Monitor, see Web Image Monitor Help. For details about DeskTopBinder, see the manuals supplied with DeskTopBinder.

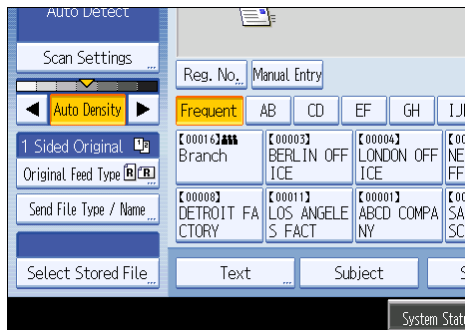
Changing a password

Enter the password for accessing the stored file.

★ Important

- **Be sure not to forget the password. If you forget it, consult the system administrator of the machine.**

1. Press [Select Stored File].



The list of stored files appears.

2. Press [Manage / Delete File].

3. Select the file containing the file information you want to change.

If you select a password-protected stored file, a screen for entering the password appears. Enter the password, and then press [OK].

4. Press [Change Password].

5. Using the number keys, enter a new four to eight-digit password.

6. Press [OK].

7. Enter the same number again using the number keys.
8. Press [OK].
9. Press [Exit].

 **Note**

- Using Web Image Monitor or DeskTopBinder, you can also change the password of a file stored in the machine from the client computer. For details about Web Image Monitor, see Web Image Monitor Help. For details about DeskTopBinder, see the manuals supplied with DeskTopBinder.

5. Saving Scan Files on a Removable Memory Device

If the optional media slot is installed on your machine, you can save scan files on a removable memory device using the scanner function.

Before Saving Files on a Removable Memory Device

This section explains saving scan files on a removable memory device and provides related cautions.

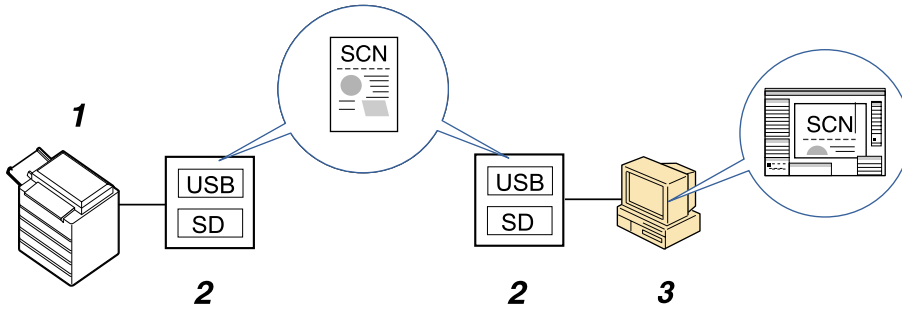
Overview of Saving Files on a Removable Memory Device

5

The following diagram explains saving scan files on a removable memory device.

Important

- This machine supports FAT16 format USB memory sticks and SD cards. Other forms of removable memory device are not compatible.
- Make sure that the format of the removable memory device is FAT16.
- Saving might fail if the USB memory stick features password protection or other security features.
- Certain types of USB memory sticks cannot be used.
- Do not connect the optional media slot to other machines.
- Connect only USB memory sticks to the USB slot, not any other form of USB device.
- Do not turn the machine's main power switch to off while data is being written. Doing so can 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.



Z22807S

1. This Machine

If the optional media slot is installed, the machine can save scan files on a removable memory device.

2. Removable Memory Device

Scan files are saved on a removable memory device.

3. Client Computer

Using applications on a client computer, scan files saved on a removable memory device can be printed or viewed.

↓ Note

- Files saved on a removable memory device will not appear in the list of stored files.
- Files saved on a removable memory device cannot be printed or sent using the machine's control panel. To perform operations on files saved on a removable memory device, you must use an application on a client computer.

Basic Procedure for Saving Scan Files on a Removable Memory Device

Use the following procedure to save scan files on a removable memory device.

1. Insert a removable memory device in the media slot.

You can connect only one removable memory device at a time.

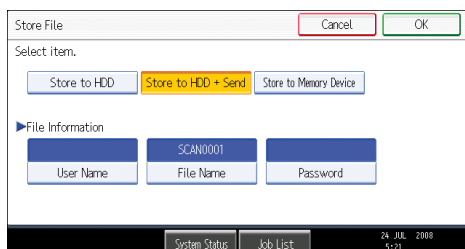
2. Make sure that no previous settings remain.

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

3. Place originals.

4. Press [Store File].

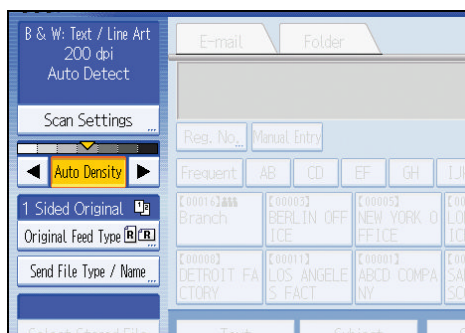
5. Press [Store to Memory Device].



6. Press [OK].

7. If necessary, press [Scan Settings] to specify scanner settings such as resolution and scan size.

For details, see "Various Scan Settings".



8. If necessary, specify the scanning density.

For details, see "Adjusting Image Density".

9. If necessary, press [Original Feed Type] to specify settings such as original orientation.

For details, see "Setting of Original Feed Type".

10. If necessary, press [Send File Type / Name] to specify settings such as file format and file name.

For details, see "Specifying the File Type and File Name".

11. 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.

12. Press [Exit].

13. Remove the memory device from the media slot.

Do not remove the memory device while writing is in process. Doing so can corrupt the data that is stored on it.

Note

- You cannot specify where the data is saved. Files are saved in the root directory of the removable memory device.
- Up to 2 GB of data can be saved. However, depending on the number of files already stored on the removable memory device, new files might not be saved, even if there appears to be sufficient free space.
- 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].
- To cancel writing, press the [Clear/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.
- The LED lamp on the media slot flashes when an inserted SD card is being accessed and remains lit when a USB memory stick is attached.

Reference

- p.143 "Various Scan Settings"
- p.151 "Adjusting Image Density"
- p.152 "Setting of Original Feed Type"
- p.160 "Specifying the File Type and File Name"

6. Delivering Scan Files

Using the ScanRouter delivery software, you can deliver by various methods scan files produced by the machine.

Before Delivering Files

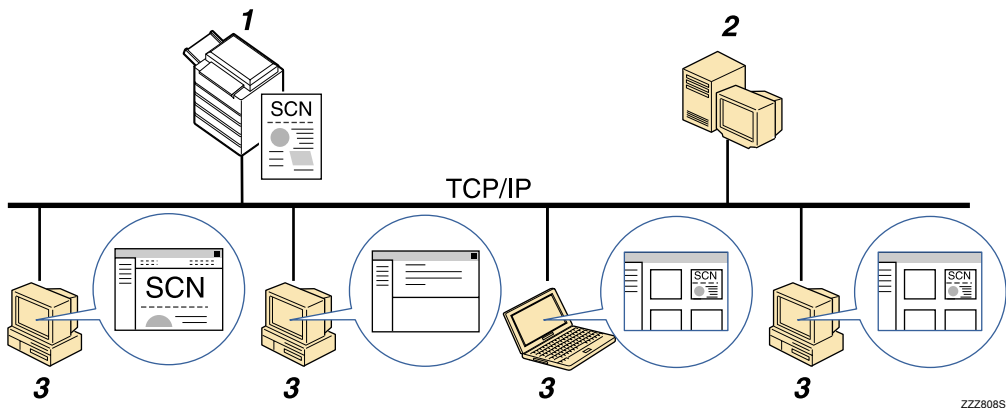
This section describes the necessary preparations and the procedure for using the network delivery scanner.

★ Important

- To use the network delivery scanner function, your network must have a delivery server on which the ScanRouter delivery software (optional) is installed. You must also register destination and sender information on the delivery server. For details about the ScanRouter delivery software, see the manuals that are supplied with it.

Overview of Scan File Delivery

This section describes the process for delivering files using the network delivery scanner.



1. This machine

You can send scan files to the delivery server.

2. Delivery server

Install the ScanRouter delivery software on this computer to use it as the delivery server.

After receiving a scan file, the delivery server delivers the file according to the setting specified for the destination.

The delivery settings are as follows:

- Storing the file in an in-tray
- Delivering the file by e-mail
- Storing the file in a selected folder

For details about the ScanRouter delivery software, see the manuals supplied with ScanRouter delivery software.

3. Client Computer

How to check a file from the client computer depends on the delivery method.

For example, you can check a file by one of the following methods:

- Use DeskTopBinder to view a file delivered to the in-tray.
- Use e-mail software to receive e-mail with an attached file.
- Browse a folder for a stored file.

Preparing to Deliver Files

To deliver scanned files, you must first perform the following:

- Check the machine is properly connected to the network
- Configure the network settings in [System Settings]
- Configure the necessary settings in [Scanner Features]
- Configure the settings in ScanRouter delivery software

6

Checking the machine is properly connected to the network

Check that this machine is properly connected to the network.

For details about how to connect this machine to a network, see "Connecting to the Interface", Network and System Settings Guide.

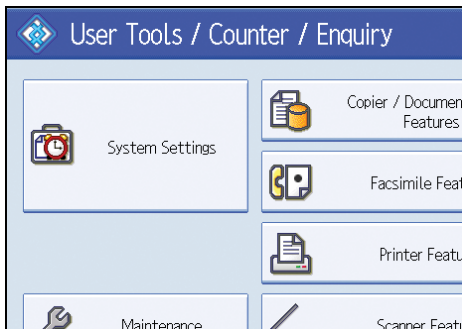
Configuring the network settings in [System Settings]

Configure the network settings in [System Settings] according to your environment and how you will be using the machine.

The following procedure explains connecting this machine to an IPv4 network using Ethernet cable.

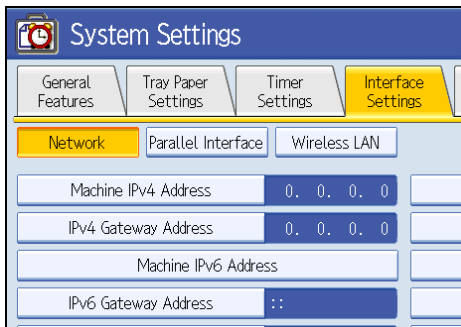
Note that the settings you must configure will vary depending on your operating environment. For details about network settings and configuration procedures, see "Network Settings Required to Use the Network Delivery Scanner", Network and System Settings Guide.

1. Press the [User Tools/Counter] key, and then press [System Settings].



The System Settings screen appears.

2. Press the [Interface Settings] tab.

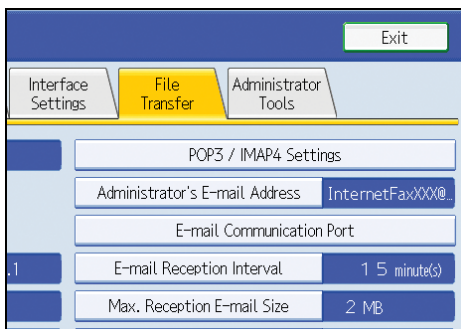


3. Press [Machine IPv4 Address] to specify the machine's IPv4 address.

To specify a static IPv4 address for this machine, press Specify, and then enter the IPv4 address and subnet mask.

To obtain an IPv4 address from a DHCP server automatically, press [Auto-Obtain (DHCP)].

4. Press [IPv4 Gateway Address], and then enter the IPv4 gateway address.
5. Press [Effective Protocol], and then make [IPv4] active.
6. Press the [File Transfer] tab.



7. Press [Delivery Option], and then press [On].

8. Press [Exit] twice.

↓ Note

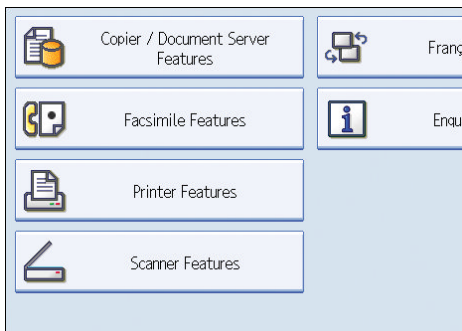
- If an extended wireless LAN board (optional) is installed, press [LAN Type] on the [Interface Settings] tab, then press [Ethernet], and then configure the network settings.

Configure the necessary settings in [Scanner Features]

Using [Scanner Features], you can make or change various settings related to the scanner function, such as compressing scan data or viewing the scanner journal. Configure the scanner settings according to your environment and how you will be using the machine.

This section explains how to display the Scanner Features screen. For details about the settings on this screen, see "Scanner Features".

1. Press the [User Tools/Counter] key, and then press [Scanner Features].



The Scanner Features screen appears.

2. Press the [General Settings], [Scan Settings], [Send Settings], or [Initial Settings] tabs and configure the relevant settings on those tabs.

📖 Reference

- p.175 "Scanner Features"

Configure the settings in ScanRouter delivery software

Using SR Manager (a tool for the ScanRouter delivery software), register this machine as an I/O device. In addition, register destinations and specify such settings as the delivery type and sender.

For details about settings, see the manuals supplied with the ScanRouter delivery software.

↓ Note

- To view files delivered to an in-tray, DeskTopBinder Lite must be installed on the client computer. For details about installing DeskTopBinder Lite, see "Installing DeskTopBinder Lite from the Supplied CD-ROM".

- The settings you must configure in [System Settings] vary depending on your network environment. For details about network settings, see "Connecting the Machine", Network and System Settings Guide.

Reference

- p.117 "Installing DeskTopBinder Lite from the Supplied CD-ROM"

Installing DeskTopBinder Lite from the Supplied CD-ROM

This section explains how to install DeskTopBinder Lite on a client computer from the supplied CD-ROM. To view or receive files delivered to the in-trays, you must install DeskTopBinder Lite on the client computer.

1. Make sure Windows is running on the client computer, and then insert the CD-ROM into the CD-ROM drive.

The installer starts.

2. Click [DeskTopBinder Lite].

The [DeskTopBinder Lite Setup] dialog box appears.

For the subsequent installation steps, see the Setup Guide displayed from the [DeskTopBinder Lite Setup] dialog box.

Note



- Before you start the installation, check the system requirements for DeskTopBinder Lite. For details, see "Software Supplied on CD-ROM".
- You can install the software using the auto-run program. For details about the auto-run program, see "Auto-Run Program".

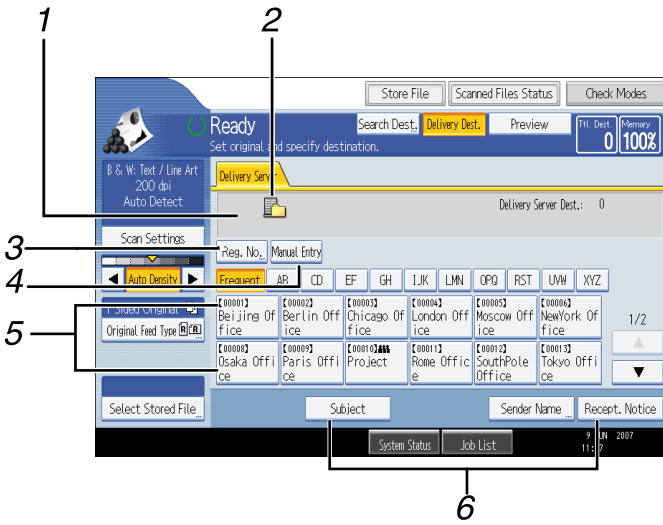
Reference

- p.188 "Software Supplied on CD-ROM"
- p.188 "Auto-Run Program"

Network Delivery Scanner Screen

This section describes the screen layout when using the network delivery scanner.

The function items displayed serve as selector keys. You can select or specify an item by pressing it. When you select or specify an item on the display panel, it is highlighted like []. Keys that cannot be selected appear like [].



BAP009S

1. Destination Field

The specified destination appears. If more than one destination has been specified, press [▲] or [▼] to scroll through the destinations.

2. Network delivery scanner icon

Indicates that the network delivery scanner screen is displayed.

3. [Reg. No.]

Press this key to specify the destination using a 3-digit registration number.

4. [Manual Entry]

To send a file by e-mail via the delivery server to a destination not registered in the delivery server's Destination List, press this key to display the soft keyboard. Then use the soft keyboard to enter the e-mail address. For details about how to send a file by e-mail via the delivery server, see ScanRouter delivery software manual.

5. Destination List

The list of destinations registered in the delivery server appears. If all of the destinations cannot be displayed, press [▲] or [▼] to switch the screen.

The (###) symbol indicates a group destination.

6. [Subject] [Sender Name] [Recept. Notice]

Specify the subject, sender, and whether or not to enable Message Disposition Notification for the file to be transmitted.

Basic Procedure for Delivering Files

This section explains the basic procedure for delivering scan files using the network delivery scanner.

★ Important

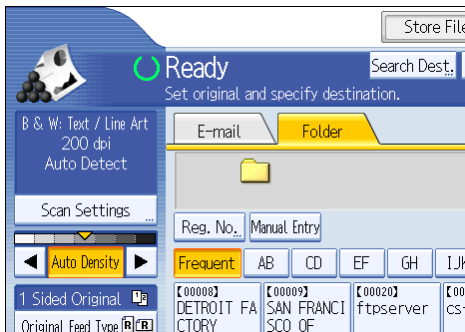
- You must register destinations and senders in advance using the ScanRouter delivery software installed on the delivery server.

1. Make sure that no previous settings remain.

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

2. If the E-mail screen or Scan to Folder screen appears, switch to the network delivery scanner screen.

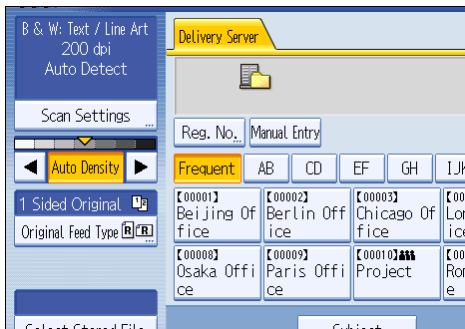
For details, see "Switching to the Network Delivery Scanner Screen".



3. Place originals.

4. If necessary, press [Scan Settings] to specify scanner settings such as resolution and scan size.

For details, see "Various Scan Settings".



5. If necessary, specify the scanning density.

For details, see "Adjusting Image Density".

6. If necessary, press [Original Feed Type] to specify settings such as original orientation.

For details, see "Setting of Original Feed Type".

7. Specify the destination.

You can specify multiple destinations.

For details, see "Specifying Delivery Destinations".

8. If necessary, press [Subject] to specify the e-mail subject.

For details, see "Entering the Subject of the E-mail to Be Transmitted via the Delivery Server".

9. If necessary, press [Sender Name] to specify the sender.

For details, see "Specifying the Sender".

10. Press the [Start] key.

If you are scanning batches, place the next originals.

Note

- By pressing [Manual Entry] on the network delivery scanner screen, you can send a file by e-mail via the delivery server's network. For details about entering the e-mail address directly, see "Entering an E-mail Address Manually".
- If you have selected more than one destination, press [▲] or [▼] next to the destination field to scroll through the destinations.
- To cancel a selected destination, display the destination in the destination field, and then press the [Clear/Stop] key. You can cancel a destination selected from the address book by pressing the selected destination again.
- You can use the Message Disposition Notification function when sending e-mail via delivery server. An e-mail is sent to the sender selected in step 9, notifying him/her that the recipient has read his/her e-mail. To specify this setting, press [Recept. Notice].
- To enable the Return Receipt function, you must specify the SMTP e-mail transmission settings using ScanRouter delivery software. For details about specifying this setting, see the ScanRouter delivery software manual. Note, however, that if the e-mail software used at the destination does not support Message Disposition Notification (MDN), e-mail notification that the e-mail has been opened may not be sent.
- Register the sender's e-mail address using the ScanRouter delivery software in advance.
- If you press [Check Modes] before pressing the [Start] key, the initial scanner screen switches to the Check Modes screen. You can use the Check Modes screen to check the settings such as destinations. For details, see "Check Modes".
- If you press [Preview] and start scanning while [Preview] is highlighted, the Preview screen appears. For details, see "Preview".
- To cancel scanning, press the [Clear/Stop] key.
- You can also store a scan file and simultaneously deliver it. For details, see "Simultaneous Storage and Delivery".

- After scan files are delivered, the destination, sender, and subject fields will be automatically cleared. If you want to preserve the information in these fields, contact your local dealer.

Reference

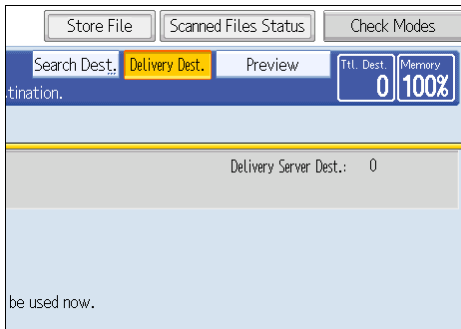
- p.122 "Switching to the Network Delivery Scanner Screen"
- p.143 "Various Scan Settings"
- p.151 "Adjusting Image Density"
- p.152 "Setting of Original Feed Type"
- p.123 "Specifying Delivery Destinations"
- p.131 "Entering the Subject of the E-mail to Be Transmitted via the Delivery Server"
- p.127 "Specifying the Sender"
- p.32 "Entering an E-mail Address Manually"
- p.14 "Check Modes"
- p.15 "Preview"
- p.132 "Simultaneous Storage and Delivery"

Switching to the Network Delivery Scanner Screen

This section explains how to switch the screen to the network delivery scanner screen.

If the E-mail screen or Scan to Folder screen is being displayed, switch to the network delivery scanner screen.

1. Press [Delivery Dest.].



The network delivery scanner screen appears.

↓ Note

- You cannot switch the screen while e-mail or other destinations are being specified. To clear the specified destination, display the destination in the destination field of each screen, and then press the [Clear/Stop] key.
- When WSD is enabled, [Swch Dest.List] appears instead of [Delivery Dest.]. To switch to the network delivery screen, press [Swch Dest.List], and then press [Delivery Server].

Specifying Delivery Destinations

This section explains how to specify delivery destinations.

Note

- You can specify multiple destinations.

Selecting Destinations Registered in the Delivery Server's Address Book

This section explains how to select destinations registered in the delivery server's address book

You can select a delivery destination registered in Destination List of the delivery server by any of the following methods:

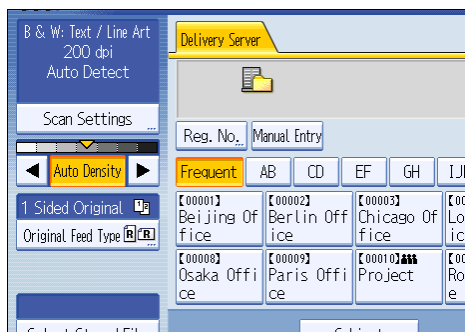
- Select the destination from the delivery destination list
- Select the destination by entering the registration numbers
- Select the destination by searching in the delivery server

6

Selecting a destination from the Destination List

From the destination list, select a destination.

- In the destination list, press the key including the destination name.



The selected destination is highlighted and also is displayed in the destination field at the top of the screen.

Destinations are registered in the delivery server under captions. The destination list is updated automatically.

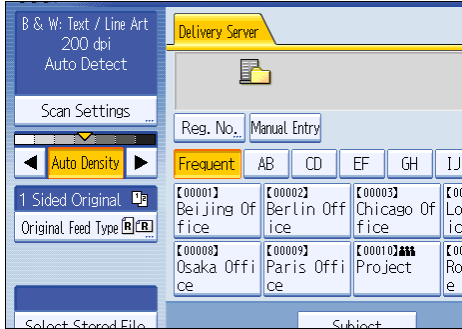
Note

- If the target destination does not appear, press [▲] or [▼] to scroll through the destinations until it does.
- Depending on the security setting, some destinations may not appear in the destination list.

Selecting destinations by entering their registration numbers

Select a destination by entering its Short ID number (registered using the ScanRouter delivery software). For details about how to set Short IDs, see the manuals supplied with the ScanRouter delivery software.

1. Press [Reg. No.].



2. Using the number keys, enter the three-digit registration number, and then press the [#] key.

You can also enter a registration number of fewer than three digits.

Example: To enter 009

Press the [9] key, and then press the [#] key.

By pressing [Change], you can change the selected destination.

3. Press [OK].

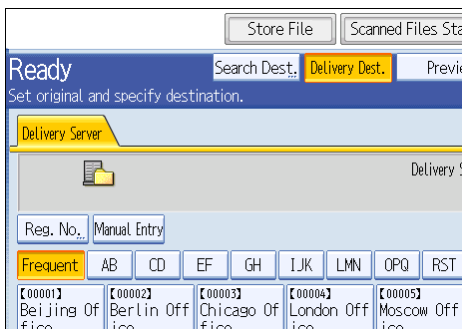
Note

- To cancel a selected destination, press [▲] or [▼] next to the destination field to scroll through the destinations until the one you want to cancel appears, and then press the [Clear/Stop] key.

Selecting destinations by searching the delivery server's Destination List

In the delivery server's Destination List, you can search for destinations and select them.

1. Press [Search Dest.].



2. To search by destination name, press [Name].

To search by comment, press [Comment].

The soft keyboard appears.

You can also search by combining [Name] and [Comment].

3. Enter the beginning of the destination name.

To search by comment, enter the beginning of the comment.

4. Press [OK].**5. If necessary, press [Advanced Search] to specify the detailed search criteria, and then press [OK].**

By pressing [Advanced Search], you can search by [Name] and [Comment]. You can specify search criteria such as [Beginning Word] or [End Word]. You can refine your search using multiple criteria.

Advanced Search			
Specify search conditions.			
Name	Beginning Word	End Word	Exact Match
Comment	Beginning Word	End Word	Exact Match

6. Press [Start Search].

Destinations that match the search criteria are displayed.

7. Select the destination.**8. Press [OK].****↓ Note**

- The Comment search function searches for destinations by comment information, which is a registration item required by the ScanRouter delivery software.
- By pressing [Details], you can view details about the selected destinations.
- Up to 100 destinations can be displayed as search results.
- By pressing [Advanced Search], the following criteria appear:
 - [Beginning Word]: The names which start with the entered character or characters are targeted. For example, to search for "ABC", enter "A".
 - [End Word]: The names which end with the entered character or characters are targeted. For example, to search for "ABC", enter "C".
 - [Exact Match]: The names which correspond to an entered character or characters are targeted.

For example, to search for "ABC", enter "ABC".

- [Include one Word]: The names which contain an entered character or characters are targeted.

For example, to search for "ABC", enter "A", "B", or "C".

- [Exclude Words]: The names which do not contain an entered character or characters are targeted.

For example, to search for "ABC", enter "D".

Specifying the Sender

This section explains how to specify the e-mail sender when sending a file by e-mail via the delivery server.

You can specify the sender by any of the following methods:

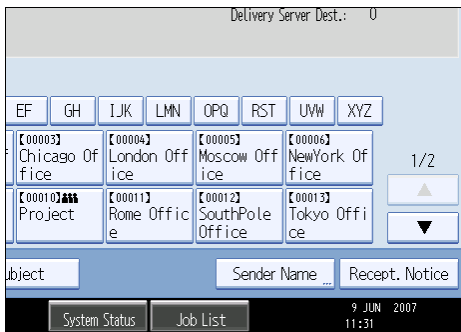
- Select the sender from the sender list
- Select the sender by entering the registration number
- Select the sender by searching the delivery server's Destination List

Selecting a Sender from the Sender List

This section explains how to select a sender from the sender list.

The sender list displays destinations that are registered on the delivery server.

1. Press [Sender Name].



2. Select the sender.

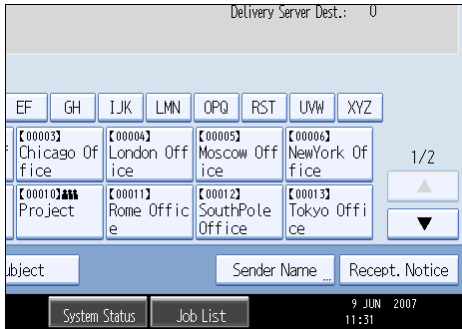
3. Press [OK].

Selecting the Sender by Entering the Registration Number

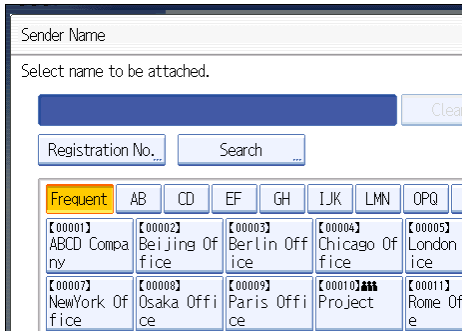
Select a sender by entering its Short ID number (registered using the ScanRouter delivery software).

For details about how to set Short IDs, see the manuals supplied with the ScanRouter delivery software.

1. Press [Sender Name].



2. Press [Registration No.].



3. Using the number keys, enter the three-digit registration number assigned to the required destination folder.

If the entered number is less than five digits, press the [#] key after the last number.

Example: To enter 006

Press the [6] key, and then press the [#] key.

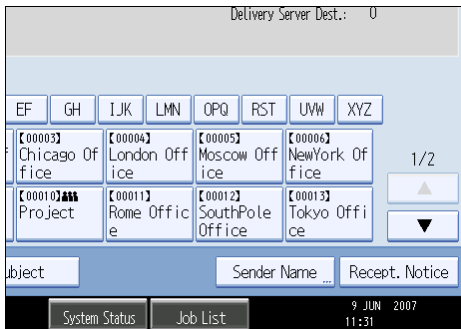
By pressing [Change], you can change the selected destination.

4. Press [OK] twice.

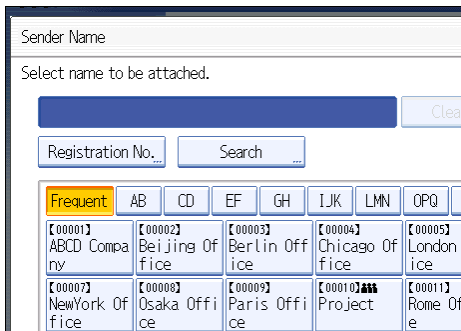
Selecting a Sender by Searching the Delivery Server's Destination List

This section explains how to select a sender by searching the delivery server's Destination List.

1. Press [Sender Name].



2. Press [Search].



3. To search by destination name, press [Name].

To search by comment, press [Comment].

The soft keyboard appears.

You can also search by combining [Name] and [Comment].

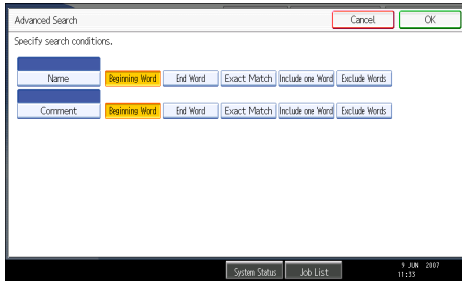
4. Enter the beginning of the sender's name.

To search by comment, enter beginning of the comment.

5. Press [OK].

6. If necessary, press [Advanced Search] to specify the detailed search criteria, and then press [OK].

By pressing [Advanced Search], you can search by [Name] and [Comment]. You can specify search criteria such as [Beginning Word] or [End Word]. You can refine your search using multiple criteria.



7. Press [Start Search].

Destinations that match the search criteria are displayed.

8. Select the sender.

9. Press [OK].

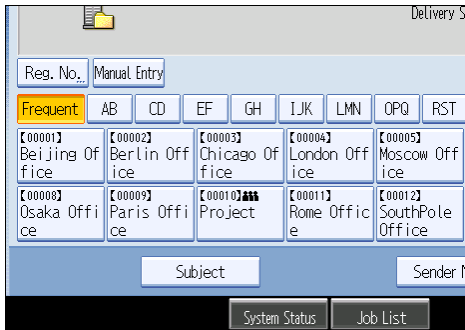
Note

- The Comment search function searches for destinations by comment information, which is a registration item required by the ScanRouter delivery software.
- By pressing [Details], you can view details about the selected sender.
- Up to 100 items can be displayed as the search results.
- By pressing [Advanced Search], the following criteria appear:
 - [Beginning Word]: The names which start with the entered character or characters are targeted. For example, to search for "ABC", enter "A".
 - [End Word]: The names which end with the entered character or characters are targeted. For example, to search for "ABC", enter "C".
 - [Exact Match]: The names which correspond to an entered character or characters are targeted. For example, to search for "ABC", enter "ABC".
 - [Include one Word]: The names which contain an entered character or characters are targeted. For example, to search for "ABC", enter "A", "B", or "C".
 - [Exclude Words]: The names which do not contain an entered character or characters are targeted. For example, to search for "ABC", enter "D".

Entering the Subject of the E-mail to Be Transmitted via the Delivery Server

This section explains how to enter the e-mail subject when sending a file by e-mail via the delivery server.

1. Press [Subject].



2. Enter the subject.

To enter characters, press [Text Entry].

To enter symbols, press [Symbol Entry].

To add predefined User Text registered on this machine, press [User Text].

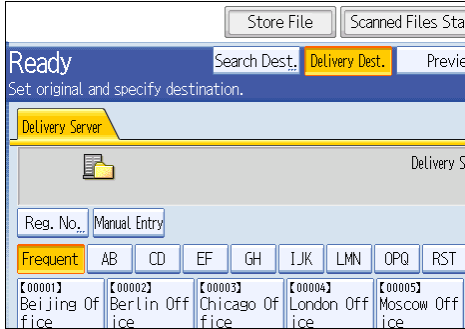
For details about entering the text, see "Entering Text", About This Machine.

3. Press [OK].

Simultaneous Storage and Delivery

This section explains how to store a file and simultaneously deliver it.

1. Press [Store File].



2. Make sure that [Store to HDD + Send] is selected.

3. If necessary, specify the stored file's information, such as [User Name], [File Name], and [Password].

For details, see "Specifying File Information for a Stored File".

4. Press [OK].

5. Specify the setting for delivering the file, and then send the file.

For details about delivering a file, see "Basic Procedure for Delivering Files".

Note

- Depending on the security setting, [Access Privileges] may appear instead of [User Name]. For details about specifying [Access Privileges], consult the administrator.
- You can resend stored files. To resend stored files, select the files on the Select Stored File screen, and then send them. For details, see "Sending a Stored File".

Reference

- p.93 "Specifying File Information for a Stored File"
- p.119 "Basic Procedure for Delivering Files"
- p.102 "Sending a Stored File"

7. Scanning Originals with the Network TWAIN Scanner

The TWAIN driver allows you to scan originals on the machine from a client computer via the network.

Before Using the Network TWAIN Scanner

This section describes the preparations and procedure for using the network TWAIN scanner.

★ Important

- To use the network TWAIN scanner, you must install the TWAIN driver, which is on the supplied CD-ROM. For details about installing the TWAIN driver, see "Installing the TWAIN Driver from the Supplied CD-ROM".
- To use the network TWAIN scanner, a TWAIN-compliant application, such as DeskTopBinder, must be installed on the client computer. DeskTopBinder Lite is on the supplied CD-ROM. For details about installing DeskTopBinder Lite, see "Installing DeskTopBinder Lite from the Supplied CD-ROM".

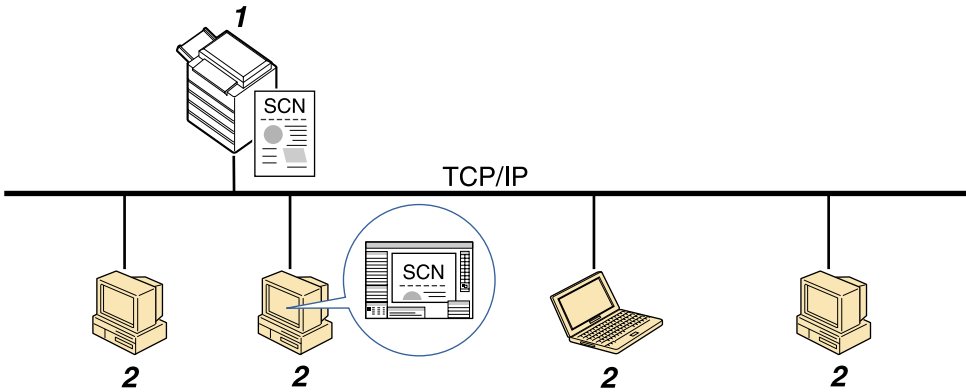
📖 Reference

- p.136 "Installing the TWAIN Driver from the Supplied CD-ROM"
- p.117 "Installing DeskTopBinder Lite from the Supplied CD-ROM"

Overview of the Network TWAIN Scanner

This section describes the network TWAIN scanner function.

In the TWAIN scanner mode, you can share this machine among multiple computers. Therefore, you don't have to prepare a special computer for scanner or reconnect the scanner and each computer every time you need to use it.



ZZZ805S

1. This Machine

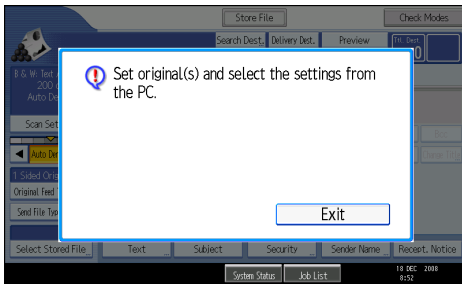
Scans an original after receiving a scan instruction from a client computer, and then sends the scan file over the network to the client computer.

2. Client Computer

Specifies the scanner settings and controls the scanner using an application, such as DeskTopBinder Lite, that supports the network TWAIN scanner. Receives the files scanned by the machine and displays them using an application that supports the network TWAIN scanner.

Note

- When using the machine as a network TWAIN scanner, you do not need to press the [Scanner] key on the machine's control panel. The screen switches automatically when you scan an original from a client computer using the TWAIN driver. To use functions other than the network TWAIN scanner, press [Exit].



Preparing to Use the Network TWAIN Scanner

To use this machine as a network TWAIN scanner, you must first perform the following:

- Check the machine is properly connected to the network
- Configure the network settings in [System Settings]
- Install the TWAIN driver on a client computer
- Install a TWAIN-compliant application on the same client computer

Checking the machine is properly connected to the network

Check that this machine is properly connected to the network.

For details about how to connect this machine to a network, see "Connecting to the Interface", Network and System Settings Guide.

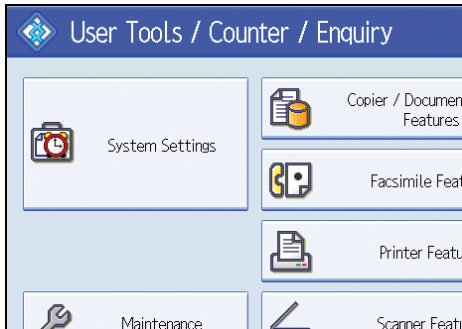
Configuring the network settings in [System Settings]

Configure the network settings in [System Settings] according to your environment and how you will be using the machine.

The following procedure explains connecting this machine to an IPv4 network using Ethernet cable.

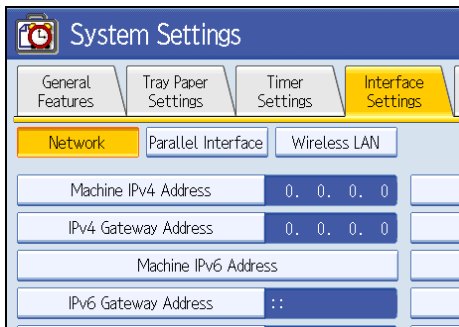
Note that the settings you must configure will vary depending on your operating environment. For details about network settings and configuration procedures, see "Network Settings Required to Use Network TWAIN Scanner", Network and System Settings Guide.

1. Press the [User Tools/Counter] key, and then press [System Settings].



The System Settings screen appears.

2. Press the [Interface Settings] tab.



3. Press [Machine IPv4 Address] to specify the machine's IPv4 address.

To specify a static IPv4 address for this machine, press [Specify], and then enter the IPv4 address and subnet mask.

To obtain an IPv4 address from a DHCP server automatically, press [Auto-Obtain (DHCP)].

4. Press [IPv4 Gateway Address], and then enter the IPv4 gateway address.
5. Press [Effective Protocol], and then make [IPv4] active.
6. Press [Exit] twice.

↓ Note

- If an extended wireless LAN board (optional) is installed, press [LAN Type] on the [Interface Settings] tab, then press [Ethernet], and then configure the network settings.

Installing the TWAIN driver on a client computer

Install the TWAIN driver on your computer.

For details about installing the TWAIN driver, see "Installing the TWAIN Driver from the Supplied CD-ROM".

Reference

- p.136 "Installing the TWAIN Driver from the Supplied CD-ROM"

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. DeskTopBinder Lite is included on the supplied CD-ROM.

For details about installing DeskTopBinder Lite, see "Installing DeskTopBinder Lite from the Supplied CD-ROM".

Reference

- p.117 "Installing DeskTopBinder Lite from the Supplied CD-ROM"

7

Installing the TWAIN Driver from the Supplied CD-ROM

This section explains how to install the TWAIN driver on a client computer from the supplied CD-ROM.

To use the network TWAIN scanner, you must install the TWAIN driver on a client computer.

1. Start Windows, and then insert the CD-ROM labeled into the CD-ROM drive of the client computer.

The installer starts.

2. Click [TWAIN Driver].

3. 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 "Software Supplied on CD-ROM".
- You can install the software using the auto-run program. For details about the auto-run program, see "Auto-Run Program".
- If the installer does not start automatically, see "Auto-Run Program".
- 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.

Reference

- p. 188 "Software Supplied on CD-ROM"
- p. 188 "Auto-Run Program"

Basic Network TWAIN Scanner Procedure

This section explains the basic procedure for scanning with the network TWAIN scanner.

★ Important

- To use the network TWAIN scanner, a TWAIN-compliant application, such as DeskTopBinder and the TWAIN driver must be installed on the client computer.
- Under the Windows XP SP2/Vista or Windows Server 2003/2003 R2/2008 operating system, when the Windows firewall or an antivirus program is enabled, "Cannot find the scanner." or "No response from the scanner." may appear and scanning with the TWAIN scanner may fail. In this case, change the settings of the Windows firewall or antivirus program. For details, see Windows Help.

The following procedure uses Windows XP and DeskTopBinder Lite by way of example.

1. On the [Start] menu, point to [All Programs], point to DeskTopBinder, and then click DeskTopBinder.
2. On the [Tools] menu, click [Scanner Settings...].
3. Click [Select Scanner Driver...].
4. Select the name of the machine you want to use in the list, and then click [Select].
5. Click [OK].
6. Place originals.
7. On the [File] menu, point to [Add Document], and then click [Scan...] to display the Scanner Control dialog box.

The Scanner Control dialog box and DeskTopBinder Viewer will appear.

A dialog box that is used to control a scanner using the TWAIN driver is referred to as the Scanner Control dialog box.

8. Make settings according to such factors as the type of original, type of scanning, and orientation of the original.

For details, see the TWAIN driver Help.

9. In the Scanner Control dialog box, click [Scan].

Depending on the security setting, if you press [Scan], a dialog box for entering the user name and password may appear.

If there are more originals to be scanned, place the next original, and then click [Continue].

If there are no more originals to be scanned, click [Complete].

10. On the [File] menu of the DeskTopBinder Viewer, click [Exit].
11. Enter the document name, and then click [OK].

The DeskTopBinder Viewer closes and the image is stored in DeskTopBinder Lite.

Note

- If you have already selected a scanner, you do not need to select the scanner unless you want to change it.
- Using DeskTopBinder, you can edit and print scan files. For more information about DeskTopBinder, see DeskTopBinder manuals.
- The model name of the connected scanner appears in the title bar of the Scanner Control dialog box. If there is more than one scanner of the same model on the network, make sure you have selected the correct scanner. If you have not, click [Select Scanner Driver...], and then select the scanner again. If the correct scanner does not appear in the list, check that the scanner is correctly connected to the network and that its IPv4 address has been specified. If the correct scanner still does not appear; in the Network Connection Tool that is installed with the TWAIN driver, select the [Use a specific scanner.] check box, and then specify the IP address or host name of the scanner you want to use. For details, see the Help for the Network Connection Tool.
- If you are scanning originals from DeskTopBinder using the network TWAIN scanner, you cannot cancel scanning without first saving the documents. If you are no longer using the documents, save them first, and then delete them using DeskTopBinder.

Scan Settings When Using TWAIN Scanner

This section explains how to specify original orientation and scan setting for a bundle of mixed size originals when using the TWAIN scanner.

Setting Original Orientation on the TWAIN Scanner

To correctly display the top/bottom orientation of the scanned original on a client computer, the placement of the original and the settings made in the Scanner Control dialog box must match.

1. Open the Scanner Control dialog box.

For details about how to open the Scanner Control dialog box, see "Basic Network TWAIN Scanner Procedure".

2. In the [Original Scan Method:] list, select the place where the original is placed.

3. In the [Orig.Orientn.:] list, select [←□ Long Edge] or [←□ Short Edge].

4. In the [Orientation:] list, select [←↻ Right 90 deg. / ↻ Right 90 deg.], [←↻ Left 90 deg. / ↻ Left 90 deg.], [←□ Standard 0 deg. / □ Standard 0 deg.], or [←↻ 180 deg. / ↻ 180 deg.].

5. If an original is placed in the ADF, from the drop down menu of [Scan Settings:], select [1 Sided], [2 Sided(Top to Top)], or [2 Sided(Top to Bottom)].

7

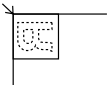

Reference

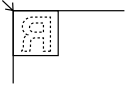

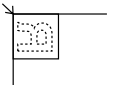

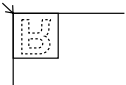

- p.138 "Basic Network TWAIN Scanner Procedure"

Placing Originals









The following table shows the relationship between the original orientation and the Scanner Properties dialog box settings:

Exposure Glass

Original Orientation	TWAIN Scanner Control Dialog Box Key
<p>top edge touches top left of exposure glass</p>  <p>This orientation is the TWAIN driver's standard setting. Place originals in this orientation normally.</p>	

Original Orientation	TWAIN Scanner Control Dialog Box Key
top edge touches rear of exposure glass 	 Standard 0 deg.
bottom edge touches left side of exposure glass 	 Right 90 deg.
bottom edge touches top of exposure glass 	 180 deg.

ADF

Original Orientation	TWAIN Scanner Control Dialog Box Key
top edge of original placed first 	 Left 90 deg.
top edge touches rear of ADF 	 Standard 0 deg.
bottom edge touches left side of ADF 	 Right 90 deg.
bottom edge touches top of ADF 	 180 deg.

Note

- Originals are normally rectangular (R) or horizontally long (LR). However, the table above uses squares to make original orientation easier to understand. Even if the actual shape of the original is different, the combination of original orientation and the orientation specified on the scanner driver does not change.
- For details about the Scanner Control dialog box, see the TWAIN driver Help.
- Depending on the settings, originals of different sizes are scanned differently.

When Scanning Originals of Mixed Sizes Using TWAIN Scanner

This section explains the differences between scanning mixed-size originals using the TWAIN scanner and normal scanning.

- If [Auto detect(Mixed-size)] is selected in the [Original Size:] list, the machine detects the length of each original and then scans them.
- If [Auto detect(Uni-size)] is selected in the [Original Size:] list, the machine detects the size of the first original of the batch and scans all subsequent originals at that size.

Note

- The paper guides cannot be adjusted to small size originals, which may cause slightly tilted scanning.

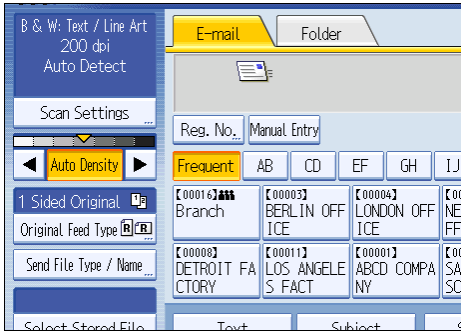
8. Various Scan Settings

This chapter describes various scan settings.

Specifying Scan Settings

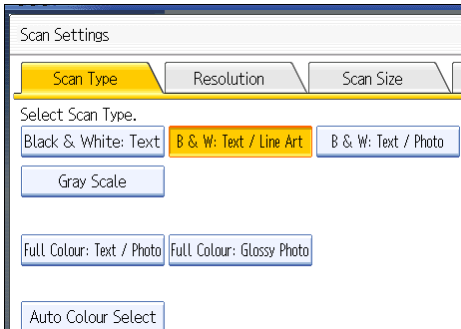
This section explains how to make scan settings.

1. Press [Scan Settings].



2. Specify resolution, scan size, and other settings, as required.

For details about individual scan setting items, see "Scan Settings".



3. Press [OK].

Reference

- p.144 "Scan Settings"

Scan Settings

This section describes the items for Scan Settings.

Scan Type

Select a scan type that is appropriate for your original.

[Black & White: Text]

Appropriate to increase OCR readability using an OCR-compliant application.

- [Dropout Colour]

You can select not to scan the following colors: [Chromatic Colour], [Red], [Green], and [Blue]. When you select a color to leave out of the scan, specify its level of coverage. There are five levels. Press [Narrow] to leave out colors that are closest to the specified color. Press [Wide] to broaden the coverage of the specified color and not scan those colors.

[B & W: Text / Line Art]

Standard black and white originals containing mainly characters. Creates scanned images suitable for printing.

[B & W: Text / Photo]

Originals containing a mixture of photographs, pictures and characters (two-value). Creates scanned images suitable for printing.

[Black & White: Photo]

Originals containing photographs and other pictures (two-value). Creates scanned images suitable for printing.

[Gray Scale]

Originals containing photographs and other pictures (multi-value). Creates scanned images suitable for displaying on a computer screen.

[Full Colour: Text / Photo]

Originals for color printing mainly consisting of characters.

[Full Colour: Glossy Photo]

Originals of silver salt photographs and other color pictures.

[Auto Colour Select]

Scans originals by automatically judging the colors of the originals.

↓ Note

- [Dropout Colour] can be set when [Black & White: Text] is selected for [Scan Type].

- If [Auto Colour Select] is selected, the machine may fail to correctly judge colors depending on the scanning condition or the contents of originals.
- If you select [High Compression PDF] as the file type, you must then select one of the following for Scan Type: [Gray Scale], [Full Colour: Text / Photo], or [Full Colour: Glossy Photo].

Resolution

Select resolution for scanning originals.

Select [100 dpi], [200 dpi], [300 dpi], [400 dpi], or [600 dpi] as the scanning resolution.

Note

- If [High Compression PDF] is selected as the file type, you cannot select [100 dpi]. For details about file types, see "Specifying the File Type and File Name".

Reference

- p.160 "Specifying the File Type and File Name"

Scan Size

Select the size of the original to be scanned.

[Auto Detect]

Scans original sizes using the automatic size detect function.

[Mixed Original Sizes]

Select [Mixed Original Sizes] to scan a batch of originals that have different lengths.

Originals are scanned by the ADF and the length of each is automatically detected.

[Custom Size]

Select [Custom Size] to scan originals whose sizes do not match a standard template or to scan only a part of an original.

You can specify the length and width of your originals in mm or inches.

Template size

Select a template size to scan originals at a specified size regardless of the actual size of the originals you have placed.

You can specify the following template sizes:

A3 \square , A4 \square , A4 \square , A5 \square , A5 \square , B4 JIS \square , B5 JIS \square , B5 JIS \square , 11 × 17 \square , 8 $\frac{1}{2}$ × 14 \square , 8 $\frac{1}{2}$ × 13 \square , 8 $\frac{1}{2}$ × 11 \square , 8 $\frac{1}{2}$ × 11 \square , 5 $\frac{1}{2}$ × 8 $\frac{1}{2}$ \square , 5 $\frac{1}{2}$ × 8 $\frac{1}{2}$ \square

Note

- Selecting both [Mixed Original Sizes] and [Erase Border] reduces the scanning speed.

- You can enter 140 mm (5.5 inches) or higher in Original Size (X1 and Y1) under [Custom Size].

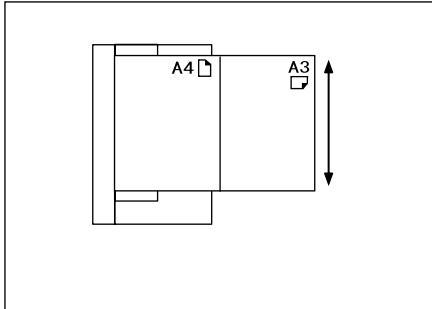
Relationship of original of mixed sizes and scan size

Scanning methods for originals mixed with different sizes (such as A3 & A4 or B4 & B5) differ depending on the settings you make for the scan size and whether you use the exposure glass or the ADF.

- If you select [Mixed Original Sizes], the machine detects the length of each original and scans them.
- If a template size is selected, the machine scans originals at the selected size regardless of the actual size of originals. If an original is smaller than the selected size, the machine applies margins to the scan area.
- If [Auto Detect] is selected for scanning originals from the exposure glass, the machine detects the size of individual originals and scans accordingly.
- If only [Auto Detect] is selected for scanning originals from the ADF, the machine detects the size of the first original and scans all the other originals based on that size.

↓ Note

- When scanning originals of different length at the same time, place them correctly by referring to the chart below. The paper guides cannot be adjusted to small size originals, which may cause slightly tilted scanning.



BPT021S

- If you do not select [Mixed Original Sizes] and place originals of different sizes in the ADF, paper jams might occur or parts of the originals might not be scanned.


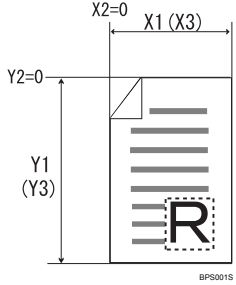

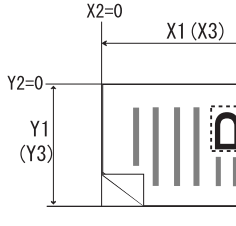
Scanning the entire area of a custom size original

This section explains how to specify a custom size for scanning the entire area of an original. If you want to scan the entire area of a custom size original, select [Custom Size] as the scan size.

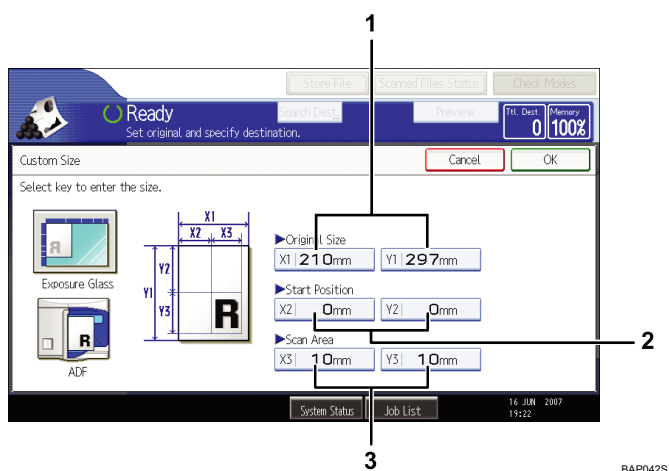
To display the custom size setting screen, on the initial scanner screen, press [Scan Settings] > [Scan Size] > [Custom Size].

The following tables explain how to measure custom size originals and how to specify the scan settings on the custom size settings screen.

How to measure sizes

Orientation and placement of original	Measuring method for scanning the entire area of a custom size original
In the  orientation on the exposure glass or in the ADF	
In the  orientation on the exposure glass or in the ADF	

Scan settings on the custom size setting screen



1. Original Size (X1 and Y1)

Specify the length and width of the original.

Enter the actual width and length in [X1] and [Y1], respectively, and then press the [#] key.

2. Start Position (X2 and Y2)

Set Start Position to 0 mm (0 inch).

Enter "0" in both [X2] and [Y2], and then press the [#] key.

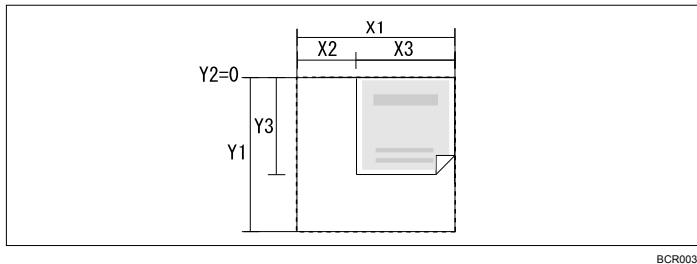
3. Scan Area (X3 and Y3)

Specify the same values as Original Size (X1, Y1).

Enter the same values in [X3] and [Y3] as Original Size (X1 and Y1 respectively), and then press the [#] key.

↓ Note

- For X1 and Y1, you can specify 140 mm (5.5 inches) or larger.
- When scanning originals using [Custom Size], you cannot enter specific values in [Original Size] and [Start Position]. To configure the scan area, specify [Scan Area] and [Start Position] first, and then [Original Size].
- To scan an original that is smaller than 140 mm (5.5 inches), configure the settings as though you were scanning part of an original that is larger than 140 mm (5.5 inches). For example: to scan a CD label on the exposure glass, specify X1~X3 and Y1~Y3 based on the chart below. For details about scanning procedures, see "Scanning part of a custom size original".



- For details about how to place originals, see "Setting of Original Feed Type".

8

📖 Reference

- p.148 "Scanning part of a custom size original"
- p.152 "Setting of Original Feed Type"

Scanning part of a custom size original

If you want to scan only a part of a custom size original, select [Custom Size] as the scan size.


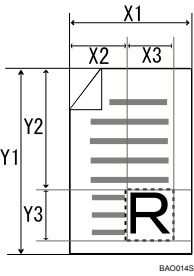

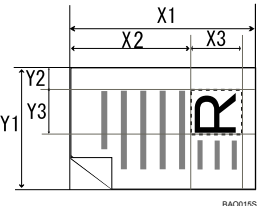

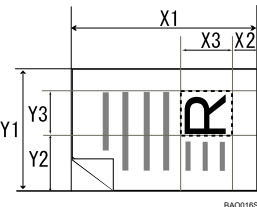
To display the custom size setting screen, on the initial scanner screen, press [Scan Settings] > [Scan Size] > [Custom Size].

To scan part of an original, measure Original Size (X1 and Y1), Start Position (X2 and Y2), and Scan Area (X3 and Y3) on the surface of the original, and then enter those values in the same order on the custom size setting screen.

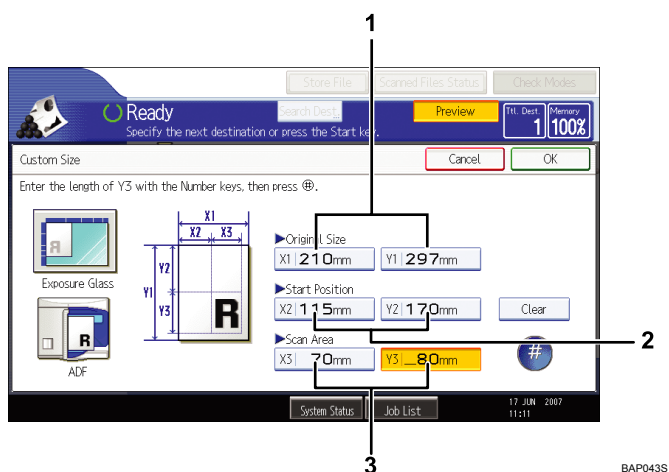
Measuring methods differ depending on where the original is placed and the orientation it is placed in. For details about how to measure Original Size (X1 and Y1), Start Position (X2 and Y2), and Scan Area (X3 and Y3) correctly, see "How to measure sizes".

Enter the sizes while referring to "Scan settings on the custom size setting screen".

How to measure sizes

Orientation and placement of original	Measuring method for scanning the "R" section
In the  orientation on the exposure glass or in the ADF.	 <p style="text-align: center;">BAO0145</p>
In the  orientation in the ADF.	 <p style="text-align: center;">BAO0155</p>
In the  orientation on the exposure glass.	 <p style="text-align: center;">BAO0165</p>

Scan settings on the custom size setting screen



1. Original Size (X1 and Y1)

Specify the original's entire size.

Enter the actual values in [X1] and [Y1] while referring to "How to measure sizes", and then press the [#] key.

2. Start Position (X2 and Y2)

Specify the scanning start position.

Enter the actual values in [X2] and [Y2] while referring to "How to measure sizes", and then press the [#] key.

3. Scan Area (X3 and Y3)

Specify sizes of the area you want to scan.

Enter the actual values in [X3] and [Y3] while referring to "How to measure sizes", and then press the [#] key.

↓ Note

- When scanning originals using [Custom Size], you cannot enter specific values in [Original Size] and [Start Position]. To configure the scan area, specify [Scan Area] and [Start Position] first, and then [Original Size].
- For details about how to place originals, see "Setting of Original Feed Type".

📖 Reference

- p.152 "Setting of Original Feed Type"

Edit

Make editing settings.

[Erase Border]

Deletes the borders of the scanned original according to the specified width.

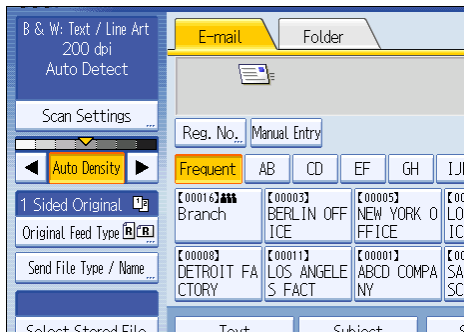
If you select [Same Width], you can specify a uniform width for deletion all around the original (top, bottom, left, and right sides). If you select [Different Width], you can specify a different width for deletion for each side.

Adjusting Image Density

This section explains how to adjust image density.

To adjust image density, press [◀] or [▶], at the left and right of [Auto Density]. These buttons increase or decrease the image density in single increments up to 7.

Selecting [Auto Density] corrects scanning density to improve resolution of paper types such as non-white paper like newspaper or transparent originals.



Note

- When scanning originals in full color, you can specify the [Auto Density] level in [Background Density of ADS (Full Colour)] under [Scanner Features]. For details, see "Scan Settings".

Reference

- p.179 "Scan Settings"

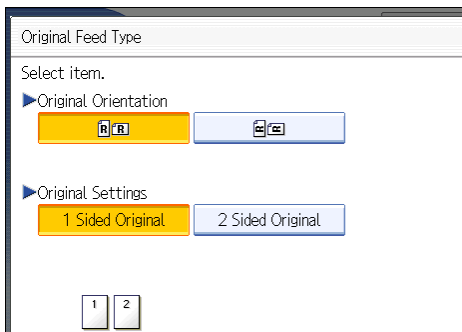
Setting of Original Feed Type

This section explains Original Feed Type settings such as orientation and scan sides of originals.

Original Orientation

This section explains how to correctly display the top/bottom orientation of scanned originals on a client computer screen.

1. Press [Original Feed Type].
2. Press [R/R] or [L/L] to select the same orientation as that of original.



3. Press [OK].

8

Placing Originals

To correctly display the top/bottom orientation of the scanned original on a client computer, the placement of the original and the settings made on the control panel must match.

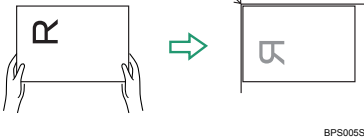

Place originals correctly by referring to the following tables:

Exposure Glass

Place the original face down on the exposure glass in either the left-right (landscape) or up-down (portrait) orientation.

Original orientation and control panel key selection

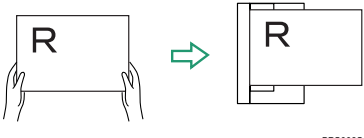

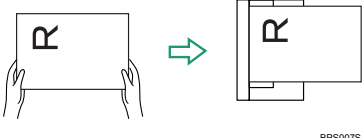

Original orientation	Control panel key
top edge touches rear of exposure glass 	

Original orientation	Control panel key
<p>top edge touches top left corner of exposure glass</p>  <p style="text-align: right; font-size: small;">BPS006S</p>	

ADF

Hold the original so that its text is in the natural readable orientation, and then place it face up in the ADF.

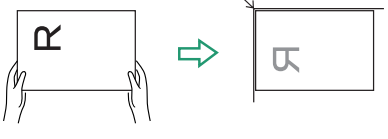
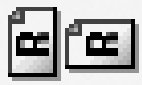
Original orientation and control panel key selection

Original orientation	Control panel key
<p>top edge touches rear of ADF</p>  <p style="text-align: right; font-size: small;">BPS008S</p>	
<p>top edge placed first</p>  <p style="text-align: right; font-size: small;">BPS007S</p>	

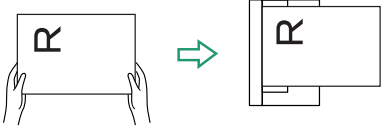

↓ Note

- When you specify full color, gray scale, or [Auto Colour Select] for Scan Type, and single page TIFF/JPEG or multi-page TIFF is selected as the file type, refer to the tables below for how to place originals. Originals placed in orientations that are not recommended in the table might appear incorrectly top/bottom oriented on client computer displays.

Exposure glass

Original orientation	Control panel key
<p>top edge touches top left corner of exposure glass</p>  <p style="text-align: right; font-size: small;">BPS005S</p>	

ADF

Original orientation	Control panel key
<p>top edge placed first</p>  <p style="text-align: right; font-size: small;">BPS007S</p>	

Original Settings

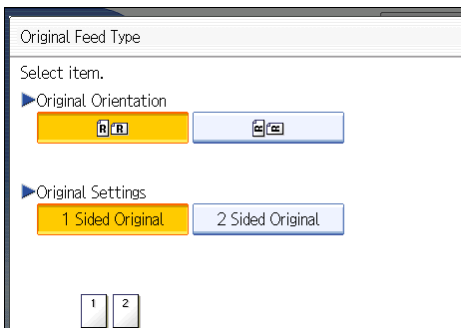
8

This section explains the settings for the scanning the sides of originals.

One-sided original

This section explains the settings for scanning only one side of originals.

1. Press [Original Feed Type].
2. In [Original Settings], select [1 Sided Original].

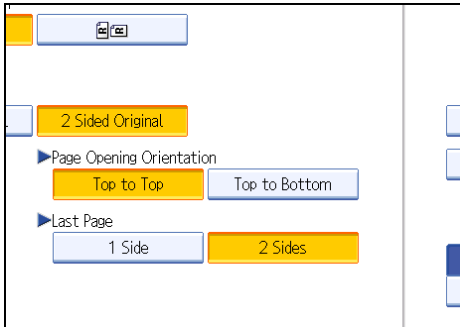


3. Press [OK].

Two-sided original

This section explains the settings for scanning both sides of originals.

1. Press [Original Feed Type].
2. In [Original Settings], select [2 Sided Original].
3. In [Page Opening Orientation], select [Top to Top] or [Top to Bottom] according to the binding orientation of the originals.



Binding orientation and required page opening orientation

Binding orientation	Page opening orientation
	Top to Top
	Top to Bottom

4. If the last page of the last original is blank, in [Last Page], select [1 Side] or [2 Sides].

To skip the last page, select [1 Side].

To scan the last page as blank page, select [2 Sides].

5. Press [OK].

⬇ Note

- If you selected [Divide], the setting made here is applied to the last page of each batch of divided originals.

Batch, SADF

This section explains the settings you need to configure if you want to scan a large number of originals in several batches and send them together as a single job.

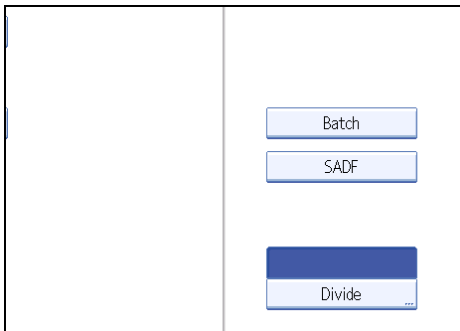
To scan originals in several batches using the [Start] key, select [Batch].

To scan the originals individually in the ADF, select [SADF].

- If you select [Batch], scanning starts when you place the additional originals and press the [Start] key. When all the originals have been scanned, press the [#] key. If you select [Batch], regardless of the default settings, the machine waits until additional originals are placed.
- If [SADF] is selected, scanning starts as soon as you place additional originals in the ADF. Select which operation the machine performs while waiting for additional originals in [Wait Time for Next Original(s): SADF] under [Scanner Features]. For details about [Wait Time for Next Original(s): SADF], see "Scan Settings".

1. Press [Original Feed Type].

2. Select [Batch] or [SADF].



3. Press [OK].

8 Note

- If [SADF] is selected, scanning starts as soon as you place additional originals in the ADF. However, in the following cases you must press the [Start] key to start scanning additional originals.
 - After scanning additional originals using the exposure glass
 - After changing settings while waiting for additional originals
 - After opening/closing the ADF
- For more details about procedures, see "Scanning Multiple Pages of Originals as One File".

Reference

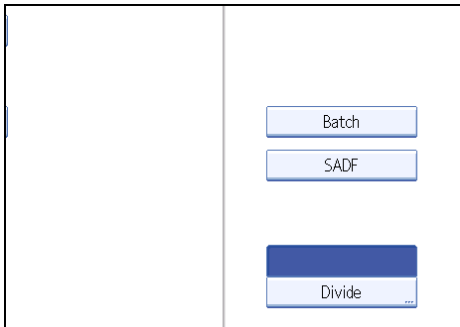
- p.179 "Scan Settings"
- p.158 "Scanning Multiple Pages of Originals as One File"

Divide

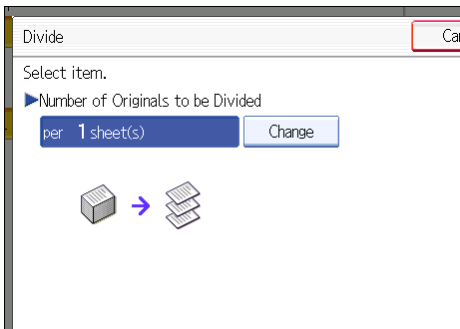
This section explains settings for dividing multiple originals by a specified number of pages and then sending them.

1. Press [Original Feed Type].

2. Press [Divide].



3. Press [Change], and then use the number keys to enter the number of pages you want to divide the job into sets of.



4. Press the [#] key.

5. If necessary, press [Division Check].

When you select [Division Check], if the originals were not scanned in order due to a paper jam or multi-sheet feed, a screen for stopping or continuing scanning appears at the end of the scan.

6. Press [OK] twice.

The current settings are displayed.

↓ Note

- If the last page of a batch of divided two-sided originals is blank, you can skip that page. To skip scanning, in [Last Page] under [2 Sided Original], select [1 Side]. To scan the last page as a blank page, select [2 Sides]. For details, see "Two-sided original".

📖 Reference

- p.155 "Two-sided original"

Scanning Multiple Pages of Originals as One File

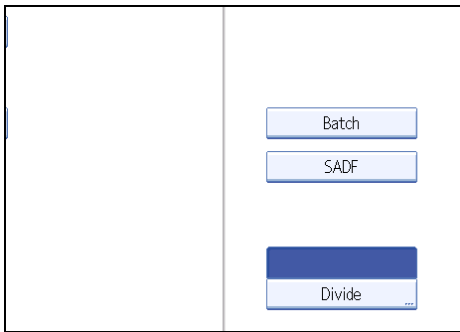
This section explains the procedure for sending multiple originals as a multi-page file or storing them as a single stored file.

★ Important

- To send multiple originals as a multi-page file, in [Send File Type / Name], select a multi-page file type. For details about file types, see "Specifying the File Type".

1. Press [Original Feed Type].
2. Select [Batch] or [SADF].

To scan originals using the exposure glass, select [Batch]. To scan originals using the ADF, select [SADF]. For detail about [Batch] and [SADF], see "Batch, SADF".



3. Press [OK].
4. Place originals.
5. Make settings for sending or storing.
6. Press the [Start] key to scan originals.

If [Batch] is selected, place additional originals, and then press the [Start] key.

If [SADF] is selected, scanning starts automatically when you place additional originals. Place subsequent originals after the originals have been scanned.

Repeat this step until all originals are scanned.

7. After all originals are scanned, press the [#] key.

Storing or transmission starts.

↓ Note

- If [Batch] is selected, originals can be scanned using the ADF.
- When scanning originals using the exposure glass, depending on the settings for [Wait Time for Next Orig.: Exposure Glass] under [Scanner Features], the machine can wait for additional originals even if [Batch] is not selected in [Original Feed Type]. For details about [Wait Time for Next Orig.: Exposure Glass], see "Scan Settings".

- If, under [Scanner Features], [Set Wait Time] is set for [Wait Time for Next Orig.: Exposure Glass] or [Wait Time for Next Original(s): SADF], place additional originals within the specified time. When the countdown ends, transmission or storage starts automatically. To start transmission or storage before the countdown is completed, press the [#] key. Countdown is canceled if Scan Settings or other settings are changed in the meantime. Place additional originals, and then press the [Start] key. The machine scans the originals and the countdown is resumed. For details about [Wait Time for Next Orig.: Exposure Glass] and [Wait Time for Next Original(s): SADF], see "Scan Settings".
- If [SADF] is selected, scanning from the exposure glass is enabled after scanning from the ADF. If this happens, you must press the [Start] key to start scanning.

Reference

- p.155 "Batch, SADF"
- p.160 "Specifying the File Type"
- p.179 "Scan Settings"

Specifying the File Type and File Name

This section explains the procedure for specifying the file type, file name, and security for PDF files.

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: [TIFF / JPEG], [PDF], [High Compression PDF]

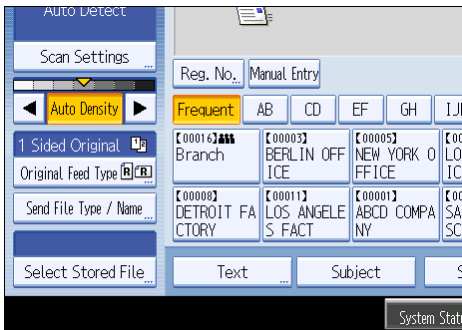
If you select a single-page file type when scanning multiple originals, one file is created for each single page and the number of files sent is the same as the number of pages scanned.

- Multi-page: [TIFF], [PDF], [High Compression PDF]

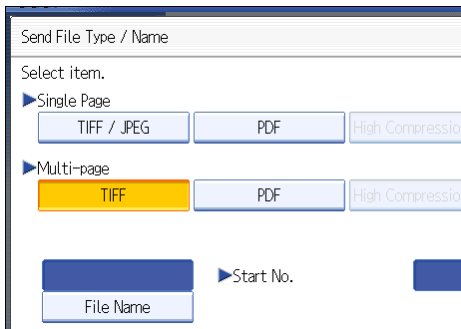
If you select a multi-page file type when scan multiple originals, scanned pages are combined and sent as a single file.

Selectable file types differ depending on the scan settings and other conditions. For details about file types, see "Notes About and Limitations of File Types".

1. Press [Send File Type / Name].



2. Select a file type.



3. Press [OK].

Note

- To deliver files, specify the file type using the delivery server computer. For details, see the manuals provided with the ScanRouter delivery software.
- If you select [Store to HDD] under [Store File], you cannot specify the file type.
- If you select [Store to HDD + Send] under [Store File], files are sent in the specified file type by e-mail or Scan to Folder. However, files cannot be stored in the specified format—instead, they are automatically stored in one of the following file types, depending on the compression and Scan Type settings:
 - JPEG
 - Under [Scanner Features], [Compression (Gray Scale / Full Colour)] is set to [On], and originals are scanned in full color or gray scale.
 - TIFF
 - All other scanings
- The version of the created PDF files is 1.4.
- High Compression PDF files retain the character legibility of uncompressed PDF files but have much lower data volume. For details about the limitations of High Compression PDF files, see "Notes About and Limitations of File Types".

Reference

- p.161 "Notes About and Limitations of File Types"

Notes About and Limitations of File Types

Depending on the file format you select, the following limitations will apply:

Single Page [TIFF / JPEG]

- Originals scanned in black and white are sent as TIFF files.

- According to the settings specified for [Compression (Gray Scale / Full Colour)] under [Scanner Features], originals scanned in full color or gray scale are sent in one of the following file types:
 - [On] : JPEG file
 - [Off] : TIFF file

Multi-page [TIFF]

- When full color, gray scale, or [Auto Colour Select] is specified under [Scan Type] and [Compression (Gray Scale / Full Colour)] is set to [On] under [Scanner Features], you cannot select [TIFF] under [Multi-page].
- Even if you select [TIFF] under [Multi-page], files stored in JPEG format are automatically changed to multi-page PDF files and then sent.

High Compression PDF

- You cannot select [High Compression PDF] if:
 - [Store to HDD + Send] is selected under [Store File].
 - [Black & White: Text], [B & W: Text / Line Art], [B & W: Text / Photo], [Black & White: Photo], or [Auto Colour Select] is selected under [Scan Type].
 - [100 dpi] is selected as the resolution.
 - [Preview] is selected.
 - The machine is working with the ScanRouter delivery software and the Capture function is in use. For details about the capture function, see the manuals provided with the ScanRouter delivery software.
- Adobe Acrobat Reader 5.0 / Adobe Reader 6.0 and later versions support High Compression PDF.
- High Compression PDF files cannot be displayed correctly using DeskTopBinder Easy Viewer. For details about the capture function, see the manuals supplied with the ScanRouter delivery software.

Specifying the File Name

This section explains the procedure for specifying a file name.

Scanned file will be given a file name consisting of the time and date of scanning, 4-digit page number, etc.

- Single-page and divided multi-page files are assigned file names that contain the date and time of scanning and a four-digit page number. An underscore is inserted between the date and time and the four-digit page number.

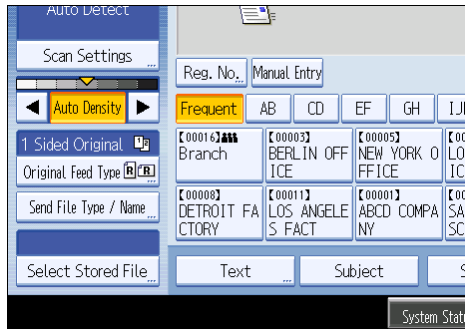
(Example: For a file scanned in single-page TIFF at 10 ms, 15 sec., 15:30 hours on Dec. 31, 2020, the file name will be 20201231153015010_0001.tif)

- Multi-page files are given file names that contain the time and date of scanning.

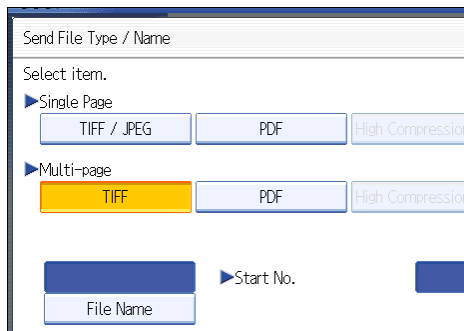
(Example: For a file scanned in multi-page TIFF at 10 ms, 15 sec., 15:30 hours on Dec. 31, 2020, the file name will be 20201231153015010.tif)

If necessary, you can change the file name.

1. Press [Send File Type / Name].



2. Press [File Name].



The soft keyboard appears.

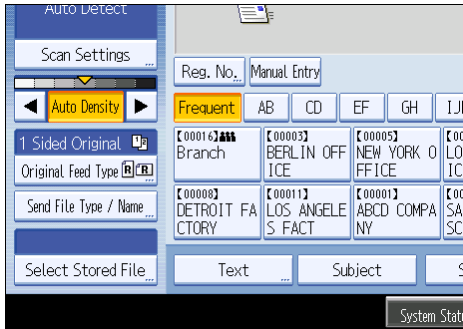
3. Enter a file name.

4. Press [OK] twice.

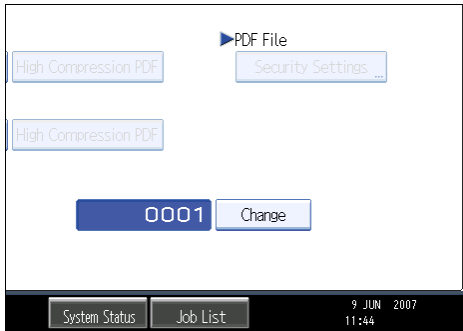
Changing the starting digit of file name serial numbers

A single-page file is assigned a serial number after the file name. The starting number of this serial number can be changed as follows:

1. Press [Send File Type / Name].



2. Press [Change] to the right of the entry box.



3. Using the number keys, enter the starting digit of the serial number.

4. Press the [#] key.

5. Press [OK].

Note

- You can change the starting digit only if a single-page file type is selected.
- You can change the number of digits in the serial number. Change the number under [Scanner Features], [No. of Digits for Single Page Files]. You can select 4 or 8.

Security Settings for PDF Files

This section explains security settings for PDF files.

Use security settings to prevent unauthorized access to PDF files.

★ Important

- Security settings can be made for PDF and High Compression PDF files only.

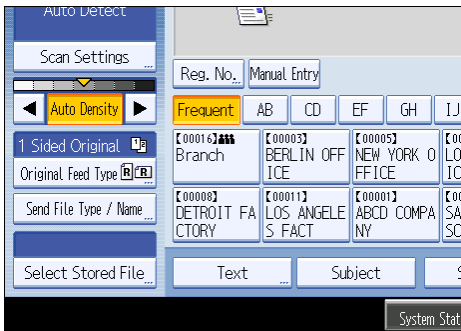
Encrypting PDF files

Set a document password to protect and encrypt a PDF file. Only users who have the password can open and decrypt the PDF file.

★ Important

- Encryption is possible only for scan files that are sent by e-mail or Scan to Folder and saved on a removable memory device.
- You cannot open an encrypted file without a document password. Make sure you do not forget the file's password.

1. Press [Send File Type / Name].

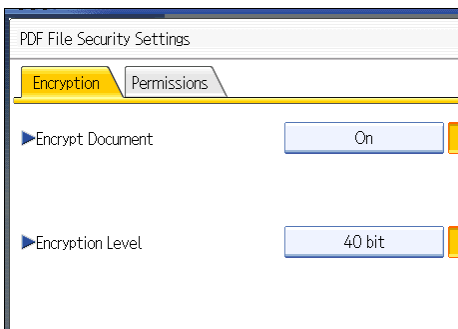


2. Check that [PDF] or [High Compression PDF] is selected.

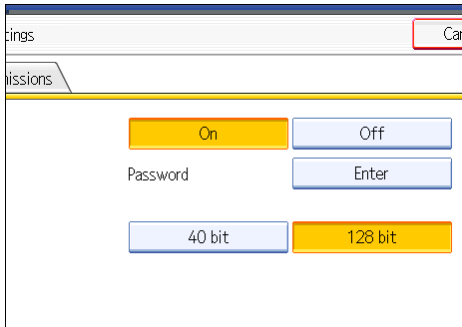
3. Press [Security Settings].

4. Select [Encryption].

5. In [Encrypt Document], select [On].



6. In [Password], press [Enter].



7. Enter a password, and then press [OK].

The password entered here will be required to open the PDF file.

8. Enter the password again to confirm it, and then press [OK].

9. In [Encryption Level], select [40 bit] or [128 bit].

10. Press [OK] twice.

↓ **Note**

- A document password cannot be the same as the master password.
- Document passwords can contain up to 32 alphanumeric characters.
- You cannot use Adobe Acrobat Reader 3.0 or 4.0 to view PDF files that were created using [128 bit] encryption.
- If [Low Resolution Only] is selected as the print permission, you cannot select [40 bit] as the PDF encryption level.

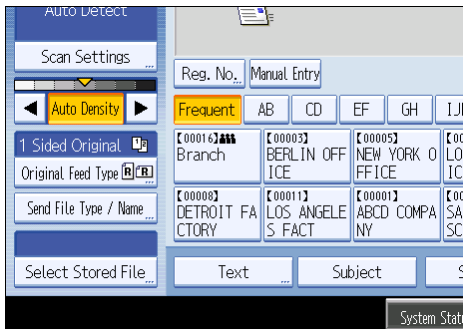
Changing security permissions for PDF files

Set a master password to restrict unauthorized printing, changing, copying, or extracting of a PDF file's content. Only users who have the master password can reset or change these restrictions.

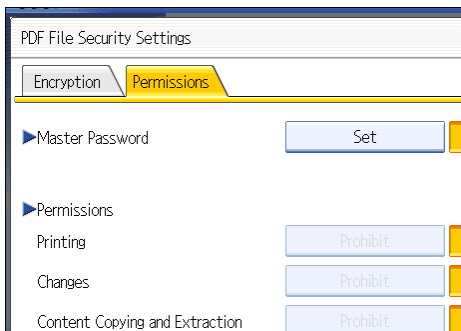
★ **Important**

- Encryption is possible only for scan files that are sent by e-mail or Scan to Folder and saved on a removable memory device.
- You cannot reset or change a file's restriction settings without the master password. Write down the master password and keep it secure.

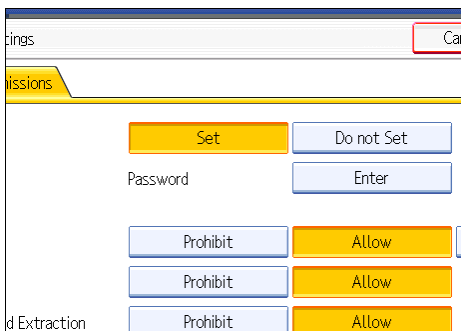
1. Press [Send File Type / Name].



- 2. Check that [PDF] or [High Compression PDF] is selected.**
- 3. Press [Security Settings].**
- 4. Select the [Permissions] tab.**
- 5. In [Master Password], select [Set].**



6. In [Password], press [Enter].



7. Enter a password, and then press [OK].

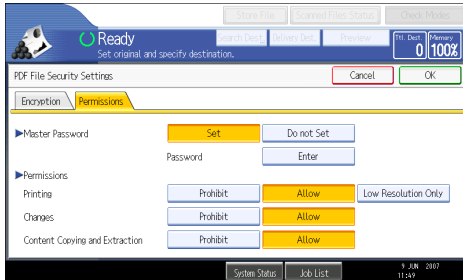
The password entered here will be required to change the security settings of the PDF file.

8. Enter the password again to confirm it, and then press [OK].

9. Select the security permission setting.

You can specify the following security settings:

- Print permission: [Prohibit], [Allow], or [Low Resolution Only]
- Editing permission: [Prohibit] or [Allow]
- Copying or extracting content permission: [Prohibit] or [Allow]



10. Press [OK] twice.

Note

- The master password cannot be the same as a document password.
- Master passwords can contain up to 32 alphanumeric characters.
- If [40 bit] is selected as the PDF encryption level, you cannot select [Low Resolution Only] as the print permission.

Programs

You can register frequently used settings in the machine memory and recall them for future use.

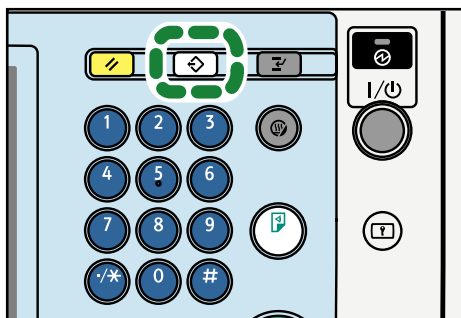
Note

- You can register up to 10 programs for the scanner mode.
- Programs are not deleted by turning the power off or by pressing the [Clear Modes] key unless the content is deleted or newly registered.
- The following settings can be registered to programs: Scan Settings, 1 Sided/2 Sided Original, Top to Top/Top to Bottom, 1 Side/2 Sides for the Last Page, Divide, Original Orientation, File Type, Batch/SADF, Store File, Preview, Reception Notice, and Security (E-mail Encryption and Signature).
- Setting made on the simplified display cannot be registered to a program.

Registering Frequently Used Settings

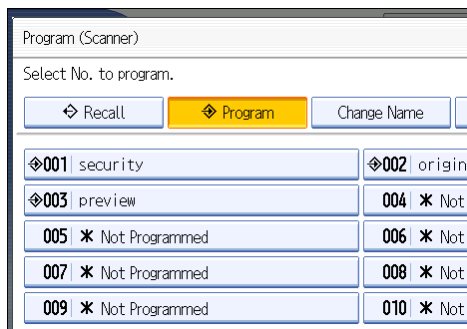
To register frequently used settings in a program:

1. On the initial scanner screen, make the settings you want to register in a program.
2. Press the [Program] key.



BQC001S

3. Press [Program].




4. Select the number of the program in which you want to register the settings.

Program numbers with  already have settings in them.

5. Enter the program name.

6. Press [OK].

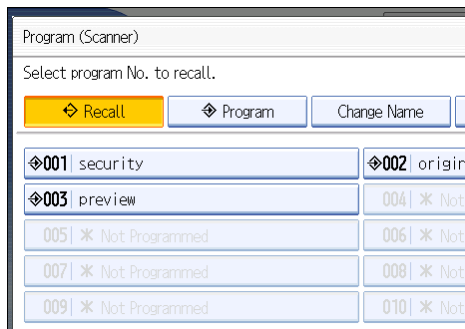
The Program screen reappears. When the settings are successfully registered,  appears on the left side of the registered program number and the program name appears on the right side. The initial screen reappears after a moment.

Recalling a Registered Content

To recall settings registered in a program and use them for scanning:


1. Press the [Program] key.

2. Press [Recall].



3. Press the number of the program you want to recall.

Settings registered in the program are recalled and the initial scanner screen reappears.

Settings are not registered in numbers that appear without .

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

Changing a Registered Program

To change the settings registered to a program:

1. Press the [Program] key.

2. Press [Recall].

3. Press the number of the program you want to change.

Settings registered in the program are recalled and the initial scanner screen reappears.

4. Change settings of the program.

5. Press the [Program] key.
6. Press [Program].
7. Press the number of the program whose settings you changed or the number of a different program in which you want to register the changed settings.
8. If you select a program that is already registered, a confirmation message appears. To overwrite the program, press [Yes].

If you select a new program number, you can omit this step. Proceed to the next step.

9. Enter a program name.
10. Press [OK].

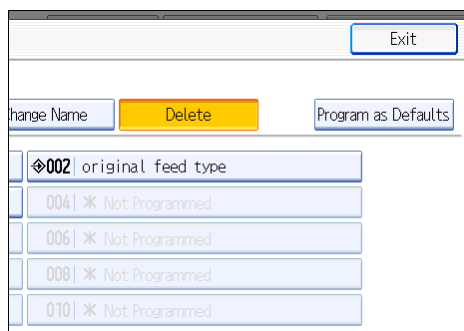
If overwritten, the registered program is deleted.

The new program name appears briefly, and then the initial screen reappears after a moment.

Deleting a Program

To delete a registered program:

1. Press the [Program] key.
2. Press [Delete].



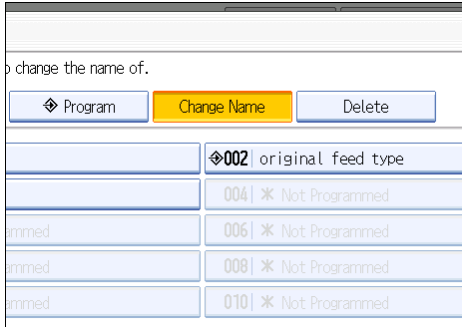
3. Press the number of the program you want to delete.
A confirmation screen appears.
4. Press [Yes].
The program is deleted, and the initial screen reappears after a moment.

Changing the Registered Program Name

To change the name of a registered program:

1. Press the [Program] key.

2. Press [Change Name].



3. Press the number of the program whose name you want to change.

The soft keyboard appears.

4. Enter a new program name.

5. Press [OK].

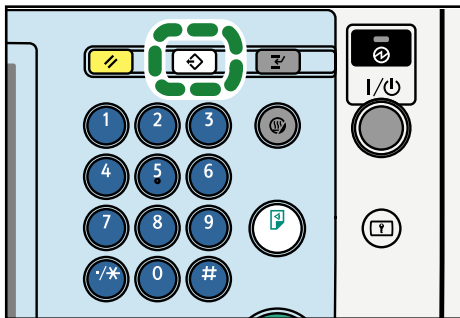
The new program name appears briefly, and then the initial screen reappears.

Changing the Default Functions of the Scanner's Initial Display

This section explains how to set defaults for the initial screen, which appears when the machine is turned on or when settings are cleared or reset.

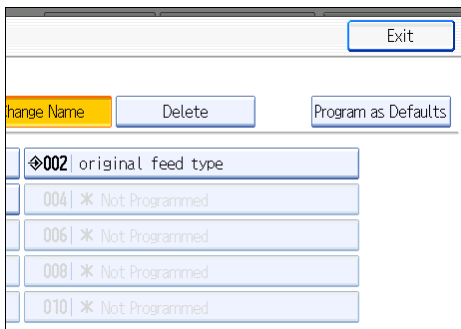
The following settings can be registered as defaults: Scan Settings, 1 Sided/2 Sided Original, Top to Top/Top to Bottom, 1 Side/2 Sides for the Last Page, Divide, Original Orientation, File Type, Batch/SADF, Store File, Preview, Reception Notice, and Security (E-mail Encryption and Signature).

1. Make the necessary scan settings on the initial screen.
2. Press the [Program] key.



BQC001S

3. Press [Program as Defaults].



4. Press [Program].

A confirmation screen appears.

5. Press [Yes].

The current settings are registered as defaults, and then the initial screen reappears.

↓ Note

- To restore the initial screen's original default settings, press [Restore Factory Defaults].

- Default settings for the initial screen can be registered for normal screens and simplified displays respectively.

9. Scanner Features

This chapter describes the user tools in the Scanner Features menu.

Accessing User Tools

This section describes how to access User Tools.

User Tools allows you to change the settings of [Scanner Features].

↓ Note

- Procedures for configuring system settings differ from procedures for configuring other settings. You must return to the initial screen when you finish configuring the system settings. For details about returning to the initial screen, see "Closing User Tools".
- Any changes you make in [Scanner Features] remain in effect even if the main power switch or operation switch is turned off, or the [Energy Saver] or [Clear Modes] key is pressed.
- Depending on the sending method, some settings cannot be applied.

📖 Reference

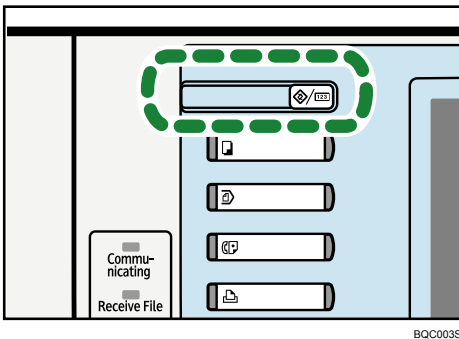
- p.176 "Closing User Tools"

Changing User Tools

This section describes how to change the settings of [Scanner Features].

★ Important

- If Administrator Authentication Management is specified, contact your administrator.
1. Press the [User Tools/Counter] key.



2. Press [Scanner Features].
3. Select the item you want to change.
4. Change settings by following instructions on the display, and then press [OK].

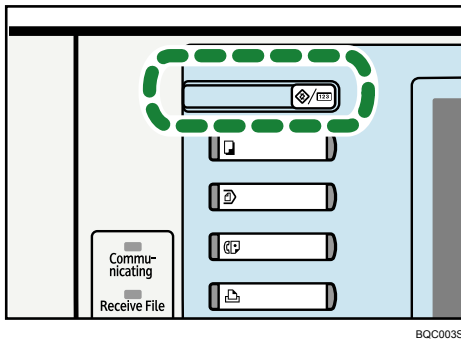
Note

- To cancel changes made to the settings and return to the initial display, press the [User Tools/Counter] key.

Closing User Tools

This section describes how to quit User Tools.

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



Note

- You can also quit User Tools by pressing [Exit].

General Settings

This section describes the user tools on the [General Settings] tab in [Scanner Features].

Default settings are shown in **bold type**.

Switch Title

Select the title to be shown on the destination list.

The default setting is **Title 1**.

Update Delivery Server Destination List

Press [Update Delivery Server Destination List] to update the receivers from the delivery server. To use this function, it is necessary to set [Delivery Option] to [On].

For details about "Delivery Option", see "File Transfer", Network and System Settings Guide.

Search Destination

Select a destination list to be used in "Search Destination". To search from LDAP server, it is necessary to register the LDAP server in [System Settings] and set [LDAP Search] to [On].

The default setting is **Address Book**.

For details about "LDAP Search", see "Administrator Tools", Network and System Settings Guide.

TWAIN Standby Time

If the machine receives a TWAIN scanning request while it is writing data to memory or performing e-mail, Scan to Folder, network delivery, or WSD scanning jobs, it switches to the network TWAIN scanner function either immediately or after a specified standby time elapses following the last key operation.

Use this setting to select whether the machine switches to TWAIN immediately or waits until the standby time elapses when it receives a TWAIN scanning request.

The default setting is **Set Time, 10 second(s)**.

If you select [Immediate], the machine will switch to the network TWAIN scanner function immediately.

If you select [Set Time], enter a standby time using the number keys (3-30 seconds). The machine will switch to the network TWAIN scanner function when the time set here elapses following the last key operation.

Destination List Display Priority 1

Select a destination list to be displayed when the machine is in the initial state.

You can select [E-mail / Folder], [Delivery Server], or [WSD].

The default setting is **Delivery Server**.

Destination List Display Priority 2

In the machine's address book, select which address book appears by default.

You can select either [E-mail Address] or [Folder].

The default setting is **E-mail Address**.

Print & Delete Scanner Journal

Up to 250 transmission/delivery results can be checked on this machine. If the stored transmission/delivery results reach 250, select whether to print the delivery journal.

The default setting is **On**.

- On

The transmission/delivery journal is printed automatically. The printed journal is deleted.

- Off

Transmission/delivery results are deleted one by one as new results are stored.

- Do not Print: Disable Send

Transmission/delivery cannot be performed when the journal is full.

When printed, all records are deleted after printing. When not printed, records over the limit are automatically deleted in succession from the oldest record.

While the journal is being printed, files with the status waiting cannot be sent.

Print Scanner Journal

The scanner journal is printed and deleted.

Delete Scanner Journal

The scanner journal is deleted without being printed.

Scan Settings

This section describes the user tools in the [Scan Settings] tab under [Scanner Features].

Default settings are shown in **bold type**.

A.C.S. Sensitivity Level

Sets the sensitivity level for judging color/black and white for scanning originals when [Scan Type] is set to [Auto Colour Select].

The default setting is the middle of 5 adjustment levels.

Wait Time for Next Orig.: Exposure Glass

If you want to divide your originals and scan them separately using the exposure glass and then send them together as a single job, select [Continuous Wait], [Off], or [Set Wait Time] as the waiting status.

The default setting is **Set Wait Time, 60 second(s)**.

If you specify [SADF] or [Batch] for the [Original Feed Type] setting, the [Wait Time for Next Orig.: Exposure Glass] setting becomes invalid.

If [Off] is selected, the machine forwards the scan data as soon as it finishes scanning each original.

If [Set Wait Time] is selected, enter the wait time in seconds (3-999) for placing additional originals with the number keys. Scanning will start if additional originals are placed and the [Start] key is pressed within this time. You can end scanning and begin transmission by pressing the [#] key within this time. Once the specified time has elapsed, transmission starts automatically.

If [Continuous Wait] is selected, the machine will wait for additional originals until the [#] key is pressed. Scanning will start when additional originals are placed and the [Start] key is pressed. You can end scanning and begin sending by pressing the [#] key.

If originals are placed in the ADF (auto document feeder), transmission will start without waiting for additional originals after all originals in the ADF have been scanned, regardless of the specified settings.

If a paper misfeed occurs or any of the following operations are performed while the machine is waiting for additional originals, the countdown stops and does not start again until the [#] key is pressed.

- Changing the settings such as the scan settings
- Opening the upper cover of the ADF
- Pressing the [Interrupt] key to activate the copy mode

Wait Time for Next Original(s): SADF

If you want to divide your originals and scan them separately using the ADF and then send them together as a single job, select [Set Wait Time] or [Continuous Wait] as the waiting status.

The default setting is **Set Wait Time, 60 second(s)**.

This setting is valid if [SADF] is specified for [Original Feed Type] when scanning.

If [Set Wait Time] is selected, enter the wait time in seconds (3-999) for placing additional originals with the number keys. Scanning will start automatically if additional originals are placed within this time. You can end scanning and begin transmission by pressing the [#] key within this time. Once the specified time has elapsed, transmission starts automatically.

If [Continuous Wait] is selected, the machine will wait for the additional originals until the [#] key is pressed. Scanning will start automatically when additional originals are placed. You can end scanning and begin sending by pressing the [#] key.

Even if originals are placed on the exposure glass, the machine will operate according to the specified settings. However, every time originals are placed on the exposure glass, you must press the [Start] key to start scanning.

If a paper misfeed occurs or any of the following operations are performed while the machine is waiting for additional originals, the countdown stops and does not start again until the [#] key is pressed.

- Changing the settings such as the scan settings
- Opening the upper cover of the ADF
- Pressing the [Interrupt] key to activate the copy mode

Background Density of ADS (Full Colour)

Characteristics due to the type of paper such as nonwhiteness like newspaper or transparent originals can be reduced by correcting the scanning density.

The default setting is the middle of 5 adjustment levels.

Send Settings

This section describes the user tools in the [Send Settings] tab under [Scanner Features].

Default settings are shown in **bold type**.

Compression (Black & White)

Select whether or not to compress black and white scan files.

The default setting is **On**.

Compression reduces the time required for transferring the scan file.

The actual time required for file transfer will vary depending on the file size and network load.

Compression (Gray Scale / Full Colour)

Specify whether or not to compress multi-level (grayscale / full color) scan files.

The default setting is **On**.

If you select [On], you can specify the compression level between one and five.

The image quality is better for lower compression, but the time required for file transfer increases accordingly.

The actual time required for file transfer will vary depending on the file size and network load.

High Compression PDF Level

Select compression level when creating high compression PDF files.

The default setting is **Standard**.

Max. E-mail Size

Select whether or not to limit the size of an e-mail to which an image is attached.

The default setting is **On, 2048KB**.

When [On] is selected, enter the size limit (128-102400 KB) with the number keys.

When the SMTP limits the size, match that setting.

Divide & Send E-mail

This function is effective only when [On] is selected for [Max. E-mail Size].

Select whether or not an image exceeding the size specified in [Max. E-mail Size] should be divided and sent using more than one e-mail.

The default setting is **Yes (per max. size)**.

The default maximum number of divisions is **5**.

When [Yes (per Max. Size)] is selected, enter the Max. Number of Divisions (2- 500) with the number keys.

When [TIFF] or [PDF] under [Multi-page] is selected for [File Type], the image will not be divided even if [Yes (per Page)] is selected.

When [Yes (per Max. Size)] is selected, some received files may not be able to be restored, depending on the type of e-mail software.

When [No] is selected, the e-mail is not sent if its size exceeds the limit, and an error message appears. The scan file is discarded.

Set the maximum e-mail size within the capacity of the SMTP server.

Insert Additional E-mail Info

Select the language in which e-mail information such as title, document name, and sender's name is sent.

If you select [On], select one of the following 22 languages:

British English, American English, German, French, Italian, Spanish, Dutch, Portuguese, Polish, Czech, Swedish, Finnish, Hungarian, Norwegian, Danish, Japanese, Simplified Chinese, Traditional Chinese, Russian, Hangul, Catalan, and Turkish.

The default setting is **On, British English**.

The e-mail text which is a template cannot be changed.

No. of Digits for Single Page Files

Sets digit number for serial number to attach to Single Page file name.

The default setting is **4 Digits**.

Stored File E-mail Method

Specify the e-mail setting for sending stored files. You can select [Send File] or [Send URL Link]. This setting can be used for the following:

The default setting is **Send File**.

- Send File
Sending Stored Files by E-mail
- Send URL Link
Simultaneous Storage and Sending by E-mail

If you select [Send File], actual files are attached to e-mails.

If you select [Send URL Link], URL links to file locations are attached to e-mails.

If [Send URL Link] is selected in [Stored File E-mail Method], a phishing warning may appear after you receive a stored file e-mail, depending on your e-mail application. To prevent phishing warnings appearing after you receive a stored file e-mail, you must add the sender to your e-mail application's exclusion list. For details about how to do this, see your e-mail application's Help.

Default E-mail Subject

If an e-mail subject is not entered on the machine's control panel, the default e-mail subject is applied when scan files are sent by e-mail.

Select whether to use the host name or a specified text as the default e-mail subject.

The default setting is **Host Name**.

If you select [Host Name], the host name configured on the [Interface Settings] tab under [System Settings] is applied.

Initial Settings

This section describes the user tools in the [Initial Settings] tab under [Scanner Features].

Menu Protect

You can specify user access levels for functions whose settings can be changed by users other than the administrator. Using Menu Protect, you can prevent unauthenticated users from changing the user tools.

Menu Protect is a Scanner Features setting item. You can also specify user access levels for each function's default setting.

For details, consult your administrator.

10. Appendix

Relationship between Resolution and Scan Size

This section explains the relationship between resolution and scan size.

Resolution and scan size are inversely related. The higher the resolution (dpi) is set, the smaller the area that can be scanned. Similarly, the larger the scan area, the lower the resolution that can be set.

The relationship between the scanning resolution and scan size is shown below. If the combination is unreadable, "Exceeded max. data capacity. Check the scanning resolution, then press the Start key again." appears on the machine's control panel display. Change the condition until scanning is enabled.

↓ Note

- Image compression level can limit Maximum image size.

When Using the E-mail, Folder Sending, WSD Scanner, Storing, or Network Delivery Functions

This section explains the relationship between resolution and scan size when using the e-mail, Scan to Folder, WSD Scanner, storing, or network delivery functions.

If [Black & White: Text], [B & W: Text / Line Art], [B & W: Text / Photo], [Black & White: Photo], or [Gray Scale] is selected for Scan Type:

All combinations up to A3 and 600 dpi can be scanned.

If [Full Colour: Text / Photo] or [Full Colour: Glossy Photo] is selected as Scan Type:

The scan size determines the maximum resolution possible.

Refer to the table below for the maximum resolution available for each scan size.

Scan size and maximum resolution

Scan size	Maximum resolution (dpi)
A3, B4, 11×17, Legal ($8\frac{1}{2}\times 14$), $8\frac{1}{2}\times 13$	400
A4, A5, A6, A7, B5, B6, Letter ($8\frac{1}{2}\times 11$), $5\frac{1}{2}\times 8\frac{1}{2}$	600

↓ Note

- Enter B6, A6, and A7 sizes directly.
 - B6 (128 mm/5.0 inches × 182 mm/7.1 inches)
 - A6 (105 mm/4.1 inches × 148 mm/5.8 inches)

- A7 (74 mm/2.9 inches × 105 mm/4.1 inches)

When Using as a TWAIN Scanner

This section explains the relationship between resolution and scan size when using the machine as a TWAIN scanner.

To specify the scan area or resolution on the machine you are using as a network TWAIN scanner directly, see the TWAIN driver Help.

↓ Note

- Certain original types and resolution settings can reduce scanning quality.

If [Binary(Text)], [Binary(Photo)], [Gray Scale], [8 Colors], or [8 Colors(Photo)] is selected in [Col./Grad.]:

The scan size determines the maximum possible resolution.

Refer to the table below for the maximum resolution available for each scan size.

Scan size and maximum resolution

Scan size	Maximum resolution (dpi)
A3, 11×17	600
B4	693
Legal (8 ¹ / ₂ ×14)	728
8 ¹ / ₂ ×13	785
Letter (8 ¹ / ₂ ×11)	825
A4	848
B5	979
A5, B6, A6, 5 ¹ / ₂ ×8 ¹ / ₂	1200

If [16770K colors] is selected in [Col./Grad.]:

The scan size determines the maximum possible resolution.

Refer to the table below for the maximum resolution available for each scan size.

Scan size and maximum resolution

Scan size	Maximum resolution (dpi)
A3	425

Scan size	Maximum resolution (dpi)
11×17	432
B4	491
Legal (8 ¹ / ₂ ×14)	542
8 ¹ / ₂ ×13	563
A4	601
Letter (8 ¹ / ₂ ×11)	612
B5	695
A5	852
5 ¹ / ₂ ×8 ¹ / ₂	865
B6	984
A6	1200

Software Supplied on CD-ROM

This section explains the applications on the supplied CD-ROM.

Auto-Run Program

This section explains the auto-run program.

When the CD-ROM is inserted into a client computer running Windows 2000/XP/Vista or Windows Server 2003/2003 R2/2008, the installer starts up automatically (auto run) to install various software.

Note

- For installation, log on as an Administrators group member.
- Auto-run program may not automatically work with certain operating system settings. If this happens, start "Setup.exe" on the CD-ROM root directory.
- To disable auto-run, set CD-ROM while pressing the Shift key. Keep the Shift key pressed until the computer finishes reading from the CD-ROM.
- If [Cancel] is clicked during installation, the installation of all the software thereafter will be stopped. If cancelled, reinstall the remaining software after restarting the client computer.

TWAIN Driver

This section tells you the file path to the TWAIN driver and the TWAIN driver's system requirements.

You must install this driver if you want to scan originals or use the machine as a network TWAIN scanner.

File path

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

`\DRIVERS\TWAIN`

System requirements

- Computer hardware
PC/AT-compatible machines that support the operating system properly
- Operating system
Microsoft Windows 2000/XP/Vista
Microsoft Windows Server 2003/2003 R2/2008
- Display resolution
800 × 600 pixels, 256 colors or higher

DeskTopBinder Lite

This section tells you the file path to DeskTopBinder Lite, the DeskTopBinder Lite system requirements, and the applications that are installed with DeskTopBinder Lite.

DeskTopBinder is installed on the client computers to integrate and manage various kinds of files such as scan files, files created with applications, and existing scan files. This software allows you to use various functions for stored scan files such as viewing stored files. Also, with ScanRouter delivery software, you can view the files stored in in-trays of the delivery server or use other functions for stored files. For details about DeskTopBinder Lite, see DeskTopBinder Lite manuals or DeskTopBinder Lite Help.

File path

DeskTopBinder Lite is stored in the following folder on the CD-ROM provided with this machine:

\UTILITY\DESKV2

System requirements

- Computer hardware
 - PC/AT-compatible machines that support the following operating system properly
- Operating system
 - Microsoft Windows 2000 Professional SP1 or later
 - Microsoft Windows 2000 Server SP1 or later
 - Microsoft Windows 2000 Advanced Server SP1 or later
 - Microsoft Windows XP Professional/Home Edition
 - Microsoft Windows Vista Ultimate/Enterprise/Business/Home Premium/Home Basic
 - Microsoft Windows Server 2003 Standard Edition/Enterprise Edition
 - Microsoft Windows Server 2003 R2 Standard Edition/Enterprise Edition
 - Microsoft Windows Server 2008 Standard/Enterprise
- Display resolution
 - 800 × 600 pixels, 64K colors or higher

Software installed with DeskTopBinder Lite

- Auto Document Link
 - Auto Document Link on the client computer monitors in-trays of the delivery server periodically, retrieves files delivered to in-trays, and notifies the user of delivery.
- Function Palette
 - Function Palette allows you to use DeskTopBinder functions such as Scan using TWAIN scanner or Print without starting DeskTopBinder. To use these functions from Function Palette, you must first configure those using DeskTopBinder Extended Features. For details about Function Palette, see DeskTopBinder manuals.
- SmartDeviceMonitor for Client

SmartDeviceMonitor for Client provides functions for continuous device status monitoring on the network via TCP/IP or IPX/SPX.

Values of Various Set Items for Transmission/Storage/Delivery Function

This section explains the values of various transmission/storage/delivery function settings.

Note

- Depending on the type or settings of the file or original, you may not be able to specify the destination or enter the maximum number of characters stated below.

Transmission Function

This section explains the values of transmission function settings.

Sending e-mail

The following table tells you the maximum values of the e-mail sending function settings.

Values of Set Items for Sending by E-mail

Item	Maximum value	Comments
Number of subject line characters	128 alphanumeric characters	-
Number of e-mail message characters	<ul style="list-style-type: none"> Selecting from the list: 400 alphanumeric characters (80 alphanumeric characters × 5 lines) Entering manually: 80 alphanumeric characters 	You cannot enter messages from the list and manually at the same time.
Number of e-mail address characters	128 alphanumeric characters	E-mail addresses found via LDAP server search cannot be selected if they contain more than 128 characters.
Number of addresses you can specify at the same time	500 addresses	You can specify 100 destinations by direct entry, including LDAP search. Select the remaining 400 destinations from registered addresses.

Item	Maximum value	Comments
Sendable file size	725.3 MB per file	-
Sendable number of pages	2,000 pages per file	-

Folder transmission

The following table tells you the maximum values of the Scan to Folder function settings.

Values of Set Items for Scan to Folder

Item	Maximum value	Comments
Number of path name characters on SMB	256 alphanumeric characters	-
Number of user name characters on SMB	128 alphanumeric characters	-
Number of password characters on SMB	128 alphanumeric characters	-
Number of server name characters on FTP	64 alphanumeric characters	-
Number of path name characters on FTP	256 alphanumeric characters	-
Number of user name characters on FTP	64 alphanumeric characters	-
Number of password characters on FTP	64 alphanumeric characters	-
Number of path name characters on NCP	256 alphanumeric characters	-
Number of user name characters on NCP	128 alphanumeric characters	-
Number of password characters on NCP	64 alphanumeric characters	-
Number of addresses you can specify at the same time	50 addresses	You can specify a maximum of 50 directly entered destinations.

Item	Maximum value	Comments
Sendable file size	2,000 MB per file	-

Simultaneous transmission

The following table tells you the maximum values of settings for using the E-mail and Scan to Folder functions simultaneously.

Values of Set Items for Simultaneous transmission

Item	Maximum value	Comments
Number of destinations you can select for E-mail and Scan to Folder	550 addresses	-
Number of destinations you can select for sending by e-mail	500 addresses	You can specify a maximum of 100 directly entered destinations, including LDAP search-retrieved destinations.
Number of destinations you can set for sending by Scan to Folder	50 addresses	-

WSD scanner transmission

The following table tells you the maximum values available for the WSD scanner function settings.

Values of Set Items for WSD Scanner Transmission

Item	Maximum value	Comments
Number of destinations you can specify at the same time	1 destination	-
Sendable file size	2,000 MB per file	-
Sendable number of pages	2,000 pages per file	-

Storage Function

The following table tells you the maximum values of the storage function settings.

Values of Set Items for File Storage

Item	Maximum value	Comments
Number of file name characters	64 alphanumeric characters	On the control panel, the first 16 characters are displayed. When viewing the stored files from a client computer using DeskTopBinder, all the entered characters can be viewed.
Number of user name characters	20 alphanumeric characters	On the control panel, the first 16 characters are displayed. When viewing the stored files from a client computer using DeskTopBinder, all the entered characters can be viewed.
Number of password characters	4-8 digit number	-
Number of stored files you can select at the same time	30 files	-
Storable number of files	3,000 files	This is the total number of files stored under the scanner, copier, document server, and printer functions.
Storable number of pages	10,000 pages	This is the total number of files stored under the scanner, copier, document server, and printer functions.
Storable number of pages per file	2,000 pages	-
Storable size	2,000 MB per file	-

Network Delivery Function

The following table tells you the values of setting items for the network delivery scanner function.

Values of Set Items for Network Delivery

Item	Maximum value	Comments
Number of subject line characters	128 alphanumeric characters	This is the total number of characters selected from the list and the number of characters entered directly from text.
Number of e-mail address characters	128 alphanumeric characters	-
Number of addresses you can specify at the same time	500 addresses	You can specify 65 destinations by direct entry, including LDAP search. Select the remaining 435 destinations from registered addresses. The maximum number of destinations you can specify differs depending on which ScanRouter delivery software you are using. For details, see the manuals supplied with the ScanRouter delivery software.
Sendable file size	2,000 MB per file	-

About WIA Scanning

WIA allows computers that are running Windows Vista to perform scanning through the network.

★ Important

- To use this machine as a WIA scanner, you must first download the WIA driver from the supplier's Web site and install it on your computer.

Network TWAIN also allows you to perform scanning through a network; however, TWAIN and WIA do not provide the same scan functions.

The following table tells you the functions available or not available with TWAIN and WIA. For details about TWAIN, see "Scanning Originals with the Network TWAIN Scanner".

📖 Reference

- p.133 "Scanning Originals with the Network TWAIN Scanner"

Functions of the TWAIN and WIA scanners

Functions	TWAIN	WIA
1. Scan		
Scan from the exposure glass	Yes	Yes
Continuous scanning from the ADF	Yes	Yes
Specify the number of originals to be scanned from the ADF	Yes *1	Yes *1
Preview	Yes	Yes *2
Auto detect		
<ul style="list-style-type: none"> • When scanning from the exposure glass 	Yes	No
<ul style="list-style-type: none"> • When scanning from the ADF (Mixed-size) 	Yes	Yes
<ul style="list-style-type: none"> • When scanning from the ADF (Uni-size) 	Yes	No
Scan using an application that do not have user interface	Yes	Yes
2. Setting		
Driver selection	Yes	Yes
Initial Settings		
<ul style="list-style-type: none"> • Unit of Measure: (mm, inch, pixel) 	Yes	No

Functions	TWAIN	WIA
• Compression	Yes	No
Deskew	Yes	No
Start from Scanner	Yes	No
Orient.auto detect	Yes	No
Save/Delete Mode	Yes	No
Specify original size		
• When scanning from the exposure glass	Yes	Yes *1
• When scanning from the ADF	Yes	Yes
Orig.Orientn.:	Yes	Yes *1
Orientation:	Yes	Yes *1
Scan Settings:		
• 1 Sided	Yes	Yes
• 2 Sided	Yes	Yes
• 2 Sided (Top to Top, Top to Bottom)	Yes	No
Resolution	Yes	Yes
Brightness:	Yes	Yes
Contrast:	Yes	Yes
Threshold:	Yes	Yes *1
Col./Grad.:		
• Binary	Yes	Yes
• Gray Scale	Yes	Yes
• 8 Colors	Yes	No
• 16770K colors (Full color)	Yes	Yes
Gam-Curve:	Yes	No
Eras.Bgrnd:	Yes	No

Functions	TWAIN	WIA
Advanced		
• Filter (Filter, Dropout Col.)	Yes	No
• Color Matching (ICM:, Inversion)	Yes	No
Save/Delete Scanning Area	Yes	No
Specify original size (specify scan area manually)	Yes	No
Comb./Series	Yes	No
Endorser	Yes	No
3. Properties		
General		
• Diagnosis (Scan test)	No	Yes
Authenticate		
• User Code:	Yes	Yes
• General User Authentication	Yes	Yes
Network Connection		
• Settings for using a specific scanner	Yes	Yes
• SNMP V3 Auth.information	Yes	Yes
Driver version display	Yes	Yes

*1 You might not be able to specify settings for this function from some applications.

*2 The preview does not reflect changes made for settings while it is displayed. To display the preview image with the changed settings applied, first close the preview, and then open it again.

Specifications

The following table tells you the specifications of the scanner.

Specifications

Component	Specifications
Type	Full-color scanner
Scan method	Flatbed scanning
Image sensor type	CCD Image Sensor
Scan type	Sheet, book, three-dimensional object
Original sizes that can be scanned	<ul style="list-style-type: none"> Length 140~297 mm (5¹/₂~11 inches) Width 140~432 mm (5¹/₂~17 inches)
Scan sizes automatically detectable from the exposure glass	<ul style="list-style-type: none"> Metric version A3, B4 JIS, A4, A4, B5 JIS, B5 JIS, A5, 8¹/₂ × 13 Inch version 11 × 17, 8¹/₂ × 14, 8¹/₂ × 11, 8¹/₂ × 11, 5¹/₂ × 8¹/₂
Scan sizes automatically detectable from the ADF	<ul style="list-style-type: none"> Metric version A3, B4 JIS, A4, A4, B5 JIS, B5 JIS, A5, A5, B6, B6, 11 × 17, 8¹/₂ × 11, 8¹/₂ × 11, 8¹/₂ × 13 Inch version A3, A4, A4, 11 × 17, 8¹/₂ × 14, 8¹/₂ × 11, 8¹/₂ × 11, 5¹/₂ × 8¹/₂, 5¹/₂ × 8¹/₂, 10 × 14, 7¹/₄ × 10¹/₂

Component	Specifications
Scan speed	<p>When using the E-mail/Scan to Folder/WSD/network delivery scanner function (Original size: A4, Resolution: 200 dpi, 1-side scanning):</p> <p>Black and white: 80 pages/min</p> <p>(Scan Type: B & W: Text / Line Art, Compression (Black & White): MH, ITU-T No1 Chart)</p> <p>Full Color: 55 pages/min</p> <p>(Scan Type: Full Colour: Text / Photo, Compression (Gray Scale / Full Colour): Default, Original Chart)</p> <p>Scanning speed differs depending on the following; operating environment of the machine and computer, scan settings, and the content of originals (denser images require more time).</p>
Tone	<p>Black and white: 2 tones</p> <p>Full color / Gray scale: 256 tones</p>
Basic scanning resolution	600 dpi
Image compression type for black and white (two-value)	TIFF (MH, MR, MMR)
Image compression type for gray scale/full color	JPEG
Interface	<ul style="list-style-type: none"> • Basic 10BASE-T, 100BASE-TX • Optional 1000BASE-T, IEEE 802.11a/g (Wireless LAN)
Network protocol	TCP/IP
Selectable scanning resolutions when using the E-mail function (main scanning × sub scanning)	100 dpi, 200 dpi, 300 dpi, 400 dpi, 600 dpi
Protocol for sending e-mail	SMTP, POP3
Sendable file formats when using the E-mail function	TIFF, JPEG, PDF, High Compression PDF

Component	Specifications
Selectable scanning resolutions when using the Scan to Folder function (main scanning × sub scanning)	100 dpi, 200 dpi, 300 dpi, 400 dpi, 600 dpi
Protocol for Scan to Folder	SMB, FTP, NCP
Sendable file formats when using the Scan to Folder function	TIFF, JPEG, PDF, High Compression PDF
Protocol for sending using WSD	Web Services on Devices for scanning
Selectable scanning resolution when using TWAIN scanner (main scanning × sub scanning)	100 dpi to 1200 dpi
Protocol for TWAIN scanner	TCP/IP
Operating system for TWAIN scanner	Windows 2000/XP/Vista, Windows Server 2003/2003 R2/2008
Selectable scanning resolutions when using the network delivery scanner function (main scanning × sub scanning)	100 dpi, 200 dpi, 300 dpi, 400 dpi, 600 dpi
Selectable scanning resolutions when using WIA scanner (main scanning × sub scanning)	100 dpi to 1200 dpi
Protocol for WIA scanner	TCP/IP
Operating system for WIA scanner	Windows Vista (SP1 or later), Windows Server 2008 (WIA scanner can function under both 32- and 64-bit operating systems.)

Note

- Specifications are subject to change without notice.

Trademarks

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

Pentium® is a registered trademark of Intel Corporation.

NetWare® is a registered trademark of Novell, Inc.

Microsoft®, Windows®, Windows NT®, Windows Server®, and Windows Vista® are either registered trademarks or trademarks of Microsoft Corporation in the U.S. and/or other countries.

Mac OS is a trademark of Apple Inc., registered in the U.S. and other countries.

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 the Windows operating systems are as follows:

- The product name of Windows 98 is Microsoft® Windows® 98.
- The product name of Windows Me is Microsoft® Windows® Millennium Edition (Windows Me).
- 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 Home Edition
 - Microsoft® Windows® XP Professional
- The product names of Windows Vista are as follows:
 - Microsoft® Windows Vista® Ultimate
 - Microsoft® Windows Vista® Enterprise
 - Microsoft® Windows Vista® Business
 - Microsoft® Windows Vista® Home Premium
 - Microsoft® Windows Vista® Home Basic
- 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

Microsoft® Windows Server® 2008 Datacenter

- The product names of Windows NT 4.0 are as follows:

Microsoft® Windows NT® Workstation 4.0

Microsoft® Windows NT® Server 4.0

INDEX

A

A.C.S. Sensitivity Level.....	179
Access Privileges.....	45, 74, 92, 93, 132
Accessing User Tools.....	175
Address book	
registering destination folders.....	55
registering e-mail addresses.....	22
ADF.....	141, 153
Adjusting image density.....	151
Advanced Search.....	31, 34, 40, 63
Auto Colour Select.....	144
Auto Density.....	151
Auto Detect.....	145
Auto-run program.....	188

B

B & W Text / Line Art.....	144
B & W Text / Photo.....	144
Background Density of ADS (Full Colour).....	180
Basic operation	
delivering scan files.....	119
network TWAIN scanner.....	138
saving on a memory device.....	111
sending scan files by e-mail.....	25
sending scan files by Scan to Folder.....	58
storing scan files.....	91
WSD scanner.....	80
Batch.....	155, 158
Black & White Photo.....	144
Black & White Text.....	144

C

CD-ROM.....	188
Certificate.....	47
Change Access Priv.....	106
Change File Name.....	106
Change Name.....	171
Change Password.....	107
Change User Name.....	105
Check Modes.....	14
Compression (Black & White).....	181
Compression (Gray Scale / Full Colour).....	181
Confirmation displays.....	14
Check Modes.....	14

Preview.....	15
Scanned Files Status.....	17
Connecting to the network.....	20, 21, 53, 76, 114, 134
Custom Size.....	145
scanning part of an original.....	148
scanning the entire area.....	146

D

Delete.....	171
Delete File.....	104
Delete Scanner Journal.....	178
Delivering scan files.....	113, 119
Delivery.....	113
Delivery Dest.....	122
Delivery destination.....	123
Delivery server.....	113
DeskTopBinder Lite.....	100, 101, 116, 117, 136, 189

Destination (delivery)

searching the delivery server's destination list.....	124
selecting by entering the registration numbers.....	124
selecting from the delivery server's address book.....	123
selecting from the list.....	123

Destination (e-mail)

entering manually.....	32
registering a directly-entered destination in the address book.....	36
searching an LDAP server.....	33
searching the machine's address book.....	31
selecting by entering the registration numbers.....	30
selecting from the list.....	29
selecting from the machine's address book.....	29

Destination (folder)

entering the path of the NetWare server directly.....	70
entering the path to a shared network folder manually.....	65
entering the path to an FTP server manually.....	68
registering the path to the selected destination in the address book.....	73
searching the machine's address book.....	63
selecting by entering the registration numbers.....	62
selecting from the list.....	61
selecting from the machine's address book.....	61
specifying the path by browsing the NetWare server.....	72
specifying the path by browsing the shared network folder.....	66

Destination (WSD scanner)	
searching the destination.....	84
selecting the destination.....	83
Destination list.....	24, 29, 57, 61, 79, 118, 123
Destination List Display Priority 1.....	177
Destination List Display Priority 2.....	177
Display	
confirmation displays.....	14
Simplified Display.....	13
Display panel.....	13
Divide.....	156
Divide & Send E-mail.....	181
Dropout Colour.....	144

E

E-mail destination.....	29
E-mail message.....	43
entering manually.....	44
selecting from the list.....	43
E-mail screen.....	23, 28
E-mail sender.....	38
Edit.....	150
Enabling WSD.....	77
Encryption	
e-mail.....	46
PDF.....	165
Erase Border.....	150
Expand Group Dest.....	15
Exposure glass.....	140, 152

F

File Name.....	162
sending files.....	160
stored files.....	93
File type.....	160
FTP.....	52, 68
FTP server.....	52
Full Colour Glossy Photo.....	144
Full Colour Text / Photo.....	144
Functions.....	11

G

General Settings.....	177
Gray Scale.....	144

H

High Compression PDF.....	160, 161
High Compression PDF Level.....	181
How to read this manual.....	9

I

Initial Settings.....	184
Insert Additional E-mail Info.....	182
Install	
DeskTopBinder Lite.....	117
TWAIN driver.....	136

K

Key Colour.....	14
-----------------	----

L

Laws and regulations.....	10
LDAP server.....	19, 33
Legal prohibition.....	10
Limitations of file types.....	161

M

Manage / Delete File.....	104
Manual Entry.....	24, 57, 118
Manuals for this machine.....	6
Max. E-mail Size.....	181
Memory device.....	109, 111
Menu Protect.....	184
Mixed Original Sizes.....	145, 146
Mixed size originals.....	142, 146
Multi-page.....	160
Multiple pages scanned as one file.....	158

N

NCP.....	52, 69
NetWare server.....	53, 69
Network delivery function.....	194
Network delivery scanner screen.....	117, 122
Network TWAIN scanner.....	133
No. of Digits for Single Page Files.....	182
Notes.....	9
Notes about file types.....	161
Notice.....	8

O

One sided original.....	154
Original Feed Type.....	152
Original orientation.....	152
TWAIN scanner.....	140
Original Settings.....	154
Outline	
delivering scan files.....	113
network TWAIN scanner.....	133
saving on a memory device.....	109
sending scan files by e-mail.....	19
sending scan files by Scan to Folder.....	51
storing scan files.....	89
WSD scanner.....	75

P

Password.....	94
PDF.....	160
changing security permissions.....	166
encryption.....	165
security.....	164
Permissions.....	166
Preparation	
network TWAIN scanner.....	134
sending scan files by e-mail.....	20
sending scan files by Scan to Folder.....	53
WSD scanner.....	76
Preview	
viewing a file before sending.....	15
Prg. Dest.....	36, 73
Print & Delete Scanner Journal.....	178
Print List.....	18
Print Scanner Journal.....	178
Program as Defaults.....	173
Programs.....	169
changing.....	170, 171
defaults.....	173
deleting.....	171
recalling.....	170
registering.....	169

R

Recall.....	170
Recept. Notice.....	26, 120
Reg. No.....	24, 57, 118
Registering of WSD scanner.....	78

Registration number.....	30, 39, 62, 124, 127
Resolution.....	145
Resolution and scan size.....	185
e-mail.....	185
network delivery.....	185
Scan to Folder.....	185
storing.....	185
TWAIN scanner.....	186
Restore Factory Defaults.....	173
Result of sending.....	17

S

S/MIME.....	46
SADF.....	155, 158
Saving on a memory device.....	109, 111
Scan profile	
changing.....	86
creating.....	87
Scan settings.....	140, 143, 179
Scan Size.....	145
Scan to e-mail.....	19
Scan to Folder.....	51
Scan to Folder destination.....	61
Scan to Folder screen.....	56, 60
Scan Type.....	144
Scanner Features.....	22, 55, 116
accessing.....	175
changing.....	175
quitting.....	176
Scanner functions.....	11
ScanRouter delivery software.....	113, 116
Screen layout	
delivering scan files.....	117
list of stored files.....	96
sending scan files by e-mail.....	23
sending scan files by Scan to Folder.....	56
WSD scanner.....	79
Search Dest.....	31, 33, 63, 84, 124
Search Destination.....	177
Security	
e-mail.....	46
encryption (e-mail).....	46
PDF.....	164
signature.....	47
Security Settings.....	164
Select Stored File.....	96

Send Settings.....	181	Stored File E-mail Method.....	182
Sender (delivery).....	127	Storing scan files.....	89
searching the delivery server's destination list.....	128	specifying a file name.....	93
selecting by entering a registration number.....	127	specifying a password.....	94
selecting from the list.....	127	specifying a user name.....	93
Sender (e-mail).....	38	specifying file information.....	93
searching the machine's address book.....	39	Subject.....	42, 131
selecting by entering a registration number.....	39	Switch Title.....	177
selecting from the list.....	38	Switching screen	
Sender Name.....	38, 39, 127, 128	E-mail.....	28
Sending a stored file.....	102	network delivery scanner.....	122
Sending scan files by e-mail.....	19, 25	Scan to Folder.....	60
Sending scan files by Scan to Folder.....	58	WSD scanner.....	82
Sending scan files to folders.....	51	Symbols.....	9
Sending scan files with WSD.....	75, 80	System Settings.....	20, 53, 76, 114, 134
Sending the URL by e-mail.....	48	T	
Serial number.....	163	Template size.....	145
Signature.....	47	Text.....	43, 44
Simplified Display.....	13	TIFF.....	160
Single Page.....	160	TIFF / JPEG.....	160
SmartDeviceMonitor for Admin.....	23	Trademarks.....	202
SMB.....	51, 64	Transmission function.....	191
SMTP server.....	19	TWAIN driver.....	136, 138, 188
Specifications.....	199	TWAIN scanner.....	133, 138, 140, 142
Storage function.....	193	TWAIN Standby Time.....	177
Store File.....	91	Two sided original.....	155
Store to HDD.....	91	U	
Store to HDD + Send.....	45, 74, 132	Update.....	79
Stored file		Update Delivery Server Destination List.....	177
changing a file name.....	106	URL.....	48
changing a password.....	107	User Name.....	93
changing a user name.....	105	User Tools	
changing information.....	105	accessing.....	175
checking.....	99	changing.....	175
checking from a client computer.....	100	quitting.....	176
checking from the list.....	99	V	
deleting.....	104	Values of set items.....	191
displaying the list.....	96	e-mail.....	191
displaying with DeskTopBinder Lite.....	101	network delivery.....	194
displaying with Web Image Monitor.....	101	Scan to Folder.....	192
managing.....	104	simultaneous transmission.....	193
Preview screen.....	100	storage.....	193
searching by file name.....	98	WSD scanner.....	193
searching by user name.....	97		
searching the list.....	97		
sending.....	102		

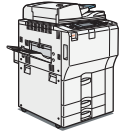
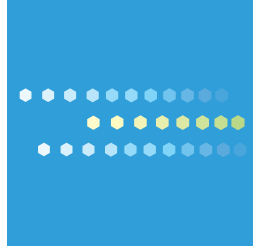
W

Wait Time for Next Orig. Exposure Glass.....	179
Wait Time for Next Original(s) SADF.....	179
Web Image Monitor.....	23, 100, 101
WIA scanning.....	196
WSD scanner.....	75
WSD scanner destination.....	83
WSD scanner screen.....	79, 82

MEMO

MEMO

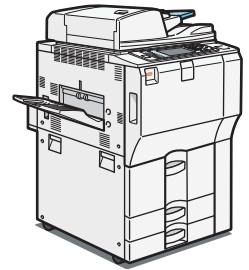
MEMO





9060/9070/9080/9090
MP 6001/MP 7001/MP 8001/MP 9001
LD360/LD370/LD380/LD390
Aficio™ MP 6001/7001/8001/9001

Operating Instructions Network and System Settings Guide



-
- 1** System Settings
 - 2** Connecting the Machine
 - 3** Using a Printer Server
 - 4** Monitoring and Configuring the Printer
 - 5** Registering Addresses and Users for Facsimile/Scanner Functions
 - 6** Special Operations under Windows
 - 7** Appendix

TABLE OF CONTENTS

Manuals for This Machine.....	10
Notice.....	12
Important.....	12
How to Read This Manual.....	13
Symbols.....	13
Notes.....	13
About IP Address.....	14
Laws and Regulations.....	15
Legal Prohibition.....	15
Display Panel.....	16
Accessing User Tools.....	17
Changing Default Settings.....	17
Quitting User Tools.....	18
1. System Settings	
General Features.....	19
Output Tray Settings.....	25
Tray Paper Settings.....	26
Timer Settings.....	31
Interface Settings.....	34
Network.....	34
Parallel Interface.....	37
Wireless LAN.....	38
Print List.....	40
File Transfer.....	42
Administrator Tools.....	49
Programming the LDAP server.....	59
Programming the LDAP server.....	59
Changing the LDAP server.....	63
Deleting the LDAP server.....	63
Programming the Realm.....	65
Programming the Realm.....	65
Changing the Realm.....	66
Deleting the Realm.....	67

System Settings on Main and Sub-machines.....	68
General Features.....	68
Tray Paper Settings.....	71
Timer Settings.....	73
Administrator Tools.....	74

2. Connecting the Machine

Connecting to the Interface.....	79
Connecting to the Ethernet Interface.....	80
Connecting to the Gigabit Ethernet Interface.....	81
Connecting to the USB (Type B) Interface.....	83
Connecting to the IEEE 1284 Interface.....	84
Connecting to the Wireless LAN Interface.....	85
Network Settings Required to Use the Printer/LAN-Fax.....	88
Ethernet.....	88
Wireless LAN.....	89
Network Settings Required to Use Internet Fax.....	91
Ethernet.....	91
Wireless LAN.....	93
Network Settings Required to Use E-mail Function.....	95
Ethernet.....	95
Wireless LAN.....	96
Network Settings Required to Use Scan to Folder Function.....	99
Ethernet.....	99
Wireless LAN.....	100
Network Settings Required to Use the Network Delivery Scanner.....	102
Ethernet.....	102
Wireless LAN.....	103
Network Settings Required to Use WSD Scanner.....	105
Ethernet.....	105
Wireless LAN.....	106
Network Settings Required to Use Network TWAIN Scanner.....	108
Ethernet.....	108
Wireless LAN.....	109

Network Settings Required to Use Document Server.....	111
Ethernet.....	111
Wireless LAN.....	112
Using Utilities to Make Network Settings.....	114
Interface Settings.....	114
File Transfer.....	120
Connecting the Machine to a Telephone Line and Telephone.....	123
Connecting the Telephone Line.....	123
Selecting the Line Type.....	123

3. Using a Printer Server

Preparing Printer Server.....	125
Using NetWare.....	126
Setting Up as a Print Server (NetWare 3.x).....	127
Setting Up as a Print Server (NetWare 4.x, 5/5.1, 6/6.5).....	128
Using Pure IP in the NetWare 5/5.1 or 6/6.5 Environment.....	129
Setting Up as a Remote Printer (NetWare 3.x).....	131
Setting Up as a Remote Printer (NetWare 4.x, 5/5.1, 6/6.5).....	133

4. Monitoring and Configuring the Printer

Using Web Image Monitor.....	137
Displaying Top Page.....	138
When User Authentication is Set.....	140
About Menu and Mode.....	140
Access in the Administrator Mode.....	142
List of Setting Items.....	142
Displaying Web Image Monitor Help.....	149
Using SmartDeviceMonitor for Admin.....	151
Installing SmartDeviceMonitor for Admin.....	152
Changing the Network Interface Board Configuration.....	153
Locking the Menus on the Machine's Control Panel.....	154
Changing the Paper Type.....	155
Managing User Information.....	155
Configuring the Energy Saver Mode.....	161
Setting a Password.....	161

Checking the Machine Status.....	162
Changing Names and Comments.....	163
Load Fax Journal.....	164
Viewing and Deleting Spool Print Jobs.....	165
Managing Address Information.....	165
Using SmartDeviceMonitor for Client.....	167
Monitoring Printers.....	167
Checking the Machine Status.....	168
When Using IPP with SmartDeviceMonitor for Client.....	168
Printer Status Notification by E-Mail.....	170
Setting the Account for E-mail Notification.....	172
Mail Authentication.....	172
Auto E-mail Notification.....	173
On-demand E-mail Notification.....	174
Format of On-demand E-mail Messages.....	175
Remote Maintenance by telnet.....	176
Using telnet.....	176
access.....	177
appletalk.....	178
authfree.....	178
autonet.....	179
bonjour.....	180
btconfig.....	181
devicename.....	181
dhcp.....	182
dhcp6.....	183
diprint.....	183
dns.....	184
domainname.....	186
etherauth.....	187
etherconfig.....	187
help.....	187
hostname.....	187

ifconfig.....	188
info.....	189
ipp.....	190
ipsec.....	190
ipv6.....	191
logout.....	191
lpr.....	191
netware.....	192
passwd.....	193
pathmtu.....	194
prnlog.....	194
route.....	194
rhpp.....	196
set.....	196
show.....	199
slp.....	199
smb.....	200
snmp.....	200
sntp.....	204
spoolsw.....	205
ssdp.....	205
ssh.....	206
status.....	207
syslog.....	207
upnp.....	207
web.....	207
wiconfig.....	208
wins.....	213
wsmfp.....	214
8021x.....	215
SNMP.....	217
Getting Printer Information over the Network.....	218
Current Printer Status.....	218

Printer configuration.....	225
Understanding the Displayed Information.....	227
Print Job Information.....	227
Print Log Information.....	227
Configuring the Network Interface Board.....	228
Message List.....	239
System Log Information.....	239

5. Registering Addresses and Users for Facsimile/Scanner Functions

Address Book.....	249
Managing names in the Address Book.....	252
Sending fax by Quick Dial.....	252
Sending e-mail by Quick Dial.....	253
Sending received fax documents or scanned files to a shared folder directly.....	253
Preventing unauthorized user access to shared folders from the machine.....	253
Managing users and machine usage.....	253
Registering Names.....	255
Registering Names.....	255
Changing a Registered Name.....	256
Deleting a Registered Name.....	257
Authentication Information.....	259
Registering a User Code.....	259
Changing a User Code.....	261
Deleting a User Code.....	262
Displaying the Counter for Each User.....	264
Printing the Counter for Each User.....	264
Printing the Counter for All Users.....	265
Clearing the Number of Prints.....	266
Fax Destination.....	268
Registering a Fax Destination.....	269
Changing a Fax Destination.....	271
Deleting a Fax Destination.....	273
Registering an IP-Fax Destination.....	275
Changing a Registered IP-Fax Destination.....	276

Deleting a Registered IP-Fax Destination.....	279
E-mail Destination.....	281
Registering an E-mail Destination.....	281
Changing an E-mail Destination.....	283
Deleting an E-mail Destination.....	284
Registering Folders.....	286
Registering an SMB Folder.....	286
Changing an SMB Folder.....	289
Deleting an SMB registered folder.....	291
Registering an FTP Folder.....	292
Changing an FTP folder.....	294
Deleting an FTP folder.....	296
Registering an NCP folder.....	297
Changing an NCP registered folder.....	300
Deleting an NCP folder.....	302
Registering Names to a Group.....	303
Registering a Group.....	303
Registering Names to a Group.....	304
Adding a Group to Another Group.....	306
Displaying Names Registered in a Group.....	307
Removing a Name from a Group.....	308
Deleting a Group Within Another Group.....	309
Changing a Group Name.....	310
Deleting a Group.....	312
Registering a Protection Code.....	313
Registering a Protection Code to a Single User.....	313
Registering a Protection Code to a Group User.....	314
Registering SMTP and LDAP Authentication.....	316
SMTP Authentication.....	316
LDAP Authentication.....	317

6. Special Operations under Windows

Printing Files Directly from Windows.....	321
Setup.....	321

Using a Host Name Instead of an IPv4 Address.....	321
Printing Commands.....	322
Printing with Bluetooth Connection.....	326
Supported Profiles.....	326
Adding a Bluetooth Printer.....	326

7. Appendix

When Using Windows Terminal Service/MetaFrame.....	329
Operating Environment.....	329
Supported Printer Drivers.....	329
Limitations.....	329
Using DHCP.....	331
Using AutoNet.....	331
Configuring the WINS Server.....	332
Using Web Image Monitor.....	332
Using telnet.....	332
Using the Dynamic DNS Function.....	334
Updating.....	334
DNS servers targeted for operation.....	335
DHCP servers targeted for operation.....	335
Setting the dynamic DNS function.....	335
Precautions.....	337
Connecting a Dial-Up Router to a Network.....	337
NetWare Printing.....	338
When the IEEE 802.11 Interface Unit is Installed.....	340
Configuring IEEE 802.1X.....	341
Installing a Site Certificate.....	341
Installing Device Certificate.....	342
Setting Items of IEEE 802.1X for Ethernet.....	343
Setting Items of IEEE 802.1X for Wireless LAN.....	344
Specifications.....	346
Copyrights.....	349
expat.....	349
NetBSD.....	349

Sablotron.....	351
JPEG LIBRARY.....	352
SASL.....	352
MD4.....	353
MD5.....	353
Samba(Ver 3.0.4).....	353
RSA BSAFE®.....	354
Open SSL.....	354
Open SSH.....	356
Open LDAP.....	360
Heimdal.....	361
IPS™ print language emulations.....	361
Trademarks.....	362
INDEX	365

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.
- The printed and electronic versions of a manual have the same contents.
- 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.

About This Machine

Before using the machine, be sure to read the section of this manual entitled Safety Information.

This manual introduces the machine's various functions. It also explains the control panel, preparation procedures for using the machine, how to enter text, how to install the CD-ROMs provided, and how to replace paper, toner, staples, and other consumables.

Troubleshooting

Provides a guide for resolving common usage-related problems.

Copy and Document Server Reference

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

Facsimile Reference

Explains Facsimile functions and operations.

Printer Reference

Explains Printer functions and operations.

Scanner Reference

Explains Scanner functions and operations.

Network and System Settings Guide

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

Security Reference

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 "Setting Up the Machine", Security Reference.

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

PostScript 3 Supplement

Explains how to set up and use PostScript 3.

Other manuals

- UNIX Supplement
- Quick Reference Copy Guide
- Quick Reference Printer Guide
- Quick Reference Fax Guide
- Quick Reference Scanner Guide
- Manuals for DeskTopBinder Lite
 - DeskTopBinder Lite Setup Guide
 - DeskTopBinder Introduction Guide
 - Auto Document Link Guide

↓ Note

- Manuals provided are specific to machine types.
- 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.
- The following software products are referred to using general names:

Product Name	General name
DeskTopBinder Lite and DeskTopBinder Professional* 1	DeskTopBinder
ScanRouter EX Professional* 1 and ScanRouter EX Enterprise* 1	the ScanRouter delivery software

* 1 Optional

Notice

Important

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.

For good copy quality, the supplier recommends that you use genuine toner from the supplier.

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

How to Read This Manual

Symbols

This manual uses the following symbols:

CAUTION

Indicates important safety notes.

Ignoring these notes could result in moderate or minor injury, or damage to the machine or to property. Be sure to read these notes. They can be found in the "Safety Information" section of About This Machine.

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 that appear on the machine's display panel.

[]

Indicates the names of keys on the machine's control panel.

Notes

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

Two kinds of size notation are employed in this manual. With this machine refer to the inch version.

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

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.

This machine comes in four models which vary in copy/print speed.

About IP Address

In this manual, "IP address" covers both IPv4 and IPv6 environments. Read the instructions that are relevant to the environment you are using.

Laws and Regulations

Legal Prohibition

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.

Display Panel

The display panel shows machine status, error messages, and function menus.

The function items displayed serve as selector keys. You can select or specify an item by lightly pressing it.

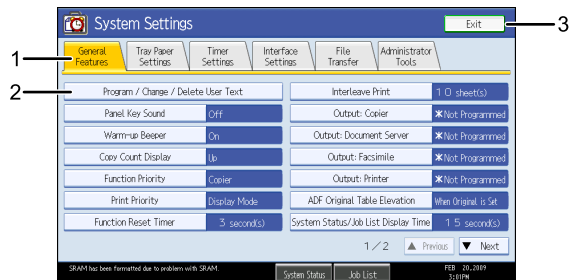
When you select or specify an item on the display panel, it is highlighted like **Program / Change**. Keys appearing as **OK** cannot be used.

★ Important

- A force or impact of more than 30 N (about 3 kgf) will damage the display panel.

To display the following screen, press the [User Tools/Counter] key to display the User Tools menu, and then press [System Settings].

Using the System Settings menu screen as an example, this section explains how to use the machine's display panel.



1. The menu tabs for various settings appear. To display the setting you want to specify or change, press the appropriate menu tab.
2. A list of settings appears. To specify or change a setting, press the appropriate key in the list.
3. Press this to quit the User Tools menu.

Accessing User Tools

This section describes how to access User Tools menu.

User Tools allow you to change or set defaults.

↓ Note

- Operations for system settings differ from normal operations. Always quit User Tools when you have finished.
- Any changes you make with User Tools remain in effect even if the main power switch or operation switch is turned off, or the [Energy Saver] or [Clear Modes] key is pressed.

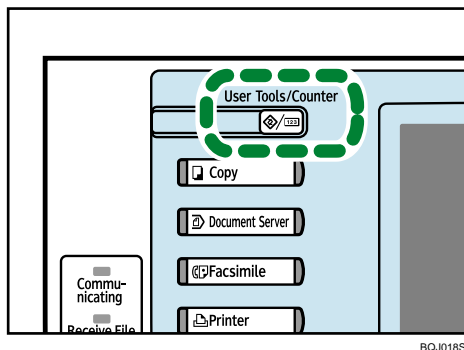
Changing Default Settings

This section describes how to change the settings of User Tools.

★ Important

- If **Administrator Authentication Management** is specified, contact your administrator.

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



2. Press [System Settings].

3. Select the user tool you want to change.

4. Change settings by following instructions on the display, and then press [OK].

↓ Note

- To cancel changes made to settings and return to the initial display, press the [User Tools/Counter] key.
- For details about specifying System Settings, see "System Settings".
- For details about specifying other settings such as changing the language, checking inquiry and counter, see "Remarks", About This Machine.

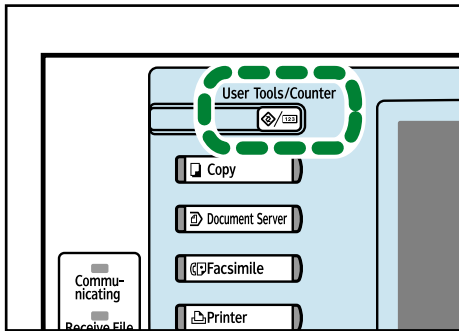
Reference

- p.19 "System Settings"

Quitting User Tools

This section describes how to quit the settings of User Tools.

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



BQJ018S

Note

- You can also quit User Tools by pressing [Exit].

1. System Settings

This chapter describes user tools in the System Settings menu. For details on how to access System Settings, see "Accessing User Tools".

General Features

This section describes the user tools in the General Features menu under System Settings.

Program / Change / Delete User Text

You can register text phrases you often use when specifying settings, such as ".com" and "Regards".

You can register up to 40 entries.

- Program / Change
 1. Press the [User Tools / Counter] key.
 2. Press [System Settings].
 3. Check that [General Features] is selected.
 4. Press [Program / Change / Delete User Text].
 5. Check that [Program / Change] is selected.
 6. Select the user text you want to change.
 - To program new user text, press [Not Programmed].
 7. Enter the user text, and then press [OK].
 - Enter the user text using up to 80 characters.
 8. Press [Exit].
 9. Press the [User Tools / Counter] key.
- Delete
 1. Press the [User Tools / Counter] key.
 2. Press [System Settings].
 3. Check that [General Features] is selected.
 4. Press [Program / Change / Delete User Text].
 5. Press [Delete].
 6. Select the user text you want to delete.
 7. Press [Yes].
 8. Press [Exit].
 9. Press the [User Tools / Counter] key.

Panel Key Sound

The beeper (key tone) sounds when a key is pressed.

The default setting is [Medium].

Warm-up Beeper (copier/Document Server)

You can have the beeper sound when the machine becomes ready to copy after leaving Energy Saver mode, or when the power is turned on.

The default setting is [On].

If the Panel Tone setting is [Off], the beeper does not sound, whatever the Warm Up Notice setting.

Copy Count Display (copier/Document Server)

The copy counter can be set to show the number of copies made (count up) or the number of copies yet to be made (count down).

The default setting is [Up].

Function Priority

Specify the mode to be displayed immediately after the operation switch is turned on, or when System Reset mode is turned on.

The default setting is [Copier].

Print Priority

Print Priority is given to the mode selected.

The default setting is [Display Mode].

Function Reset Timer

You can set the length of time the machine waits before changing modes when using the multi-access function.

This is useful if you are making many copies and have to change settings for each copy. If you set a longer reset period, you can prevent interruption from other functions.

The default setting is [Set Time].

When you select [Set Time], enter the time (3-30 seconds, in 1 second increments) using the number keys.

The default setting for Function Reset Time is "3 second(s)".

The Function Reset Timer setting is ignored if [Immediate] is set for Print Priority.

Interleave Print

Set the number of sheets to be output at the time of operation by interruption.

The default setting is 10 sheet(s).

Output: Copier (copier)

Specify a tray to which documents are delivered.

The default setting is [Copy Tray].

The default setting is [Finisher upper Tray]. (When the Finisher Tray is installed.)

Output: Document Server (Document Server)

Specify a tray to which documents are delivered.

The default setting is [Copy Tray].

The default setting is [Finisher upper Tray]. (When the Finisher Tray is installed.)

Output: Facsimile (facsimile)

Specify a tray to which documents are delivered.

The default setting is [Copy Tray].

The default setting is [Finisher upper Tray]. (When the Finisher Tray is installed.)

Output: Printer (printer)

Specify a tray to which documents are delivered.

The default setting is [Copy Tray].

The default setting is [Finisher upper Tray]. (When the Finisher Tray is installed.)

ADF Original Table Elevation

Set when to raise the ADF plate after placing originals on the Auto Document Feeder (ADF).

The default setting is [When Original is Set].

System Status/Job List Display Time

Specify how long to display the System Status and Job List display for.

The default setting is [On], "15 second(s)".

By selecting [On], you can specify a display time between 10 and 999 seconds.

Time Interval between Printing Jobs

Specify the time interval between printing jobs.

The default setting time is 3 seconds.

Key Repeat

You can enable or disable repetition of an operation if a key on the screen or control panel is pressed continuously.

The default setting is [Normal].

Z-fold Position

If you specify Z-folding, set the fold-back position in 0.1 inch (1 mm) increments. The setting ranges of the folding position for each paper size are shown below:

Inch version:

- A3: 0.1" - 1.0"
- B4 JIS: 0.1" - 0.7"
- A4: 0.1" - 0.7"

- 11 × 17: 0.1" - 0.8"
- 8 1/2 × 14: 0.1" - 0.7"
- 8 1/2 × 11: 0.1" - 0.7"
- Others: 0.1" - 0.7"

Metric version:

- A3: 2 - 25 mm
- B4 JIS: 2 - 17 mm
- A4: 2 - 17 mm
- 11 × 17: 2 - 20 mm
- 8 1/2 × 14: 2 - 17 mm
- 8 1/2 × 11: 2 - 17 mm
- Others: 2 - 17 mm

Half Fold Position

If you specify half folding, set the fold-back position in 0.1 inch (1 mm) increments. The setting ranges of the folding position for each paper size are shown below:

Inch version:

- A3: -0.4" - 0.4"
- B4 JIS: -0.4" - 0.4"
- A4: -0.4" - 0.4"
- 11 × 17: -0.4" - 0.4"
- 8 1/2 × 14: -0.4" - 0.4"
- 8 1/2 × 11: -0.4" - 0.4"
- Others: -0.4" - 0.4"

Metric version:

- A3: -10 - 10 mm
- B4 JIS: -10 - 10 mm
- A4: -10 - 10 mm
- 11 × 17: -10 - 10 mm
- 8 1/2 × 14: -10 - 10 mm
- 8 1/2 × 11: -10 - 10 mm
- Others: -10 - 10 mm

Letter Fold-out Position

If you specify letter fold-out folding, set the fold-back position in 0.1 inch (1 mm) increments. The setting ranges of the folding position for each paper size are shown below:

Inch version:

- A3: -0.4" - 0.4"
- B4 JIS: -0.4" - 0.4"
- A4: -0.4" - 0.4"
- 11 × 17: -0.4" - 0.4"
- 8 1/2 × 14: -0.4" - 0.4"
- 8 1/2 × 11: -0.4" - 0.4"
- Others: -0.4" - 0.4"

Metric version:

- A3: -10 - 10 mm
- B4 JIS: -10 - 10 mm
- A4: -10 - 10 mm
- 11 × 17: -10 - 10 mm
- 8 1/2 × 14: -10 - 10 mm
- 8 1/2 × 11: -10 - 10 mm
- Others: -10 - 10 mm

Letter Fold-in Position

If you specify letter fold-in folding, set the fold-back position in 0.1 inch (1 mm) increments. The setting ranges of the folding position for each paper size are shown below:

Inch version:

- A3: 0.1" - 0.3"
- B4 JIS: 0.1" - 0.3"
- A4: 0.1" - 0.3"
- 11 × 17: 0.1" - 0.3"
- 8 1/2 × 14: 0.1" - 0.3"
- 8 1/2 × 11: 0.1" - 0.3"
- Others: 0.1" - 0.3"

Metric version:

- A3: 2 - 7 mm
- B4 JIS: 2 - 7 mm
- A4: 2 - 7 mm
- 11 × 17: 2 - 7 mm
- 8 1/2 × 14: 2 - 7 mm

- $8\frac{1}{2} \times 11$: 2 - 7 mm
- Others: 2 - 7 mm

Double Parallel Fold Position

If you specify double parallel folding, set the fold-back position in 0.1 inch (1 mm) increments. The setting ranges of the folding position for each paper size are shown below:

Inch version:

- A3: -0.4" - 0.4"
- B4 JIS: -0.4" - 0.4"
- A4: -0.4" - 0.4"
- 11×17 : -0.4" - 0.4"
- $8\frac{1}{2} \times 14$: -0.4" - 0.4"
- $8\frac{1}{2} \times 11$: -0.4" - 0.4"
- Others: -0.4" - 0.4"

Metric version:

- A3: -10 - 10 mm
- B4 JIS: -10 - 10 mm
- A4: -10 - 10 mm
- 11×17 : -10 - 10 mm
- $8\frac{1}{2} \times 14$: -10 - 10 mm
- $8\frac{1}{2} \times 11$: -10 - 10 mm
- Others: -10 - 10 mm

Gate Fold Position

If you specify gate folding, set the fold-back position in 0.1 inch (1 mm) increments. The setting ranges of the folding position for each paper size are shown below:

Inch version:

- A3: 0.1" - 0.5"
- B4 JIS: 0.1" - 0.5"
- A4: 0.1" - 0.5"
- 11×17 : 0.1" - 0.5"
- $8\frac{1}{2} \times 14$: 0.1" - 0.5"
- $8\frac{1}{2} \times 11$: 0.1" - 0.5"
- Others: 0.1" - 0.5"

Metric version:

- A3: 2 - 12 mm

- B4 JIS: 2 - 12 mm
- A4: 2 - 12 mm
- 11 × 17: 2 - 12 mm
- 8 1/2 × 14: 2 - 12 mm
- 8 1/2 × 11: 2 - 12 mm
- Others: 2 - 12 mm

Reference

- p.17 "Accessing User Tools"

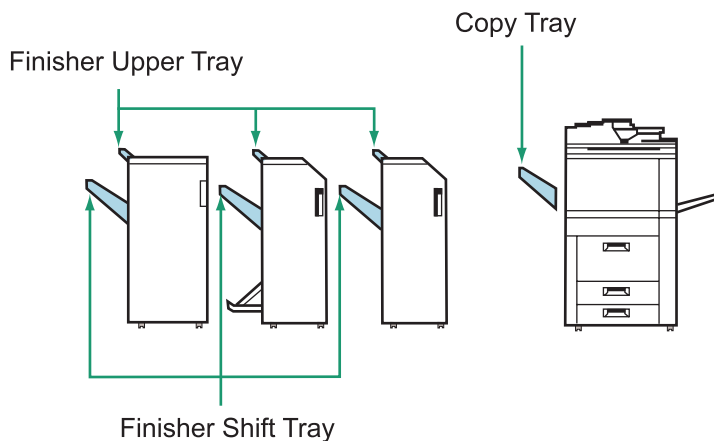
Output Tray Settings

This section describes the output tray settings.

Some trays are not displayed according to the option to install.

Important

- When Finisher is installed, Finisher Upper Tray and Finisher Shift Tray are displayed. The default setting is Finisher Upper Tray.
- You cannot interrupt the current stapling job even if a stapling job is specified by a different function.
- When the optional finisher (SR4030, SR4040 or SR4050) is installed and stapling or shift-sorting is specified, the job will be delivered to the finisher shift tray regardless of the output tray specified.
- When Finisher SR4050 is installed, the Finisher Shift Tray cannot be set as the output tray.



BPV001S

Tray Paper Settings

This section describes the user tools in the Tray Paper Settings menu under System Settings.

★ Important

- If the specified paper size differs from the actual size of the paper loaded in the paper tray, a misfeed might occur because the correct paper size was not detected.

Paper Tray Priority: Copier (copier/Document Server)

Specify the tray to supply paper for output.

The default setting is [Tray 1].

Paper Tray Priority: Facsimile (facsimile)

Specify the tray to supply paper for output.

The default setting is [Tray 1].

Paper Tray Priority: Printer (printer)

Specify the tray to supply paper for output.

The default setting is [Tray 1].

Tray Paper Size: Tray 2 - 3

Select the size of the paper loaded in the paper tray.

The paper sizes you can set for tray 2 - 3 are as follows:

- [Auto Detect]
- [11 × 17□], [11 × 15□], [11 × 14□], [10 × 15□], [8¹/₂ × 14□], [8¹/₂ × 13□], [8¹/₂ × 11□], [8¹/₄ × 14□], [8¹/₄ × 13□], [8 × 13□], [8 × 10¹/₂□], [7¹/₄ × 10¹/₂□], [5¹/₂ × 8¹/₂□], [A3□], [A4□], [A5□], [B4 JIS□], [B5 JIS□], [210 × 340m/m□], [8K□], [16K□]
- [8¹/₂ × 11□], [7¹/₄ × 10¹/₂□], [5¹/₂ × 8¹/₂□], [A4□], [A5□], [B5 JIS□], [182 × 210m/m□], [170 × 210m/m□], [16K□],
- [Custom size]

You can specify a custom size of between 5.5 - 11.7 inch (139.7 - 297.0 mm) vertically, and between 5.5 - 17.0 inch (139.7 - 432.0 mm) horizontally. When finisher SR4030 / 4040 is installed, horizontal size is between 5.5 - 19.2 inch (139.0 - 487.6 mm).

For details about auto detect paper size, see About This Machine.

Printer Bypass Paper Size

Specify the size of the paper in the bypass tray when printing data from the computer.

The paper sizes you can set for bypass tray are as follows:

- [Auto Detect]

- [11 × 17], [11 × 14], [8¹/₂ × 14], [8¹/₂ × 13], [8¹/₂ × 11], [8¹/₄ × 13], [8 × 13], [7¹/₄ × 10¹/₂], [5¹/₂ × 8¹/₂][A3], [A4], [A5], [A6], [B4 JIS], [B5 JIS], [B6 JIS],
- [8¹/₂ × 11], [7¹/₄ × 10¹/₂], [5¹/₂ × 8¹/₂], [A4], [A5], [B5 JIS]
- [Custom Size]

You can specify a custom size of between 4.0 - 12.0 inch (100.0 - 305.0 mm) vertically, and between 5.5 - 23.7 inch (139.7 - 600.0 mm) horizontally.

When finisher SR4030 / 4040 is installed, horizontal size is between 5.5 - 19.2 inch (139.0 - 487.6 mm).

When finisher SR4050 is installed, horizontal size is between 5.5 - 18.1 inch (139.0 - 458 mm).

For details about auto detect paper size, see About This Machine.

For details about specifying custom paper sizes, contact your sales or service representative.

Paper Type: Bypass Tray

Sets the display so you can see what type of paper is loaded in the bypass tray.

The paper types you can set for the bypass tray are as follows:

- [No Display], [Recycled Paper], [Special Paper], [Color Paper 1], [Color Paper 2], [Letterhead], [Label Paper], [Translucent Paper], [Preprinted Paper], [Bond Paper], [Cardstock], [Prepunched Paper], [OHP (Transparency)]

The paper thicknesses you can set for the bypass tray are as follows:

- [Plain Paper] (52 - 80 g/m², 14.0 - 20.0 lb. Bond)
- [Middle Thick] (81 - 103 g/m², 21.0 - 28.0 lb. Bond)
- [Thick Paper] (104 - 216 g/m², 39.0 - 80.0 lb. Cover)

The default setting for "Paper Type" is [No Display].

The default setting for "Paper Thickness" is [Plain Paper].

For details about the relations between possible paper sizes and thickness, see "Recommended Paper Sizes and Types", About This Machine.

For details about the recommended conditions for using thick paper, see "Thick Paper", About This Machine.

Paper Type: Tray 1

Sets the display so you can see what type of paper is loaded in the paper tray 1.

The print function uses this information to automatically select the paper tray.

The paper types you can set for the paper tray 1 are as follows:

- [No Display], [Recycled Paper], [Special Paper], [Color Paper 1], [Color Paper 2], [Letterhead], [Translucent Paper], [Preprinted Paper], [Bond Paper], [Prepunched Paper]

The paper thicknesses you can set for the paper tray 1 are as follows:

- [Plain Paper] (52 - 80 g/m², 14.0 - 20.0 lb. Bond)
- [Middle Thick] (81 - 103 g/m², 21.0 - 28.0 lb. Bond)
- [Thick Paper] (104 - 216 g/m², 39.0 - 80.0 lb. Cover)

The default setting for "Paper Type" is [No Display].

The default setting for "Paper Thickness" is [Plain Paper].

The default setting for "Apply Duplex" is [Yes].

The default setting for "Apply Auto Paper Select" is [Yes].

The key mark is displayed next to the paper tray if [No] is selected in "Auto Paper Select".

Apply Auto Paper Select can only be selected for the copier function if [No Display] and [Recycled Paper] are selected. If [No] is selected, Apply Auto Paper Select is not valid.

For details about the relations between possible paper sizes and thickness, see "Recommended Paper Sizes and Types", About This Machine.

For details about the recommended conditions for using thick paper, see "Thick Paper", About This Machine.

Paper Type: Tray 2 - 3

Sets the display so you can see what type of paper is loaded in the paper tray 2 - 3.

The print function uses this information to automatically select the paper tray.

When "Tab stock" is selected in the paper type, the tab position can be set between 0.0 and 0.6 inch in 0.1 inch increments by using [←] [→].

The default setting is 0.5 inch.

The paper types you can set for the paper tray 2 - 3:

- [No Display], [Recycled Paper], [Special Paper], [Color Paper 1], [Color Paper 2], [Letterhead], [Translucent Paper], [Preprinted Paper], [Bond Paper], [Prepunched Paper], [Tab Stock]

The paper thicknesses you can set for the paper tray 2-3 are as follows:

- [Plain Paper] (52 - 80 g/m², 14.0 - 20.0 lb. Bond)
- [Middle Thick] (81 - 103 g/m², 21.0 - 28.0 lb. Bond)
- [Thick Paper] (104 - 216 g/m², 39.0 - 80.0 lb. Cover)

The default setting for "Paper Type" is [No Display].

The default setting for "Paper Thickness" is [Plain Paper].

The default setting for "Apply Duplex" is [Yes].

The default setting for "Apply Auto Paper Select" is [Yes].

The key mark is displayed next to the paper tray if [No] is selected in "Apply Auto Paper Select".

Apply Auto Paper Select can only be selected for the copier function if [No Display] and [Recycled Paper] are selected. If [No] is selected, Apply Auto Paper Select is not valid.

For details about the relations between possible paper sizes and thickness, see "Recommended Paper Sizes and Types", About This Machine.

For details about the recommended conditions for using thick paper, see "Thick Paper", About This Machine.

Paper Type : LCT

Sets the display so you can see what type of paper is loaded in the LCT.

The print function uses this information to automatically select the paper tray.

The paper types you can set for the LCT:

- [No Display], [Recycled Paper], [Special Paper], [Color Paper 1], [Color Paper 2], [Letterhead], [Preprinted Paper], [Bond Paper], [Prepunched Paper]

The paper thicknesses you can set for the LCT are as follows:

- [Plain Paper] (52 - 80 g/m², 14.0 - 20.0 lb. Bond)
- [Middle Thick] (81 - 103 g/m², 21.0 - 28.0 lb. Bond)
- [Thick Paper] (104 - 216 g/m², 39.0 - 80.0 lb. Cover)

The default setting for "Paper Type" is [No Display].

The default setting for "Paper Thickness" is [Plain Paper].

The default setting for "Apply Duplex" is [Yes].

The default setting for "Apply Auto Paper Select" is [Yes].

The key mark is displayed next to the paper tray if [No] is selected in "Apply Auto Paper Select".

Apply Auto Paper Select can only be selected for the copier function if [No Display] and [Recycled Paper] are selected. If [No] is selected, Apply Auto Paper Select is not valid.

For details about the relations between possible paper sizes and thickness, see "Recommended Paper Sizes and Types", about this machine.

For details about the recommended conditions for using thick paper, see "Thick Paper", About This Machine.

Front Cover Sheet Tray

Allows you to specify and display the paper tray that is setting cover sheets.

After selecting the paper tray, you can also specify the display timing and copy method for two-sided copying.

The default setting is [Off].

When [At Mode Selected] is selected, front cover sheet tray settings only appear when the cover function or slip sheet function is selected.

When [Full Time] is selected, the front cover sheet tray is always displayed.

Back Cover Sheet Tray

Specify which paper tray you want to load the back covers from, and make sure confirmation of your setting is displayed. When you have selected the tray, specify the confirmation timing and the copy method for two-sided copying.

The default setting is [Off].

When [At Mode Selected] is selected, back cover sheet tray settings only appear when the cover function or slip sheet function is selected.

When [Full Time] is selected, the front cover sheet tray is always displayed.

Slip Sheet Tray

You can specify and display the paper tray that is used for setting slip sheets.

You can also specify the display timing and copy method for two-sided copying.

The default setting is [Off].

When [At Mode Selected] is selected, slip sheet tray settings only appear when the cover function or slip sheet function is selected.

When [Full Time] is selected, the slip sheet tray is always displayed.

Designation Sheet 1 Tray, Designation Sheet 2 Tray

Specify which paper tray you want to load the chapter division sheets from, and make sure confirmation of your setting is displayed. When you have selected the tray, specify the confirmation timing and the copy method for two-sided copying.

The default setting is [Off].

When [At Mode Selected] is selected, designation sheet 1 tray or designation sheet 2 tray settings only appear when the cover function, slip sheet function or designation sheet tray is selected.

When [Full Time] is selected, the slip sheet tray is always displayed.

Note

- The paper guide for the LCT is fixed for A4, 8 1/2 × 11 size paper. Contact your service representative if you need to change the paper size.
- When paper of the same type and size is loaded in two different paper trays and you want to specify tray for 2 Sided Copy. If one of the trays is specified as the default in Paper Tray Priority, assign 2 Sided Copy to that tray.
- Functions using the front cover sheet tray setting are the front cover function and front/back cover function.
- The function for using Designation sheet 1 tray or Designation sheet 2 tray is designate.

Reference

- p.17 "Accessing User Tools"

Timer Settings

This section describes the user tools in the Timer Settings menu under System Settings.

Auto Off Timer

After a specified period has passed, following job completion, the machine automatically turns off, in order to conserve energy. This function is called "Auto Off".

The machine status after the Auto Off operation is referred to as "Sleep mode".

For the Auto Off Timer, specify the time to elapse before Auto Off.

The default setting is "1" minute.

The time can be set from 1 to 240 minutes, using the number keys.

Auto Off may not work when error messages appear.

Energy Saver Timer

Set the amount of time the machine waits before switching to lower-power mode after copying has finished or the last operation is performed.

The default setting is "1" minute.

The time can be set from 1 to 240 minutes, using the number keys.

Auto Off may not work when error messages appear.

Panel Off Timer

Set the amount of time the machine waits before switching the panel off after copying has finished or the last operation is performed.

Enter a time interval between 10 seconds and 240 minutes, using the number keys.

The default setting is "10" second (s).

System Auto Reset Timer

The System Reset setting automatically switches the screen to that of the function set in Function Priority when no operations are in progress, or when an interrupted job is cleared. This setting determines the system reset interval.

The time can be set from 10 to 999 seconds, using the number keys.

The default setting is [On], "60" second (s).

Copier / Document Server Auto Reset Timer (copier/Document Server)

Specifies the time to elapse before copier and Document Server modes reset.

If [Off] is selected, the machine does not automatically switch to the user code entry screen.

The time can be set from 10 to 999 seconds, using the number keys.

The default setting is [On], "60" second (s).

Facsimile Auto Reset Timer (facsimile)

Specify the time to elapse before the facsimile mode resets.

The time can be set from 30 to 999 seconds, using the number keys.

The default setting is "30" second (s).

Printer Auto Reset Timer (printer)

Specify the time to elapse before the printer function resets.

The time can be set from 10 to 999 seconds, using the number keys.

The default setting is [On], "60" second (s).

Scanner Auto Reset Timer (scanner)

Specify the time to elapse before the scanner function resets.

If [Off] is selected, the machine will not automatically switch to the user code entry screen.

The time can be set from 10 to 999 seconds, using the number keys.

The default setting is [On], "60" second (s).

Set Date

Set the date for the copier's internal clock using the number keys.

To change between year, month, and day, press [←] and [→].

Set Time

Set the time for the copier's internal clock using the number keys.

Enter the time using the 12-hour format (in 1 second increments).

To change between hours, minutes and seconds, press [←] and [→].

Auto Logout Timer

Specify whether or not to automatically log out a user when the user does not operate the machine for a specified period of time after logging in.

The time can be set from 60 to 999 seconds, in one second increments, using the number keys.

The default setting is [On], "180" second (s).

Weekly Timer Code

Set a password (using not more than eight digits) for turning on the power during the time periods when "Weekly Timer" turns off the machine's power. If you have selected "On", enter the password. When you select "on", you cannot use the machine even if you turn the power switch to "On", unless you enter the password. If you select "Off", you do not have to enter a password to switch on the machine, you need only turn the power switch to "On".

The default setting is [Off].

Weekly Timer: Monday – Sunday

Set the daily time when the power is switched on/off.

Power On Time

Power Off Time

Enter the time using the 12-hour system.

Enter the "hour" and "minute" using the number keys.

E Reference

- p.17 "Accessing User Tools"

Interface Settings

This section describes the user tools in the Interface Settings menu under System Settings.

1

Network

This section describes the user tools in the Network menu under Interface Settings.

Machine IPv4 Address

Specify the machine's IPv4 network address.

The default setting is [Auto-Obtain (DHCP)].

When you select [Specify], enter the IPv4 address and subnet mask as "xxx.xxx.xxx.xxx" ("x" indicates a number).

When you select [Specify], make sure that IPv4 address is different from that of other machines on the network.

The physical address (MAC address) also appears.

IPv4 Gateway Address

A gateway is a connection or interchange point between two networks.

Specify the gateway address for the router or host computer used as a gateway.

The default setting is "0.0.0.0".

Machine IPv6 Address

Displays the machine's IPv6 network address.

- Link-local Address
The machine's specified link-local address appears.
- Manual Configuration Address
The machine's manually configured address appears.
- Stateless Address: 1-5
The specified stateless address appears.

IPv6 Gateway Address

Displays the machine's IPv6 gateway address.

IPv6 Stateless Address Autoconfiguration

Specify IPv6 Stateless Address Autoconfiguration.

The default setting is [Active].

DNS Configuration

Make settings for the DNS server.

The default setting is [Auto-Obtain (DHCP)].

When you select [Specify], enter the DNS Server IPv4 address as "xxx.xxx.xxx.xxx" ("x" indicates a number).

DDNS Configuration

Specify the DDNS settings.

The default setting is [Active].

IPsec

Specify the machine's IPsec function Active/Inactive.

The default setting is [Inactive].

Domain Name

Specify the domain name.

The default setting is [Auto-Obtain (DHCP)].

When you select [Specify], enter the domain name using up to 63 characters.

WINS Configuration

Specify the WINS server settings.

The default setting is [On].

If [On] is selected, enter the WINS Server IPv4 address as "xxx.xxx.xxx.xxx" ("x" indicates a number).

If DHCP is in use, specify the Scope ID. Enter a Scope ID using up to 31 characters.

Effective Protocol

Select the Protocol to use in the network.

The default setting for "IPv4" is [Active].

The default setting for "IPv6" is [Inactive].

The default setting for "NetWare" is [Inactive].

The default setting for "SMB" is [Active].

The default setting for "AppleTalk" is [Active].

NCP Delivery Protocol

Select the protocol NCP delivery.

The default setting is [TCP / IP Priority].

If you select [IPX Only] or [TCP / IP Only], you cannot switch the protocol even if you cannot connect with it. If "NetWare" in "Effective Protocol" is set to [Inactive], you can only use TCP/IP.

NW Frame Type

Select the frame type when you use NetWare.

The default setting is [Auto Select].



SMB Computer Name

Specify the SMB computer name.
 Enter the computer name using up to 15 characters.
 "*" + , / ; < > = ? [\] | . and spaces cannot be entered.
 Do not set a computer name starting with RNP and rnp.
 Use uppercase letters for alphabets.

SMB Work Group

Specify the SMB work group.
 Enter the computer name using up to 15 characters.
 "*" + , / ; < > = ? [\] | . and spaces cannot be entered.
 Use uppercase letters for alphabet.

Ethernet Speed

Set the access speed for networks.
 The default setting is [Auto Select].
 Select a speed that matches your network environment. [Auto Select] should usually be selected.

	10Mbps Half Duplex	10Mbps Full Duplex	100Mbps Half Duplex	100Mbps Full Duplex	Auto Select
10Mbps Half Duplex	●	—	—	—	●
10Mbps Full Duplex	—	●	—	—	—
100Mbps Half Duplex	—	—	●	—	●
100Mbps Full Duplex	—	—	—	●	—
Auto Select	●	—	●	—	●

IEEE 802.1X Authentication for Ethernet

Specify the IEEE 802.1X authentication for Ethernet.
 The default setting is [Inactive].
 For details about IEEE 802.1X authentication, see "Configuring IEEE 802.1X".

Restore IEEE 802.1X Authentication to Defaults

You can return the IEEE 802.1X authentication settings to their defaults.

For details about IEEE 802.1X authentication, see "Configuring IEEE 802.1X".

LAN Type

When you have installed the Wireless LAN interface unit, select the method of connection.

The default setting is [Ethernet].

[LAN Type] is displayed when wireless LAN board is installed. If Ethernet and Wireless LAN are both connected, the selected interface has priority.

Ping Command

Check the network connection with ping command using given IPv4 address.

If you fail to connect to the network, check the following, and then retry the ping command.

- Make sure that "IPv4" in [Effective Protocol] is set to [Active].
- Check that the machine with assigned IPv4 address is connected to the network.
- There is a possibility that the same IPv4 address is used for the specified equipment.

Permit SNMPv3 Communication

Set the encrypted communication of SNMPv3.

The default setting is [Encryption / Cleartext].

If you select to [Encryption Only], you need to set an encryption password for the machine.

Permit SSL / TLS Communication

Set the encrypted communication of SSL/TLS.

The default setting is [Ciphertext Priority].

If you set to [Ciphertext Only], you need to install the SSL certificate for the machine.

Host Name

Specify the host name.

Enter the host name using up to 63 characters.

Machine Name

Specify the machine name.

Enter the machine name using up to 31 characters.

Reference

- p.17 "Accessing User Tools"
- p.341 "Configuring IEEE 802.1X"

Parallel Interface

This section describes the user tools in the Parallel Interface menu under Interface Settings.

[Parallel Interface] is displayed when this machine is installed with the IEEE 1284 interface board.

Parallel Timing

Sets the timing for the control signal of the parallel interface.

Normally, you do not need to change this setting.

The default setting is [ACK Outside].

Parallel Communication Speed

Sets the communication speed for the parallel interface. If the speed is too high, data may not be transferred smoothly. If this happens, change the setting to [Standard].

The default setting is [High Speed].

Selection Signal Status

Sets the level for the select signal of the parallel interface.

The default setting is [High].

Input Prime

Sets whether to validate or invalidate the input prime signal upon reception.

Normally, you do not need to change this setting.

The default setting is [Inactive].

Bidirectional Communication

Sets the printer's response mode to a status acquisition request when using a parallel interface. If you experience problems using another manufacturer's machine, set this to [Off].

The default setting is [On].

When set to [Off], the bidirectional communication function will be disabled, and the printer driver will not be installed under Windows Auto Detect function.

Signal Control

Specifies how error during printing or sending facsimile from the computer is to be dealt with.

Normally, you do not need to change this setting.

The default setting is [Job Acceptance Priority].

Reference

- p.17 "Accessing User Tools"

Wireless LAN

This section describes the user tools in the Wireless LAN menu under Interface Settings.

[Wireless LAN] is displayed when this machine is installed with the wireless LAN interface board.

Be sure to make all settings simultaneously.

Communication Mode

Specifies the communication mode of the wireless LAN.

The default setting is [Infrastructure Mode].

SSID Setting

Specifies SSID to distinguish the access point in [Infrastructure Mode] or [802.11 Ad-hoc Mode].

The characters that can be used are ASCII 0x20-0x7e (32 bytes).

If blank is specified in [802.11 Ad-hoc Mode], "ASSID" appears.

Ad-hoc Channel

Specify the channel to use when [802.11 Ad-hoc Mode] has been selected. Set the channel that matches the type of wireless LAN being used.

The following channels are available:

- IEEE 802.11 a/b/g Wireless LAN

Frequency range:

2412 - 2462 MHz (1 - 11 channels)

5180 - 5320 MHz (36, 40, 44 and 48 channels)

The default setting is [11].

The channel in use might differ depending on the country.

Security Method

Specifies the encryption of the Wireless LAN.

The default setting is [Off].

If you select [WEP], always enter WEP key. If you select [WPA], specify the encryption and authentication methods.

Specify "WPA", when [Communication Mode] is set to [Infrastructure Mode].

- WEP

If you select [WEP], enter WEP key.

When using 64 bit WEP, up to 10 characters can be used for hexadecimal and up to five characters for ASCII. When using 128 bit WEP, up to 26 characters can be used for hexadecimal and up to 13 characters for ASCII.

The number of characters that can be entered is limited to 10 or 26 for hexadecimal and 5 or 13 for ASCII.

- WPA
 - WPA Encryption Method
Select either [TKIP] or [CCMP (AES)].
 - WPA Authent. Method

Select either [WPA-PSK], [WPA], [WPA2-PSK], or [WPA2].

If you selected [WPA-PSK] or [WPA2-PSK], enter the pre-shared key (PSK) of 8- 63 characters in ASCII code.

When [WPA] or [WPA2] are selected, authentication settings and certificate installation settings are required. For details about setting methods, see "Configuring IEEE 802.1X".

Wireless LAN Signal

When using in infrastructure mode, you can check the machine's radio wave status using the control panel.

Radio wave status is displayed when you press [Wireless LAN Signal].

Restore Factory Defaults

You can return the wireless LAN settings to their defaults.

Reference

- p.17 "Accessing User Tools"
- p.341 "Configuring IEEE 802.1X"

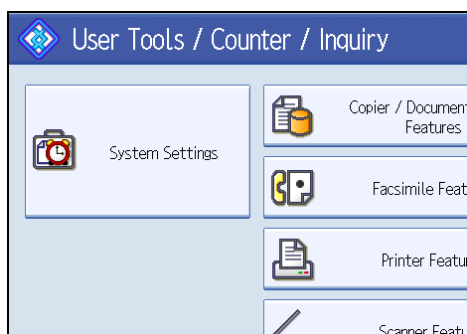
Print List

This section describes how to print the configuration page.

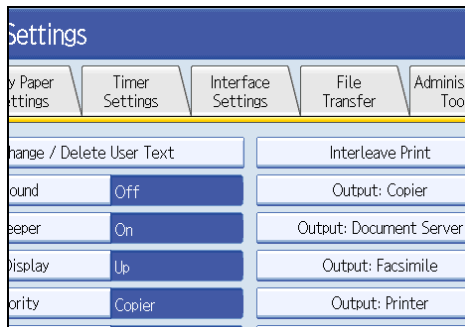
You can check items related to the network environment.

The configuration page shows the current network settings and network information.

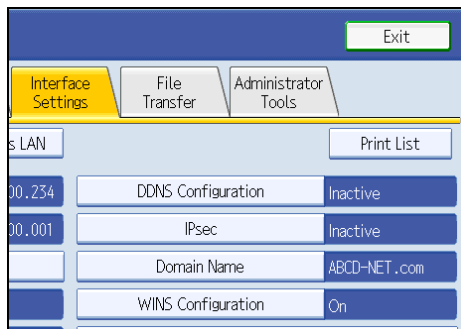
1. Press the [User Tools / Counter] key.
2. Press [System Settings].



3. Press [Interface Settings].



4. Press [Print List].



5. Press the [Start] key.

The configuration page is printed.

6. Press [Exit].

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

↓ Note

- You can also exit by pressing [Exit] on the User Tools main menu.

📖 Reference

- p.17 "Accessing User Tools"

File Transfer

This section describes the user tools in the File Transfer menu under System Settings.

1

Delivery Option

Enables or disables sending stored or scanned documents to the ScanRouter delivery server.

The default setting is [Off].

Specify this option when selecting whether or not to use the ScanRouter delivery software. If you do, you will have to preregister I/O devices in the ScanRouter delivery software.

Capture Server IPv4 Address

Specify the capture server IPv4 address.

This setting appears when the File Format Converter is installed, and when the capture function is being used by the ScanRouter delivery software.

Fax RX File Transmission

Specify how to deliver fax files received via the different lines.

- Setting per Line

Specifies whether or not received fax documents are sent to the ScanRouter delivery software for each fax line.

- G3 Port 1
- G3 Port 2
- G3 Port 3
- E-mail
- IP-Fax

The default setting is [Do not Deliver].

The lines appear according to the operating environment.

- RX File Delivery

Specifies whether or not received fax documents are sent to the ScanRouter delivery software for each fax line.

The default setting is [Do not Deliver].

- Print at Deliver

Specify whether or not received fax documents sent to the ScanRouter delivery software should also be printed at the same time.

The default setting is [Do not Print].

- File to Deliver

Specify whether all received fax documents or only received fax documents that include delivery codes (documents with an ID or SUB/SEP codes) are sent to the ScanRouter delivery software.

The default setting is [All Files].

- Delivery Failure File

If a fax is received but cannot be sent via the ScanRouter delivery software, it is stored in the machine's memory. If received document deletion is set to "1(On)", documents that cannot be stored due to insufficient memory or an internal hard disk error will automatically be deleted, and a Reception File Erased Report will be printed.

For details about the Reception File Erased Report, see "Reception File Setting" in the "Facsimile Reference". To print a stored file, select [Print File], and to delete stored files, select [Delete File].

- Print File
- Delete File

This setting appears when the delivery function is being used by the ScanRouter delivery software.

SMTP Server

Specify the SMTP server name.

If DNS is in use, enter the host name.

If DNS is not in use, enter the SMTP server IPv4 address.

The default setting for "Port No." is "25".

Enter the server name using up to 127 characters. Spaces cannot be entered.

Enter port number between 1 and 65535 using the number keys, and then press the [#] key.

The SMTP server shares the same port number with the Direct SMTP server.

SMTP Authentication

Specify SMTP authentication (PLAIN, LOGIN, CRAMMD5, DIGEST-MD5). When sending e-mail to an SMTP server, you can enhance the SMTP server security level using authentication that requires entering the user name and password.

If the SMTP server requires authentication, set [SMTP Authentication] to [On], and then specify the user name, password and encryption.

Enter the user name and password to be set for the Administrator's e-mail address when using Internet Fax.

The default setting is [Off].

- Enter the user name using up to 191 characters.
Spaces cannot be entered. Depending on the SMTP server type, "realm" must be specified. Add "@" after the user name, as in "user name@realm".
- Enter the E-mail address using up to 128 characters.
- Enter the password using up to 128 characters.
Spaces cannot be entered.
- Select Encryption as follows:

"Encryption"-[Auto]

Use if the authentication method is PLAIN, LOGIN, CRAM-MD5, or DIGEST-MD5.

"Encryption"-[On]

Use if the authentication method is CRAMMD5 or DIGEST-MD5.

"Encryption"-[Off]

Use if the authentication method is PLAIN, or LOGIN.

POP before SMTP

Specify POP authentication (POP before SMTP).

When sending e-mail to an SMTP server, you can enhance the SMTP server security level by connecting to the POP server for authentication.

The default setting is [Off].

If you set POP before SMTP to [On], specify the waiting time after authentication, user name, e-mail address, and password.

- Wait Time after Authent.: "300" msec.

Specify [Wait Time after Authent.] from zero to 10,000 milliseconds, in increments of one millisecond.

- User Name

Enter the user name using up to 191 characters. Spaces cannot be entered.

- E-mail Address

Enter the E-mail Address using up to 128 characters. Spaces cannot be entered.

- Password

Enter the password using up to 128 characters. Spaces cannot be entered.

To enable POP server authentication before sending e-mail via the SMTP server, set [POP before SMTP] to [On]. E-mail is sent to the SMTP server after the time specified for [Wait Time after Authent.] has elapsed.

If you select [On], enter server name in POP3/IMAP4 Settings. Also, check POP3 port number in E-mail Communication Port.

Reception Protocol

Specify the Reception Protocol for receiving Internet Fax.

The default setting is [POP3].

POP3 / IMAP4 Settings

Specify the POP3/IMAP4 server name for receiving Internet faxes.

The specified POP3/IMAP4 server name is used for [POP before SMTP].

The default setting is [Auto].

- Server Name

If DNS is in use, enter the host name.

If DNS is not in use, enter the POP3/IMAP4 or server IPv4 address.

Enter POP3/IMAP4 server name using up to 127 characters. Spaces cannot be entered.

- Select Encryption as follows:

"Encryption" -[Auto]

Password encryption is automatically set according to the POP/IMAP server settings.

"Encryption" -[On]

Encrypt password.

"Encryption" -[Off]

Do not encrypt password.

Administrator's E-mail Address

Specify the Administrator's E-mail Address.

If a failure occurs in the machine or consumables need to be replaced, e-mail messages are sent to the Administrator's E-mail Address by E-mail Notification function.

On e-mailed scanned documents, if the sender is not specified this appears as the sender's address.

When sending e-mail under the Internet fax function, administrator's e-mail address will appear as the sender's address under the following conditions:

- The sender has not been specified and the machine's e-mail address has not been registered.
- The specified sender is not registered in the machine's address book and the machine's e-mail address has not been registered.

When conducting SMTP authentication for the transmitted files under the Internet fax function, the Administrator's E-mail Address will appear in the "From:" box. If you have specified the user name and e-mail address in [SMTP Authentication], make sure to specify this setting.

Enter up to 128 characters.

On e-mailed scanned documents, if [Auto Specify Sender Name] is [Off], specify the sender.

E-mail Communication Port

Specify the port numbers for receiving Internet faxes. The specified POP3 port number is used for [POP before SMTP].

The default setting for POP3 is "110".

The default setting for IMAP4 is "143".

Enter a port number between 1 and 65535 using the number keys, and then press the [#] key.

E-mail Reception Interval

Specify, in minutes, the time interval for receiving Internet faxes via POP3 or IMAP4 server.

The default setting is [On], "15 minute (s)".

If [On] is selected, the time can be set from 2 to 1440 minutes in increments of one minute.

Max. Reception E-mail Size

Specify the maximum reception e-mail size for receiving Internet faxes.

The default setting is "2" MB.

Enter a size from 1 - 50 MB in increments of one megabyte.

E-mail Storage in Server

Specify whether or not to store received Internet fax e-mails on the POP3 or IMAP4 server.

The default setting is [Off].

Default User Name / Password (Send)

Specify the user name and password required when sending scan files directly to a shared folder on a computer running Windows, to an FTP server, or to a NetWare server.

Enter in up to 128 characters.

Program / Change / Delete E-mail Message

You can program, change, or delete the e-mail message used when sending an Internet fax or scan file as an attachment.

- Program/Change:

1. Press the [User Tools / Counter] key.
2. Press [System Settings].
3. Press [File Transfer].
4. Press [▼Next].
5. Press [Program / Change / Delete E-mail Message].
6. Check that [Program / Change] is selected.
7. Press [*Not Programmed].

To change the registered e-mail message, select the e-mail message to change.

8. Press [Change] under the "Name".
9. Enter a name, and then press [OK].
Enter the name using up to 20 characters.
10. Press [Edit].
To start a new line, press [OK] to return to the e-mail message screen, and then press [▼Next] in "Select Line to Edit:".
11. Enter the text, and then press [OK].
Enter up to five lines of text. Each line can consist of up to 80 characters.
12. Press [OK].
13. Press [Exit].
14. Press the [User Tools / Counter] key.

- Delete:
 1. Press the [User Tools / Counter] key.
 2. Press [System Settings].
 3. Press [File Transfer].
 4. Press [▼Next].
 5. Press [Program / Change / Delete E-mail Message].
 6. Press [Delete].
 7. Select the e-mail message to delete.

The confirmation message about deleting appears.
 8. Press [Yes].
 9. Press [Exit].
 10. Press the [User Tools / Counter] key.

Auto Specify Sender Name

Set whether or not to specify the name of the sender when sending e-mail.

The default setting is [Off].

- On

If you select [On], the specified e-mail address will appear in the "From:" box. If you do not specify the sender's address, the administrator's e-mail address will appear in the "From:" box.

If you do not specify the sender when sending a file by e-mail under the fax function, or if the specified e-mail address is not registered in the machine's address book, the machine's e-mail address will appear in the "From:" box. If the machine does not have an e-mail address, the administrator's e-mail address will appear in the "From:" box.

- Off

If you select [Off], the specified e-mail address will appear in the "From:" box, but you cannot send e-mail without specifying the sender's e-mail address. Under the fax function, you cannot send e-mail if the specified sender's e-mail address is not registered in the machine's address book.

Fax E-mail Account

Specify e-mail address, user name and password for receiving Internet faxes.

The default setting is [Do not Receive].

- E-mail Address

Enter an e-mail address using up to 128 characters.
- User Name

Enter a user name using up to 191 characters.
- Password

Enter a password using up to 128 characters.

Scanner Resend Interval Time

Specifies the interval the machine waits before resending a scan file, if it cannot be sent to the delivery server or mail server.

The default setting is "300" second (s).

The interval time can be set from 60 to 900 seconds in one second increments, using the number keys.

This setting is for the scanner function.

This setting is not valid for the WSD scanner function.

Number of Scanner Resends

Sets a maximum number of times a scan file is resent to the delivery server or mail server.

The default setting is [On], "3" time (s).

If [On] is selected, the number of times can be set from 1 to 99.

This setting is for the scanner function.

This setting is not valid for the WSD scanner function.

Reference

- p.17 "Accessing User Tools"

Administrator Tools

This section describes the user tools in the Administrator Tools menu under System Settings.

Administrator Tools are used by the administrator. To change these settings, contact the administrator.

We recommend specifying Administrator Authentication before making Administrator Tools settings.

Address Book Management

You can add, change or delete information registered in the Address Book.

For details, see "Address Book".

- Program / Change

You can register and change names as well as user codes.

- Names

You can register a name, key display, registration number, and title selection.

- Auth. Info

You can register a user code, and specify the functions available to each user code. You can also register user names and passwords to be used when sending e-mail, sending files to folders, or accessing an LDAP server.

- Protection

You can register a protection code.

- Fax Dest.

You can register a fax number, international TX mode, fax header, label insertion, IP-Fax destination, and protocol.

- E-mail

You can register an e-mail address.

- Folder

You can register the protocol, path, port number, and server name.

- Add to Group

You can put names registered in the Address Book into a group.

- Delete

You can delete a name from the Address Book.

You can register up to 2,000 names.

You can register up to 500 user codes.

You can also register and manage names in the Address Book using Web Image Monitor or SmartDeviceMonitor for Admin.

Address Book: Program / Change / Delete Group

Names registered in the Address Book can be added into a group. You can then easily manage the names registered in each group.

• Program / Change

You can register and change groups.

• Names

You can register a name, key display, registration number, and title selection.

• Programmed User/Group

You can check the names or groups registered in each group.

• Protection

You can register a protection code.

• Add to Group

You can put groups registered in the Address Book into a group.

• Delete

You can delete a group from the Address Book.

You can register up to 100 groups.

You can also register and manage groups in the Address Book using Web Image Monitor or SmartDeviceMonitor for Admin.

Use SmartDeviceMonitor for Admin provided with the printer scanner unit.

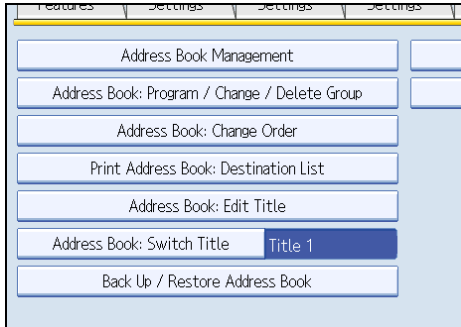
Address Book: Change Order

Changes the order of registered names.

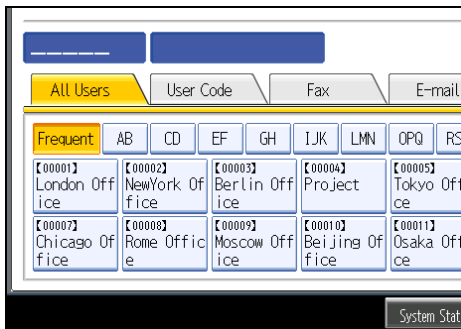
You can rearrange the order of items on the same page, but you cannot move items to another page.

For example, you cannot move an item from "PLANNING" ([OPQ]) to "DAILY" ([CD]).

1. Press the [User Tools / Counter] key.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [Address Book: Change Order].

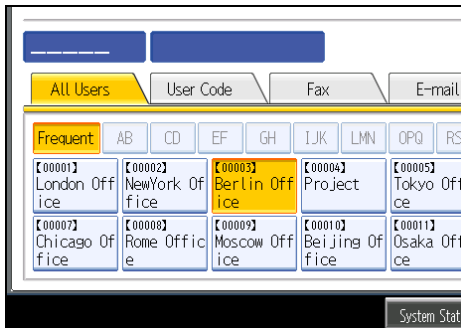


5. Press the name key to be moved.



You can select a name using the number keys.

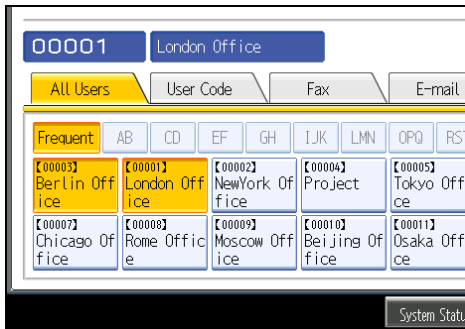
6. Press the name key in place you want to move it to.



The user key is moved to the selected position, and the user key currently at the selected position is moved forward or backward.

If you move the selected user key forward, the user key currently at the selected position is moved backward.

If you move the selected user key backward, the user key currently at the selected position is moved forward.



You can also select a name using the number keys.

Print Address Book: Destination List

You can print the destination list registered in the Address Book.

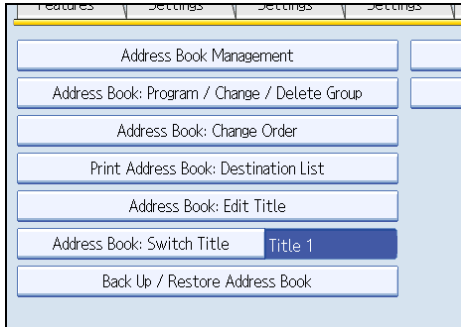
- Print in Title 1 Order
Prints the Address Book in Title 1 order.
- Print in Title 2 Order
Prints the Address Book in Title 2 order.
- Print in Title 3 Order
Prints the Address Book in Title 3 order.
- Print Group Dial List
Prints the group Address Book.
 1. Press the [User Tools / Counter] key.
 2. Press [System Settings].
 3. Press [Administrator Tools].
 4. Press [Print Address Book: Destination List].
 5. Select the print format.
 6. To print the list on two-sided pages, select [Print on 2 Sides].
 7. Press the [Start] key.

The list prints out.

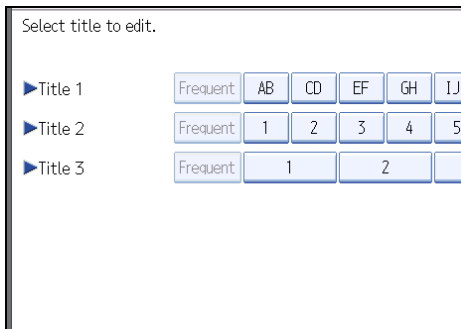
Address Book: Edit Title

You can edit the title to easily find a user.

1. Press the [User Tools / Counter] key.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [Address Book: Edit Title].



5. Press the title key you want to change.



6. Enter the new name, and then press [OK].
7. Press [OK].
8. Press the [User Tools / Counter] key.

Address Book: Switch Title

Specifies the title to select a name.

The default setting is [Title 1].

Back Up / Restore Address Book

You can back up the machine's address book to external storage or restore the backup copy from the external storage.

Restore data overwrites Address Book data stored on the machine, and clears the counter of each registered user of the machine.

- Back Up
You can back up the machine's address book to external storage.
- Restore
You can restore the backup copy of the address book from external storage.
- Format
You can format the external storage.
- Obtain Memory Device Info

The free space and occupied space of the external storage are displayed.

Data Carry-over Setting for Address Book Auto Program

By using Data Carry-over Settings for Address Book Auto Program, you can carry over user authentication information that has already been registered to the address book of the Windows authentication, LDAP authentication, or integration server authentication.

The default setting is [Do not Carry-over].

If you select [Carry-over Data], use the number keys to enter the registration number of the data you wish to carry over from an address book.

For details about the Windows authentication, LDAP authentication, or Integration server authentication, consult your administrator.

Display / Print Counter

Allows you to view and print the number of prints.

- **Display / Print Counter**
Displays the number of prints for each function (Total, Copier, Printer, A3/DLT, Duplex, Fax Prints, Send / TX Total, Fax Transmission, Scanner Send).
- **Print Counter List**
Prints out a list of the number of prints made under each function.

Display / Clear / Print Counter per User

Allows you to view and print the numbers of prints accessed with user codes, and to set those values to 0.

Press [**▲**Previous] and [**▼**Next] to show all the numbers of prints.

The number of prints may differ from the counter values shown in Display/Print Counter.

- **Print Counter List for All Users**
Prints the counter value for all the users.
- **Clear Counter List for All Users**
Resets the counter value for all the users.
- **Print Counter List Per User**
Prints the counter value for each user.
- **Clear Counter List Per User**
Resets the counter value for each user.
- **Select All on the Page**
Select all the users on the page.

User Authentication Management

- **User Code Auth.**
Using User Code Authentication, you can limit the available functions and supervise their use.

When using User Code Authentication, register the user code.

Using the Printer PC Control function, you can obtain a log of prints corresponding to the codes entered using the printer driver.

For details about Basic Authentication, Windows Authentication, LDAP Authentication, and Integration Server Authentication, consult your administrator.

Function to Restrict

- Copier
- Document Server
- Facsimile
- Printer
- Printer: PC Control
- Scanner

Printer Job Authentication

- Entire
- Simple (Limitation)
- Simple (All)
- Basic Auth.
- Windows Auth.
- LDAP Auth.
- Integration Svr. Auth.
- Off

The default setting is [Off].

Enhanced Authentication Management

For details about this function, consult your administrator.

Administrator Authentication Management

For details about this function, consult your administrator.

Program / Change Administrator

For details about this function, consult your administrator.

Key Counter Management

Specify the functions you want to manage with the key counter.

- Copier
- Document Server
- Facsimile
- Printer

- Scanner

External Charge Unit Management

For details about this function, consult your administrator.

Enhanced External Charge Unit Management

For details about this function, consult your administrator.

Extended Security

Specify whether or not to use the extended security functions. For details about the extended security functions, consult your administrator.

Auto Delete File in Document Server

Specify whether documents stored in the Document Server will or will not be deleted after a specified period of time.

The default setting is [On], "3" day (s).

If you select [On], documents stored subsequently are deleted after the specified period.

If you select [Off], documents are not automatically deleted.

If you select [On], enter a number of days from 1 to 180 (in 1 day increments).

The default is 3 days, this means documents are deleted 3 days (72 hours) after they are stored.

Delete All Files in Document Server

You can delete files stored in the Document Server, including files stored for Sample Print, Locked Print, Hold Print, and Stored Print under the printer function.

Even if a password is always set, all documents are deleted.

A confirmation message appears. To delete all documents, select [Yes].

Program / Change / Delete LDAP Server

Program the LDAP server to find up e-mail destinations in the LDAP server Address Book directly. This function is possible when sending scan files by e-mail using the scanner or fax function.

- Name
- Server Name
- Search Base
- Port Number
- Use Secure Connection (SSL)
- Authentication
- User Name
- Password
- Realm Name
- Search Conditions

- Search Options

To start an LDAP search, make sure that the items listed below are set. For other items, check your environment and make any necessary changes.

This function supports LDAP Version 2.0 and 3.0.

To use the LDAP server, select [On] under LDAP Search.

For details about how to program the LDAP Server, see "Programming the LDAP server".

LDAP Search

Specify whether or not to use the LDAP server for searching.

The default setting is [Off].

If you select [Off], LDAP server list will not appear on the searching display.

Program / Change / Delete Realm

Program the realm to be used for Kerberos authentication.

- Realm Name
- KDC Server Name
- Domain Name

Be sure to set both the realm name and KDC server name when programming a realm.

For details about Program/Change/Delete Realm, see "Programming the Realm".

AOF (Always On)

Specify whether or not to use Auto Off.

The default setting is [On].

Firmware Version

You can check the version of the software installed in this machine.

Network Security Level

For details about this function, consult your administrator.

Auto Erase Memory Setting

For details about this function, consult your administrator.

Erase All Memory

For details about this function, consult your administrator.

Delete All Logs

For details about this function, consult your administrator.

Transfer Log Setting

For details about this function, consult your administrator.

Data Security for Copying

For details about this function, consult your administrator.

Print Backup: Delete All Files

To delete a print backup document, press [Yes].

Print Backup: Compression

Set the compression method for the document you want to back up.

The default setting is [High Compression].

Print Backup: Default Format

Set the default format for the document you want to back up.

The default setting is [For Printing].

Print Backup: Default Resolution

Set the default resolution for the document you want to back up.

The default setting is 50 %.

Fixed USB Port

Specify whether or not to fix the USB port.

The default setting is [Off].

If set to [Level 1]

It is not necessary to install a new driver when the printer driver of this machine has already been installed on the PC.

If set to [Level 2]

Please contact your service representative for details.

Reference

- p.17 "Accessing User Tools"
- p.59 "Programming the LDAP server"
- p.65 "Programming the Realm"

Programming the LDAP server

This section describes how to specify the LDAP server settings.

This function supports LDAP version 2.0 and 3.0.

Program the LDAP server to find e-mail destinations in the LDAP server Address Book directly.

This function is possible when sending scan files by e-mail using the scanner or fax function.

To start an LDAP search, make sure that the items listed below are set. For other items, check your environment and make any necessary changes.

- Server Name
- Search Base
- Port Number
- Authentication
- Search Conditions

If [Kerberos Authentication] is selected be sure to set the "User Name", "Password", and the "Realm Name".

If [Digest Authentication] or [Cleartext Authentication] is selected be sure to set the "User Name" and "Password".

To use the LDAP server in Administrator Tools, select [On] under "LDAP Search".

The LDAP version 2.0 does not support Digest Authentication.

To select Kerberos Authentication, a realm must be registered in advance.

Programming the LDAP server

This section describes how to program the LDAP server.

1. Press the [User Tools / Counter] key.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [▼Next] twice.
5. Press [Program / Change / Delete LDAP Server].
6. Check that [Program/Change] is selected.
7. Select the LDAP server you want to program or change.
When programming the server, select [*Not Programmed].
8. Press [Change] under "Name".
9. Enter the name, and then press [OK].
10. Press [Change] under "Server Name".

11. Enter the server name, and then press [OK].

12. Press [Change] under "Search Base".

Select a root folder to start the search from e-mail addresses registered in the selected folder are search targets.

13. Enter the search base, and then press [OK].

For example, if the search target is the sales department of ABC company, enter "dc=sales department, o=ABC". (In this example, the description is for an active directory. "dc" is for the organization unit, and "o" is for the company.)

Search base registration may be required depending on your server environment. When registration is required, unspecified searches will result in error.

Check your server environment and enter any required specifications.

14. Press [Change] under "Port Number".

Specify the port number for communicating with the LDAP server. Specify a port that is compliant with your environment.

15. Enter the port number using the number keys, and then press the [#] key.

When SSL is set to [On], the port number automatically changes to "636".

16. Under "Use Secure Connection (SSL)", press [On].

Use SSL to communicate with the LDAP server.

For SSL to function, the LDAP server must support SSL.

If you set SSL to [On], the port number automatically changes to "636".

If you do not enable SSL, security problems may occur. To enable SSL, you must use the machine's settings. For details, consult your network administrator.

17. Press [▼Next].

18. Select the authentication method.

To make a search request to the LDAP server, use the administrator account for authentication.

Authentication settings must comply with your server's authentication settings. Check your server settings before setting this machine.

[Digest Authentication] is available only with LDAP Version 3.0.

If you select [Cleartext Authentication], a password is sent to the LDAP server as is, without any encryption processing.

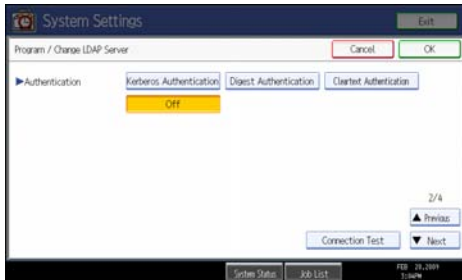
If you select [Digest Authentication], a password is sent using an encryption process that prevents passwords from being revealed during transmission to the LDAP server.

If you select [Kerberos Authentication], a password is sent using an encryption process that prevents passwords from being revealed during transmission to the KDC server where authentication occurs.

If you select [Off], proceed to step 24.

If you select [Digest Authentication] or [Cleartext Authentication], proceed to step 19 to 22, and then proceed to step 24.

If you select [Kerberos Authentication], proceed to step 19 to 23, and then proceed to step 24.



19. Press [Change] under "User Name".

When [Kerberos Authentication], [Digest Authentication], or [Cleartext Authentication] is selected for the authentication setting, use the administrator account name and password. Do not enter the administrator account name and password when using authentication for each individual or each search.

20. Enter the user name, and then press [OK].

Procedures for the user name setting differ depending on server environment. Check your server environment before making the setting.

Example: Domain Name\User Name, User Name@Domain Name, CN=Name, OU=Department Name, DC=Server Name

21. Press [Change] under "Password".

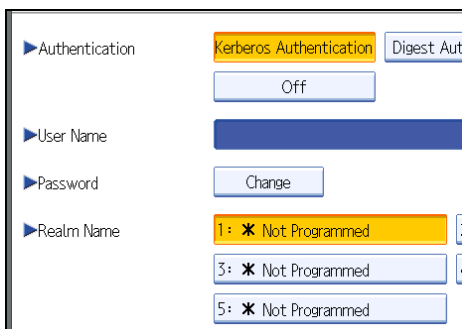
22. Enter the password, and then press [OK].

The user name and password are required for administrator authentication to access the LDAP server.

You can connect to the LDAP server using a user name and password stored in the Address Book. For details, see "Registering SMTP and LDAP Authentication".

If you select [Digest Authentication] or [Cleartext Authentication], proceed to step 24.

23. Select the Realm.



24. Press [Connection Test].

Access the LDAP server to check that the proper connection is established. Check authentication works according to the authentication settings.

25. Press [Exit].

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

This function does not check search conditions or the search base.

26. Press [▼Next].

27. Press [Change] for items you want to use as search conditions from the following: "Name", "E-mail Address", "Fax Number", "Company Name", and "Department Name".

You can enter an attribute as a typical search keyword. Using the entered attribute, the function searches the LDAP server's Address Book.

28. Enter the attribute you want to use when searching for e-mail addresses, and then press [OK].

The attribute value may change depending on the server environment. Check that the attribute value complies with your server environment before setting it.

You can leave items blank, but you cannot leave attributes blank when searching for e-mail addresses from the LDAP server Address Book.

29. Press [▼Next].

30. Press [Change] under "Attribute".

31. Enter the attribute you want to use when searching for e-mail addresses, and then press [OK].

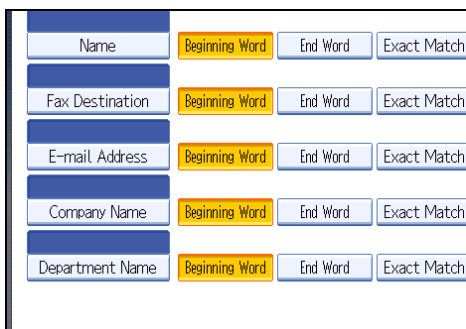
The attribute value may change depending on the server environment. Check that the attribute complies with your server environment before setting it.

32. Press [Change] under "Key Display".

33. Enter the key display, and then press [OK].

The registered "Key Display" appears as a keyword for searching LDAP.

- Without key display registration



- With key display registration

Name	Beginning Word	End Word	Exact Match
Fax Destination	Beginning Word	End Word	Exact Match
E-mail Address	Beginning Word	End Word	Exact Match
Company Name	Beginning Word	End Word	Exact Match
Department Name	Beginning Word	End Word	Exact Match
EmpLOYEENo.	Beginning Word	End Word	Exact Match

The key does not appear on the search screen unless both "Attribute" and "Key Display" are registered. Make sure you register both to use the optional search.

34. Press [OK].
35. Press [Exit].
36. Press the [User Tools / Counter] key.

Reference

- p.316 "Registering SMTP and LDAP Authentication"

Changing the LDAP server

This section describes how to change the programmed LDAP server.

1. Press the [User Tools / Counter] key.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [▼Next] twice.
5. Press [Program / Change / Delete LDAP Server].
6. Check that [Program / Change] is selected.
7. Select the LDAP server you want to change.
8. Change the settings as necessary.
9. Press [OK] after changing each item.
10. Press [Exit].
11. Press the [User Tools / Counter] key.

Deleting the LDAP server

This section describes how to delete the programmed LDAP server.

1. Press the [User Tools / Counter] key.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [▼Next] twice.
5. Press [Program / Change / Delete LDAP Server].
6. Press [Delete].
7. Select the LDAP server you want to delete.
8. Press [Yes].
9. Press [Exit].
10. Press the [User Tools / Counter] key.

Programming the Realm

This section describes how to specify the Realm settings.

Program the realm to be used for Kerberos authentication.

A realm is the network area in which Kerberos authentication is used. After confirming the network environment, specify the necessary items.

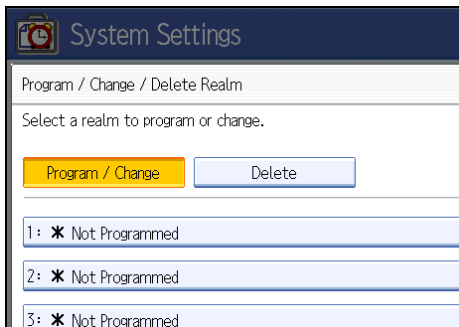
You can register up to 5 realms.

1

Programming the Realm

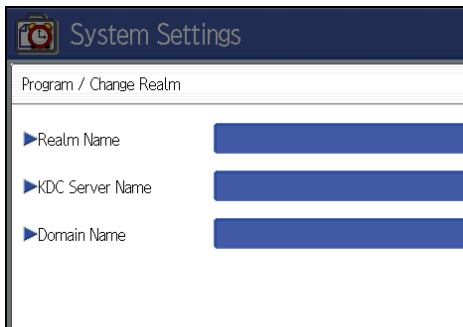
This section describes how to program the Realm.

1. Press the [User Tools / Counter] key.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [▼Next] twice.
5. Press [Program / Change / Delete Realm].
6. Check that [Program / Change] is selected.



7. Press [*Not Programmed].

8. Press [Change] under "Realm Name".



9. Enter the realm name, and then press [OK].

Enter the realm name, or host name.

You can enter a realm name using up to 64 characters.

10. Press [Change] under "KDC Server Name".

11. Enter the KDC server name, and then press [OK].

Enter the KDC server name, host name, or IPv4 address.

You can enter a KDC server name using up to 64 characters.

12. Press [Change] under "Domain Name".

13. Enter the domain name, and then press [OK].

Enter the domain name, or host name.

You can enter a domain name using up to 64 characters.

14. Press [OK].

15. Press [Exit].

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

Changing the Realm

This section describes how to change the programmed Realm.

1. Press the [User Tools / Counter] key.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [▼Next] twice.
5. Press [Program / Change / Delete Realm].
6. Check that [Program / Change] is selected.
7. Select the Realm you want to change.

8. To change the realm name, press [Change] under “Realm Name”.
9. Enter the realm name, and then press [OK].
You can enter a realm name using up to 64 characters.
10. To change the KDC server name, press [Change] under “KDC Server Name”.
11. Enter the KDC server name, and then press [OK].
You can enter a KDC server name using up to 64 characters.
12. To change the domain name, press [Change] under “Domain Name”.
13. Enter the domain name, and then press [OK].
You can enter a domain name using up to 64 characters.
14. Press [OK].
15. Press [Exit].
16. Press the [User Tools / Counter] key.

Deleting the Realm

This section describes how to delete the programmed Realm.

1. Press the [User Tools / Counter] key.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [▼Next] twice.
5. Press [Program / Change / Delete Realm].
6. Press [Delete].
7. Select the realm you want to delete.
8. Press [Yes].
9. Press [Exit].
10. Press the [User Tools / Counter] key.

System Settings on Main and Sub-machines

This section describes the System Settings on the two machines during Connect Copy.

When connect copy is in progress, the [User Tools / Counter] keys of the sub-machines remain disabled. To change the default settings, first press [Connect Copy], which is highlighted on main machine's control screen, then clear the connect copy job, and then make the required changes.

General Features

How the defaults in the General Features of copying of the main and sub-machines are used in connect copy will be explained.

Program / Change / Delete User Text

- The main machine applies the setting that has been made on it. Sub-machines also apply their own respective settings.

Panel Key Sound

- The main machine applies the setting that has been made on it. Sub-machines also apply their own respective settings.

Warm-up Beeper

- The main machine applies the setting that has been made on it. Sub-machines also apply their own respective settings.

Copy Count Display

- Settings made on the main and sub-machines do not affect the connect copy.
- The copy counter is always displayed as Up (count up).

Function Priority

- Settings made on the main and sub-machines do not affect the connect copy.
- When the Auto Reset time of the main machine has lapsed, Connect Copy will be cancelled. After that, the machine switches back to the mode selected in Function Priority upon reaching the System Reset time.

Print Priority

- Settings made on the main and sub-machines do not affect the connect copy.
- When the Auto Reset time of the main machine has lapsed, Connect Copy will be cancelled. After that, the machine switches back to the mode selected in Function Priority upon reaching the System Reset time.

Function Reset Timer

- Settings made on the main and sub-machines do not affect the connect copy.

Interleave Print

- Settings made on the main and sub-machines do not affect the connect copy.

Output: Copier

- The main machine applies the setting that has been made on it. Sub-machines also apply their own respective settings.

Output: Document Server

- The main machine applies the setting that has been made on it. Sub-machines also apply their own respective settings.

Output: Facsimile (facsimile)

- The main machine applies the setting that has been made on it. Sub-machines also apply their own respective settings.

Output: Printer

- The main machine applies the setting that has been made on it. Sub-machines also apply their own respective settings.

ADF Original Table Elevation

- The main machine applies the setting that has been made on it. Sub-machine settings do not affect connect copy.

System Status/Job List Display Time

- The main machine applies the setting that has been made on it. Sub-machines also apply their own respective settings.

1

Key Repeat

- The main machine applies the setting that has been made on it. Sub-machines also apply their own respective settings.

Z-fold Position

- The main machine applies the setting that has been made on it. Sub-machines also apply their own respective settings.
- Make the same settings on both machines.

Half Fold Position

- The main machine applies the setting that has been made on it. Sub-machines also apply their own respective settings.
- Make the same settings on both machines.

Letter Fold-out Position

- The main machine applies the setting that has been made on it. Sub-machines also apply their own respective settings.
- Make the same settings on both machines.

Letter Fold-in Position

- The main machine applies the setting that has been made on it. Sub-machines also apply their own respective settings.
- Make the same settings on both machines.

Double Parallel Fold Position

- The main machine applies the setting that has been made on it. Sub-machines also apply their own respective settings.
- Make the same settings on both machines.

Gate Fold Position

- The main machine applies the setting that has been made on it. Sub-machines also apply their own respective settings.
- Make the same settings on both machines.

Tray Paper Settings

How the defaults in the Tray Paper Settings of copying of the main and sub-machines are used in connect copy will be explained.

Paper Tray Priority: Copier

- The main machine applies the setting that has been made on it. Sub-machines also apply their own respective settings.

Paper Tray Priority: Facsimile (facsimile)

- The main machine applies the setting that has been made on it. Sub-machines also apply their own respective settings.

Paper Tray Priority: Printer

- The main machine applies the setting that has been made on it. Sub-machines also apply their own respective settings.

Tray Paper Size: Tray 2, Tray Paper Size: Tray 3

- The main machine applies the setting that has been made on it. Sub-machines also apply their own respective settings.
- Both the main and sub-machines should have the same paper tray settings. Only paper trays with the same size, orientation and paper type of paper can be used in Connect Copy mode.

Printer Bypass Paper Size

- The main machine applies the setting that has been made on it. Sub-machines also apply their own respective settings.

Paper Type: Bypass Tray

- The bypass tray can only be used with the Covers and Chapter functions.

1

Paper Type: Tray 1

- The main machine applies the setting that has been made on it. Sub-machines also apply their own respective settings.
- Paper size, orientation, and type settings that match those currently made on both the main and sub-machines can be used for connect copy. To get the most from the connect copy function, we recommend you make the same paper settings on both the main and sub-machines.

Paper Type: Tray 2, Paper Type: Tray 3

- The main machine applies the setting that has been made on it. Sub-machines also apply their own respective settings.
- Paper size, orientation, and type settings that match those currently made on both the main and sub-machines can be used for connect copy. To get the most from the connect copy function, we recommend you make the same paper settings on both the main and sub-machines.

Front Cover Sheet Tray

- The main machine applies the setting that has been made on it. Sub-machines also apply their own respective settings.

Back Cover Sheet Tray

- The main machine applies the setting that has been made on it. Sub-machines also apply their own respective settings.

Slip Sheet Tray

- The main machine applies the setting that has been made on it. Sub-machines also apply their own respective settings.

Designation Sheet 1 Tray, Designation Sheet 2 Tray

- The main machine applies the setting that has been made on it. Sub-machines also apply their own respective settings.

Timer Settings

How the defaults in the Timer Settings of copying of the main and sub-machines are used in connect copy will be explained.

Auto Off Timer

- The main machine applies the setting that has been made on it. Sub-machine settings do not affect connect copy.

Energy Saver Timer

- Settings made on the main and sub-machines do not affect the connect copy.
- In Connect Copy mode, neither machine will enter Energy Saver modes (Low Power mode, or Energy Saver mode).

Panel Off Timer

- Settings made on the main and sub-machines do not affect the connect copy.
- In Connect Copy mode, neither machine will enter Energy Saver modes (Low Power mode, or Energy Saver mode).

System Auto Reset Timer

- Settings made on the main machine do not affect connect copy. Only sub-machines can be used for interruption copying.
- When the System Reset time has lapsed, Interrupt mode on the sub-machine will be cancelled.

Copier / Document Server Auto Reset Timer

- Settings made on the main and sub-machines do not affect the connect copy.

Facsimile Auto Reset Timer (facsimile)

- Settings made on the main and sub-machines do not affect the connect copy.

Printer Auto Reset Timer

- Settings made on the main and sub-machines do not affect the connect copy.

Scanner Auto Reset Timer

- Settings made on the main and sub-machines do not affect the connect copy.

1

Set Date

- The main machine applies the setting that has been made on it. Sub-machines also apply their own respective settings.

Set Time

- The main machine applies the setting that has been made on it. Sub-machines also apply their own respective settings.

Auto Logout Timer

- Settings made on the main and sub-machines do not affect the connect copy.

Weekly Timer Code

- Settings made on the main and sub-machines do not affect the connect copy.

Weekly Timer: Monday - Sunday

- The main machine applies the setting that has been made on it. Sub-machine settings do not affect connect copy.
- In Connect Copy mode, Weekly timer settings on the sub-machine will be disabled.

Administrator Tools

How the defaults in the Administrator Tools of copying of the main and sub-machines are used in connect copy will be explained.

Address Book Management

- Settings made on the main and sub-machines do not affect the connect copy.

Address Book: Program / Change / Delete Group

- Settings made on the main and sub-machines do not affect the connect copy.

Address Book: Change Order

- Settings made on the main and sub-machines do not affect the connect copy.

Print Address Book: Destination List

- Settings made on the main and sub-machines do not affect the connect copy.

Address Book: Edit Title

- Settings made on the main and sub-machines do not affect the connect copy.

Address Book: Switch Title

- Settings made on the main and sub-machines do not affect the connect copy.

Back Up / Restore Address Book

- Settings made on the main and sub-machines do not affect the connect copy.

Data Carry-Over Setting for Address Book Auto Program

- Settings made on the main and sub-machines do not affect the connect copy.

Display / Print Counter

- Settings made on the main and sub-machines do not affect the connect copy.

Display / Clear / Print Counter per User

- Settings made on the main and sub-machines do not affect the connect copy.

User Authentication Management

- The main machine applies the setting that has been made on it. Sub-machine settings do not affect connect copy.

Enhanced Authentication Management

- The main machine applies the setting that has been made on it. Sub-machine settings do not affect connect copy.

Administrator Authentication Management

- The main machine applies the setting that has been made on it. Sub-machine settings do not affect connect copy.

Program / Change Administrator

- The main machine applies the settings that have been made on it. Sub-machines also apply the settings made on the main machine, regardless of the settings made on them.

Key Counter Management

- The main machine applies the settings that have been made on it. Sub-machines also apply the settings made on the main machine, regardless of the settings made on them.

External Charge Unit Management

- Settings made on the main and sub-machines do not affect the connect copy.

Extended Security

- Settings made on the main and sub-machines do not affect the connect copy.

Auto Delete File in Document Server

- The main machine applies the setting that has been made on it. Sub-machine settings do not affect connect copy.

Delete All Files in Document Server

- The main machine applies the setting that has been made on it. Sub-machine settings do not affect connect copy.

Program / Change / Delete LDAP Server

- Settings made on the main and sub-machines do not affect the connect copy.

LDAP Search

- Settings made on the main and sub-machines do not affect the connect copy.

AOF (Always On)

- Settings made on the main and sub-machines do not affect the connect copy.
- During Connect Copy, neither machine is turned off automatically. The power will be turned off only when you exit from Connect Copy mode.

Firmware Version

- Settings made on the main and sub-machines do not affect the connect copy.

Network Security Level

- Settings made on the main and sub-machines do not affect the connect copy.

Auto Erase Memory Setting

- Settings made on the main and sub-machines do not affect the connect copy.

Erase All Memory

- Settings made on the main and sub-machines do not affect the connect copy.

Delete All Logs

- The main machine applies the setting that has been made on it. Sub-machines also apply their own respective settings.

Transfer Log Setting

- The main machine applies the setting that has been made on it. Sub-machines also apply their own respective settings.

Data Security for Copying

- The main machine applies the setting that has been made on it. Sub-machine settings do not affect connect copy.

Print Backup: Delete All Files

- Settings made on the main and sub-machines do not affect the connect copy.

Print Backup: Compression

- Settings made on the main and sub-machines do not affect the connect copy.

1

Print Backup: Default Format

- Settings made on the main and sub-machines do not affect the connect copy.

Print Backup: Default Resolution

- Settings made on the main and sub-machines do not affect the connect copy.

2. Connecting the Machine

This chapter describes how to connect the machine to the network and specify the network settings.

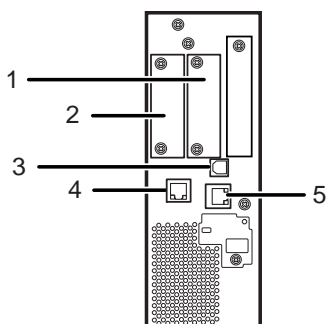
Connecting to the Interface

This section explains how to identify the machine's interface and connect the machine according to the network environment.

2

⚠ CAUTION

- A network interface cable with a ferrite core must be used for RF interference suppression.



BPV006S

1. Slot A

Install an optional interface or expansion board in this slot.

The Bluetooth interface, File Format Converter, or one of the following interface boards can be installed in this slot:

- IEEE 1284 interface board: Required if you want to connect an IEEE 1284 cable to this machine. When installed in Slot A, this board allows you to connect the machine to a computer through an IEEE 1284 cable.
- Wireless LAN interface unit: Required if you want to connect this machine to a wireless LAN. When installed in Slot A, this unit allows you to connect the machine to an IEEE 802.11 a or IEEE 802.11 b/g wireless LAN.

2. Slot B

Install the optional Copy Connector.

- Copy Connector (optional): Required if you want to connect this machine to a sub-machine in order to use the connect copy function.

3. USB 2.0 [Type B] interface

Port for connecting the USB 2.0 [Type B] interface cable.

4. Gigabit Ethernet port (optional)

Port for using the 1000BASE-T, 100BASE-TX, or 10BASE-T cable.

5. 10 Base-T, 100 Base-TX port

Port for connecting the 100BASE-TX or 10BASE-T cable.

↓ Note

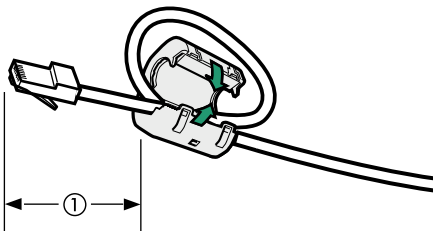
- Slot A can contain one module only: You can install only one 1284 Interface board, one Wireless LAN Interface Unit, one Bluetooth Unit, or one File Format Converter at a time in this slot.
- The Ethernet and Gigabit Ethernet port cannot be used simultaneously. If the optional Gigabit Ethernet board is installed, connect the Ethernet cable to the port on the Gigabit Ethernet board. Communication with the machine will fail if cables are connected to both ports simultaneously.

Connecting to the Ethernet Interface

This section describes how to connect an Ethernet cable to the Ethernet interface.

★ Important

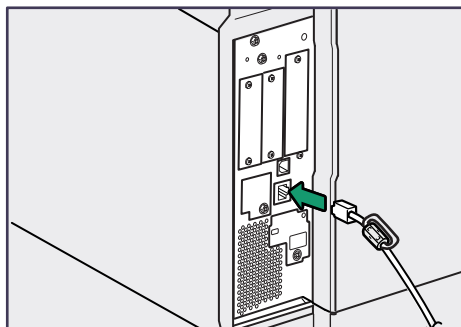
- If the main power switch is on, turn it off.
 - Use the following Ethernet cables.
 - Unshielded Twisted Pair Cable (UTP) or Shielded Twisted Pair Cable (STP) and Category type 5 or more
1. Make a loop 3 cm (1.2 inches) from the end of the Ethernet cable and attach the included ferrite core to the loops as shown.



BBM011S

2. Make sure the main power is switched off.

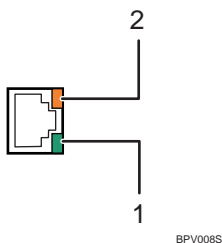
3. Connect the Ethernet interface cable to the 10BASE-T/100BASE-TX port.



BPV007S

4. Connect the other end of the Ethernet interface cable to a network connection device such as a hub.

5. Turn on the main power switch of the machine.



BPV008S

1. Indicator (green)

When 10BASE-T is operating, the LED is lit green. When 100BASE-TX is operating it is turned off.

2. Indicator (yellow)

When 100BASE-TX is operating, the LED is lit yellow. When 10BASE-T is operating, it is turned off.

↓ Note

- For details about how to turn on the main power switch, see "Turning On the Power", About This Machine.
- For details about installing the printer driver, see "Preparing the Machine", Printer Reference.

Connecting to the Gigabit Ethernet Interface

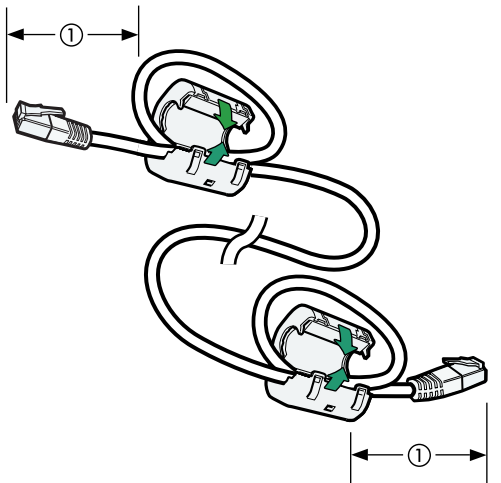
This section describes how to connect the Ethernet interface cable to the Gigabit Ethernet port.

★ Important

- If the main power switch is on, turn it off.
- Use the following Ethernet cables.

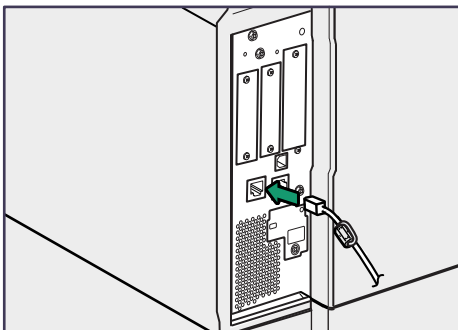
- When using 100BASE-TX/10BASE-T:
Unshielded Twisted Pair Cable (UTP) or Shielded Twisted Pair Cable (STP) and Category type 5 or more
- When using 1000BASE-T:
Unshielded Twisted Pair Cable (UTP) or Shielded Twisted Pair Cable (STP) and Category type 5e or more

1. Make loops 3 cm (1.2 inches) from the end of each Ethernet cable and attach included ferrite cores to each loop as shown.



BAX007S

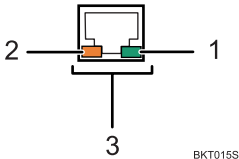
2. Make sure the main power is switched off.
3. Connect the Ethernet interface cable to the Gigabit Ethernet port.



BPV010S

4. Connect the other end of the Ethernet interface cable to a network connection device such as a hub.

5. Turn on the main power switch of the machine.



1. Indicator (green)

When 10BASE-T is operating, the LED is lit green. When 100BASE-TX is operating it is turned off.

2. Indicator (yellow)

When 100BASE-TX is operating, the LED is lit yellow. When 10BASE-T is operating, it is turned off.

3. Indicators (both green and yellow)

When 1000BASE-T is operating, both LED are lit.

↓ Note

- For details about how to turn on the main power switch, see "Turning On the Power", About This Machine.
- For details about installing the printer driver, see "Preparing the Machine", Printer Reference.

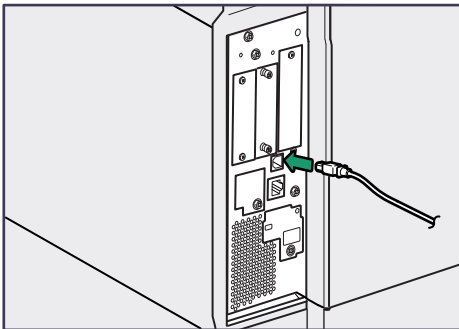
Connecting to the USB (Type B) Interface

This section describes how to connect the USB2.0 (Type B) interface cable to the USB2.0 port.

⚠ CAUTION

- Properly shielded and grounded cables and connectors must be used for connections to a host computer (and/or peripheral) in order to meet emission limits.

1. Connect the USB2.0 (Type B) interface cable to the USB2.0 port.



2. Connect the other end to the USB2.0 port on the host computer.

↓ Note

- This machine does not come with a USB interface cable. Make sure you purchase the appropriate cable for the machine and your computer.
- The USB2.0 interface board is supported by Windows 2000/XP/Vista, Windows Server 2003/2003 R2/2008, Mac OS X 10.3.3 or higher.
 - For Mac OS:
To use Macintosh, the machine must be equipped with the optional PostScript 3 unit. When used with Mac OS X 10.3.3 or higher, a transfer speed of USB2.0 is supported.
- For details about installing the printer driver, see "Preparing the Machine", Printer Reference.

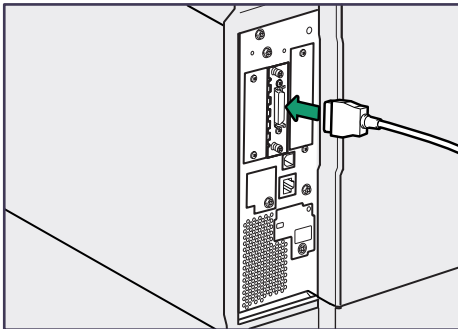
Connecting to the IEEE 1284 Interface

This section describes how to connect the IEEE 1284 interface cable to the IEEE 1284 interface board.

⚠ CAUTION

- Properly shielded and grounded cables and connectors must be used for connections to a host computer (and/or peripheral) in order to meet emission limits.

- 1. Make sure the main power switch on the machine is off.**
- 2. Turn off the main power switch of the host computer.**
- 3. Connect the IEEE 1284 interface cable to the IEEE 1284 port.**



You might have to use a conversion adapter to connect the cable to the interface. For details about acquiring a conversion adapter, consult your sales or service representative.

- 4. Connect the other end of the cable into the interface connector on the host computer.**
Check the shape of the connector to the computer. Connect the cable firmly.
- 5. Turn on the main power switch of the machine.**

6. Turn on the host computer.

When using Windows 2000/XP/Vista and Windows Server 2003/2003 R2/2008, a printer driver installation screen might appear when the computer is turned on. If this happens, click [Cancel] on the screen.

↓ Note

- For details about how to turn on the main power switch, see "Turning On the Power", About This Machine.
- For details about installing the printer driver, see "Preparing the Machine", Printer Reference.

2

Connecting to the Wireless LAN Interface

This section describes how to connect to the wireless LAN interface.

↓ Note

- Check the machine's IPv4 address and subnet mask, or the IPv6 address settings.
- For details about how to set the IPv4 address and subnet mask from the control panel of the machine, see "Interface Settings".
- Before using this machine with a wireless LAN interface, you must select [Wireless LAN] in [LAN Type].

📖 Reference

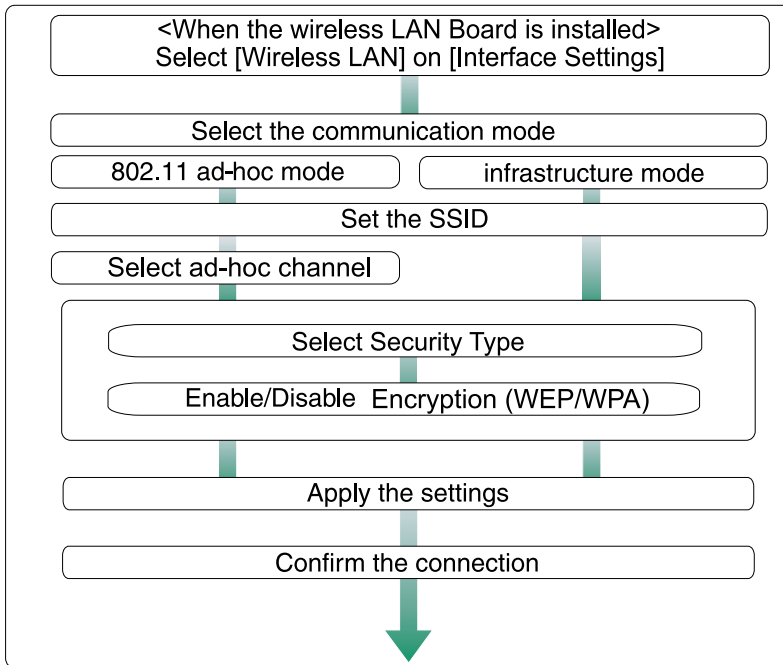
- p.34 "Interface Settings"

Setup Procedure

This section describes how to setup wireless LAN interface.

Set up wireless LAN according to the following procedure:

■ Wireless LAN setup procedure



BBM002S

↓ Note

- Select [802.11 Ad-hoc Mode] when connecting Windows XP as a wireless LAN client using Windows XP standard driver or utilities, or when not using the infrastructure mode.
- When [802.11 Ad-hoc Mode] is selected in Communication mode, select the channel for [Ad-hoc Channel]. Set a channel that matches the type of wireless LAN being used. For details about setting the Ad-hoc Channel, see "Interface Settings".
- You can specify either "WEP" or "WPA" to the Security Method.
- Specify "WPA", when [Communication Mode] is set to [Infrastructure Mode].
- If you select the [WPA] option for Security Method, select one of the following: [WPA-PSK], [WPA], [WPA2-PSK], or [WPA2]. If you select [WPA-PSK] or [WPA2-PSK], enter your PSK. If you select [WPA] or [WPA2], authentication settings and certificate installation settings are required. For details about setting methods, see "Configuring IEEE 802.1X".
- For details about how to specify wireless LAN settings from the control panel on the machine, see "Interface Settings".

📖 Reference

- p.34 "Interface Settings"
- p.341 "Configuring IEEE 802.1X"

Checking the Signal

This section describes how to check the machine's radio wave status.

When using in infrastructure mode, you can check the machine's radio wave status using the control panel.

1. Press the [User Tools/Counter] key.
2. Press [System Settings].
3. Press [Interface Settings].
4. Press [Wireless LAN].
5. Press [Wireless LAN Signal].

The machine's radio wave status appears.

6. After checking radio wave status, press [Exit].
7. Press the [User Tools/Counter] key.

Network Settings Required to Use the Printer/ LAN-Fax

This section lists the network settings required for using the printer or LAN-Fax function.

★ Important

- These settings should be made by the system administrator, or with the advice of the system administrator.

Ethernet

This section lists the settings required for using the printer or LAN-Fax function with an Ethernet connection.

For details about how to specify the settings, see "Interface Settings".

Menu	User Tool	Setting Requirements
Interface Settings/Network	Machine IPv4 Address	Necessary
Interface Settings/Network	IPv4 Gateway Address	As required
Interface Settings/Network	Machine IPv6 Address	As required
Interface Settings/Network	IPv6 Gateway Address	As required
Interface Settings/Network	IPv6 Stateless Address Autoconfiguration	As required
Interface Settings/Network	DNS Configuration	As required
Interface Settings/Network	DDNS Configuration	As required
Interface Settings/Network	IPsec	As required
Interface Settings/Network	Domain Name	As required
Interface Settings/Network	WINS Configuration	As required
Interface Settings/Network	Effective Protocol	Necessary
Interface Settings/Network	NCP Delivery Protocol	As required
Interface Settings/Network	NW Frame Type	As required
Interface Settings/Network	SMB Computer Name	As required

Menu	User Tool	Setting Requirements
Interface Settings/Network	SMB Work Group	As required
Interface Settings/Network	Ethernet Speed	As required
Interface Settings/Network	IEEE 802.1X Authentication for Ethernet	As required
Interface Settings/Network	LAN Type	Necessary
Interface Settings/Network	Permit SNMPv3 Communication	As required
Interface Settings/Network	Permit SSL / TLS Communication	As required
Interface Settings/Network	Host Name	As required
Interface Settings/Network	Machine Name	As required

↓ Note

- For the Effective Protocol setting, check that the protocol you want to use is set to [Active].
- [LAN Type] is displayed when the wireless LAN board is installed. If Ethernet and wireless LAN are both connected, the selected interface has priority.

📖 Reference

- p.34 "Interface Settings"

Wireless LAN

This section lists the settings required for using the printer or LAN-Fax function with a wireless LAN connection.

For details about how to specify the settings, see "Interface Settings".

Menu	User Tool	Setting Requirements
Interface Settings/Network	Machine IPv4 Address	Necessary
Interface Settings/Network	IPv4 Gateway Address	As required
Interface Settings/Network	Machine IPv6 Address	As required
Interface Settings/Network	IPv6 Gateway Address	As required
Interface Settings/Network	IPv6 Stateless Address Autoconfiguration	As required

Menu	User Tool	Setting Requirements
Interface Settings/Network	DNS Configuration	As required
Interface Settings/Network	DDNS Configuration	As required
Interface Settings/Network	IPsec	As required
Interface Settings/Network	Domain Name	As required
Interface Settings/Network	WINS Configuration	As required
Interface Settings/Network	Effective Protocol	Necessary
Interface Settings/Network	NCP Delivery Protocol	As required
Interface Settings/Network	NW Frame Type	As required
Interface Settings/Network	SMB Computer Name	As required
Interface Settings/Network	SMB Work Group	As required
Interface Settings/Network	LAN Type	Necessary
Interface Settings/Network	Permit SNMPv3 Communication	As required
Interface Settings/Network	Permit SSL / TLS Communication	As required
Interface Settings/Network	Host Name	As required
Interface Settings/Network	Machine Name	As required
Interface Settings/Wireless LAN	Communication Mode	Necessary
Interface Settings/Wireless LAN	Ad-hoc Channel	As required
Interface Settings/Wireless LAN	SSID Setting	As required
Interface Settings/Wireless LAN	Security Method	As required

↓ Note

- For the Effective Protocol setting, check that the protocol you want to use is set to [Active].
- [Wireless LAN] and [LAN Type] are displayed when the wireless LAN interface board is installed. If both Ethernet and wireless LAN are connected, the selected interface takes precedence.

📖 Reference

- p.34 "Interface Settings"

Network Settings Required to Use Internet Fax

This section lists the network settings required for using Internet Fax.

★ Important

- These settings should be made by the system administrator, or with the advice of the system administrator.

2

Ethernet

This section lists the settings required for using Internet Fax with an Ethernet connection.

For details about how to specify the settings, see "Interface Settings" and "File Transfer".

Menu	User Tool	Setting Requirements
Interface Settings/Network	Machine IPv4 Address	Necessary
Interface Settings/Network	IPv4 Gateway Address	Necessary
Interface Settings/Network	Machine IPv6 Address	As required
Interface Settings/Network	IPv6 Gateway Address	As required
Interface Settings/Network	IPv6 Stateless Address Autoconfiguration	As required
Interface Settings/Network	DNS Configuration	As required
Interface Settings/Network	DDNS Configuration	As required
Interface Settings/Network	IPsec	As required
Interface Settings/Network	Domain Name	As required
Interface Settings/Network	WINS Configuration	As required
Interface Settings/Network	Effective Protocol	Necessary
Interface Settings/Network	Ethernet Speed	As required
Interface Settings/Network	IEEE 802.1X Authentication for Ethernet	As required
Interface Settings/Network	LAN Type	Necessary
Interface Settings/Network	Permit SNMPv3 Communication	As required

Menu	User Tool	Setting Requirements
Interface Settings/Network	Permit SSL / TLS Communication	As required
Interface Settings/Network	Host Name	As required
File Transfer	SMTP Server	Necessary
File Transfer	SMTP Authentication	As required
File Transfer	POP before SMTP	As required
File Transfer	Reception Protocol	As required
File Transfer	POP3 / IMAP4 Settings	As required
File Transfer	Administrator's E-mail Address	As required
File Transfer	E-mail Communication Port	Necessary
File Transfer	E-mail Reception Interval	As required
File Transfer	Max. Reception E-mail Size	As required
File Transfer	E-mail Storage in Server	As required
File Transfer	Program / Change / Delete E-mail Message	As required
File Transfer	Fax E-mail Account	Necessary

↓ Note

- For the Effective Protocol setting, check that the protocol you want to use is set to [Active].
- [LAN Type] is displayed when the wireless LAN interface board is installed. If both Ethernet and wireless LAN are connected, the selected interface takes precedence.
- SMTP Server and Fax E-mail Account must be specified in order to send Internet Fax.
- When POP before SMTP is set to [On], also make settings for Reception Protocol and POP3 / IMAP4 Settings.
- When SMTP Authentication is set to [On], also make setting for Administrator's E-mail Address.
- POP3 / IMAP4 Settings, E-mail Communication Port, and Fax E-mail Account must be specified in order to receive Internet Fax.
- When setting POP before SMTP to [On], check POP3 port number in E-mail Communication Port.

📖 Reference

- p.34 "Interface Settings"

- p.42 "File Transfer"

Wireless LAN

This section lists the settings required for using Internet Fax with a wireless LAN connection.

For details about how to specify the settings, see "Interface Settings" and "File Transfer".

2

Menu	User Tool	Setting Requirements
Interface Settings/Network	Machine IPv4 Address	Necessary
Interface Settings/Network	IPv4 Gateway Address	Necessary
Interface Settings/Network	Machine IPv6 Address	As required
Interface Settings/Network	IPv6 gateway Address	As required
Interface Settings/Network	IPv6 Stateless Address Autoconfiguration	As required
Interface Settings/Network	DNS Configuration	As required
Interface Settings/Network	DDNS Configuration	As required
Interface Settings/Network	IPsec	As required
Interface Settings/Network	Domain Name	As required
Interface Settings/Network	WINS Configuration	As required
Interface Settings/Network	Effective Protocol	Necessary
Interface Settings/Network	LAN Type	Necessary
Interface Settings/Network	Permit SNMPv3 Communication	As required
Interface Settings/Network	Permit SSL / TLS Communication	As required
Interface Settings/Network	Host Name	As required
Interface Settings/Wireless LAN	Communication Mode	Necessary
Interface Settings/Wireless LAN	SSID Setting	As required
Interface Settings/Wireless LAN	Ad-hoc Channel	As required
Interface Settings/Wireless LAN	Security Method	As required

Menu	User Tool	Setting Requirements
File Transfer	SMTP Server	Necessary
File Transfer	SMTP Authentication	As required
File Transfer	POP before SMTP	As required
File Transfer	Reception Protocol	As required
File Transfer	POP3 / IMAP4 Settings	As required
File Transfer	Administrator's E-mail Address	As required
File Transfer	E-mail Communication Port	Necessary
File Transfer	E-mail Reception Interval	As required
File Transfer	Max. Reception E-mail Size	As required
File Transfer	E-mail Storage in Server	As required
File Transfer	Program / Change / Delete E-mail Message	As required
File Transfer	Fax E-mail Account	Necessary

↓ Note

- For the Effective Protocol setting, check that the protocol you want to use is set to [Active].
- [Wireless LAN] and [LAN Type] are displayed when the wireless LAN interface board is installed. If both Ethernet and wireless LAN are connected, the selected interface takes precedence.
- SMTP Server and Fax E-mail Account must be specified in order to send Internet Fax.
- When POP before SMTP is set to [On], you must also make settings for Reception Protocol and POP3 / IMAP4 Settings.
- When SMTP Authentication is set to [On], you must also make settings for Administrator's E-mail Address.
- POP3 / IMAP4 Settings, E-mail Communication Port, and Fax E-mail Account must be specified in order to receive Internet Fax.
- When setting POP before SMTP to [On], check POP3 port number in E-mail Communication Port.

📖 Reference

- p.34 "Interface Settings"
- p.42 "File Transfer"

Network Settings Required to Use E-mail Function

This section lists the network settings required for sending e-mail.

★ Important

- These settings should be made by the system administrator, or with the advice of the system administrator.

2

Ethernet

This section lists the settings required for sending e-mail with an Ethernet connection.

For details about how to specify the settings, see "Interface Settings" and "File Transfer".

Menu	User Tool	Setting Requirements
Interface Settings/Network	Machine IPv4 Address	Necessary
Interface Settings/Network	IPv4 Gateway Address	Necessary
Interface Settings/Network	Machine IPv6 Address	As required
Interface Settings/Network	IPv6 Gateway Address	As required
Interface Settings/Network	IPv6 Stateless Address Autoconfiguration	As required
Interface Settings/Network	DNS Configuration	As required
Interface Settings/Network	DDNS Configuration	As required
Interface Settings/Network	IPsec	As required
Interface Settings/Network	Domain Name	As required
Interface Settings/Network	WINS Configuration	As required
Interface Settings/Network	Effective Protocol	Necessary
Interface Settings/Network	Ethernet Speed	As required
Interface Settings/Network	IEEE 802.1X Authentication for Ethernet	As required
Interface Settings/Network	LAN Type	Necessary

Menu	User Tool	Setting Requirements
Interface Settings/Network	Permit SNMPv3 Communication	As required
Interface Settings/Network	Permit SSL / TLS Communication	As required
Interface Settings/Network	Host Name	As required
File Transfer	SMTP Server	Necessary
File Transfer	SMTP Authentication	As required
File Transfer	POP before SMTP	As required
File Transfer	Reception Protocol	As required
File Transfer	POP3 / IMAP4 Settings	As required
File Transfer	Administrator's E-mail Address	As required
File Transfer	E-mail Communication Port	As required
File Transfer	Program / Change / Delete E-mail Message	As required
File Transfer	Scanner Resend Interval Time	As required
File Transfer	Number of Scanner Resends	As required

↓ Note

- For the Effective Protocol setting, check that the protocol you want to use is set to [Active].
- [LAN Type] is displayed when the wireless LAN interface board is installed. If both Ethernet and wireless LAN are connected, the selected interface takes precedence.
- When POP before SMTP is set to [On], also make settings for Reception Protocol and POP3 / IMAP4 Settings.
- When setting POP before SMTP to [On], check POP3 port number in E-mail Communication Port.

📖 Reference

- p.34 "Interface Settings"
- p.42 "File Transfer"

Wireless LAN

This section lists the settings required for sending e-mail with a Wireless LAN connection.

For details about how to specify the settings, see "Interface Settings" and "File Transfer".

Menu	User Tool	Setting Requirements
Interface Settings/Network	Machine IPv4 Address	Necessary
Interface Settings/Network	IPv4 Gateway Address	Necessary
Interface Settings/Network	Machine IPv6 Address	As required
Interface Settings/Network	IPv6 Gateway Address	As required
Interface Settings/Network	IPv6 Stateless Address Autoconfiguration	As required
Interface Settings/Network	DNS Configuration	As required
Interface Settings/Network	DDNS Configuration	As required
Interface Settings/Network	IPsec	As required
Interface Settings/Network	Domain Name	As required
Interface Settings/Network	WINS Configuration	As required
Interface Settings/Network	Effective Protocol	Necessary
Interface Settings/Network	LAN Type	Necessary
Interface Settings/Network	Permit SNMPv3 Communication	As required
Interface Settings/Network	Permit SSL / TLS Communication	As required
Interface Settings/Network	Host Name	As required
Interface Settings/Wireless LAN	Communication Mode	Necessary
Interface Settings/Wireless LAN	SSID Setting	As required
Interface Settings/Wireless LAN	Ad-hoc Channel	As required
Interface Settings/Wireless LAN	Security Method	As required
File Transfer	SMTP Server	Necessary
File Transfer	SMTP Authentication	As required
File Transfer	POP before SMTP	As required
File Transfer	Reception Protocol	As required

Menu	User Tool	Setting Requirements
File Transfer	POP3 / IMAP4 Settings	As required
File Transfer	Administrator's E-mail Address	As required
File Transfer	E-mail Communication Port	As required
File Transfer	Program / Change / Delete E-mail Message	As required
File Transfer	Scanner Resend Interval Time	As required
File Transfer	Number of Scanner Resends	As required

↓ Note

- For the Effective Protocol setting, check that the protocol you want to use is set to [Active].
- [Wireless LAN] and [LAN Type] are displayed when the wireless LAN interface board is installed. If both Ethernet and wireless LAN are connected, the selected interface takes precedence.
- When POP before SMTP is set to [On], you must also make settings for Reception Protocol and POP3 / IMAP4 Settings.
- When setting POP before SMTP to [On], check POP3 port number in E-mail Communication Port.

📖 Reference

- p.34 "Interface Settings"
- p.42 "File Transfer"

Network Settings Required to Use Scan to Folder Function

This section lists the network settings required for sending files.

★ Important

- These settings should be made by the system administrator, or with the advice of the system administrator.

2

Ethernet

This section lists the settings required for sending files with an Ethernet connection.

For details about how to specify the settings, see "Interface Settings" and "File Transfer".

Menu	User Tool	Setting Requirements
Interface Settings/Network	Machine IPv4 Address	Necessary
Interface Settings/Network	IPv4 Gateway Address	Necessary
Interface Settings/Network	DNS Configuration	As required
Interface Settings/Network	DDNS Configuration	As required
Interface Settings/Network	IPsec	As required
Interface Settings/Network	Domain Name	As required
Interface Settings/Network	WINS Configuration	As required
Interface Settings/Network	Effective Protocol	Necessary
Interface Settings/Network	Ethernet Speed	As required
Interface Settings/Network	IEEE 802.1X Authentication for Ethernet	As required
Interface Settings/Network	LAN Type	Necessary
Interface Settings/Network	Permit SNMPv3 Communication	As required
Interface Settings/Network	Permit SSL / TLS Communication	As required
Interface Settings/Network	Host Name	As required

Menu	User Tool	Setting Requirements
File Transfer	Default User Name / Password (Send)	As required
File Transfer	Scanner Resend Interval Time	As required
File Transfer	Number of Scanner Resends	As required

↓ Note

- For the Effective Protocol setting, check that the protocol you want to use is set to [Active].
- [LAN Type] is displayed when the wireless LAN interface board is installed. If both Ethernet and wireless LAN are connected, the selected interface takes precedence.

📖 Reference

- p.34 "Interface Settings"
- p.42 "File Transfer"

Wireless LAN

This section lists the settings required for sending files with a Wireless LAN connection.

For details about how to specify the settings, see "Interface Settings" and "File Transfer".

Menu	User Tool	Setting Requirements
Interface Settings/Network	Machine IPv4 Address	Necessary
Interface Settings/Network	IPv4 Gateway Address	Necessary
Interface Settings/Network	DNS Configuration	As required
Interface Settings/Network	DDNS Configuration	As required
Interface Settings/Network	IPsec	As required
Interface Settings/Network	Domain Name	As required
Interface Settings/Network	WINS Configuration	As required
Interface Settings/Network	Effective Protocol	Necessary
Interface Settings/Network	LAN Type	Necessary
Interface Settings/Network	Permit SNMPv3 Communication	As required

Menu	User Tool	Setting Requirements
Interface Settings/Network	Permit SSL / TLS Communication	As required
Interface Settings/Network	Host Name	As required
Interface Settings/Wireless LAN	Communication Mode	Necessary
Interface Settings/Wireless LAN	SSID Setting	As required
Interface Settings/Wireless LAN	Ad-hoc Channel	As required
Interface Settings/Wireless LAN	Security Method	As required
File Transfer	Default User Name / Password (Send)	As required
File Transfer	Scanner Resend Interval Time	As required
File Transfer	Number of Scanner Resends	As required

↓ Note

- For the Effective Protocol setting, check that the protocol you want to use is set to [Active].
- [Wireless LAN] and [LAN Type] are displayed when the wireless LAN interface board is installed. If both Ethernet and wireless LAN are connected, the selected interface takes precedence.

📖 Reference

- p.34 "Interface Settings"
- p.42 "File Transfer"

Network Settings Required to Use the Network Delivery Scanner

This section lists the network settings required for delivering data to the network.

★ Important

- These settings should be made by the system administrator, or with the advice of the system administrator.

Ethernet

This section lists the settings required for delivering data to the network with an Ethernet connection.

For details about how to specify the settings, see "Interface Settings" and "File Transfer".

Menu	User Tool	Setting Requirements
Interface Settings/Network	Machine IPv4 Address	Necessary
Interface Settings/Network	IPv4 Gateway Address	As required
Interface Settings/Network	DNS Configuration	As required
Interface Settings/Network	DDNS Configuration	As required
Interface Settings/Network	IPsec	As required
Interface Settings/Network	Domain Name	As required
Interface Settings/Network	WINS Configuration	As required
Interface Settings/Network	Effective Protocol	Necessary
Interface Settings/Network	Ethernet Speed	As required
Interface Settings/Network	IEEE 802.1X Authentication for Ethernet	As required
Interface Settings/Network	LAN Type	Necessary
Interface Settings/Network	Permit SNMPv3 Communication	As required
Interface Settings/Network	Permit SSL / TLS Communication	As required
Interface Settings/Network	Host Name	As required

Menu	User Tool	Setting Requirements
File Transfer	Delivery Option	Necessary
File Transfer	Fax RX File Transmission	As required
File Transfer	Scanner Resend Interval Time	As required
File Transfer	Number of Scanner Resends	As required

↓ Note

- For the Effective Protocol setting, check that the protocol you want to use is set to [Active].
- [LAN Type] is displayed when the wireless LAN interface board is installed. If both Ethernet and wireless LAN are connected, the selected interface takes precedence.
- If Delivery Option is set to [On], check that IPv4 Address is specified.

📖 Reference

- p.34 "Interface Settings"
- p.42 "File Transfer"

Wireless LAN

This section lists the settings required for delivering data to the network with a wireless LAN connection. For details about how to specify the settings, see "Interface Settings" and "File Transfer".

Menu	User Tool	Setting Requirements
Interface Settings/Network	Machine IPv4 Address	Necessary
Interface Settings/Network	IPv4 Gateway Address	As required
Interface Settings/Network	DNS Configuration	As required
Interface Settings/Network	DDNS Configuration	As required
Interface Settings/Network	IPsec	As required
Interface Settings/Network	Domain Name	As required
Interface Settings/Network	WINS Configuration	As required
Interface Settings/Network	Effective Protocol	Necessary
Interface Settings/Network	LAN Type	Necessary

Menu	User Tool	Setting Requirements
Interface Settings/Network	Permit SNMPv3 Communication	As required
Interface Settings/Network	Permit SSL / TLS Communication	As required
Interface Settings/Network	Host Name	As required
Interface Settings/Wireless LAN	Communication Mode	Necessary
Interface Settings/Wireless LAN	SSID Setting	As required
Interface Settings/Wireless LAN	Ad-hoc Channel	As required
Interface Settings/Wireless LAN	Security Method	As required
File Transfer	Delivery Option	Necessary
File Transfer	Fax RX File Transmission	As required
File Transfer	Scanner Resend Interval Time	As required
File Transfer	Number of Scanner Resends	As required

↓ Note

- For the Effective Protocol setting, check that the protocol you want to use is set to [Active].
- [Wireless LAN] and [LAN Type] are displayed when the wireless LAN interface board is installed. When both Ethernet and wireless LAN are connected, the selected interface takes precedence.
- If Delivery Option is set to [On], check that IPv4 Address is specified.

📖 Reference

- p.34 "Interface Settings"
- p.42 "File Transfer"

Network Settings Required to Use WSD Scanner

This section lists the network settings required for using WSD Scanner function.

★ Important

- These settings should be made by the system administrator, or with the advice of the system administrator.

2

Ethernet

This section lists the settings required for using WSD Scanner function with an Ethernet connection.

For details about how to specify the settings, see "Interface Settings".

Menu	User Tool	Setting Requirements
Interface Settings/Network	Machine IPv4 Address	Necessary
Interface Settings/Network	IPv4 Gateway Address	As required
Interface Settings/Network	DNS Configuration	As required
Interface Settings/Network	DDNS Configuration	As required
Interface Settings/Network	IPsec	As required
Interface Settings/Network	Domain Name	As required
Interface Settings/Network	WINS Configuration	As required
Interface Settings/Network	Effective Protocol	Necessary
Interface Settings/Network	NCP Delivery Protocol	As required
Interface Settings/Network	NW Frame Type	As required
Interface Settings/Network	SMB Computer Name	As required
Interface Settings/Network	SMB Work Group	As required
Interface Settings/Network	Ethernet Speed	As required
Interface Settings/Network	IEEE 802.1X Authentication for Ethernet	As required
Interface Settings/Network	LAN Type	Necessary
Interface Settings/Network	Permit SNMPv3 Communication	As required

Menu	User Tool	Setting Requirements
Interface Settings/Network	Permit SSL / TLS Communication	As required
Interface Settings/Network	Host Name	As required
Interface Settings/Network	Machine Name	As required

↓ Note

- For the Effective Protocol setting, check that the protocol you want to use is set to [Active].
- [LAN Type] is displayed when the wireless LAN board is installed. If Ethernet and wireless LAN are both connected, the selected interface has priority.

📖 Reference

- p.34 "Interface Settings"

Wireless LAN

This section lists the settings required for using WSD Scanner function with a wireless LAN connection.

For details about how to specify the settings, see "Interface Settings".

Menu	User Tool	Setting Requirements
Interface Settings/Network	Machine IPv4 Address	Necessary
Interface Settings/Network	IPv4 Gateway Address	As required
Interface Settings/Network	DNS Configuration	As required
Interface Settings/Network	DDNS Configuration	As required
Interface Settings/Network	IPsec	As required
Interface Settings/Network	Domain Name	As required
Interface Settings/Network	WINS Configuration	As required
Interface Settings/Network	Effective Protocol	Necessary
Interface Settings/Network	NCP Delivery Protocol	As required
Interface Settings/Network	NW Frame Type	As required
Interface Settings/Network	SMB Computer Name	As required

Menu	User Tool	Setting Requirements
Interface Settings/Network	SMB Work Group	As required
Interface Settings/Network	LAN Type	Necessary
Interface Settings/Network	Permit SNMPv3 Communication	As required
Interface Settings/Network	Permit SSL / TLS Communication	As required
Interface Settings/Network	Host Name	As required
Interface Settings/Network	Machine Name	As required
Interface Settings/Wireless LAN	Communication Mode	Necessary
Interface Settings/Wireless LAN	Ad-hoc Channel	As required
Interface Settings/Wireless LAN	SSID Setting	As required
Interface Settings/Wireless LAN	Security Method	As required

↓ Note

- For the Effective Protocol setting, check that the protocol you want to use is set to [Active].
- [Wireless LAN] and [LAN Type] are displayed when the wireless LAN interface board is installed. If both Ethernet and wireless LAN are connected, the selected interface takes precedence.

📖 Reference

- p.34 "Interface Settings"

Network Settings Required to Use Network TWAIN Scanner

This section lists the network settings required for using the TWAIN Scanner under the network environment.

★ Important

- These settings should be made by the system administrator, or with the advice of the system administrator.

Ethernet

This section lists the settings required for using the network TWAIN Scanner with an Ethernet connection.

For details about how to specify the settings, see "Interface Settings".

Menu	User Tool	Setting Requirements
Interface Settings/Network	Machine IPv4 Address	Necessary
Interface Settings/Network	DNS Configuration	As required
Interface Settings/Network	DDNS Configuration	As required
Interface Settings/Network	IPsec	As required
Interface Settings/Network	Domain Name	As required
Interface Settings/Network	WINS Configuration	As required
Interface Settings/Network	Effective Protocol	Necessary
Interface Settings/Network	Ethernet Speed	As required
Interface Settings/Network	IEEE 802.1X Authentication for Ethernet	As required
Interface Settings/Network	LAN Type	Necessary
Interface Settings/Network	Permit SNMPv3 Communication	As required
Interface Settings/Network	Permit SSL / TLS Communication	As required
Interface Settings/Network	Host Name	As required

Note

- For the Effective Protocol setting, check that the protocol you want to use is set to [Active].
- [LAN Type] is displayed when the wireless LAN interface board is installed.
- When both Ethernet and wireless LAN are connected, the selected interface takes precedence.

Reference

- p.34 "Interface Settings"

Wireless LAN

This section lists the settings required for using the network TWAIN Scanner with a wireless LAN connection. For details about how to specify the settings, see "Interface Settings".

Menu	User Tool	Setting Requirements
Interface Settings/Network	Machine IPv4 Address	Necessary
Interface Settings/Network	IPv4 Gateway Address	As required
Interface Settings/Network	DNS Configuration	As required
Interface Settings/Network	DDNS Configuration	As required
Interface Settings/Network	IPsec	As required
Interface Settings/Network	Domain Name	As required
Interface Settings/Network	WINS Configuration	As required
Interface Settings/Network	Effective Protocol	Necessary
Interface Settings/Network	LAN Type	Necessary
Interface Settings/Network	Permit SNMPv3 Communication	As required
Interface Settings/Network	Permit SSL / TLS Communication	As required
Interface Settings/Network	Host Name	As required
Interface Settings/Wireless LAN	Communication Mode	Necessary
Interface Settings/Wireless LAN	SSID Setting	As required
Interface Settings/Wireless LAN	Ad-hoc Channel	As required
Interface Settings/Wireless LAN	Security Method	As required

 **Note**

- For the Effective Protocol setting, check that the protocol you want to use is set to [Active].
- [Wireless LAN] and [LAN Type] are displayed when the wireless LAN interface board is installed.
When both Ethernet and wireless LAN are connected, the selected interface takes precedence.

 **Reference**

- p.34 "Interface Settings"

Network Settings Required to Use Document Server

This section lists the settings required for using the Document Server function under the network environment.

★ Important

- These settings should be made by the system administrator, or with the advice of the system administrator.

2

Ethernet

This section lists the settings required for using the Document Server function with an Ethernet connection.

For details about how to specify the settings, see "Interface Settings".

Menu	User Tool	Setting Requirements
Interface Settings/Network	Machine IPv4 Address	Necessary
Interface Settings/Network	IPv4 Gateway Address	As required
Interface Settings/Network	Machine IPv6 Address	As required
Interface Settings/Network	IPv6 Gateway Address	As required
Interface Settings/Network	IPv6 Stateless Address Autoconfiguration	As required
Interface Settings/Network	DNS Configuration	As required
Interface Settings/Network	DDNS Configuration	As required
Interface Settings/Network	IPsec	As required
Interface Settings/Network	Domain Name	As required
Interface Settings/Network	WINS Configuration	As required
Interface Settings/Network	Effective Protocol	Necessary
Interface Settings/Network	Ethernet Speed	As required
Interface Settings/Network	IEEE 802.1X Authentication for Ethernet	As required
Interface Settings/Network	LAN Type	Necessary

Menu	User Tool	Setting Requirements
Interface Settings/Network	Permit SNMPv3 Communication	As required
Interface Settings/Network	Permit SSL / TLS Communication	As required
Interface Settings/Network	Host Name	As required

↓ Note

- For the Effective Protocol setting, check that the protocol you want to use is set to [Active].
- [LAN Type] is displayed when the wireless LAN interface board is installed.
- When both Ethernet and wireless LAN are connected, the selected interface takes precedence.

📖 Reference

- p.34 "Interface Settings"

Wireless LAN

This section lists the settings required for using the Document Server function with a wireless LAN connection. For details about how to specify the settings, see "Interface Settings".

Menu	User Tool	Setting Requirements
Interface Settings/Network	Machine IPv4 Address	Necessary
Interface Settings/Network	IPv4 Gateway Address	As required
Interface Settings/Network	Machine IPv6 Address	As required
Interface Settings/Network	IPv6 Gateway Address	As required
Interface Settings/Network	IPv6 Stateless Autoconfiguration	As required
Interface Settings/Network	DNS Configuration	As required
Interface Settings/Network	DDNS Configuration	As required
Interface Settings/Network	IPsec	As required
Interface Settings/Network	Domain Name	As required
Interface Settings/Network	WINS Configuration	As required
Interface Settings/Network	Effective Protocol	Necessary

Menu	User Tool	Setting Requirements
Interface Settings/Network	LAN Type	Necessary
Interface Settings/Network	Permit SNMPv3 Communication	As required
Interface Settings/Network	Permit SSL / TLS Communication	As required
Interface Settings/Network	Host Name	As required
Interface Settings/Wireless LAN	Communication Mode	Necessary
Interface Settings/Wireless LAN	SSID Setting	As required
Interface Settings/Wireless LAN	Ad-hoc Channel	As required
Interface Settings/Wireless LAN	Security Method	As required
Interface Settings/Wireless LAN	Transmission Speed	As required

↓ Note

- For the Effective Protocol setting, check that the protocol you want to use is set to [Active].
- [Wireless LAN] and [LAN Type] are displayed when the wireless LAN interface board is installed. When both Ethernet and wireless LAN are connected, the selected interface takes precedence.

📖 Reference

- p.34 "Interface Settings"

Using Utilities to Make Network Settings

This section describes how to make network settings using utilities.

You can also specify network settings using utilities such as Web Image Monitor, SmartDeviceMonitor for Admin, and telnet.

2

↓ Note

- These settings should be made by the system administrator, or with the advice of the system administrator.
- For details about using Web Image Monitor, see "Using Web Image Monitor".
- For details about using SmartDeviceMonitor for Admin, see "Using SmartDeviceMonitor for Admin".
- For details about using telnet, see "Remote Maintenance by telnet".

📖 Reference

- p.137 "Using Web Image Monitor"
- p.151 "Using SmartDeviceMonitor for Admin"
- p.176 "Remote Maintenance by telnet"

Interface Settings

This section describes how to make Interface settings using utilities.

Change settings by using Web Image Monitor, SmartDeviceMonitor for Admin, and telnet.

[Network] → [Machine IPv4 Address] → [Auto-Obtain (DHCP)]

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Can be used for specifying the setting.
- telnet: Can be used for specifying the setting.

[Network] → [Machine IPv4 Address] → [Specify] → "IPv4 Address"

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Can be used for specifying the setting.
- telnet: Can be used for specifying the setting.

[Network] → [Machine IPv4 Address] → [Specify] → "Subnet Mask"

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Can be used for specifying the setting.
- telnet: Can be used for specifying the setting.

[Network] → [IPv4 Gateway Address]

- Web Image Monitor: Can be used for specifying the setting.

- SmartDeviceMonitor for Admin: Can be used for specifying the setting.
- telnet: Can be used for specifying the setting.

[Network] → [Machine IPv6 Address] → "Manual Configuration Address"

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.
- telnet: Can be used for specifying the setting.

[Network] → [IPv6 Gateway Address]

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.
- telnet: Can be used for specifying the setting.

[Network] → [IPv6 Stateless Address Autoconfiguration]

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.
- telnet: Can be used for specifying the setting.

[Network] → [DNS Configuration] → [Auto-Obtain (DHCP)]

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.
- telnet: Can be used for specifying the setting.

[Network] → [DNS Configuration] → [Specify] → "DNS Server 1-3"

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.
- telnet: Can be used for specifying the setting.

[Network] → [DDNS Configuration]

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.
- telnet: Can be used for specifying the setting.

[Network] → [IPsec]

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.
- telnet: Can be used for specifying the setting.

[Network] → [Domain Name] → [Auto-Obtain (DHCP)]

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.

- telnet: Can be used for specifying the setting.

[Network] → [Domain Name] → [Specify] → "Domain Name"

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.
- telnet: Can be used for specifying the setting.

[Network] → [WINS Configuration] → [On] → "Primary WINS Server"

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.
- telnet: Can be used for specifying the setting.

[Network] → [WINS Configuration] → [On] → "Secondary WINS Server"

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.
- telnet: Can be used for specifying the setting.

[Network] → [WINS Configuration] → [On] → "Scope ID"

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.
- telnet: Can be used for specifying the setting.

[Network] → [WINS Configuration] → [Off]

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.
- telnet: Can be used for specifying the setting.

[Network] → [Effective Protocol] → "IPv4"

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: You can specify the TCP/IP settings if SmartDeviceMonitor for Admin is communicating with the machine using IPX/SPX.
- telnet: Can be used for specifying the setting.

[Network] → [Effective Protocol] → "IPv6"

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.
- telnet: Can be used for specifying the setting.

[Network] → [Effective Protocol] → "NetWare"

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: You can specify the IPX/SPX settings if SmartDeviceMonitor for Admin is communicating with the machine using TCP/IP.

- telnet: Can be used for specifying the setting.

[Network] → [Effective Protocol] → "SMB"

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Can be used for specifying the setting.
- telnet: Can be used for specifying the setting.

[Network] → [Effective Protocol] → "AppleTalk"

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Can be used for specifying the setting.
- telnet: Can be used for specifying the setting.

[Network] → [NCP Delivery Protocol] → [IPX Priority]

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Can be used for specifying the setting.
- telnet: Cannot be used for specifying the setting.

[Network] → [NCP Delivery Protocol] → [TCP / IP Priority]

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Can be used for specifying the setting.
- telnet: Cannot be used for specifying the setting.

[Network] → [NCP Delivery Protocol] → [IPX Only]

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Can be used for specifying the setting.
- telnet: Cannot be used for specifying the setting.

[Network] → [NCP Delivery Protocol] → [TCP / IP Only]

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Can be used for specifying the setting.
- telnet: Cannot be used for specifying the setting.

[Network] → [NW Frame Type] → [Auto Select]

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.
- telnet: Can be used for specifying the setting.

[Network] → [NW Frame Type] → [Ethernet II]

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.
- telnet: Can be used for specifying the setting.

[Network] → [NW Frame Type] → [Ethernet 802.2]

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.
- telnet: Can be used for specifying the setting.

[Network] → [NW Frame Type] → [Ethernet 802.3]

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.
- telnet: Can be used for specifying the setting.

[Network] → [NW Frame Type] → [Ethernet SNAP]

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.
- telnet: Can be used for specifying the setting.

[Network] → [SMB Computer Name]

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.
- telnet: Can be used for specifying the setting.

[Network] → [SMB Work Group]

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.
- telnet: Can be used for specifying the setting.

[Network] → [Ethernet Speed]

- Web Image Monitor: Cannot be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.
- telnet: Cannot be used for specifying the setting.

[Network] → [IEEE 802.1X Authentication for Ethernet]

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.
- telnet: Can be used for specifying the setting.

[Network] → [LAN Type] → [Ethernet]

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.
- telnet: Can be used for specifying the setting.

[Network] → [LAN Type] → [Wireless LAN]

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.
- telnet: Can be used for specifying the setting.

[Network] → [Ping Command]

- Web Image Monitor: Cannot be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.
- telnet: Cannot be used for specifying the setting.

[Network] → [Permit SNMPv3 Communication] → [Encryption Only]

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.
- telnet: Can be used for specifying the setting.

[Network] → [Permit SNMPv3 Communication] → [Encryption / Cleartext]

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.
- telnet: Can be used for specifying the setting.

[Network] → [Permit SSL / TLS Communication] → [Ciphertext Only]

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.
- telnet: Cannot be used for specifying the setting.

[Network] → [Permit SSL / TLS Communication] → [Ciphertext Priority]

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.
- telnet: Cannot be used for specifying the setting.

[Network] → [Permit SSL / TLS Communication] → [Ciphertext/Cleartext]

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.
- telnet: Cannot be used for specifying the setting.

[Network] → [Host Name]

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Can be used for specifying the setting.
- telnet: Can be used for specifying the setting.

[Network] → [Machine Name]

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.
- telnet: Can be used for specifying the setting.

[Wireless LAN] → [Communication Mode] → [802.11 Ad-hoc Mode]

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.
- telnet: Can be used for specifying the setting.

[Wireless LAN] → [Communication Mode] → [Infrastructure Mode]

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.
- telnet: Can be used for specifying the setting.

[Wireless LAN] → [SSID Setting]

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.
- telnet: Can be used for specifying the setting.

[Wireless LAN] → [Ad-hoc Channel]

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.
- telnet: Can be used for specifying the setting.

[Wireless LAN] → [Security Method]

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.
- telnet: Can be used for specifying the setting.

File Transfer

This section describes how to make File Transfer settings using utilities.

Change settings by using Web Image Monitor, SmartDeviceMonitor for Admin, and telnet.

[File Transfer] → [SMTP Server]

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.
- telnet: Cannot be used for specifying the setting.

[File Transfer] → [SMTP Authentication]

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.
- telnet: Cannot be used for specifying the setting.

[File Transfer] → [POP before SMTP]

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.
- telnet: Cannot be used for specifying the setting.

[File Transfer] → [Reception Protocol] → [POP3]

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.
- telnet: Cannot be used for specifying the setting.

[File Transfer] → [Reception Protocol] → [IMAP4]

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.
- telnet: Cannot be used for specifying the setting.

[File Transfer] → [Reception Protocol] → [SMTP]

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.
- telnet: Cannot be used for specifying the setting.

[File Transfer] → [POP3 / IMAP4 Settings]

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.
- telnet: Cannot be used for specifying the setting.

[File Transfer] → [Administrator's E-mail Address]

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.
- telnet: Cannot be used for specifying the setting.

[File Transfer] → [E-mail Communication Port]

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.
- telnet: Cannot be used for specifying the setting.

[File Transfer] → [E-mail Reception Interval]

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.
- telnet: Cannot be used for specifying the setting.

[File Transfer] → [Max. Reception E-mail Size]

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.
- telnet: Cannot be used for specifying the setting.

[File Transfer] → [E-mail Storage in Server]

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.
- telnet: Cannot be used for specifying the setting.

[File Transfer] → [Default User Name / Password (Send)]

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.
- telnet: Cannot be used for specifying the setting.

[File Transfer] → [Fax E-mail Account]

- Web Image Monitor: Can be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.
- telnet: Cannot be used for specifying the setting.

[File Transfer] → [Scanner Resend Interval Time]

- Web Image Monitor: Cannot be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.
- telnet: Cannot be used for specifying the setting.

[File Transfer] → [Number of Scanner Resends]

- Web Image Monitor: Cannot be used for specifying the setting.
- SmartDeviceMonitor for Admin: Cannot be used for specifying the setting.
- telnet: Cannot be used for specifying the setting.

Connecting the Machine to a Telephone Line and Telephone

This section describes how to connect the machine to the telephone lines and select the line type.

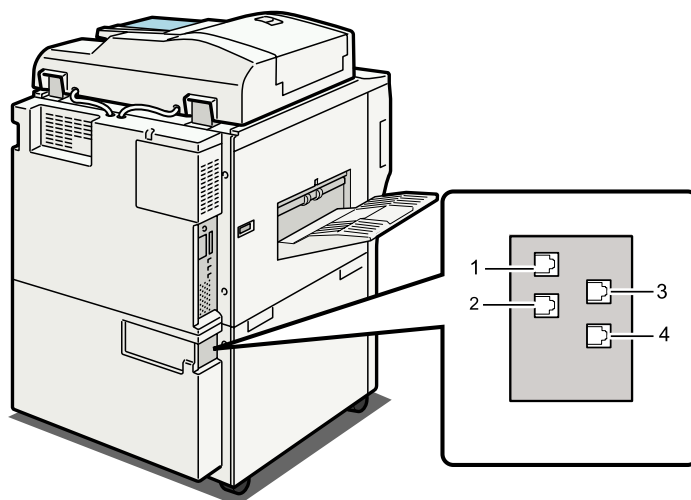
2

Connecting the Telephone Line

To connect the machine to a telephone line, use a snap-in modular type connector.

★ Important

- Make sure the connector is the correct type before you start.



BPV0138

1. Extra G3 interface unit connector
2. Extra G3 interface unit connector
3. G3 interface unit connector
4. External telephone connector

Selecting the Line Type

Select the line type to which the machine is connected. There are two types: tone and pulse dial.

Select the line type using Administrator Tools.

↓ Note

- This function is not available in some regions.

3. Using a Printer Server

This chapter describes how to configure the machine as a network printer.

Preparing Printer Server

This section explains how to configure the machine as a Windows network printer. The machine is configured to enabling network clients to use it. When the network printer is connected via SmartDeviceMonitor for Client, you can set the printing notification function to notify clients of the results of their print jobs.

★ Important

- Under Windows XP Professional or Windows Server 2003/2003 R2, to change printer properties in the [Printer] or [Printers and Faxes] window, you need Printer Management access authentication; under Windows Vista, and Windows Server 2008, Full Control access authentication. Log on to the file server as an Administrator or member of the PowerUsers group.

1. Open the [Printers and Faxes] window from the [Start] menu.

The [Printers and Faxes] window appears.

2. Click the icon of the machine you want to use. On the [File] menu, click [Properties]. The printer properties appear.

3. On the [Sharing] tab, click [Share this printer].

4. To share the machine with users using a different version of Windows, click [Additional Drivers...].

If you have installed an alternative driver by selecting [Share As:] during the printer driver installation, this step can be ignored.

5. Click [OK], and then close the printer properties.

Using NetWare

This section describes the setting procedure for network printers in the NetWare environment. In the NetWare environment, you can connect the machine as a “print server” or “remote printer”.

★ Important

- IPv6 cannot be used on this function.

Setting procedure

3

- When using the machine as a print server
 1. Installing SmartDeviceMonitor for Admin
 2. Setting the network interface board
 3. Turning the machine off and then back on
- When using the machine as a remote printer
 1. Installing SmartDeviceMonitor for Admin
 2. Setting the network interface board
 3. Setting NetWare
 4. Starting the print server

↓ Note

- This procedure assumes an environment is already prepared for normal NetWare running the printing service setting.
- The procedure is explained with the following example settings:
 - File server's name ...CAREE
 - Print server's name ...PSERV
 - Printer's name ...R-PRN
 - Queue name ...R-QUEUE

Using SmartDeviceMonitor for Admin

To use the machine in a NetWare environment, use SmartDeviceMonitor for Admin to set the NetWare printing environment.

Printers listed by SmartDeviceMonitor for Admin

SmartDeviceMonitor for Admin lists printers connected to the network. If you cannot identify the machine you want to configure, print configuration page, and then check the machine name.

↓ Note

- The NetWare Client provided by Novell is required to set the printing environment using SmartDeviceMonitor for Admin under the following environments:
 - NDS or Bindery mode in Windows 2000

- NDS or Bindery mode in Windows XP
- For details about SmartDeviceMonitor for Admin, see "Using SmartDeviceMonitor for Admin".

Reference

- p.151 "Using SmartDeviceMonitor for Admin"

Setting Up as a Print Server (NetWare 3.x)

Follow the procedure below to connect the machine as a print server using NetWare 3.x.

3

1. Start Web Image Monitor.

2. Click [Login].

A dialog box for entering the login user name and password appears.

3. Enter the login user name and password, and then click [Login].

For details about the login user name and password, consult your network administrator.

4. Click [Configuration] in the left area, and then click [NetWare Print Settings].

- **Print Server Name:** Enter the NetWare print server name. To use the interface board as a print server, enter the name of a print server that is not active on the file server. Use up to 47 characters.
- **Logon Mode:** Specify whether to designate a file server or NDS tree when logging on to NetWare.
- **File Server Name:** When a file server name is entered here, only the specified file server is searched for. This item is mandatory. Use up to 47 characters.
- **NDS Tree:** To enable NDS mode, enter the name of the NDS tree you want to log on to. Use up to 32 alphanumeric characters.
- **NDS Context Name:** To enable NDS mode, enter the print server context. Use up to 127 characters.
- **Operation Mode:** Specify whether to use the interface board as a print server or a remote printer.
- **Remote Printer No.:** This item is effective when the interface board is specified as a remote printer. Enter the same number as the number of the printer to be created on the print server (0 to 254 characters).
- **Job Timeout:** When the interface board is used as a NetWare remote printer, the printer cannot detect when a print job ends. Therefore, the printer terminates printing when a certain period of time has elapsed since it last received print data (i.e., when it has not received print data for a certain period of time). Specify here this period of time (3 to 255 seconds). The initial value is 15 (seconds).
- **Frame Type:** Select the frame type from the drop-down menu.
- **Print Server Protocol:** Select the protocol for NetWare from the drop-down menu.
- **NCP Delivery Protocol:** Select the protocol for NCP delivery.

5. Confirm the settings, and then click [Device Name].

Configuration is now complete. Wait several before restarting Web Image Monitor.

6. Click [Logout].

Note

- To check the configuration is correct, enter the following from the command prompt:
F:> USERLIST
- If the printer works as configured, the name of the print server appears as a connected user.
- If you cannot identify the printer you want to configure, check the printer name against the configuration page printed from the printer.
- If no printer names appear in the list, match the frame types of IPX/SPXs for the computer and printer. Use the [Network] dialog box of Windows to change the frame type of the computer.
- For details about Web Image Monitor, see "Using Web Image Monitor".
- For details about login user names and passwords, see Security Reference, which is the administrator's manual.

Reference

- p.137 "Using Web Image Monitor"

Setting Up as a Print Server (NetWare 4.x, 5/5.1, 6/6.5)

Follow the procedure below to connect the machine as a print server using NetWare 4.x, NetWare 5/5.1, or NetWare 6 / 6.5.

Important

- When using the printer as a print server in NetWare 4.x, NetWare 5/5.1, or NetWare 6/6.5, set it to the NDS mode.
- When using NetWare 5/5.1 or NetWare 6/6.5, set the printer as a print server.

1. Start Web Image Monitor.

2. Click [Login].

A dialog box for entering the login user name and password appears.

3. Enter the login user name and password, and then click [Login].

For details about the login user name and password, consult your network administrator.

4. Click [Configuration] in the left area, and then click [NetWare Print Settings].

5. Confirm the settings, and then click [Device Name].

Configuration is now complete. Wait several minutes before restarting Web Image Monitor.

6. Click [Logout].

7. Quit Web Image Monitor.

↓ Note

- To check the configuration is correct, enter the following from the command prompt:
F:> USERLIST
- If the printer works as configured, the name of the print server appears as a connected user.
- If you cannot identify the printer you want to configure, check the printer name against the configuration page printed from the printer. If no printer names appear in the list, match the frame types of IPX/SPXs for the computer and printer. Use the [Network] dialog box of Windows to change the frame type of the computer.
- For details about Web Image Monitor, see "Using Web Image Monitor".
- For details about login user names and passwords, see Security Reference, which is the administrator's manual.

📖 Reference

- p.137 "Using Web Image Monitor"

Using Pure IP in the NetWare 5/5.1 or 6/6.5 Environment

Follow the procedure below to connect the machine as a print server in a pure IP environment of NetWare 5/5.1 or NetWare 6/6.5.

★ Important

- When creating a queued print server in a pure IP environment of NetWare 5/5.1 or NetWare 6/6.5, create a print queue on the file server using NetWare Administrator.
- This printer is not available as a remote printer for use in a pure IP environment.
- To use the printer in a pure IP environment, set it to IPv4.

Setting up using NWadmin

1. From Windows, start NWadmin.

For details about NWadmin, see the NetWare manuals.

2. Select the object in which the print queue is located in the directory tree, and then click [Create] on the [Object] menu.

3. In the [Class of new object] box, click [Print Queue], and then click [OK].

4. In the [Print Queue Name] box, enter the name of the print queue.

5. In the [Print Queue Volume] box, click [Browse].

6. In the [Available objects] box, click the volume in which the print queue is created, and then click [OK].

3

7. Check the settings, and then click [Create].
 8. Select the object in which the printer is located, and then click [Create] on the [Object] menu.
 9. In the [Class of new object] box, click [Printer], and then click [OK]. For NetWare 5, click [Printer (Non NDPS)].
 10. In the [Printer name] box, enter the printer name.
 11. Select the [Define additional properties] check box, and then click [Create].
 12. Click [Assignments], and then click [Add] in the [Assignments] area.
 13. In the [Available objects] box, click the queue you created, and then click [OK].
 14. Click [Configuration], click [Parallel] in the [Printer type] list, and then click [Communication].
 15. Click [Manual load] in the [Communication type] area, and then click [OK].
 16. Check the settings, and then click [OK].
 17. Select a context specified, and then click [Create] on the [Object] menu.
 18. In the [Class of new object] box, click [Print Server], and then click [OK]. For NetWare 5, click [Print Server (Non NDPS)].
 19. In the [Print Server Name] box, enter the print server name.
20. Select the [Define additional properties] check box, and then click [Create].
 21. Click [Assignments], and then click [Add] in the [Assignments] area.
 22. In the [Available objects] box, click the queue you created, and then click [OK].
 23. Check the settings, and then click [OK].
 24. Start the print server by entering the following from the console of the NetWare server.

Use the same print server name specified using SmartDeviceMonitor for Admin.

If the print server is in operation, quit and restart it.

To quit

```
CAREE: unload pserver
```

To start

```
CAREE: load pserver [print server name]
```

Setting up using Web Image Monitor

1. Start Web Image Monitor.
2. Click [Login].

A dialog box for entering the login user name and login password appears.
3. Enter the login user name and password, and then click [Login].

For details about the login user name and password, consult your network administrator.

4. Click [Configuration] in the left area, and then click [NetWare Print Settings].

5. Confirm the settings, and then click [Device Name].

Configuration is now complete. Wait several minutes before restarting Web Image Monitor.

6. Click [Logout].

7. Quit Web Image Monitor.

↓ Note

- If you cannot identify the printer you want to configure, check the printer name against the configuration page printed from the printer.
- If no printer names appear in the list, match the frame types of IPX/SPXs for the computer and printer. Use the [Network] dialog box of Windows to change the frame type of the computer.
- For details about Web Image Monitor, see "Using Web Image Monitor".
- For details about login user names and passwords, see Security Reference, which is the administrator's manual.

📖 Reference

- p.137 "Using Web Image Monitor"

Setting Up as a Remote Printer (NetWare 3.x)

Follow the procedure below to use the machine as a remote printer under NetWare 3.x.

Setting up using PCONSOLE

1. Enter "PCONSOLE" from the command prompt.

```
F:> PCONSOLE
```

2. Create a print queue.

When using the existing print queue, go to the procedure for creating a printer.

3. From the [Available Options] menu, select [Print Queue Information], and then press the [Enter] key.

4. Press [Insert] key, and then enter a print queue name.

5. Press [Esc] key to return to the [Available Options] menu.

6. Set up the network connection to a printer.

7. On the [Available Options] menu, click [Print Server Information], and then press the [Enter] key.

8. To create a new print server, press the [Insert] key, and then enter a print server name.

For a currently defined print server, select a print server in the [Print Server] list.

Use the same printer name specified using SmartDeviceMonitor for Admin.

9. From the [Print Server Information] menu, select [Print Server Configuration].

10. From the [Print Server Configuration] menu, select [Printer Configuration].

11. Select the printer indicated as [Not Installed].

Use the same printer number specified as the remote printer number using SmartDeviceMonitor for Admin.

12. To change the printer name, enter a new name.

A name "printer x" is assigned to the printer. The "x" stands for the number of the selected printer.

13. As type, select [Remote Parallel, LPT1].

The IRQ, Buffer size, Starting form, and Queue service mode are automatically configured.

14. Press the [Esc] key, and then click [Yes] on the confirmation message.

15. Press the [Esc] key to return to [Print Server Configuration Menu].

16. Assign print queues to the created printer.

17. From [Print Server Configuration Menu], select [Queues Serviced By Printer].

18. Select the printer created.

19. Press the [Insert] key to select a queue serviced by the printer.

You can select several queues.

20. Follow the instructions on the screen to make other necessary settings.

Following these steps, check that the queues are assigned.

21. Press the [Esc] key until "Exit?" appears, and then select [Yes] to exit PCONSOLE.

22. Start the print server by entering the following from the console of the NetWare server.

If the print server is in operation, quit and restart it.

To quit

```
CAREE: unload pserver
```

To start

```
CAREE: load pserver [print server name]
```

If the printer works as configured, the message "Waiting for job" appears.

Setting up using Web Image Monitor

1. Start Web Image Monitor.

2. Click [Login].

A dialog box for entering the login user name and login password appears.

3. Enter the login user name and password, and then click [Login].

For details about the login user name and password, consult your network administrator.

4. Click [Configuration] in the left area, and then click [NetWare Print Settings].

5. Confirm the settings, and then click [Device Name].

Configuration is now complete. Wait several minutes before restarting Web Image Monitor.

6. Click [Logout].

7. Quit Web Image Monitor.

↓ Note

- If you cannot identify the printer you want to configure, check the printer name against the configuration page printed from the printer.
- If no printer names appear in the list, match the frame types of IPX/SPXs for the computer and printer. Use the [Network] dialog box of Windows to change the frame type of the computer.
- For details about Web Image Monitor, see "Using Web Image Monitor".
- For details about login user names and passwords, see Security Reference, which is the administrator's manual.

📖 Reference

- p.137 "Using Web Image Monitor"

Setting Up as a Remote Printer (NetWare 4.x, 5/5.1, 6/6.5)

Follow the procedure below to use the printer as a remote printer under NetWare 4.x, 5/5.1 and 6/6.5.

★ Important

- To use the printer as a remote printer under NetWare 4.x, 5/5.1, 6/6.5, set it to NDS mode.
- Do not use the printer as a remote printer when Pure IP is used.

Setting up using NWadmin

1. From Windows, start NWadmin.

For details about NWadmin, see the NetWare manuals.

2. Set up the network connection to a print queue. Select the object in which the print queue is located in the directory tree, and then click [Create] on the [Object] menu.

3. In the [Class of new object] box, click [Print Queue], and then click [OK].

4. In the [Print Queue Name] box, enter the name of the print queue.

5. In the [Print Queue Volume] box, click [Browse].

6. In the [Available objects] box, click the volume in which the print queue is created, and then click [OK].

7. Check the settings, and then click [Create].

8. Set up the network connection to a printer. Select the object in which the printer is located, and then click [Create] on the [Object] menu.

9. In the [Class of new object] box, click [Printer], and then click [OK]. For NetWare 5, click [Printer (Non NDPS)].
10. In the [Printer name] box, enter the printer name.
11. Select the [Define additional properties] check box, and then click [Create].
12. Assign print queues to the created printer. Click [Assignments], and then click [Add] in the [Assignments] area.
13. In the [Available objects] box, click the queue you created, and then click [OK].
14. Click [Configuration], click [Parallel] in the [Printer type] list, and then click [Communication].
15. Click [Manual load] in the [Communication type] area, and then click [OK]. Check the settings, and then click [OK].
16. Set up the network connection to a print server. Select a context specified, and then click [Create] on the [Object] menu.
17. In the [Class of new object] box, click [Print Server], and then click [OK]. For NetWare 5, click [Print Server (Non NDPS)].
18. In the [Print Server Name:] box, enter the print server name.
Use the same print server name specified using SmartDeviceMonitor for Admin.
19. Select the [Define additional properties] check box, and then click [Create].
20. Assign the printer to the created print server. Click [Assignments], and then click [Add] in the [Assignments] area.
21. In the [Available objects] box, click the queue you created, and then click [OK].
22. In the [Printers] area, click the printer you assigned, and then click [Printer Number].
23. Enter the printer number, and then click [OK]. Check the settings, and then click [OK].
Use the same printer number specified as the remote printer number using SmartDeviceMonitor for Admin.
24. Start the print server by entering the following from the console of the NetWare server.
If the print server is in operation, quit and restart it.
To exit
CAREE: unload pserver
To start
CAREE: load pserver [print server name]
25. Enter the printer server name as the context name, and then press the [Enter] key.
26. Select the printer name on the context menu, and then press the [Enter] key.

Setting up using Web Image Monitor

1. Start Web Image Monitor.

2. Click [Login].

A dialog box for entering the login user name and login password appears.

3. Enter the login user name and password, and then click [Login].

For details about the login user name and password, consult your network administrator.

4. Click [Configuration] in the left area, and then click [NetWare Print Settings].**5. Confirm the settings, and then click [Device Name].**

Configuration is now complete. Wait several minutes before restarting Web Image Monitor.

6. Click [Logout].**7. Quit Web Image Monitor.****Note**

- If you cannot identify the printer you want to configure, check the printer name against the configuration page printed from the printer.
- If no printer names appear in the list, match the frame types of IPX/SPXs for the computer and printer. Use the [Network] dialog box of Windows to change the frame type of the computer.
- For details about Web Image Monitor, see "Using Web Image Monitor".
- For details about login user names and passwords, see Security Reference, which is the administrator's manual.

Reference

- p.137 "Using Web Image Monitor"

4. Monitoring and Configuring the Printer

This chapter describes how to monitoring and configuring the printer.

Using Web Image Monitor

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

Available operations

The following operations can be remotely performed using Web Image Monitor from a client computer.

- Displaying machine status or settings
- Checking the print job status or history
- Checking, modifying, printing, or deleting print jobs stored in the Document Server
- Interrupting currently printing jobs
- Resetting the machine
- Managing the Address Book
- Making machine settings
- Making network protocol settings
- Making security settings

Configuring the machine

To perform the operations from Web Image Monitor, TCP/IP is required. After the machine is configured to use TCP/IP, operations from Web Image Monitor become available.

Recommended Web browser

- Windows:
 - Internet Explorer 5.5 SP2 or higher
 - Firefox 1.0 or higher
- Mac OS:
 - Firefox 1.0 or higher
 - Safari 1.0, 1.2, 2.0 (412.2) or higher

Web Image Monitor supports screen reader software. We recommend JAWS 7.0 or a later version.

Note

- Safari cannot be used on Mac OS X 10.4.1.

- Display and operation problems can occur if you do not enable JavaScript and cookies, or if you are using a non-recommended Web Browser.
- If you are using a proxy server, change the Web browser settings. Contact your administrator for information about the settings.
- If you click your browser's back button but the previous page does not appear, click the browser's refresh button and try again.
- Machine information is not automatically updated. To perform an update, click [Refresh] in the display area.
- We recommend using Web Image Monitor in the same network.
- If the machine is firewall-protected, it cannot be accessed from computers outside the firewall.
- When using the machine under DHCP, the IP address may be automatically changed by the DHCP server settings. Enable DDNS setting on the machine, and then connect using the machine's host name. Alternatively, set a static IP address to the DHCP server.
- If the HTTP port is disabled, connection to the machine using the machine's URL cannot be established. SSL setting must be enabled on this machine. For details, consult your network administrator.
- When using the SSL encryption protocol, enter "https://(machine's IP address or host name)/".
- Internet Explorer must be installed on your computer. Use the most recent available version. We recommend Internet Explorer 6.0 or later.
- When you are using Firefox, fonts and colors may be different, or tables may be out of shape.
- When using a host name under Windows Server 2003/2003 R2/2008, or Windows Vista with IPv6 protocol, perform host name resolution using an external DNS server. The host file cannot be used.
- To use JAWS 7.0 under Web Image Monitor, you must be running Windows OS and Microsoft Internet Explorer 5.5 SP2, or a later version.

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".**

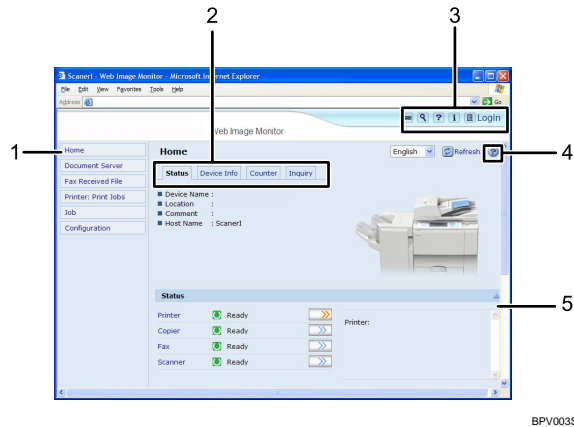
1. **Start your Web browser.**
2. **Enter "http://(machine's IP address or host name)/" in your Web browser's URL bar.**

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)/".

Every Web Image Monitor page is divided into the following areas:



BPV003S

4

1. Menu area

If you select menu, its content will be shown on the work area, or the sub area.

2. Tab area

Details about each menu appear.

3. 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.

4. Help

Use Help to view or download Help file contents.

5. Display area

Displays the contents of the item selected in the menu area.

Machine information in the display area is not automatically updated. Click [Refresh] at the upper right in the display area to update the machine information. Click the Web browser's [Refresh] button to refresh the entire browser screen.

Note

- When using a host name under Windows Server 2003/2003 R2/2008, or Windows Vista with IPv6 protocol, perform host name resolution using an external DNS server. The host file cannot be used.

When User Authentication is Set

Login (using Web Image Monitor)

Follow the procedure below to log on when user authentication is set.

1. Click [Login].
2. Enter a login user name and password, and then click [Login].

For details about the login user name and password, consult your network administrator.

Note

- For user code authentication, enter a user code in [Login User Name], and then click [Login].
- The procedure may differ depending on the Web browser used.

4

Log out (using Web Image Monitor)

Click [Logout] to log off.

Note

- When you log on and make the setting, always click [Logout].

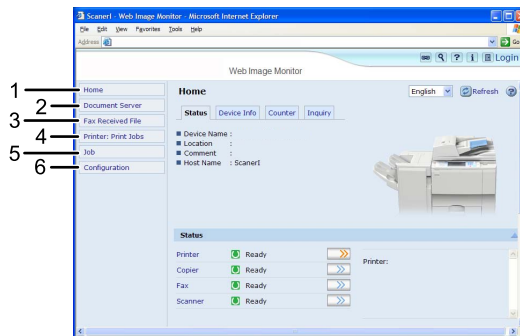
About Menu and Mode

There are two modes available with Web Image Monitor: guest mode and administrator mode.

Displayed Items may differ depending on the machine type.

Guest Mode

In the guest mode, machine status, settings, and print job status can be viewed, but the machine settings cannot be changed.



BPV004S

1. Home

The [Status], [Device Info], [Counter], and [Inquiry] tab are displayed. Details of the tab menu are displayed on the work area.

2. Document Server

Display files stored in the Document Server.

3. Fax Received File

Display received fax files.

4. Printer: Print Jobs

Allows you to display list of Sample Print, Locked Print, Hold Print, and Stored Print jobs.

5. Job

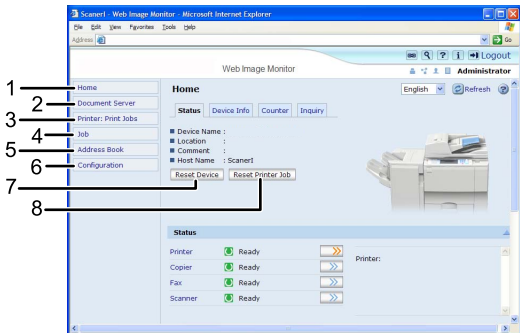
Display all print files.

6. Configuration

Display current machine and network settings.

Administrator Mode

In the administrator mode, you can configure various machine settings.



BPV005S

1. Home

The [Status], [Device Info], [Counter], and [Inquiry] tab are displayed. Details of the tab menu are displayed on the work area.

2. Document Server

Display files stored in the Document Server.

3. Printer: Print Jobs

Allows you to display list of Locked Print, Sample Print, Hold Print, and Stored Print jobs.

4. Job

Display all print files.

5. Address Book

User information can be registered, displayed, changed, and deleted.

6. Configuration

Make system settings for the machine, interface settings, and security.

7. Reset Device

Click to reset the printer. If a print job is being processed, the printer will be reset after the print job is completed. This button is located on Top Page.

8. Reset Printer Job

Click to reset current print jobs and print jobs in queue. This button is located on Top Page.

Access in the Administrator Mode

4

Follow the procedure below to access Web Image Monitor in the administrator mode.

1. On Top Page, click [Login].

The window for entering the login user name and password appears.

2. Enter your login user name and password, and then click [Login].

For details about the login user name and password, consult your network administrator.

List of Setting Items

The following tables show Web Image Monitor items that can be viewed or modified depending on the selected mode on the Web browser. Select one of the following modes to log on Web Image Monitor:

- Guest mode: logged on as a user
- Administrator mode: logged on as an administrator

Home

Status

Menu	Guest mode	Administrator mode
Reset Device	None	Modify
Reset Printer Job	None	Modify
Status	Read	Read
Toner	Read	Read
Input Tray	Read	Read
Output Tray	Read	Read

Device Info

Menu	Guest mode	Administrator mode
Functions	Read	Read
System	Read	Read
Version	Read	Read
Printer Language	Read	Read

Counter

Menu	Guest mode	Administrator mode
Copier	Read	Read
Printer	Read	Read
Fax	Read	Read
Send/TX Total	Read	Read
Fax Transmission	Read	Read
Scanner Send	Read	Read
Coverage	Read	Read
Other Function(s)	Read	Read

Inquiry

Menu	Guest mode	Administrator mode
Machine Maintenance/Repair	Read	Read
Sales Representative	Read	Read

Document Server

Document Server

Guest mode	Administrator mode
Read/Modify	Read/Modify

Fax Received File

Guest mode	Administrator mode
Read/Modify	None

Printer: Print Jobs

Print Job List

Guest mode	Administrator mode
Read/Modify	Read/Modify

4

Job

Job List

Menu	Guest mode	Administrator mode
Current/Waiting Jobs	Read	Read/Modify
Job History	Read	Read

Printer

Menu	Guest mode	Administrator mode
Job History	Read	Read
Error Log	Read	Read

Fax History

Menu	Guest mode	Administrator mode
Transmission	Read	Read/Modify
Reception	Read	Read/Modify
LAN-Fax	Read	Read

Document Server

Menu	Guest mode	Administrator mode
Print Job History	Read/Modify	Read/Modify

Menu	Guest mode	Administrator mode
Fax Remote Send History	Read/Modify	Read/Modify
Scanner Remote Send History	Read/Modify	Read/Modify

Address Book

Menu	Guest mode	Administrator mode
Address Book	None	Read/Modify

Configuration

Device Settings

Menu	Guest mode	Administrator mode
System	Read	Read/Modify
Paper	Read	Read/Modify
Date/Time	Read	Read/Modify
Timer	Read	Read/Modify
Logs	None	Read/Modify
E-mail	Read	Read/Modify
Auto E-mail Notification	None	Read/Modify
On-demand E-mail Notification	None	Read/Modify
File Transfer	None	Read/Modify
User Authentication Management	None	Read/Modify
Administrator Authentication Management	None	Read/Modify
Program/Change Administrator	None	Read/Modify
LDAP Server	None	Read/Modify

Menu	Guest mode	Administrator mode
Firmware Update	None	Read/Modify
Program/Change Realm	None	Modify

Printer

Menu	Guest mode	Administrator mode
Basic Settings	Read	Read/Modify
Tray Parameters (PCL)	None	Read/Modify
Tray Parameters (PS)	None	Read/Modify
Virtual Printer Settings	Read	Read/Modify
PDF Temporary Password	Modify	None
PDF Group Password	None	Modify
PDF Fixed Password	None	Modify

Fax

Menu	Guest mode	Administrator mode
Initial Settings	None	Read/Modify
Send / Reception Settings	None	Read/Modify
IP-Fax Settings	None	Read/Modify
IP-Fax Gateway Settings	None	Read/Modify
Parameter Settings	None	Read/Modify

Scanner

Menu	Guest mode	Administrator mode
General Settings	Read	Read/Modify
Scan Settings	Read	Read/Modify
Send Settings	Read	Read/Modify

Menu	Guest mode	Administrator mode
Initial Settings	Read	Read/Modify
Default Settings for Normal Screens on Device	Read	Read/Modify
Default Settings for Simplified Screens on Device	Read	Read/Modify

Interface

Menu	Guest mode	Administrator mode
Interface Settings	Read	Read/Modify
Wireless LAN Settings	Read	Read/Modify

4

Network

Menu	Guest mode	Administrator mode
IPv4	Read	Read/Modify
IPv6	Read	Read/Modify
NetWare	Read	Read/Modify
AppleTalk	Read	Read/Modify
SMB	Read	Read/Modify
SNMP	None	Read/Modify
SNMPv3	None	Read/Modify
SSDP	None	Read/Modify
Bonjour	Read	Read/Modify
System Log	Read	Read

Security

Menu	Guest mode	Administrator mode
Network Security	None	Read/Modify

Menu	Guest mode	Administrator mode
Access Control	None	Read/Modify
IPP Authentication	None	Read/Modify
SSL/TLS	None	Read/Modify
ssh	None	Read/Modify
Site Certificate	None	Read/Modify
Device Certificate	None	Read/Modify
IPsec	None	Read/Modify
User Lockout Policy	None	Read/Modify
IEEE 802.1X (WPA/WPA2)	None	Read/Modify
S/MIME	None	Read/Modify

RC Gate

Menu	Guest mode	Administrator mode
Setup RC Gate	None	Read/Modify
Update RC Gate Firmware	None	Read
RC Gate Proxy Server	None	Read/Modify

Webpage

Menu	Guest mode	Administrator mode
Webpage	Read	Read/Modify

Extended Feature Settings

Menu	Guest mode	Administrator mode
Startup Setting	None	Read/Modify
Extended Feature Info	None	Read
Install	None	Read/Modify

Menu	Guest mode	Administrator mode
Uninstall	None	Read/Modify
Change Allocation	None	Read/Modify
Administrator Tools	None	Read/Modify
Additional Program Setup Setting	None	Read/Modify
Install Additional Program	None	Read/Modify
Uninstall Additional Program	None	Read/Modify
Copy Extended Features	None	Read/Modify
Copy Card Save Data	None	Read/Modify

↓ Note

- Some items are not displayed depending on the security settings.

Displaying Web Image Monitor Help

When using Help for the first time, clicking the icon marked “?” (🔍🔍) makes the following screen appear, in which you can view Help in two different ways, as shown below:

Viewing Help on our Web site

Downloading Help to your computer

Downloading and Checking Help

You can download Help to your computer. As the Help URL, you can specify the path to the local file to view the Help without connecting to the Internet.

↓ Note

- By clicking “?” (🔍) in the header area, the contents of Help appear.
- By clicking “?” (🔍), the Help icon in the display area, Help for the setting items in the display area appears.

Downloading Help

1. In the [OS] list, select the operating system.
2. In the [Language] list, select the language.

3. Click [Download].
4. Download Help by following the instructions on the screen.
5. Store the downloaded compressed file in a given location, and then decompress the file.

To create a link for the Help button (??), save the downloaded Help files on a Web server.

Linking the URL of the downloaded Help

You can link the URL of the help file on a computer or Web server to the “?” button.

1. Log on to Web Image Monitor in the administrator mode.
2. In the menu area, click [Configuration].
3. Click [Webpage].
4. In the [Set Help URL Target] box, enter the URL of the help file.

If you saved the help file to "C:\HELP\EN", enter "file://C:/HELP/". For example, if you saved the file to a Web server, and the URL of the index file is "http:// a.b.c.d/HELP/EN/index.html", enter "http://a.b.c.d/HELP/".

5. Click [OK].

↓ Note

- If you save the Help files on your hard disk, you must access them directly - you cannot link to them using the Help button (??).

Using SmartDeviceMonitor for Admin

Using SmartDeviceMonitor for Admin, you can monitor the network printers. Also, you can change the configuration of the network interface board using TCP/IP or IPX/SPX.

★ Important

- IPv6 cannot be used on this function.

Protocol stack provided with Operating System

- Windows 2000
TCP/IP
IPX/SPX
NetWare
Novell Client for Windows 2000/XP/2003
- Windows Server 2003/2003 R2
TCP/IP
IPX/SPX
Novell Client for Windows 2000/XP/2003
- Windows Server 2008
TCP/IP
- Windows XP
TCP/IP
IPX/SPX
Novell Client for Windows 2000/XP/2003
- Windows Vista
TCP/IP
Novell Client for Windows Vista

Available operations

The following functions are available:

- Limits settings done from the control panel, and disables changes made to certain items.
- Enables selection of paper type loaded in the machine.
- Switches to, and comes out of Energy Saver mode.
- Checks information about printing, paper quantity, etc.
- Simultaneously monitors multiple printers. When there are many printers, you can create groups and classify printers to facilitate management.
- Checks the machine's network settings and detailed device information.

- Enables you to change the machine's network settings.
- You can check details of print jobs sent from a computer.
- Allows you to check job histories of printed, faxed (LAN-Fax), scanned, and photocopied documents identified by user codes.
- Allows selection of functions such as printing and scanning for each user code.
- Fax numbers and e-mail addresses stored in the machine can be changed and saved by computer.
- You can check each fax job history entry.
- You can make settings for and display the status changes of group devices.
- Using Address Management Tool, you can manage LAN-Fax numbers, user names for Scan to Folder, and addresses for sending and receiving Internet faxes.
- The e-mail sender's name and folder can be protected.

Installing SmartDeviceMonitor for Admin

Follow the procedure below to install SmartDeviceMonitor for Admin

- 1. Quit all applications currently running.**
- 2. Insert the CD-ROM into the CD-ROM drive.**

The installer starts.

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

The following languages are available: Czech, Danish, German, English, Spanish, French, Italian, Hungarian, Dutch, Norwegian, Polish, Portuguese, Finnish, Swedish, Chinese Simple and Chinese Traditional.

- 4. Click SmartDeviceMonitor for Admin.**

- 5. Click [Next].**

The software license agreement appears in the License Agreement dialog box.

- 6. After reading through its contents, click [Next].**

- 7. Follow the instructions on the screen.**

A message appears when the installation is completed.

- 8. Click [OK].**

A message about restarting the computer may appear. Restart the computer to complete installation.

↓ Note

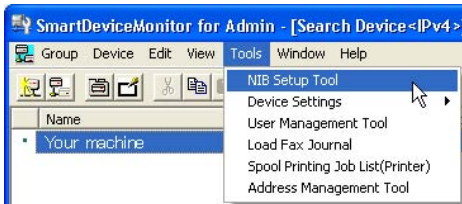
- Auto Run may not work under certain operating system settings. In this case, launch "Setup.exe" located on the CD-ROM root directory.

- If you are required to restart the computer after installing SmartDeviceMonitor for Admin, restart the computer and continue the configuration.

Changing the Network Interface Board Configuration

Follow the procedure below to change the network interface board configuration using SmartDeviceMonitor for Admin.

1. **Start SmartDeviceMonitor for Admin.**
2. **On the [Group] menu, point to [Search Device], and then click [IPv4], [IPX/SPX] or [IPv4 SNMPv3].**
A list of machines using the selected protocol appears.
Select the protocol of the machine whose configuration you want to change.
If you are using IPv4 SNMPv3, enter the user authentication.
3. **In the list, select a machine whose configuration you want to change.**
4. **On the [Tools] menu, click [NIB Setup Tool].**



A Web browser opens and the window for entering the login user name and password for the Web Image Monitor administrator appears.

NIB Setup Tool starts. Click [Web browser], and then click [OK].

5. **Enter the login user name and password, and then click [Login].**
For details about the login user name and password, consult your network administrator.
6. **Configure settings using Web Image Monitor.**
7. **Click [Logout].**
8. **Quit Web Image Monitor.**
9. **Quit SmartDeviceMonitor for Admin.**

↓ Note

- For details about login user names and passwords, see Security Reference, which is the administrator's manual.
- For details about Web Image Monitor, see "Using Web Image Monitor".

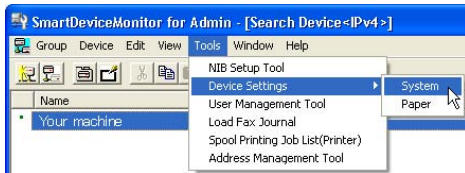
Reference

- p.137 "Using Web Image Monitor"

Locking the Menus on the Machine's Control Panel

Follow the procedure below to lock the menus on the machine's control panel.

1. **Start SmartDeviceMonitor for Admin.**
2. **On the [Group] menu, point to [Search Device], and then click [IPv4], [IPX/SPX] or [IPv4 SNMPv3].**
A list of machines using the selected protocol appears.
Select the protocol of the machine whose configuration you want to change.
If you are using IPv4 SNMPv3, enter the user authentication.
3. **Select a machine.**
4. **On the [Tools] menu, point to [Device Settings], and then click [System].**



A Web browser opens and the window for entering the login user name and password for the Web Image Monitor administrator appears.

5. **Enter the login user name and password, and then click [Login].**
For details about the user name and password, consult your network administrator.
The [System] page of Web Image Monitor appears.
6. **On the [Protect Printer Display Panel], select [Level 1] or [Level 2].**
7. **Click [OK].**
8. **Click [Logout].**
9. **Quit Web Image Monitor.**
10. **Quit SmartDeviceMonitor for Admin.**

Note

- For details about login user names and passwords, see Security Reference, which is the administrator's manual.
- For details about Web Image Monitor, see "Using Web Image Monitor".

Reference

- p.137 "Using Web Image Monitor"

Changing the Paper Type

Follow the procedure below to change the paper type.

1. Start SmartDeviceMonitor for Admin.

2. On the [Group] menu, point to [Search Device], and then click [IPv4], [IPX/SPX] or [IPv4 SNMPv3].

A list of machines using the selected protocol appears.

Select the protocol of the machine whose configuration you want to change.

If you are using IPv4 SNMPv3, enter the user authentication.

3. In the list, select a machine whose configuration you want to change.

4. On the [Tools] menu, point to [Device Settings], and then click [Paper].

A Web browser opens and the window for entering the login user name and password for the Web Image Monitor administrator appears.

5. Enter the login user name and password, and then click [Login].

For details about the login user name and password, consult your network administrator.

The [Paper] page appears.

Select a paper type in the [Paper Type] list for each tray. Enter required setting items.

6. Click [Logout].

7. Quit Web Image Monitor.

8. Quit SmartDeviceMonitor for Admin.

Note

- For details about login user names and passwords, see Security Reference, which is the administrator's manual.
- For details about Web Image Monitor, see "Using Web Image Monitor".
- For details about setting items, see Help in the General Settings on Configuration page.

Reference

- p.137 "Using Web Image Monitor"

Managing User Information

Follow the procedure below to manage the user's information using SmartDeviceMonitor for Admin.

Prints jobs can be managed and functions restricted by user codes.

Starting User Management Tool

Follow the procedure below to start User Management Tool.

1. Start SmartDeviceMonitor for Admin.
2. On the [Group] menu, point to [Search Device], and then click [IPv4], [IPX/SPX] or [IPv4 SNMPv3].

A list of machines using the selected protocol appears.

Select the protocol of the machine whose configuration you want to change.

If you are using IPv4 SNMPv3, enter the user authentication.

3. In the list, select a machine you want to manage.
4. On the [Tools] menu, click [User Management Tool].



A Web browser opens and the window for entering the login user name and password for the Web Image Monitor administrator appears.

5. Enter the login user name and password, and then click [Login].

For details about the login user name and password, consult your network administrator.

User Management Tool starts.

Note

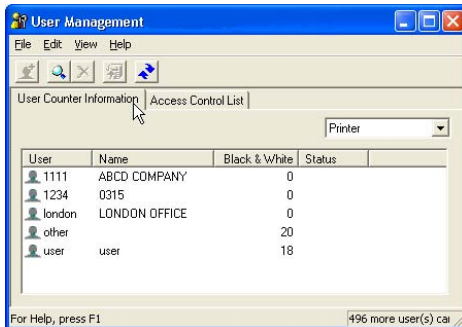
- For details about login user names and passwords, see Security Reference, which is the administrator's manual.
- For details about User Management Tool, see SmartDeviceMonitor for Admin Help.

Displaying the Number of Sheets Printed

Follow the procedure below to display the number of sheets printed under each user.

1. Start SmartDeviceMonitor for Admin User Management Tool.

2. Click the [User Counter Information] tab of User Management Tool.



The number of pages printed under each user appears.

3. Click [Exit] on the [File] menu to quit User Management Tool.

4

Exporting the information about the number of pages printed

Follow the procedure below to export the information of the number of pages printed under each user as a csv file.

1. Start SmartDeviceMonitor for Admin User Management Tool.
2. Click the [User Counter Information] tab of User Management Tool.
3. On the [File] menu, click [Export User Statistics List].



4. Specify the save location and file name, and then click [Save].
5. Click [Exit] on the [File] menu to quit User Management Tool.

Resetting the number of pages printed to 0.

Follow the procedure below to reset the number of pages printed under each user to 0.

1. Start SmartDeviceMonitor for Admin User Management Tool.
2. Click the [User Counter Information] tab of User Management Tool.
3. Select the user whose information you want to reset.

- 4. On the [Edit] menu, click [Reset User Counters].



4

- 5. Select the check box of the items you want to reset, and then click [OK].

A confirmation message appears.

- 6. Click [OK].

The count for the selected paper type becomes 0 and [Modified] is displayed for [Status].

- 7. On the [Edit] menu, click [Apply Settings].



Changes are applied to information on the User Counter Information tab.

- 8. Click [Exit] on the [File] menu to quit User Management Tool.

Restricting Functions

Follow the procedure below to restrict use of individual functions.

1. Start SmartDeviceMonitor for Admin User Management Tool.
2. Click the [User Counter Information] tab of User Management Tool.
3. Click the user whose functions you want to restrict.
4. On the [Edit] menu of User Management Tool, click [Restrict Access To Device].



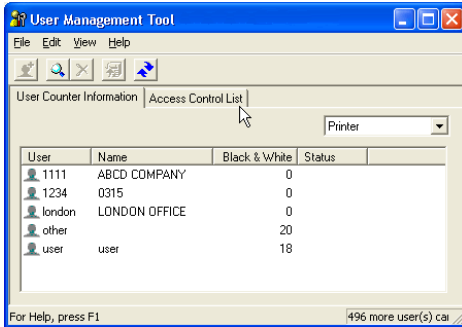
5. Select the check box of the functions you want to restrict.
6. Click [OK].
A confirmation message appears.
7. Click [Yes].
The settings are applied.
8. Click [Exit] on the [File] menu to quit User Management Tool.

Setting Applicable Functions to New Users

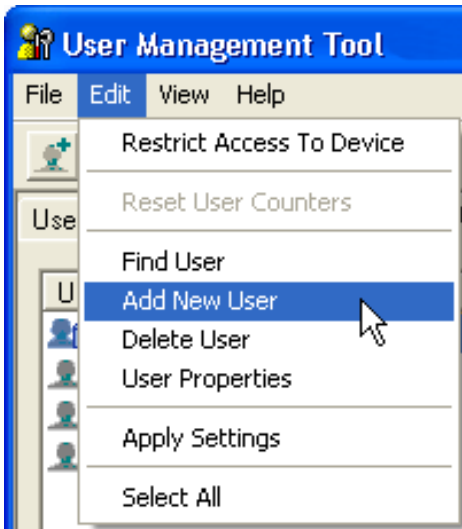
Follow the procedure below to add new users and set functions applicable to them.

1. Start SmartDeviceMonitor for Admin User Management Tool.

2. Click the [Access Control List] tab of User Management Tool.



3. On the [Edit] menu, click [Add New User].



4. Enter the user code and user name.

5. Select the check box of the functions applicable to the new user.

If the check boxes are unavailable, there is no restriction to use that function.

6. Click [OK].

The user is added, and [New] is displayed for [Status].

7. On the [Edit] menu, click [Apply Settings].

The settings are applied.

8. Click [Exit] on the [File] menu to quit User Management Tool.

Note

- For details about setting restrictions, see SmartDeviceMonitor for Admin Help.

Configuring the Energy Saver Mode

Follow the procedure below to configure Energy Saver mode.

1. Start SmartDeviceMonitor for Admin.
2. On the [Group] menu, point to [Search Device], and then click [IPv4], [IPX/SPX] or [IPv4 SNMPv3].

A list of machines using the selected protocol appears.

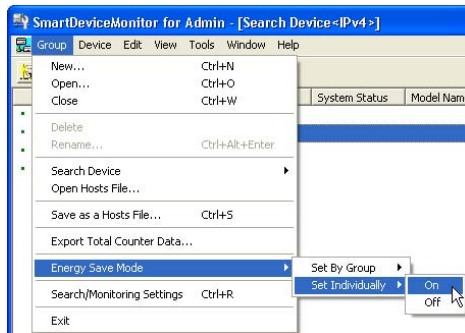
Select the protocol of the machine whose configuration you want to change.

If you are using IPv4 SNMPv3, enter the user authentication.

3. Select the machine whose settings you want to make.

To make settings for all machines in the selected group, select no machine.

4. Click the [Group] menu, point to [Energy Save Mode], [Set Individually], and then click [On].



To select all the machines in the group, select [Set By Group].

To disable Energy Save mode, click [Off].

5. Quit SmartDeviceMonitor for Admin.

Note

- For details about the setting for Energy Saver mode, see SmartDeviceMonitor for Admin Help.

Setting a Password

Follow the procedure below to set a password.

1. Start SmartDeviceMonitor for Admin.
2. On the [Group] menu, point to [Search Device], and then click [IPv4], [IPX/SPX] or [IPv4 SNMPv3].

A list of machines using the selected protocol appears.

Select the protocol of the machine whose configuration you want to change.

If you are using IPv4 SNMPv3, enter the user authentication.

3. In the list, select a machine whose configuration you want to change.
4. On the [Tools] menu, click [NIB Setup Tool].



4

A Web browser opens and the dialog box for entering the login user name and password for the Web Image Monitor administrator appears.

NIB Setup Tool starts when the network interface board is default. Follow the instructions on the screen.

5. Enter the login user name and password, and then click [Login].
For details about the user name and password, consult your network administrator.
6. Click [Configuration].
7. Click [Program/Change Administrator] on the [Device Settings] area, and then change the settings.
8. Click [OK].
9. Click [Logout].
10. Quit Web Image Monitor.
11. Quit SmartDeviceMonitor for Admin.

↓ Note

- For details about login user names and passwords, see Security Reference, which is the administrator's manual.

Checking the Machine Status

Follow the procedure below to check machine status.

1. Start SmartDeviceMonitor for Admin.
2. On the [Group] menu, point to [Search Device], and then click [IPv4], [IPX/SPX] or [IPv4 SNMPv3].

A list of machines using the selected protocol appears.

Select the protocol of the machine whose configuration you want to change.

If you are using TCP/IP SNMPv3, enter the user authentication.

3. Click the [View] menu, and then click [Select List Columns].
4. From [Device] in the [Select List Columns] dialog box, select the items you want to display, and then click [Add].
Selected items will move to [Show].
5. Move all the items you want to display, and then click [OK].
An icon in the list indicates the machine's status.
6. For information about a machine's status, select the machine you want to know about, and then click [Open] in the [Device Settings] menu.
The dialog box of the selected machine appears.
7. Click the application whose status you want to view.
The machine's status is displayed.
8. Quit SmartDeviceMonitor for Admin.

↓ Note

- For details about items in the dialog box, see SmartDeviceMonitor for Admin Help.

Changing Names and Comments

Follow the procedure below to change the names and comments of the machine.

1. Start SmartDeviceMonitor for Admin.
2. On the [Group] menu, point to [Search Device], and then click [IPv4], [IPX/SPX] or [IPv4 SNMPv3].
A list of machines using the selected protocol appears.
Select the protocol of the machine whose configuration you want to change.
If you are using IPv4 SNMPv3, enter the user authentication.
3. Select a machine in the list, and then click [NIB Setup Tool] on the [Tools] menu.
A Web browser opens and the window for entering the login user name and password for the Web Image Monitor administrator appears.
NIB Setup Tool starts when the network interface board is default. Follow the instructions on the screen.
4. Enter the login user name and password, and then click [Login].
For details about the login user name and password, consult your network administrator.
5. Click [Configuration].
6. Click [System] on the [Device Settings] area, and then change the settings.
7. Click [OK].
8. Click [Logout].

9. Quit Web Image Monitor.

10. Quit SmartDeviceMonitor for Admin.

Note

- In the [Device Name] box, enter a device name on the machine using up to 31 characters.
- In the [Comment] box, enter a comment on the machine using up to 31 characters.
- For details about login user names and passwords, see Security Reference, which is the administrator's manual.
- For details about Web Image Monitor, see "Using Web Image Monitor".

Reference

- p.137 "Using Web Image Monitor"

Load Fax Journal

1. Start SmartDeviceMonitor for Admin.

2. On the [Group] menu, point to [Search Device], and then click [IPv4], [IPX/SPX] or [IPv4 SNMPv3].

A list of machines using the selected protocol appears.

Select the protocol of the machine whose configuration you want to change.

If you are using IPv4 SNMPv3, enter the user authentication.

3. Select a machine in the list, and then click [Load Fax Journal] on the [Tools] menu.

A Web browser opens and the window for entering the login user name and password for the Web Image Monitor administrator appears.

4. Enter the login user name and password, and then click [Login].

For details about the login user name and password, consult your network administrator.

[Fax Journal] area appears in the Web Image Monitor.

5. Click [Logout].

6. Quit Web Image Monitor.

7. Quit SmartDeviceMonitor for Admin.

Note

- For details, see Help in Fax Journal area.
- For details about login user names and passwords, see Security Reference, which is the administrator's manual.
- For details about Web Image Monitor, see "Using Web Image Monitor".

Reference

- p.137 "Using Web Image Monitor"

Viewing and Deleting Spool Print Jobs

1. **Start SmartDeviceMonitor for Admin.**
2. **On the [Group] menu, point to [Search Device], and then click [IPv4], [IPX/SPX] or [IPv4 SNMPv3].**
A list of machines using the selected protocol appears.
Select the protocol of the machine whose configuration you want to change.
If you are using IPv4 SNMPv3, enter the user authentication.
3. **Select a machine in the list, and then click [Spool Printing Job List(Printer)] on the [Tools] menu.**
A Web browser opens and the dialog box for entering the login user name and password for the Web Image Monitor administrator appears.
4. **Enter the login user name and password, and then click [Login].**
For details about the login user name and password, consult your network administrator.
[Spool Printing Job List] appears in the Web Image Monitor.
5. **Click [Logout].**
6. **Quit Web Image Monitor.**
7. **Quit SmartDeviceMonitor for Admin.**

Note

- To display Spool Printing Job List, [Spool Printing] must be set to [Active] on Web Image Monitor in advance.
- To delete the Spool Printing Job, select the document you want to delete and then click [Delete].
- For details, see Help in the [Spool Printing Job List] area.
- For details about login user names and passwords, see Security Reference, which is the administrator's manual.
- For details about Web Image Monitor, see "Using Web Image Monitor".

Reference

- p.137 "Using Web Image Monitor"

Managing Address Information

1. **Start SmartDeviceMonitor for Admin.**

2. On the [Group] menu, point to [Search Device], and then click [IPv4], [IPX/SPX] or [IPv4 SNMPv3].

A list of machines using the selected protocol appears.

Select the protocol of the machine whose configuration you want to change.

If you are using IPv4 SNMPv3, enter the user authentication.

3. Select a machine in the list, and then click [Address Management Tool] on the [Tools] menu.

The dialog box for entering the login user name and password appears.

4. Enter the login user name and password, and then click [OK].

For details about the login user name and password, consult your network administrator.

[Address Management Tool] starts. Make the necessary settings.

5. Click [Exit].

6. Quit SmartDeviceMonitor for Admin.

 **Note**

- For details, see Address Management Tool Help.
- For details about login user names and passwords, see Security Reference, which is the administrator's manual.

Using SmartDeviceMonitor for Client

To view the status of machines using SmartDeviceMonitor for Client, configure SmartDeviceMonitor for Client beforehand.

Monitoring Printers

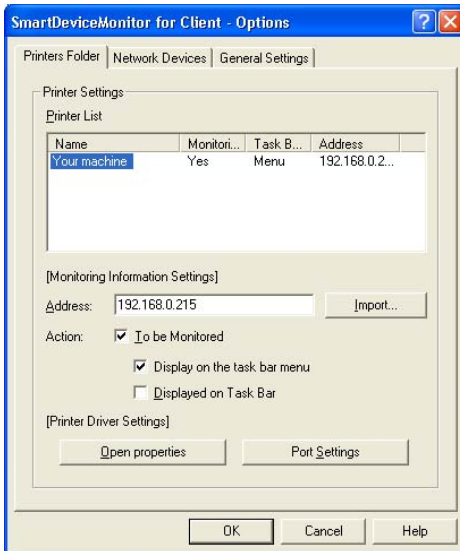
Follow the procedure below to monitor the machine using SmartDeviceMonitor for Client.

1. Right-click the SmartDeviceMonitor for Client icon, point to [Properties], and then click [Monitor Device Settings...].



The [SmartDeviceMonitor for Client - Options] dialog box appears.

2. On the [Printers Folder] tab, select the machine you want to monitor, and then select the [To be Monitored] check box in the Monitoring Information Settings area.



To display the machine status on the task bar, you must first select the [To be Monitored] check box, and then select the [Displayed on Task Bar] check box.

3. Click [OK].

The dialog box closes and the configured machine is monitored.

Note

- For details about status icons, see SmartDeviceMonitor for Client Help.

Checking the Machine Status

Follow the procedure below to check machine status using SmartDeviceMonitor for Client.

1. Right-click the SmartDeviceMonitor for Client icon, and then click the machine.



The machine status appears in the dialog box.

Note

- For details about items in the dialog box, see SmartDeviceMonitor for Client Help.

When Using IPP with SmartDeviceMonitor for Client

When using IPP with SmartDeviceMonitor for Client, note the following:

- The network printer can only receive one print job from SmartDeviceMonitor for Client at a time. While the network printer is printing, another user cannot access it until the job is finished. In this case, SmartDeviceMonitor for Client tries to access the network printer until the retry interval expires.
- If SmartDeviceMonitor for Client cannot access the network printer and times out, it will stop sending the print job. In this case, you should cancel the paused status from the print queue window. SmartDeviceMonitor for Client will resume access to the network printer. You can delete the print job from the print queue window, but canceling a print job printed by the network printer might cause the next job sent from another user to be incorrectly printed.
- If a print job sent from SmartDeviceMonitor for Client is interrupted and the network printer cancels the job because something went wrong, send the print job again.
- Print jobs sent from another computer do not appear in the print queue window, regardless of protocol.
- If various users send print jobs using SmartDeviceMonitor for Client to network printers, the printing order might not be the same as that in which the jobs were sent.
- An IP address cannot be used for the IPP port name because the IP address is used for the SmartDeviceMonitor for Client port name.

- When setting SSL, a protocol for encrypted communication, under environment which server authentication is issued, enter "https://(machine's IP address or host name)/ ". Internet Explorer must be installed on your computer. Use the highest version. Internet Explorer 6.0 or higher is recommended.
- If the [Security Alert] dialog box appears when accessing the machine using IPP to create or configure an IPP port, or when printing, install the certificate. To select the certificate store location when using Certificate Import Wizard, click [Place all certificates in the following store], and then click [Local Computer] under [Trusted Root Certification Authorities].

 **Note**

- For details about SSL settings, consult your network administrator.

Printer Status Notification by E-Mail

Whenever a paper tray becomes empty or paper is jammed, an e-mail alert is issued to the registered addresses to notify the printer status.

For this notification, you can make the e-mail notification settings.

Notification timing and e-mail content can be set.

★ Important

- **Depending on your e-mail application, a phishing warning might appear after you receive an e-mail message. To prevent phishing warnings appearing after you receive e-mail from a specified sender, you must add the sender to your e-mail application's exclusion list. For details about how to do this, see your e-mail application's Help.**

4

The e-mail notification functions you can set are as follows:

- Auto e-mail notification
Information including the machine status is automatically sent by e-mail. Before you use this function, register the e-mail address to be used.
- On-demand e-mail notification
Information including the machine status is sent by e-mail when a request from the administrator is received.

The information that can be notified by auto e-mail notification is as follows:

- Call Service
- Out of Toner
- Toner Almost Empty
- Paper Misfeed
- Cover Open
- Out of Paper
- Almost Out of Paper
- Paper Tray Error
- Output Tray Full
- Unit Connection Error
- Duplex Unit Error
- Waste Toner Bottle is Full
- Waste Toner Bottle is Almost Full
- Add Staples
- Hole Punch Receptacle is Full

- File Storage Memory Full Soon
- Log Error
- Device Access Violation
- Replacement Required: Unit
- Replacement Required Soon: Unit

1. Log on to Web Image Monitor in administrator mode.

2. In the menu area, click [Configuration].

3. Click [E-mail] on the [Device Settings] area.

4. Make the following settings:

- Items in the Reception column: Make the necessary settings for sending and receiving e-mail.
- Items in the SMTP column: Configure the SMTP server. Check your mailing environment, and then specify the necessary items. You can also perform mail authentication for the SMTP server.
- Items in the POP before SMTP column: Configure the POP server. Check your mailing environment, and then specify the necessary items. You can also perform mail authentication for the POP server.
- Items in the POP3/IMAP4 column: Configure the POP3 or IMAP4 server. Check your mailing environment, and then specify the necessary items.
- Items in the E-mail Communication Port column: Configure the port to be used for access to the mail server.
- Items in the Fax E-Mail Account column: Specify these items if you want to use on-demand e-mail notification.
- Items in the E-mail Notification Account column: Specify these items if you want to use e-mail notification.

5. Click [OK].

6. Click [Logout].

7. Quit Web Image Monitor.

Note

- For details about login user name and password, see Security Reference, which is the administrator's manual.
- For details about the settings, see Web Image Monitor Help.
- For details about Web Image Monitor, see "Using Web Image Monitor".

Reference

- p.137 "Using Web Image Monitor"

Setting the Account for E-mail Notification

Before you use Auto E-mail Notification or On-demand E-mail notification, setup an e-mail account to be used for the function. Perform the following configuration task in Web Image Monitor.

1. Log on to Web Image Monitor in administrator mode.
2. Click [Configuration] in the menu area, and then click [E-mail] on the [Device Settings] area.
3. Make the following settings in E-mail Notification Account:
 - E-mail Notification E-mail Address: Enter the address using alphanumeric characters.
 - Receive E-mail Notification: Specify whether to use on-demand e-mail notification.
 - E-mail Notification User Name: Enter the administrator's user name as the mail originator name.
 - E-mail Notification Password: Enter the password of the mail notification user.
4. Click [OK].
5. Click [Logout].
6. Quit Web Image Monitor.

↓ Note

- The user name and e-mail address that is already registered as e-mail destination cannot be specified as the recipient of e-mail notification.

Mail Authentication

You can configure mail authentication to prevent illegal use of the mail server.

SMTP Authentication

Specify SMTP authentication.

When mail is sent to the SMTP server, authentication is performed using the SMTP AUTH protocol by prompting the mail originator to enter the user name and password. This prevents illegal use of the SMTP server.

1. Log on to Web Image Monitor in administrator mode.
2. Click [Configuration] in the menu area, and then click [E-mail] on the [Device Settings] area.
3. Make the following settings in SMTP column:
 - SMTP Server Name: Enter the IP address or host name of the SMTP server.
 - SMTP Port No.: Enter the port number used when sending e-mail to the SMTP server.
 - SMTP Authentication: Enable or disable SMTP authentication.
 - SMTP Auth. E-mail Address: Enter the e-mail address.
 - SMTP Auth. User Name: Enter the SMTP account name.

- SMTP Auth. Password: To set or change the password for SMTP AUTH.
- SMTP Auth. Encryption: Select whether to encrypt the password or not.
Encryption-Auto Select: If the authentication method is PLAIN, LOGIN, CRAM-MD5, or DIGEST-MD5.
Encryption-Active: If the authentication method is CRAM-MD5 or DIGEST-MD5.
Encryption-Inactive: If the authentication method is PLAIN or LOGIN.

4. Click [OK].
5. Click [Logout].
6. Quit Web Image Monitor.

POP before SMTP Authentication

Select whether to log on to the POP3 server before sending e-mail.

1. Log on to Web Image Monitor in administrator mode.
2. Click [Configuration] in the menu area, and then click [E-mail] on the [Device Settings] area.
3. Make the following settings in POP before SMTP column:
 - POP before SMTP: Enable or disable POP before SMTP.
 - POP E-mail Address: Enter the e-mail address.
 - POP User Name: Enter the POP account name.
 - POP Password: To set or change the POP password.
 - Timeout setting after POP Auth.: Enter the time available before connecting to the SMTP server after logging on to the POP server.
4. Click [OK].
5. Click [Logout].
6. Quit Web Image Monitor.

Auto E-mail Notification

1. Log on to Web Image Monitor in administrator mode.
2. Click [Configuration] in the menu area, and then click [Auto E-mail Notification] on the [Device Settings] area.

The dialog box for making notification settings appears.

3. Make the following settings:
 - Notification Message: You can set this according to your needs, for example, the machine's location, service representative contact information.
 - Items in the Groups to Notify column: E-mail notification addresses can be grouped as required.

- Items in the Select Groups/Items to Notify column: Select groups for each notification type, such as machine status and error.

To make detailed settings for these items, click [Edit] next to [Detailed Settings of Each Item].

4. Click [OK].
5. Click [Logout].
6. Quit Web Image Monitor.

 **Note**

- For details about Web Image Monitor, see "Using Web Image Monitor".
- For details about the settings, see Web Image Monitor Help.

 **Reference**

- p.137 "Using Web Image Monitor"

On-demand E-mail Notification

1. Log on to Web Image Monitor in administrator mode.
2. Click [Configuration] in the menu area, and then click [On-demand E-mail Notification] on the [Device Settings] area.

The dialog box for making notification settings appears.

3. Make the following settings:

- Notification Subject: Enter a text string to be added to the subject line of return e-mails.
- Notification Message: You can set this according to your needs, for example, the machine's location, service representative contact information.
- Restriction to Device Status Info.: Select whether or not to allow access to the information such as the machine settings and status.
- Items in the Receivable E-mail Address/Domain Name Settings column: Enter an e-mail address or domain name to use for requesting information by e-mail and to receive its return e-mail.

4. Click [OK].
5. Click [Logout].
6. Quit Web Image Monitor.

 **Note**

- For details about Web Image Monitor, see "Using Web Image Monitor".
- For details about the settings, see Web Image Monitor Help.

 **Reference**

- p.137 "Using Web Image Monitor"

Format of On-demand E-mail Messages

To use mail notification, you need to send an on-demand e-mail message to this machine.

Using your mail software, enter the following:

Item	Description
Subject (Referred to as Subject)	Enter "requeststatus".
From (Referred to as From)	Specify a valid mail address. The device information will be sent to the address specified here.

 **Note**

- A mail message must be within 1 MB in size.
- E-mail may be incomplete if sent immediately after power on.
- The subject is not case sensitive.
- The body of a request e-mail has no meaning. Any text written in the e-mail body is ignored.

Remote Maintenance by telnet

★ Important

- Remote Maintenance should be protected so that access is allowed to administrators only.
- The password is the same as the one of Web Image Monitor administrator. When the password is changed using “mshell”, other's change also.

Using telnet

4

Follow the procedure below to use telnet.

★ Important

- Only one user at a time can log on to perform remote maintenance.
- If you are using Windows Vista, you must enable the telnet server and telnet client beforehand.

1. Use the IP address or the host name of the machine to start telnet.

```
% telnet "IP address"
```

2. Enter your user name and password.

For details about the user name and password, consult your network administrator.

For user authentication, enter a login user name and password.

For user code authentication, enter a user code in User Name.

3. Enter a command.

4. Quit telnet.

```
msh> logout
```

The configuration message about saving the changes appears.

5. Enter “yes” to save the changes, and then press the [Enter] key.

If you do not want to save the changes, enter “no”, and then press the [Enter] key. To make further changes, enter “return” at the command line, and then press the [Enter] key.

↓ Note

- If the message “Can not write NVRAM information” appears, the changes are not saved. Repeat the procedure above.
- When the changes are saved, the network interface board is reset automatically with that changes.
- When the network interface board resets, the print job in print process will be printed. However, print jobs in queue will be canceled.

access

Use the “access” command to view and configure access control. You can also specify two or more access ranges.

View settings

```
msh> access
```

IPv4 configuration display

```
msh> access ID range
```

IPv6 configuration display

```
msh> access ID range6
```

IPv6 access mask configuration display

```
msh> access ID mask6
```

IPv4 configuration

```
msh> access ID range “start-address end-address”
```

Example: to specify accessible IPv4 addresses between 192.168.0.10 and 192.168.0.20:

```
msh> access 1 range 192.168.0.10 192.168.0.20
```

IPv6 configuration

```
msh> access ID range6 “start-address end-address”
```

Example: to specify accessible IPv6 addresses between 2001:DB8::100 and 2001:DB8::200.

```
msh> access 1 range6 2001:DB8::100 2001:DB8::200
```

IPv6 access mask configuration

```
msh> access ID mask6 “base-address prefixlen”
```

Example: to specify accessible IPv6 addresses to 2001:DB8::/32

```
msh> access 1 mask6 2001:DB8:: 32
```

Access control initialization

```
msh> access flush
```

- Use the “flush” command to restore the default settings so that all access ranges become “0.0.0.0” for IPv4, and “::” for IPv6.

Note

- You can specify each IPv6 entry by either range or mask. For the range parameter, you can select “start-address end-address”. For the mask parameter, you can select “baseaddress prefixlen”.
- The access range restricts computers from use of the machine by IP address. If you do not need to restrict printing, make the setting “0.0.0.0” for IPv4, and “::” for IPv6.
- Valid ranges must be from lower (start address) to higher (end address).

- For IPv4 and IPv6, you can select an ID number between 1 and 5.
- IPv6 can register and select the range and the mask for each access ranges.
- IPv6 mask ranges between 1 - 128 can be selected.
- Up to five access ranges can be specified. The entry is invalid if the target number is omitted.
- You cannot send print jobs, or access Web Image Monitor and diprint from a restricted IP address.

appletalk

Use the "appletalk" command to view and configure AppleTalk parameters.

View settings

```
msh> appletalk
```

- [2] means "active" and [0] means "inactive".
- The default is [2].

Changing PAP timeout configuration

```
msh> appletalk ptimeout value > 0
```

- Timeout value becomes effective.

```
msh> appletalk ptimeout value = 0
```

- Timeout value becomes ineffective.

authfree

Use the "authfree" command to view and configure AuthFree parameters.

View settings

The following command displays the current AuthFree settings:

```
msh> authfree
```

- If print job authentication exclusion is not set, authentication exclusion control cannot be displayed.

IPv4 address settings

```
msh> authfree "ID" range_addr1 range_addr2
```

IPv6 address settings

```
msh> authfree "ID" range6_addr1 range6_addr2
```

IPv6 address mask configuration

```
msh> authfree "ID" mask6_addr1 masklen
```

Parallel/USB settings

```
msh> authfree [parallel | usb] [on|off]
```

- To enable authfree, set to on. To disable authfree, set to off. Always specify the interface.

Authentication exclusion control initialization

```
msh> authfree flush
```

autonet

Use the “autonet” command to configure AutoNet parameters.

View settings

The following command displays the current AutoNet settings:

```
msh> autonet
```

Configuration

You can configure AutoNet settings.

```
msh> autonet {on|off}
```

- {on} means “active” and {off} means “inactive”.

Current interface priority configuration display

```
msh> autonet priority
```

Interface priority configuration

```
msh> autonet priority “interface_name”
```

- You can give interface's AutoNet parameter priority.
- Priority settings are available when multiple interfaces are installed.
- wlan can be specified only when the IEEE 802.11 interface is installed.

Interface	Interface configured
ether	Ethernet interface
wlan	IEEE 802.11 interface

Note

- If an interface is not selected, the current interface connection settings remain in effect.
- For details about AutoNet, refer to autonet parameters.

bonjour

Use the “`bonjour`” command to display `bonjour`-related settings.

View settings

Bonjour settings are displayed.

```
msh> bonjour
```

Bonjour service name setting

You can specify the `bonjour` service name.

```
msh> bonjour cname “computer name”
```

- The computer name can be entered using up to 63 alphanumeric characters.
- If you do not specify a character string, the current setting is displayed.

Bonjour Installation location information setting

You can enter information about the location where the printer is installed.

```
msh> bonjour location “location”
```

- Information about location can be entered using up to 32 alphanumeric characters.
- If you do not specify a character string, current setting is displayed.

Setting order of priority for each protocol

- `msh> bonjour dprint [0-99]`
- `msh> bonjour lpr [0-99]`
- `msh> bonjour ipp [0-99]`

You can specify the order of priority for “`dprint`”, “`lpr`”, and “`ipp`”. Smaller numbers indicate higher priority.

IP TTL setting

```
msh> bonjour ip ttl [1-255]
```

You can specify the IP TTL (the number of routers a packet can pass through).

- The default is 255.

Resetting the computer name and location information

You can reset the computer name and location information.

```
msh> bonjour clear {cname|location}
```

- `cname`: Reset the computer name. The default computer name will be displayed when the computer is restarted.
- `location`: Reset the location information. The previous location information will be deleted.

Interface configuration

```
msh> bonjour linklocal “interface_name”
```

- If you do not specify an interface, the Ethernet interface is selected automatically.
- If many types of interface are installed, configure the interface that communicates with linklocal address.
- If you do not specify an interface, the Ethernet interface is automatically selected.
- wlan can be specified only when the IEEE 802.11 interface is installed.

Interface	Interface configured
ether	Ethernet interface
wlan	IEEE 802.11 interface

Setting IPP-SSL printing

```
msh> bonjour ippport {ipp|ssl}
```

- If IPP-SSL Printing is set to ssl, the IPP port number will appear as 443, and IPP-SSL printing can be performed with higher security.
- If IPP-SSL Printing is set to ipp, the IPP port number will appear as 631. Port 631 is the port for normal IPP printing.

btconfig

Use the “btconfig” command to make Bluetooth settings.

View settings

Bluetooth settings are displayed.

```
msh> btconfig
```

Mode settings

You can set the Bluetooth operation mode to {private} or {public}.

```
msh> btconfig {private|public}
```

- The default is {public}.

devicename

Use the “devicename” command to display and change the printer name.

View settings

```
msh> devicename
```

Printer name configuration

```
msh> devicename name “string”
```

- Enter a printer name using up to 31 alphanumeric characters.
- Set single names for each printer.

Printer name initialization

```
msh> devicename clear name
```

- Reset the printer name to its default.

dhcp

Use the “dhcp” command to configure DHCP settings.

View settings

The following command displays the current DHCP settings.

```
msh> dhcp
```

Configuration

You can configure DHCP.

```
msh> dhcp “interface_name” {on|off}
```

- Click {on} to enable dhcp. Click {off} to disable DHCP.
- If the DNS server address and domain name are obtained from DHCP, be sure to click {on}.
- wlan can be specified only when the IEEE 802.11 interface is installed.

Interface name	Interface configured
ether	Ethernet interface
wlan	IEEE 802.11 interface

Current interface priority configuration display

```
msh> dhcp priority
```

Interface priority configuration

```
msh> dhcp priority “interface_name”
```

- You can select which interface has DHCP parameter priority.
- Priority settings are available when multiple interfaces are installed.

DNS server address selection

```
msh> dhcp dnsaddr {dhcp|static}
```

- Specify whether to obtain the DNS server address from the DHCP server or use the address set by a user.

- To obtain the DNS server address from the DHCP server, specify "dhcp". To use the address set by a user, specify "static".

Domain name selection

```
msh> dhcp domainname {dhcp|static}
```

- Specify whether to obtain the domain name from the DNS server or use the domain name set by a user.
- To obtain the domain name from the DHCP server, specify "dhcp". To use the domain name set by a user, specify "static".

Reference

- p.331 "Using DHCP"

dhcp6

Use the "dhcp6" command to display or configure DHCPv6 settings.

View settings

The following command displays the current DHCPv6 settings.

```
msh> dhcp6
```

DHCPv6-lite configuration and display

```
msh> dhcp6 "interface_name" lite {on|off}
```

Viewing and specifying DNS server address selection (obtained from the dhcpv6 server/user specified value)

```
msh> dhcp6 dnsaddr {dhco|static}
```

DUID(DHCP unique ID) deletion and display

```
msh> dhcp6 duid clear
```

Viewing and specifying the time required to re-obtain the parameter obtained from dhcpv6

```
msh> dhcp6 ooption lifetime [0-65535]
```

- It can be entered between 0 and 65535 minutes.
- The default is 60 minutes.
- If you specify "0", you cannot re-obtain the value.

diprint

The direct printing port enables direct printing from a network-connected computer.

Use the "diprint" command to change direct printing port settings.

View settings

The following command displays the current direct printing port settings:

```
msh> diprint
```

Example output:

```
port 9100
timeout=300(sec)
bidirect on
conn multi
apl async
```

- The “port” specifies the port number of the direct printing port.
- The “bidirect” setting indicates whether the direct printing port is bidirectional or not.

Setting timeout

```
msh> diprint timeout [30-5535]
```

- You can specify the timeout interval to use when the printer is expecting data from the network.
- The default is 300 seconds.
- This command functions in conjunction with the “lpr” command.

Specifying the number of concurrent connections

```
msh> diprint conn {multi|single}
```

- The above command specifies the number of concurrent diprint connections. Specify “multi” for multiple connections or “single” for a single connection.
- The default is “multi”.

dns

Use the “dns” command to configure or display DNS (Domain Name System) settings.

View settings

The following command displays current DNS settings:

```
msh> dns
```

IPv4 DNS server configuration

The following command enables or disables the IPv4 DNS server address:

```
msh> dns “ID” server “server address”
```

The following command displays a configuration using the IP address 192.168.15.16 on a DNS 1 server:

```
msh> dns 1 server 192.168.15.16
```

- You can register IPv4 DNS Server address.
- You can select an ID number between 1 and 3. You can select up to three ID numbers.
- You cannot use "255.255.255.255" as the DNS server address.

IPv6 DNS server configuration

The following command enables or disables the IPv4 DNS server address:

```
msh> dns "ID" server6 "server address"
```

- You can register IPv6 DNS Server address.
- The selectable ID number is between 1 and 3. You can select up to 3 ID.

Dynamic DNS function setting

```
msh> dns "interface_name" ddns {on|off}
```

- You can set the dynamic DNS function "active" or "inactive".
- {on} means "active" and {off} means "inactive".
- wlan can be specified only when the IEEE 802.11 interface is installed.

Interface name	Interface configured
ether	Ethernet interface
wlan	IEEE 802.11 interface

4

Specifying the record overlap operation

```
msh> dns overlap {update|add}
```

- You can specify operations performed when records overlap.
- update: To delete old records and register new records.
- add: To add new records and store the old records.
- When CNAME overlaps, it is always changed, irrespective of settings.

CNAME registration

```
msh> dns cname {on|off}
```

- You can specify whether to register CNAME.
- {on} means "active" and {off} means "inactive".
- The CNAME registered is the default name beginning with rnp. CNAME cannot be changed.

A records registration

```
msh> dns arecord {dhcp|own}
```

- dhcp: You can specify the method of registering an A record when the dynamic DNS function is enabled and DHCP is used.
- own: To register an A record using the printer as the DNS client.

The DNS server address and the domain name already designated are used for the registration.

Record updating interval settings

```
msh> dns interval [1-255]
```

- You can specify the interval after which records are updated when using the dynamic DNS function.
- The updating interval is specified hourly. It can be entered between 1 and 255 hours.
- The default is 24 hours.

resolv.conf display

```
msh> dns resolv
```

Specifying the protocol when asking names during dual stacking

```
msh> dns resolv protocol {ipv4|ipv6}
```

- Appears during dual stacking only.

4

domainname

Use the “domainname” command to display or configure the domain name settings.

You can configure the Ethernet interface, or IEEE 802.11 interface.

View settings

The following command displays the current domain name:

```
msh> domainname
```

Interface domain configuration

```
msh> domainname “interface_name”
```

Setting the Domain Name

```
msh> domainname “interface_name” name “domain name”
```

- A domain name can be entered using up to 63 alphanumeric characters.
- The Ethernet interface and IEEE 802.11 interface will have the same domain name.
- wlan can be specified only when the IEEE 802.11 interface is installed.

Interface	Interface set
ether	Ethernet interface
wlan	IEEE 802.11 interface

Deleting the Domain Name

```
msh> domainname “interface_name” clear name
```

etherauth

Use the "etherauth" command to display or modify the authentication related parameters for Ethernet.

View settings

```
msh> etherauth
```

802.1x Configuration

```
msh> etherauth 8021x {on|off}
```

- {on} means "active" and {off} means "inactive".

etherconfig

Use the "etherconfig" command to view and configure the Ethernet parameters.

View settings

```
msh> etherconfig
```

Specify Ethernet Speed

```
msh> etherconfig speed {auto|10f|10h|100f|100h}
```

- auto=Auto Select
- 10f=10 Mbps Full Duplex
- 10h=10 Mbps Half Duplex
- 100f=100 Mbps Full Duplex
- 100h=100 Mbps Half Duplex

The default is "auto".

help

Use the "help" command to display the available command list and the procedures for using those commands.

Command list display

```
msh> help
```

Display of procedure for using commands

```
msh> help "command_name"
```

hostname

Use the "hostname" command to change the printer name.

View settings

```
msh> hostname
```

IPv4 Configuration

```
msh> hostname "interface_name" "printer_name"
```

- Enter the printer name using up to 63 alphanumeric characters.
- You cannot use a printer name beginning "RNP" (in either upper or lower case).
- The Ethernet interface and IEEE 802.11 interface will have the same printer name.
- wlan can be specified only when the IEEE 802.11 interface is installed.
- If you do not specify an interface, the Ethernet interface is selected automatically.

4

Interface name	Interface configured
ether	Ethernet interface
wlan	IEEE 802.11 interface

Initializing the printer name for each interface

```
msh>hostname "interface_name" clear name
```

ifconfig

Use the "ifconfig" command to view and configure TCP/IP (IP address, subnet mask, broadcast address, default gateway address) for the printer.

View settings

```
msh> ifconfig
```

IPv4 configuration

```
msh> ifconfig "interface_name" "parameter" "address"
```

- If you did not enter an interface name, it is automatically set to the Ethernet interface.
- wlan can be specified only when the IEEE 802.11 interface is installed.

Interface name	Interface configured
ether	Ethernet Interface
wlan	IEEE 802.11 Interface

The following explains how to configure an IPv4 address 192.168.15.16 on Ethernet interface.

```
msh> ifconfig ether 192.168.15.16
```

IPv6 configuration

```
msh> ifconfig ether inet6 "interface_name" "printer_name"
```

The following explains how to configure an IPv6 address to 2001:DB8::100 with prefix length 64 on the Ethernet interface.

```
msh> ifconfig ether inet6 2001:DB8::100 64
```

Netmask configuration

```
msh> ifconfig "interface_name" netmask "address"
```

The following explains how to configure a subnet mask 255.255.255.0 on Ethernet interface.

```
msh> ifconfig ether netmask 255.255.255.0
```

Broadcast address configuration

```
msh> ifconfig "interface_name" broadcast "address"
```

Changing the interface

```
msh> ifconfig "interface" up
```

- When using the optional IEEE 802.11 interface unit, you can specify either Ethernet or IEEE 802.11 interface.

Note

- To get the above addresses, contact your network administrator.
- Use the default configuration if you cannot obtain setting addresses.
- The IP address, subnet mask and broadcast address are the same as that for the Ethernet interface and IEEE 802.11 interface.
- TCP/IP configuration is the same for both Ethernet and IEEE 802.11 interface. If interfaces are changed, the new interface inherits the configuration.
- Use "0x" as the initial two letters of a hexadecimal address.

info

Use the "info" command to display printer information such as paper tray, output tray, and printer language.

Printer information display

```
msh> info
```

Reference

- p.218 "Getting Printer Information over the Network"

ipp

Use the "ipp" command to view and configure IPP settings.

View settings

The following command displays the current IPP settings:

```
msh> ipp
```

IPP timeout configuration

Specify how many seconds the computer waits before canceling an interrupted print job. The time can be entered between 30 to 65535 seconds.

```
msh> ipp timeout [30-65535]
```

IPP user authorization configuration

Use IPP user authorization to restrict users to print with IPP. The default is "off".

```
msh> ipp auth {basic|digest|off}
```

- User authorization settings are "basic" and "digest".
- If user authorization is specified, register a user name. You can register up to 10 users.

IPP user name configuration

Configure IPP users according to the following messages:

```
msh> ipp user
```

The following message appears:

```
msh> Input user number (1 to 10):
```

Enter the number, user name, and password.

```
msh> IPP user name:user1
```

```
msh> IPP :*****
```

After configuring the settings, the following message appears:

User configuration changed.

ipsec

Use the "ipsec" command to view and configure IPsec settings.

View settings

The following command displays the current IPsec settings:

```
msh> ipsec
```

Note

- For details about displayed contents, see Security Reference.

ipv6

Use the "ipv6" command to display and configure IPv6 settings.

View Setting

```
msh> ipv6
```

IPv6 stateless address

```
msh> ipv6 stateless {on|off}
```

If "on" is selected, IPv6 requests information required for maintaining stateful connection to the router for as long as the printer power is turned on. This setting allows information from the router to be obtained constantly, and periodically refreshes the effective period of the stateless address.

logout

Use "logout" command to quit telnet.

Quit telnet

```
msh> logout
```

A confirmation message appears.

```
{yes|no|return}
```

Enter [yes], [no] or [return] by typing the word, and then press the [Enter] key.

To save the changes and quit telnet, enter [yes].

To discard the changes and quit telnet, enter [no].

To continue making changes, enter [return]

lpr

Use the "lpr" command to view and configure LPR settings.

View Setting

```
msh> lpr
```

Checking host name when deleting the job

```
msh> lpr chkhost {on|off}
```

- The default is "on".

If "on" is selected, you can delete print jobs only from the IP address of the host that sent the print job.

If LPR is disabled, you can also delete print jobs sent from IP addresses other than that of the host.

Printer Error Detection Function

```
msh> lpr prnerrchk {on|off}
```

- The default is “off”.

If you set this to “on”, the printer stops receiving data and will wait until the error is resolved before continuing processing a job.

netware

Use the “netware” command to view and configure the NetWare settings such as the print server name or file server name.

NetWare Printer Server Names

```
msh> netware pnamecharacter string
```

- Enter the NetWare print server name using up to 47 characters.

NetWare File Server Names

```
msh> netware fname character string
```

- Enter the NetWare file server name using up to 47 characters.

Encap type

```
msh> netware encap {802.3|802.2|snap|ethernet2|auto}
```

Remote Printer Number

```
msh> netware rnum [0-254]
```

- The default is 0.

Timeout

```
msh> netware timeout [3-255]
```

- The default is 15.

Printer server mode

```
msh> netware mode pserver
```

```
msh> netware mode ps
```

Remote printer mode

```
msh> netware mode rprinter
```

```
msh> netware mode rp
```

NDS context name

```
msh> netware context “character string”
```

SAP interval

```
msh> netware “sap_interval[0-3600]”
```

It can be entered between 0 and 3600 seconds.

Setting login mode for file server

```
msh> netware login server
```

Setting login mode for NDS tree

```
msh> netware login tree
```

Setting login mode for NDS tree name

```
msh> netware tree "NDS tree name"
```

File transfer protocol

```
msh> netware trans {ipv4pri|ipxpri|ipv4|ipx}
```

- If you do not specify the protocol, the current setting is displayed.

Protocol	Set Protocol
ipv4pri	IPv4+IPX(IPv4)
ipxpri	IPv4+IPX(IPX)
ipv4	IPv4
ipx	IPX

4

passwd

Use the "passwd" command to change the remote maintenance password.

Changing the password

```
msh> passwd
```

- Enter the current password.
- Enter the new password.
- Reenter the new password to confirm it.

Changing the password of the administrators using the Supervisor

```
msh> passwd {Administrator ID}
```

- Enter the new password.
- Reenter the new password to confirm it.

Note

- Be sure not to forget or lose the password.
- The password can be entered using up to 32 alphanumeric characters. Passwords are case-sensitive. For example, "R" is not the same as "r".

pathmtu

Use the “pathmtu” command to display and configure the PathMTU Discovery service function.

View settings

```
msh> pathmtu
```

Configuration

```
msh> pathmtu {on|off}
```

- The default is “on”.
- If the MTU size of the sent data is larger than the router's MTU, the router will declare it impassable, and communication will fail. If this happens, selecting the “pathmtu” to “on” optimizes the MTU size and prevents data output failure.
- Depending on the environment, information might not be obtained from the router, and communication will fail. If this happens, select the “pathmtu” to “off”.

4

prnlog

Use the “prnlog” command to obtain printer log information.

Print logs display

```
msh> prnlog
```

- Display previous print jobs.

```
msh> prnlog “ID Number”
```

- Specify the ID number of the displayed print log information to display additional details about a print job.

Reference

- p.227 "Understanding the Displayed Information"

route

Use the “route” command to view and control the routing table.

Specified route information display

```
msh> route get “destination”
```

- Specify the IPv4 address to destination.
“0.0.0.0” cannot be specified as destination address.

Enabling/disabling specified IPv4 destination

```
msh> route active {host|net} “destination” {on|off}
```

- If you do not specify {host|net}, the host setting is automatically selected.

Adding IPv4 Routing Table

```
msh> route add {host|net} "destination" "gateway"
```

- Adds a host or network route to "destination", and a gateway address to "gateway" in the table.
- Specify the IPv4 address to destination and gateway.
- If you do not specify {host|net}, the host setting is selected automatically.
- You cannot specify "0.0.0.0" as the destination address.

Setting the Default IPv4 Gateway

```
msh> route add default "gateway"
```

Deleting specified IPv4 destination from Routing Table

```
msh> route delete {host|net} "destination"
```

- If you do not specify {host|net}, the host setting is automatically selected.
- IPv4 address of destination can be specified.

Setting IPv6 Default Gateway

```
msh> route add6 default gateway
```

Adding a specified IPv6 destination to Routing Table

```
msh> route add6 "destination" "prefixlen[1-128]" "gateway"
```

- Specify the IPv6 address to destination and gateway.
- If the prefix of the address is between 1 and 127, the network is selected. If the prefix of the address is 128, the host is selected.
- You cannot register a record that has the same destination and prefix as a registered record.
- You cannot register a record that uses "0000:0000:0000:0000:0000:0000:0000:0000" as its destination.

Deleting a specified IPv6 destination from Routing Table

```
msh> route delete6 "destination" "prefixlen"
```

- Specify the IPv6 address to destination and gateway.

Display information about a specified IPv6 route information

```
msh> route get6 "destination"
```

- Specify the IPv6 address to destination and gateway.

Enabling/disabling a specified IPv6 destination

```
msh> route active6 "destination" "prefixlen[1-128]" {on|off}
```

Route initialization

```
msh> route flush
```

Note

- The maximum number of IPv4 routing tables is 16.
- The maximum number of IPv6 routing tables is 2.
- Set a gateway address when communicating with devices on an external network.
- The same gateway address is shared by all interfaces.
- “Prefixlen” is a number between 1 and 128.

rhpp

4

Use the “rhpp” command to view and configure RHPP settings.

View settings

```
msh> rhpp
```

Changing rhpp port number

```
msh> rhpp [1024-65535]
```

- The default is 59100.

Setting timeout

```
msh> rhpp timeout [30-65535]
```

- The default is 300 seconds.

Note

- “RHPP” is an abbreviation of “Reliable Host Printing Protocol”, which is a manufacturer-original printing protocol.

set

Use the “set” command to set the protocol information display “active” or “inactive”.

View settings

The following command displays protocol information (active/inactive).

```
msh> set ipv4
```

```
msh> set ipv6
```

```
msh> set ipsec
```

```
msh> set appletalk
```

```
msh> set netware
```

```
msh> set smb
```

```
msh> set protocol
```

- When protocol is specified, information about TCP/IP, AppleTalk, NetWare and SMB appears.

```
msh> set lpr
msh> set lpr6
msh> set ftp
msh> set ftp6
msh> set rsh
msh> set rsh6
msh> set diprint
msh> set diprint6
msh> set web
msh> set snmp
msh> set ssl
msh> set ssl6
msh> set nrs
msh> set rfu
msh> set rfu6
msh> set ipp
msh> set ipp6
msh> set http
msh> set http6
msh> set bonjour
msh> set bonjour6
msh> set nbt
msh> set ssdp
msh> set ssh
msh> set sftp
msh> set sftp6
msh> set wsdev
msh> set wsdev6
msh> set wsprn
msh> set wsscn
msh> set rhpp
msh> set rhpp6
```

Configuration

- Enter “up” to enable protocol, and enter “down” to disable protocol.

You can set the protocol to “active” or “inactive”.

```
msh> set ipv4 {up|down}
```

- If you disable IPv4, you cannot use remote access after logging off. If you did this by mistake, you can use the control panel to enable remote access via IPv4.
- Disabling IPv4 also disables lpr, ftp, rsh, diprint, web, snmp, ssl, ipp, http, Bonjour, wsdev, and sftp.

```
msh> set ipv6 {up|down}
```

- If you disable IPv6, you cannot use remote access after logging off. If you did this by mistake, you can use the control panel to enable remote access via IPv6.
- Disabling IPv6 also disables lpr6, ftp6, rsh6, diprint6, ssl6, ipp6, http6, Bonjour6, wsdev6, and sftp6.

```
msh> set ipsec {up|down}
```

```
msh> set appletalk {up|down}
```

```
msh> set netware {up|down}
```

```
msh> set smb {up|down}
```

```
msh> set lpr {up|down}
```

```
msh> set lpr6 {up|down}
```

```
msh> set ftp {up|down}
```

```
msh> set ftp6 {up|down}
```

```
msh> set rsh {up|down}
```

```
msh> set rsh6 {up|down}
```

```
msh> set diprint {up|down}
```

```
msh> set diprint6 {up|down}
```

```
msh> set web {up|down}
```

```
msh> set snmp {up|down}
```

```
msh> set ssl {up|down}
```

```
msh> set ssl6 {up|down}
```

- If Secured Sockets Layer (SSL, an encryption protocol) function is not available for the printer, you cannot use the function by enabling it.

```
msh> set nrs {up|down}
```

```
msh> set rfu {up|down}
```

```
msh> set rfu6 {up|down}
```



```

msh> set ipp {up|down}
msh> set ipp6 {up|down}
msh> set http {up|down}
msh> set http6 {up|down}
msh> set Bonjour {up|down}
msh> set Bonjour6 {up|down}
msh> set ssh {up|down}
msh> set sstp {up|down}
msh> set nbt {up|down}
msh> set sftp {up|down}
msh> set sftp6 {up|down}
msh> set wsdev {up|down}
msh> set wsdev6 {up|down}

```

- If “wsdev” and “wsdev6” are enabled simultaneously, both appear as “up” on the protocol information display, but both use IPv4 for WSD (Device), WSD (Printer) and WSD (Scanner).

```

msh> set wsprn {up|down}
msh> set wsscn {up|down}
msh> set rhpp {up|down}
msh> set rhpp6 {up|down}

```

show

Use the “show” command to display network interface board configuration settings.

View settings

```
msh> show
```

- If “-p” is added, you can view settings one by one.

Reference

- p.227 "Understanding the Displayed Information"

slp

Use “slp” command to view and configure SLP settings.

```
msh> slp ttl "ttl_val[1-255]"
```

- You can search the NetWare server using SLP in the PureIP environment of NetWare 5/5.1. Using the “slp” command, you can configure the value of TTL which can be used by SLP multicast packet.
- The default value of TTL is 1. A search is executed only within a local segment. If the router does not support multicast, the settings are not available even if the TTL value is increased.
- The acceptable TTL value is between 1 and 255.

smb

Use the “smb” command to configure or delete the computer or workgroup name for SMB.

Computer name settings

```
msh> smb comp “computer name”
```

- Set computer name using up to 15 characters.
- Names beginning with “RNP” or “rnp” cannot be entered.

Working group name settings

```
msh> smb group “work group name”
```

- Set workgroup name using up to 15 characters.

Comment settings

```
msh> smb comment “comment”
```

- Set comment using up to 31 characters.

Notify print job completion

```
msh> smb notif {on|off}
```

- To notify print job completion, specify “on”. Otherwise, specify “off”.

Deleting computer name

```
msh> smb clear comp
```

Deleting group name

```
msh> smb clear group
```

Deleting comment

```
msh> smb clear comment
```

View protocol

```
msh> smb protocol
```

snmp

Use the “snmp” command to display and edit SNMP configuration settings such as the community name.

View settings

```
msh> snmp
```

- Default access settings 1 is as follows:
Community name:public
IPv4 address:0.0.0.0
IPv6 address::
IPX address:00000000:000000000000
Access type:read-only
Effective Protocol:IPv4/IPv6/IPX
- Default access settings 2 is as follows:
Community name:admin
IPv4 address:0.0.0.0
IPv6 address::
IPX address:00000000:000000000000
Access type:read-write
Effective Protocol:IPv4/IPv6/IPX
- If “-p” is added, you can view settings one by one.
- To display the current community, specify its registration number.

Display

```
msh> snmp ?
```

Community name configuration

```
msh> snmp “number” name “community_name”
```

- You can configure ten SNMP access settings numbered 1-10.
- The printer cannot be accessed from SmartDeviceMonitor for Admin or SmartDeviceMonitor for Client if “public” is not registered in numbers 1-10. When changing the community name, use SmartDeviceMonitor for Admin and SNMP Setup Tool to correspond with printer settings.
- The community name can be entered using up to 15 characters.

Deleting community name

```
msh> snmp “number” clear name
```

Access type configuration

```
msh> snmp “number” type “access_type”
```

Access type	Type of access permission
no	not accessible

Access type	Type of access permission
read	read only
write	read and write
trap	user is notified of trapmessages

Protocol configuration

Use the following command to set protocols “active” or “inactive”: If you set a protocol “inactive”, all access settings for that protocol are disabled.

```
msh> snmp {ipv4|ipv6|ipx} {on|off}
```

- Specify “ipv4” for IPv4, “ipv6” for IPv6, or “ipx” for IPX/SPX.
- {on} means “active” and {off} means “inactive”.
- All protocols cannot be turned off concurrently.

Configuration of protocol for each registration number

```
msh> snmp “number” active {ipv4|ipv6|ipx} {on|off}
```

- To change the protocol of access settings, use the following command. However, if you have disabled a protocol with the above command, activating it here has no effect.

Access configuration

```
msh> snmp “number” {ipv4|ipv6|ipx} “address”
```

- You can configure a host address according to the protocol used.
- The network interface board accepts requests only from hosts that have IPv4, IPv6, and IPX addresses with access types of “read-only” or “read-write”. Enter “0” to have network interface board accept requests from any host without requiring a specific type of access.
- Enter a host address to deliver “trap” access type information to.
- To specify IPv4 or IPv6, enter “ipv4” or “ipv6” followed by a space, and then the IPv4 or IPv6 address.
- To specify IPX/SPX, enter “ipx” followed by a space, the IPX address followed by a decimal, and then the MAC address of the network interface board.

sysLocation configuration

```
msh> snmp location
```

Deleting sysLocation

```
msh> snmp clear location
```

sysContact setting

```
msh> snmp contact
```

Deleting sysContact

```
msh> snmp clear contact
```

SNMP v1v2 function configuration

```
msh> snmp v1v2 {on|off}
```

- Specify “on” to enable, and “off” to disable.

SNMP v3 function configuration

```
msh> snmp v3 {on|off}
```

- Specify “on” to enable, and “off” to disable.

SNMP TRAP configuration

```
msh> snmp trap[v1|v2|v3] {on|off}
```

- Specify “on” to enable, and “off” to disable.

Remote Configuration Authorization configuration

```
msh> snmp remote {on|off}
```

- Specify “on” to enable, and “off” to disable the SNMP v1v2 setting.

SNMP v3 TRAP configuration display

```
msh> snmp v3trap
```

```
msh> snmp v3trap [1-5]
```

- If a number from 1 to 5 is entered, settings are displayed for that number only.

Configuring a sending address for SNMP v3 TRAP

```
msh> snmp v3trap [1-5] {ipv4|ipv6|ipx} “address”
```

Configuring a sending protocol for SNMP v3 TRAP

```
msh> snmp v3trap [1-5] active {ipv4|ipv6|ipx} {on|off}
```

Configuring a user account for SNMP v3 TRAP

```
msh> snmp v3trap [1-5] account “account_name”
```

- Enter an account name using up to 32 alphanumeric characters.

Deleting an SNMP v3 TRAP user account

```
msh> snmp v3trap [1-5] clear account
```

Configuring an SNMP v3 encryption algorithm

```
msh> snmp v3auth {md5|sha1}
```

Configuring SNMP v3 encryption

```
msh> snmp v3priv {auto|on}
```

- Set “auto” for automatic encryption configuration.

- If you select “on”, plain-text communication becomes impossible - only encrypted communication is possible.

Note

- “Encrypted communication” means an encrypted password is set on the machine.

sntp

The printer clock can be synchronized with a NTP server clock using Simple Network Time Protocol (SNTP). Use the “sntp” command to change SNTP settings.

View settings

```
msh> sntp
```

NTP IPv4 server address configuration

You can specify the IPv4 address of the NTP server.

```
msh> sntp server “IPv4_address”
```

NTP hostname configuration

You can specify the hostname of the NTP server.

```
msh> sntp server “hostname”
```

Deleting NTP server configuration

```
msh> sntp server clear
```

Interval configuration

```
msh> sntp interval “polling_time”
```

- You can specify the interval at which the printer synchronizes with the operator-specified NTP server. The default is 60 minutes.
- The interval can be entered from 0, or between 15 and 10,080 minutes.
- If you set 0, the printer synchronizes with the NTP server only when you turn the printer on. After that, the printer does not synchronize with the NTP server.

Time-zone configuration

```
msh> sntp timezone “±hour_time”
```

- You can specify the time difference between the printer clock and NTP server clock. The values are between -12:00 and +13:00.

Note

- You can only select either the address or host name for the ntp server.

spoolsw

Use the “spoolsw” command to view and configure Job Spool settings.

You can only specify diprint, trap, lpr, ipp, ftp, sftp, wsd (printer), and smb (TCP/IP) protocol.

- The “spoolsw” command for configuring Job Spool settings is available only when the optional hard disk is installed.

View settings

The Job Spool setting appears.

```
msh> spoolsw
```

Job Spool setting

```
msh> spoolsw spool {on|off}
```

- Specify “on” to enable Job Spool, or “off” to disable it.

Resetting Job spool setting

```
msh> spoolsw clear job {on|off}
```

- When the printer power is cut during job spooling, this determines whether to reprint the spooled job.

Protocol configuration

```
msh> spoolsw diprint {on|off}
```

```
msh> spoolsw lpr {on|off}
```

```
msh> spoolsw ipp {on|off}
```

```
msh> spoolsw smb {on|off}
```

```
msh> spoolsw ftp {on|off}
```

```
msh> spoolsw sftp {on|off}
```

```
msh> spoolsw wsprn {on|off}
```

ssdp

Use the “ssdp” command to view and configure SSDP settings.

View settings

```
msh> ssdp
```

Setting effective time

```
msh> ssdp profile [1801-86400]
```

The default is 10800 seconds.

Advertise packet TTL settings

```
msh> sstp ttl [1-255]
```

The default is 4.

ssh

Use the “ssh” command to view and configure SSH settings.

View settings

```
msh> ssh
```

Data compression communication settings

```
msh> ssh compression {on|off}
```

The default is “on”.

SSH/SFTP communication port setting

```
msh> ssh port [22, 1024-65535]
```

The default is 22.

SSH/SFTP communication timeout setting

```
msh> ssh timeout [0-65535]
```

The default is 300.

SSH/SFTP communication login timeout setting

```
msh> ssh logintimeout [0-65535]
```

The default is 300.

Setting an open key for SSH/SFTP

```
msh> ssh genkey {512|768|1024} “character string”
```

Create an open key for SSH/SFTP communication.

Usable characters are ASCII 0x20-0x7e (32 bytes) other than “0”.

The default key length is 1024, and the character string is blank.

If you do not specify this parameter, an open key with the default value will be created.

Deleting open key for ssh/sftp communication

```
msh> ssh delkey
```

↓ Note

- If you do not specify a character string, current setting is displayed.
- ssh can be used only with sftp.

status

Use the “status” command to display the printer status.

View messages

```
msh> status
```

Reference

- p.218

syslog

Use the “syslog” command to display the information stored in the printer's system log.

View messages

```
msh> syslog
```

Reference

- p.239 "Message List"

upnp

Use the “upnp” command to display and configure the universal plug and play.

Public URL display

```
msh> upnp url
```

Public URL configuration

```
msh> upnp url "string"
```

- Enter the URL string in the character string.

web

Use the “web” command to display and configure parameters on Web Image Monitor.

View Settings

```
msh> web
```

URL Configuration

You can set URLs linked by clicking [URL] on Web Image Monitor.

```
msh> web "ID" url http:// "The URL or IP address you want to register"/
```

Specify "1" or "2" for ID as the number corresponding to the URL. Up to two URLs can be registered and specified.

Resetting URLs registered as link destinations

```
msh> web "ID" clear url
```

Specify "1" or "2" for ID as the corresponding number to the URL.

Link name configuration

You can enter the name for URL that appears on Web Image Monitor.

```
msh> web "ID" name "Name you want to display"
```

Specify "1" or "2" for ID the corresponding number to the link name.

Resetting URL names registered as link destinations

```
msh> web "ID" clear name
```

Specify "1" or "2" for ID as the number corresponding to the link name.

Help URL Configuration

You can set URLs linked by clicking "?" on Web Image Monitor.

```
msh> web help http://"Help URL or IP address"/help/
```

Resetting Help URL

```
msh> web clear help
```

4

wiconfig

Use the "wiconfig" command to make settings for IEEE 802.11.

View settings

```
msh> wiconfig
```

View IEEE 802.11 settings

```
msh> wiconfig cardinfo
```

- If IEEE 802.11 is not working correctly, its information is not displayed.

Configuration

```
msh> wiconfig "parameter"
```

Parameter	Value configured
mode {ap 802.11ad ad adhoc}	You can set the infrastructure mode (ap) or the 802.11 Ad hoc mode (802.11ad ad adhoc). The default is the infrastructure mode.

Parameter	Value configured
ssid "ID value"	<p>You can specify an SSID in infrastructure mode. The characters you can enter in the SSID string are ASCII 0x20-0x7e (32 bytes). If you do not specify a character string, the machine will connect to the nearest access point.</p> <p>The default SSID is blank.</p>
channel frequency "channel no."	<p>In 802.11 ad hoc mode, you can select a channel between 1 and 14, or 36, 40, 44, or 48.</p> <p>Be sure to set the same channel for all ports that will transmit and receive data.</p> <p>The default is "11".</p>
key "key value" val [1 2 3 4]	<p>You can specify the WEP key when entering in hexadecimal.</p> <p>With a 64-bit WEP, you can use 10 digit hexadecimal. With a 128-bit WEP, you can use 26 digit hexadecimal.</p> <p>Up to four WEP keys can be registered. Specify the number to be registered with "val".</p> <p>When a WEP is specified by key, the WEP specified by key phrase is overwritten.</p> <p>To use this function, set the same key number and WEP key for all ports that transmit data to each other. Put "0x" on the front of WEP key.</p> <p>You can omit the numbers with "val". The key number is set to 1 when making these omissions. The default is blank.</p>

Parameter	Value configured
keyphrase "phrase" val [1 2 3 4]	<p>You can specify the WEP key when entering in ASCII.</p> <p>With a 64-bit WEP, you can use 5 digit hexadecimal. With a 128-bit WEP, you can use 13 digit hexadecimal.</p> <p>Up to four WEP keys can be registered. Specify the number to be registered with "val".</p> <p>When a WEP is specified by key phrase, the WEP specified by key is overwritten.</p> <p>To use this function, set the same key number and WEP key for all ports that transmit data to each other.</p> <p>You can omit the numbers with "val". The key number is set to 1 when making these omissions. The default is blank.</p>
encval [1 2 3 4]	<p>You can specify which of the four WEP keys is used for packet encoding. "1" is set if a number is not specified.</p>
wepauth {open shared}	<p>You can set an authorization mode when using WEP. The specified value and authorized mode are as follows:</p> <p>open: open system authorized (default)</p> <p>shared: shared key authorized rate</p>
security {none wep wpa}	<p>You can specify the security mode.</p> <p>none: No encryption (default)</p> <p>wep: WEP encryption</p> <p>wpa: WPA encryption</p>
wpaenc {tkip ccmp}	<p>You can specify WPA encryption key when using WPA encryption.</p> <p>tkip: TKIP</p> <p>ccmp: CCMP (AES) (default)</p>

Parameter	Value configured
wpaauth {wpapsk wpa wpa2psk wpa2}	<p>You can specify the WPA authentication mode when using WPA encryption.</p> <p>wpapsk: WPA-PSK authentication (default)</p> <p>wpa: WPA authentication</p> <p>wpa2psk: WPA2-PSK authentication</p> <p>wpa2: WPA2 authentication</p>
psk "character string"	<p>You can specify the Pre-Shared key.</p> <p>Usable characters: ASCII 0x20-0x7e (8 to 63 bytes).</p> <p>The default is blank.</p>
eap {tls ttls leap peap} {chap mschap mschapv2 pap md5 tls}	<p>You can specify the EAP authentication type.</p> <p>tls: EAP-TLS (default)</p> <p>ttls: EAP-TTLS</p> <p>leap: LEAP</p> <p>peap: PEAP</p> <p>chap, mschap, mschapv2, pap, md5, or tls are settings for the phase 2 method, and must be set when using EAP-TTLS or PEAP.</p> <p>Do not make these settings when using other EAP authentication types.</p> <p>If you select EAP-TTLS, you can select chap, mschap, mschapv2, pap, or md5.</p> <p>If you select PEAP, you can select mschapv2 or tls.</p>
username "character string"	<p>You can specify the login user name for the Radius server.</p> <p>Usable characters: ASCII 0x20-0x7e (31 bytes).</p> <p>The default is blank.</p>

Parameter	Value configured
username2 "character string"	You can specify the phase 2 username for EAP-TTLS/PEAP phase 2 authentication. Usable characters: ASCII 0x20-0x7e (31 bytes). The default is blank.
domain "character string"	You can specify the login domain name for the Radius server. The characters you can enter are ASCII 0x20-0x7e (31 bytes), but not "@" or "\". The default is blank.
password "character string"	You can specify the login for the Radius server. Usable characters: ASCII 0x20-0x7e (128 bytes). The default is blank.
svrcert {on off}	You can set the server certificate. The default is "off".
imca {on off}	You can enable or disable the certificate when the intermediate certificate authority is present. The default is "off".
srvid "character string"	You can set the server ID and subdomain of the certificate server. Usable characters: ASCII 0x20-0x7e (128 bytes). The default is blank.
Connectinfo	Obtains connection information.
clae {a each command all}	Returns the selected setting to its default value. If you specify "all", all settings will be restored to their default values.
miccheck {on off}	You can enable or disable the MIC check function. The default setting is "On" (enabled). If you specify "Off", you cannot perform MIC checks. We recommend you specify "On" for the MIC check function when using this machine.

wins

Use the “wins” command to configure WINS server settings.

Viewing settings

```
msh> wins
```

- If the IPv4 address obtained from DHCP differs from the WINS IPv4 address, the DHCP address is the valid address.

Configuration

```
msh> wins “interface_name” {on|off}
```

- {on} means “active” and {off} means “inactive”.
- Be sure to specify the interface.
- wlan can be specified only when the IEEE 802.11 interface is installed.

Interface name	Interface configured
ether	Ethernet interface
wlan	IEEE 802.11 interface

Address configuration

Use the following command to configure a WINS server IP address:

```
wins “interface_name” {primary|secondary} “IP address”
```

- Use the “primary” command to configure a primary WINS server IP address.
- Use the “secondary” command to configure a secondary WINS server IP address.
- Do not use “255.255.255.255” as the IP address.

NBT (NetBIOS over TCP/IP) Scope ID Selection

You can specify the NBT scope ID.

```
msh> wins “interface_name” scope “scope ID”
```

- The scope ID can be entered using up to 31 alphanumeric characters.
- Be sure to specify the interface.
- wlan can be specified only when the IEEE 802.11 interface is installed.

Interface name	Interface configured
ether	Ethernet interface
wlan	IEEE 802.11 interface

wsmfp

Use the “wsmfp” command to view and configure WSD (Device), WSD (Printer) and WSD (Scanner) settings.

View settings

```
msh> wsmfp
```

Comment settings

```
msh> wsmfp comments “comment”
```

- If you do not specify a comment, current setting is displayed.

Location configuration

```
msh> wsmfp location “location”
```

- If you do not specify a comment, current setting is displayed.

Presentation URL configuration

```
msh> wsmfp url “URL”
```

- Enter the URL string in the “URL”.

WSD (Device) TCP port configuration

```
msh> wsmfp devport “port_number”
```

- The Default is 53000.

WSD (Printer) TCP port configuration

```
msh> wsmfp prnport “port_number”
```

- The Default is 53001.

WSD (Printer) Timeout configuration

```
msh> wsmfp prntimeout [30-65535]
```

- The default is 900 seconds.

WSD (Scanner) TCP port configuration

```
msh> wsmfp scnport “port_number”
```

- The Default is 53002.

Comment initialization

```
msh> wsmfp clear comments
```

Location initialization

```
msh> wsmfp clear location
```

Presentation URL initialization

```
msh> wsmfp clear url
```


8021x

Use "8021x" command to display IEEE 802.1x related information.

View settings

```
msh> 8021x
```

Configuration

```
msh> 8021x "parameter"
```

Parameter	Value configured
eap {tls ttls leap peap} {chap mschap mschapv2 pap md5 tls}	<p>You can specify the EAP authentication type.</p> <p>tls: EAP-TLS (default)</p> <p>ttls: EAP-TTLS</p> <p>leap: LEAP</p> <p>peap: PEAP</p> <p>chap, mschap, mschapv2, pap, md5, or tls are settings for the phase 2 method, and must be set when using EAP-TTLS or PEAP.</p> <p>Do not make these settings when using other EAP authentication types.</p> <p>If you select EAP-TTLS, you can select chap, mschap, mschapv2, pap, or md5.</p> <p>If you select PEAP, you can select mschapv2 or tls.</p>
Username "character string"	<p>You can specify the login user name for the Radius server.</p> <p>Usable characters: ASCII 0x20-0x7e (31 bytes).</p> <p>The default is blank.</p>
Username2 "character string"	<p>You can specify the phase 2 username for EAP-TTLS/PEAP phase 2 authentication.</p> <p>Usable characters: ASCII 0x20-0x7e (31 bytes).</p> <p>The default is blank.</p>

Parameter	Value configured
domain "character string"	<p>You can specify the login domain name for the Radius server.</p> <p>The characters you can enter are ASCII 0x20-0x7e (31 bytes), but not "@" or "\".</p> <p>The default is blank.</p>
password "character string"	<p>You can specify the login for the Radius server.</p> <p>Usable characters: ASCII 0x20-0x7e (128 bytes). The default is blank.</p>
svrcert {on off}	<p>You can set the server certificate. The default is "off".</p>
imca {on off}	<p>You can enable or disable the certificate when the intermediate certificate authority is present. The default is "off".</p>
srvid "character string"	<p>You can set the server ID and subdomain of the certificate server.</p> <p>Usable characters: ASCII 0x20-0x7e (128 bytes). The default is blank.</p>
clae {a each command all}	<p>Returns the selected setting to its default value.</p> <p>If you specify "all", all settings will be restored to their default values. However, IEEE 802.1x Auth. status (enable or disable) for Ethernet and wireless LAN will not be initialized.</p>

SNMP

Using the SNMP manager, you can get information about the machine.

The SNMP agent operating on UDP and IPX is incorporated into the built-in Ethernet board and optional IEEE 802.11 interface unit of this machine.

This machine also supports SNMPv3, which increases user authentication, data encryption, and access control security.

To encrypt communication by SNMPv3, you must specify the machine's encrypted password.

Important

- **If you changed the machine's community name, change the configuration of the connected computer accordingly, using SNMP Setup Tool. For details, see SNMP Setup Tool Help.**

The default community names are [public] and [admin]. You can get MIB information using these community names.

Start SNMP Setup Tool

- Windows 2000:
Click the [Start] button.
Point to [SmartDeviceMonitor for Admin] on the [Programs] menu.
Click [SNMP Setup Tool].
- Windows XP/Vista, Windows Server 2003/2003 R2/2008
Click the [Start] button.
Point to [SmartDeviceMonitor for Admin] on the [All Programs] menu.
Click [SNMP Setup Tool].

Getting Printer Information over the Network

This section explains details of each item displayed in the printer status and information.

Current Printer Status

This section explains how you can check the machine's status and the items displayed. Depending on the options installed on the machine, some items might not be displayed.

- UNIX: Use the "lpq" command and "rsh", "rcp", "ftp", and "sftp" parameters.
- Windows Vista, Windows Server 2008: Do not use "rsh/rcp".
- mshell: Use the "status" command.

4

Messages	Description
Access Restricted	The job was canceled because user have no authority.
Access Restricted (Classe-Code)	The job was canceled because no classification code is specified.
Add staples (Booklet: Back)	The staple of booklet finisher (back) is exhausted.
Add staples (Booklet: Both)	The staple of booklet finisher is exhausted.
Add staples (Booklet: Front)	The staple of booklet finisher (front) is exhausted.
Adjusting...	The machine is initializing or calibrating.
Call Service Center	There is a malfunction in the machine.
Canceled	The job is reset.
Canceling Job...	The job is being reset.
Cannot Eject Original Through	The original cannot be ejected.
Cannot multi-install: SD Card	The SD card has been configured using another device.
Card/Counter not inserted	The machine is waiting for prepaid card or key.
Coin or amount not inserted	The machine is waiting for coin to be inserted.
Coin/Key Counter not inserted	The machine is waiting for coin or key counter.

Messages	Description
Configuring...	Setting is being changed.
Cooling Down Fusing Unit...	The fusing unit is cooling down.
Cover Open: ADF	The document feeder is open.
Cover Open: Duplex Unit	The cover of the duplex unit is open.
Cover Open: Finisher	The cover of Finisher is open.
Cover Open: Finisher Front	The front cover of Finisher is open.
Cover Open: Front Cover	The front cover is open.
Cover Open: Upper Right Cover	The upper right cover is open.
Current Job Suspended	The current job is suspended.
Data Size Error	The data size error occurred.
Empty: Black Toner	The black toner cartridge is almost empty.
Energy Saver Mode	The machine is in Energy Saver Mode.
Envelope Setting Error: None	Printing paper type other than envelope is instructed when B2 lever is down.
Envelope Setting Error: Others	Printing envelope is instructed when B2 lever is down.
Error	An error has occurred.
Error: Address Book	An error has occurred in the data of the address book.
Error: Command Transmission	An error has occurred in the machine.
Error: DIMM Value	A memory error occurred.
Error: Ethernet Board	An Ethernet board error has occurred.
Error: HDD Board	A hard disk drive board error has occurred.
Error: Media Link Board	An error has occurred on the File Format Converter.
Error: Memory Switch	A memory switch error has occurred.
Error: Optional Font	An error has occurred in the font file of the machine.

Messages	Description
Error: Optional RAM	An error has occurred in the optional memory unit.
Error: Parallel I/F Board	An error has occurred in the parallel interface.
Error: PDL	An error has occurred in the page description language.
Error: Rem. Certificate Renewal	An error has occurred in the remote server renewal.
Error: USB Interface	An error has occurred in the USB interface.
Error: Wireless Board	An error has occurred in the wireless interface board or IEEE 802.11 interface unit.
Error: Wireless Card	Wireless card is not inserted during start up, or the IEEE 802.11 interface unit or the wireless card is taken out after start up.
Exceed Booklet Stapling Limit	The printing has exceeded the stapling limit of the booklet finisher.
Exceed Stapling Limit	The printing has exceeded the stapling limit.
Full: Finisher	Finisher tray is full.
Full: Finisher Booklet Tray	Booklet tray of Finisher is full.
Full: Finisher Shift Tray	Shift tray of Finisher is full.
Full: Finisher Shift Tray 1, 2	The shift tray 1 and 2 of Finisher are full.
Full: Finisher Upper Tray	Finisher's upper tray is full.
Full: Hole Punch Receptacle	Punch Chip receptacle for hole punch is full.
Full: Internal Tray 1	The internal tray is full.
Full: Log Data Capacity	The log data capacity is full.
Full: Waste Toner	The waste toner is full.
Full: Waste Toner Bottle 2	The waste toner bottle 2 is full.
Hex Dump Mode	It is a hex dump mode.
Immed. Trans. not connected	It did not connect directly with the other party of the transmission.

Messages	Description
Immediate Transmission Failed	An error has occurred while transmitting directly.
In Use: Copier	The copier is being used.
In Use: Fax	The fax is being used.
In Use: Finisher	Other functions is using Finisher.
In Use: Input Tray	Other functions is using the input tray.
In Use: Staple Unit	Other functions is using the staple unit.
Independent-supplier Toner	Toner that is not recommended is set.
Jobs Suspended	All jobs are suspended.
Key Card not inserted	The machine is waiting for key card to be inserted.
Key Card/Counter not inserted	The machine is waiting for key card or key counter to be inserted.
Key Counter not inserted	The machine is waiting for key counter to be left in it.
Malfunction: Booklet Processor	There is a problem with booklet finisher.
Malfunction: Ext. Charge Unit	There is a problem with the external charge unit.
Malfunction: Finisher	There is a problem with the finisher.
Malfunction: Output Tray	There is a problem with the output tray.
Malfunction: Punch Unit	There is a problem with the punch unit.
Malfunction: Staple Unit	There is a problem with the staple unit.
Malfunction: Tray 1	There is a problem with tray 1.
Malfunction: Tray 2	There is a problem with tray 2.
Malfunction: Tray 3	There is a problem with tray 3.
Memory Low: Copy	Memory shortage has occurred while the copy was operating.
Mismatch: Paper Size and Type	Indicated paper tray does not contain paper of selected size and type.

Messages	Description
Mismatch: Paper Type	Indicated paper tray does not contain paper of selected type.
Near Replacing: Black PCU	Prepare the new black photoconductor unit.
Near Replacing: Develop. Unit K	Prepare the new development unit (black).
Nearly Full: Log Data Capacity	The log is nearing data capacity
Nearly Full: Waste Toner	Waste toner bottle is nearly full.
Nearly Full: Waste Toner Bottle2	Waste toner bottle 2 is nearly full.
Need more Staples	Stapler has almost run out of staples.
No Paper: Interposer Tray	There is no paper in interposer unit.
No Paper: Selected Tray	There is no paper in specified tray.
No Paper: Tray 1	There is no paper in tray 1.
No Paper: Tray 2	There is no paper in tray 2.
No Paper: Tray 3	There is no paper in tray 3.
Not Detected: B2 Lever	B2 lever is not correctly set.
Not Detected: Black Toner	Black toner is not correctly set.
Not Detected: Duplex Feed Unit	The duplex unit is not correctly set.
Not Detected: Duplex Unit	The duplex feed unit is not correctly set.
Not Detected: Finisher	The finisher is not correctly set.
Not Detected: Fusing Unit	The fusing unit is not correctly set.
Not Detected: Input Tray	The paper feed tray is not correctly set.
Not Detected: Interposer	Interposer unit is not correctly set.
Not Detected: PCU (K)	The photoconductor unit (black) is not correctly set.
Not Detected: Transfer Unit	The transfer unit is not correctly set.
Not Detected: Tray 1	Tray 1 is not correctly set.
Not Detected: Tray 2	Tray 2 is not correctly set.

Messages	Description
Not Detected: Tray 3	Tray 3 is not correctly set.
Not Detected: WasteToner Bottle	Waste toner bottle is not correctly set.
Not Detected: Int. Transfer Unit	Int.transfer unit is not correctly set.
Not Reached, Data Deleted	Unreached job is deleted.
Not Reached, Data Stored	Unreached documents are saved.
Offline	Machine is offline.
Operating Thermo-range Error	The machine is operating outside the permissible temperature range.
Original on Exposure Glass	The original remains on the exposure glass.
Panel Off Mode	The machine is in Panel-Off mode.
Panel Off Mode>>Printing ava.	The machine is in Control Panel-Off mode.
Paper in Duplex Unit	The paper remains in the duplex unit.
Paper in Finisher	The paper remains in Finisher.
Paper Misfeed: ADF	The paper has jammed in Document Feeder.
Paper Misfeed: Duplex Feed Unit	The paper has jammed in Duplex Unit.
Paper Misfeed: Finisher	The paper has jammed in Finisher.
Paper on Finisher ShiftTray1, 2	The paper remains in Finisher Shift Tray 1 and 2.
Paper on Finisher Shift Tray 2	The paper remains in Finisher Shift Tray 2.
Prepaid Card not inserted	The prepaid card is not inserted, or has insufficient credit.
Print Complete	The print was completed.
Printing...	Printing is in progress.
Processing	Data is being processed.
Proxy Address/Port Incorrect	The proxy address and port setting is incorrect.
Proxy User /Password Incorrect	The proxy user name and password setting is incorrect.

Messages	Description
RC Gate Connection Error	Failed connect with RC Gate (Basil).
Readjusting...	The machine is readjusting itself.
Ready	The machine is ready to print.
Renewing Remote Certificate	The remote certificate is being renewed.
Replace Black PCU	It is time to replace the black photoconductor unit.
Replace Charger Kit	It is time to replace the charger kit.
Replace Cleaning Web	It is time to replace the Cleaning Web.
Replace Develop. Unit	It is time to replace the development unit.
Replace Develop. Unit (Black)	It is time to replace the development unit (black).
Replace Developer	It is time to replace the development unit.
Replace Developer (Black)	It is time to replace the development unit (black).
Replace Fusing Unit	It is time to replace the fusing unit.
Replace Int. Transfer Unit	It is time to replace the int. transfer unit.
Replace Maintenance Kit	It is time to replace the maintenance kit.
Replace Transfer Cleaning Unit	It is time to replace the transfer cleaning unit.
Replace Transfer Roller	It is time to replace the transfer roller.
Reset IPDS fonts	An IPDS font error occurred.
Retarding...	Printing has stopped momentarily to allow printed sheets to dry.
SD Card Authentication failed	SD card authentication failed.
SD Card not inserted	The machine is waiting for SD card.
Setting Remotely	The RDS setting is being processed.
Skipped due to Error	Skipped the error.
Storage Complete	The storage is complete.
Storage Failed	The storage has failed.

Messages	Description
Supplies Order Call failed	The supply order call has failed.
Suspend / Resume Key Error	Finisher stop button was pressed.
Transmission Aborted	The transmission was interrupted.
Transmission Complete	The transmission completion was completed.
Transmission Failed	The transmission has failed.
Tray Error: Chaptering	The paper feed tray specification error has occurred because chaptering as well as the normal paper use the same tray for printing.
Tray Error: Duplex Printing	Selected paper tray cannot be used for duplex printing.
Unit Left Open: ADF	Document feeder is opened.
Waiting for Job Suspension	The machine is waiting for Job Suspension.
Warming Up...	The machine is warming up.

↓ Note

- For details about UNIX commands, see UNIX Supplement.
- Check the error contents that may be printed in the configuration page.

Printer configuration

You can check the printer configuration using telnet.

This section explains the checking procedure for input/output tray and printer language.

- UNIX: Use the "info" command and "rsh", "rcp", "ftp", and "sftp" parameters.
- Windows Vista, Windows Server 2008: Do not use "rsh/rcp".
- mshell: Use the "info" command.

Input Tray

Item	Description
No.	ID number of the paper tray
Name	Name of the paper tray

Item	Description
PaperSize	Size of paper loaded in the paper tray
Status	Current status of the paper tray <ul style="list-style-type: none"> • Normal: Normal • NoInputTray: No tray • PaperEnd: No paper

Output Tray

Item	Description
No.	ID number of the output tray
Name	Name of the output tray
Status	Current status of the output tray <ul style="list-style-type: none"> • Normal: Normal • PaperExist: Paper exist • OverFlow: Paper is full • Error: Other errors

Printer Language

Item	Description
No.	ID number of the printer language used by the printer
Name	Name of the printer language used in the printer
Version	Version of the printer language

Note

- For details about UNIX commands and parameters, see UNIX Supplement.

Understanding the Displayed Information

This section explains how to read status information returned by the network interface board.

Print Job Information

Use the following command to display print job information:

- UNIX: Use the “info” command and “rsh”, “rcp”, “ftp”, and “sftp” parameters.
- Windows Vista, Windows Server 2008: Do not use “rsh/rcp”.
- mshell: Use the “info” command.

Item	Description
Rank	Print job status. <ul style="list-style-type: none"> • Active Printing or preparing for printing. • 1st, 2nd, 3rd, 4th... Waiting to be transferred to the printer.
Owner	Print request user name.
Job	Print request number.
Files	The name of the document.
Total Size	The size of the data (spooled). The default is 0 bytes.

Note

- For details about UNIX commands and parameters, see UNIX Supplement.

Print Log Information

This is a record of the most recent jobs printed.

Use the following command to display print log information:

- UNIX: Use the “prnlog” command and “rsh”, “rcp”, “ftp”, and “sftp” parameters.
- telnet : Use the “prnlog” command.

Item	Description
ID	Print request ID.
User	Print request user name.
Page	Number of pages printed
Result	<p>Print Request Result</p> <p>Communication Result</p> <ul style="list-style-type: none"> • OK Print was completed normally. However, the print result may not be as required due to printer problems. • NG Printing was not completed normally. • Canceled An "rcp", "rsh", or "lpr" command print request was canceled, possibly due to the printing application. Not applicable to the "ftp" or "rprinter" command.
Time	<p>Time the print requested was received.</p> <p>Time of print request reception</p>
User ID (when designating Job ID on telnet)	<p>Printer driver-configured User ID.</p> <p>Appears when the print request ID is specified.</p>
JobName (when designating Job ID on telnet)	<p>Name of the document for printing</p> <p>Appears when the print request ID is specified.</p>

Note

- For details about UNIX commands and parameters, see UNIX Supplement.

Configuring the Network Interface Board

Use the following command to display network interface board settings:

- telnet : Use the "show" command.

Item		Description
Common		
	Mode	
	Protocol Up/Down	Protocol Settings
	AppleTalk	
	IPv4	
	IPv6	
	IPsec	
	NetWare	
	SMB	
	Device Up/Down	Device Settings
	Parallel	
	USB	
	Bluetooth	
	Ethernet interface	
	Syslog priority	
	NVRAM version	
	Device name	
	Comment	
	Location	
	Contact	
	Soft switch	
	AppleTalk	AppleTalk settings
	Mode	
	Net	
	Object	

Item		Description
	Type	
	Zone	
TCP/IP		TCP/IP settings
	Mode (IPv4)	
	Mode (IPv6)	
	ftp	
	lpr	
	rsh	
	telnet	
	diprint	
	web	
	http	
	ftpc	
	snmp	
	ipp	
	autonet	
	Bonjour	
	ssl	
	nrs	
	rfu	
	nbt	
	ssdp	
	ssh	
	sftp	
	WSD (Device)	

Item		Description
	WSD (Printer)	
	WSD (Scanner)	
	rhpp	
IPv4		
	DHCP	
	Address	
	Netmask	
	Broadcast	
	Gateway	
IPv6		
	Stateless	
	Manual	
	Gateway	
	DHCPv6-lite	
	DUID	
	DHCPv6 option lifetime	
IPsec		
	Manual Mode	
	Excluded Protocol	
	https	
	dns	
	dhcp	
	wins	
EncapType		
Host name		

4

Item		Description
	DNS Domain	
	Access Control	Access Control settings
	IPv4	
	AccessEntry [X]	X can be set between 1 and 5.
	IPv6	
	AccessEntry [X]	X can be set between 1 and 5.
	SNTP Server	Time settings
	Time Zone	
	SNTP Server polling time	
	SYSLOG server	Websys settings
	Home page URL1	
	Home page link name1	
	Home page URL2	
	Home page link name2	
	Help page URL	
	RHPP Port	
	RHPP timeout	
	NetWare	NetWare settings
	EncapType	
	RPRINTER number	
	Print server name	
	File server name	
	Context name	
	Switch	
	Mode	

Item		Description
	NDS/Bindery	
	Packet negotiation	
	Login Mode	
	Print job timeout	
	Protocol	
	SAP interval time	
	NDS Tree Name	
	Transfer Protocol	
SMB		SMB settings
	Switch	
	Mode	
	Direct print	
	Notification	
	Workgroup name	
	Computer name	
	Comment	
	Share name [1]	
	Protocol	
Wireless LAN		Wireless LAN settings
	Host Name	
	Communication Mode	
	SSID	
	Channel	
	Security	
	WEP Authentication	

Item		Description
	WEP Encryption key number	
	WEP Encryption keys [X]	X can be set between 1 and 4.
	WPA Encryption	
	WPA Authentication	
	Pre-Shared Key	
	User name	
	Domain name	
	EAP Type	
	Password	
	Phase 2 user name	
	Phase 2 Method TTLS	
	Phase 2 Method PEAP	
	Server cert.	
	Intermediate CA	
	Server ID	
	Sub domain	
	MIC check	
DNS		DNS settings
	IPv4	
	Server [X]	X can be set between 1 and 3.
	Selected IPv4 DNS Server	
	IPv6	
	Server [X]	X can be set between 1 and 3.
	Selected IPv6 DNS Server	
	Resolver Protocol	

Item	Description
Domain Name	
ether	
wlan	
DDNS	
ether	
wlan	
Ethernet	
802.1X Authentication	
WINS	WINS settings
ether	
Primary WINS	
Secondary WINS	
wlan	
Primary WINS	
Secondary WINS	
Bluetooth	Bluetooth settings
Bluetooth mode	Bluetooth connection mode
SSDP	SSDP settings
UUID	
Profile	
TTL	
UPnP	UPnP settings
URL	
Bonjour	Bonjour settings
Computer Name (cname)	

Item		Description
	Local Hostname (ether)	
	Local Hostname (wlan)	
	Location	
	Priority (diprint)	
	Priority (lpr)	
	Priority (ipp)	
	IP TTL	
	LinkLocal Route for Multi I/F	
	IPP Port	
SNMP		SNMP settings
	SNMPv1v2	
	SNMPv3	
	protocol	
	v1Trap	
	v2Trap	
	v3Trap	
	SNMPv1v2 Remote Setting	
	SNMPv3 Privacy	
ssh		ssh settings
	Compression	
	Port	
	TimeOut	
	Login TimeOut	
AuthFree		Authfree settings
	IPv4	

Item		Description
	AuthFree Entry [X]	X can be set between 1 and 5.
	IPv6	
	AuthFree Entry [X]	X can be set between 1 and 5.
	Parallel	
	USB	
LPR		
	lprm check host	
	lpr prnerr chk	
Certificate		
	Verification	
WS-MFP		
	Network Device Name	
	Comments	
	Location	
	Presentation URL	
	WSD (Device) TCP Port	
	WSD (Printer) TCP Port	
	WSD (Printer) Job Timeout	
	WSD (Scanner) TCP Port	
	MetadataVersion	
	UUID	
IEEE 802.1X		IEEE 802.1X settings
	User Name	
	Domain name	
	EAP Type	

Item	Description
Password	
Phase 2 user name	
Phase 2 Method TTLS	
Phase 2 Method PEAP	
Server cert	
Intermediate CA	
Server ID	
Sub domain	
Shell mode	Remote maintenance tool mode

Message List

This is a list of messages that appear in the machine's system log. The system log can be viewed using the "syslog" command.

System Log Information

Use the following command to display the system log information:

- UNIX: Use the "syslog" command and "rsh", "rcp", "ftp", and "sftp" parameters.
- Windows Vista, Windows Server 2008: Do not use "rsh/rcp".
- telnet: Use the "syslog" command.

Message	Problem and solutions
Access to NetWare server <file server name> denied. Either there is no account for this print server on the NetWare server or password was incorrect.	Login to the file server failed when the print server was online. Make sure the print server is registered in <file server name>. If a password is specified for the print server, delete the password.
account is unavailable: same account name be used.	User account is disabled. This could be because it use the same account name as the administrator account.
account is unavailable: The authentication password is not set up.	User account is disabled. This could be because the authentication password is not set, and only the encryption account is set.
account is unavailable: encryption is impossible.	Encryption is not possible and account is disabled. This could be because: <ul style="list-style-type: none"> • Security option is not installed. • Encryption password has not been specified.
add_sess_IPv4: bad trap addr: <IPv4 address>, community: <community name>	The IPv4 address (0.0.0.0.) is unavailable when the community access type is TRAP. Specify the host IPv4 address for the TRAP destination.
add_sess_IPv6: bad trap addr: <IPv6 address>, community: <community name>	The IPv6 address [::] is unavailable when the community access type is TRAP. Specify the host IPv6 address for the TRAP destination.
add_sess_IPv4: community <community name> already defined.	The same community name already exists. Use another community name.

Message	Problem and solutions
add_sess_IPv6: community <community name> already defined.	The same community name already exists. Use another community name.
add_sess_IPX: bad trap addr: <IPX address> community <community name>	The IPX address (00:00:00:00:00:00) is unavailable when the community access type is TRAP. Specify the host IPX address for the TRAP destination.
add_sess_IPX: community <communityname> already defined.	The same community name already exists. Use another community name.
adjust time server <NTP server name> offset: xx sec.	ncsd tells you the timing of the NTP server and whether or not the time system clock is set. NTP Server: NTP server name offset: number of seconds of delay (minus number if a time in advance is specified)
ANONYMOUS FTP LOGIN FROM <IP address>, <password>	An anonymous user logged in from the post <IP address> using the password <password>.
Attach FileServer=<file server>	Connection to the file server as the nearest server has been established.
Attach to print queue <print queue name>	The system connects to the print queue when the print server goes online.
authenticating	The supplicant is authenticating with the access point (EAP or WPA).
authentication mode mismatch	The authentication mode of the access point is different from the authentication mode of the supplicant. Use the authentication mode between the access point and the supplicant.
child process exec error !	The network service failed to start. Turn the printer off and then on. If this does not work, contact your service or sales representative.
cipher suite mismatch	The uni-cast / multi-cast suite (TKIP/AES/WEP) of the access point is different from the suite used by the supplicant.

Message	Problem and solutions
client EAP method rejected	The authentication mode of the access point is different with the authentication mode of the supplicant. Use the same authentication mode between the access point and the supplicant.
Client password rejected	The client's password was rejected. Check the client password.
Client TLS certificate rejected	The client's TLS certificate was rejected. Check the certificate.
connected DHCPv6 server <IPv6 address>	The IP address was successfully received from the DHCPv6 server.
Could not attach to FileServer <error number>	Connection to the file server could not be established when the remote printer went online. The file server refused the connection for unknown reason. Check the file server's configuration.
Could not attach to PServer <print server>	Connection to the print server has not been established when the remote printer is turned on. The print server has refused the connection. Check the print server configuration.
connection from <IP address>	A user logged in from the host <IP address>.
Current Interface Speed: xxx Mbps	Speed of the network (10Mbps, 100 Mbps, or 1Gbps).
Current IPX address <IPX address>	The current IP address is <IPX address>.
Duplicate IP=<IP address> (from<MAC address>).	A conflicting IPv4 or IPv6 address was used. Each IPv4 or IPv6 address must be unique. Check the device address in [MAC address].
DHCPv6 server not found.	The DHCPv6 server was not found. Make sure that the DHCPv6 is on the network.
Established SPX Connection with PServer, (RPSocket=<socket number>, connID=<connection ID>)	Connection to the print server was established when the remote printer went online.

Message	Problem and solutions
Frametype=<frametype name>	The specified frame type name <frame type name> is for NetWare use.
IEEE 802.11 Card does NOT support WPA .	A wireless card that does not support WPA is installed. Install a wireless card that supports WPA.
IEEE 802.11 Card Firmware REV.<version>	Displays the version number of the 802.11 card's firmware.
IEEE 802.11 current channel <channel number>	Displays the current channel number of the active wireless card (in ad hoc and infrastructure mode).
IEEE 802.11 MAC Address = <MAC address>	Displays the MAC address of the wireless interface.
IEEE 802.11 SSID <ssid> (AP MAC Address <MAC address>)	The MAC address and SSID of the access point are connected in infrastructure mode.
IEEE 802.11 <communication mode> mode	Displays IEEE 802.11 communication mode.
(IKE phase-1) mismatched authentication type: local=<authentication type 1> remort=<authentication type 2>	This machine's <authentication type 1> in IKE phase 1 does not match the communicating host's <authentication type 2>, Make sure this machine's ISAKMP SA authentication type matches that of the communicating host.
(IKE phase-1) mismatched encryption type: <encryption algorithm 1> remort=<encryption algorithm 2>	This machine's ISAKMP SA Oakley group <encryption algorithm 1> in IKE phase 1 does not match the communicating host's ISAKMP SA Oakley group < encryption algorithm 2>, Make sure this machine's ISAKMP SA Oakley group matches that of the communicating host.
(IKE phase-1) mismatched DH group: local=<DH group number 1> remort=<DH group number 2>	This machine's ISAKMP SA Oakley group <DH group number 1> in IKE phase 1 does not match the communicating host's ISAKMP SA Oakley group <DH group number 2>, Make sure this machine's ISAKMP SA Oakley group matches that of the communicating host.
(IKE phase-1) mismatched hash type: local=<Hash Algorithm 1> remort=<Hash Algorithm 2>	This machine's ISAKMP SA <Hash Algorithm 1> in IKE phase 1 does not match the communicating host's ISAKMP SA <Hash Algorithm 2>, Make sure this machine's ISAKMP SA Hash Algorithm matches that of the communicating host.

Message	Problem and solutions
Interface (interface name): Duplicate IP Address (<IP address>).	The same IP (IPv4 or IPv6) address was used. Each IP address must be unique. Check the address of the device indicated in [IP address].
<Interface name> card removed	The interface managed by the supplicant has been removed.
<Interface name> interface down	The interface managed by the supplicant is disabled, or cannot connect to the access point.
<Interface name> interface up	The interface managed by the supplicant is enabled, or is connected to the access point.
< Interface > started with IP: < IP address >	IP address (IPv4 or IPv6 address) has been set for the interface and is operating.
< Interface >: Subnet overlap.	The same IP address (IPv4, or IPv6 address) and the subnet mask is used with other device.
job canceled. jobid=%d.	The spooled job was canceled due to error or user request.
Lease Time=<lease time>(sec), RenewTime=<renew time>(sec).	The resource lease time received from the DHCP server is displayed in [lease time] in seconds. The renewal time is displayed in [renew time] in seconds.
LEAP challenge to access point failed	The LEAP challenge to the access point has failed.
Login to fileserver <file server name> (<IPX IP>), <NDS BINDERY>	When the print server was online, the system logged in to <file server> in NDS or BINDERY mode. The transfer protocol in use is also displayed.
Memory allocate error.	Date cannot be obtained. Disconnect the USB cable, and then connect it.
MIC failure TKIP counter measures started	The supplicant using TKIP has detected two instances of tampering within 60 seconds and has started counter measures.
MIC failure TKIP counter measures stopped	Counter measures have stopped after 60 seconds (since the supplicant using TKIP started counter measures against tampering).

Message	Problem and solutions
Name registration failed. name=<NetBIOS name>	Name registration of <NetBIOS Name> failed. Change to a different NetBIOS name.
Name registration success in Broadcast name=<NetBIOS name>	Name registration by <NetBIOS Name> broadcast was successful.
Name registration success. WINS server=<WINS server address> NetBIOS Name=<NetBIOS name>	Name registration of <NetBIOS Name> to <WINS server address> was successful.
no RADIUS/authentication server	The supplicant has received a message reporting that a usable RADIUS server cannot be found.
no smart card detected on device	PEAP/GTC (Generic Token Card) is selected, but a smart card using GTC authentication cannot be found.
no WPA information element in probe response, rescanning	There is no WPA information on the response from the SSID probe of the access point you want to use. The supplicant is rescanning.
Open log file <file name>	The specified log file was opened when the print server was online.
Printer <printer name> has no queue	The print queue is not assigned to the printer when the print server was online. Assign the print queue to the printer using NetWare administrator account, and then restart the printer.
Printer queue <print queue name> cannot be serviced by printer 0, <print server name>	The print queue cannot be established when the print server is online. Make sure that the print queue exists on the specified file server.
Print server <print server name> has no printer	The printer was not assigned to the print server when the print server was online. Use the NetWare administrator account to assign the printer, and then restart the printer.
Print sessions full	No more print jobs can be accepted. Wait a while before sending any more print jobs.
Required file server (<file server name>) not found	The required file server <file server name> could not be found.

Message	Problem and solutions
sap enable. saptype=<SAP type>, sapname=<SAP name>	The SAP function was started. The SAP packet is issued to advertise the service in the SAP table on the NetWare server.
server certificate invalid	The server ID is disabled. Check the server authentication.
server identity invalid	The server ID is disabled. Check the server authentication.
server not trusted	The RADIUS server cannot be trusted.
session IPv4 <community name> not defined.	The requested community name is not defined.
session IPv6 <community name> not defined.	The requested community name is not defined.
session_IPX <community name> not defined.	The requested community name is not defined.
Set context to <NDS context name>	The NDS context name <NDS context name> has been set.
shutdown signal received. network service rebooting...	The smbd service has started.
SMTPC: failed to get smtp server ip-address.	The SMTP server IP address could not be obtained. This could be because: <ul style="list-style-type: none"> • The specified DNS server could not be found. • No connection to the network has been established. • The specified DNS server could not be found. • An incorrect DNS server is specified. • The specified SMTP server IP address could not be found in the DNS server.
SMTPC: failed to connect smtp server. timeout.	Connection to the SMTP server failed due to timeout. This could be because the specified SMTP server name is incorrect, or no connection to the network has been established, or the network configuration is incorrect, so there is no response from the SMTP server. Check the SMTP server name, or the network connection and configuration.

Message	Problem and solutions
SMTPC: refused connect by smtp server.	Connection to the SMTP server is denied. This could be because server other than the SMTP server has been specified, or the specified SMTP server port number is incorrect. Check the SMTP server name, port number, or the SMTP server port number.
SMTPC: no smtp server. connection close.	Connection to the SMTP server failed due to no response from SMTP. This could be because a server other than the SMTP server has been specified, or the specified SMTP server port number is incorrect. Check the SMTP server name, port number, or the SMTP server port number.
SMTPC: failed to connect smtp server.	Connection to the SMTP server failed. This could be because no connection to the network has been established, or the network configuration is incorrect, so there is no response from the SMTP server, or the specified SMTP server name is incorrect, or the specified SMTP server IP address could not be found in the DNS server, or a server other than the SMTP server has been specified, or the specified SMTP server port number is incorrect. Check the DNS Server's IP address and SMTP server's IP address, or the SMTP server name and SMTP port number, or the SMTP server's SMTP port number, or the network connection and configuration.
SMTPC: username or password wasn't correct. [response code] (information)	Connection to the SMTP server failed, because the specified SMTP user name is incorrect, or the specified SMTP password is incorrect. Check the SMTP user name and password.
Snmp over IPv4 is ready.	Communication over IPv4 with snmp is available.
Snmp over IPv6 is ready.	Communication over IPv6 with snmp is available.
Snmp over IPX is ready.	Communication over IPX with snmp is available.
success key received	The supplicant received the EAP-Success key.

Message	Problem and solutions
success but invalid key	The supplicant received a message reporting that EAP authentication was successful, but the EAPOL key was invalid.
supplicant unbound	The supplicant is not connected to the unbound access point.
There is problem in dhcp server operation.	There is a problem with the DHCP server. If multiple DHCP servers are active on the network, check that they are assigning unique IP addresses to each machine.
The print server received error <error number> during attempt to log in to the network. Access to the network was denied. Verify that the print server name and password are correct.	Login to the file server failed when the print server was online. The print server is not registered or a password is specified. Register the print server without specifying a password.
trap account is unavailable.	v3Trap cannot be sent. This could be because the Trap destination account is different from the account specified by the printer.
unauthenticated	The authentication failed. The supplicant was denied access to the access point, or was not authenticated.
Updated (option name)(value) via DHCPv6 Server	The parameter obtained from the DHCP server has been updated.
usbd is disabled.	Plug and Play is unavailable because the machine is in security mode. Enable USB D in Security Mode.
waiting for keys	The supplicant is waiting for the session key.
WINS name registration: No response to server (WINS server address)	There was no response from the WINS server. Check that the correct WINS server address is entered. Also, check that the WINS server is functioning properly.
WINS wrong scope ID=<scope ID>	The scope ID is invalid. Use a valid scope ID.

Message	Problem and solutions
write error occurred. (diskfull)	A "diskfull" error occurred while the machine was writing to the spool file. Wait for the current print job to finish, When it finishes, more HDD space will be available. Only pages that were spooled when the error occurred will be printed.
write error occurred. (fatal)	A "fatal" error occurred while the machine was writing to the spool file. Wait for the current print job to finish, When it finishes, more HDD space will be available. Only pages that were spooled when the error occurred will be printed.
WSD (Device) started.	WS-Device has started.
WSD (Printer) started.	WS-Printer has started.
WSD (Scanner) started.	WS-Scanner has started.
#[nfa (process ID)] <time date> + Failed to send logos to a log collection server <IP address>.	An error occurred while trying to send a log file to both the primary and secondary log collection servers.
#[nfa (process ID)] <time date> + Failed to send logs to a collection server <IP address> n time(s) in 1 hour.	60 minutes has passed since the last log entry. During that time, an error occurred while trying to send the log file to both the primary and secondary log collection servers.

Note

- For details about UNIX commands and parameters, see UNIX Supplement.

5. Registering Addresses and Users for Facsimile/Scanner Functions

This chapter describes how to register destinations and users in the Address Book. For details on how to access System Settings, see "Accessing System Settings".

Address Book

This section describes Address Book settings.

Registering information such as the names of users and their e-mail addresses in the Address Book allows you to manage them easily.

★ Important

- Address Book data is stored on the hard disk. It can be lost if there is some kind of hard disk failure.
- The manufacturer shall not be held responsible for any damages resulting in data loss.

5

You can register and manage the following items in the Address Book:

Names

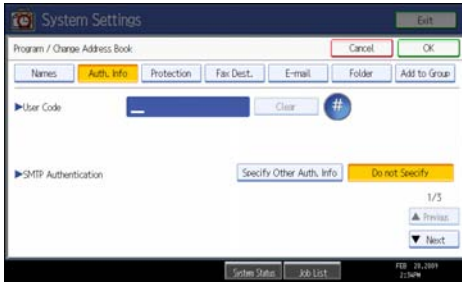
You can register the name of the user and the key display. This is the basic information required for managing users of the machine.

To register a fax number or e-mail address in the address book, you must register information such as the user name and destination name in advance.



Auth. Info

You can register user codes in order to restrict particular functions to certain users, and to check their use of each function. You can also register login user names and login passwords to be used when sending e-mail, sending to folders, or accessing an LDAP server.



Protection

You can set protection codes to stop sender's name from being used or folders from being accessed without authorization.

5



Fax Dest.

You can register fax numbers, line, fax header and select label insertion.

When using IP-Fax, you can register the IP-Fax destination and select the protocol.



E-mail

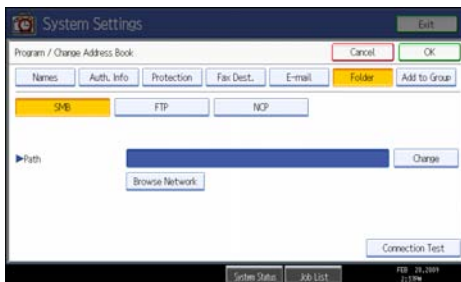
You can register e-mail destinations in the Address Book.



Folder

You can register the protocol, path name and server name.

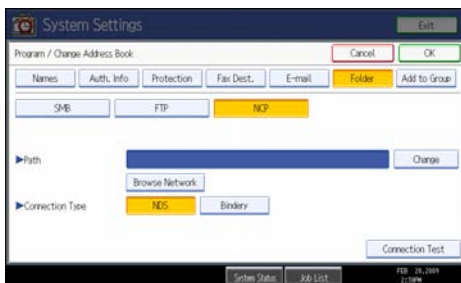
- SMB



- FTP



- NCP



Add to Group

You can put registered e-mail and folder destinations into a group for easier management.



Note

- You can also use Web Image Monitor to register names in the Address Book. With SmartDeviceMonitor for Admin, you can register multiple names at the same time. For details about using Web Image Monitor, see Web Image Monitor Help.
- Using Address Management Tool in SmartDeviceMonitor for Admin, you can backup Address Book data. We recommend backing up data when using the Address Book. For operating instructions, see SmartDeviceMonitor for Admin Help.

5

Managing names in the Address Book

By registering a name and key display beforehand, you can specify e-mail and folder destinations simply by selecting the name key.

Reference

- p.255 "Registering Names"

Sending fax by Quick Dial

Register a fax number in the Address Book so you can specify it only by selecting the fax destination, shown on the fax initial display when sending a fax. When label insertion is set to "On", the receiver's name and standard messages are printed on the fax message when it is received at the other end.

By registering IP-Fax destinations in the Address Book, you can specify a destination simply by selecting it from the destinations that appear in the initial fax display. Registered IP-Fax numbers can be used and printed as sender's IP-Fax numbers.

Reference

- p.268 "Fax Destination"

Sending e-mail by Quick Dial

By registering e-mail addresses in the Address Book, you can specify e-mail destinations simply by selecting them from the fax initial display when sending a document by Internet fax or e-mail.

You can also specify an e-mail address by selecting the destination shown on the initial scanner display when sending a document using the scanner function. A registered e-mail address can be used as the sender's address, and the sender's addresses are automatically entered in the "From" field of an e-mail header.

Reference

- p.281 "E-mail Destination"

Sending received fax documents or scanned files to a shared folder directly

After registering the path name, user name and password, you can connect to a shared folder simply by selecting the destination shown on the initial facsimile display whenever sending files using the facsimile function to a shared folder. You can also connect to a shared folder by selecting the destination shown on the initial scanner display whenever sending files using the scanner function.

To share the folder using Windows, select the SMB protocol.

To register the folder to the FTP server, select the FTP protocol.

To register the folder to the NetWare server, select the NCP protocol.

Reference

- p.286 "Registering Folders"

Preventing unauthorized user access to shared folders from the machine

After registering a protection code, you can specify the object of protection to prevent an e-mail destination from being used without permission.

You can prevent unauthorized access to registered folders.

Reference

- p.313 "Registering a Protection Code"

Managing users and machine usage

Register user codes to limit users to the following functions and check their use of each function:

- Copier
- Document Server

- Facsimile
- Printer
- Scanner

Reference

- p.259 "Authentication Information"

Registering Names

Register user information including their names.

The user name is useful for selecting a destination when sending faxes or e-mail.

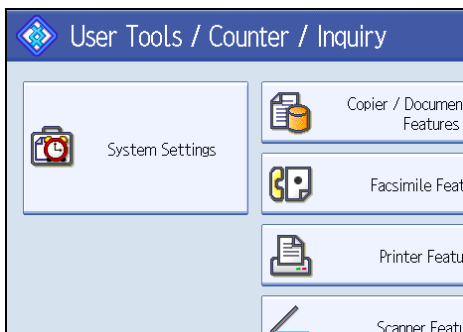
You can also use it as a folder destination.

You can register up to 2000 names.

Registering Names

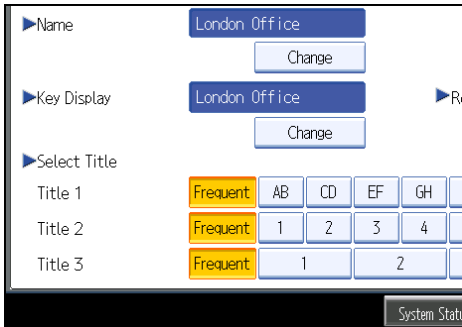
This section describes how to register names.

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



3. Press [Administrator Tools].
4. Press [Address Book Management].
5. Check that [Program / Change] is selected.
6. Press [New Program].
7. Press [Change] on the right of the Name.
The name entry display appears.
8. Enter the name, and then press [OK].

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



The keys you can select are as follows:

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

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

10. Press [OK].

11. Press [Exit].

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

Note

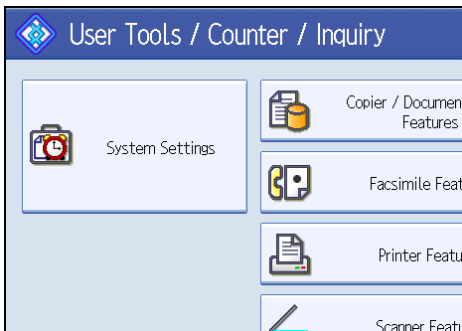
- The name can be used for documents in the Document Server. For details about the Document Server, see "Using the Document Server", Copy and Document Server Reference.

Changing a Registered Name

This section describes how to change a name.

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

2. Press [System Settings].



3. Press [Administrator Tools].
4. Press [Address Book Management].
5. Check that [Program / Change] is selected.
6. Select the registered name you want to change.
Press the name key, or enter the registered number using the number keys.
7. To change the name or key display, press [Change] on the right of the "Name" or "Key Display".
8. Enter the name or key display, and then press [OK].
9. To change the title, press the key for the classification you want to use from "Select Title".
10. To change the registration number, press [Change] under "Registration No.".
11. Enter a new registration number using the number keys, and then press the [#] key.
12. Press [OK].
13. Press [Exit].
14. Press the [User Tools / Counter] key.

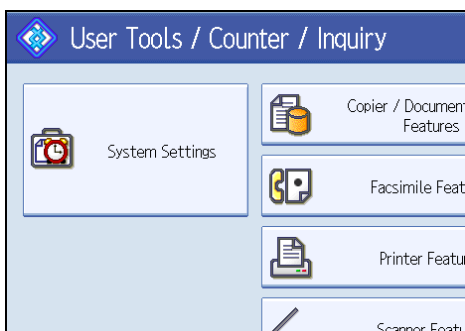
↓ Note

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

Deleting a Registered Name

This section describes how to delete a name.

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



3. Press [Administrator Tools].
4. Press [Address Book Management].
5. Press [Delete].

6. Select the name you want to delete.

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

7. Press [Yes].

8. Press [Exit].

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

Authentication Information

Following describes the procedure for authenticating a user code.

★ Important

- **The functions associated with each user code are the same. If you change or delete user codes, management data and limits associated with that code become invalid.**

Register user codes to limit users to the following functions and check their use of each function:

- Copier
- Document Server
- Facsimile
- Printer
- Scanner

↓ Note

- You can register up to 500 user codes.
- The number of copies made of documents stored in the Document Server using the facsimile function is counted for each user code. This allows you to check each user's usage.
- The number of copies scanned using the scanner function is counted for each user code. This allows you to check each user's usage.
- To automatically register the printer driver user code, select [PC Control] under Printer for the printer in User Code Authentication. To use the user code set in User Tools, set the user codes registered in User Tools for the printer driver.
- For details about setting user codes for the printer driver, see the printer driver Help.

📖 Reference

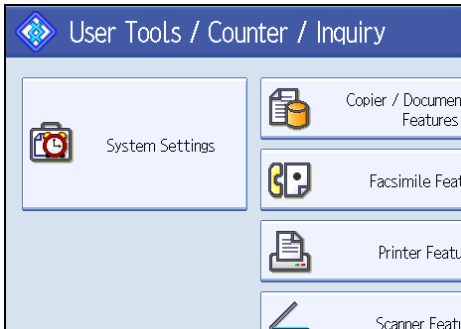
- p.49 "Administrator Tools"

Registering a User Code

This section describes how to register a user code.

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

2. Press [System Settings].



3. Press [Administrator Tools].

4. Press [Address Book Management].

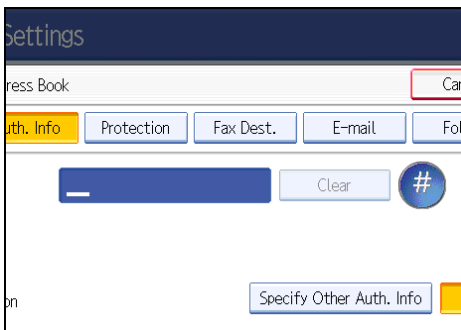
5. Check that [Program / Change] is selected.

6. Press the name whose code is to be registered, or enter the registered number using the number key.

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

7. Press [Auth. Info].

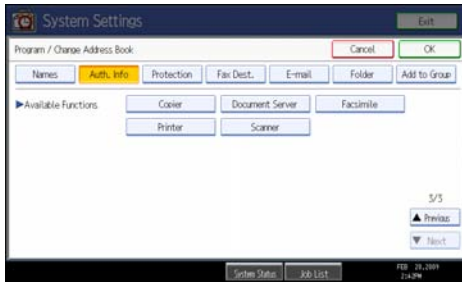
8. Enter the user code using the number keys, and then press the [#] key.



If you make a mistake, press [Clear] or the [Clear/Stop] key.

9. Press [▼Next] twice.

10. Select the functions to be used with the user code from "Available Functions".



11. Press [OK].

12. Press [Exit].

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

Note

- You can enter a one-to eight-digit user code.
- To register the name, see "Registering Names".

Reference

- p.255 "Registering Names"

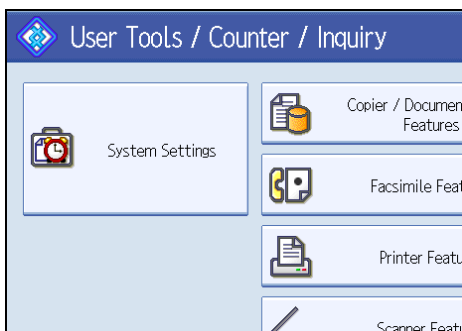
Changing a User Code

This section describes how to change a user code.

Important

- Even if you change a user code, the counter value will not be cleared.

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



3. Press [Administrator Tools].
4. Press [Address Book Management].

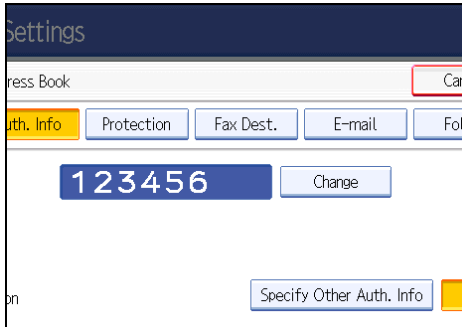
5. Check that [Program / Change] is selected.

6. Select the user whose user code you want to change.

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

7. Press [Auth. Info].

8. Press [Change], and then enter the new user code using the number keys.



5

9. Press the [#] key.

10. To change the available functions, press [Auth. Info], and then press [▼Next] twice.

11. Press the key to select the functions to enable them.

Press the key to highlight it, and then the function is enabled. To cancel a selection, press the highlighted key.

12. Press [OK].

13. Press [Exit].

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

Note

- To change the name, key display and title, see "Registering Names".

Reference

- p.255 "Registering Names"

Deleting a User Code

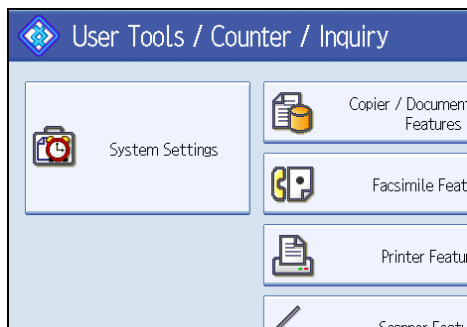
This section describes how to delete a user code.

Important

- After clearing the user code, the counter is automatically cleared.

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

2. Press [System Settings].



3. Press [Administrator Tools].

4. Press [Address Book Management].

5. Press [Program / Change].

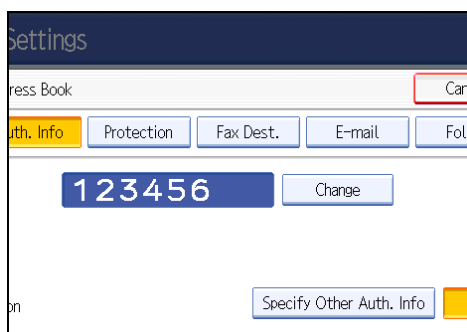
6. Select the name whose code is to be deleted.

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

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

7. Press [Auth. Info].

8. Press [Change] to delete the user code, and then press the [#] key.



9. Press [OK].

10. Press [Exit].

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

↓ Note

- To delete a name from the Address Book entirely, see "Registering Names".

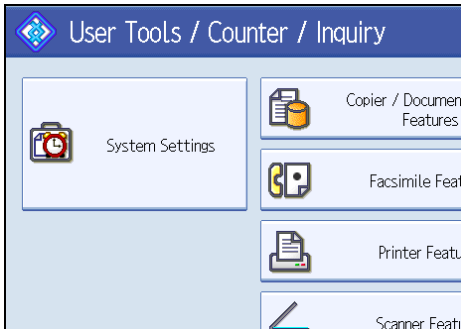
📖 Reference

- p.255 "Registering Names"

Displaying the Counter for Each User

This section describes how to display the counter for each user.

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



5

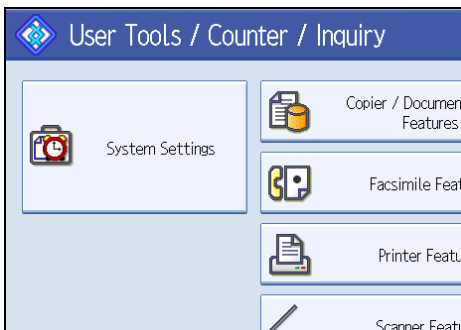
3. Press [Administrator Tools].
4. Press [Display / Clear / Print Counter per User].
5. Select the function usage you want to print from [Print Counter], [Transmission Counter] or [Scanner Counter].

Counters for individual function usage under each user code appear.

Printing the Counter for Each User

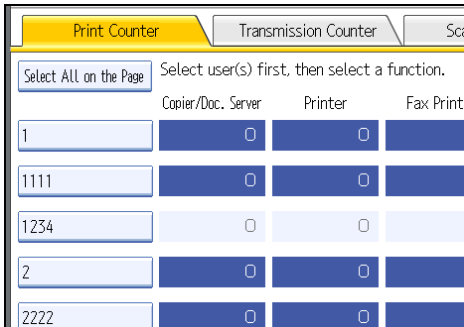
This section describes how to print the counter for each user.

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



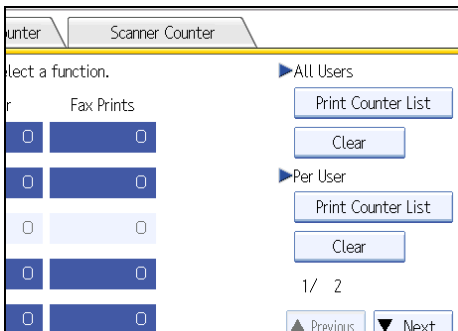
3. Press [Administrator Tools].
4. Press [Display / Clear / Print Counter per User].

5. Select a user code from the left side of the display.



Press [Select All on the Page] to select all user codes on the page.

6. Press [Print Counter List] under "Per User".



Enter the user code, and then press the [#] key if the user code is registered.

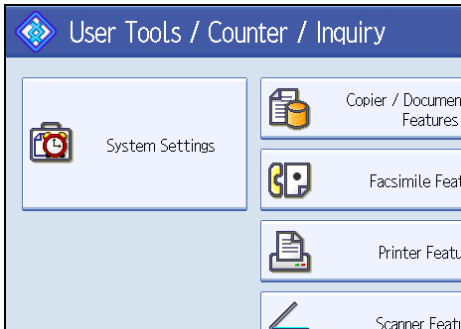
- 7. Select the function usage you want to print from [Copier Counter], [Printer Counter], [Fax Prints], [Fax Transmission], [Scanner Counter], and [Total Prints].**
- 8. Press [Print].**

Printing the Counter for All Users

This section describes how to print the counter for all users.

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

2. Press [System Settings].

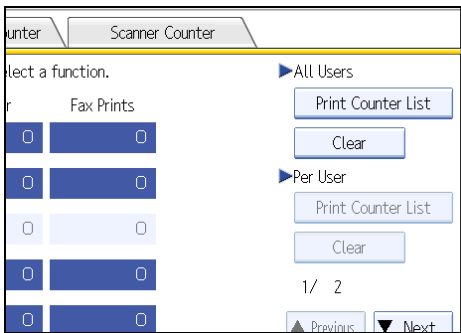


3. Press [Administrator Tools].

4. Press [Display / Clear / Print Counter per User].

5. Press [Print Counter List] under "All Users".

5



Enter the user code, and then press the [#] key if the user code is registered.

6. Select the function usage you want to print from [Copier Counter], [Printer Counter], [Fax Prints], [Fax Transmission], [Scanner Counter], and [Total Prints].

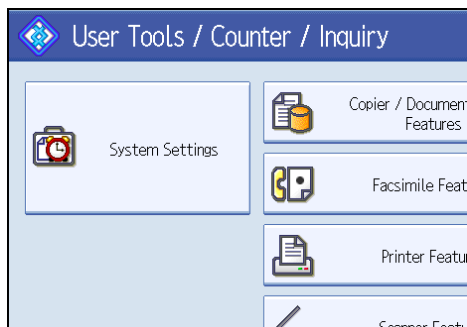
7. Press [Print].

Clearing the Number of Prints

This section describes how to clear the counter.

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

2. Press [System Settings].



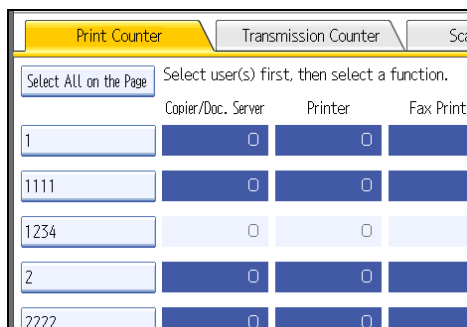
3. Press [Administrator Tools].

4. Press [Display / Clear / Print Counter per User].

5. Select the user code to clear.

6. To clear the number of prints made under a user code, select the user code from the left side of the display.

5



Press [Select All on the Page] to select all user codes on the page.

7. Press [Clear] under "Per User".

8. Select the function usage you want to clear from [Copier Counter], [Printer Counter], [Fax Prints], [Fax Transmission], [Scanner Counter], and [All Counters].

9. Press [OK].

10. To clear the number of prints for all user codes, press [Clear] under "All Users".

11. Select the function usage you want to clear from [Copier Counter], [Printer Counter], [Fax Prints], [Fax Transmission], [Scanner Counter], and [All Counters].

12. Press [OK].

13. Press [Exit].

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

Fax Destination

This section describes the procedure for registering, changing, and deleting Fax Destinations.

Register a fax destination so you do not need to enter fax numbers each time, and can send documents that have been scanned in using the facsimile function.

- It is easy to select the fax destination if you register "Name" and "Key Display" for the fax destination.
- You can register fax destinations as a group. For details about registering a group, see "Fax Destination".
- You can register fax destinations by selecting them from redial function.
- Registered Fax numbers can be used as sender's Fax numbers.

There are two types of fax destination, as shown below:

- **Fax Destination**
Select this to send the fax over the telephone network.
- **IP-Fax**
Select this to send the fax to a machine on a TCP/IP network.
You cannot send the fax to a machine on another network if that network is behind a firewall.

You can program the following items in a fax destination:

Fax number

Registers the destination's fax number. You can enter a fax number using up to 128 digits. You must include every digit in the number.

SUB Code

Registering a SUB Code allows you to use Confidential Transmission to send messages to the other fax machines which support a similar function called "SUB Code". See "Setting SUB Codes for Transmission", Facsimile Reference.

SEP Code

Registering a SEP Code allows you to use Polling Reception to receive faxes from the other fax machines which support Polling Reception. See "Setting SEP Codes for Reception", Facsimile Reference.

Select Line

When installing the G3 unit board, select the line each other.

International TX mode

When setting the International TX mode to [On], the machine transmits more carefully by lowering transmission speed. However, communication times increase.

Fax header

You can select to print a fax header on fax messages the other party receives.

The default is "1st Name".

Label insertion

Use label insertion to print information such as the destination name on the sheet printed out at the destination.

Data is printed as follows:

- Destination Name

The destination name specified in [Fax Destination] is printed with "To" before it at the top of the sheet.

- Standard Message

A registered two-line sentence is printed under "Destination Name".

To use this function, set Label Insertion to [On] when programming fax destinations and also press [Label Insertion] when sending fax documents.

Fax header and label insertion are also printed when sending by e-mail using the fax function.

You can program a standard message other than those registered in the machine.

See "Program/Change/Delete Standard Message", Facsimile Reference.

You can program the following items in an IP-Fax Destination:

IP-Fax

Register the IP-Fax destination. You can register the name using up to 128 characters. You must make this setting when using IP-Fax.

This setting only works if the IP-Fax function has been selected.

SUB Code

Registering a SUB Code allows you to use Confidential Transmission to send messages to the other fax machines which support a similar function called "SUB Code". See "Setting SUB Codes for Transmission", Facsimile Reference.

SEP Code

Registering a SEP Code allows you to use Polling Reception to receive faxes from the other fax machines which support Polling Reception. See "Setting SEP Codes for Reception", Facsimile Reference.

Select Protocol

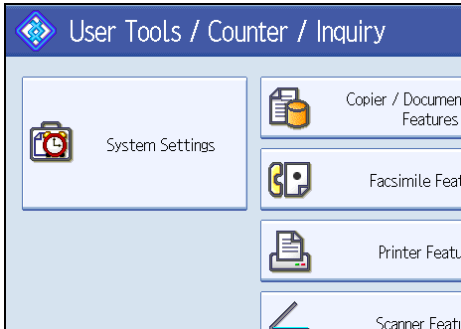
Select the protocol for the IP-Fax transmission.

This setting only works if the IP-Fax function has been selected.

Registering a Fax Destination

This section describes how to register a fax destination.

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



3. Press [Administrator Tools].
4. Press [Address Book Management].
5. Check that [Program / Change] is selected.
6. Select the name whose fax destination you want to register.
Press the name key, or enter the registered number using the number keys.
7. Press [Fax Dest.].
8. Press [Change] under "Fax Destination".
9. Enter the fax number using the number keys, and then press [OK].



10. Specify optional settings such as "SUB Code", "SEP Code", and "International TX Mode".
11. Press [OK].
12. Press [Exit].
13. Press the [User Tools / Counter] key.

Note

- To register the name, see "Registering Names".
- When a group is registered, you can also add this fax destination to the group. For details about registering groups, see "Registering Names to a Group".

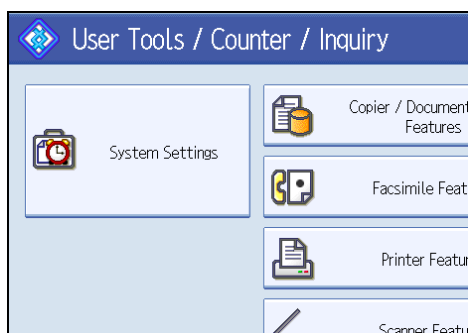
Reference

- p.255 "Registering Names"
- p.303 "Registering Names to a Group"

Changing a Fax Destination

This section describes how to change a registered fax destination.

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



3. Press [Administrator Tools].
4. Press [Address Book Management].
5. Check that [Program / Change] is selected.
6. Select the name whose fax destination you want to change.

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

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

7. Press [Fax Dest.].
8. Change the settings.
9. Press [OK].
10. Press [Exit].
11. Press the [User Tools / Counter] key.

Note

- To change the name, key display and title, see "Registering Names".

Reference

- p.255 "Registering Names"

To change the fax number

This section describes how to change the fax number.

1. Press [Change] under "Fax Destination".
2. Enter the new fax number using the number keys, and then press [OK].

To select line

This section describes how to select the line.

1. Press [Select Line] under "Fax Destination".
2. Select the using line.
3. Press [OK].

5

To program the SUB Code

This section describes how to program the SUB Code.

1. Press [Adv. Features], and then press [SUB Code].
2. Press [Change] under "TX SUB Code".
3. Enter the new SUB Code, and then press [OK].
4. To change the password, press [Change] under "Password (SID)".
5. Enter the new password, and then press [OK].
6. Press [OK].

To program the SEP Code

This section describes how to program the SEP Code.

1. Press [Adv. Features], and then press [SEP Code].
2. Press [Change] under "RX SEP Code".
3. Enter the new SEP Code, and then press [OK].
4. To change the password, press [Change] under "Password (PWD)".
5. Enter the new password, and then press [OK].
6. Press [OK].

To set the International TX Mode

This section describes how to set the International TX Mode.

1. Press [Change] under "International TX Mode".
2. Select [Off] or [On], and then press [OK].

To select the fax header

This section describes how to select the fax header.

You can register the fax header in Program Fax Information in the system settings for Facsimile Features.

1. Press [Change] under "Fax Header".
2. Select [1st Name] or [2nd Name], and then press [OK].

To set label insertion

This section describes how to set label insertion.

When Label Insertion is set to ON, the receiver's name and standard messages are printed on the fax message when it is received at the other end.

1. Press [Change] under "Label Insertion".
2. Press [On].
3. Press [Change] under "Line 2".
4. Select the new standard message or press [Manual Entry] to enter the new message.
5. Enter the new message, and then press [OK].
6. Press [OK].
7. Press [Change] under "Line 3".
8. Select the new standard message, and then press [OK].
9. Press [OK].

Note

- To change the name, key display and title, see "Registering Names".

Reference

- p.255 "Registering Names"

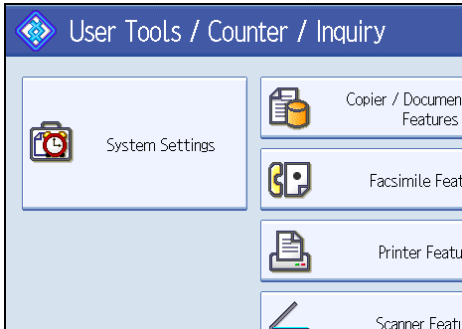
Deleting a Fax Destination

This section describes how to delete a registered 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 [System Settings].



5

3. Press [Administrator Tools].
4. Press [Address Book Management].
5. Check that [Program / Change] is selected.
6. 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, fax number, folder name, e-mail address, or IP-Fax destination.

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



10. Press [OK].
11. Press [Exit].

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

↓ Note

- To delete the name, key display, and title, see "Registering Names".

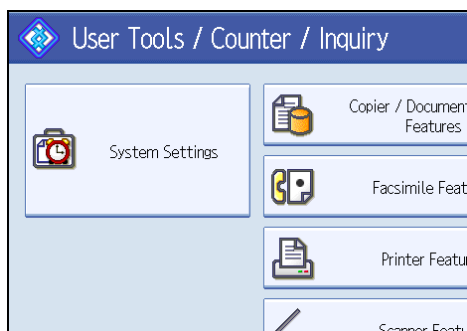
📖 Reference

- p.255 "Registering Names"

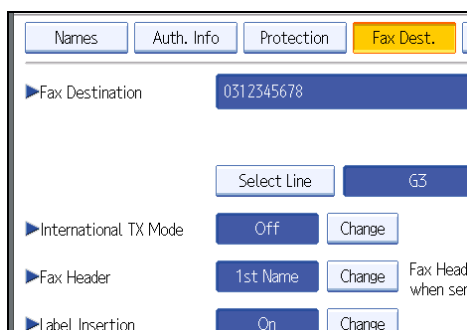
Registering an IP-Fax Destination

This section describes how to register an IP-Fax Destination.

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



3. Press [Administrator Tools].
4. Press [Address Book Management].
5. Check that [Program / Change] is selected.
6. Select the name whose IP-Fax destination you want to register.
Press the name key, or enter the registered number using the number keys.
7. Press [Fax Dest.].
8. Press [Select Line], and then select [H.323] or [SIP].



9. Press [OK].
10. Press [Change] under "Fax Destination".
11. Enter the IP-Fax destination.
12. Press [OK].
13. Press [OK].
14. Press [Exit].
15. Press the [User Tools / Counter] key.

Note

- To register the name, see "Registering Names".

Reference

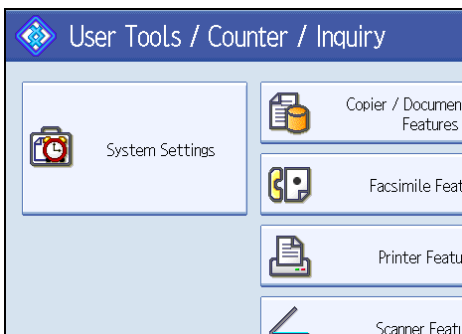
- p.255 "Registering Names"

5

Changing a Registered IP-Fax Destination

This section describes how to change an IP-Fax Destination.

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

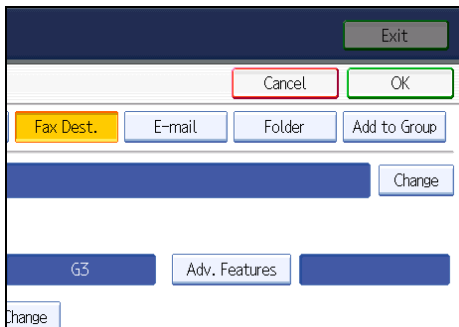


3. Press [Administrator Tools].
4. Press [Address Book Management].
5. Check that [Program / Change] is selected.
6. Select the name whose IP-Fax destination you want to change.

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

7. Press [Fax Dest.].

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



Enter the new destination, and then press [OK].

9. Press [OK].

10. Press [Exit].

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

↓ Note

- To change the name, key display and title, see "Registering Names".

📖 Reference

- p.255 "Registering Names"

To change the IP-Fax Destination

This section describes how to change a registered IP-Fax destination.

1. Press [Change] under "Use Name as".
2. Enter the new destination, and then press [OK].

To change the protocol

This section describes how to select the protocol.

1. Press [Select Line].
2. Select [H.323] or [SIP].
3. Press [OK].

To program the SUB Code

This section describes how to program the SUB Code.

1. Press [Adv. Features], and then press [SUB Code].

2. Press [Change] under "TX SUB Code".
3. Enter the SUB Code, and then press [OK].
4. To enter a password, press [Change] under "Password (SID)".
5. Enter a password using the number keys, and then press [OK].
6. Press [OK].

To program the SEP Code

This section describes how to program the SEP Code.

1. Press [Adv. Features], and then press [SEP Code].
2. Press [Change] under "RX SEP Code".
3. Enter a SEP Code using the number keys, and then press [OK].
4. To enter a password, press [Change] under "Password (PWD)".
5. Enter a password using the number keys, and then press [OK].
6. Press [OK].

5

To select the fax header

This section describes how to select the fax header.

1. Press [Change] under "Fax Header".
2. Select [1st Name] or [2nd Name], and then press [OK].

To set label insertion

This section describes how to set label insertion.

When Label Insertion is set to ON, the receiver's name and standard messages are printed on the fax message when it is received at the other end.

1. Press [Change] under "Label Insertion".
2. Press [On].
3. Press [Change] under "Line 2".
4. Select the new standard message or press [Manual Entry] to enter the new message.
5. Enter the new message, and then press [OK].
6. Press [OK].
7. Press [Change] under "Line 3".
8. Select the new standard message, and then press [OK].

9. Press [OK].

↓ Note

- To change the name, key display and title, see "Registering Names".

📖 Reference

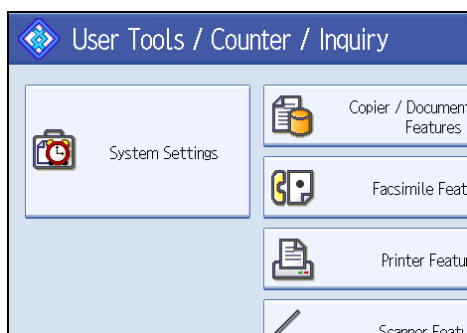
- p.255 "Registering Names"

Deleting a Registered IP-Fax Destination

This section describes how to delete a registered IP-Fax destination.

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 [System Settings].



3. Press [Administrator Tools].
4. Press [Address Book Management].
5. Press [Program / Change].
6. Select the name whose IP-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, fax number, folder name, e-mail address, or IP-Fax destination.

7. Press [Fax Dest.].
8. Press [Change] under "Fax Destination".
9. Press [Delete All], and then press [OK].
10. Press [OK].
11. Press [Exit].

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

↓ Note

- To delete the name, key display and title, see "Registering Names".

📖 Reference

- p.255 "Registering Names"

E-mail Destination

This section describes the procedure for registering, changing, and deleting E-mail Destination.

Register e-mail destinations so you do not need to enter an e-mail address every time, and can send scan files from scanner or fax function by e-mail.

- It is easy to select the e-mail destination if you register "Name" and "Key Display" as the e-mail destination.
- You can register e-mail destinations as a group.
- You can use the e-mail address as the sender's address when sending scan files in scanner mode. If you want to do this, set a protection code on the sender address to prevent unauthorized access.

↓ Note

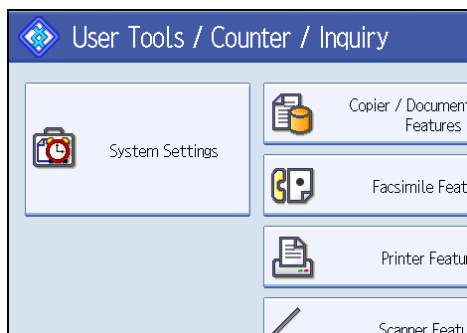
- You can select an e-mail address from an LDAP server, and then register it in the Address Book. See "Sending Scan Files by E-mail", Scanner Reference.
- You can set the machine to send a Transmission Result Report by e-mail whenever a transmission is sent. See Facsimile Reference.

5

Registering an E-mail Destination

This section describes how to register an e-mail destination.

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

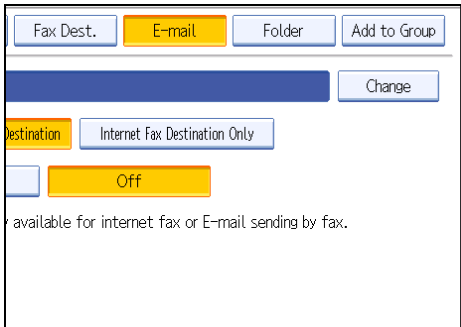


3. Press [Administrator Tools].
4. Press [Address Book Management].
5. Check that [Program / Change] is selected.
6. Select the name whose e-mail address you want to register.

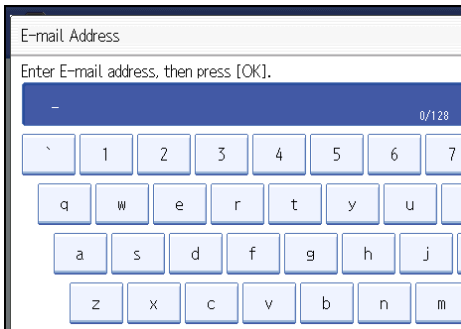
Press the name key, or enter the registered number using the number keys.

7. Press [E-mail].

8. Press [Change].



9. Enter the e-mail address.



10. Press [OK].

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

If [E-mail / Internet Fax Destination] is specified, registered e-mail addresses appear in both 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.

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

13. Press [OK].

14. Press [Exit].

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

Note

- You can enter up to 128 characters for the e-mail address.
- To register the name, see "Registering Names".

Reference

- p.255 "Registering Names"

Changing an E-mail Destination

This section describes how to change an e-mail destination.

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

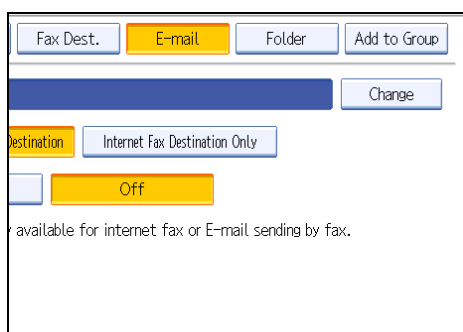


3. Press [Administrator Tools].
4. Press [Address Book Management].
5. Check that [Program / Change] is selected.
6. Select the name whose e-mail address you want to change.

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

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

7. Press [E-mail].
8. Press [Change] under "E-mail Address".



9. Enter the e-mail address, and then press [OK].
10. Press [OK].
11. Press [Exit].
12. Press the [User Tools / Counter] key.

↓ Note

- To change the name, key display and title, see "Registering Names".

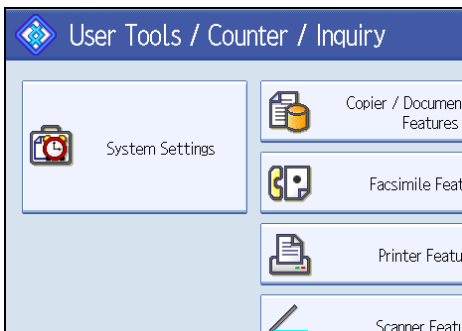
📖 Reference

- p.255 "Registering Names"

Deleting an E-mail Destination

This section describes how to delete an e-mail destination.

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



3. Press [Administrator Tools].
4. Press [Address Book Management].
5. Check that [Program / Change] is selected.
6. 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, fax number, folder name, e-mail address, or IP-Fax destination.

7. Press [E-mail].
8. Press [Change] under "E-mail Address".
9. Press [Delete All], and then press [OK].
10. Press [OK].
11. Press [Exit].
12. Press the [User Tools / Counter] key.

↓ Note

- To delete the name, key display and title, see "Registering Names".

 **Reference**

- p.255 "Registering Names"

Registering Folders

This section describes the procedure for registering, changing, and deleting folders.

By registering a shared folder, you can send scan files or received fax documents to it directly.

There are three types of protocol you can use:

- SMB
For sending files to shared Windows folders.
- FTP
Use when sending files to an FTP server.
- NCP
Use when sending files to a NetWare server.

↓ Note

- For details about protocols, server names, and folder levels, consult your network administrator.
- You can prevent unauthorized users from accessing folders from the machine. See "Registering a Protection Code".
- You can only select either SMB, FTP, or NCP. If you change protocol after finishing your settings, all previous entries are cleared.

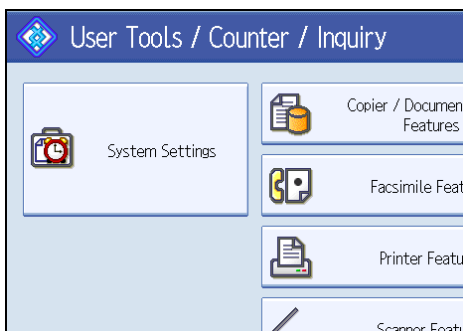
📖 Reference

- p.313 "Registering a Protection Code"

Registering an SMB Folder

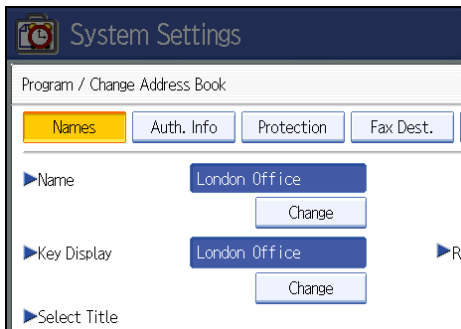
This section describes how to register an SMB folder.

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



3. Press [Administrator Tools].

4. Press [Address Book Management].
5. Check that [Program / Change] is selected.
6. Select the name whose folder you want to register.
Press the name key, or enter the registered number using the number keys.
7. Press [Auth. Info], and then press [▼Next].

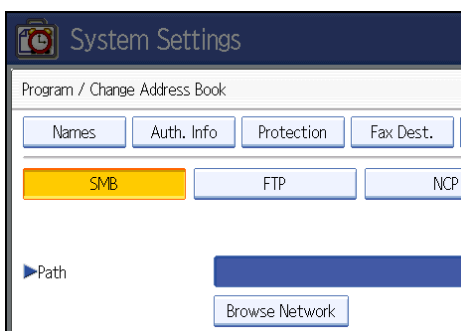


8. Press [Specify Other Auth. Info] on the right side of Folder Authentication.

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

9. Press [Change] under "Login User Name".
10. Enter the login user name, and then press [OK].
11. Press [Change] under "Login Password".
12. Enter the password, and then press [OK].
13. Enter the password again to confirm, and then press [OK].
14. Press [Folder].
15. Press [SMB].

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



16. Specify the path.

For details about how to specify the path manually, see "Locating the SMB folder manually".

For details about how to specify the path using Browse Network, see "Locating the SMB folder using Browse Network".

17. Press [Connection Test] to check the path is set correctly.

18. Press [Exit].

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

19. Press [OK].

20. Press [Exit].

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

Note

- To register the name, see "Registering Names".
- You can enter up to 64 characters for the user name.
- You can enter up to 64 characters for the password.
- You can enter a path using up to 128 characters.
- If User Authentication is specified, contact your administrator.

Reference

- p.255 "Registering Names"

Locating the SMB folder manually

This section describes how to locate the SMB folder manually.

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

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

Note

- Enter the path using this format: "\\ServerName\Share- Name\PathName".
- You can also enter an IPv4 address.
- You can enter a path using up to 128 characters.

Locating the SMB folder using Browse Network

This section describes how to locate the SMB folder using Browse Network.

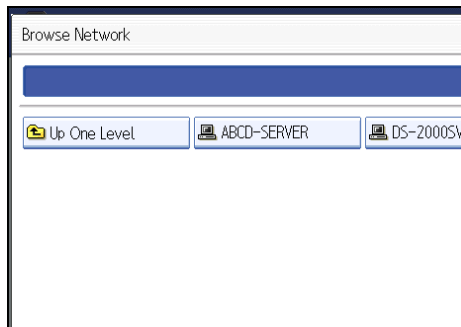
1. Press **[Browse Network]**.

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

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

2. Select a client computer.

Shared folders under it appear.



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

3. Select the folder you want to register.

4. Press **[OK]**.

If a Login Screen Appears

This section describes how to log on to the machine if the login screen appears when you try to access a folder by browsing the network.

If you have not specified folder authentication, or if an incorrect user name or password has been entered for folder authentication, the login screen appears.

1. Enter the login user name, and then press **[OK]**.

Enter the login user name specified for folder authentication.

2. Enter the password, and then press **[OK]**.

The path to the selected folder appears.

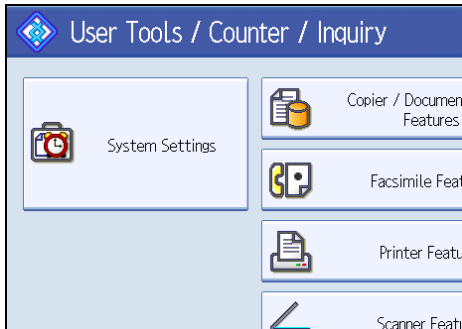
If a message appears, press **[Exit]**, and then enter the login user name and password again.

Changing an SMB Folder

This section describes how to change settings of the registered SMB folder.

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

2. Press [System Settings].



3. Press [Administrator Tools].

4. Press [Address Book Management].

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

5

6. Select the name whose folder you want to change.

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

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

7. Press [Folder].

8. Select the items you want to change.

When specifying a folder, enter the path directly or select it by referencing the network. For more information, see "Locating the SMB folder manually" and "Locating the SMB folder using Browse Network".

9. Press [Connection Test] to check the path is set correctly.

10. Press [Exit].

11. Press [OK].

12. Press [Exit].

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

↓ Note

- To change the name, key display and title, see "Registering Names".

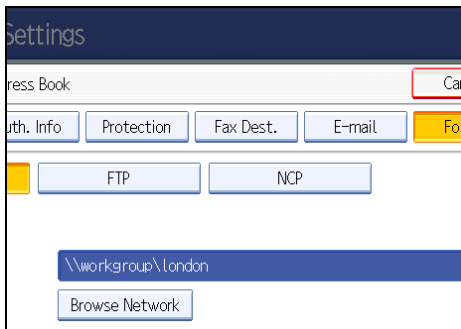
📖 Reference

- p.255 "Registering Names"

Changing the protocol

This section describes how to change the protocol.

1. Press [FTP] or [NCP].



A confirmation message appears.

2. Press [Yes].

Changing the protocol will clear all settings made under the previous protocol.

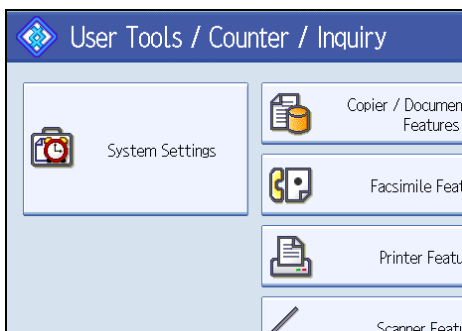
3. Enter each item again.

5

Deleting an SMB registered folder

This section describes how to delete the registered SMB folder.

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



3. Press [Administrator Tools].
4. Press [Address Book Management].
5. Check that [Program / Change] is selected.
6. 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, fax number, folder name, e-mail address, or IP-Fax destination.

7. Press [Folder].
8. Press the protocol which is not currently selected.
A confirmation message appears.
9. Press [Yes].
10. Press [OK].
11. Press [Exit].
12. Press the [User Tools / Counter] key.

Note

- To delete the name, key display and title, see "Registering Names".

Reference

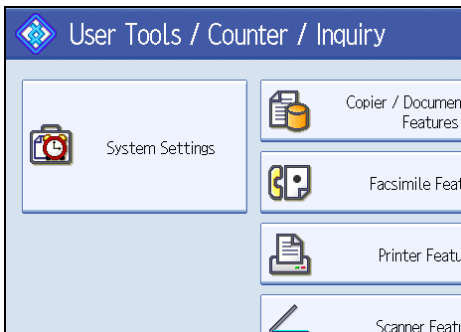
- p.255 "Registering Names"

5

Registering an FTP Folder

This section describes how to register an FTP folder.

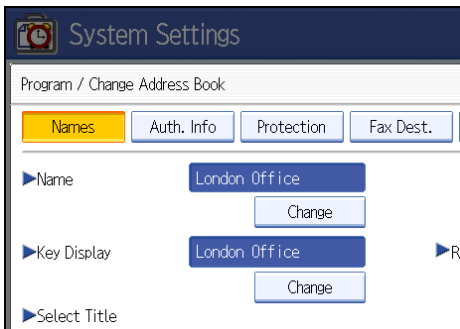
1. Press the [User Tools / Counter] key.
2. Press [System Settings].



3. Press [Administrator Tools].
4. Press [Address Book Management].
5. Check that [Program / Change] is selected.
6. Select the name whose folder you want to register.

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

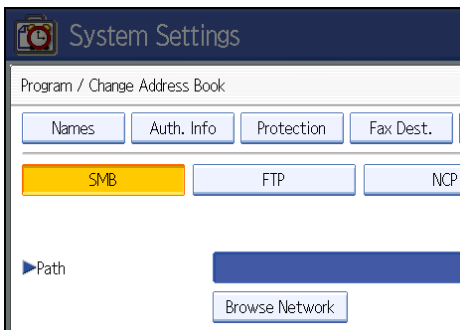
7. Press [Auth. Info], and then press [▼Next].



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

When [Do not Specify] is selected, the FTP User Name and FTP Password that you have specified in Default User Name/Password (Send) of File Transfer settings applies. For details, see "File Transfer".

9. Press [Change] under "Login User Name".
10. Enter the login user name, and then press [OK].
11. Press [Change] under "Login Password".
12. Enter the password, and then press [OK].
13. Enter the password again to confirm, and then press [OK].
14. Press [Folder].
15. Press [FTP].



16. Press [Change] under "Server Name".
17. Enter the server name, and then press [OK].
18. Press [Change] under "Path".
19. Enter the path, and then press [OK].

You can enter an absolute path, using this format: "\\user\home\username"; or a relative path, using this format: "directory\sub-directory".

If you leave the path blank, the login directory is assumed to be the current working directory.

You can also enter an IPv4 address.

You can enter a path using up to 256 characters.

20. To change the port number, press [Change] under "Port Number".
21. Enter the port number using the number keys, and then press the [#] key.
You can enter 1 to 65535.
22. Press [Connection Test] to check the path is set correctly.
23. Press [Exit].
If the connection test fails, check the settings, and then try again.
24. Press [OK].
25. Press [Exit].
26. Press the [User Tools / Counter] key.

Note

- To register the name, see "Registering Names".
- You can enter up to 191 characters for the user name.
- You can enter up to 128 characters for the password.
- You can enter a server name using up to 64 characters.
- If User Authentication is specified, contact your administrator.

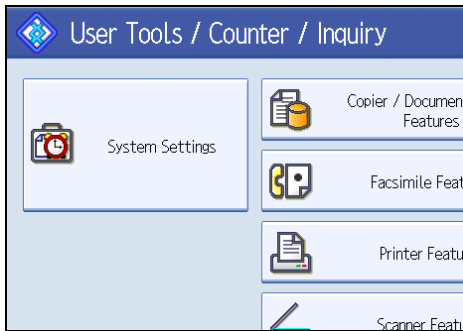
Reference

- p.42 "File Transfer"
- p.255 "Registering Names"

Changing an FTP folder

This section describes how to change the registered FTP folder.

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



3. Press [Administrator Tools].
4. Press [Address Book Management].
5. Check that [Program / Change] is selected.
6. Select the name whose folder you want to change.
Press the name key, or enter the registered number using the number keys.
You can search by the registered name, fax number, folder name, e-mail address, or IP-Fax destination.
7. Press [Folder].
8. Select the items you want to change.
9. Press [Connection Test] to check the path is set correctly.
10. Press [Exit].
11. Press [OK].
12. Press [Exit].
13. Press the [User Tools/Counter] key.

↓ Note

- To change the name, key display and title, see "Registering Names".

📖 Reference

- p.255 "Registering Names"

Changing the protocol

This section describes how to change the protocol.

1. Press [SMB] or [NCP].

Names	Auth. Info	Protection	Fax Dest.
SMB	FTP	NCP	
▶ Server Name	abcserver		
▶ Path	user/home/username		
▶ Port Number	21	Change	

A confirmation message appears.

2. Press [Yes].

Changing the protocol will clear all settings made under the previous protocol.

3. Enter each item again.

Changing the registered FTP folder

This section describes how to change the registered FTP folder.

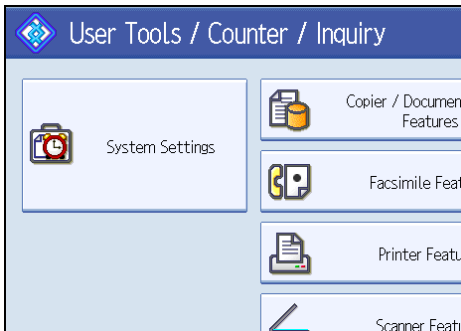
1. Press [Change] under "Port Number".
2. Enter the new port number, and then press the [#] key.
3. Press [Change] under "Server Name".
4. Enter the new server name, and then press [OK].
5. Press [Change] under "Path".
6. Enter the new path, and then press [OK].

5

Deleting an FTP folder

This section describes how to delete the registered FTP folder.

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



3. Press [Administrator Tools].
4. Press [Address Book Management].
5. Check that [Program / Change] is selected.
6. 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, fax number, folder name, e-mail address, or IP-Fax destination.

7. Press [Folder].

8. Press the protocol which is not currently selected.

A confirmation message appears.

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

- To delete a name entirely, see "Registering Names".

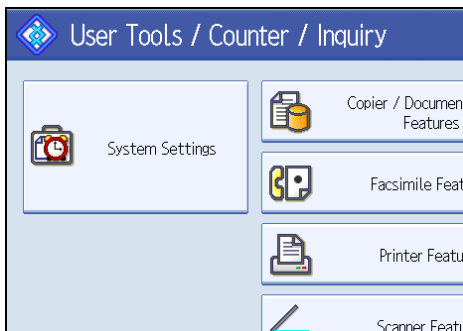
📖 Reference

- p.255 "Registering Names"

Registering an NCP folder

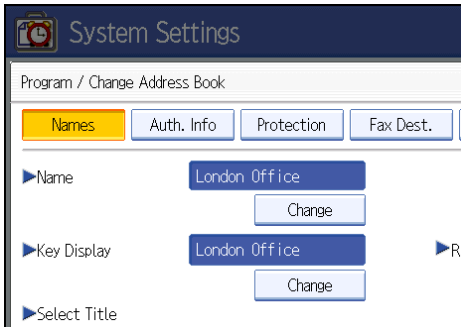
5

This section describes how to register an NCP folder.

1. Press the [User Tools / Counter] key.**2. Press [System Settings].****3. Press [Administrator Tools].****4. Press [Address Book Management].****5. Check that [Program / Change] is selected.****6. Press the name you want to register or enter the registered number using the number keys.**

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

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



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

When [Do not Specify] is selected, the NCP User Name and NCP Password that you have specified in Default User Name/Password (Send) of File Transfer settings applies. For details, see "File Transfer".

5

9. Press [Change] under "Login User Name".

10. Enter the login user name, and then press [OK].

11. Press [Change] under "Login Password".

12. Enter the password, and then press [OK].

13. Enter the password again to confirm, and then press [OK].

14. Press [Folder].

15. Press [NCP].



16. Select "Connection Type".

If you want to specify a folder in an NDS tree, press [NDS]. If you want to specify a folder on a NetWare server, press [Bindery].

If you have set "Connection Type" to [NDS], enter the user name followed by the name of the context where the user object is located. If the user name is "user" and the context name is "context", enter "user.context".

17. Specify the path.

For details about how to specify the path manually, see "Locating the NCP folder manually".

For details about how to specify the path using Browse Network, see "Locating the NCP folder using Browse Network".

18. Press [Connection Test] to check the path is set correctly.

19. Press [Exit].

20. Press [OK].

21. Press [Exit].

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

Note

- To register the name, see "Registering Names".
- You can enter up to 128 characters for the user name.
- You can enter up to 64 characters for the password.
- To specify a folder, you can either enter the path manually or locate the folder by browsing the network.
- If User Authentication is specified, contact your administrator.

Reference

- p.42 "File Transfer"
- p.255 "Registering Names"

Locating the NCP folder manually

This section describes how to locate the NCP folder manually.

1. Press [Change] under "Path".

2. Enter the path where the folder is located.

3. Press [OK].

4. Press [Connection Test] to check the path is set correctly.

5. Press [Exit].

Note

- If you set "Connection Type" to [NDS], and if the NDS tree name is "tree", the name of the context including the volume is "context", the volume name is "volume" and the folder name is "folder", then the path will be "\\tree\volume\context\folder".
- If you set "Connection Type" to [Bindery], and if the NetWare server name is "server", the volume name is "volume" and the folder name is "folder", then the path will be "\\server\volume\folder".
- You can enter a path using up to 256 characters.
- If the connection test fails, check the settings, and then try again.

Locating the NCP folder using Browse Network

This section describes how to locate the NCP folder using Browse Network.

1. Press [Browse Network].
2. If you have set "Connection Type" to [NDS], a list of items in the NDS tree appears. If you have set "Connection Type" to [Bindery], a list of items on the NetWare server appears.
3. Search for the destination folder in the NDS tree or NetWare server.

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

4. Select the folder you want to register.
5. Press [OK].

↓ Note

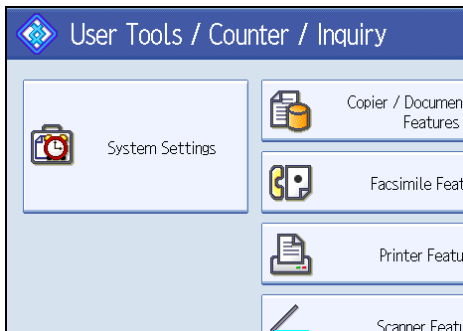
- Only the folders you are allowed to access appear in [Browse Network].
- If the languages used on the machine and the destination you want to view differ, the items in the list may not appear correctly.
- Up to 100 items can be displayed in the list.

5

Changing an NCP registered folder

This section describes how to change the registered NCP folder.

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



3. Press [Administrator Tools].
4. Press [Address Book Management].
5. Check that [Program / Change] is selected.
6. Select the user of the registered folder you want to change.

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

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

7. Press [Folder].

8. Select "Connection Type".

If you want to specify a folder in an NDS tree, press [NDS]. If you want to specify a folder on a NetWare server, press [Bindery].

9. Specify the folder.

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

10. Press [Connection Test] to check the path is set correctly.

11. Press [Exit].

12. Press [OK].

13. Press [Exit].

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

Note

- To change the name, key display and title, see "Registering Names".

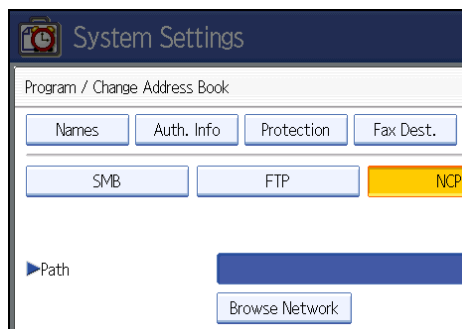
Reference

- p.255 "Registering Names"

Changing the protocol

This section describes how to change the protocol.

1. Press [SMB] or [FTP].



2. A confirmation message appears. Press [Yes].

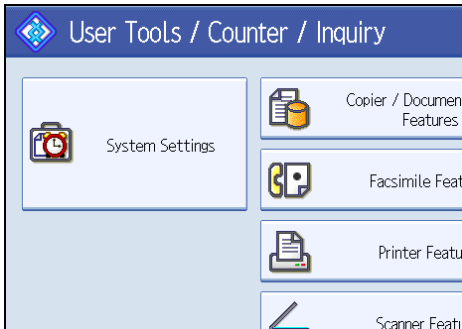
Changing the protocol will clear all settings made under the previous protocol.

3. Enter each item again.

Deleting an NCP folder

This section describes how to delete the registered NCP folder.

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



5

3. Press [Administrator Tools].
4. Press [Address Book Management].
5. Check that [Program / Change] is selected.
6. Select a user of the 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, fax number, folder name, e-mail address, or IP-Fax destination.

7. Press [Folder].
8. Press the protocol which is not currently selected.
A confirmation message appears.
9. Press [Yes].
10. Press [OK].
11. Press [Exit].
12. Press the [User Tools / Counter] key.

Note

- To delete a name entirely, see "Registering Names".

Reference

- p.255 "Registering Names"

Registering Names to a Group

This section describes how to register names to a group.

You can register names to a group to enable easy management of e-mail addresses and folders for each group.

To add names to a group, the groups must be registered beforehand.

★ Important

- When using Scan to Folder function, you cannot send scan files to a group with over 50 folders registered.
- The maximum number of destinations registerable to a group is 100.

↓ Note

- You can set a protection code to prevent unauthorized access to the folders registered in a group. For details, see "Registering a Protection Code".

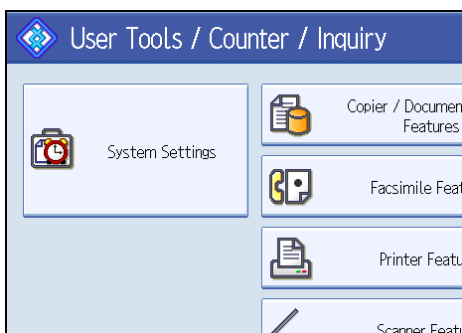
📖 Reference

- p.313 "Registering a Protection Code"

Registering a Group

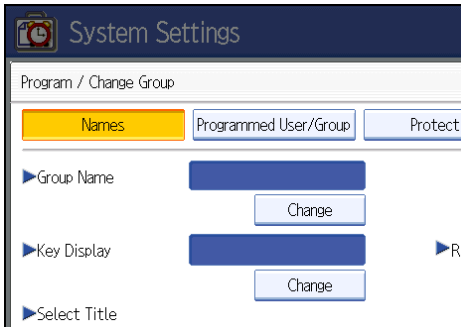
This section describes how to register a group.

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



3. Press [Administrator Tools].
4. Press [Address Book: Program / Change / Delete Group].
5. Check that [Program / Change] is selected.
6. Press [New Program].

7. Press [Change] under "Group Name".



8. Enter the group name, and then press [OK].

The Key Display name is set automatically.

9. Press the title key under "Select Title", if necessary.

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 page for each title.

10. When you want to change the key display, press [Change] under "Key Display".

11. Enter the key display, and then press [OK].

12. Press [OK].

13. Press [Exit].

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

Registering Names to a Group

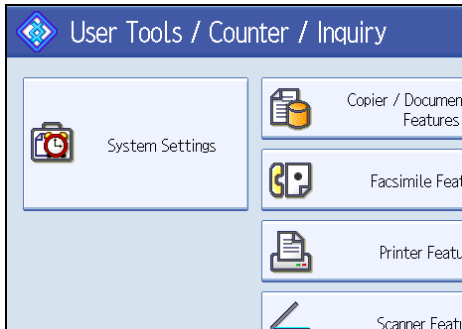
This section describes how to register names to a registered group.

You can put names that have been registered in the Address Book into a group.

When registering new names, you can also register groups at the same time.

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

2. Press [System Settings].



3. Press [Administrator Tools].

4. Press [Address Book Management].

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

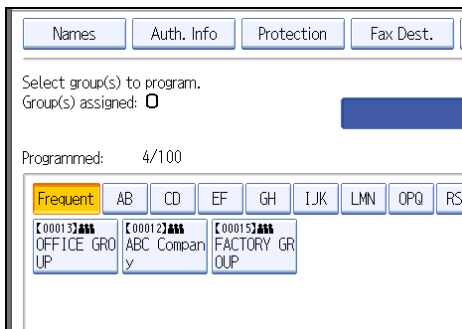
6. Select the name to register in a group.

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

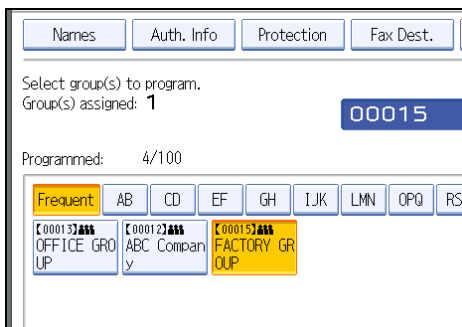
You can search by the registered name, fax number, folder name, e-mail address, or IP-Fax destination.

7. Press [Add to Group].

8. Select a group to which you want to add the name.



The group key that you have selected becomes highlighted, and the name is added to it.

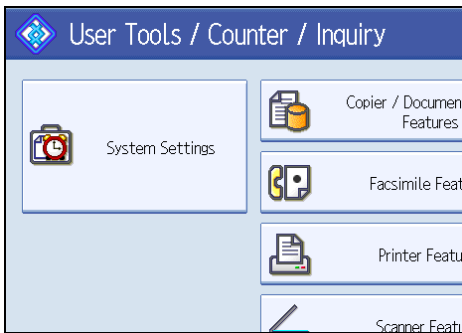


9. Press [OK].
10. Press [Exit].
11. Press the [User Tools / Counter] key.

Adding a Group to Another Group

This section describes how to add a group to another group.

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

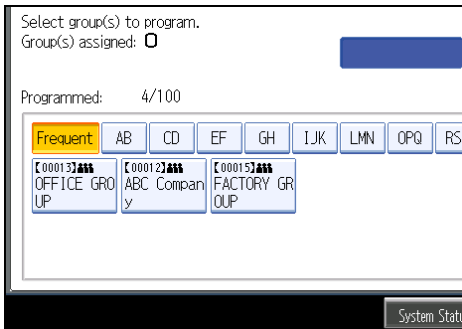


3. Press [Administrator Tools].
4. Press [Address Book: Program / Change / Delete Group].
5. Check that [Program / Change] is selected.
6. Select the group that you want to put into another group.

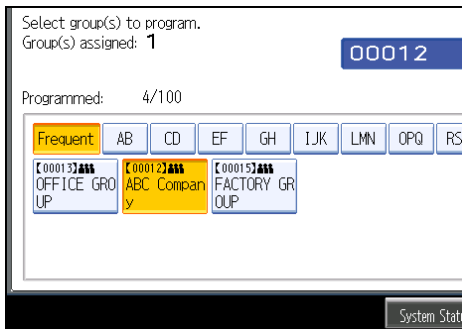
Press the group key, or enter the registered number using the number keys.

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

7. Press [Add to Group].
8. Select the group to which you want to add.



The group key that you have selected becomes highlighted, and the group is added to it.



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

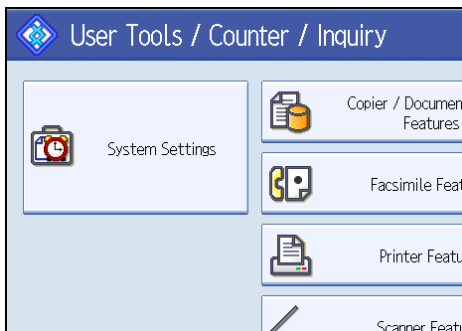
5

Displaying Names Registered in a Group

This section describes how to display names registered in a group.

You can check the names or groups registered in each group.

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



3. Press [Administrator Tools].
4. Press [Address Book: Program / Change / Delete Group].
5. Check that [Program / Change] is selected.
6. Select the group where the members you want to check is registered.

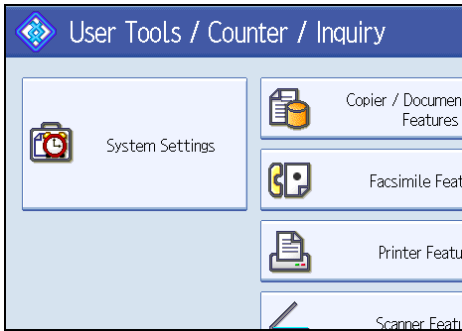
You can search by the registered name, fax number, folder name, e-mail address, or IP-Fax destination.

7. Press **[Programmed User / Group]**.
All the names registered will be displayed.
8. Press **[OK]**.
9. Press **[Exit]**.
10. Press the **[User Tools / Counter]** key.

Removing a Name from a Group

This section describes how to remove a name from a group.

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



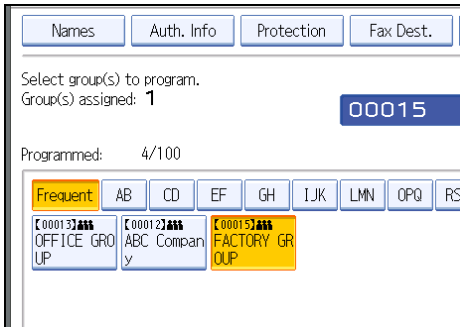
3. Press **[Administrator Tools]**.
4. Press **[Address Book Management]**.
5. Check that **[Program / Change]** is selected.
6. Select the name to remove from a group.

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

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

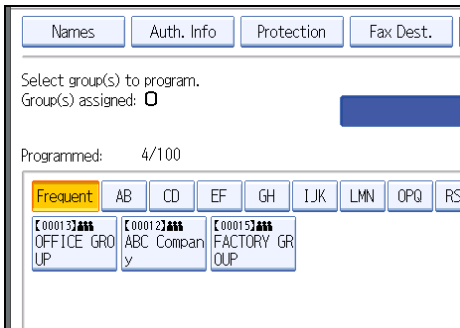
7. Press **[Add to Group]**.

8. Select the group from which you want to remove the name.



The group key is deselected and the name is removed from it.

9. Press [OK].



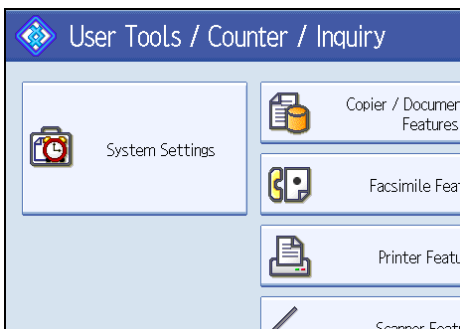
10. Press [Exit].

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

Deleting a Group Within Another Group

This section describes how to delete a group within another group.

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



3. Press [Administrator Tools].
4. Press [Address Book: Program / Change / Delete Group].
5. Check that [Program / Change] is selected.
6. Select the group that you want to delete from.

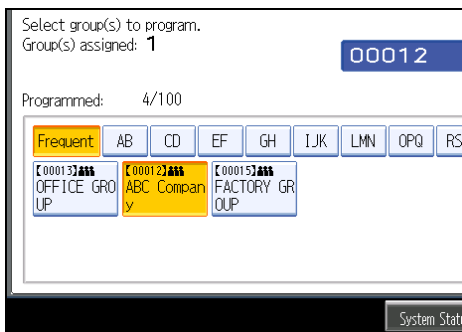
Press the group key, or enter the registered number during the number keys.

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

7. Press [Add to Group].

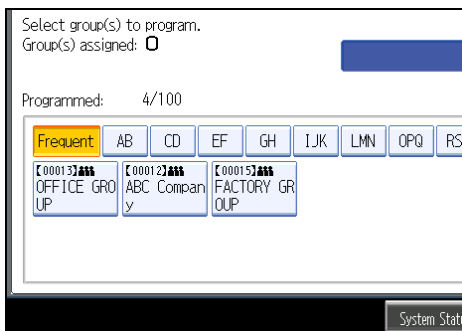
The keys of groups in which the group is registered appear highlighted.

8. Select the group that you want to delete from.



The group key is deselected and the group is deleted from it.

9. Press [OK].

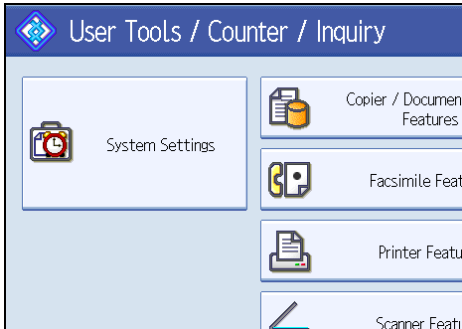


10. Press [Exit].
11. Press the [User Tools / Counter] key.

Changing a Group Name

This section describes how to change a group name.

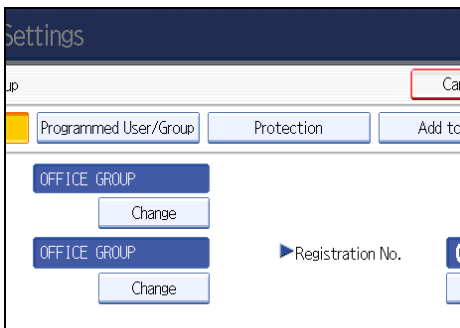
1. Press the [User Tools / Counter] key.
2. Press [System Settings].



3. Press [Administrator Tools].
4. Press [Address Book: Program / Change / Delete Group].
5. Check that [Program / Change] is selected.
6. Press the group key you want to change.

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

7. To change the group name and key display, press [Change] under "Group Name" or "Key Display".

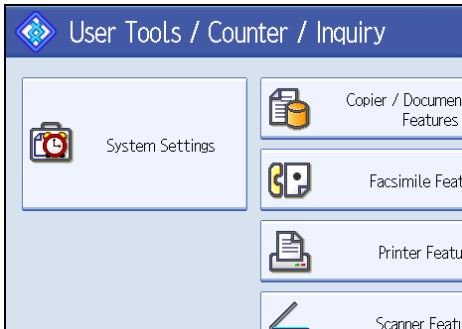


8. Enter the new group name or key display, and then press [OK].
9. To change the title, press the title key under "Select Title".
10. To change the registration number, press [Change] under "Registration No.".
11. Enter the new registration number using the number keys.
12. Press the [#] key.
13. Press [OK].
14. Press [Exit].
15. Press the [User Tools / Counter] key.

Deleting a Group

This section describes how to delete a group.

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



3. Press [Administrator Tools].
4. Press [Address Book: Program / Change / Delete Group].
5. Press [Delete].
6. Press a group key you want to delete.
You can search by the registered name, fax number, folder name, e-mail address, or IP-Fax destination.
7. Press [Yes].
8. Press [Exit].
9. Press the [User Tools / Counter] key.

Registering a Protection Code

This section describes how to register a Protection Code.

You can stop sender's names or folders being accessed by setting a protection code.

You can use this function to protect the following:

- Folders
You can prevent unauthorized access to folders.
- Sender's names
You can prevent misuse of sender's names.

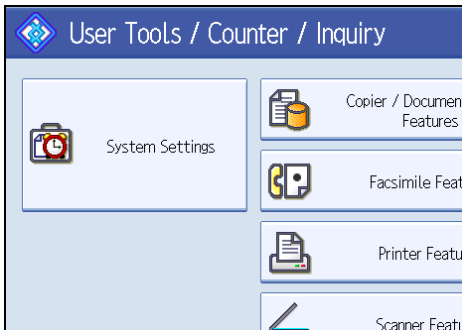
Registering a Protection Code to a Single User

This section describes how to register a Protection code to a single user.

5

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

2. Press [System Settings].



3. Press [Administrator Tools].

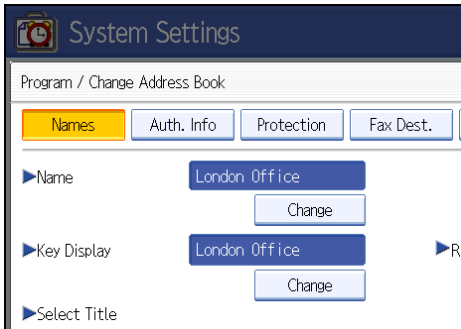
4. Press [Address Book Management].

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

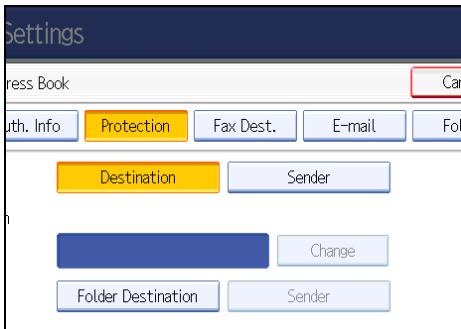
6. Select the name whose protection code you want to register.

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

7. Press [Protection].



8. Press [Destination] or [Sender] under "Use Name as".



Both [Destination] and [Sender] can be selected at the same time.

9. Press [Change] under "Protection Code".

10. Enter a protection code using the number keys, and then press the [#] key.

11. Press [OK].

12. Press [Exit].

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

Note

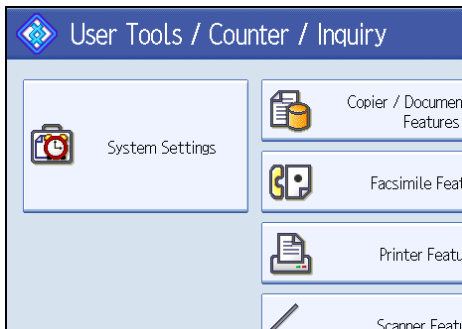
- Specify a protection code of up to eight digits. You can also specify "Protection" without specifying a protection code.
- To change the protection code settings, repeat step 3 to 11.

Registering a Protection Code to a Group User

This section describes how to register a Protection Code to a Group User.

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

2. Press [System Settings].



3. Press [Administrator Tools].

4. Press [Address Book: Program / Change / Delete Group].

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

6. Press the group key you want to register or enter the registered number using the number keys.

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

7. Press [Protection].

8. Press [Folder Destination] under "Protection Object".

9. Press [Change] under "Protection Code".

10. Enter a protection code using the number keys, and then press the [#] key.

11. Press [OK].

12. Press [Exit].

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

Note

- Specify a protection code of up to eight digits. You can also specify "Protection" without specifying a protection code.
- To change the protection code settings, repeat step 3 to 11.

Registering SMTP and LDAP Authentication

This section describes how to register SMTP and LDAP Authentication.

SMTP Authentication

This section describes how to register SMTP Authentication.

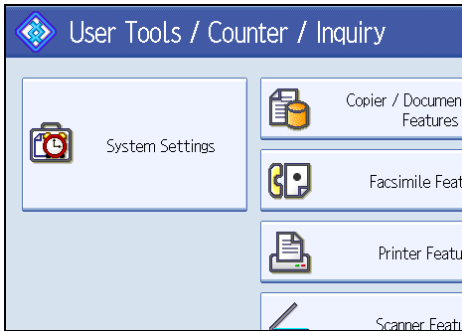
For each user registered in the Address Book, you can register a login user name and login password to be used when accessing an SMTP server.

To use an SMTP server, you need to program it beforehand.

★ Important

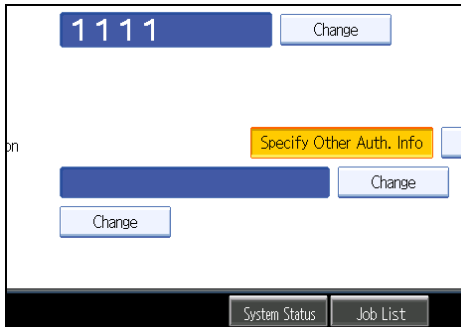
- When [Do not Specify] is selected for SMTP Authentication the User Name and Password that you have specified in SMTP Authentication of File Transfer settings applies. For details, see "File Transfer".

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



3. Press [Administrator Tools].
4. Press [Address Book Management].
5. Check that [Program / Change] is selected.
6. Press the name you want to register or enter the registered number using the number keys.
You can search by the registered name, fax number, folder name, e-mail address, or IP-Fax destination.
7. Press [Auth. Info].
8. Press [Specify Other Auth. Info] under "SMTP Authentication".

9. Press [Change] under "Login User Name".



10. Enter the login user name, and then press [OK].
11. Press [Change] under "Login Password".
12. Enter the password, and then press [OK].
13. Enter the password again to confirm, and then press [OK].
14. Press [OK].
15. Press [Exit].
16. Press the [User Tools / Counter] key.

Note

- To register the name, see "Registering Names".
- You can enter up to 191 characters for the user name.
- When using POP before SMTP Authentication, you can enter up to 63 characters.
- You can enter up to 128 characters for the password.
- To change the SMTP Authentication settings, repeat step 3 to 14.

Reference

- p.42 "File Transfer"
- p.255 "Registering Names"

LDAP Authentication

This section describes how to register LDAP Authentication.

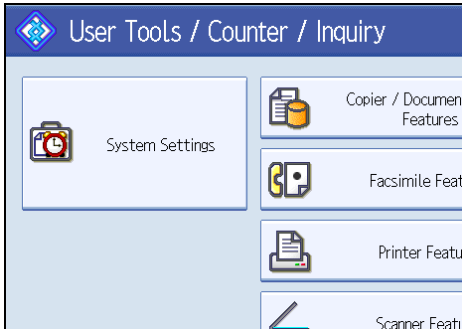
For each user registered in the Address Book, you can register a login user name and login password to be used when accessing an LDAP server.

To use an LDAP server, you need to program it beforehand. For details, see "Programming the LDAP server".

★ Important

- When [Do not Specify] is selected for LDAP Authentication, the User Name and Password that you have specified in Program / Change LDAP Server of Administrator Tools settings applies. For details, see "Programming the LDAP server".

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

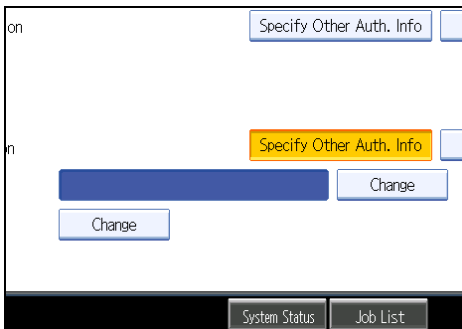


5

3. Press [Administrator Tools].
4. Press [Address Book Management].
5. Check that [Program / Change] is selected.
6. Press the name you want to register or enter the registered number using the number keys.

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

7. Press [Auth. Info], and then press [▼Next].
8. Press [Specify Other Auth. Info] under "LDAP Authentication".
9. Press [Change] under "Login User Name".



10. Enter the login user name, and then press [OK].
11. Press [Change] under "Login Password".
12. Enter the password, and then press [OK].

13. Enter the password again to confirm, and then press [OK].
14. Press [OK].
15. Press [Exit].
16. Press the [User Tools / Counter] key.

Note

- To register the name, see "Registering Names".
- You can enter up to 128 characters for the user name.
- You can enter up to 128 characters for the password.
- To change the LDAP Authentication settings, repeat step 3 to 14.

Reference

- p.59 "Programming the LDAP server"
- p.255 "Registering Names"

6. Special Operations under Windows

This chapter describes how to print files directly from Windows, or print with Bluetooth devices.

Printing Files Directly from Windows

You can print files directly using Windows commands. For example, you can print PostScript files for PostScript 3.

Windows 2000/XP/Vista, Windows Server 2003/2003 R2/2008

You can print files directly using `lpr`, `rcp`, `ftp` or `sftp` command.

Windows Vista, Windows Server 2008

You can not print files using `rcp` command.

Setup

Follow the procedure below to make network environment settings.

1. **Enable TCP/IP with the control panel, and then set up the printer's network environment about TCP/IP including IP addresses.**

TCP/IP of the printer is set as default.

2. **Install a TCP/IP in Windows to set up the network environment.**

Consult the network administrator for the local setting information.

3. **To print under Windows 2000/XP/Vista, Windows Server 2003/2003 R2/2008, install "Printing service for UNIX" as the network application.**

Reference

- p.331 "Using DHCP"

Using a Host Name Instead of an IPv4 Address

When a host name is defined, you can specify a printer by host name instead of IP address. The host names vary depending on the network environment.

When using DNS

Use the host name set to the data file on the DNS server.

When setting the IPv4 address of a printer using DHCP

Use the printer name on the configuration page as the host name.

In other cases

Add the IP address and host name of the network printer to the hosts file on the computer used for printing. Methods of addition vary depending on operating systems.

1. Open the hosts file using memo pad files, for instance.

The hosts file is in the following folder:

```
\WINNT\SYSTEM32\DRIVERS\ETC\HOSTS
```

"\WINNT" is the directory of the installation destination for Windows 2000/XP/Vista, and Windows Server 2003/2003 R2/2008.

2. Add an IPv4 or IPv6 address and host name to the hosts file using the following format:

```
192.168.15.16 host # NP
```

"192.168.15.16" is the IPv4 address, "host" is the printer's host name, and "#NP" is replaced by comments. Insert a space or tab between "192.168.15.16" and "host", between "host" and "#NP" respectively, using one line for this format.

```
2001:DB::100 host # NP
```

"2001:DB::100" is the IPv6 address, "host" is the printer's host name, and "#NP" is replaced by comments. Insert a space or tab between "2001:DB::100" and "host", between "host" and "#NP" respectively, using one line for this format.

3. Save the file.

↓ Note

- When using a host name under Windows Server 2003/2003 R2/2008, or Windows Vista, with IPv6 protocol, perform host name resolution using an external DNS server. The host file cannot be used.

Printing Commands

The following explains printing operations using the "lpr", "rcp", "ftp" and "sftp" commands.

Enter commands using the command prompt window. The location of the command prompts varies depending on operating systems:

- Windows 2000
[Start] - [Programs] - [Accessories] - [Command Prompt]
- Windows XP/Vista, Windows Server 2003/2003 R2/2008
[Start] - [All Programs] - [Accessories] - [Command Prompt]

Note

- Match the data format of the file to be printed with the emulation mode of the printer.
- If the message "print requests full" appears, no print jobs can be accepted. Try again when sessions end. For each command, the amount of possible sessions is indicated as follows:
 - lpr: 5 (When the spool printing function is available: 10)
 - rcp, rsh: 5
 - ftp: 3
 - sftp: 3
- Enter the file name in a format including the path from the directory executing commands.
- The "option" specified in a command is an intrinsic printer option and its syntax is similar to printing from UNIX. For details, see UNIX Supplement.

lpr**When specifying a printer by IP address**

```
c:> lpr -Sprinter's IP address [-Poption] [-o] \pass name\file name
```

When using a host name instead of an IP address

```
c:> lpr -Sprinter's host name [-Poption] [-o] \pass name\file name
```

When printing a binary file, add the "-o" option (lowercase O, and lowercase L).

When using a printer with the host name "host" to print a PostScript file named "file 1" located in the "C:\PRINT" directory, the command line is as follows:

```
c:> lpr -Shost -Pfiletype=RPS -o C:\PRINT\file1
```

Printing from the virtual printer

```
C:\>lpr -S "printer's IP address" -P[virtual printer name] [-o] \path name\file name
```

Note

- For details about the virtual printer configuration, see "Using the Virtual Printer", Printer Reference.

rcp

First, register the printer's host name in the hosts file.

```
c:> rcp [-b] \pass name\file name [pass name\file name...] printer's host name:
[option]
```

In file names, "*" and "?" can be used as wild cards.

When printing a binary file, add the "-b" option.

When using a printer with the host name "host" to print a PostScript file named "file 1" or "file 2" located in the "C:\PRINT" directory, the command line is as follows:

```
c:> rcp -b C:\PRINT\file1 C:\PRINT\file2 host:filetype=RPS
```

Printing from the virtual printer

```
c:> rcp [-b] \path name\file name [\path name\file name...] printer's host name:  
[virtual printer name]
```

↓ Note

- For details about the virtual printer configuration, see "Using the Virtual Printer", Printer Reference.

ftp / sftp

Use the "put" or "mput" command according to the number of files to be printed.

When one file is printed

```
ftp> put \pass name\file name [option]
```

Printing from the virtual printer

```
ftp> put \path name\file name [virtual printer name]
```

When multiple files are printed

```
ftp> mput \pass name\file name [\pass name\file name...] [option]
```

Follow the procedure below to print using the "ftp" command.

1. **Formulate the printer's IP address or the host name of the hosts file printer as an argument and use the "ftp" command.**

```
% ftp "printer's IP address"
```

2. **Enter the user name and password, and then press the [Enter] key.**

For details about the user name and password, consult your network administrator.

User:

Password:

When user authentication is set, enter a login user name and password.

3. **When printing a binary file, set the file mode to binary.**

```
ftp> bin
```

When printing a binary file in ASCII mode, print may not come out correctly.

4. **Specify files to be printed.**

The following shows the examples of printing a PostScript file named "file 1" in the "C:\PRINT" directory and printing file 1 and file 2.

```
ftp> put C:\PRINT\file1 filetype=RPS
```

```
ftp> mput C:\PRINT\file1 C:\PRINT\file2
```

5. Quit ftp.

```
ftp> bye
```

↓ Note

- "=", ",", "_", and ";" cannot be used for filenames. File names will be read as option strings.
- If you are using ftp, you cannot specify an option using the "mput" command.
- If you are using ftp, you cannot specify an option using the "pwd" command.
- If you are using sftp, you cannot specify an option using the "cd" command.
- If you are using sftp, you cannot specify an option using the "pwd" command.
- To use SFTP, you must create an open key for SSH communication. Use Web Image Monitor to create an open key. For details, see Web Image Monitor help.
- If personal authentication (Basic, Windows, LDAP, or Integrated Server Authentication) is enabled, only authenticated users (users authenticated by login user name and password) can log on.
- For "mput" command, "*" and "?" can be used as wild cards in file names.
- When printing a binary file in ASCII mode, print may not come out correctly.
- For details about login user name and password, see Security Reference, which is the administrator's manual.
- For details about the virtual printer configuration, see "Using the Virtual Printer", Printer Reference.

Printing with Bluetooth Connection

This describes how to print with Bluetooth devices.

Supported Profiles

The following profiles are supported:

- SPP (Serial Port Profile)
- HCRP (Hardcopy Cable 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.

Restrictions on BIP

- For BIP connection, a module including PostScript 3 must be installed in the machine.
- 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

The following procedures explain how to install a Bluetooth printer on a computer that is running Windows XP or Windows Vista.

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 perform a printer installation, your account must have **Manage Printers** permission. Log on as an **Administrators** or **Power Users** group member.
- 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

1. On the [Start] menu, click [Printers and Faxes].

The [Printers and Faxes] window appears.

2. Click [Add a printer].

The [Add Printer Wizard] window opens.

3. Click [Next >].

4. 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.

5. Click [No, I will not connect], and then click [Next >].

6. Click [Install from a list or specific location (Advanced)], and then click [Next >].

7. 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 >].

8. If the [Hardware Installation] window appears, click [Continue].

9. If the installation was successful, click [Finish].

10. Select [Test Print], and then click [Next >].

11. 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

★ Important

- To perform a printer installation, your account must have **Manage Printers** permission. Log on as an **Administrators** or **Power Users** group member.

1. On the [Start] menu, click [Control Panel].
2. In the “Hardware and Sound” area, click [Printers].
3. In the top part of the window, click [Add a printer].
4. 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.

5. From the list of discovered devices, select the printer 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 printer you select is a Bluetooth printer.

6. 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.
7. In the [Found New Hardware] window, select the printer driver you want to use, and then click [Next].

The printer driver installation starts.

8. If the [Windows Security] window appears, click [Install this driver software anyway].
9. Click [Close].
10. If you want to change the printer name, enter the new name in the [Printer Name Settings] window.
11. 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.

7. Appendix

When Using Windows Terminal Service/ MetaFrame

The following explains how to use Windows Terminal Service and Maintenance.

Operating Environment

The following operating systems and MetaFrame versions are supported.

Windows 2000 Server / Advanced Server

- MetaFrame Presentation Server 3.0
- Citrix Presentation Server 4.0

Windows server 2003/2003 R2

- MetaFrame Presentation Server 3.0
- Citrix Presentation Server 4.0

Supported Printer Drivers

When Windows Terminal Service is operating

- PCL drivers
- PostScript 3
- RPCS drivers

Note

- Some RPCS printer driver functions do not work if Windows Terminal Service is installed.

Limitations

The following limitations apply to the Windows Terminal Service environment.

These limitations are built in Windows Terminal Service or MetaFrame.

Windows Terminal Service

In the Windows Terminal Service environment, some of the printer driver's functions are unavailable. In an environment where Windows Terminal Service is installed, some of the printer driver's functions is unavailable, even if any function of Windows Terminal Service is not used. When you install

SmartDeviceMonitor for Client in an environment where the Terminal Service is running on the Windows 2000 Server family computer, be sure to install it using the install mode. The following are the two methods of installation using the install mode:

1. Use [Add/Remove Programs] in [Control Panel] to install SmartDeviceMonitor for Client.
2. Enter the following command in the MS-DOS command prompt.

```
CHANGE USER / INSTALL
```

To quit the install mode, enter the following command in the MS-DOS command prompt.

```
CHANGE USER / EXECUTE
```

MetaFrame's [Auto-creating client printers]

Using [Auto-creating client printers] can select a logical printer created by copying the client's local printer data to the MetaFrame server. We strongly recommend testing this function in your network environment before using it for your work.

- The settings for optional equipment will not be stored in the server after the equipment is disconnected. The settings for optional equipment will be restored to its defaults each time the client computer logs on to the server.
- When printing a large number of bitmap images or using the server in a WAN environment over dial-up lines such as ISDN, printing may not be possible or errors may occur, depending on data transfer rates.

7

MetaFrame's [Printer driver replication]

Using [Printer driver replication] can distribute printer drivers across all servers in a server farm. We strongly recommend testing this function in your network environment before using it for your work.

- If the printer drivers are not properly copied, install them directly onto each server.

Using DHCP

You can use the printer in a DHCP environment. You can also register the printer NetBIOS name on a WINS server when it is running.

- Printers that register the printer NetBIOS name on a WINS server must be configured for the WINS server.
- Supported DHCP servers are Microsoft DHCP Server included with Windows 2000 Server, and Windows Server 2003/2003 R2, and Windows Server 2008, and the DHCP server included with NetWare and UNIX.
- If you do not use the WINS server, reserve the printer's IP address in the DHCP server so the same IP address is assigned every time.
- To use the WINS server, change the WINS server setting to "active" using the control panel.
- Using the WINS server, you can configure the host name via the remote network printer port.
- DHCP relay-agent is not supported. If you use DHCP relay-agent on a network via ISDN, it will result in increased line charges. This is because your computer connects to the ISDN line whenever a packet is transferred from the printer.
- If there is more than one DHCP server, use the same setting for all servers. The machine operates using data from the DHCP server that responds first.
- DHCP servers can operate in an IPv6 environment, but they cannot be configured to allocate IPv6 addresses or obtain host names.

7

Using AutoNet

If the printer IPv4 address is not automatically assigned by the DHCP server, a temporary IP address starting with 169.254 and not used on the network can be automatically selected by the printer.

↓ Note

- The IP address assigned by the DHCP server is given priority over that selected by AutoNet.
- You can confirm the current IPv4 address on the configuration page.
- When AutoNet is running, the NetBIOS name is not registered on the WINS server.
- The machine cannot communicate with devices that do not have the AutoNet function. However, this machine can communicate with Macintosh computers running Mac OS X 10.2.3. or higher.

Configuring the WINS Server

This section explains configuring the WINS server.

The printer can be configured to register its NetBIOS name with a WINS server when the power is turned on. This enables the NetBIOS name of the printer to be specified from SmartDeviceMonitor for Admin even in a DHCP environment.

↓ Note

- The WINS server is supported with Windows 2000 Servers WINS Manager.
- For details about the WINS server settings, see Windows Help.
- If there is no reply from the WINS server, the NetBIOS name is registered by broadcast.
- The NetBIOS name can be entered using up to 13 alphanumeric characters.

Using Web Image Monitor

1. **Start a Web browser.**
2. **Enter "http://(machine's IP address or host name) /" in the address bar to access the printer whose settings you want to change.**
Top Page of Web Image Monitor appears.
3. **Click [Login].**
The dialog box for entering the user name and password appears.
4. **Enter the user name and password, and then click [Login].**
Contact your administrator for information about the settings.
5. **In the left area, click [Configuration], and then click [Network].**
6. **Click [TCP/IP].**
7. **Check that [Enable] is selected for [WINS] in the [Ethernet + Wireless LAN] column, and then enter the WINS server IPv4 address in [Primary WINS Server] and [Secondary WINS Server].**
8. **Click [Apply].**
9. **Quit Web Image Monitor.**

📖 Reference

- p.137 "Using Web Image Monitor"

Using telnet

You can also use telnet to configure WINS.

Use the "wins" command to make the setting with telnet.

 **Reference**

- p.176 "Remote Maintenance by telnet"

Using the Dynamic DNS Function

Dynamic DNS is a function which dynamically updates (registers and deletes) records (A record, AAAA record, CNAME, and PTR record) managed by the DNS server. When a DNS server is part of the network environment to which this printer, a DNS client, is connected, records can be dynamically updated using this function.

Updating

Updating procedure varies depending on whether the printer IP address is static or acquired by DHCP.

★ Important

- **Dynamic update using message authentication (TSIG, SIG(0)) is not supported.**

For a static IPv4 setting

If the IP address or host name is changed, the A and PTR records are updated. If the A record is registered, CNAME is also registered. CNAMEs that can be registered are as follows:

- Ethernet and IEEE 802.11
RNPXXXXXX (XXXXXX represents the last 3 hexadecimal bytes of the MAC address)
However, if CNAME (PRNXXXXXX) overlaps with the host name, CNAME will not be registered.

For DHCPv4 settings

As a substitute for the printer, the DHCP server updates the record, and one of the following occurs:

- When the printer acquires the IP address from the DHCP server, the DHCP server updates the A and PTR records.
- When the printer acquires the IP address from the DHCP server, the printer updates the A record, and the DHCP server updates the PTR record.

If the A record is registered, CNAME is also registered. CNAMEs that can be registered are as follows:

- Ethernet and IEEE 802.11
RNPXXXXXX (XXXXXX represents the last 3 hexadecimal bytes of the MAC address)

For IPv6 settings

This machine updates the AAAA record and PTR record.

It also updates CNAME when the AAAA record is updated.

When a stateless address is newly set, it is automatically registered on the DNS server also.

↓ Note

- When the dynamic DNS function is not used, records managed by the DNS server must be updated manually, if the printer's IP address is changed.
- To update the record using the printer, the DNS server has to have one of the following:

- No security settings are made.
- If security settings are made, an IP-specified client (this printer) permits updating.

DNS servers targeted for operation

For static IP setting

- Microsoft DNS servers with standard Windows 2000 Server/Windows Server 2003/2003 R2/2008 features
- BIND 8.2.3 or higher

For DHCP setup, when the printer updates the A record

- Microsoft DNS servers with standard Windows 2000 Server/Windows Server 2003/2003 R2/2008 features
- BIND 8.2.3 or higher

For DHCP setup, when the DHCP server updates records

- Microsoft DNS servers with standard Windows 2000 Server/Windows Server 2003/2003 R2/2008 features
- BIND 8.2.3 or higher
- DNS servers with standard NetWare 5 (or a higher version) features

For IPv6 setting

- Microsoft DNS servers with standard Windows Server 2003/2003 R2/2008 features
- BIND 9.2.3 or higher

DHCP servers targeted for operation

As a substitute for the printer, DHCP servers capable of updating the A record and PTR record are as follows:

- Microsoft DHCP servers with standard Windows 2000 Server (Service Pack 3 or higher versions)/Windows Server 2003/2003 R2/2008 features
- ISC DHCP 3.0 or higher
- DHCP server with standard NetWare 5 features

Setting the dynamic DNS function

Make settings with telnet using the "dns" command.

 **Note**

- For details, see "Remote Maintenance by telnet".

 **Reference**

- p.176 "Remote Maintenance by telnet"

Precautions

Please pay attention to the following when using the network interface board. When configuration is necessary, follow the appropriate procedures below.

Connecting a Dial-Up Router to a Network

When using NetWare (file server)

If the NetWare file server and printer are on opposite sides of a router, packets are sent back and forth continuously, possibly incurring communications charges. Because packet transmission is a feature of NetWare, you need to change the configuration of the router. If the network you are using does not allow you to configure the router, configure the machine instead.

Configuring the router

Filter packets so they do not pass over the dial-up router.

↓ Note

- The MAC address of the filtering printer is printed on the printer configuration page.
- For more information about configuring the printer if the router cannot be configured, see the following instructions.

Configuring the printer with NetWare

1. Following the setup method described earlier in this manual, configure the file server.
2. Set the frame type for NetWare environment.

↓ Note

- For more information about selecting a frame type, see "Interface Settings".

📖 Reference

- p.34 "Interface Settings"

Configuring the printer without NetWare

1. When not printing, the network interface board sends packets over the network. Set NetWare to "inactive".

↓ Note

- For more information about selecting a protocol, see "Interface Settings".

📖 Reference

- p.34 "Interface Settings"

When using network utility

If the machine is connected to a network, observe the following points when setting up the machine or changing settings:

For more details, see the operating instructions and Help for the ScanRouter delivery software and DeskTopBinder.

When a dial-up router is connected in a network environment

The settings for the delivery server to be connected must be made appropriately for the machine with the ScanRouter delivery software, Auto Document Link, or DeskTopBinder. In addition, set up connected devices using the I/O settings of the ScanRouter delivery software administration utility.

If the network environment changes, make the necessary changes for the delivery server using the machine, the administration utility of client computers, Auto Document Link, and DeskTopBinder. Also, set the correct information for the connected devices using the I/O settings of the ScanRouter delivery software administration utility.

★ Important

- **If the machine is set up to connect to the delivery server via a dial-up router, the router will dial and go online whenever a connection to the delivery server is made. Telephone charges may be incurred.**

When connected to a computer that uses dial-up access

- Do not install the ScanRouter delivery software on a computer which uses dial-up access.
- When using the ScanRouter delivery software, DeskTopBinder, Auto Document Link, or a TWAIN driver on a computer with dial-up access, a dial-up connection may be performed when connecting to the delivery server and other equipment, depending on the setup. If the computer is set up to connect to the Internet automatically, the confirmation dialog box will not appear, and telephone charges may be incurred without your being aware of it. To prevent unnecessary connections, the computer should be set up so the confirmation dialog box always appears before establishing a connection. Do not make unnecessary connections when using the above listed software.

NetWare Printing

★ Important

- **IPv6 cannot be used on this function.**

Form feed

You should not configure form feed on NetWare. Form feed is controlled by the printer driver on Windows. If NetWare form feed is configured, the printer might not work properly. If you want to change form feed settings, always configure them using Windows.

- Under Windows 2000/XP and Windows Server 2003/2003 R2, clear the [Form feed] check box on the [NetWare Settings] tab in the printer properties dialog box.

Banner page

You should not configure a banner page on NetWare. If you want to change the banner page setting, always configure it using Windows.

- Under Windows 2000/XP and Windows Server 2003/2003 R2, clear the [Enable banner] check box on the [NetWare Settings] tab in the printer properties dialog box.

Printing after resetting the machine

After resetting the remote printer, the connection from the print server will be cut off for about 30-40 seconds before re-connecting. Depending on the NetWare specification, print jobs may be accepted, but they will not be printed during this interval.

When using the machine as a remote printer, wait about two minutes after resetting before attempting to print.

When the IEEE 802.11 Interface Unit is Installed

Please pay attention to the following when using the IEEE 802.11 interface on the network.

When using the wireless LAN interface on the network, note the following:

When moving the machine

Detach the antennas when relocating the machine locally.

After moving the machine, reattach the antennas, ensuring that:

- The antennas are positioned clear of obstacles.
- There is 1.6 to 2.4 inch (40 to 60 mm) between the antennas, so that they do not touch.
- The exposure glass cover and the ADF do not knock the antennas.

If the network area provides poor radio environment

Where radio wave conditions are bad, the network may not function due to interrupted or failed connections. When checking the wireless LAN signal and the access point, follow the procedure below to improve the situation:

- Position the access point nearer to the machine.
- Clear the space between access point and machine of obstructions.
- Move radio wave generating appliances, such as microwaves, away from the machine and access point.

Note

- For more information about access point radio wave conditions, refer to the access point manual.

Configuring IEEE 802.1X

IEEE 802.1X can be configured using Web Image Monitor's administrator mode. 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:

If a certificate is required, configure all settings after installing the certificate.

EAP Types Requiring a "Site Certificate"

EAP-TLS, EAP-TTLS, PEAP (Necessary except LEAP)

EAP Types Requiring a "Site Certificate" and a "Device Certificate"

EAP-TLS, PEAP (Phase 2 is for TLS only)

★ Important

- To set IEEE 802.1X, you must enable SSL. For details about setting SSL configuration, see "Protection Using Encryption", Security Reference.
- To set IEEE 802.1X, you must use Web Image Monitor.

Installing a Site Certificate

7

1. Access the authentication server and obtain the CA certificate.

Methods of obtaining certificates differ according to the operating system you are using.

2. Log on to Web Image Monitor in the administrator mode.

3. Click [Configuration].

4. [Site Certificate] in the "Security" area.

5. Click [Browse] on the "Site Certificate to Import" window, and then select the CA certificate you obtained.

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. Click [Logout].

10. Quit the Web Image Monitor.

Installing Device Certificate

1. Log on to Web Image Monitor in the administrator mode.
2. Click [Configuration].
3. Click [Device Certificate] in "Security" area.
4. Click [Certificate 2] on the "Device Certificate" window, and then click [Request].
5. Enter appropriate "Common Name" and "Country Code" on "Certificate Information" page, and then click [OK].
6. "Updating..." appears. Wait for about 2 minutes, and then click [OK].
7. Click [Details], shown in the "Device Certificate" window as the memo pad icon for "Requesting".
8. Select all, and then copy the entire "Text for Requested Certificate" text that is displayed in the "Certificate Status" window.
9. Access the certificate authority server, and then obtain the CA signified certificate using the text copied into "Text for Requested Certificate" windows.

Obtaining the certificate differs depending on the environment you want to use.

10. Click [Certificate 2] on "Device Certificate" window, and then click [Install].
11. Using a text editor, open the CA signified certificate downloaded in step 11, and then copy over all the text.
12. In the [Install Certificate] window, paste all the text copied into the CA signified certificate.
13. Click [OK].
14. "Updating..." appears. Wait for about one or two minutes, and then click [OK].
15. Check that the "Device Certificate" shows "Installed".
16. Click [Certificate 2] on "Certification", and then click [OK].
17. Click [Logout].
18. Quit Web Image Monitor.

↓ Note

- If you request two certificates simultaneously, the certificate authority might not display either certificate. Click [Cancel Request] to cancel the request.
- You can select [Certificate 1-4] in the "Device Certificate" window. Note that if you select [Certificate 1] in the "Device Certificate" window, you must select "Certificate 1" in the "IEEE 802.1X(WPA/WPA2)" drop down menu in the "Certification" window.
- Click [Cancel Request] to cancel the request for the server certificate.
- If "Not found" appears after clicking [OK] in steps 6 and 14, wait one or two minutes, and then click [Refresh].

Setting Items of IEEE 802.1X for Ethernet

1. Log on to Web Image Monitor in the administrator mode.
2. Click [Configuration].
3. Select [IEEE 802.1X (WPA/WPA2)] in "Security" area.
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".

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".

PEAP

- Click [Change] in "Password", and then enter the password set in the RADIUS server.
- 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".

7. Click [OK].
8. Click [Configuration], and then click [Interface Settings] in the "Interface" area.
9. Select [Active] in "Ethernet Security".
10. Click [OK].
11. Click [Logout].
12. Quit the Web Image Monitor.

Note

- If there is a problem with settings, you might not be able to communicate with the printer. To identify the problem, print a network summary.
- If you cannot identify the problem, reset the printer interface to normal, and then repeat the procedure from the beginning.

Setting Items of IEEE 802.1X for Wireless LAN

1. Log on to Web Image Monitor in the administrator mode.
2. Click [Configuration].
3. Select [IEEE 802.1X (WPA/WPA2)] in "Security" area.
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".

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”.

PEAP

- Click [Change] in “Password”, and then enter the password set in the RADIUS server.
 - 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”.
7. Click [OK].
 8. Click [Configuration], and then click [Wireless LAN Settings] in the “Interface” area.
 9. Select [Wireless LAN] in “LAN Type”.
 10. Select [Infrastructure Mode] in “Communication Mode”.
 11. Enter the alphanumeric characters (a-z, A-Z, or 0-9) in [SSID] according to the access point you want to use.
 12. Select [WPA] in “Security Method”.
 13. Select [TKIP] or [CCMP (AES)] in “WPA Encryption Method” according to the access point you want to use.
 14. Select [WPA] or [WPA2] in “WPA Authentication Method”.
 15. Click [OK].
 16. Click [Logout].
 17. Quit the Web Image Monitor.

↓ Note

- If there is a problem with settings, you might not be able to communicate with the printer. To identify the problem, print a network summary.
- If you cannot identify the problem, reset the printer interface to normal, and then repeat the procedure from the beginning.

Specifications

Interface	1000BASE-T, 100BASE-TX, 10BASE-T, IEEE 802.11 a/b/g
Frame type	Ethernet II, IEEE 802.2, IEEE 802.3, SNAP
Printer (LAN-Fax)	TCP/IP (IPv4/IPv6)
	LPR
	RSH
	RCP
	DIPRINT
	FTP
	IPP
	IPP-SSL
	IPX/SPX (NetWare)
	AppleTalk
	SMB
	WSD (Printer)
Internet Fax	TCP/IP (IPv4/IPv6)
	SMTP
	SMTP-C
	POP3
	IMAP4
Network Scanner	IPv4
	RSH
	FTP
	FTP-C

	SMTP
	SMTP-C
	POP3
	SMB
	NCP
	WSD (Scanner)
Document Server	TCP/IP (IPv4/IPv6)
	FTP
	FTP-C
	HTTP
	HTTPS
Management Function	TCP/IP (IPv4/IPv6)
	RSH
	RCP
	FTP
	FTP-C
	SNMP
	SNMP-C
	HTTP
	HTTPS
	TELNET (mshell)
	NBT
	DHCP
	DNS
	DNS-C
	LDAP

To use IPP and SMB, use the SmartDeviceMonitor for Client port.

To use IPP under Windows XP/Vista, Windows Server 2003/2003 R2/2008, use the Standard IPP port.

To use IPP under Windows 2000, use SmartDeviceMonitor for Client.

AppleTalk can be used when the PostScript 3 module is installed.

Under Windows Vista, or Windows Server 2008, WSD (Printer), WSD (Scanner), uses the WSD Port.

Copyrights

expat

- The software including controller, etc. (hereinafter "software") installed on this product uses the expat under the conditions mentioned below.
- The product manufacturer provides warranty and support to the software of the product including the expat, and the product manufacturer makes the initial developer and copyright holder of the expat, free from these obligations.
- Information relating to the expat is available at:
<http://expat.sourceforge.net/>

Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center, Ltd. and Clark Cooper.

Copyright (c) 2001, 2002 Expat maintainers.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

NetBSD

1. Copyright Notice of NetBSD

For all users to use this product:

This product contains NetBSD operating system:

For the most part, the software constituting the NetBSD operating system is not in the public domain; its authors retain their copyright.

The following text shows the copyright notice used for many of the NetBSD source code. For exact copyright notice applicable for each of the files/binaries, the source code tree must be consulted.

A full source code can be found at <http://www.netbsd.org/>.

Copyright (c) 1999, 2000 The NetBSD Foundation, Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

This product includes software developed by The NetBSD Foundation, Inc. and its contributors.

4. Neither the name of The NetBSD Foundation nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE NETBSD FOUNDATION, INC. AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE FOUNDATION OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

7

2. Authors Name List

All product names mentioned herein are trademarks of their respective owners.

The following notices are required to satisfy the license terms of the software that we have mentioned in this document:

- This product includes software developed by the University of California, Berkeley and its contributors.
- This product includes software developed by Jonathan R. Stone for the NetBSD Project.
- This product includes software developed by the NetBSD Foundation, Inc. and its contributors.
- This product includes software developed by Manuel Bouyer.
- This product includes software developed by Charles Hannum.
- This product includes software developed by Charles M. Hannum.
- This product includes software developed by Christopher G. Demetriou.
- This product includes software developed by Tools GmbH.
- This product includes software developed by Terrence R. Lambert.
- This product includes software developed by Adam Glass and Charles Hannum.
- This product includes software developed by Theo de Raadt.

- This product includes software developed by Jonathan Stone and Jason R. Thorpe for the NetBSD Project.
- This product includes software developed by the University of California, Lawrence Berkeley Laboratory and its contributors.
- This product includes software developed by Christos Zoulas.
- This product includes software developed by Christopher G. Demetriou for the NetBSD Project.
- This product includes software developed by Paul Kranenburg.
- This product includes software developed by Adam Glass.
- This product includes software developed by Jonathan Stone.
- This product includes software developed by Jonathan Stone for the NetBSD Project.
- This product includes software developed by Winning Strategies, Inc.
- This product includes software developed by Frank van der Linden for the NetBSD Project.
- This product includes software developed for the NetBSD Project by Frank van der Linden.
- This product includes software developed for the NetBSD Project by Jason R. Thorpe.
- The software was developed by the University of California, Berkeley.
- This product includes software developed by Chris Provenzano, the University of California, Berkeley, and contributors.

Sablotron

Sablotron (Version 0.82) Copyright (c) 2000 Ginger Alliance Ltd. All Rights Reserved.

a) The application software installed on this product includes the Sablotron software Version 0.82 (hereinafter, "Sablotron 0.82"), with modifications made by the product manufacturer. The original code of the Sablotron 0.82 is provided by Ginger Alliance Ltd., the initial developer, and the modified code of the Sablotron 0.82 has been derived from such original code provided by Ginger Alliance Ltd.

b) The product manufacturer provides warranty and support to the application software of this product including the Sablotron 0.82 as modified, and the product manufacturer makes Ginger Alliance Ltd., the initial developer of the Sablotron 0.82, free from these obligations.

c) The Sablotron 0.82 and the modifications thereof are made available under the terms of Mozilla Public License Version 1.1 (hereinafter, "MPL 1.1"), and the application software of this product constitutes the "Larger Work" as defined in MPL 1.1. The application software of this product except for the Sablotron 0.82 as modified is licensed by the product manufacturer under separate agreement (s).

d) The source code of the modified code of the Sablotron 0.82 is available at: <http://support-download.com/services/device/sablot/notice082.html>

e) The source code of the Sablotron software is available at: <http://www.gingerall.com>

f) MPL 1.1 is available at: <http://www.mozilla.org/MPL/MPL-1.1.html>

JPEG LIBRARY

- The software installed on this product is based in part on the work of the Independent JPEG Group.

SASL

CMU libsassl

Tim Martin

Rob Earhart

Rob Siemborski

Copyright (c) 2001 Carnegie Mellon University. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name "Carnegie Mellon University" must not be used to endorse or promote products derived from this software without prior written permission.

For permission or any other legal details, please contact:

Office of Technology Transfer

Carnegie Mellon University

5000 Forbes Avenue

Pittsburgh, PA 15213-3890

(412) 268-4387, fax: (412) 268-7395

tech-transfer@andrew.cmu.edu

4. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by Computing Services at Carnegie Mellon University (<http://www.cmu.edu/computing/>)."

CARNEGIE MELLON UNIVERSITY DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CARNEGIE MELLON UNIVERSITY BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

MD4

Copyright (c) 1990-2, RSA Data Security, Inc. All rights reserved.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD4 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD4 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

MD5

Copyright (c) 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

Samba(Ver 3.0.4)

For SMB transmission, this machine uses Samba ver 3.0.4 (hereinafter referred to as Samba 3.0.4).

Copyright (c) Andrew Tridgell 1994-1998.

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, USA.

Note

- The source code for SMB transmission by this machine can be downloaded from the following website:
<http://support-download.com/services/scbs>

RSA BSAFE®



- This product includes RSA BSAFE(c) cryptographic or security protocol software from RSA Security Inc.
- RSA and BSAFE are registered trademarks of RSA Security Inc. in the United States and/or other countries.
- RSA Security Inc. All rights reserved.

7

Open SSL

Copyright (c) 1998-2004 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (ey@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (ey@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (ey@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (ey@cryptsoft.com)" The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence.

[including the GNU Public Licence.]

Open SSH

7

The licences which components of this software fall under are as follows. First, we will summarize and say that all components are under a BSD licence, or a licence more free than that.

OpenSSH contains no GPL code.

1)

Copyright (c) 1995 Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland All rights reserved

As far as I am concerned, the code I have written for this software can be used freely for any purpose. Any derived versions of this software must be clearly marked as such, and if the derived work is incompatible with the protocol description in the RFC file, it must be called by a name other than "ssh" or "Secure Shell".

[Tatu continues]

However, I am not implying to give any licenses to any patents or copyrights held by third parties, and the software includes parts that are not under my direct control. As far as I know, all included source code is used in accordance with the relevant license agreements and can be used freely for any purpose (the GNU license being the most restrictive); see below for details.

[However, none of that term is relevant at this point in time. All of these restrictively licenced software components which he talks about have been removed from OpenSSH, i.e.,

- RSA is no longer included, found in the OpenSSL library
- IDEA is no longer included, its use is deprecated
- DES is now external, in the OpenSSL library
- GMP is no longer used, and instead we call BN code from OpenSSL

- Zlib is now external, in a library
- The make-ssh-known-hosts script is no longer included
- TSS has been removed
- MD5 is now external, in the OpenSSL library
- RC4 support has been replaced with ARC4 support from OpenSSL
- Blowfish is now external, in the OpenSSL library

[The licence continues]

Note that any information and cryptographic algorithms used in this software are publicly available on the Internet and at any major bookstore, scientific library, and patent office worldwide. More information can be found e.g. at "<http://www.cs.hut.fi/crypto>".

The legal status of this program is some combination of all these permissions and restrictions. Use only at your own responsibility. You will be responsible for any legal consequences yourself; I am not making any claims whether possessing or using this is legal or not in your country, and I am not taking any responsibility on your behalf.

NO WARRANTY

BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

2)

The 32-bit CRC compensation attack detector in deattack.c was contributed by CORE SDI S.A. under a BSD-style license.

Cryptographic attack detector for ssh - source code

Copyright (c) 1998 CORE SDI S.A., Buenos Aires, Argentina. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that this copyright notice is retained.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES ARE DISCLAIMED. IN NO EVENT SHALL CORE SDI S.A. BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OR MISUSE OF THIS SOFTWARE.

Ariel Futoransky <futo@core-sdi.com>

<<http://www.core-sdi.com>>

3)

One component of the ssh source code is under a 3-clause BSD license, held by the University of California, since we pulled these parts from original Berkeley code.

Copyright (c) 1983, 1990, 1992, 1993, 1995

The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

4)

Remaining components of the software are provided under a standard 2-term BSD licence with the following names as copyright holders:

Markus Friedl

Theo de Raadt

Niels Provos

Dug Song

Kevin Steves

Daniel Kouril

Wesley Griffin

Per Allansson

Jason Downs

Solar Designer

Todd C. Miller

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

5)

Portable OpenSSH contains the following additional licenses:

c) Compatibility code (openbsd-compat)

Apart from the previously mentioned licenses, various pieces of code in the openbsd-compat/ subdirectory are licensed as follows:

Some code is licensed under a 3-term BSD license, to the following copyright holders:

Todd C. Miller

Theo de Raadt

Damien Miller

Eric P. Allman

The Regents of the University of California

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Open LDAP

The OpenLDAP Public License Version 2.8, 17 August 2003.

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions in source form must retain copyright statements and notices,
2. Redistributions in binary form must reproduce applicable copyright statements and notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution, and
3. Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time. Each revision is distinguished by a version number. You may use this Software under terms of this license revision or under the terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS CONTRIBUTORS "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S) OR OWNER(S) OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The names of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission. Title to copyright in this Software shall at all times remain with copyright holders.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Copyright (c) 1999-2003 The OpenLDAP Foundation, Redwood City, California, USA. All Rights Reserved. Permission to copy and distribute verbatim copies of this document is granted.

Heimdal

Copyright (c) 1997-2005 Kungliga Tekniska Högskolan (Royal Institute of Technology, Stockholm, Sweden). All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the Institute nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE INSTITUTE AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE INSTITUTE OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

IPS™ print language emulations

Copyright (c) 1987-2006 Zoran Corporation. All rights reserved.

Trademarks

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

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

Apple, AppleTalk, Bonjour, EtherTalk, Macintosh, Mac OS, Mac OS X, and TrueType are registered trademarks of Apple Inc, registered in the U.S. and other countries.

Citrix® and MetaFrame® are registered trademarks of Citrix Systems, Inc.

IPS is a trademark or registered trademark of Zoran Corporation and/or its subsidiaries in the United States or other countries.

Linux® is the registered trademark of Linus Torvalds in the U.S. and 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.

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.

7

UNIX is a registered trademark in the United States and other countries, licensed exclusively through, X/Open Company Limited.

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

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 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

INDEX

A

Account for e-mail notification.....	172
Ad-hoc channel.....	39
Adding a group to another group.....	306
Address book.....	249
Address book change order.....	50
Address book edit title.....	52
Address book management.....	49
Address book program / change / delete group..	50
Address book switch title.....	53
ADF Original Table Elevation.....	21
Administrator authentication management.....	55
Administrator mode.....	140
Administrator tools.....	49
Administrator's e-mail address.....	45
AOF.....	57
Authentication information.....	259
Auto delete file in document server.....	56
Auto erase memory setting.....	57
Auto logout timer.....	32
Auto off timer	
type 1.....	31
Auto specify sender name.....	47
AutoNet.....	331

B

Back Cover Sheet Tray.....	30
Back up / Restore address book.....	53
Bidirectional communication.....	38
Bluetooth.....	326
adding a printer.....	326

C

Capture server IP address.....	42
Changing a fax destination.....	271
Changing a group name.....	310
Changing a Registered IP-Fax destination.....	276
Changing a registered name.....	256
Changing a user code.....	261
Changing an e-mail destination.....	283
Changing an FTP folder.....	294
Changing an NCP registered folder.....	300
Changing an SMB folder.....	289

Clearing the number of prints.....	266
Communication mode.....	39
Connecting the telephone line.....	123
Connecting to the interfaces.....	79
Copier/Document server auto reset timer.....	31
Copy Count Display.....	20
Copyrights.....	349

D

Data Carry-over Setting for Address Book Auto-program.....	54
Data security for copying.....	58
DDNS configuration.....	35
Default user name / password (send).....	46
Delete all files in document server.....	56
Delete all logs.....	57
Deleting a fax destination.....	273
Deleting a group.....	312
Deleting a group within another group.....	309
Deleting a registered IP-Fax destination.....	279
Deleting a registered name.....	257
Deleting a user code.....	262
Deleting an e-mail destination.....	284
Deleting an FTP folder.....	296
Deleting an NCP folder.....	302
Deleting an SMB registered folder.....	291
Delivery option.....	42
Designation Sheet 1 Tray, Designation Sheet 2 Tray	30
DHCP.....	331
DHCPv6.....	331
Dial-up router.....	337
Direct printing.....	321
Display / Clear / Print counter per user.....	54
Display / Print counter.....	54
Display Panel.....	16
Displayed information.....	227
Displaying names registered in a group.....	307
Displaying the counter for each user.....	264
DNS configuration.....	34
Document server	
Ethernet.....	111
wireless LAN.....	112
Domain name.....	35

Double Parallel Fold Position.....	24
Dynamic DNS.....	334

E

E-mail	
Ethernet.....	95
wireless LAN.....	96
E-mail communication port.....	45
E-mail destination.....	281
E-mail reception interval.....	45
E-mail storage in server.....	46
Effective Protocol.....	35
Energy Saver Timer.....	31
Enhanced Authentication Management.....	55
Enhanced external charge unit management....	56
Erase all memory.....	57
Ethernet interface.....	80
Ethernet speed.....	36
Extended security.....	56
External charge unit management.....	56

F

Facsimile auto reset timer.....	32
Fax destination.....	268
Fax e-mail account.....	47
Fax number.....	268
Fax RX file transmission.....	42
File transfer.....	42
Firmware version.....	57
Fixed USB port.....	58
Format of on-demand e-mail messages.....	175
Front Cover sheet tray.....	29
ftp.....	218, 225, 227, 239, 322
Function Priority.....	20
Function Reset Timer.....	20

G

Gate Fold Position.....	24
General features.....	19
General Features.....	68
Gigabit Ethernet interface.....	81
Group	
registering names to group.....	304
Guest mode.....	140

H

Half Fold Position.....	22
Host name.....	37, 321

I

IEEE 1284 Interface.....	84
IEEE 802.11 a/b/g interface	
checking the signal.....	87
connecting.....	85
setup procedure.....	85
IEEE 802.11 interface.....	340
IEEE 802.1X.....	341
device certificate.....	342
Ethernet.....	343
site certificate.....	341
wireless LAN.....	344
IEEE 802.1X authentication for Ethernet.....	36
info.....	225, 227
Input prime.....	38
Interface settings.....	34
Interleave Print.....	20
Internet Fax	
Ethernet.....	91
wireless LAN.....	93
IP address.....	14
IPP.....	190
IPsec.....	35
IPv4 gateway address.....	34
IPv6.....	191
IPv6 gateway address.....	34
IPv6 stateless address autoconfiguration.....	34

K

Key counter management.....	55
Key Repeat.....	21

L

LAN type.....	37
Laws and regulations.....	15
LDAP.....	59
changing.....	63
deleting.....	63
programming.....	59
LDAP authentication.....	317
LDAP search.....	57

Legal prohibition.....	15	Network security level.....	57
Letter Fold-in Position.....	23	Network settings	
Letter Fold-out Position.....	22	file transfer.....	120
Limitations.....	329	interface settings.....	114
Line type.....	123	Network TWAIN scanner	
Locating the NCP folder manually.....	299	Ethernet.....	108
Locating the NCP folder using browse network.....	300	wireless LAN.....	109
Locating the SMB folder manually.....	288	Notes.....	13
Locating the SMB folder using Browse Network.....	288	Notice.....	12
Login		Number of scanner resends.....	48
administrator mode.....	142	NW frame type.....	35
Web Image Monitor.....	140	O	
lpr.....	218, 322	Output Copier.....	20
M		Output Document Server.....	21
Machine IPv4 address.....	34	Output Facsimile.....	21
Machine IPv6 address.....	34	Output Printer.....	21
Machine name.....	37	Output tray settings.....	25
Machine status.....	168	P	
Managing names in the address book.....	252	Panel Key Sound.....	20
Managing users and machine usage.....	253	Panel off timer.....	31
Max. reception e-mail size.....	46	Paper Tray Priority	
Message.....	239	copier.....	26
MetaFrame.....	329	facsimile.....	26
Monitoring printers.....	167	printer.....	26
N		Paper Type	
NCP delivery protocol.....	35	bypass tray.....	27
NetWare.....	126	LCT.....	29
banner page.....	339	tray 1.....	27
form feed.....	338	tray 2.....	27
printing.....	338	tray 3 (lower paper tray).....	28
NetWare 3.x.....	127, 131	tray 4 (lower paper tray).....	28
NetWare 4.x.....	128, 133	Parallel communication speed.....	38
NetWare 5.....	128, 129, 133	Parallel Interface.....	37
NetWare 5.1.....	128, 129, 133	Parallel timing.....	38
NetWare 6.....	128, 129, 133	Permit SNMPv3 communication.....	37
NetWare 6.5.....	128, 129, 133	Permit SSL / TLS communication.....	37
Network.....	34	Ping command.....	37
Network delivery scanner		POP before SMTP.....	44
Ethernet.....	102	POP3 / IMAP4 settings.....	44
wireless LAN.....	103	Preventing unauthorized user access to shared folders from the machine.....	253
Network interface board configuration.....	228	Print address book destination list.....	52
		Print Backup	
		Compression.....	58

Default Format.....	58	rcp.....	322
Default Resolution.....	58	sftp.....	322
Delete All Files.....	58	Printing the counter for all users.....	265
Print job information		Printing the counter for each user.....	264
ftp.....	227	prnlog.....	227
info.....	227	Program / Change / Delete e-mail message.....	46
rcp.....	227	Program / Change / Delete LDAP server.....	56
rsh.....	227	Program / Change / Delete realm.....	57
sftp.....	227	Program / Change administrator.....	55
Print List.....	40	Program/Change/Delete User Text.....	19
Print log information		Pure IP environment	
ftp.....	227	NetWare 5.....	129
prnlog.....	227	NetWare 5.1.....	129
rcp.....	227	NetWare 6.....	129
rsh.....	227	NetWare 6.5.....	129
sftp.....	227		
Print Priority.....	20	R	
Print server		rcp.....	218, 225, 227, 239, 322
NetWare 4.x.....	128	Realm.....	65
NetWare 5.....	128	changing.....	66
NetWare 5.1.....	128	deleting.....	67
NetWare 6.....	128	programming.....	65
NetWare 6.5.....	128	Reception protocol.....	44
Print Server		Registering a fax destination.....	269
NetWare 3.x.....	127	Registering a FTP folder.....	292
Printer auto reset timer.....	32	Registering a Group.....	303
Printer configuration		Registering a protection code.....	313
ftp.....	225	Registering a protection code to a group user.....	314
info.....	225	Registering a protection code to a single user.....	313
rcp.....	225	Registering a user code.....	259
rsh.....	225	Registering an e-mail destination.....	281
sftp.....	225	Registering an IP-Fax destination.....	275
Printer server.....	125	Registering an NCP folder.....	297
Printer status		Registering an SMB folder.....	286
ftp.....	218	Registering folders.....	286
rcp.....	218	Registering names.....	255
rsh.....	218	Registering names to a group.....	303
sftp.....	218	Remote maintenance.....	176
status.....	218	Remote printer	
Printer Status		NetWare 3.x.....	131
lpr.....	218	NetWare 4.x.....	133
Printer/LAN-Fax		NetWare 5.....	133
Ethernet.....	88	NetWare 5.1.....	133
wireless LAN.....	89		
Printing commands			
ftp.....	322		
lpr.....	322		

NetWare 6.....	133
NetWare 6.5.....	133
Removing a name from a group.....	308
Restore factory defaults.....	40
Restore IEEE 802.1X authentication to defaults.....	36
rsh.....	218, 225, 227, 239

S

Scan to folder function	
Ethernet.....	99
wireless LAN.....	100
Scanner auto reset timer.....	32
Scanner resend interval time.....	48
Security method.....	39
Selection signal status.....	38
Sending e-mail by quick dial.....	253
Sending fax by quick dial.....	252
Sending scanned files to a shared folder directly.....	253
Set date.....	32
Set time.....	32
sftp.....	218, 225, 227, 239, 322
Signal control.....	38
Slip sheet tray.....	30
SmartDeviceMonitor for Admin.....	151
address information.....	165
comments.....	163
Energy Saver Mode.....	161
exporting the information on about the number of pages printed.....	157
fax journal.....	164
installing.....	152
locking the menus.....	154
machine status.....	162
names.....	163
Network Interface Board.....	153
new users.....	159
number of sheets printed.....	156
paper type.....	155
resetting the number of pages printed.....	157
restricting functions.....	159
setting a password.....	161
spool print.....	165
User Information.....	155
user management tool.....	156
SmartDeviceMonitor for Client.....	167

IPP.....	168
machine status.....	168
monitoring printers.....	167
SMB computer name.....	36
SMB work group.....	36
SMTP authentication.....	43, 316
SMTP server.....	43
SNMP.....	217
SSID setting.....	39
status.....	218
Supported printer drivers.....	329
Symbol.....	13
syslog.....	239
System auto reset timer.....	31
System log information	
ftp.....	239
rcp.....	239
rsh.....	239
sftp.....	239
syslog.....	239
System Settings on Main and Sub-machines.....	68
System Status/Job List Display Time.....	21

T

telnet.....	176
8021x.....	215
access.....	177
appletalk.....	178
authfree.....	178
autonet.....	179
bonjour.....	180
btconfig.....	181
devicename.....	181
dhcp.....	182
dhcp6.....	183
diprint.....	183
dns.....	184
domainname.....	186
etherauth.....	187
etherconfig.....	187
help.....	187
hostname.....	187
ifconfig.....	188
info.....	189
ipsec.....	190
logout.....	191
lpr.....	191

netware.....	192
passwd.....	193
pathmtu.....	194
prnlog.....	194
rhpp.....	196
route.....	194
set.....	196
show.....	199
slp.....	199
smb.....	200
snmp.....	200
sntp.....	204
spoolsw.....	205
ssdp.....	205
ssh.....	206
status.....	207
syslog.....	207
upnp.....	207
web.....	207
wiconfig.....	208
wins.....	213
wsmfp.....	214
Time interval between Printing Jobs.....	21
Timer settings.....	31
To change the fax number.....	272
To change the SEP code.....	272
To change the SUB code.....	272
To select line.....	272
To select the fax header.....	273
To set label insertion.....	273
To set the international TX mode.....	272
Top Page.....	138
Trademarks.....	362
Transfer log setting.....	57
Tray paper settings.....	26
Tray Paper Size	
tray 1.....	27
tray 2.....	27
Tray 2-3.....	26
tray 3 (lower paper tray).....	27
tray 4 (lower paper tray).....	27

U

USB interface.....	83
User Authentication management.....	54
User tools.....	17
change the settings.....	17

quit the settings.....	18
------------------------	----

V

Virtual printer.....	322
----------------------	-----

W

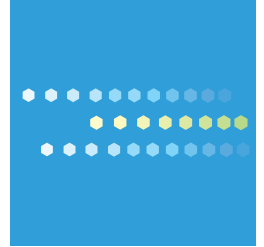
Warm-up Beeper.....	20
Web Image Monitor.....	137
administrator mode.....	140
auto e-mail notification.....	173
e-mail notification.....	170
guest mode.....	140
help.....	149
log out.....	140
login.....	140
mail authentication.....	172
menu.....	140
mode.....	140
on-demand e-mail notification.....	174
setting items.....	142
top page.....	138
Weekly Timer.....	32
Weekly Timer Cord.....	32
Windows Terminal Service.....	329
WINS configuration.....	35
WINS server.....	332
telnet.....	332
Web Image Monitor.....	332
Wireless LAN.....	38, 340
Wireless LAN interface	
checking the signal.....	87
connecting.....	85
setup procedure.....	85
Wireless LAN signal.....	40
WSD scanner	
Ethernet.....	105
wireless LAN.....	106

Z

Z-fold Position.....	21
----------------------	----

MEMO

MEMO

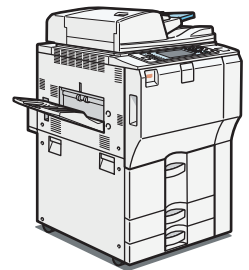


Type for 9060/MP 6001/LD360/Aficio MP 6001
Type for 9070/MP 7001/LD370/Aficio MP 7001
Type for 9080/MP 8001/LD380/Aficio MP 8001
Type for 9090/MP 9001/LD390/Aficio MP 9001



9060/9070/9080/9090
MP 6001/MP 7001/MP 8001/MP 9001
LD360/LD370/LD380/LD390
Aficio™ MP 6001/7001/8001/9001

Operating Instructions Security Reference



-
- 1** Getting Started
 - 2** Configuring Administrator Authentication
 - 3** Configuring User Authentication
 - 4** Protecting Data from Information Leaks
 - 5** Securing Information Sent over the Network or
Stored on Hard Disk
 - 6** Managing Access to the Machine
 - 7** Enhanced Network Security
 - 8** Specifying the Extended Security Functions
 - 9** Troubleshooting
 - 10** Appendix

TABLE OF CONTENTS

Manuals for This Machine.....	8
Notice.....	10
Important.....	10
How to Read This Manual.....	11
Symbols.....	11
IP Address.....	11
Notes.....	11
Laws and Regulations.....	12
Legal Prohibition.....	12

1. Getting Started

Before Using the Security Functions.....	13
Setting Up the Machine.....	14
Enhanced Security.....	16
Glossary.....	17
Security Measures Provided by this Machine.....	18
Using Authentication and Managing Users.....	18
Ensuring Information Security.....	18
Limiting and Controlling Access.....	20
Enhancing Network Security.....	21

2. Configuring Administrator Authentication

Administrators.....	23
User Administrator.....	23
Machine Administrator.....	24
Network Administrator.....	24
File Administrator.....	24
Supervisor.....	24
About Administrator Authentication.....	25
Enabling Administrator Authentication.....	27
Specifying Administrator Privileges.....	27
Registering the Administrator.....	30
Logging on Using Administrator Authentication.....	33
Logging off Using Administrator Authentication.....	34
Changing the Administrator.....	34

Using Web Image Monitor to Configure Administrator Authentication.....	35
--	----

3. Configuring User Authentication

Users.....	37
About User Authentication.....	38
Configuring User Authentication.....	39
Enabling User Authentication.....	41
User Code Authentication.....	42
Specifying User Code Authentication.....	42
Basic Authentication.....	46
Specifying Basic Authentication.....	46
Windows Authentication.....	53
Specifying Windows Authentication.....	54
Installing Internet Information Services (IIS) and Certificate Services.....	62
Creating the Server Certificate.....	62
If the fax number cannot be obtained.....	63
Installing the Device Certificate (Issued by a Certificate Authority).....	63
LDAP Authentication.....	65
Specifying LDAP Authentication.....	66
Integration Server Authentication.....	73
Specifying Integration Server Authentication.....	73
Printer Job Authentication.....	80
If User Authentication is Specified.....	83
If User Code Authentication is Specified.....	83
If Basic, Windows, LDAP or Integration Server Authentication is Specified.....	84
Logging on Using Web Image Monitor.....	85
Logging off Using Web Image Monitor.....	85
User Lockout Function.....	86
Auto Logout.....	88
Authentication Using an External Device.....	91

4. Protecting Data from Information Leaks

Preventing Unauthorized Copying.....	93
Unauthorized Copy Prevention.....	93
Data Security for Copying.....	94

Printing Limitations.....	96
Notice.....	96
Configuring Unauthorized Copy Prevention and Data Security for Copying.....	96
Printing a Confidential Document.....	99
Specifying Locked Print File.....	99
Printing a Locked Print File.....	100
Deleting Locked Print Files.....	101
Changing the Password of a Locked Print File.....	102
Unlocking a Locked Print File.....	103
Configuring Access Permissions for Stored Files.....	105
Specifying User and Access Permissions for Stored Files.....	106
Specifying Access Permissions for Files Stored Using the Scanner and Fax Functions.....	108
Specifying User and Access Permissions for Files Stored by a Particular User.....	112
Specifying Passwords for Stored Files.....	114
Unlocking Files.....	115

5. Securing Information Sent over the Network or Stored on Hard Disk

Preventing Information Leakage Due to Unauthorized Transmission.....	117
Restricting Destinations.....	117
Using S/MIME to Protect E-mail Transmission.....	119
E-mail Encryption.....	119
Attaching an Electronic Signature.....	121
Protecting the Address Book.....	127
Configuring Address Book Access Permissions.....	127
Encrypting Data in the Address Book.....	128
Encrypting Data on the Hard Disk.....	131
Enabling the Encryption Settings.....	131
Printing the Encryption Key.....	133
Updating the Encryption Key.....	134
Canceling Data Encryption.....	136
Deleting Data on the Hard Disk.....	137
Auto Erase Memory.....	137
Erase All Memory.....	142

6. Managing Access to the Machine

Preventing Changes to Machine Settings.....	145
Menu Protect.....	147
Specifying Menu Protect.....	147
Limiting Available Functions.....	152
Specifying Which Functions are Available.....	152
Managing Log Files.....	154
Using the Control Panel to Specify Log File Settings.....	154
Using Web SmartDeviceMonitor to Manage Log Files.....	156
Using Web Image Monitor to Manage Log Files.....	156
Logs that can be Managed Using Web Image Monitor.....	160

7. Enhanced Network Security

Preventing Unauthorized Access.....	167
Access Control.....	167
Enabling and Disabling Protocols.....	168
Specifying Network Security Level.....	176
Encrypting Transmitted Passwords.....	180
Specifying a Driver Encryption Key.....	180
Specifying a Group Password for PDF files.....	181
Specifying an IPP Authentication Password.....	183
Protection Using Encryption.....	185
SSL (Secure Sockets Layer) Encryption.....	185
User Settings for SSL (Secure Sockets Layer).....	190
Setting the SSL/TLS Encryption Mode.....	190
SNMPv3 Encryption.....	192
Transmission Using IPsec.....	194
Encryption and Authentication by IPsec.....	194
Encryption Key Auto Exchange Settings and Encryption Key Manual Settings.....	195
IPsec Settings.....	196
Encryption Key Auto Exchange Settings Configuration Flow.....	204
Encryption Key Manual Settings Configuration Flow.....	209
telnet Setting Commands.....	210
Authentication by telnet.....	218

"authfree" Command.....	218
Authentication by IEEE802.1X.....	219

8. Specifying the Extended Security Functions

Specifying the Extended Security Functions.....	221
Changing the Extended Security Functions.....	221
Extended Security Settings.....	222
Other Security Functions.....	227
Fax Function.....	227
Scanner Function.....	227
Weekly Timer Code.....	228
Limiting Machine Operations to Customers Only.....	231
Settings.....	231
Additional Information for Enhanced Security.....	234
Settings You Can Configure Using the Control Panel.....	234
Settings You Can Configure Using Web Image Monitor.....	236
Settings You Can Configure When IPsec Is Available/Unavailable.....	237

9. Troubleshooting

If Authentication Fails.....	241
If a Message is Displayed.....	241
If an Error Code is Displayed.....	243
If the Machine Cannot Be Operated.....	259

10. Appendix

Supervisor Operations.....	265
Logging on as the Supervisor.....	265
Logging off as the Supervisor.....	266
Changing the Supervisor.....	266
Resetting the Administrator's Password.....	267
Machine Administrator Settings.....	269
System Settings.....	269
Copier / Document Server Features.....	272
Facsimile Features.....	273
Printer Features.....	274
Scanner Features.....	275

Settings via Web Image Monitor.....	276
Settings via SmartDeviceMonitor for Admin.....	281
Network Administrator Settings.....	282
System Settings.....	282
Facsimile Features.....	283
Printer Features.....	283
Scanner Features.....	284
Settings via Web Image Monitor.....	284
Settings via SmartDeviceMonitor for Admin.....	287
File Administrator Settings.....	288
System Settings.....	288
Facsimile Features.....	288
Printer Features.....	288
Settings via Web Image Monitor.....	289
User Administrator Settings.....	290
System Settings.....	290
Settings via Web Image Monitor.....	290
Settings via SmartDeviceMonitor for Admin.....	291
Document Server File Permissions.....	293
The Privilege for User Account Settings in the Address Book.....	295
User Settings - Control Panel Settings.....	299
Copier / Document Server Features.....	300
Printer Functions.....	305
Printer Features.....	306
Scanner Features.....	311
Facsimile Features.....	313
System Settings.....	316
User Settings - Web Image Monitor Settings.....	324
Device Settings.....	325
Printer.....	332
Scanner.....	340
Fax.....	343
Interface.....	346

Network.....	348
Webpage.....	352
Functions That Require Options.....	353
Trademarks.....	354
INDEX	357

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.
- The printed and electronic versions of a manual have the same contents.
- 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.
- For enhanced security, we recommend that you first make the following settings. For details, see "Setting Up the Machine".
 - Install the Device Certificate.
 - Enable SSL (Secure Sockets Layer) Encryption.
 - Change the user name and password of the administrator using Web Image Monitor.

About This Machine

Before using the machine, be sure to read the section of this manual entitled Safety Information.

This manual introduces the machine's various functions. It also explains the control panel, preparation procedures for using the machine, how to enter text, how to install the CD-ROMs provided, and how to replace paper, toner, staples, and other consumables.

Troubleshooting

Provides a guide for resolving common usage-related problems.

Copy and Document Server Reference

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

Facsimile Reference

Explains Facsimile functions and operations.

Printer Reference

Explains Printer functions and operations.

Scanner Reference

Explains Scanner functions and operations.

Network and System Settings Guide

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

Security Reference

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

PostScript 3 Supplement

Explains how to set up and use PostScript 3.

Other manuals

- Unix Supplement
- Quick Reference Copy Guide
- Quick Reference Printer Guide
- Quick Reference Fax Guide
- Quick Reference Scanner Guide
- Manuals for DeskTopBinder Lite
 - DeskTopBinder Lite Setup Guide
 - DeskTopBinder Introduction Guide
 - Auto Document Link Guide

Note

- Manuals provided are specific to machine types.
- 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.
- The following software products are referred to using general names:

Product name	General name
DeskTopBinder Lite and DeskTopBinder Professional * 1	DeskTopBinder
ScanRouter EX Professional * 1 and ScanRouter EX Enterprise * 1	the ScanRouter delivery software
Web SmartDeviceMonitor Professional IS * 1 and Web SmartDeviceMonitor Standard * 1	Web SmartDeviceMonitor

* 1 Optional

Notice

Important

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.

For good copy quality, the supplier recommends that you use genuine toner from the supplier.

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

How to Read This Manual

Symbols

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 that appear on the machine's display panel.

[]

Indicates the names of keys on the machine's control panel.

IP Address

In this manual, "IP address" covers both IPv4 and IPv6 environments. Read the instructions that are relevant to the environment you are using.

Notes

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

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

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.

Laws and Regulations

Legal Prohibition

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.

1. Getting Started

This chapter describes the machine's security features and how to specify initial security settings.

Before Using the Security Functions

★ Important

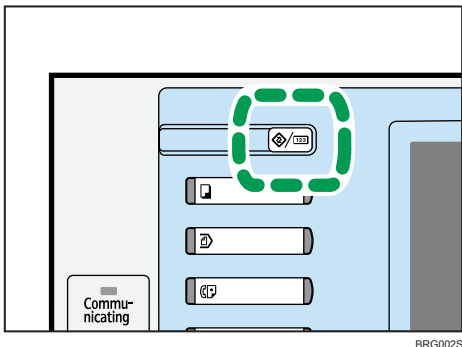
- **If the security settings are not specified, the machine may be damaged by malicious attackers.**
 1. To prevent this machine being stolen or willfully damaged, etc., install it in a secure location.
 2. Purchasers of this machine must make sure that people who use it do so appropriately, in accordance 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 Reference 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.

Setting Up the Machine

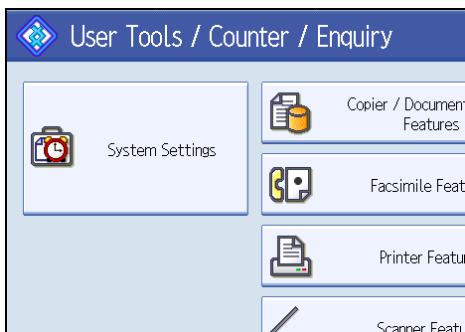
1

This section explains how to enable encryption of transmitted data and configure the administrator account. If you want higher security, make the following setting before using the machine.

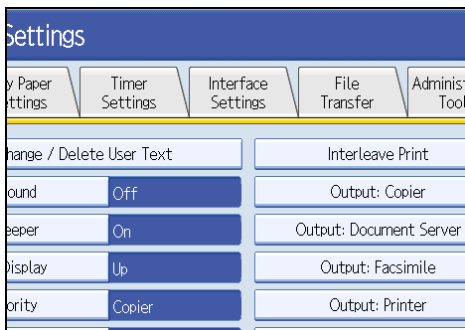
- 1. Turn the machine on.
- 2. Press the [User Tools] key.



- 3. Press [System Settings].



- 4. Press [Interface Settings].



5. Specify IPv4 Address.

For details on how to specify the IPv4 address, see "Interface Settings", Network and System Settings Guide.

6. Connect the machine to the network.

7. Start Web Image Monitor, and then log on to the machine as the administrator.

For details about logging on to Web Image Monitor as an administrator, see "Using Web Image Monitor to Configure Administrator Authentication".

8. Install the device certificate.

For information on how to install the device certificate, see "Protection Using Encryption".

9. Enable secure sockets layer (SSL).

For details about enabling SSL, see "Protection Using Encryption".

10. Enter the administrator's user name and password.

For details about specifying the administrator user name and password, see "Registering the Administrator".

The administrator's default account (user name: "admin"; password: blank) is unencrypted between steps 6 to 9. If acquired during this time, this account information could be used to gain unauthorized access to the machine over the network.

If you consider this risky, we recommend that you specify a temporary administrator password for accessing Web Image Monitor for the first time, before connecting to the network in step 6.

We recommend you change the supervisor's password also. For details about changing the supervisor's user name and password, see "Changing the Supervisor".

Reference

- p.35 "Using Web Image Monitor to Configure Administrator Authentication"
- p.185 "Protection Using Encryption"
- p.30 "Registering the Administrator"
- p.266 "Changing the Supervisor"

Enhanced Security

1

This machine's security functions can be enhanced by managing the machine and its users using the improved authentication functions.

By specifying access limits for the machine's functions and the documents and data stored in the machine, information leaks and unauthorized access can be prevented.

Data encryption also prevents unauthorized data access and tampering via the network.

The machine also automatically checks the configuration and supplier of the firmware each time the main power is switched on and whenever firmware is installed.

Authentication and Access Limits

Using authentication, administrators manage the machine and its users. To enable authentication, information about both administrators and users must be registered in order to authenticate users via their login user names and passwords.

Four types of administrators manage specific areas of machine usage, such as settings and user registration.

Access limits for each user are specified by the administrator responsible for user access to machine functions and documents and data stored in the machine.

For details about the administrator, see "Administrators".

For details about the user, see "Users".

Encryption Technology

This machine can establish secure communication paths by encrypting transmitted data and passwords.

Reference

- p.23 "Administrators"
- p.37 "Users"

Glossary

Administrator

There are four types of administrators according to administrative function: machine administrator, network administrator, file administrator, and user administrator. We recommend a different person for each administrator role.

In this way, you can spread the workload and limit unauthorized operation by a single administrator.

Basically, administrators make machine settings and manage the machine; but they cannot perform normal operations, such as copying and printing.

User

A user performs normal operations on the machine, such as copying and printing.

File Creator (Owner)

This is a user who can store files in the machine and authorize other users to view, edit, or delete those files.

Registered User

Users with personal information registered in the Address Book who have a login password and user name.

Administrator Authentication

Administrators are authenticated by their login user name and login password, supplied by the administrator, when specifying the machine's settings or accessing the machine over the network.

User Authentication

Users are authenticated by a login user name and login password, supplied by the user, when specifying the machine's settings or accessing the machine over the network.

The user's login user name and password, as well as such personal information items as facsimile number and e-mail address, are stored in the machine's address book. The personal information can be obtained from the Windows domain controller (Windows authentication), LDAP Server (LDAP authentication), or Integration Server (Integration Server authentication) connected to the machine via the network. The "Integration Server" is the computer on which Authentication Manager is installed.

Login

This action is required for administrator authentication and user authentication. Enter your login user name and login password on the machine's control panel. A login user name and login password may also be required when accessing the machine over the network or using such utilities as Web Image Monitor and SmartDeviceMonitor for Admin.

Logout

This action is required with administrator and user authentication. This action is required when you have finished using the machine or changing the settings.

Security Measures Provided by this Machine

1

Using Authentication and Managing Users

Enabling Authentication

To control administrators' and users' access to the machine, perform administrator authentication and user authentication using login user names and login passwords. To perform authentication, the authentication function must be enabled. For details about authentication settings, see "Configuring User Authentication".

Specifying Authentication Information to Log on

Users are managed using the personal information managed in the machine's Address Book.

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 information on specifying information to log on, see "Basic Authentication".

Specifying Which Functions are Available

This can be specified by the user administrator. Specify the functions available to registered users. By making this setting, you can limit the functions available to users. For information on how to specify which functions are available, see "Limiting Available Functions".

Reference

- p.39 "Configuring User Authentication"
- p.46 "Basic Authentication"
- p.152 "Limiting Available Functions"

Ensuring Information Security

Preventing Unauthorized Copying (Unauthorized Copy Prevention)

Using the printer driver, you can embed a mask and pattern in the printed document. For details about preventing unauthorized copying, see "Preventing Unauthorized Copying". For information on how to specify Unauthorized Copy Prevention, see "Configuring Unauthorized Copy Prevention and Data Security for Copying".

Preventing Unauthorized Copying (Data Security for Copying)

Using the printer driver to enable data security for the copying function, you can print a document with an embedded pattern of hidden text.

The optional Copy Data Security Unit is required if you want to gray out copies or store "data security for copying" documents. For details about Data Security for Copying, see "Data Security for Copying".

Printing Confidential files

Using the printer's Locked Print, you can store files in the machine as confidential files and then print them. You can print a file using the machine's control panel and collect it on the spot to prevent others from seeing it. For details about printing confidential files, see "Printing a Confidential Document".

Protecting Stored Files from Unauthorized Access

You can specify who is allowed to use and access scanned files and the files in Document Server. You can prevent activities such as the printing of stored files by unauthorized users. For details about protecting stored files from unauthorized access, see "Configuring Access Permissions for Stored Files".

Protecting Stored Files from Theft

You can specify who is allowed to use and access scanned files and the files in Document Server. You can prevent activities such as the sending and downloading of stored files by unauthorized users. For details about protecting stored files from theft, see "Configuring Access Permissions for Stored Files".

Preventing Data Leaks Due to Unauthorized Transmission

You can specify in the Address Book which users are allowed to send files using the scanner or fax function.

You can also limit the direct entry of destinations to prevent files from being sent to destinations not registered in the Address Book. For details about preventing data leaks due to unauthorized transmission, see "Preventing Information Leakage Due to Unauthorized Transmission".

Using S/MIME to Protect E-mail Transmission

When sending mail from the scanner or forwarding a fax to a user registered in the Address Book, you can use S/MIME to protect its contents from interception and alteration, and attach an electronic signature to guarantee the sender's identity. For details about using S/MIME to protect e-mail transmission, see "Using S/MIME to Protect E-mail Transmission".

Protecting Registered Information in the Address Book

You can specify who is allowed to access the data in the Address Book. You can prevent the data in the Address Book being used by unregistered users.

To protect the data from unauthorized reading, you can also encrypt the data in the Address Book. For details about protecting registered information in the Address Book, see "Protecting the Address Book".

Managing Log Files

The logs record failed access attempts and the names of users who accessed the machine successfully. You can use this information to help prevent data leaks.

To transfer the log data, Web SmartDeviceMonitor is required. For details about managing log files, see "Managing Log Files".

Encrypting Data on the Hard Disk

Encrypt data stored on the hard disk to prevent information leakage. The HDD Encryption Unit is required for hard disk data encryption. For details, see "Encrypting Data on the Hard Disk".

Overwriting the Data on the Hard Disk

To prevent data leaks, you can set the machine to automatically overwrite temporary data. We recommend that before disposing of the machine, you overwrite all the data on the hard disk.

To overwrite the hard disk data, the optional DataOverwriteSecurity Unit is required. For details about overwriting the data on the hard disk, see "Deleting Data on the Hard Disk".

Reference

- p.93 "Preventing Unauthorized Copying"
- p.96 "Configuring Unauthorized Copy Prevention and Data Security for Copying"
- p.94 "Data Security for Copying"
- p.99 "Printing a Confidential Document"
- p.105 "Configuring Access Permissions for Stored Files"
- p.117 "Preventing Information Leakage Due to Unauthorized Transmission"
- p.119 "Using S/MIME to Protect E-mail Transmission"
- p.127 "Protecting the Address Book"
- p.154 "Managing Log Files"
- p.131 "Encrypting Data on the Hard Disk"
- p.137 "Deleting Data on the Hard Disk"

Limiting and Controlling Access

Preventing Modification or Deletion of Stored Data

You can allow selected users to access stored scan files and files stored in Document Server.

You can permit selected users who are allowed to access stored files to modify or delete the files. For details about limiting and controlling access, see "Configuring Access Permissions for Stored Files".

Preventing Modification of Machine Settings

The machine settings that can be modified depend on the type of administrator account.

Register the administrators so that users cannot change the administrator settings. For details about preventing modification of machine settings, see "Preventing Changes to Machine Settings".

Limiting Available Functions

To prevent unauthorized operation, you can specify who is allowed to access each of the machine's functions. For details about limiting available functions for users and groups, see "Limiting Available Functions".

Reference

- p.105 "Configuring Access Permissions for Stored Files"
- p.145 "Preventing Changes to Machine Settings"

- p.152 "Limiting Available Functions"

Enhancing Network Security

1

Preventing Unauthorized Access

You can limit IP addresses or disable ports to prevent unauthorized access over the network and protect the Address Book, stored files, and default settings. For details about preventing unauthorized access, see "Preventing Unauthorized Access".

Encrypting Transmitted Passwords

Prevent login passwords, group passwords for PDF files, and IPP authentication passwords from being revealed by encrypting them for transmission.

Also, encrypt the login password for administrator authentication and user authentication. For details about encrypting transmitted passwords, see "Encrypting Transmitted Passwords".

Safer Communication Using SSL, SNMPv3 and IPsec

You can encrypt this machine's transmissions using SSL, SNMPv3, and IPsec. By encrypting transmitted data and safeguarding the transmission route, you can prevent sent data from being intercepted, analyzed, and tampered with. For details about safer communication using SSL, SNMPv3 and IPsec, see "Protection Using Encryption" and "Transmission Using IPsec".

Reference

- p.167 "Preventing Unauthorized Access"
- p.180 "Encrypting Transmitted Passwords"
- p.185 "Protection Using Encryption"
- p.194 "Transmission Using IPsec"

2. Configuring Administrator Authentication

This chapter describes what an administrator can do, how to register an administrator, how to specify administrator authentication, and how to log on to and off from the machine as an administrator.

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. There are four types of administrators: machine administrator, network administrator, file administrator and user administrator. Sharing administrator tasks eases the burden on individual administrators while also limiting unauthorized operation by administrators. One person can act as more than one type of administrator. You can also specify a supervisor who can change each administrator's password. 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 "Registering the Administrator", and for instructions on changing the administrator's password, see "Supervisor Operations". For details on Users, see "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.

📖 Reference

- p.30 "Registering the Administrator"
- p.265 "Supervisor Operations"
- p.37 "Users"

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.

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.

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.

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.

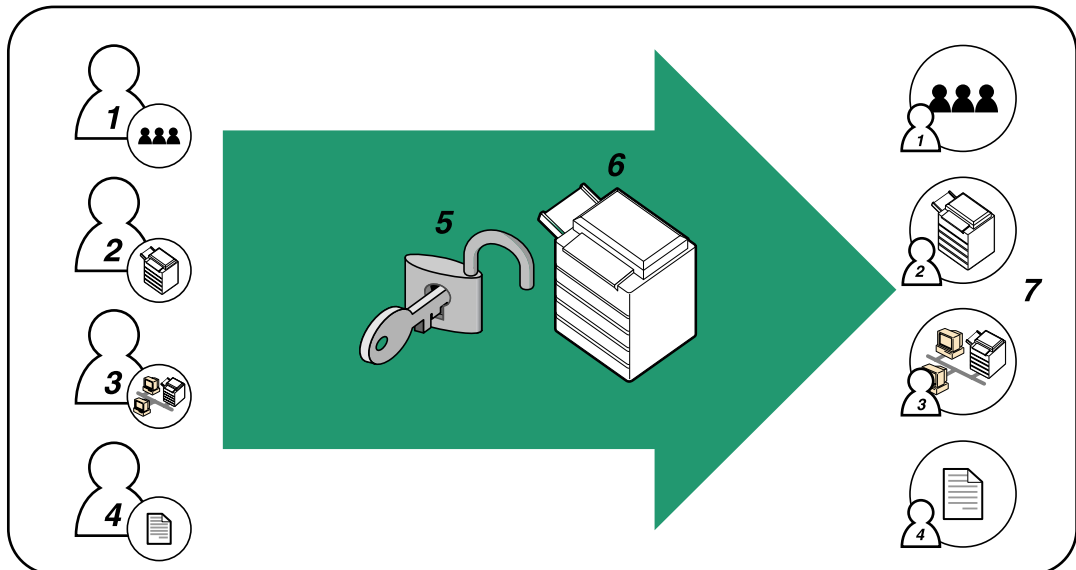
Supervisor

The supervisor can delete an administrator's password and specify a new one. The supervisor cannot specify defaults or use normal functions. However, if any of the administrators forget their password and cannot access the machine, the supervisor can provide support.

About Administrator Authentication

There are four types of administrators: user administrator, machine administrator, network administrator, and file administrator.

For details about each administrator, see "Administrators".



BBC005S

1. User Administrator

This administrator manages personal information in the Address Book. You can register/delete users in the Address Book or change users' personal information.

2. Machine Administrator

This administrator manages the machine's default settings. It is possible to enable only the machine administrator to set data security for copying, log deletion and other defaults.

3. Network Administrator

This administrator 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 be specified by the network administrator only.

4. File Administrator

This administrator manages permission to access stored files. You can specify passwords for Locked Print files stored in the Document Server so that only authorized users can view and change them.

5. Authentication

Administrators must enter their login user name and password to be authenticated.

6. This machine

7. Administrators manage the machine's settings and access limits.

 **Reference**

- p.23 "Administrators"

Enabling Administrator Authentication

To control administrators' access to the machine, perform administrator authentication using login user names and passwords. 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 on 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 authorities are granted to a single login user name. For instructions on registering the administrator, see "Registering the Administrator".

You can specify the login user name, login password, and encryption password for each administrator. The encryption password is a password for performing encryption when specifying settings using Web Image Monitor or SmartDeviceMonitor for Admin. The password registered in the machine must be entered when using applications such as SmartDeviceMonitor for Admin. 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 "Configuring User Authentication".

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.

Reference

- p.30 "Registering the Administrator"
- p.39 "Configuring User Authentication"

Specifying Administrator Privileges

To specify administrator authentication, set Administrator Authentication Management to [On]. In addition, if enabled in the settings, you can choose how the initial settings are divided among the administrators as controlled items.

To log on as an administrator, use the default login user name and login password.

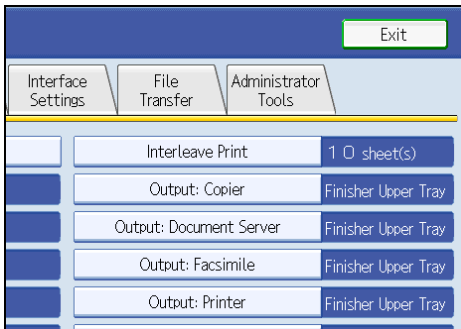
The defaults are "admin" for the login name and blank for the password. For details about changing the administrator password using the supervisor's authority, see "Supervisor Operations".

For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

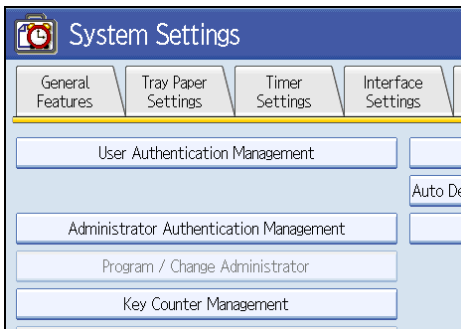
★ Important

- 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 authority. For instructions on registering the supervisor, see "Supervisor Operations".
- 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] key.
2. Press [System Settings].
3. Press [Administrator Tools].

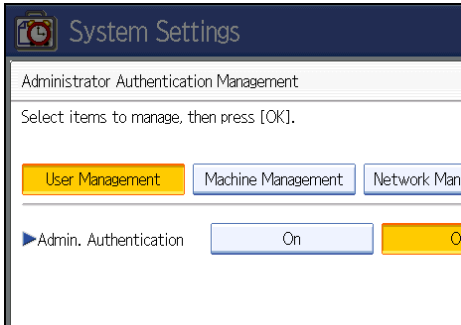


4. Press [Administrator Authentication Management].

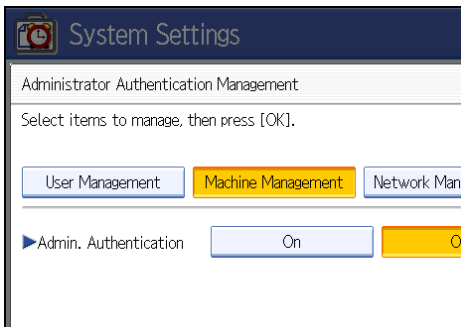


If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

5. Press [User Management], [Machine Management], [Network Management], or [File Management] to select which settings to manage.

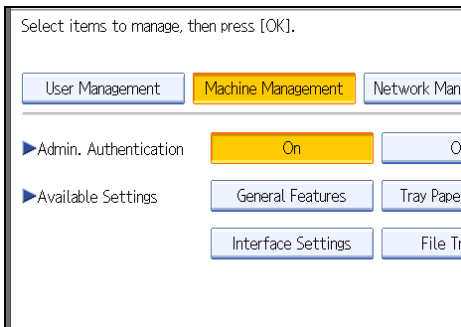


6. Set "Admin. Authentication" to [On].



"Available Settings" appears.

7. Select the settings to manage from "Available Settings".



The selected settings will be unavailable to users.

"Available Settings" varies depending on the administrator.

For details about "Available Settings", see "Limiting Available Functions".

To specify administrator authentication for more than one category, repeat steps 5 to 7.

8. Press [OK].
9. Press the [User Tools] key.

Reference

- p.265 "Supervisor Operations"
- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"
- p.152 "Limiting Available Functions"

2

Registering the Administrator

If administrator authentication has been specified, we recommend only one person take each administrator role.

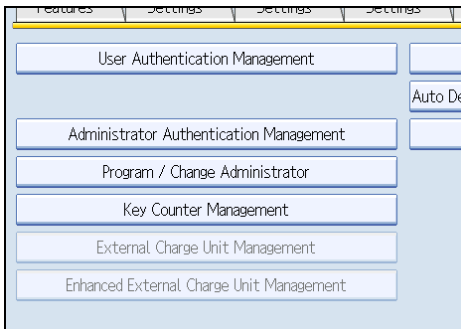
The sharing of administrator tasks eases the burden on individual administrators while also limiting unauthorized operation by a single administrator. You can register up to four login user names (Administrators 1-4) to which you can grant administrator privileges.

Administrator authentication can also be specified via Web Image Monitor. For details, see Web Image Monitor Help.

If administrator authentication has already been specified, log on using a registered administrator name and password.

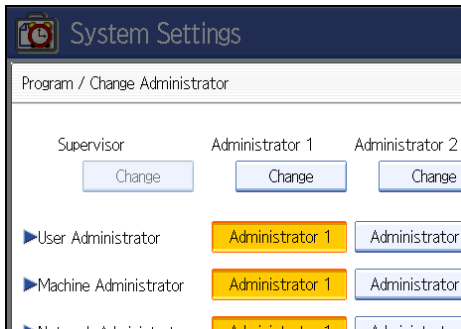
For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

1. Press the [User Tools] key.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [Program / Change Administrator].

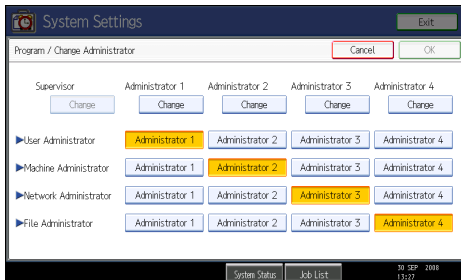


If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

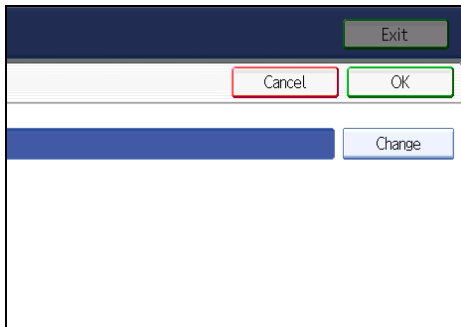
5. In the line for the administrator whose authority you want to specify, press [Administrator 1], [Administrator 2], [Administrator 3] or [Administrator 4], and then press [Change].



If you allocate each administrator's authority to a different person, the screen appears as follows:

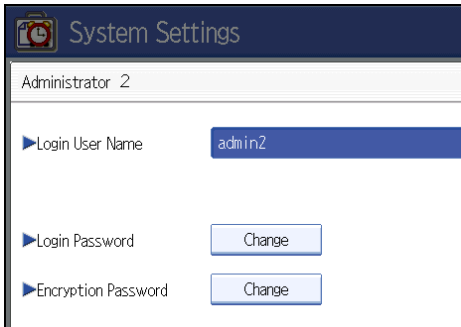


6. Press [Change] for the login user name.



7. Enter the login user name, and then press [OK].

8. Press [Change] for the login password.



9. 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 "Specifying the Extended Security Functions".

10. If a password reentry screen appears, enter the login password, and then press [OK].

11. Press [Change] for the encryption password.

12. Enter the encryption password, and then press [OK].

13. If a password reentry screen appears, enter the encryption password, and then press [OK].

14. Press [OK] twice.

You will be automatically logged off.

15. Press the [User Tools] key.

Note

- You can use up to 32 alphanumeric characters and symbols when registering login user names and login passwords. Keep in mind that passwords are case-sensitive.
- User names cannot contain numbers only, a space, colon (:), or quotation mark ("), nor can they be left blank.
- Do not use Japanese, Traditional Chinese, Simplified Chinese, or Hangul double-byte characters when entering the login user name or password. If you use multi-byte characters when entering the login user name or password, you cannot authenticate using Web Image Monitor.

Reference

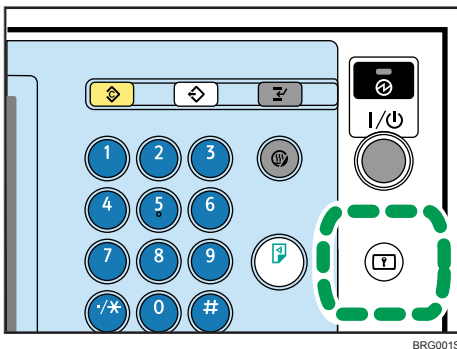
- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"
- p.221 "Specifying the Extended Security Functions"

Logging on Using Administrator Authentication

If administrator authentication has been specified, log on using an administrator's user name and password. This section describes how to log on. When you log on with a user name that has multiple administrator privileges, one of the administrator privileges associated with that name is displayed.

1. Press [User Tools] key.
2. Press the [Login/Logout] key.

2



The message, "Press [Login], then enter login user name and login password." appears.



3. Press [Login].
If you do not want to log on, press [Cancel].
4. Enter the login user name, and then press [OK].
When you log on to the machine for the first time as the administrator, enter "admin".
5. Enter the login password, and then 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 on as an administrator, enter the administrator's login user name and login password.
- If you log on using administrator authority, the name of the administrator logging on appears.

- If you log on using a login user name with the authority of more than one administrator, "Administrator" appears.
- If you try to log on 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] key to change the default.

2

Logging off Using Administrator Authentication

If administrator authentication has been specified, be sure to log off after completing settings. This section explains how to log off after completing settings.

1. Press the [Login/Logout] key.
2. Press [Yes].

Changing the Administrator

Change the administrator's login user name and login password. You can also assign administrator authority to the login user names [Administrator 1] to [Administrator 4]. To combine the authorities of multiple administrators, assign multiple administrators to a single administrator.

For example, to assign machine administrator authority and user administrator authority to [Administrator 1], press [Administrator 1] in the lines for the machine administrator and the user administrator.

For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

1. Press the [User Tools] key.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [Program / Change Administrator].
If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.
5. In the line for the administrator you want to change, press [Administrator 1], [Administrator 2], [Administrator 3] or [Administrator 4], and then press [Change].
6. Press [Change] for the setting you want to change, and re-enter the setting.
7. Press [OK].
8. Press [OK] twice.
You will be automatically logged off.
9. Press the [User Tools] key.

Reference

- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"

Using Web Image Monitor to Configure Administrator Authentication

2

Using Web Image Monitor, you can log on to the machine and change the administrator settings. This section describes how to access Web Image Monitor.

For details about Web Image Monitor, see Web Image Monitor Help.

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.

The top page of Web Image Monitor appears.

3. **Click [Login].**
4. **Enter the login name and password of an administrator, and then click [Login].**
5. **Make settings as desired.**

Note

- When logging on as an administrator use the login name and password of an administrator set in the machine. The default login name is "admin" and the password is blank.

3. Configuring User Authentication

This chapter describes what a user can do, how to specify user authentication, and how to log onto and off from the machine as a user.

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 "Administrators". For details about registering users in the Address Book, see "Administrator Tools", Network and System Settings Guide, SmartDeviceMonitor for Admin Help, or Web Image Monitor Help.

★ 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.

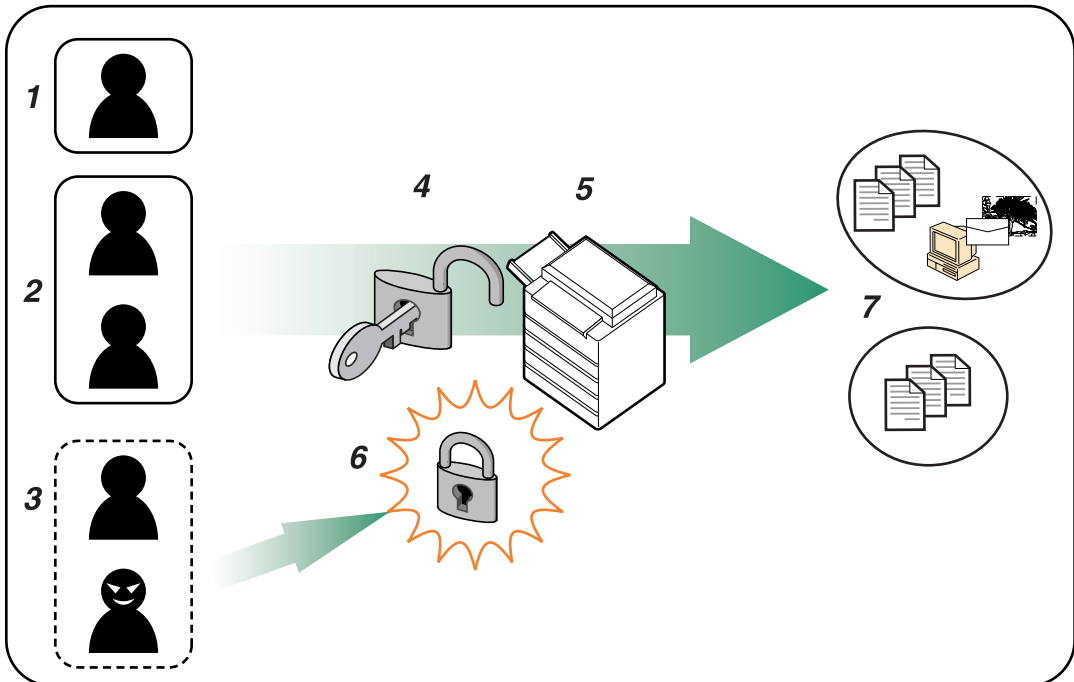
📖 Reference

- p.23 "Administrators"

About User Authentication

This machine has an authentication function to prevent unauthorized access.

By using login user name and login password, you can specify access limits for individual users and groups of users.



BBC004S

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. Authentication

Using a login user name and password, user authentication is performed.

5. This Machine

6. Access Limit

Using authentication, unauthorized users are prevented from accessing the machine.

7. Authorized users and groups can use only those functions permitted by the administrator.

Configuring User Authentication

Specify administrator authentication and user authentication according to the following chart:

<p>Administrator Authentication</p> <p>See "Enabling Administrator Authentication".</p>	<p>Specifying Administrator Privileges</p> <p>See "Specifying Administrator Privileges".</p> <p>Registering the Administrator</p> <p>See "Registering the Administrator".</p>
<p>User Authentication</p> <p>See "Enabling User Authentication".</p>	<p>Specifying User Authentication</p> <p>Authentication that requires only the machine:</p> <ul style="list-style-type: none"> • User Code Authentication See "User Code Authentication". • Basic Authentication See "Basic Authentication". <p>Authentication that requires external devices:</p> <ul style="list-style-type: none"> • Windows Authentication See "Windows Authentication". • LDAP Authentication See "LDAP Authentication". • Integration Server Authentication See "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.

📖 Reference

- p.27 "Enabling Administrator Authentication"
- p.41 "Enabling User Authentication"
- p.27 "Specifying Administrator Privileges"
- p.30 "Registering the Administrator"
- p.42 "User Code Authentication"
- p.46 "Basic Authentication"

- p.53 "Windows Authentication"
- p.65 "LDAP Authentication"
- p.73 "Integration Server Authentication"

Enabling 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.

↓ Note

- 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.
- You can specify User Code authentication without specifying administrator authentication.
- 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", Network and System Settings Guide. For details about changing passwords, see "Specifying Login User Names and Passwords".
- You cannot use more than one authentication method at the same time.
- User authentication can also be specified via Web Image Monitor. For details, see Web Image Monitor Help.

📖 Reference

- p.49 "Specifying Login User Names and Passwords"

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", Network and System Settings Guide.

For details about specifying the user code for the printer driver, see Printer Reference or the printer driver Help.

For details about specifying the TWAIN driver user code, see the TWAIN driver Help.

3

★ 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

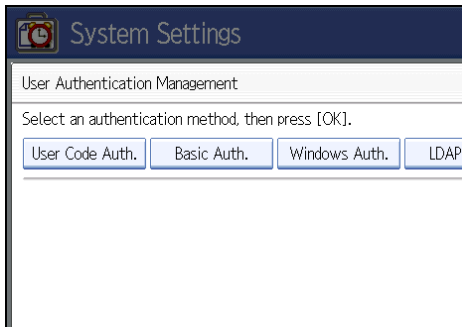
This can be specified by the machine administrator.

For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

1. Press the [User Tools] key.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [User Authentication Management].

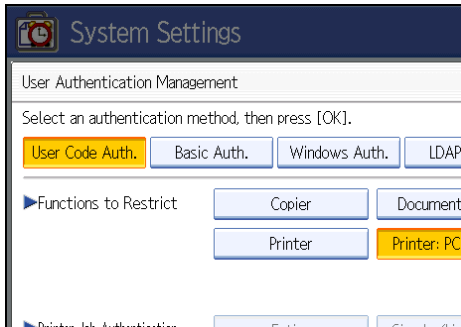
If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

5. Select [User Code Auth.].



If you do not want to use user authentication management, select [Off].

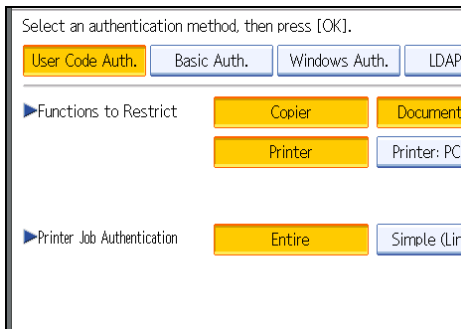
6. Select which of the machine's functions you want to limit.



The selected settings will be unavailable to users.

For details about limiting available functions for individuals or groups, see "Limiting Available Functions".

7. Select the "Printer Job Authentication" level.



If you select [Entire] or [Simple (All)], proceed to "Selecting Entire or Simple (All)".

If you select [Simple (Limitation)], proceed to "Selecting Simple (Limitation)".

For a description of the printer job authentication levels, see "Printer Job Authentication".

Reference

- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"
- p.152 "Limiting Available Functions"
- p.44 "Selecting Entire or Simple (All)"
- p.44 "Selecting Simple (Limitation)"
- p.80 "Printer Job Authentication"

Selecting Entire or Simple (All)

If you select [Entire], you cannot print using a printer driver or a device that does not support authentication. To print under an environment that does not support authentication, select [Simple (All)] or [Simple (Limitation)].

If you select [Simple (All)], you can print even with unauthenticated printer drivers or devices. Specify this setting if you want to print with a printer driver or device that cannot be identified by the machine or if you do not require authentication for printing. However, note that, because the machine does not require authentication in this case, it may be used by unauthorized users.

3

1. Press [OK].
2. Press [Exit].

A confirmation message appears.

If you press [Yes], you will be automatically logged off.

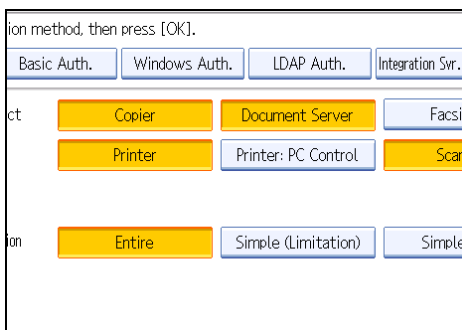
3. Press the [User Tools] key.

Selecting Simple (Limitation)

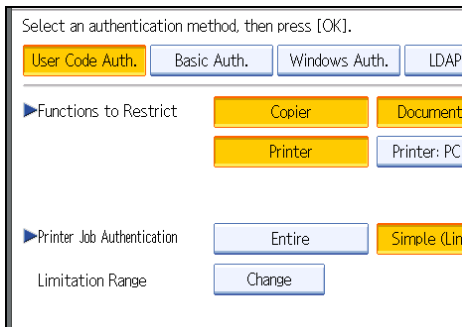
If you select [Simple (Limitation)], you can specify clients for which printer job authentication is not required. Specify [Parallel Interface: Simple], [USB: Simple] and the clients' IPv4 address range in which printer job authentication is not required. Specify this setting if you want to print using unauthenticated printer drivers or without any printer driver. Authentication is required for printing with non-specified devices.

If you select [Simple (Limitation)], you can print even with unauthenticated printer drivers or devices. Specify this setting if you want to print with a printer driver or device that cannot be identified by the machine or if you do not require authentication for printing. However, note that, because the machine does not require authentication in this case, it may be used by unauthorized users.

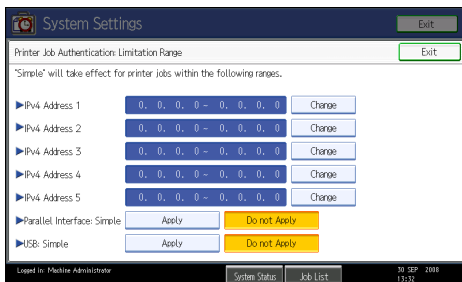
1. Press [Simple (Limitation)].



2. Press [Change].



3. Specify the range in which [Simple (Limitation)] is applied to "Printer Job Authentication".



You can specify the IPv4 address range to which this setting is applied, and whether or not to apply the setting to the parallel and USB interfaces.

4. Press [Exit].

5. Press [OK].

6. Press [Exit].

A confirmation message appears.

If you press [Yes], you will be automatically logged off.

7. Press the [User Tools] key.

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.

3

Specifying Basic Authentication

Before beginning to configure the machine, make sure that administrator authentication is properly configured under "Administrator Authentication Management".

This can be specified by the machine administrator.

For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

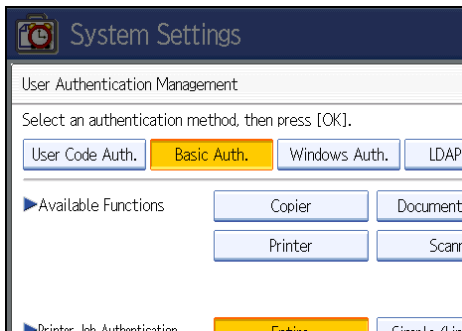
1. Press the [User Tools] key.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [User Authentication Management].

If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

5. Select [Basic Auth.].

If you do not want to use user authentication management, select [Off].

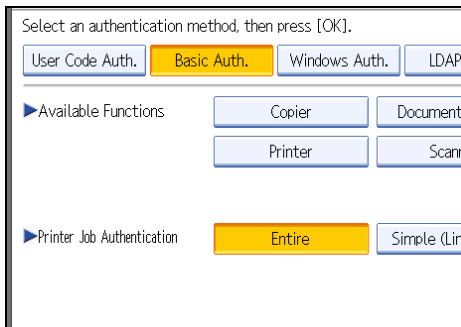
6. Select which of the machine's functions you want to permit.



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 "Limiting Available Functions".

7. Select the "Printer Job Authentication" level.



If you select [Entire] or [Simple (All)], proceed to "Selecting Entire or Simple (All)".

If you select [Simple (Limitation)], proceed to "Selecting Simple (Limitation)".

For a description of the printer job authentication levels, see "Printer Job Authentication".

Reference

- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"
- p.152 "Limiting Available Functions"
- p.47 "Selecting Entire or Simple (All)"
- p.48 "Selecting Simple (Limitation)"
- p.80 "Printer Job Authentication"

Selecting Entire or Simple (All)

If you select [Entire], you cannot print using a printer driver or a device that does not support authentication. To print under an environment that does not support authentication, select [Simple (All)] or [Simple (Limitation)].

If you select [Simple (All)], you can print even with unauthenticated printer drivers or devices. Specify this setting if you want to print with a printer driver or device that cannot be identified by the machine or if you do not require authentication for printing. However, note that, because the machine does not require authentication in this case, it may be used by unauthorized users.

1. Press [Exit].

2. Press [OK].

A confirmation message appears.

If you press [Yes], you will be automatically logged off.

3. Press the [User Tools] key.

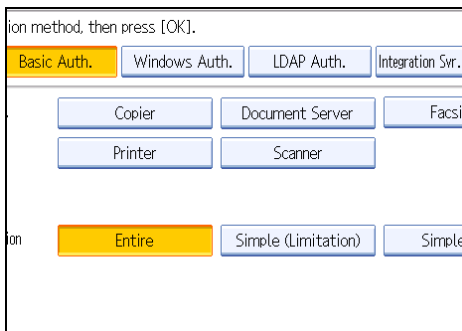
Selecting Simple (Limitation)

If you select [Simple (Limitation)], you can specify clients for which printer job authentication is not required. Specify [Parallel Interface: Simple], [USB: Simple] and the clients' IPv4 address range in which printer job authentication is not required. Specify this setting if you want to print using unauthenticated printer drivers or without any printer driver. Authentication is required for printing with non-specified devices.

If you select [Simple (Limitation)], you can print even with unauthenticated printer drivers or devices. Specify this setting if you want to print with a printer driver or device that cannot be identified by the machine or if you do not require authentication for printing. However, note that, because the machine does not require authentication in this case, it may be used by unauthorized users.

3

1. Press [Simple (Limitation)].



2. Press [Change].

3. Specify the range in which [Simple (Limitation)] is applied to "Printer Job Authentication".

You can specify the IPv4 address range to which this setting is applied, and whether or not to apply the setting to the parallel and USB interfaces.

4. Press [Exit].

5. Press [OK].

6. Press [Exit].

A confirmation message appears.

If you press [Yes], you will be automatically logged off.

7. Press the [User Tools] key.

Authentication Information Stored in the Address Book

This can be specified by the user administrator.

For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

If you have specified User Authentication, you can specify access limits for individual users and groups of users. Specify the setting in the Address Book for each user.

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", Network and System Settings Guide.

User authentication can also be specified via SmartDeviceMonitor for Admin or Web Image Monitor.

Reference

- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"

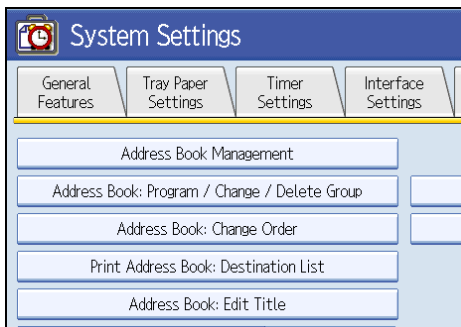
3

Specifying Login User Names and Passwords

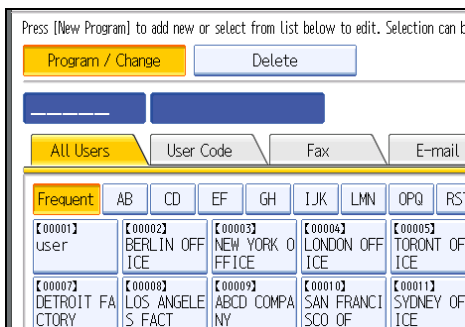
In "Address Book Management", specify the login user name and login password to be used for User Authentication Management.

Login user names can contain up to 32 characters; passwords can contain up to 128 characters. Both user names and passwords can contain alphanumeric characters and symbols. User names cannot contain spaces, colons, or quotation marks, and cannot be blank.

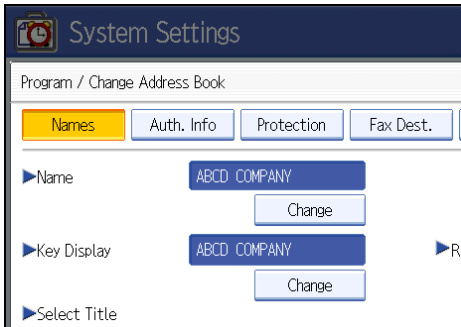
1. Press the [User Tools] key.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [Address Book Management].



5. Select the user or group.

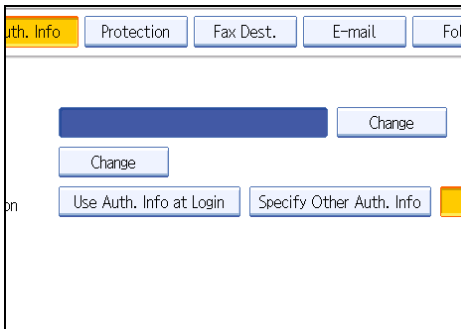


6. Press [Auth. Info].



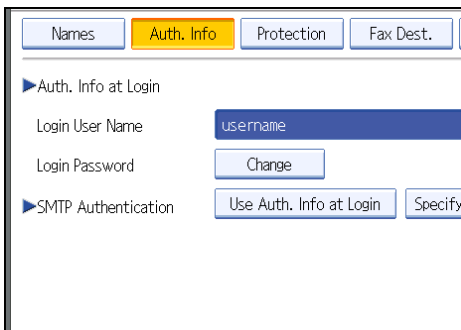
3

7. Press [Change] for "Login User Name".



8. Enter a login user name, and then press [OK].

9. Press [Change] for "Login Password".



10. Enter a login password, and then press [OK].

11. If a password reentry screen appears, enter the login password, and then press [OK].

12. Press [OK].

13. Press [Exit] twice.

14. Press the [User Tools] key.

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".

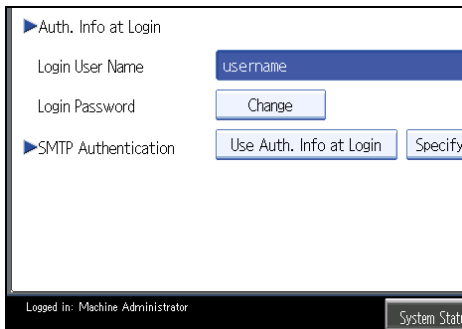
If you do not want to use the login user name and password specified in "Address Book Management" for "SMTP Authentication", "Folder Authentication", or "LDAP Authentication", see "Address Book" Network and System Settings Guide.

For details about specifying login user name and login password, see "Specifying Login User Names and Passwords".

★ 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.
- To use "Use Auth. Info at Login" for "SMTP Authentication", a login password up to 128 characters in length must be specified.

1. Press the [User Tools] key.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [Address Book Management].
5. Select the user or group.
6. Press [Auth. Info].
7. Select [Use Auth. Info at Login] in "SMTP Authentication".



If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

For folder authentication, select [Use Auth. Info at Login] in "Folder Authentication".

For LDAP authentication, select [Use Auth. Info at Login] in "LDAP Authentication".

8. Press [OK].
9. Press [Exit].
10. Press the [User Tools] key.

 **Reference**

- p.49 "Specifying Login User Names and Passwords"

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. If you can obtain user information, the sender's address (From:) is fixed to prevent unauthorized access when sending e-mails under the scanner function and forwarding received e-mails.

Windows authentication can be performed using one of two authentication methods: NTLM or Kerberos authentication. The operational requirements for both methods are listed below.

3

Operational Requirements for NTLM authentication

To specify NTLM authentication, the following requirements must be met:

- This machine only supports NTLMv1 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 SSL is being used, a version of Windows that supports TLS v1, SSL v2, or SSL v3 is required.
 - Windows 2000 Server
 - Windows Server 2003/Windows Server 2003 R2
 - Windows Server 2008

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 be able to support KDC (Key Distribution Center). To obtain user information when running Active Directory, use LDAP. If SSL is being used, a version of Windows that supports TLSv1, SSLv2, or SSLv3 is required. Compatible operating systems are listed below.
 - Windows 2000 Server
 - Windows Server 2003/Windows Server 2003 R2
 - Windows Server 2008

★ 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 you have created a new user in the domain controller and selected "User must change password at next logon", log on to the machine from the computer to change the password before logging on from the machine's control panel.
- If the authenticating server only supports NTLM when Kerberos authentication is selected on the machine, the authenticating method will automatically switch to NTLM.
- If Kerberos authentication and SSL encryption are set at the same time, e-mail addresses cannot be obtained.

Note

3

- Enter the login password correctly; keeping in mind that it is case-sensitive.
- 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.
- A user registered in two or more global groups can use all the functions available to members of 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".

Specifying Windows Authentication

Before beginning to configure the machine, make sure that administrator authentication is properly configured under "Administrator Authentication Management".

This can be specified by the machine administrator.

For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

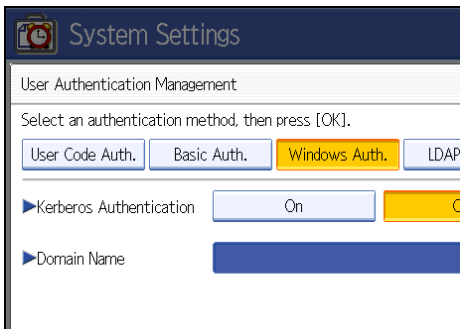
1. Press the [User Tools] key.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [User Authentication Management].

If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

5. Select [Windows Auth.].

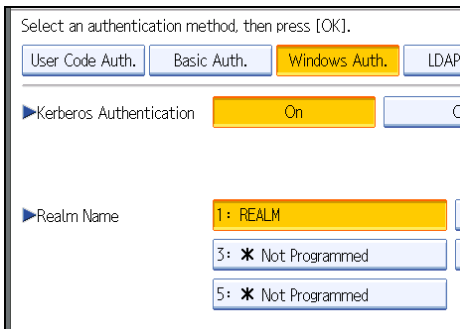
If you do not want to use user authentication management, select [Off].

6. If you want to use Kerberos authentication, press [On].



If you want to use NTLM authentication, press [Off] and proceed to step 8.

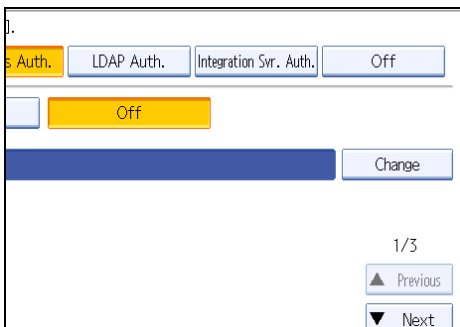
7. Select Kerberos authentication realm and proceed to step 9.



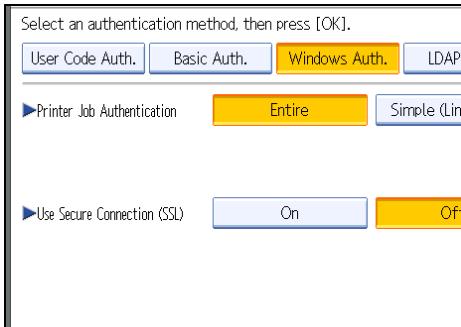
To enable Kerberos authentication, a realm must be registered beforehand. The realm name must be registered in capital letters. For details about registering a realm, see "Programming the Realm", Network and System Settings Guide.

Up to 5 realms can be registered.

8. Press [Change] for "Domain Name", enter the name of the domain controller to be authenticated, and then press [OK].



9. Select the "Printer Job Authentication" level.



3

If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

If you select [Entire] or [Simple (All)], proceed to "Selecting Entire or Simple (All)".

If you select [Simple (Limitation)], proceed to "Selecting Simple (Limitation)".

For a description of the printer job authentication levels, see "Printer Job Authentication".

Reference

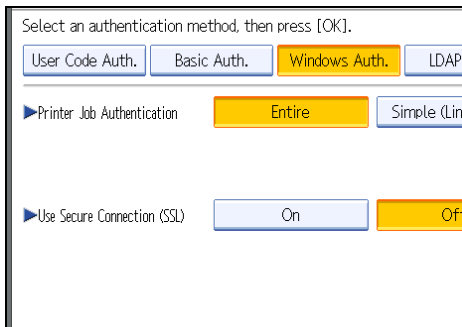
- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"
- p.56 "Selecting Entire or Simple (All)"
- p.59 "Selecting Simple (Limitation)"
- p.80 "Printer Job Authentication"

Selecting Entire or Simple (All)

If you select [Entire], you cannot print using a printer driver or a device that does not support authentication. To print in an environment that does not support authentication, select [Simple (All)] or [Simple (Limitation)].

If you select [Simple (All)], you can print even with unauthenticated printer drivers or devices. Specify this setting if you want to print with a printer driver or device that cannot be identified by the machine or if you do not require authentication for printing. However, note that, because the machine does not require authentication in this case, it may be used by unauthorized users.

1. Press [On] for "Use Secure Connection (SSL)".



If you are not using secure sockets layer (SSL) for authentication, press [Off].

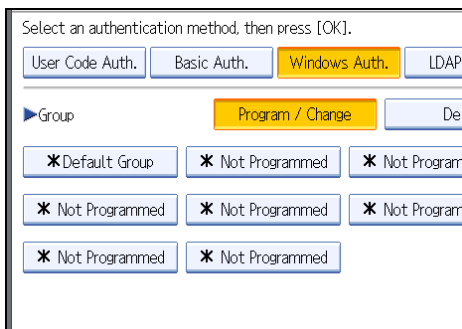
If global groups have been registered under Windows server, you can limit the use of functions for each global group.

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.

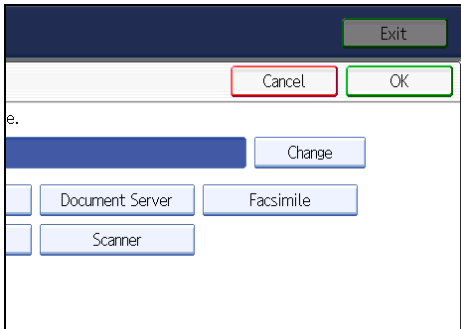
If global groups are not specified, users can use the available functions specified in [*Default Group]. If global groups are specified, users not registered in global groups can use the available functions specified in [*Default Group]. By default, all functions are available to *Default Group members. Specify the limitation on available functions according to user needs.

2. Under "Group", press [Program / Change], and then press [* Not Programmed].

If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.



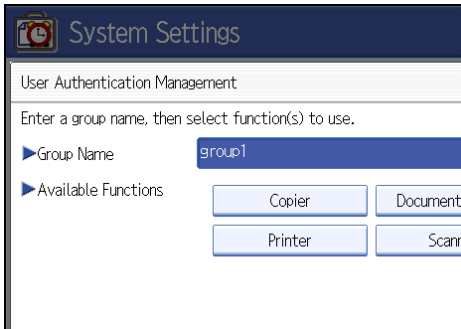
3. Under "Group Name", press [Change], and then enter the group name.



3

4. Press [OK].

5. Select which of the machine's functions you want to permit.



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 "Limiting Available Functions".

6. Press [OK] twice.

7. Press the [User Tools] key.

A confirmation message appears.

If you press [Yes], you will be automatically logged off.

Note

- 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.
- 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.

Reference

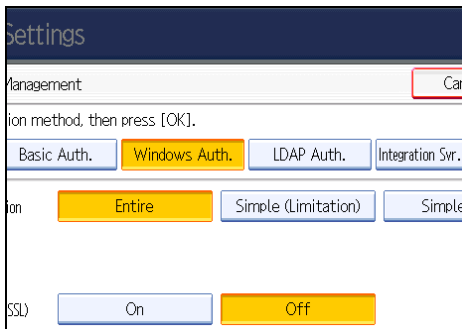
- p.152 "Limiting Available Functions"

Selecting Simple (Limitation)

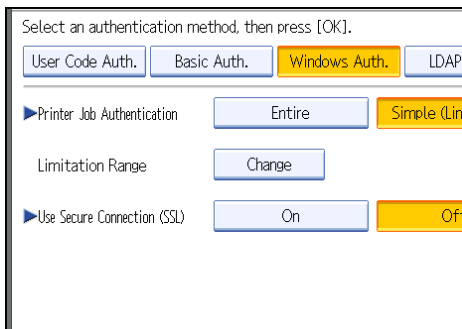
If you select [Simple (Limitation)], you can specify clients for which printer job authentication is not required. Specify [Parallel Interface: Simple], [USB: Simple] and the clients' IPv4 address range in which printer job authentication is not required. Specify this setting if you want to print using unauthenticated printer drivers or without any printer driver. Authentication is required for printing with non-specified devices.

If you select [Simple (Limitation)], you can print even with unauthenticated printer drivers or devices. Specify this setting if you want to print with a printer driver or device that cannot be identified by the machine or if you do not require authentication for printing. However, note that, because the machine does not require authentication in this case, it may be used by unauthorized users.

1. Press [Simple (Limitation)].



2. Press [Change].

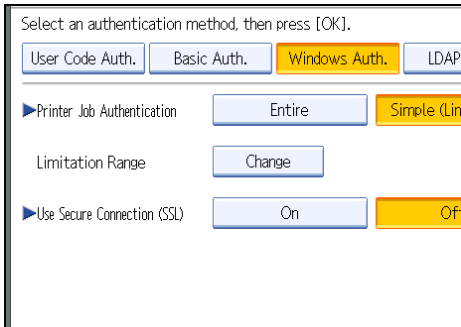


3. Specify the range in which [Simple (Limitation)] is applied to "Printer Job Authentication".

You can specify the IPv4 address range to which this setting is applied, and whether or not to apply the setting to the parallel and USB interfaces.

4. Press [Exit].

5. Press [On] for "Use Secure Connection (SSL)".



3

If you are not using secure sockets layer (SSL) for authentication, press [Off].

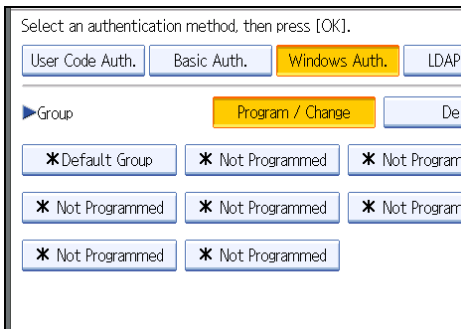
If global groups have been registered under Windows server, you can limit the use of functions for each global group.

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.

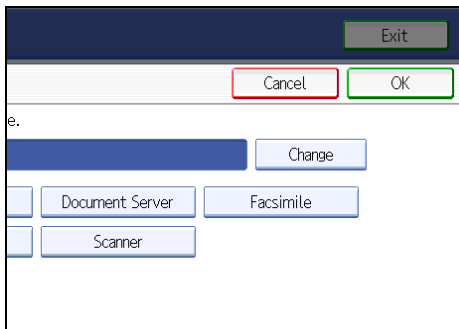
If global groups are not specified, users can use the available functions specified in [*Default Group]. If global groups are specified, users not registered in global groups can use the available functions specified in [*Default Group]. By default, all functions are available to *Default Group members. Specify the limitation on available functions according to user needs.

6. Under "Group", press [Program / Change], and then press [* Not Programmed].

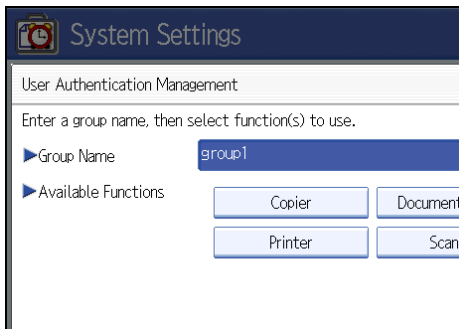
If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.



7. Under "Group Name", press [Change], and then enter the group name.



8. Press [OK].
9. Select which of the machine's functions you want to permit.



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 "Limiting Available Functions".

10. Press [OK] twice.
11. Press the [User Tools] key.

A confirmation message appears.

If you press [Yes], you will be automatically logged off.

↓ Note

- 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.
- 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.

Reference

- p.152 "Limiting Available Functions"

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.

3

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:

1. Select [Add/Remove Programs] on the Control Panel.
2. Select [Add/Remove Windows Components].
3. Select the "Internet Information Services (IIS)" check box.
4. Select the "Certificate Services" check box, and then click [Next].
5. Installation of the selected Windows components starts, and a warning message appears.
6. Click [Yes].
7. Click [Next].
8. Select the "Certificate Authority", and then click [Next].
On the displayed screen, "Enterprise root CA" is selected.
9. Enter the Certificate Authority name (optional) in "CA Identifying Information", and then click [Next].
10. Leave "Data Storage Location" at its default, and then click [Next].

Internet Information Services and Certificate services are installed.

Creating the Server Certificate

After installing Internet Information Services (IIS) and Certificate services Windows components, create the Server Certificate as follows:

1. Start Internet Services Manager.
2. Right-click [Default Web Site], and then click [Properties].
3. On the "Directory Security" tab, click [Server Certificate].

Web Server Certificate Wizard starts.

4. Click [Next].

5. Select [Create a new certificate], and then click [Next].
6. Select [Prepare the request now, but send it later], and then click [Next].
7. Enter the required information according to the instructions given by Web Server Certificate Wizard.
8. Check the specified data, which appears as "Request File Summary", and then click [Next].
The server certificate is created.

If the fax number cannot be obtained

3

If the fax number cannot be obtained during authentication, specify the setting as follows:

1. Start C:\WINNT\SYSTEM32\adminpak.
Setup Wizard starts.
2. Select [Install all of the Administrator Tools], and then click [Next].
3. On the "Start" menu, select [Run].
4. Enter "mmc", and then click [OK].
5. On the "Console", select [Add/Remove Snap-in].
6. Click [Add].
7. Select [Active Directory Schema], and then click [Add].
8. Select [Facsimile Telephone Number].
9. Right-click, and then click [Properties].
10. Select "Replicate this attribute", and then click [Apply].

Installing the Device Certificate (Issued by a Certificate Authority)

Install the device certificate using Web Image Monitor.

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. 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.

The top page of Web Image Monitor appears.

3. Click [Login].

The network administrator can log on.

Enter the login user name and password.

4. Click **[Configuration]**, and then click **[Device Certificate]** under **[Security]**.

The Device Certificate page appears.

5. Check the radio button next to the number of the certificate you want to install.
6. Click **[Install]**.
7. Enter the contents of the device certificate.
8. In the **[Certificate Request]** box, enter the contents of the device certificate received from the certificate authority.
9. Click **[OK]**.

[Installed] appears under [Certificate Status] to show that a device certificate for the machine has been installed.

10. Click **[Logout]**.

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.

Using Web Image Monitor, you can specify whether or not to check the reliability of the connecting SSL 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 LDAP server.
- Enter the user's login user name using up to 32 characters and login password using up to 128 characters.
- 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 ActiveDirectory 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".

Note

- 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.
- You can also prohibit blank passwords at login for simplified authentication. For details about LDAP Simplified authentication, contact your sales 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 "Available Functions" during LDAP Authentication. To limit the available functions for each user, register each user and corresponding "Available Functions" setting in the Address Book, or specify "Available Functions" for each registered user. The "Available Functions" setting becomes effective when the user accesses the machine subsequently.
- 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 the "Programming the LDAP Server", or "Programming the Realm", Network and System Settings Guide.
- The reference function is not available for SSL servers when a search for LDAP is in progress.

Specifying LDAP Authentication

Before beginning to configure the machine, make sure that administrator authentication is properly configured under "Administrator Authentication Management".

This can be specified by the machine administrator.

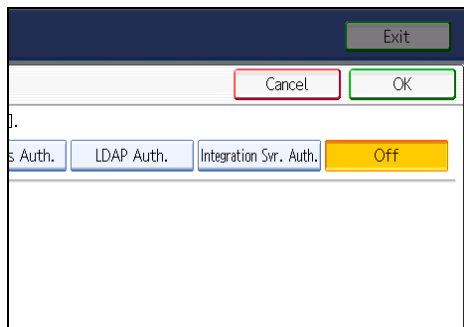
For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

1. Press the [User Tools] key.
2. Press [System Settings].
3. Press [Administrator Tools].

4. Press [User Authentication Management].

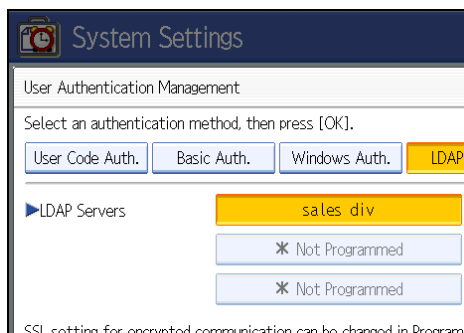
If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

5. Select [LDAP Auth.].



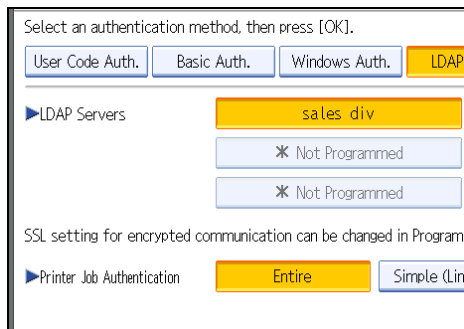
If you do not want to use user authentication management, select [Off].

6. Select the LDAP server to be used for LDAP authentication.



7. Select the "Printer Job Authentication" level.

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.



If you select [Entire] or [Simple (All)], proceed to "Selecting Entire or Simple (All)".

If you select [Simple (Limitation)], proceed to "Selecting Simple (Limitation)".

For a description of the printer job authentication levels, see "Printer Job Authentication".

Reference

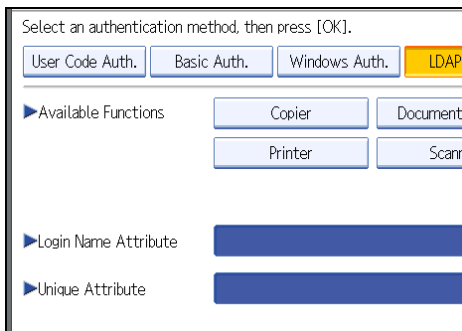
- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"
- p.56 "Selecting Entire or Simple (All)"
- p.59 "Selecting Simple (Limitation)"
- p.80 "Printer Job Authentication"

3 Selecting Entire or Simple (All)

If you select [Entire], you cannot print using a printer driver or a device that does not support authentication. To print under an environment that does not support authentication, select [Simple (All)] or [Simple (Limitation)].

If you select [Simple (All)], you can print even with unauthenticated printer drivers or devices. Specify this setting if you want to print with a printer driver or device that cannot be identified by the machine or if you do not require authentication for printing. However, note that, because the machine does not require authentication in this case, it may be used by unauthorized users.

1. Select which of the machine's functions you want to permit.

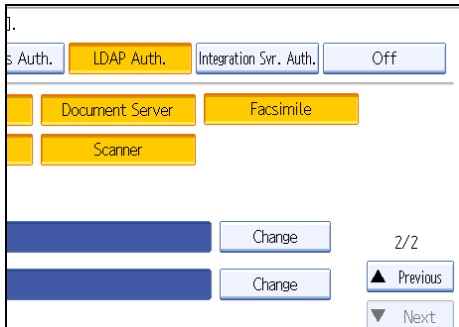


LDAP Authentication will be applied to the selected functions.

Users can use the selected functions only.

For details about specifying available functions for individuals or groups, see "Limiting Available Functions".

2. Press [Change] for "Login Name Attribute".



3. 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.

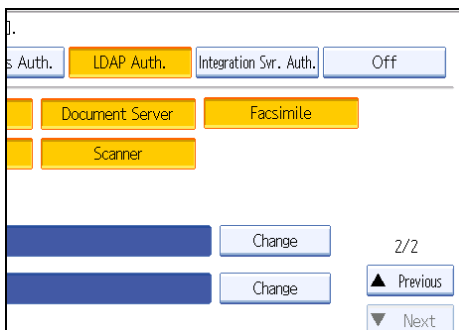
To specify multiple login attributes, place a comma (,) between them. The search will return hits for either or both attributes.

Also, if you place an equal sign (=) between a login attribute and a value (for example: `cn=abcde, uid=xyz`), the search will return only hits that match the values specified for 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.

4. Press [Change] for "Unique Attribute".



5. 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.

6. Press [OK].

7. Press the [User Tools] key.

A confirmation message appears.

If you press [Yes], you will be automatically logged off.

Reference

- p.152 "Limiting Available Functions"

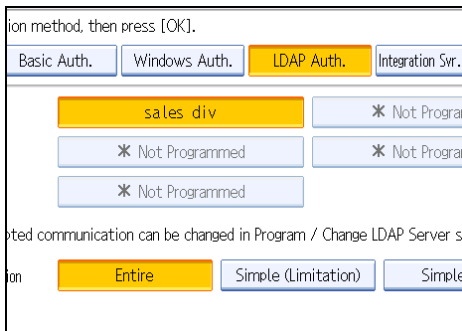
3

Selecting Simple (Limitation)

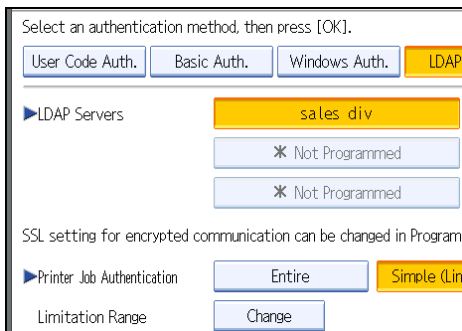
If you select [Simple (Limitation)], you can specify clients for which printer job authentication is not required. Specify [Parallel Interface: Simple], [USB: Simple] and the clients' IPv4 address range in which printer job authentication is not required. Specify this setting if you want to print using unauthenticated printer drivers or without any printer driver. Authentication is required for printing with non-specified devices.

If you select [Simple (Limitation)], you can print even with unauthenticated printer drivers or devices. Specify this setting if you want to print with a printer driver or device that cannot be identified by the machine or if you do not require authentication for printing. However, note that, because the machine does not require authentication in this case, it may be used by unauthorized users.

1. Press [Simple (Limitation)].



2. Press [Change].

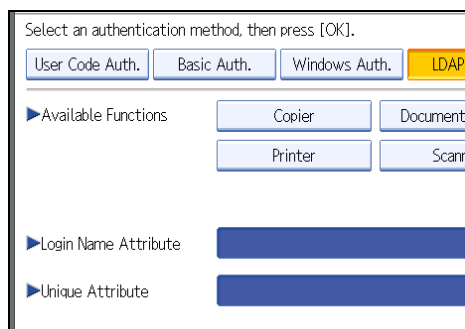


3. Specify the range in which [Simple (Limitation)] is applied to "Printer Job Authentication".

You can specify the IPv4 address range to which this setting is applied, and whether or not to apply the setting to the parallel and USB interfaces.

4. Press [Exit].

5. Select which of the machine's functions you want to permit.



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 "Limiting Available Functions".

6. Press [Change] for "Login Name Attribute".

7. 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.

8. Press [Change] for "Unique Attribute".

9. 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.

10. Press [OK].

11. Press the [User Tools] key.

A confirmation message appears.

If you press [Yes], you will be automatically logged off.

 **Reference**

- p.152 "Limiting Available Functions"

Integration Server Authentication

To use Integration Server authentication, you need a server on which ScanRouter software that supports authentication is installed.

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 Web SmartDeviceMonitor 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.

↓ Note

- The default administrator name for ScanRouter System or Web SmartDeviceMonitor, "Admin," differs from the server, "admin".

Specifying Integration Server Authentication

Before beginning to configure the machine, make sure that administrator authentication is properly configured under "Administrator Authentication Management".

This can be specified by the machine administrator.

For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

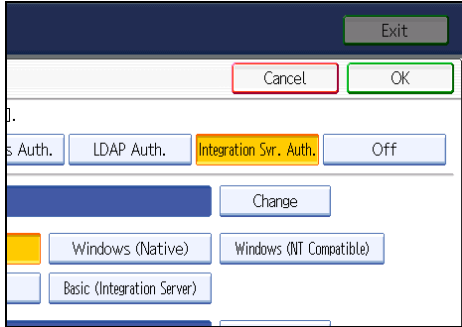
1. Press the [User Tools] key.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [User Authentication Management].

If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

5. Select [Integration Svr. Auth.].

If you do not want to use User Authentication Management, select [Off].

6. Press [Change] for "Server Name".



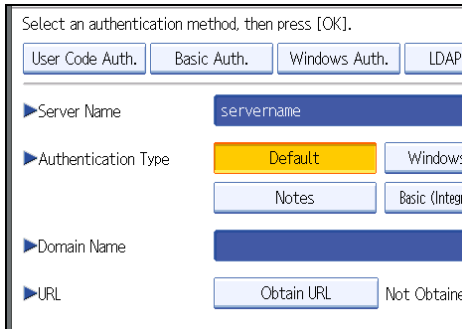
Specify the name of the server for external authentication.

7. Enter the server name, and then press [OK].

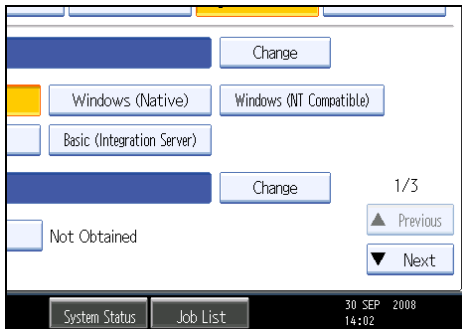
Enter the IPv4 address or host name.

8. In "Authentication Type", select the authentication system for external authentication.

Select an available authentication system. For general usage, select [Default].



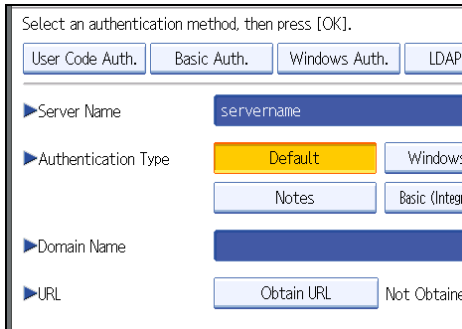
9. Press [Change] for "Domain Name".



10. Enter the domain name, and then press [OK].

You cannot specify a domain name under an authentication system that does not support domain login.

11. 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".

12. Press [Exit].

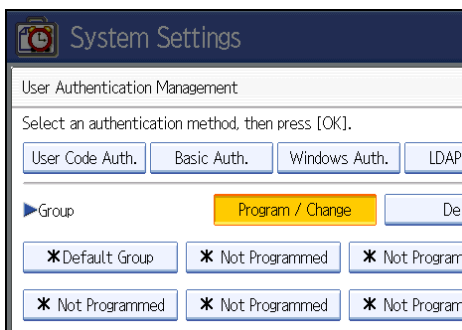
In the "Authentication Type", if you have not registered a group, proceed to step 17.

If you have registered a group, proceed to step 13.

If you set "Authentication Type" to [Windows (Native)] or [Windows (NT Compatible)], you can use the global group.

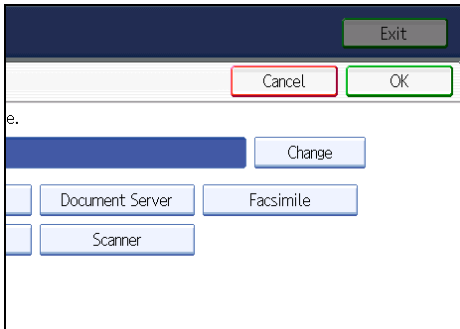
If you set "Authentication Type" to [Notes], you can use the Notes group. If you set "Authentication Type" to [Basic (Integration Server)], you can use the groups created using the Authentication Manager.

13. Under "Group", press [Program / Change], and then press [* Not Programmed].



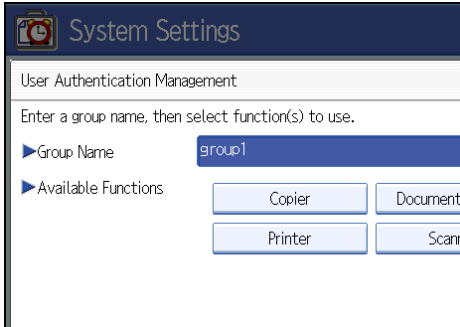
If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

14. Under "Group Name", press [Change], and then enter the group name.



3

15. Press [OK].
16. Select which of the machine's functions you want to permit.

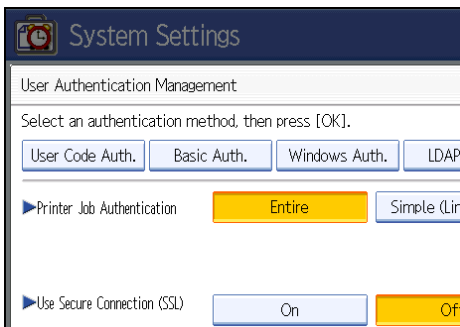


Authentication will be applied to the selected functions.

Users can use the selected functions only.

For details about specifying available functions for individuals or groups, see "Limiting Available Functions".

17. Press [OK].
18. Select the "Printer Job Authentication" level.



If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

If you select [Entire] or [Simple (All)], proceed to "Selecting Entire or Simple (All)".

If you select [Simple (Limitation)], proceed to "Selecting Simple (Limitation)".

For a description of the printer job authentication levels, see "Printer Job Authentication".

Reference

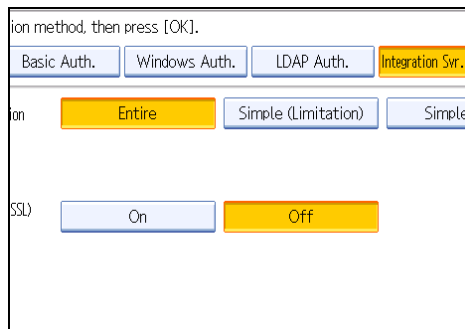
- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"
- p.152 "Limiting Available Functions"
- p.77 "Selecting Entire or Simple (All)"
- p.77 "Selecting Simple (Limitation)"
- p.80 "Printer Job Authentication"

Selecting Entire or Simple (All)

If you select [Entire], you cannot print using a printer driver or a device that does not support authentication. To print in an environment that does not support authentication, select [Simple (All)] or [Simple (Limitation)].

If you select [Simple (All)], you can print even with unauthenticated printer drivers or devices. Specify this setting if you want to print with a printer driver or device that cannot be identified by the machine or if you do not require authentication for printing. However, note that, because the machine does not require authentication in this case, it may be used by unauthorized users.

1. Press [On] for "Use Secure Connection (SSL)", and then press [OK].



To not use secure sockets layer (SSL) for authentication, press [Off].

2. Press the [User Tools] key.

A confirmation message appears.

If you press [Yes], you will be automatically logged off.

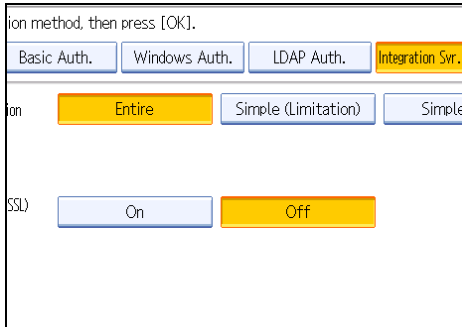
Selecting Simple (Limitation)

If you select [Simple (Limitation)], you can specify clients for which printer job authentication is not required. Specify [Parallel Interface: Simple], [USB: Simple] and the clients' IPv4 address range in which printer job

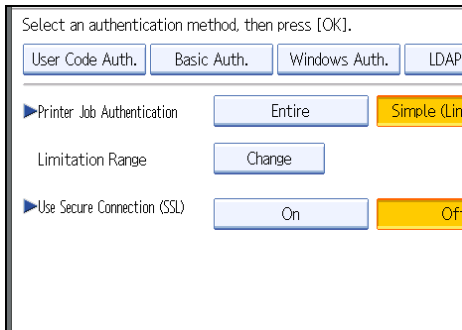
authentication is not required. Specify this setting if you want to print using unauthenticated printer drivers or without any printer driver. Authentication is required for printing with non-specified devices.

If you select [Simple (Limitation)], you can print even with unauthenticated printer drivers or devices. Specify this setting if you want to print with a printer driver or device that cannot be identified by the machine or if you do not require authentication for printing. However, note that, because the machine does not require authentication in this case, it may be used by unauthorized users.

1. Press [Simple (Limitation)].



2. Press [Change].

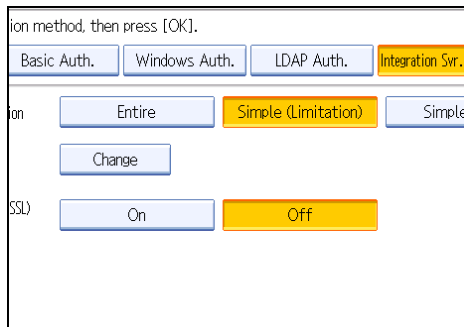


3. Specify the range in which [Simple (Limitation)] is applied to "Printer Job Authentication".

You can specify the IPv4 address range to which this setting is applied, and whether or not to apply the setting to the parallel and USB interfaces.

4. Press [Exit].

5. Press [On] for "Use Secure Connection (SSL)", and then press [OK].



To not use secure sockets layer (SSL) for authentication, press [Off].

6. Press the [User Tools] key.

A confirmation message appears.

If you press [Yes], you will be automatically logged off.

Printer Job Authentication

This section explains Printer Job Authentication.

Printer Job Authentication Levels and Printer Job Types

This section explains the relationship between printer job authentication levels and 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.

User authentication is supported by the RPCS and PCL printer drivers.

When User Authentication is set to "Off", printing is possible for all job types.

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.

User Authentication Management	Specified	Specified	Specified	Specified
Printer Job Authentication	Simple (All)	Simple (All)	Entire	Entire
Restrict Use of Simple Encryption	Off	On	Off	On
Printer Job Type 1	C	C	C	C
Printer Job Type 2	B	X	B	X
Printer Job Type 3	X	X	X	X
Printer Job Type 4	A	A	B	B
Printer Job Type 5	A	A	X	X
Printer Job Type 6	A	A	X	X
Printer Job Type 7	B	B	B	B

Printer Job Authentication

- Entire

The machine authenticates all printer jobs and remote settings, and cancels jobs and settings that fail authentication.

Printer Jobs: Job Reset

Settings: Disabled

- Simple (All)

The machine authenticates printer jobs and remote settings that have authentication information, and cancels the jobs and settings that fail authentication.

Printer jobs and settings without authentication information are performed without being authenticated.

- Simple (Limitation)

You can specify the range to apply [Simple (Limitation)] to by specifying [Parallel Interface: Simple], [USB: Simple], and the client's IPv4 address.

3

Printer Job Types

1. In the RPCS printer driver dialog box, the [Confirm authentication information when printing] and [Encrypt] check boxes are selected. In the PCL printer driver dialog box, the [User Authentication] and [Encrypt] check boxes are selected. Personal authentication information is added to the printer job. The printer driver applies advanced encryption to the login passwords. The printer driver encryption key enables driver encryption and prevents the login password from being stolen.

For details about prohibiting the use of simple encryption using "Restrict Use of Simple Encryption", see "Specifying the Extended Security Functions".

2. In the RPCS printer driver dialog box, the [Confirm authentication information when printing] check box is selected. In the PCL printer driver dialog box, the [User Authentication] and [Encrypt] check boxes are selected. Personal authentication information is added to the printer job. The printer driver applies simple encryption to login passwords.

For details about turning off "Restrict Use of Simple Encryption" and allowing the use of simple encryption, see "Specifying the Extended Security Functions".

3. In the RPCS printer driver dialog box, the [Confirm authentication information when printing] check box is not selected. In the PCL printer driver dialog box, the [User Authentication] check box is not selected. Personal authentication information is added to the printer job and is disabled.
4. When using the PostScript 3 printer driver, the printer job contains user code information. Personal authentication information is not added to the printer job but the user code information is. This also applies to recovery/parallel printing using an RPCS/PCL printer driver that does not support authentication.
5. When using the PostScript 3 printer driver, the printer job does not contain user code information. Neither personal authentication information nor user code information is added to the printer job. This also applies to recovery/parallel printing using an RPCS/PCL printer driver that does not support authentication.
6. A printer job or PDF file is sent from a host computer without a printer driver and is printed via LPR. Personal authentication information is not added to the printer job. The above is also true for Mail to Print. For details about Mail to Print, see "Reception", Facsimile Reference.

7. A PDF file is printed via ftp. Personal authentication is performed using the user ID and password used for logging on via ftp. However, the user ID and password are not encrypted.

Reference

- p.221 "Specifying the Extended Security Functions"

If User Authentication is Specified

When user authentication (User Code Authentication, Basic Authentication, Windows Authentication, LDAP Authentication, or Integration Server Authentication) is set, the authentication screen is displayed. Unless a valid user name and password are entered, operations are not possible with the machine. Log on to operate the machine, and log off when you are finished operations. Be sure to log off to prevent unauthorized users from using the machine. When auto logout timer is specified, the machine automatically logs you off if you do not use the control panel within a given time. Additionally, you can authenticate using an external device. For details about using an external device for user authentication, see "Authentication Using an External Device".

Note

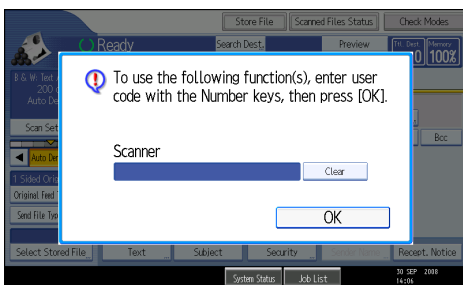
- Consult the User Administrator about your login user name, password, and user code.
- For user code authentication, enter a number registered in the Address Book as "User Code".
- The Auto Logout Timer can only be used under Basic Authentication, Windows Authentication, LDAP Authentication, or Integration Server Authentication.

Reference

- p.91 "Authentication Using an External Device"

If User Code Authentication is Specified

When User Code Authentication is set, the following screen appears.



Enter your user code.

Logging on Using the Control Panel

Use the following procedure to log in when User Code Authentication is enabled.

1. Enter a user code (up to 8 digits), and then press [OK].

When the authentication is successful, a screen showing the corresponding function is displayed.

Note

- To log off, do one of the following:
 - Press the Operation switch.
 - Press the [Energy Saver] key after jobs are completed.
 - Press the [Stop] key and the [Clear] key at the same time.

Logging on Using the Printer Driver

3

When User Code Authentication is set, specify a user code in printer properties on the printer driver. For details, see the printer driver Help.

If Basic, Windows, LDAP or Integration Server Authentication is Specified

When Basic Authentication, Windows Authentication, LDAP Authentication or Integration Server Authentication is set, the following screen appears.



Enter your login user name and password.

Logging on Using the Control Panel

Use the following procedure to log on if Basic Authentication, Windows Authentication, LDAP Authentication, or Integration Server Authentication is enabled.

1. Press [Login].
2. Enter the login user name, and then press [OK].
3. Enter the login password, and then press [OK].

The message, "Authenticating... Please wait." appears.

When the authentication is successful, a screen showing the corresponding function is displayed.

Logging off Using the Control Panel

Follow the procedure below to log off when Basic Authentication, Windows Authentication, LDAP Authentication, or Integration Server Authentication is set.

1. Press the **[Login/Logout]** key.
2. Press **[Yes]**.

The message, "Logging out... Please wait." appears.

↓ Note

- You can log off using the following procedures also.
 - Press the **[Power]** key.
 - Press the **[Energy Saver]** key.

Logging on Using the Printer Driver

When Basic Authentication, Windows Authentication, LDAP Authentication, or Integration Server Authentication is set, make encryption settings in printer properties on the printer driver, and then specify a login user name and password. For details, see the printer driver Help.

↓ Note

- When logged on using a printer driver, logging off is not required.

Logging on Using Web Image Monitor

This section explains how to log on to the machine via Web Image Monitor.

1. Click **[Login]** on the top page of Web Image Monitor.
2. Enter a login user name and password, and then click **[Login]**.

↓ Note

- For user code authentication, enter a user code in "Login User Name", and then click **[Login]**.

Logging off Using Web Image Monitor

1. Click **[Logout]** to log off.

↓ Note

- Delete the cache memory in Web Image Monitor after logging off.

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.

3

Lockout setting items

The lockout function settings can be made using Web Image Monitor.

Setting Item	Description	Setting Values	Default Setting
Lockout	Specify whether or not to enable the lockout function.	<ul style="list-style-type: none"> Active Inactive 	<ul style="list-style-type: none"> Inactive
Number of Attempts before Lockout	Specify the number of authentication attempts to allow before applying lockout.	1-10	5
Lockout Release Timer	Specify whether or not to cancel lockout after a specified period elapses.	<ul style="list-style-type: none"> Active Inactive 	<ul style="list-style-type: none"> Inactive
Lock Out User for	Specify the number of minutes after which lockout is canceled.	1-9999 min.	60 min.

Lockout release privileges

Administrators with unlocking privileges are as follows.

Locked out User	Unlocking administrator
general user	user administrator
user administrator, network administrator, file administrator, machine administrator	supervisor

Locked out User	Unlocking administrator
supervisor	machine administrator

Specifying the User Lockout Function

This can be specified by the machine administrator 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.

The top page of Web Image Monitor appears.

3. Click [Login].

The machine administrator can log on.

Enter the login user name and login password.

4. Click [Configuration], and then click [User Lockout Policy] under "Security".

The User Lockout Policy page appears.

5. Set "Lockout" to [Active].

6. In the drop down menu, select the number of login attempts to permit before applying lockout.

7. Set the "Lockout Release Timer" to [Active].

8. In the "Lock Out User for" field, enter the number of minutes until lockout is disabled.

9. Click [OK].

User Lockout Policy is set.

10. Click [Logout].

Unlocking a Locked User Account

A locked user account can be unlocked by the administrator or supervisor with unlocking privileges 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.

The top page of Web Image Monitor appears.

3. Click [Login].

The administrator or supervisor with unlocking privileges can log on.

Enter the login user name and login password.

4. Click [Address Book].

The Address Book page appears.

5. Select the locked out user's account.

6. Click [Change].

7. Set the "Lockout" to [Inactive] under "Authentication Information".

8. Click [OK].

9. Click [Logout].

3

Auto Logout

This can be specified by the machine administrator.

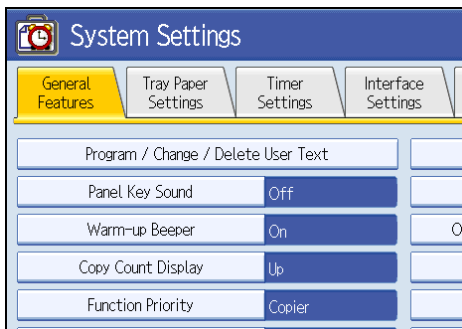
When using Basic Authentication, Windows Authentication, LDAP Authentication or Integration Server Authentication, the machine automatically logs you off if you do not use the control panel within a given time. This feature is called "Auto Logout". Specify how long the machine is to wait before performing Auto Logout.

For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

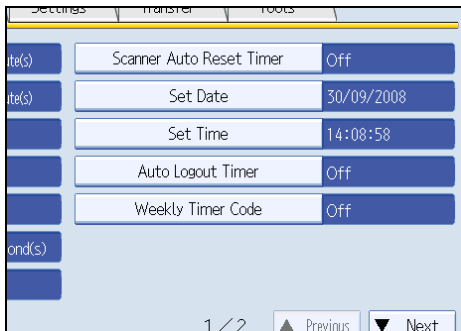
1. Press the [User Tools] key.

2. Press [System Settings].

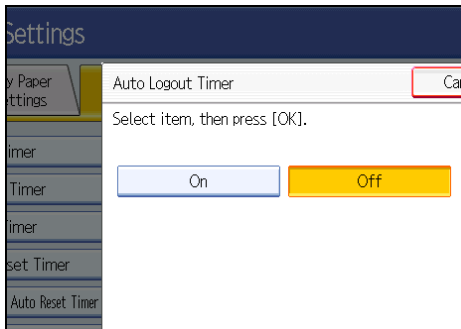
3. Press [Timer Settings].



4. Press [Auto Logout Timer].

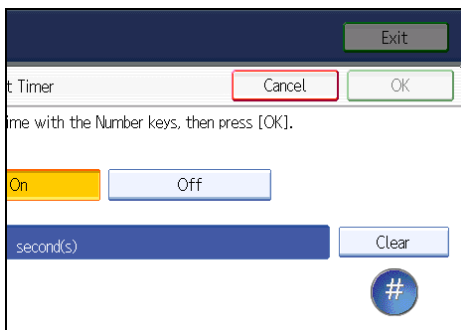


5. Select [On].



If you do not want to specify [Auto Logout Timer], select [Off].

6. Enter "60" to "999" (seconds) using the number keys, and then press [#].



7. Press the [User Tools] key.

A confirmation message appears.

If you press [Yes], you will be automatically logged off.

↓ Note

- If a paper jam occurs or a print cartridge runs out of ink, the machine might not be able to perform the Auto Logout function.

 **Reference**

- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"

Authentication Using an External Device

To authenticate using an external device, see the device manual.

For details, contact your sales representative.

4. Protecting Data from Information Leaks

This chapter describes how to protect document data.

Preventing Unauthorized 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 printer driver, specify the printer settings for unauthorized copy prevention. For details on how to specify settings for unauthorized copy prevention, see "Specifying Unauthorized Copy Prevention from the Printer Driver".

Data Security for Copying

1. Using the printer driver, specify the printer settings for data security for copying. For details on how to specify settings on the printer driver, see "Specifying Data Security for Copying from the Printer Driver".
2. Set the data security for copying function to appear gray when documents with the function are copied, scanned, or stored on the machine. For details on how to specify settings on the machine, see "Specifying Data Security for Copying Using the Control Panel".

Reference

- p.97 "Specifying Unauthorized Copy Prevention from the Printer Driver"
- p.97 "Specifying Data Security for Copying from the Printer Driver"
- p.97 "Specifying Data Security for Copying Using the Control Panel"

Unauthorized Copy Prevention

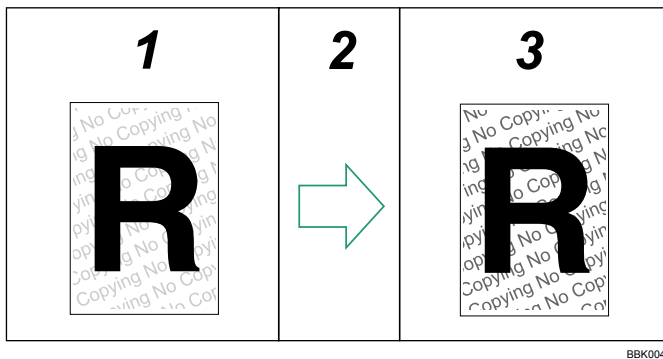
Using the printer driver, you can embed mask and pattern (for instance, a warning such as "No Copying") in the printed document.

If the document is copied, faxed, scanned, or stored in the Document Server by a copier or multifunction printer, the embedded pattern appears clearly on the copy, discouraging unauthorized copying.

To use the printer function when User Authentication is enabled, you must enter the login user name and password for the printer driver. For details, see the printer driver Help.

★ Important

- **Unauthorized copy prevention discourages unauthorized copying, but will not necessarily stop information leaks.**
- **The embedded pattern cannot be guaranteed to be copied, faxed, scanned, or stored properly in the Document Server.**
- **Depending on the machine and scanner settings, the embedded pattern may not be copied, faxed, scanned, or stored in the Document Server.**



1. Printed Documents

Using the printer driver, you can embed background images and pattern in a printed document for Unauthorized Copy Prevention.

2. The document is copied, faxed, scanned, or stored in the Document Server.

3. Printed Copies

The embedded pattern (for instance, a warning such as "No Copying") in a printed document appears clearly in printed copies.

↓ Note

- To make the embedded pattern clear, set the character size to at least 50 pt (preferably 70 to 80 pt) and character angle to between 30 and 40 degrees.

Data Security for Copying

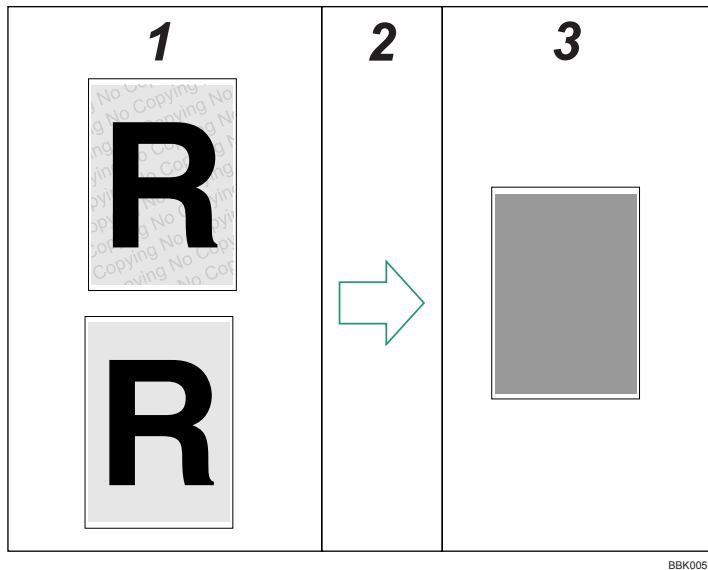
Using the printer driver to enable data security for copying, you can print a document with an embedded pattern of hidden text. This output method is called "data security for copying".

If a data security for copying document is copied or stored in the Document Server using a copier or multifunction printer with the Copy Data Security Unit, protected pages are grayed out in the copy, preventing

confidential information from being copied. Also if a document with embedded pattern is detected, the machine beeps. An unauthorized copy log is also stored. To gray out copies of data security for copying documents when they are copied, faxed, scanned, or stored in the Document Server, the optional Copy Data Security Unit must be installed in the machine.

★ Important

- If a document with embedded pattern for data security for copying is copied, faxed, scanned, or stored in the Document Server by a copier or multi-function printer without the Copy Data Security Unit, the embedded pattern appears conspicuously in the copy. However, character relief may differ depending on the copier or multifunction printer model in use or document scan setting.
- The machine does not beep with a data security for copying document is detected while using the network TWAIN scanner.



1. Documents with data security for copying
2. The document is copied, faxed, scanned, or stored in the Document Server.
3. Printed Copies

Text and images in the document are grayed out in printed copies.

↓ Note

- You can also embed pattern in a document protected by data security for copying. However, if such a document is copied or stored in the Document Server using a copier or multi-function printer with the Copy Data Security Unit, the copy is grayed out, so the embedded pattern does not appear on the copy.
- If misdetection occurs, contact your service representative.

- If a document with embedded pattern for data security for copying is copied, faxed, scanned, or stored in the Document Server using a copier or multi-function printer without the Copy Data Security Unit, the embedded pattern appears clearly on the copy.
- If a data security for copying document is detected, the machine beeps.
- If the scanned data security for copying document is registered as a user stamp, the machine does not beep. The file registered as a user stamp is grayed out, and no entry is added to the unauthorized copying log.

Printing Limitations

4

The following is a list of limitations on printing with unauthorized copy prevention and data security for copying.

Unauthorized copy prevention / Data security for copying

You can print using only the RPCS printer driver.

If you use this function when the resolution is set to less than 600 dpi, the resolution will be automatically increased to 600 dpi.

You cannot partially embed pattern in the printed document.

You can only embed pattern that is entered in the text box of the printer driver.

Printing with embedding takes longer than normal printing.

Data security for copying Only

Select 182 × 257 mm / 7.2 × 10.1 inches or larger as the paper size.

Select a paper type of Plain or Recycled with a brightness of 70% or more.

If you select Duplex, the data security for copying function may not work properly due to printing on the back of sheets.

Notice

1. The supplier does not guarantee that unauthorized copy prevention and data security for copying will always work. Depending on the paper, the model of the copier or multi-function printer, and the copier or printer settings, unauthorized copy prevention and data security for copying may not work properly.
2. The supplier is not liable for any damage caused by using or not being able to use unauthorized copy prevention and data security for copying.

Configuring Unauthorized Copy Prevention and Data Security for Copying

This section describes Printing with Unauthorized Copy Prevention and Data Security for Copying.

Specifying Unauthorized Copy Prevention from the Printer Driver

Using the printer driver, specify the printer settings for unauthorized copy prevention.

To use the printer function when User Authentication is enabled, you must enter the login user name and password for the printer driver. For details about logging on, see the printer driver Help.

For details about specifying data security for copying using the printer driver, see the printer driver Help.

1. **Open the printer driver dialog box.**
2. **Click [Add/Change Custom Settings].**
3. **On the Edit tab, select the "Unauthorized copy..." check box.**
4. **Click [Control Settings...].**
5. **In the text box in the [Unauthorized copy prevention: Text] group, enter the text to be embedded in the printed document.**

Also, specify [Font:], [Font style:], and Size.

6. **Click [OK].**

Specifying Data Security for Copying from the Printer Driver

If a printed document using this function is copied or stored in the Document Server by a copier or multi-function printer, the copy is grayed out.

Using the printer driver, specify the printer settings for data security for copying.

To use the printer function when User Authentication is enabled, you must enter the login user name and password for the printer driver. For details about logging on, see the printer driver Help.

For details about specifying data security for copying using the printer driver, see the printer driver Help.

1. **Open the printer driver dialog box.**
2. **Click [Add/Change Custom Settings].**
3. **On the Edit tab, select the "Unauthorized copy..." check box.**
4. **Click [Control Settings...].**
5. **Check the [Data security for copying] check box in the [Unauthorized copy prevention: Pattern] group.**
6. **Click [OK].**

Specifying Data Security for Copying Using the Control Panel

This can be specified by the machine administrator.

For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

To use this function, the Copy Data Security Unit must be installed.

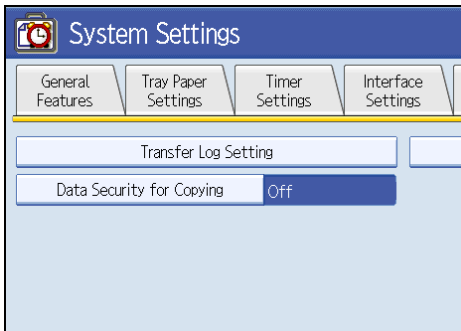
If a document printed is copied, faxed, scanned, or stored in the Document Server, the copy is grayed out.

★ Important

- If a document that is not copy-guarded is copied, faxed, scanned, or stored, the copy or stored file is not grayed out.

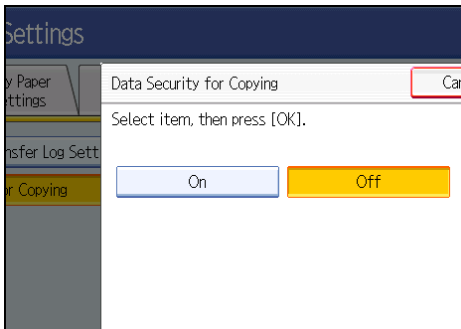
1. Press the [User Tools] key.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [Data Security for Copying].

4



If the setting you want to specify does not appear, press [▼Next] to scroll down to other settings.

5. Press [On].



If you do not want to specify "Data Security for Copying", select [Off].

6. Press [OK].
7. Press [Exit].
8. Press the [User Tools] key.

📖 Reference

- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"

Printing a Confidential Document

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.
- Confidential documents can be printed regardless of the User Authentication settings.

Note

- To store files temporarily, select [Stored Print] in the printer driver. If you select [Share stored print files] in [Job Type Details], you can also share these files.

4

Specifying Locked Print File

Using the printer driver, specify a Locked Print file.

If user authentication has been enabled, you must enter the login user name and login password using the printer driver. For details about logging on, see the printer driver Help.

Locked Print is allowed even if user authentication is not yet configured. For configuring this setting, see "Locked Print", Printer Reference.

Word Pad is used in this procedure.

1. **Open the printer driver dialog box.**
2. **Set "Job type" to [Locked Print] under the "Print Settings" tab.**
3. **Click [Details...].**
4. **Enter the user ID and password.**

Enter the user ID using up to 8 alphanumeric characters.

Enter the password using 4 to 8 numbers.

Enter the classification code using up to 32 alphanumeric characters.

Classification codes allow you to collate log files that show the number of pages printed under each code.

The password entered here lets you use the Locked Print function.

To print a Locked Print file, enter the same password on the control panel.

The password is encrypted during data transmission.

5. **Click [OK].**

A confirmation message appears.

6. Confirm the password by re-entering it.
7. Click [OK].
8. Print the locked document.

Printing a Locked Print File

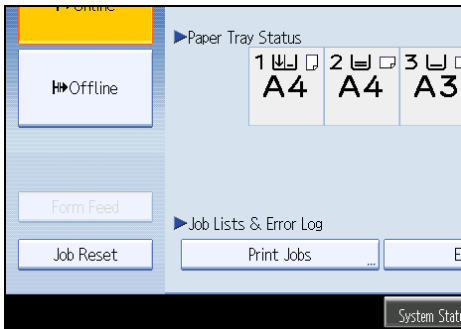
To print a Locked Print file, you must be at the machine and print the file using the control panel.

To print Locked Print files, the password is required. If you do not enter the correct password, you cannot print the files. The file administrator can change the user password if it is forgotten.

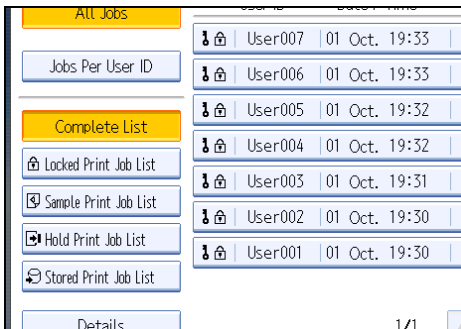
For details about logging on and logging off with user authentication, see "If User Authentication is Specified".

This can also be specified via Web Image Monitor. For details, see Web Image Monitor Help.

1. Press the [Printer] key.
2. Press [Print Jobs].



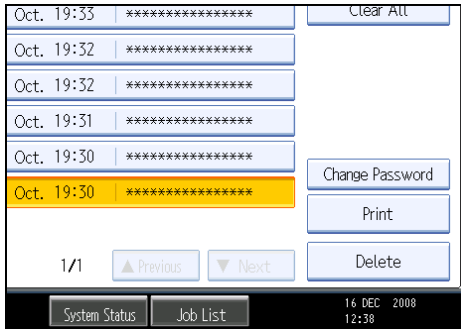
3. Press [Locked Print Job List].



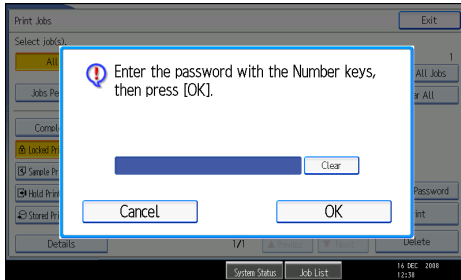
Only Locked Print files belonging to the user who has logged on appear.

4. Select the Locked Print file to print.

5. Press [Print].



6. Enter the password for the stored file, and then press [OK].



Enter the password specified in step 4 of "Specifying a Locked Print File".

7. Press [Yes].

Reference

- p.83 "If User Authentication is Specified"

Deleting Locked Print Files

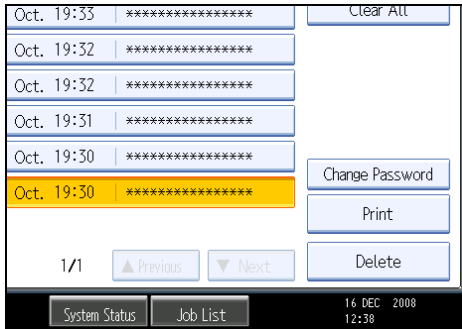
This can be specified by the file creator (owner).

To delete Locked Print files, you must enter the password for the files. If the password has been forgotten, ask the file administrator to change the password.

This can also be specified via Web Image Monitor. For details, see Web Image Monitor Help.

- 1. Press the [Printer] key.**
- 2. Press [Print Jobs].**
- 3. Press [Locked Print Job List].**
- 4. Select the file.**

5. Press [Delete].



6. 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 on.

7. Press [Yes].

Note

- Locked Print files can also be deleted by the file administrator.

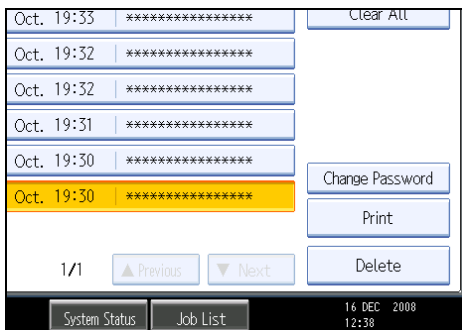
Changing the Password of a Locked Print File

This can be specified by the file creator (owner) or file administrator.

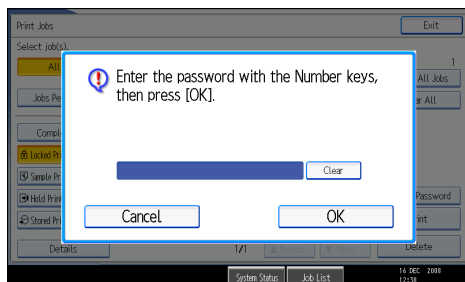
If the password has been forgotten, the file administrator changes the password to restore access.

This can also be specified via Web Image Monitor. For details, see Web Image Monitor Help.

1. Press the [Printer] key.
2. Press [Print Jobs].
3. Press [Locked Print Job List].
4. Select the file.
5. Press [Change Password].

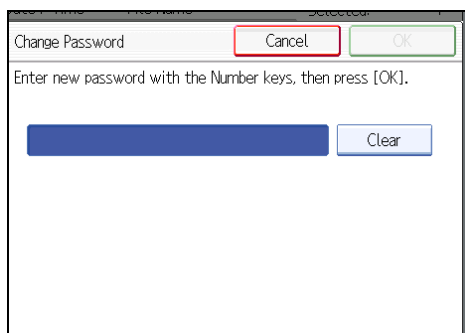


6. Enter the password for the stored file, and then press [OK].



The file administrator does not need to enter the password.

7. Enter the new password for the stored file, and then press [OK].



8. If a password reentry screen appears, enter the login password, and then press [OK].

The password entry screen does not appear if the file administrator is logged on.

Unlocking a Locked Print File

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 "Specifying the Extended Security Functions".

Only the file administrator can unlock files. For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

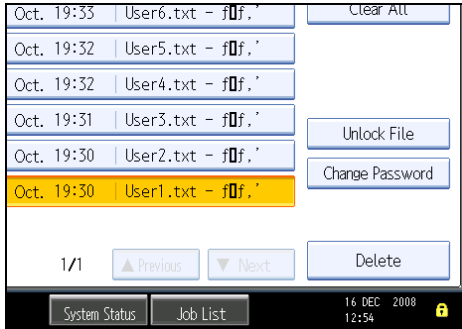
This can also be specified via Web Image Monitor. For details, see Web Image Monitor Help.

1. Press the [Printer] key.
2. Press [Print Jobs].
3. Press [Locked Print Job List].

4. Select the file.

The  icon appears next to a file locked by the Enhance File Protection function.

5. Press [Unlock File].



4

6. Press [Yes].

The  icon disappears.

Note

- You can use the same procedure to unlock stored print files also.

Reference

- p.221 "Specifying the Extended Security Functions"
- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"

Configuring Access Permissions for Stored Files

This section describes Specifying Access Permission for Stored Files.

You can specify who is allowed to access stored scan files and files stored in the 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.

Access Permission

To limit the use of stored files, you can specify four types of access permissions.

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.

4

Note

- For details about assigning a password to a stored file, see "Specifying Passwords for Stored Files".
- Files can be stored by any user who is allowed to use the Document Server, copy function, scanner function or fax function.
- Using Web Image Monitor, you can check the content of stored files. For details, see Web Image Monitor Help.
- Access permission to documents sent from the printer driver and stored on the machine can only be set on Web Image Monitor.
- The default access permission for the file creator (owner) is "Read-only". You can also specify the access permission.

Password for Stored Files

- Passwords for stored files can be specified by the file creator (owner) or file administrator.
- You can obtain greater protection against the unauthorized use of files.
- Even if User Authentication is not set, passwords for stored files can be set.

Reference

- p.114 "Specifying Passwords for Stored Files"

Specifying User and Access Permissions for Stored Files

This can be specified by the file creator (owner) or file administrator.

Specify the users and their access permissions for each stored file.

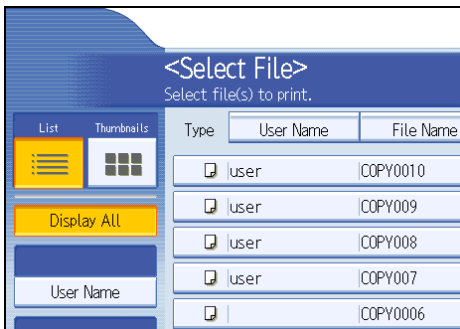
By making this setting, only users granted access permission can access stored files.

For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

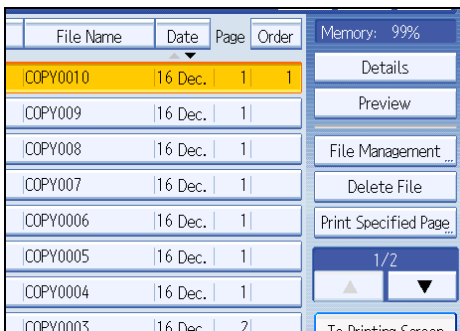
★ Important

- 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).

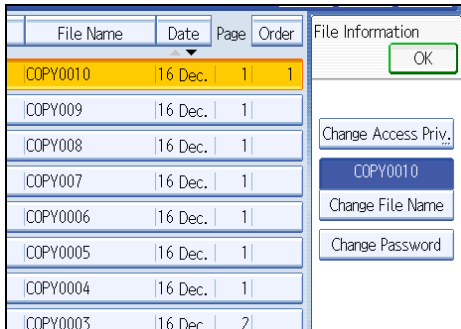
1. Press the [Document Server] key.
2. Select the file.



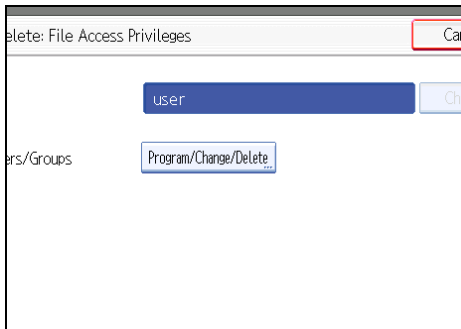
3. Press [File Management].



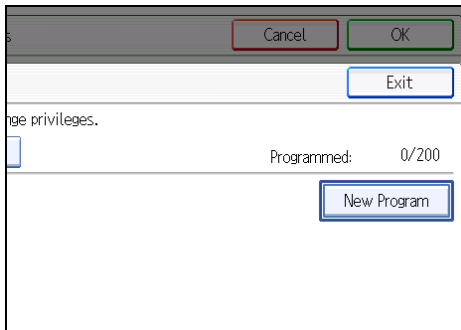
4. Press [Change Access Priv.].



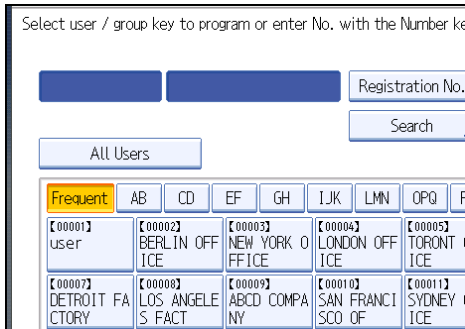
5. Press [Program/Change/Delete].



6. Press [New Program].



7. Select the users or groups you want to assign permission to.

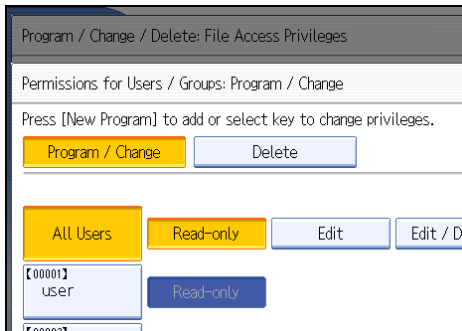


You can select more than one user.

By pressing [All Users], you can select all the users.

8. Press [Exit].

9. Select the user who you want to assign access permission to, and then select the permission.



Select the access permission from [Read-only], [Edit], [Edit / Delete], or [Full Control].

10. Press [Exit].

11. Press [OK].

Reference

- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"

Specifying Access Permissions for Files Stored Using the Scanner and Fax Functions

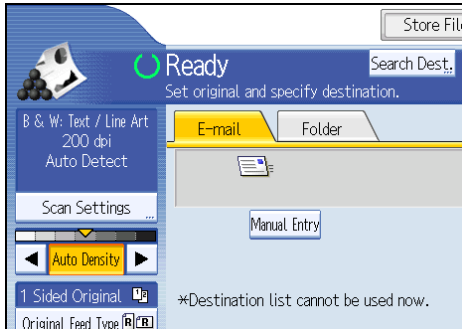
If user authentication is set for the scanner function, you can specify access privileges for stored files when storing them in the Document Server. You can also change the access privileges for the file.

Specifying Access Permissions When Storing a File

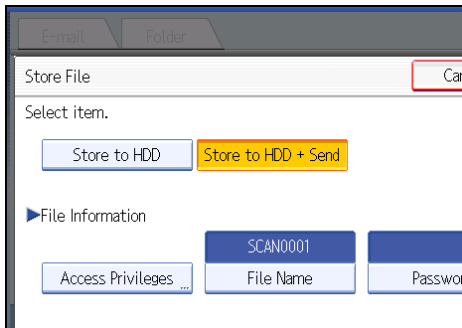
This section explains how to specify the access privileges and then store a file in the Document Server under the scanner or fax function.

The scanner screen is used to illustrate the procedure.

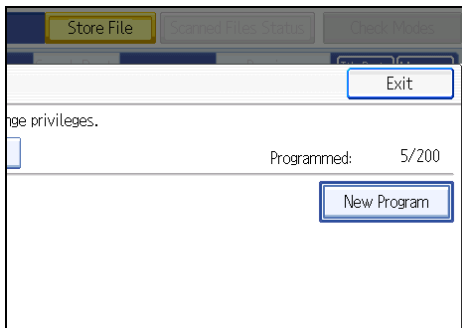
1. Press [Store File].



2. Press [Access Privileges].



3. Press [New Program].



4. Select the users or groups you want to assign permission to.

You can select more than one user.

By pressing [All Users], you can select all the users.

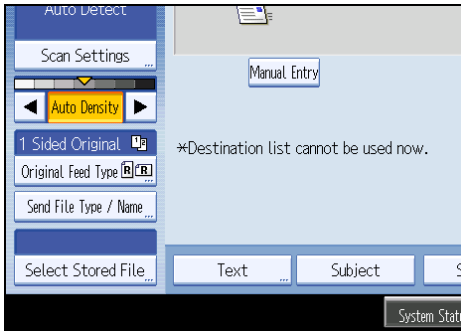
5. Press [Exit].
6. Select the user who you want to assign access permission to, and then select the permission.
Select the access permission from [Read-only], [Edit], [Edit / Delete], or [Full Control].
7. Press [Exit].
8. Press [OK].
9. Store files in the Document Server.

Specifying Access Permissions for Stored Files

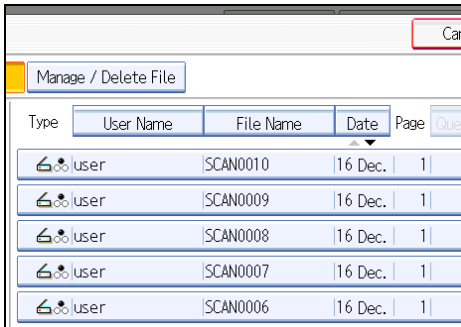
This section explains how to change access privileges for a file stored in the Document Server under the scanner or fax function.

4

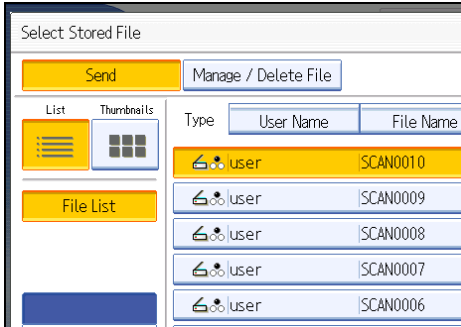
1. Press [Select Stored File].



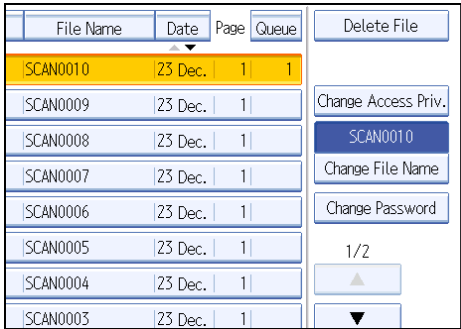
2. Select the file.



3. Press [Manage / Delete File].

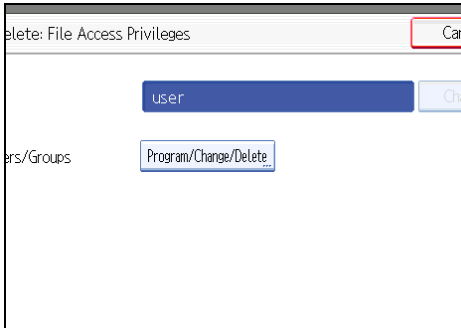


4. Press [Change Access Priv.].

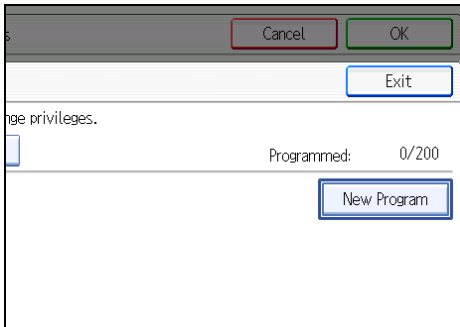


4

5. Press [Program/Change/Delete].



6. Press [New Program].



7. Select the users or groups you want to assign permission to.

You can select more than one user.

By pressing [All Users], you can select all the users.

8. Press [Exit].

9. Select the user who you want to assign access permission to, and then select the permission.

Select the access permission from [Read-only], [Edit], [Edit / Delete], or [Full Control].

10. Press [Exit].

11. Press [OK].

4

Specifying User and Access Permissions for Files Stored by a Particular User

This can be specified by the file creator (owner) or user administrator.

Specify the users and their access permission to files stored by a particular user.

Only those users granted access permission can access stored files.

This makes managing access permission easier than specifying and managing access permissions for each stored file.

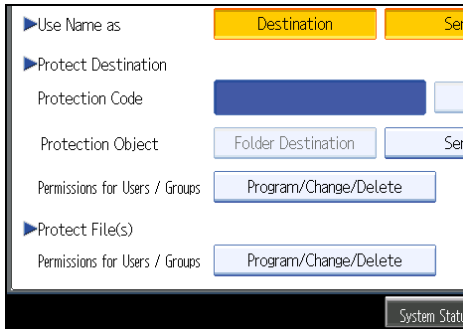
For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

★ Important

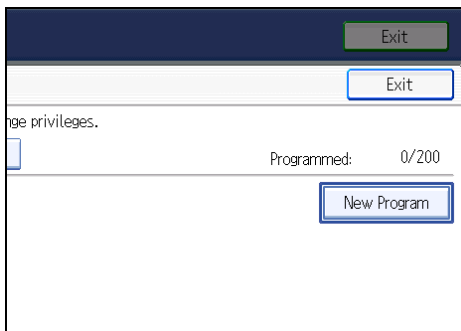
- If files become inaccessible, be sure to enable the user administrator, so that the user administrator can reset the access permission for the files in question.

1. Press the [User Tools] key.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [Address Book Management].

5. Select the user or group.
6. Press [Protection].
7. Under "Protect File(s)", press [Program/Change/Delete] for "Permissions for Users/Groups".



8. Press [New Program].



9. Select the users or groups to register.
You can select more than one user.
By pressing [All Users], you can select all the users.
10. Press [Exit].
11. Select the user who you want to assign access permission to, and then select the permission.
Select the access permission from [Read-only], [Edit], [Edit / Delete], or [Full Control].
12. Press [Exit].
13. Press [OK].
14. Press [Exit].
15. Press the [User Tools] key.

Reference

- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"

Specifying Passwords for Stored Files

This can be specified by the file creator (owner) or file administrator.

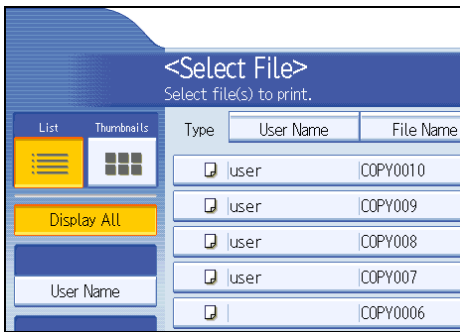
Specify passwords for stored files.

This provides increased protection against unauthorized use of files.

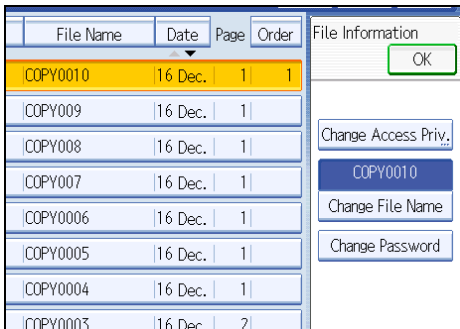
For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".


1. Press the [Document Server] key.
2. Select the file.

4



3. Press [File Management].
4. Press [Change Password].



5. Enter the password using the number keys.
You can use 4 to 8 numbers as the password for the stored file.
6. Press [OK].
7. Confirm the password by re-entering it using the number keys.
8. Press [OK].
The  icon appears next to a stored file protected by password.
9. Press [OK].

Reference

- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"

Unlocking 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.

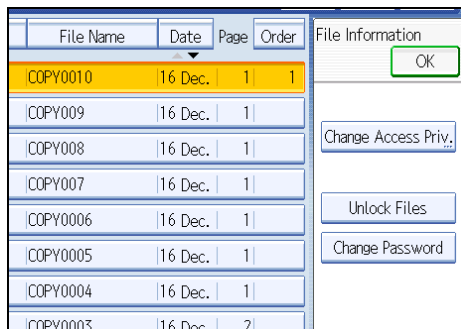
"Enhance File Protection" is one of the extended security functions. For details about this and other extended security functions, see "Specifying the Extended Security Functions".

Only the file administrator can unlock files.

For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

1. Press the [Document Server] key.
2. Select the file.
3. Press [File Management].
4. Press [Unlock Files].

The  icon appears next to a file locked by the Enhance File Protection function.



5. Press [Yes].

The  icon changes to the  icon.

6. Press [OK].

Reference

- p.221 "Specifying the Extended Security Functions"
- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"

5. Securing Information Sent over the Network or Stored on Hard Disk

This chapter describes how to protect information transmitted through the network or stored on the hard disk from unauthorized viewing and modification.

Preventing Information Leakage Due to Unauthorized Transmission

This section describes Preventing Data Leaks Due to Unauthorized Transmission.

If user authentication is specified, the user who has logged on will be designated as the sender to prevent data from being sent by an unauthorized person masquerading as the user.

You can also limit the direct entry of destinations to prevent files from being sent to destinations not registered in the Address Book.

5

Restricting Destinations

This can be specified by the user administrator.

Make the setting to disable the direct entry of e-mail addresses under the scanner and fax functions.

By making this setting, the destinations are restricted to addresses registered in the Address Book.

If you set "Restrict Use of Destinations" to [On], you can prohibit users from directly entering e-mail addresses, or Folder Path in order to send files. If you set "Restrict Use of Destinations" to [Off], "Restrict Adding of User Destinations" appears. In "Restrict Adding of User Destinations", you can restrict users from registering data in the Address Book.

If you set "Restrict Adding of User Destinations" to [Off], users can directly enter e-mail addresses, and Folder Path in "Prg. Dest." on the fax and scanner screens. If you set "Restrict Adding of User Destinations" to [On], users can specify destinations directly, but cannot use "Prg. Dest." to register data in the Address Book. When this setting is made, only the user administrator can change the Address Book. "Restrict Use of Destinations" and "Restrict Adding of User Destinations" are extended security functions. For more information about these and the extended security functions, see "Specifying the Extended Security Functions".

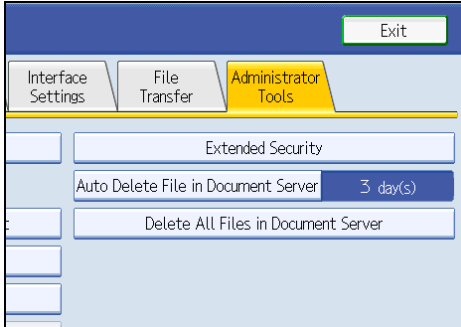
"Restricting Destinations" can also be specified using Web Image Monitor or SmartDeviceMonitor for Admin. For details, see the Help for these applications.

For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

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

3. Press [Administrator Tools].

4. Press [Extended Security].

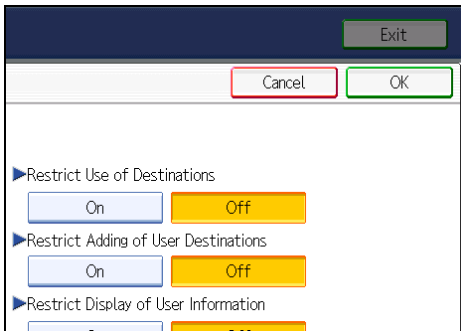


If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

5. Press [On] for "Restrict Use of Destinations".

If "Restrict Use of Destinations" is set to [On], "Restrict Adding of User Destinations" does not appear.

5



6. Press [OK].

7. Press the [User Tools] key.

Reference

- p.221 "Specifying the Extended Security Functions"
- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"

Using S/MIME to Protect E-mail Transmission

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.

For details about using S/MIME with the scanner function, see "Security Settings to E-mails", Scanner Reference.

For details about using S/MIME with the fax function, see "Internet Fax Transmission" or "E-mail Transmission", or "Folder Transmission", Facsimile Reference.

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
- Netscape Messenger 7.1 and later
- Lotus Notes R5 and later

★ Important

- To use S/MIME, you must first specify "Administrator's E-mail Address" in [System Settings].

↓ Note

- If an electronic signature is specified for an e-mail, the administrator's address appears in the "From" field and the address of the user specified as "sender" appears in the "Reply To" field.
- When 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.

E-mail Encryption

To send encrypted e-mail using S/MIME, the user certificate must first be prepared using Web Image Monitor and registered in the Address Book by the user administrator. Registering the certificate in the Address Book specifies each user's public key. After installing the certificate, specify the encryption algorithm using Web Image Monitor. The network administrator can specify the algorithm.

E-mail Encryption

1. Prepare the user certificate.

2. Install the user certificate in the Address Book using Web Image Monitor. (The public key on the certificate is specified in the Address Book.)
3. Specify the encryption algorithm using Web Image Monitor.
4. Using the shared key, encrypt the e-mail message.
5. The shared key is encrypted using the user's public key.
6. The encrypted e-mail is sent.
7. The receiver decrypts the shared key using a secret key that corresponds to the public key.
8. The e-mail is decrypted using the shared key.

Note

- There are three types of user certificates that can be installed on this machine, "DER encoded binary X.509", "Base 64 encoded X.509", and "PKCS #7 certificate".
- When installing a user certificate to the Address Book using Web Image Monitor, you might see an error message if the certificate file contains more than one certificate. If this error message appears, install the certificates one at a time.

5

Specifying the User Certificate

This can be specified by the user administrator.

Each user certificate must be prepared in advance.

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.

The top page of Web Image Monitor appears.

3. Click [Login].

The user administrator can log on.

Enter the login user name and login password.

4. Click [Address Book].

The Address Book page appears.

5. Select the user for whom the certificate will be installed, and then click [Change].

The Change User Information screen appears.

6. Enter the user address in the "E-mail Address" field under "E-mail".

7. Click [Change] in "User Certificate".

8. Click [Browse], select the user certificate file, and then click [Open].

9. Click [OK].

The user certificate is installed.

10. Click [OK].**11. Click [Logout].**

Specifying the Encryption Algorithm

This can be specified by the network administrator.

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.

The top page of Web Image Monitor appears.

3. Click [Login].

The network administrator can log on.

Enter the login user name and login password.

4. Click [Configuration], and then click [S/MIME] under "Security".

The S/MIME settings page appears.

5. Select the encryption algorithm from the drop down menu next to "Encryption Algorithm" under "Encryption".**6. Click [OK].**

The algorithm for S/MIME is set.

7. Click [Logout].

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.

★ Important

- To install an S/MIME device certificate, you must first register "Administrator's E-mail Address" in [System Settings] as the e-mail address for the device certificate. Note that even if you will not be using S/MIME, you must still specify an e-mail address for the S/MIME device certificate.

Electronic Signature

1. Install a device certificate on the machine. (The secret key on the certificate is configured on the machine.)
2. Attach the electronic signature to an e-mail using the secret key provided by the device certificate.
3. Send the e-mail with the electronic signature attached to the user.
4. The receiver requests the public key and device certificate from the machine.
5. Using the public key, you can determine the authenticity of the attached electronic signature to see if the message has been altered.

Configuration flow (self-signed certificate)

1. Creating and installing the device certificate.
Create and install the device certificate using Web Image Monitor.
2. Make certificate settings.
Make settings for the certificate to be used for S/MIME using Web Image Monitor.
3. Make electronic signature settings.
Make settings for the electronic signature using Web Image Monitor.

Configuration flow (certificate issued by a certificate authority)

1. Create the device certificate.
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.
Install the device certificate using Web Image Monitor.
3. Make certificate settings.
Make settings for the certificate to be used for S/MIME using Web Image Monitor.
4. Make electronic signature settings.
Make settings for the electronic signature using Web Image Monitor.

Creating and Installing the Self-Signed Certificate

This can be specified by the network administrator.

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. **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.

The top page of Web Image Monitor appears.

3. Click [Login].

The network administrator can log on.

Enter the login user name and login password.

4. Click [Configuration], and then click [Device Certificate] under "Security".**5. Check the radio button next to the number of the certificate you want to create.****6. Click [Create].****7. Make the necessary settings.****8. Click [OK].**

The setting is changed.

9. Click [OK].

A security warning dialog box appears.

10. Check the details, and then click [OK].

"Installed" appears under "Certificate Status" to show that a device certificate for the printer has been installed.

11. Click [Logout].**↓ Note**

- Click [Delete] to delete the device certificate from the machine.

Creating the Device Certificate (Issued by a Certificate Authority)

This can be specified by the network administrator.

Create the device certificate using Web Image Monitor. For details about the displayed and selectable items and settings, see Web Image Monitor Help.

Use this procedure to create a device certificate issued by a certificate authority.

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.

The top page of Web Image Monitor appears.

3. Click [Login].

The network administrator can log on.

Enter the login user name and login password.

4. Click [Configuration], and then click [Device Certificate] under "Security".

The Device Certificate page appears.

5. Check the radio button next to the number of the certificate you want to request.

6. Click [Request].

7. Make the necessary settings.

8. Click [OK].

9. Click [OK].

"Requesting" appears for "Certificate Status".

10. Click [Logout].

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

The application procedure depends on the certificate authority. For details, contact the certificate authority.

For application details, click the Web Image Monitor Details icon and use the information shown in "Certificate Details".

5

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)

This can be specified by the network administrator.

Install the device certificate using Web Image Monitor. For details about displayed and selectable items and settings, see Web Image Monitor Help.

Use this procedure to install a server certificate issued by a certificate authority.

Enter the details of the device certificate issued by the certificate authority.

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.

The top page of Web Image Monitor appears.

3. Click [Login].

The network administrator can log on.

Enter the login user name and login password.

4. Click [Configuration], and then click [Device Certificate] under "Security".

The Device Certificate page appears.

5. Check the radio button next to the number of the certificate you want to install.**6. Click [Install].****7. Enter the details of the device certificate.**

In the Certificate Request box, enter the details of the device certificate received from the certificate authority.

8. Click [OK].**9. Click [OK].**

"Installed" appears under "Certificate Status" to show that a device certificate for the machine has been installed.

10. Click [Logout].

5

Selecting the Device Certificate

This can be specified by the network administrator.

Select the device certificate to be used for S/MIME 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.

The top page of Web Image Monitor appears.

3. Click [Login].

The network administrator can log on.

Enter the login user name and login password.

4. Click [Configuration], and then click [Device Certificate] under "Security".

The Device Certificate page appears.

5. Select the certificate to be used for the electronic signature from the drop down box in "S/MIME" under "Certification".**6. Click [OK].**

The certificate to be used for the S/MIME electronic signature is set.

7. Click [OK].

8. Click [Logout].

Specifying the Electronic Signature

This can be specified by the network administrator.

After installing the device certificate on the machine, configure the electronic signature using Web Image Monitor. 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. **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.

The top page of Web Image Monitor appears.

3. **Click [Login].**

The network administrator can log on.

Enter the login user name and login password.

4. **Click [Configuration], and then click [S/MIME] under "Security".**

The S/MIME settings page appears.

5. **Select the digest algorithm to be used in the electronic signature next to "Digest Algorithm" under "Signature".**
6. **Select the method for attaching the electronic signature when sending e-mail from the scanner next to "When Sending E-mail by Scanner" under "Signature".**
7. **Select the method for attaching the electronic signature when forwarding received fax messages in "When Transferring by Fax" under "Signature".**
8. **Select the method for attaching the electronic signature when forwarding stored documents next to "When Transferring Files Stored in Document Server (Utility)" under "Signature".**
9. **Click [OK].**

The settings for the S/MIME electronic signature are enabled.
10. **Click [Logout].**

Protecting the Address Book

If user authentication is specified, the user who has logged on will be designated as the sender to prevent data from being sent by an unauthorized person masquerading as the user.

To protect the data from unauthorized reading, you can also encrypt the data in the Address Book.

Configuring Address Book Access Permissions

This can be specified by the registered user.

Access permission can also be specified by a user granted full control or the user administrator.

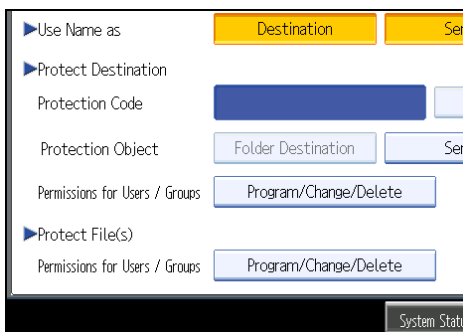
You can specify who is allowed to access the data in the Address Book.

By making this setting, you can prevent the data in the Address Book being used by unregistered users.

For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

5

1. Press the [User Tools] key.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [Address Book Management].
5. Select the user or group.
6. Press [Protection].
7. Press [Program/Change/Delete] for "Permissions for Users/Groups", under "Protect Destination".



8. Press [New Program].
9. Select the users or groups to register.

You can select more than one user.

By pressing [All Users], you can select all the users.

10. Press [Exit].
11. Select the user who you want to assign access permission to, and then select the permission.
Select the permission, from [Read-only], [Edit], [Edit / Delete], or [Full Control].
12. Press [Exit].
13. Press [OK].
14. Press [Exit].
15. Press the [User Tools] key.

Reference

- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"

5

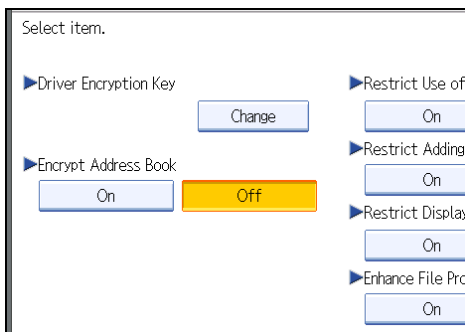
Encrypting Data in the Address Book

This can be specified by the user administrator.

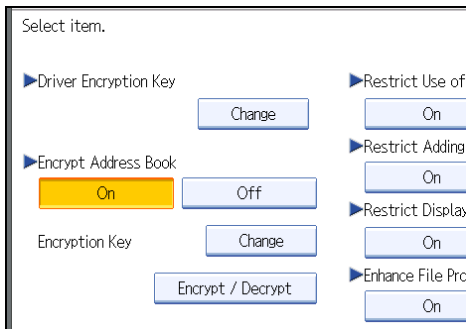
You can encrypt the data in the Address Book using the extended security function, "Encrypt Address Book". For details about this and other extended security functions, see "Specifying the Extended Security Functions".

For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

1. Press the [User Tools] key.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [Extended Security].
If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.
5. Press [On] for "Encrypt Address Book".



6. Press [Change] for "Encryption Key".

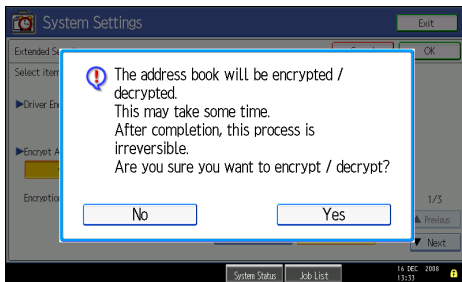


7. Enter the encryption key, and then press [OK].

Enter the encryption key using up to 32 alphanumeric characters.

8. Press [Encrypt / Decrypt].

9. 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.

10. Press [Exit].

11. Press [OK].

12. Press the [User Tools] key.

↓ Note

- If you register additional users after encrypting the data in the Address Book, those users are also encrypted.

 **Reference**

- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"
- p.221 "Specifying the Extended Security Functions"

Encrypting Data on the Hard Disk

This can be specified by the machine administrator.

For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

In order to use this function, the HDD Encryption Unit option is required.

Prevent information leakage by encrypting the Address Book, authentication information, and stored documents as the data is written. In addition, if the machine malfunctions or needs to be replaced, your service representative can easily transfer existing data to a new machine.

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 the document server
- Temporary stored documents
- Logs
- Network I/F setting information
- System settings information

Reference

- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"

Enabling the Encryption Settings

Use the following procedure to enable the encryption settings at initial set up, or after encryption settings have been canceled and settings must be made again.

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.
- Encryption begins after you have completed the control panel procedure and rebooted the machine using the [Stand by] - [On] function. If there is unencrypted data on the hard disk that must be both

transferred and encrypted, rebooting will take about three and a half hours. If there is encrypted data on the hard disk that must be re-encrypted, rebooting will also take about three and a half hours. 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 using the [Stand by] - [On] procedure.

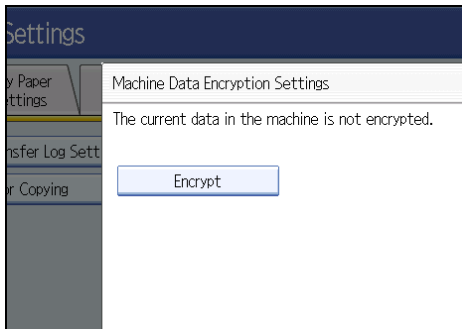
- If you want to specify encryption of unencrypted data with erase-by-overwrite, select [Random Numbers] as the overwrite method, and set the number of overwrites to "3". The entire process will take about six hours. If you specify re-encryption of encrypted data, the entire process will also take about six hours.
- 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 the document server.

5

1. Press the [User Tools] key.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [Machine Data Encryption Settings].

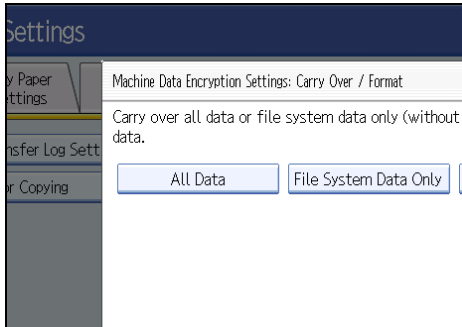
If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

5. Press [Encrypt].



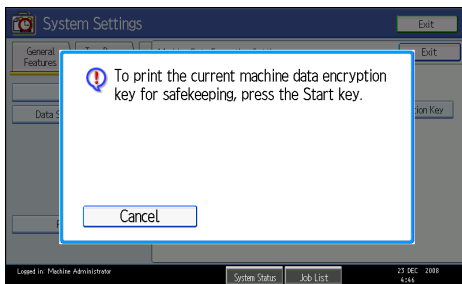
6. Select the data to be carried over to the hard disk and not be reset.

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].



7. Press the [Start] key.

The encryption key for backup data is printed.



8. Press [OK].



9. Press [Exit].

10. Press [Exit].

11. Press the [User Tools] key.

12. Turn off the power and the main power switch, and then turn the main power switch back on.

For details about turning off the power, see "Turning On the Power", About This Machine.

Printing the Encryption Key

Use the following procedure to print the key again if it has been lost or misplaced.

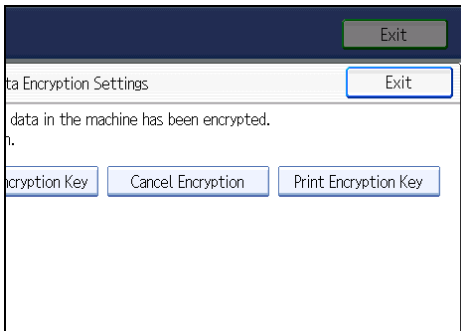
★ Important

- 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. Press the [User Tools] key.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [Machine Data Encryption Settings].

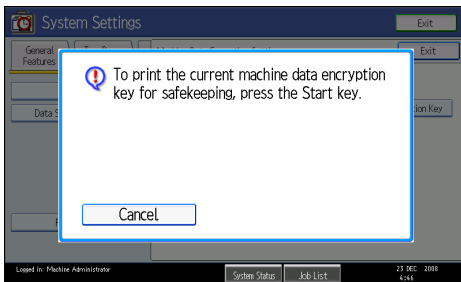
If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

5. Press [Print Encryption Key].



6. Press the [Start] key.

The encryption key for retrieving backup data is printed.



7. Press [Exit].

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

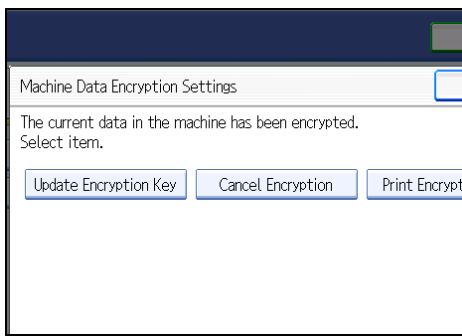
- The encryption key is required for recovery if the machine malfunctions. Be sure to store the encryption key safely for retrieving backup data.

- 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.

1. Press the [User Tools] key.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [Machine Data Encryption Settings].

If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

5. Press [Update Encryption Key].



6. 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].

7. Press the [Start] key.

The encryption key for retrieving the backup data is printed.

8. Press [OK].



9. Press [Exit].
10. Press [Exit].
11. Press the [User Tools] key.

12. Turn off the power and the main power switch, and then turn the main power switch back on.

For details about turning off the power, see "Turning On the Power", About This Machine.

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.
- Before disposing of a hard disk, note that even if [Format All Data] is selected and encryption is canceled, data stored on the hard disk is not erased.

5

1. Press the [User Tools] key.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [Machine Data Encryption Settings].
If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.
5. Press [Cancel Encryption].
6. 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].
7. Press [OK].
8. Press [Exit].
9. Press [Exit].
10. Press the [User Tools] key.
11. Turn off the power and the main power switch, and then turn the main power switch back on.

For details about turning off the power, see "Turning On the Power", About This Machine.

Deleting Data on the Hard Disk

This can be specified by the machine administrator.

To use this function, the optional DataOverwriteSecurity Unit must be installed.

The machine's hard disk stores all document data from the copier, printer and scanner functions. It also stores the data of users' document servers 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.

Auto Erase Memory

5

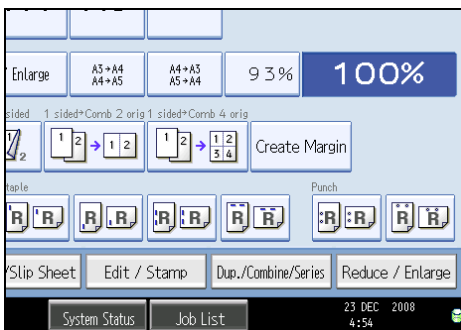
A document scanned in copier, or scanner mode, or print data sent from a printer driver is temporarily stored on the machine's hard disk. Even after the job is completed, it remains in the hard disk as temporary data. Auto Erase Memory erases the temporary data on the hard disk by writing over it.



Overwriting starts automatically once the job is completed.

The copier, fax and printer functions take priority over the Auto Erase Memory function. If a copy, fax or print job is in progress, overwriting will only be done after the job is completed.

Overwrite Icon

If this option has been correctly installed and is functioning properly, the Data Overwrite icon will be indicated in the bottom right hand corner of the panel display of your machine when Auto Erase Memory is set to [On].



	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.

5

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. It 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. The default is 3 times.

↓ Note

- Default: Random Numbers
- NSA stands for "National Security Agency", U.S.A.
- DoD stands for "Department of Defense", U.S.A.

Using Auto Erase Memory

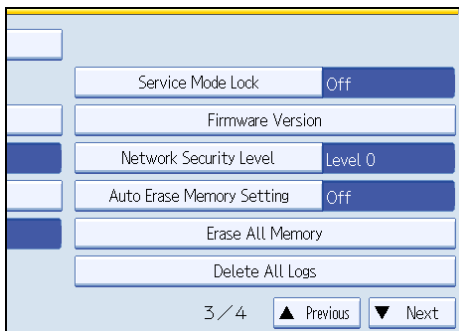
This can be specified by the machine administrator.

For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

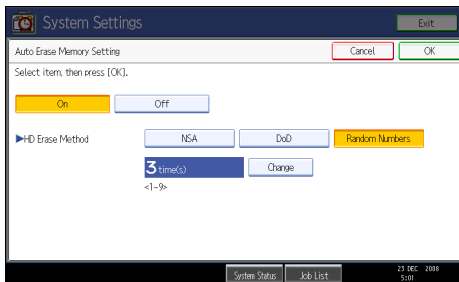
★ Important

- 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.

1. Press the [User Tools] key.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [▼Next] repeatedly until [Auto Erase Memory Setting] appears.
5. Press [Auto Erase Memory Setting].



6. Press [On].
7. Select the method of overwriting.



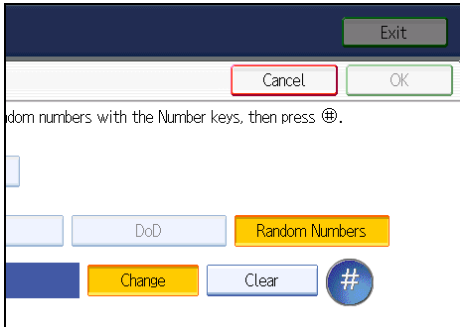
If you select [NSA] or [DoD], proceed to step 10.

If you select [Random Numbers], proceed to step 8.

For details about the methods of overwriting, see "Methods of Overwriting".

8. Press [Change].

9. Enter the number of times that you want to overwrite using the number keys, and then press [#].



10. Press [OK].

Auto Erase Memory is set.

5

↓ **Note**

- If the main power switch is turned to [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 to [Off] before Auto Erase Memory is completed, overwriting will continue once the main power switch is turned back to [On].
- If an error occurs before overwriting is completed, turn off the main power. Turn it on, and then repeat from step 1.
- If you specify to both overwrite and encrypt the data, the data will all be encrypted.

📖 **Reference**

- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"
- p.138 "Methods of Overwriting"

Canceling Auto Erase Memory

This can be specified by the machine administrator.

For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

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".

Reference

- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"

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
- PDF Direct Print data

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

Data scanned with network TWAIN scanner will not be overwritten by Auto Erase Memory.

Data Not Overwritten by Auto Erase Memory

- Documents stored by the user in the 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 the Document Server.
- Information registered in the Address Book

Data stored in the Address Book can be encrypted for security. For details, see "Protecting the Address Book".

- Counters stored under each user code

Reference

- p.127 "Protecting the Address Book"

Erase All Memory

This can be specified by the machine administrator.

For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

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.

5

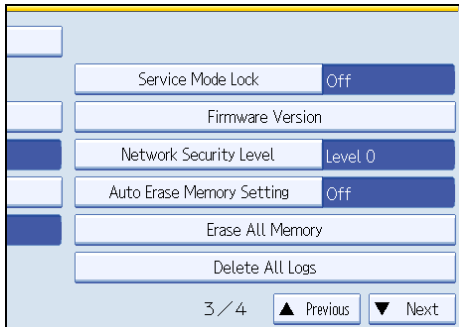
Important

- If you select "Erase All Memory", the following are also deleted: user codes, counters under each user code, user stamps, data stored in the Address Book, printer fonts downloaded by users, applications using Embedded Software Architecture, SSL server certificates, and the machine's network settings.
- If the main power switch is turned to [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.
- Before erasing the hard disk, you can back up user codes, counters for each user code, and Address Book data using SmartDeviceMonitor for Admin. For details, see SmartDeviceMonitor for Admin Help.
- Other than pausing, no operations are possible during the "Erase All Memory" process. If [Random Numbers] is specified and the number of overwrites set to "3", the erase process will take about two and a half hours.

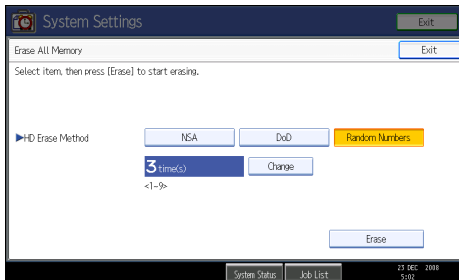
Using Erase All Memory

1. Disconnect communication cables connected to the machine.
2. Press the [User Tools] key.
3. Press [System Settings].
4. Press [Administrator Tools].
5. Press [▼Next] repeatedly until [Erase All Memory] appears.

6. Press [Erase All Memory].



7. Select the method of overwriting.



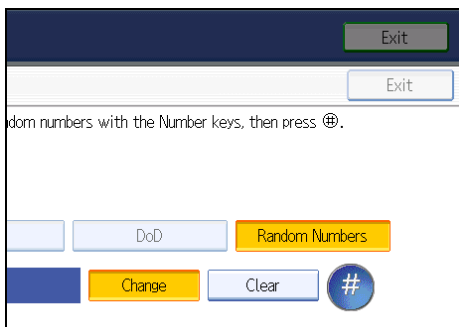
If you select [NSA] or [DoD], proceed to step 10.

If you select [Random Numbers], proceed to step 8.

For details about the methods of overwriting, see "Methods of Overwriting".

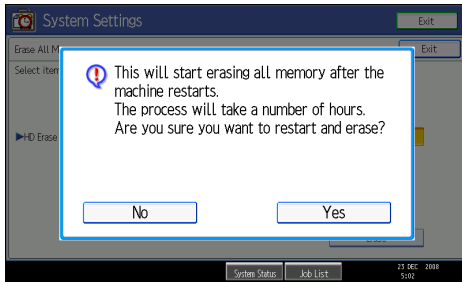
8. Press [Change].

9. Enter the number of times that you want to overwrite using the number keys, and then press [#].



10. Press [Erase].

11. Press [Yes].



12. When overwriting is completed, press [Exit], and then turn off the main power.

Before turning the power off, see "Turning On the Power", About This Machine.

Note

- Should the main power switch be turned to [Off] before "Erase All Memory" is completed, overwriting will continue once the main power switch is turned back to [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.

Reference

- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"
- p.138 "Methods of Overwriting"

Suspending Erase All Memory

The overwriting process can be suspended temporarily.

★ Important

- **Erase All Memory cannot be cancelled.**
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 the Power", About This Machine.

Note

- To resume overwriting, turn on the main power.

6. Managing Access to the Machine

This chapter describes how to prevent unauthorized access to and modification of the machine's settings.

Preventing Changes to Machine Settings

This section describes Preventing Modification of Machine Settings.

The administrator type determines which machine settings can be modified. Users cannot change the administrator settings. In "Available Settings" under "Administrator Authentication Management", the administrator can select which settings users cannot specify. For details about the administrator roles, see "Administrators".

Register the administrators before using the machine. For instructions on registering the administrator, see "Registering the Administrator".

Type of Administrator

Register the administrator on the machine, and then authenticate the administrator using the administrator's login user name and password. The administrator can also specify [Available Settings] in "Admin. Authentication" to prevent users from specifying certain settings. Administrator type determines which machine settings can be modified. The following administrator types are possible:

- User Administrator
For a list of settings that the user administrator can specify, see "User Administrator Settings".
- Machine Administrator
For a list of settings that the machine administrator can specify, see "Machine Administrator Settings".
- Network Administrator
For a list of settings that the network administrator can specify, see "Network Administrator Settings".
- File Administrator
For a list of settings that the file administrator can specify, see "File Administrator Settings".

Menu Protect

Use this function to specify the permission level for users to change those settings accessible by non-administrators.

You can specify Menu Protect for the following settings:

- Copier / Document Server Features
- Facsimile Features
- Printer Features
- Scanner Features

For a list of settings that users can specify according to the Menu Protect level, see "User Settings - Control Panel Settings", "User Settings - Web Image Monitor Settings".

Reference

- p.23 "Administrators"
- p.30 "Registering the Administrator"
- p.290 "User Administrator Settings"
- p.269 "Machine Administrator Settings"
- p.282 "Network Administrator Settings"
- p.288 "File Administrator Settings"
- p.299 "User Settings - Control Panel Settings"
- p.324 "User Settings - Web Image Monitor Settings"

Menu Protect

The administrator can also limit users' access permission to the machine's settings. The machine's "System Settings" menu and the printer's regular menus can be locked so they cannot be changed. This function is also effective when management is not based on user authentication. For a list of settings that users can specify according to the Menu Protect level, see "User Settings - Control Panel Settings", or "User Settings - Web Image Monitor Settings".

Reference

- p.299 "User Settings - Control Panel Settings"
- p.324 "User Settings - Web Image Monitor Settings"

Specifying Menu Protect

This can be specified by the machine administrator.

For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

You can set menu protect to [Off], [Level 1], or [Level 2]. If you set it to [Off], no menu protect limitation is applied. To limit access to the fullest extent, select [Level 2].

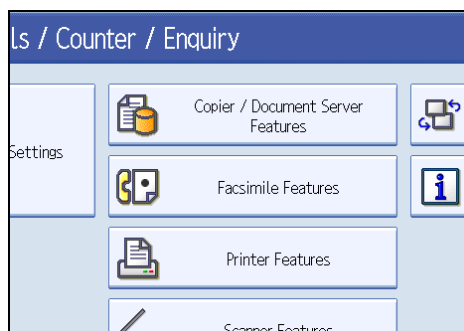
Reference

- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"

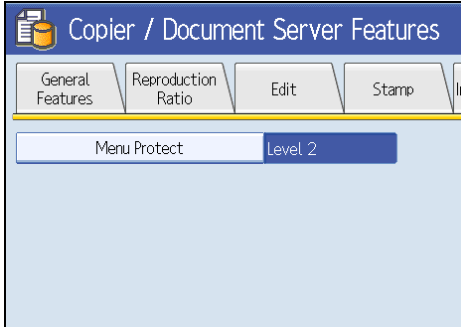
Copy Function

To specify "Menu Protect" in "Copier / Document Server Features", set "Machine Management" to [On] in "Administrator Authentication Management" in "Administrator Tools" in "System Settings".

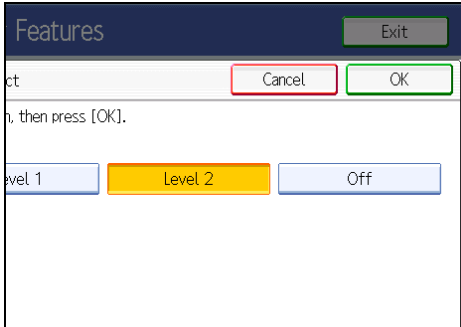
1. Press the [User Tools] key.
2. Press [Copier / Document Server Features].



- 3. Press [Administrator Tools].
- 4. Press [Menu Protect].



- 5. Select the menu protect level, and then press [OK].



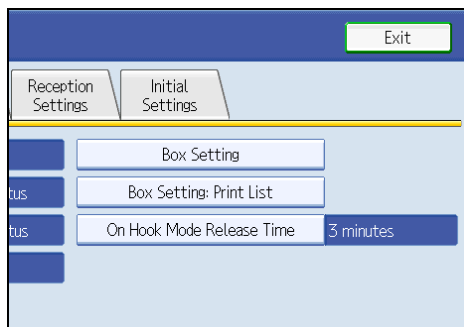
- 6. Press the [User Tools] key.

Fax Function

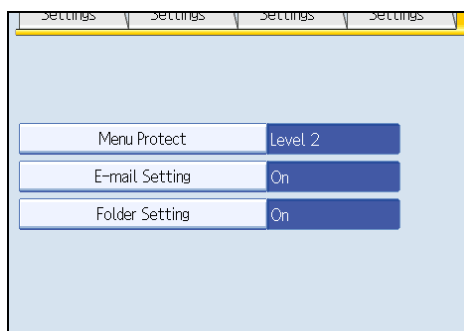
To specify "Menu Protect" in "Facsimile Features", set "Machine Management" to [On] in "Administrator Authentication Management" in "Administrator Tools" in "System Settings".

- 1. Press the [User Tools] key.
- 2. Press [Facsimile Features].

3. Press [Initial Settings].

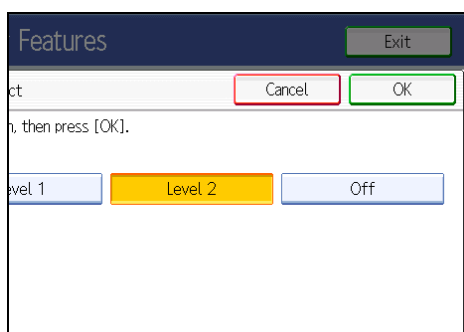


4. Press [Menu Protect].



If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

5. Select the menu protect level, and then press [OK].



6. Press the [User Tools] key.

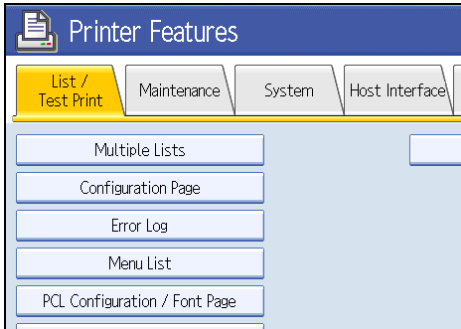
Printer Function

To specify "Menu Protect" in "Printer Features", set "Machine Management" to [On] in "Administrator Authentication Management" in "Administrator Tools" in "System Settings".

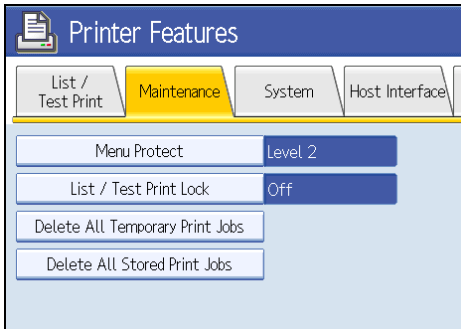
1. Press the [User Tools] key.

2. Press [Printer Features].

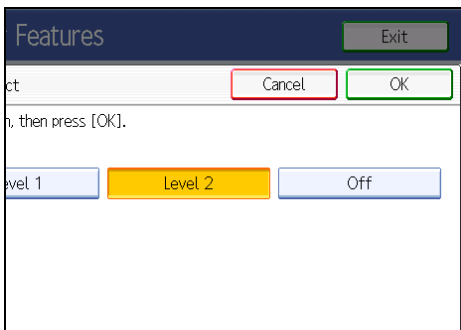
3. Press [Maintenance].



4. Press [Menu Protect].



5. Select the menu protect level, and then press [OK].



6. Press the [User Tools] key.

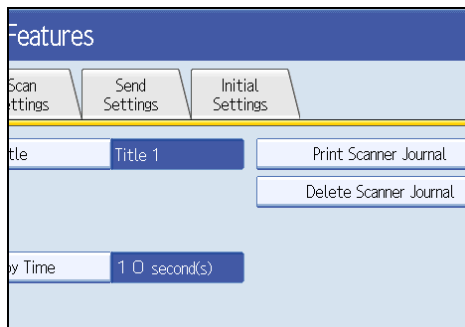
Scanner Function

To specify "Menu Protect" in "Scanner Features", set "Machine Management" to [On] in "Administrator Authentication Management" in "Administrator Tools" in "System Settings".

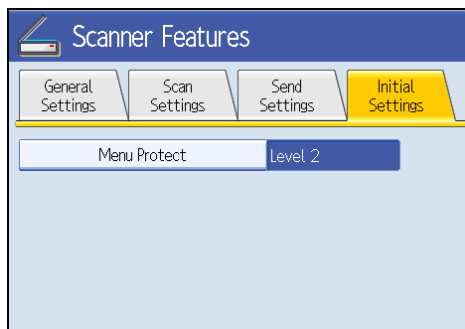
1. Press the [User Tools] key.

2. Press [Scanner Features].

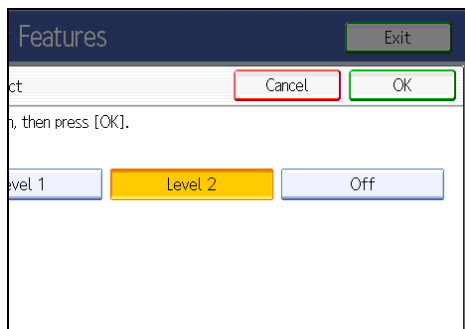
3. Press [Initial Settings].



4. Press [Menu Protect].



5. Select the menu protect level, and then press [OK].



6. Press the [User Tools] key.

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, and printer functions.

Specifying Which Functions are Available

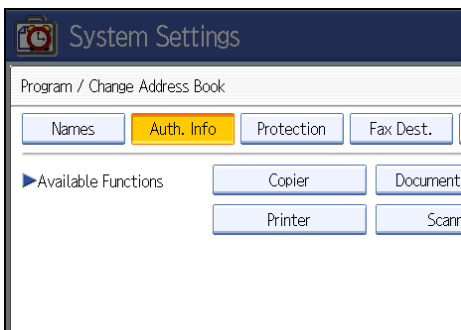
This can be specified by the user administrator.

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

For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

6

1. Press the [User Tools] key.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [Address Book Management].
5. Select the user.
6. Press [Auth. Info].
7. In "Available Functions", select the functions you want to specify.



If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

8. Press [OK].
9. Press [Exit].
10. Press the [User Tools] key.

 **Reference**

- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"

Managing Log Files

The logs created by this machine allow you to track access to the machine, identities of users, and usage of the machine's various functions. For security, you can encrypt the logs. This prevents users who do not have the encryption key from accessing log information.

Note however that logs are data heavy and will consume hard disk space. To make hard disk space available, you might need to periodically delete the log files.

The logs can be viewed using Web Image Monitor or Web SmartDeviceMonitor. You can also convert log files into CSV files for downloading. To use Web SmartDeviceMonitor, you must specify the log transfer setting under Web SmartDeviceMonitor in advance.

Log Types

This machine creates two types of log: the job log and the access log.

- Job Log

Stores details of user file-related operations such as copying, printing, and saving in the 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 activity, stored file operations such as creating, editing, and deleting, service engineer operations such as hard disk formatting, system operations such as viewing the results of log transfers and specifying settings for copy protection, and security operations such as specifying settings for encryption, unauthorized access detection, user lockout, and firmware authentication.

Using the Control Panel to Specify Log File Settings

This can be specified by the machine administrator.

For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

You can specify settings such as whether or not to transfer logs to Web SmartDeviceMonitor and whether or not to delete all logs.

Reference

- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"

Disabling Log Transfer to Web SmartDeviceMonitor

Use the following procedure to disable log transfer from the machine to Web SmartDeviceMonitor. Note that you can change the log transfer setting to [Inactive] only if it is already set to [Active].

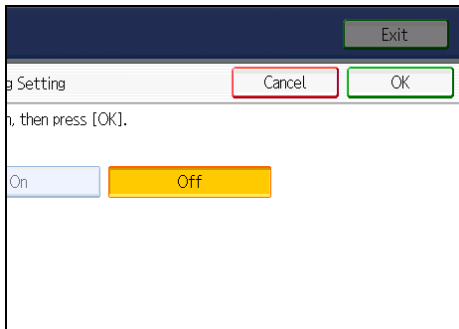
For details about Web SmartDeviceMonitor, contact your sales representative.

For details about the transfer log setting, see Web SmartDeviceMonitor manual.

1. Press the [User Tools] key.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [Transfer Log Setting].

If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

5. Press [Off].



6. Press [OK].
7. Press the [User Tools] key.

Specifying Delete All Logs

By deleting the log stored in the machine, you can free up space on the hard disk.

To delete all logs from the control panel, you must use Web SmartDeviceMonitor or enable the Job Log or Access Log collection settings using Web Image Monitor first.

1. Press the [User Tools] key.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [Delete All Logs].

If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

The confirmation screen appears.

5. Press [Yes].

6. Press [Exit].
7. Press the [User Tools] key.

Using Web SmartDeviceMonitor to Manage Log Files

For details about using Web SmartDeviceMonitor to manage Log Files, see the manual supplied with the Using Web SmartDeviceMonitor.

Using Web Image Monitor to Manage Log Files

This can be specified by the machine administrator.

For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

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.

6

Reference

- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"

Specifying Log Collect Settings

Specify collection log settings. The Log collection levels are listed below.

Job Log Collect Level

Level 1

User Settings

Access Log Collect Level

Level 1

Level 2

User Settings

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.

The top page of Web Image Monitor appears.

3. Click [Login].

The machine administrator can log on using the appropriate login user name and login password.

4. Click [Configuration], and then click [Logs] under Device Settings.**5. Select Collect Job Logs to specify Job Log settings, or select Collect Access Logs to specify Access Log settings, and then select [Active].****6. Specify the recording levels for either Job Log Collect Level or Access Log Collect Level.**

The settings shown for "Job Log Collect Settings Listed by Function Type" or "Access Log Collect Settings Listed by Function Type" vary depending on the collection level selected.

If you change the setting in the list, the setting for Job Log Collect Level or Access Log Collect Level automatically changes to [User Settings].

7. Click [OK].

Changes are also reflected in related log settings.

8. Click [Logout].**Note**

- The greater the Access Log Collect setting value, the more logs are collected.

Disabling Log Transfer to Web SmartDeviceMonitor

Use the following procedure to disable log transfer to Web SmartDeviceMonitor. Note that you can change the log transfer setting to [Inactive] only if it is already set to [Active].

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.

The top page of Web Image Monitor appears.

3. Click [Login].

The machine administrator can log on using the appropriate login user name and login password.

4. Click [Configuration], and then click [Logs] under Device Settings.**5. Select [Inactive] under "Transfer Logs".****6. Click [OK].****7. Click [Logout].**

Specifying Log Encryption

Use the following procedure to enable/disable log encryption.

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.

The top page of Web Image Monitor appears.

3. Click [Login].

The machine administrator can log on using the appropriate login user name and login password.

4. Click [Configuration], and then click [Logs] under Device Settings.

5. Select [Active] under "Encrypt Logs."

To disable log encryption, select [Inactive].

If other changes have been made in related log settings, they will occur at the same time.

6. Click [OK].

A confirmation message appears.

7. Click [OK].

The log is encrypted.

8. Click [Logout].

Note

- In order to enable encryption, either Collect Job Logs or Collect Access Logs, or both must be set to [Active].
- If the data stored in the machine has been encrypted with the optional HDD Encryption Unit, 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. 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.

The top page of Web Image Monitor appears.

3. Click [Login].

The machine administrator can log on using the appropriate login user name and login password.

4. Click [Configuration], and then click [Logs] under Device Settings.

5. Click [Delete] under "Delete All Logs".

6. Click [OK].

All job logs and device access log records are cleared.

7. Click [Logout].**↓ Note**

- On this page, "Delete All Logs" does not appear if either Collect Job Logs or Collect Access Logs are 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. Open a Web browser.**2. In the Web browser's address bar, enter "http://(the machine's IP address or host name)/" to access the machine.**

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. If you enter it as "192.168.001.010", you cannot access the machine.

The top page of Web Image Monitor appears.

3. Click [Login].

Log on using an administrator's user name and password.

4. Click [Configuration], and then click [Download Logs].**5. Click [Download].****6. Specify the folder in which you want to save the file.****7. Click [OK].****8. Click [Logout].****↓ 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.
- Downloading is slower if the number of logs is large.
- If an error occurs while the CSV file is downloading or being created, the download is cancelled and details of the error are included at the end of the file.
- For details about saving CSV log files, see your browser's Help.
- Depending on the configuration of your computer, some applications might not be able to display the downloaded CSV files.
- To collect logs, set "Collect Job Logs" and "Collect Access Logs" to [Active]. For details about setting, see Web Image Monitor Help.

- For details about the items contained in the logs, see "Attributes of Logs you can Download".

Reference

- p.164 "Attributes of Logs you can Download"

Logs that can be Managed Using Web Image Monitor

This section details the information items contained in the logs that are created for retrieval by 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. Web Image Monitor will then download the collected logs. For details, see the Help for Web Image Monitor.

Job Log Information Items

Job Log Item	Content
Copier: Copying	Details of normal and Sample Copy jobs.
Copier: Copying and Storing	Details of files stored in Document Server that were also copied at the time of storage.
Document Server: Storing	Details of files stored using the Document Server screen.
Document Server: Stored File Downloading	Details of files stored in Document Server and downloaded using Web Image Monitor or DeskTopBinder.
Utility: Storing	Details of files stored in Document Server using Auto Document Link.
Stored File Printing	Details of files printed using the Document Server screen.
Scanner: Sending	Details of sent scan files.
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	Details of scan files stored in Document Server that were also sent at the time of storage.
Scanner: Storing	Details of scan files stored in Document Server.

Job Log Item	Content
Scanner: Stored File Downloading	Details of scan files stored in Document Server and downloaded using Web Image Monitor or DeskTopBinder.
Scanner: Stored File Sending	Details of stored scan files that were also sent.
Scanner: Stored File URL Link Sending	Details of stored scan files whose URLs were sent by e-mail.
Scanner: TWAIN Driver Scanning	Details of stored scan files that were sent using Network TWAIN Scanner.
Printer: Printing	Details of normal print jobs.
Printer: Locked Print (Incomplete)	Details of unprinted Locked Print files stored on the machine.
Printer: Locked Print	Details of Locked Print files stored on the machine and printed from Web Image Monitor or the control panel.
Printer: Sample Print (Incomplete)	Details of Unprinted Sample Print files stored on the machine.
Printer: Sample Print	Details of Sample Print files stored on the machine and printed from Web Image Monitor or the control panel.
Printer: Hold Print (Incomplete)	Details of Unprinted Hold Print files stored on the machine.
Printer: Hold Print	Details of Hold Print files stored on the machine and printed from Web Image Monitor or the control panel.
Printer: Stored Print	Details of Stored Print files stored on the machine.
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 Normal Print" in printer properties).
Printer: Stored File Printing	Details of Stored Print files printed from the control panel or Web Image Monitor.
Printer: Document Server Sending	Details of files stored in Document Server when "Job Type" was set to "Send to Document Server" in printer properties.
Report Printing	Details of reports printed from the control panel.
Result Report Printing/E-mailing	Details of job results printed from the control panel or notified by e-mail.

Job Log Item	Content
Fax: Sending	Details of faxes sent from the machine.
Fax: LAN-Fax Sending	Details of fax files sent from PCs.
Fax: Storing	Details of fax files stored on the machine using the facsimile function.
Fax: Stored File Printing	Details of fax files stored on the machine and printed using the facsimile function.
Fax: Stored File Downloading	Details of fax files stored in Document Server and downloaded using Web Image Monitor or DeskTopBinder.
Fax: Receiving	Details of faxes received by the machine.
Fax: Receiving and Delivering	Details of faxes that received and delivered by the machine.
Fax: Receiving and Storing	Details of fax files that received and stored by the machine.

6

Access Log Information Items

Access Log Item	Content
Login	Times of login and identity of logged in users.
Logout	Times of logout and identity of logged out users.
File Storing	Details of files stored in Document Server.
Stored File Deletion	Details of files deleted from Document server.
All Stored Files Deletion	Details of deletions of all Document Server files.
HDD Format	Details of hard disk formatting.
Unauthorized Copying	Details of documents scanned with "data security for copying".
All Logs Deletion	Details of deletions of all logs.
Log Setting Change	Details of changes made to log settings.
Transfer Log Error	Details of changes made to log settings.
Log Collection Item Change	Details of changes made to log settings.
Collect Encrypted Communication Logs	Details of changes to job log collection levels, access log collection levels, and types of log collected.

Access Log Item	Content
Access Violation	Details of failed access attempts.
Lockout	Details of lockout activation.
Firmware: Update	Details of firmware updates.
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	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	Details of changes made to encryption keys using the Machine Data Encryption setting.
Firmware: Invalid	Details of checks for firmware validity made at times such as when the machine was switched on.
Date/Time Change	Details of changes made to date and time settings.
Web Image Monitor Auto Logout	Details of Web Image Monitor auto logouts.
File Access Privilege Change	Log for changing the access privilege to the stored files.
Password Change	Details of changes made to the login password.
Administrator Change	Details of changes of administrator.
Address Book Change	Details of changes made to address book entries.
Capture Error	Details of file capture errors.

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.

- If you format the hard disk, a log recording details of the format is created, but all actual logs up to that moment are deleted.

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.

Item	Content
Start Date/Time	Dates and times logged operations started.
End Date/Time	Dates and times logged operations ended.
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 "Logs that can be Collected".
Result	Result/outcome of the operation. "Complete" indicates the operation was completed successfully; "Failed" indicates the operation was not completed successfully. Details about failed jobs can be found in the access log.
User Entry ID	ID assigned to the entry.
User Code/User Name	User code or user name of the user who performed the operation.
Log ID	ID assigned to the log.

Job Log Information Items

Item	Content
Source	Type of the job log source. "Scan File" indicates a scan file; "Stored File" indicates a stored file; "Printer" indicates a printer driver job; "Report" indicates a printed report.
Start Date/Time	Dates and times "Scan File" and "Printer" operations started.
End Date/Time	Dates and times "Scan File" and "Printer" operations ended.
Stored File Name	Names of "Stored File" files.
Stored File ID	ID assigned to stored "Stored File" files.

Item	Content
Print File Name	Name of "Printer" files.
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.
Stored File ID	ID assigned to "Store" files.
Stored File Name	If the Target Type is "Store", the file name of the stored file is recorded.

Access Log Information Items

6

Item	Content
Access Log Type	Type of access log.
Logout Mode	Mode of logout. "Manual Logout" indicates a normal logout; "Auto logout" indicates an automatic logout.
Target User Entry ID	Entry ID of the user whose data was accessed.
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.
User Lockout Policy	The mode of operation access. "Lockout" indicates activation of password lockout; "Release" indicates deactivation of password lockout.
Lockout Release Method	"Administrator" is recorded if the machine is unlocked manually. "Lockout Release Timer" is recorded if the machine is unlocked by the lockout release timer.
Stored File ID	ID of a created or deleted file.
Stored File Name	Name of a created or deleted file.

Item	Content
File Location	Region of all file deletion. "Document Server" indicates a deletion of all files from the machine's hard disk. "SAF Region" is recorded if all files in the memory are deleted.
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.
MAC Address	Destination MAC (physical) address.
Module Name	Firmware module name.
Parts Number	Firmware module part number.
Version	Firmware version.
Access Result	Results of logged operations. "Complete" indicates an operation completed successfully; "Failed" indicates an operation completed unsuccessfully.

 **Reference**

- p.160 "Logs that can be Collected"

7. Enhanced Network Security

This chapter describes how to increase security over the network using the machine's functions.

Preventing Unauthorized Access

You can limit IP addresses, disable ports and protocols, or use Web Image Monitor to specify the network security level to prevent unauthorized access over the network and protect the Address Book, stored files, and default settings.

Access Control

This can be specified by the network administrator using Web Image Monitor.

For details, see Web Image Monitor Help.

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, IPDS, 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. **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.

The top page of Web Image Monitor appears.

3. **Click [Login].**

The network administrator can log on using the appropriate login user name and login password.

4. **Click [Configuration], and then click [Access Control] under "Security".**

The Access Control page appears.

5. 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".

6. Click [OK].

Access control is set.

7. Click [OK].

8. Click [Logout].

Enabling and Disabling Protocols

This can be specified by the network administrator.

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 Web SmartDeviceMonitor. For details about making settings using SmartDeviceMonitor for Admin or Web SmartDeviceMonitor, see the Help for each application. For details about making settings using telnet, see "Remote Maintenance by telnet ", Network and System Settings Guide. To disable SMTP on Web Image Monitor, in E-mail settings, set the protocol to anything other than SMTP. For details, see Web Image Monitor Help.

For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

Protocol	Port	Setting Method	When Disabled
IPv4	-	<ul style="list-style-type: none"> Control Panel Web Image Monitor telnet SmartDeviceMonitor for Admin Web SmartDeviceMonitor 	<p>All applications that operate over IPv4 cannot be used.</p> <p>IPv4 cannot be disabled from Web Image Monitor when using IPv4 transmission.</p>

Protocol	Port	Setting Method	When Disabled
IPv6	-	<ul style="list-style-type: none"> • Control Panel • Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Web SmartDeviceMonitor 	All applications that operate over IPv6 cannot be used.
IPsec	-	<ul style="list-style-type: none"> • Control Panel • Web Image Monitor • telnet 	Encrypted transmission using IPsec is disabled.
FTP	TCP:21	<ul style="list-style-type: none"> • Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Web SmartDeviceMonitor 	<p>Functions that require FTP cannot be used.</p> <p>You can restrict personal information from being displayed by making settings on the control panel using "Restrict Display of User Information".</p>
ssh/sftp	TCP:22	<ul style="list-style-type: none"> • Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Web SmartDeviceMonitor 	<p>Functions that require sftp cannot be used.</p> <p>You can restrict personal information from being displayed by making settings on the control panel using "Restrict Display of User Information".</p>
telnet	TCP:23	<ul style="list-style-type: none"> • Web Image Monitor 	Commands using telnet are disabled.

Protocol	Port	Setting Method	When Disabled
SMTP	TCP:25 (variable)	<ul style="list-style-type: none"> Control Panel Web Image Monitor SmartDeviceMonitor for Admin Web SmartDeviceMonitor 	Internet Fax or e-mail notification functions that require SMTP reception cannot be used.
HTTP	TCP:80	<ul style="list-style-type: none"> Web Image Monitor telnet 	Functions that require HTTP cannot be used. Cannot print using IPP on port 80.
HTTPS	TCP:443	<ul style="list-style-type: none"> Web Image Monitor telnet 	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	<ul style="list-style-type: none"> Control Panel Web Image Monitor telnet SmartDeviceMonitor for Admin Web SmartDeviceMonitor 	SMB printing functions cannot be used.
NBT	UDP:137 UDP:138	<ul style="list-style-type: none"> telnet 	SMB printing functions via TCP/IP, as well as NetBIOS designated functions on the WINS server cannot be used.

Protocol	Port	Setting Method	When Disabled
SNMPv1,v2	UDP:161	<ul style="list-style-type: none"> • Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Web SmartDeviceMonitor 	<p>Functions that require SNMPv1, v2 cannot be used.</p> <p>Using the control panel, Web Image Monitor or telnet, you can specify that SNMPv1, v2 settings are read-only, and cannot be edited.</p>
SNMPv3	UDP:161	<ul style="list-style-type: none"> • Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Web SmartDeviceMonitor 	<p>Functions that require SNMPv3 cannot be used.</p> <p>You can also make settings to require SNMPv3 encrypted transmission and restrict the use of other transmission methods using the control panel, Web Image Monitor, or telnet.</p>
RSH/RCP	TCP:514	<ul style="list-style-type: none"> • Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Web SmartDeviceMonitor 	<p>Functions that require RSH and network TWAIN functions cannot be used.</p> <p>You can restrict personal information from being displayed by making settings on the control panel using "Restrict Display of User Information".</p>

Protocol	Port	Setting Method	When Disabled
LPR	TCP:515	<ul style="list-style-type: none"> • Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Web SmartDeviceMonitor 	<p>LPR functions cannot be used.</p> <p>You can restrict personal information from being displayed by making settings on the control panel using "Restrict Display of User Information".</p>
IPP	TCP:631	<ul style="list-style-type: none"> • Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Web SmartDeviceMonitor 	<p>IPP functions cannot be used.</p>
IP-Fax	TCP:1720 (H.323) UDP:1719 (Gatekeeper) TCP/UDP:5060 (SIP) TCP:5000 (H.245) UDP:5004, 5005 (Voice) TCP/UDP:49152 (T.38)	<ul style="list-style-type: none"> • Control Panel • Web Image Monitor • SmartDeviceMonitor for Admin • Web SmartDeviceMonitor 	<p>IP-Fax connecting functions using H.323, SIP and T.38 cannot be used.</p>
SSDP	UDP:1900	<ul style="list-style-type: none"> • Web Image Monitor • telnet 	<p>Device discovery using UPnP from Windows cannot be used.</p>
Bonjour	UDP:5353	<ul style="list-style-type: none"> • Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Web SmartDeviceMonitor 	<p>Bonjour functions cannot be used.</p>

Protocol	Port	Setting Method	When Disabled
@Remote	TCP:7443 TCP:7444	<ul style="list-style-type: none"> telnet 	@Remote cannot be used.
DIPRINT	TCP:9100	<ul style="list-style-type: none"> Web Image Monitor telnet SmartDeviceMonitor for Admin Web SmartDeviceMonitor 	DIPRINT functions cannot be used.
RFU	TCP:10021	<ul style="list-style-type: none"> telnet 	You can attempt to update firmware via FTP.
NetWare	(IPX/SPX)	<ul style="list-style-type: none"> Control Panel Web Image Monitor telnet SmartDeviceMonitor for Admin Web SmartDeviceMonitor 	Cannot print with NetWare. SNMP over IPX cannot be used.
AppleTalk	(PAP)	<ul style="list-style-type: none"> Control Panel Web Image Monitor telnet 	Cannot print with AppleTalk.
WSD (Device)	TCP:53000 (variable)	<ul style="list-style-type: none"> Web Image Monitor telnet SmartDeviceMonitor for Admin Web SmartDeviceMonitor 	WSD (Device) functions cannot be used.

Protocol	Port	Setting Method	When Disabled
WSD (Printer)	TCP:53001 (variable)	<ul style="list-style-type: none"> • Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Web SmartDeviceMonitor 	WSD (Printer) functions cannot be used.
WSD (Scanner)	TCP:53002 (variable)	<ul style="list-style-type: none"> • Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Web SmartDeviceMonitor 	WSD (Scanner) functions cannot be used.
WS-Discovery	UDP/TCP:3702	<ul style="list-style-type: none"> • telnet • Web SmartDeviceMonitor 	WSD (Device, Printer, Scanner) search function cannot be used.
IPDS	TCP: 5001	<ul style="list-style-type: none"> • Web Image Monitor • telnet 	Cannot print with IPDS.
RHPP	TCP:59100	<ul style="list-style-type: none"> • Web Image Monitor • telnet 	Cannot print with RHPP.

Note

- "Restrict Display of User Information" is one of the Extended Security features. For details about making this setting, see "Specifying the Extended Security Functions".

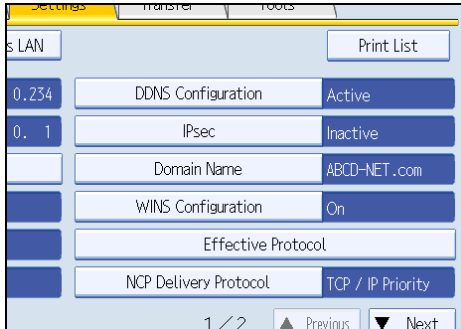
Reference

- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"
- p.221 "Specifying the Extended Security Functions"

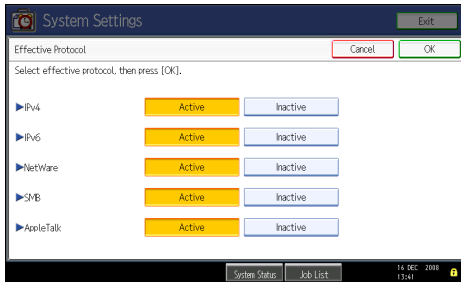
Enabling and Disabling Protocols Using the Control Panel

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

3. Press [Interface Settings].
4. Press [Effective Protocol].



5. Press [Inactive] for the protocol you want to disable.



6. Press [OK].
7. Press the [User Tools] key.

Enabling and Disabling Protocols 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.

The top page of Web Image Monitor appears.
3. Click [Login].

The network administrator can log on.

Enter the login user name and login password.
4. Click [Configuration], and then click [Network Security] under "Security".
5. Set the desired protocols to active/inactive (or open/close).
6. Click [OK].
7. Click [OK].

8. Click [Logout].

↓ Note

- To disable SMTP from Web Image Monitor, specify a protocol other than SMTP as the mail receiving protocol. See Web Image Monitor help for instructions to configure this setting.
- For details about how to configure telnet, see "Using telnet", Network and System Settings Guide. For details about how to configure SmartDeviceMonitor for Admin, see SmartDeviceMonitor for Admin help. For details about how to configure Web SmartDeviceMonitor, see the Web SmartDeviceMonitor user manual.

Specifying Network Security Level

This can be specified by the network administrator.

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.

Set the security level to [Level 0], [Level 1], or [Level 2].

Select [Level 2] for maximum security to protect confidential information. Make this setting when it is necessary to protect confidential information from outside threats.

Select [Level 1] for moderate security to protect important information. Use this setting if the machine is connected to the office local area network (LAN).

Select [Level 0] for easy use of all the features. Use this setting when you have no information that needs to be protected from outside threats.

For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

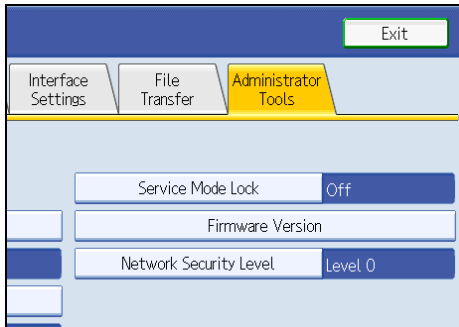
📖 Reference

- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"

Specifying Network Security Level Using the Control Panel

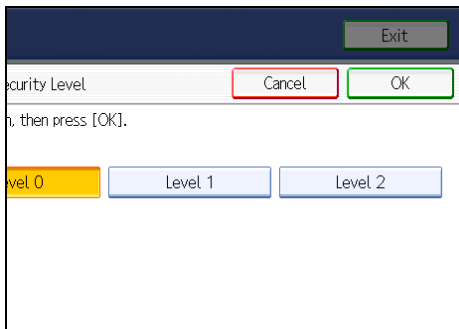
1. Press the [User Tools] key.
2. Press [System Settings].
3. Press [Administrator Tools].

4. Press [Network Security Level].



If the setting you want to specify does not appear, press [▼Next] to scroll down to other settings.

5. Select the network security level.



Select [Level 0], [Level 1], or [Level 2].

6. Press [OK].

7. Press [Exit].

8. Press the [User Tools] key.

Specifying Network Security Level 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.

The top page of Web Image Monitor appears.

3. Click [Login].

The network administrator can log on.

Enter the login user name and login password.

4. Click [Configuration], and then click [Network Security] under "Security".

5. Select the network security level in "Security Level".
6. Click [OK].
7. Click [OK].
8. Click [Logout].

Status of Functions under Each Network Security Level

Tab Name:TCP/IP

Function	Level 0	Level 1	Level 2
TCP/IP	Active	Active	Active
HTTP> Port 80	Open	Open	Open
IPP> Port 80	Open	Open	Open
IPP> Port 631	Open	Open	Close
SSL/TLS> Port 443	Open	Open	Open
SSL/TLS> Permit SSL/TLS Communication	Ciphertext Priority	Ciphertext Priority	Ciphertext Only
DIPRINT	Active	Active	Inactive
LPR	Active	Active	Inactive
FTP	Active	Active	Active
sftp	Active	Active	Active
ssh	Active	Active	Active
RSH/RCP	Active	Active	Inactive
TELNET	Active	Inactive	Inactive
Bonjour	Active	Active	Inactive
SSDP	Active	Active	Inactive
SMB	Active	Active	Inactive
NetBIOS over TCP/IPv4	Active	Active	Inactive
WSD (Device)	Active	Active	Inactive

Function	Level 0	Level 1	Level 2
WSD (Printer)	Active	Active	Inactive
WSD (Scanner)	Active	Active	Inactive
IPDS	Active	Active	Inactive
RHPP	Active	Active	Inactive

Tab Name:NetWare

Function	Level 0	Level 1	Level 2
NetWare	Active	Active	Inactive

Tab Name:AppleTalk

Function	Level 0	Level 1	Level 2
AppleTalk	Active	Active	Inactive

Tab Name:SNMP

Function	Level 0	Level 1	Level 2
SNMP	Active	Active	Active
Permit Settings by SNMPv1 and v2	On	Off	Off
SNMPv1,v2 Function	Active	Active	Inactive
SNMPv3 Function	Active	Active	Active
Permit SNMPv3 Communication	Encryption/ Cleartext	Encryption/ Cleartext	Encryption Only

Encrypting Transmitted Passwords

Prevent login passwords, group passwords for PDF files, and IPP authentication passwords from being revealed by encrypting them for transmission.

Also, encrypt the login password for administrator authentication and user authentication.

Driver Encryption Key

Encrypt the password transmitted when specifying user authentication.

To encrypt the login password, specify the driver encryption key on the machine and on the printer driver installed in the user's computer.

Group Passwords for PDF Files

DeskTopBinder Lite's PDF Direct Print function allows a PDF group password to be specified to enhance security.

To use PDF direct print, the optional PostScript 3 Unit must be installed.

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.

7

Specifying a Driver Encryption Key

This can be specified by the network administrator.

Specify the driver encryption key on the machine.

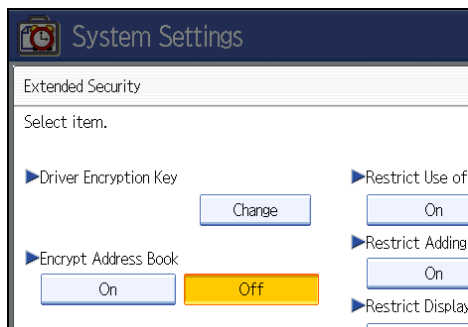
By making this setting, you can encrypt login passwords for transmission to prevent them from being analyzed.

For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

1. Press the [User Tools] key.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [Extended Security].

If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

5. For "Driver Encryption Key", press [Change].



"Driver Encryption Key" is one of the extended security functions. For details about this and other security functions, see "Specifying the Extended Security Functions".

6. 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.

7. Press [OK].

8. Press the [User Tools] key.

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 TWAIN driver, see the TWAIN driver Help.

Reference

- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"
- p.221 "Specifying the Extended Security Functions"

Specifying a Group Password for PDF files

This can be specified by the machine administrator.

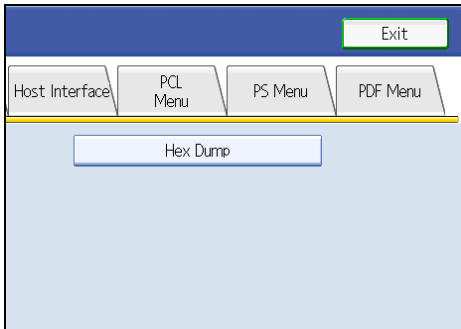
On the machine, specify the group password for PDF files.

By using a PDF group password, you can enhance security and so protect passwords from being analyzed.

For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

- 1. Press the [User Tools] key.**
- 2. Press [Printer Features].**

3. Press [PDF Menu].



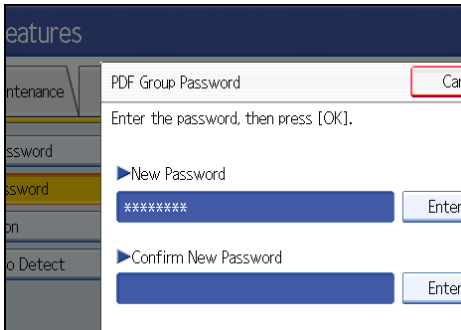
4. Press [PDF Group Password].

5. For "New Password", press [Enter].



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

7. For "Confirm New Password", press [Enter].



8. Enter the password and press [OK].

9. Press [OK].

10. Press the [User Tools] key.

Note

- The machine administrator must give users the group password for PDF files that are already registered on the machine. The users can then register it in DeskTopBinder on their computers. For details, see DeskTopBinder Help.
- Be sure to enter the same character string as that specified on the machine for the group password for PDF files.
- The group password for PDF files can also be specified using Web Image Monitor. For details, see Web Image Monitor Help.

Reference

- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"

Specifying an IPP Authentication Password

This can be specified by the network administrator.

Specify the IPP authentication passwords for the machine using Web Image Monitor.

By making this setting, you can encrypt IPP authentication passwords for transmission to prevent them from being analyzed.

- 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.

The top page of Web Image Monitor appears.

- 3. Click [Login].**

The network administrator can log on. Enter the login user name and login password.

- 4. Click [Configuration], and then click [IPP Authentication] under "Security".**

The IPP Authentication page appears.

- 5. Select [DIGEST] from the "Authentication" list.**

- 6. Enter the user name in the "User Name" box.**

- 7. Enter the password in the "Password" box.**

- 8. Click [OK].**

IPP authentication is specified.

- 9. Click [OK].**

- 10. Click [Logout].**

 **Note**

- When using the IPP port under Windows XP or Windows Server 2003/Windows Server 2003 R2, you can use the operating system's standard IPP port.

Protection Using Encryption

Establish encrypted transmission on this machine using SSL, SNMPv3, and IPsec. By encrypting transmitted data and safeguarding the transmission route, you can prevent sent data from being intercepted, analyzed, and tampered with.

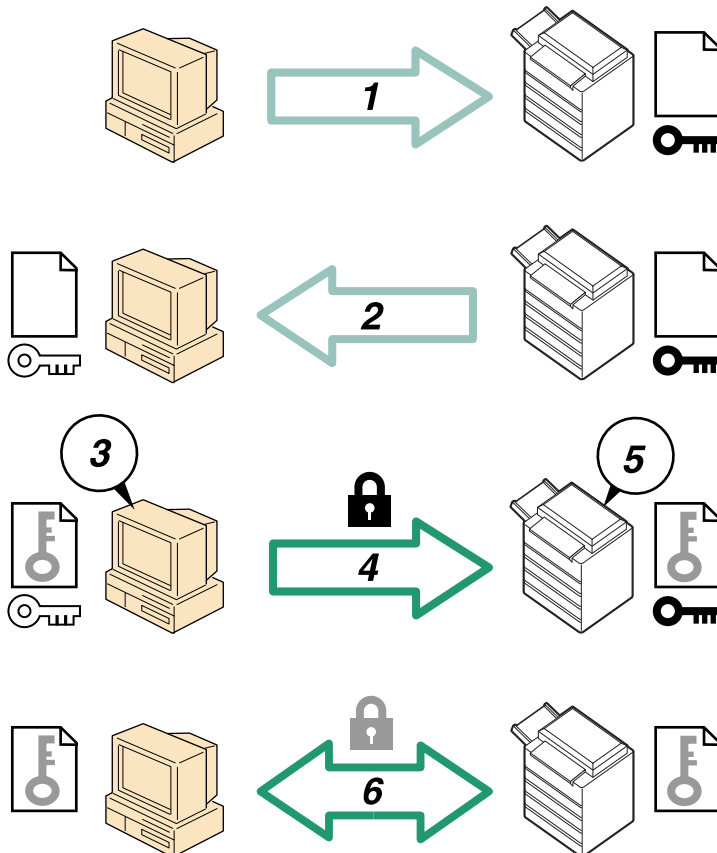
SSL (Secure Sockets Layer) Encryption

This can be specified by the network administrator.

To protect the communication path and establish encrypted communication, create and install the device certificate.

There are two ways of installing a device certificate: create and install a self-signed certificate using the machine, or request a certificate from a certificate authority and install it.

SSL (Secure Sockets Layer)



BBC003S

1. To access the machine from a user's computer, request the SSL device certificate and public key.

2. The device certificate and public key are sent from the machine to the user's computer.
3. Create a shared key from the user's computer, and then encrypt it using the public key.
4. The encrypted shared key is sent to the machine.
5. The encrypted shared key is decrypted in the machine using the private key.
6. Transmit the encrypted data using the shared key, and the data is then decrypted at the machine to attain secure transmission.

Configuration flow (self-signed certificate)

1. Creating and installing the device certificate
Install the device certificate using Web Image Monitor.
2. Enabling SSL
Enable the "SSL/TLS" setting using Web Image Monitor.

Configuration flow (certificate issued by a certificate authority)

1. Creating the device certificate
Create the device certificate using Web Image Monitor.
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

Enable the "SSL/TLS" setting using Web Image Monitor.

Note

- To confirm whether SSL 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 configuration is invalid.
- If you enable SSL for IPP (printer functions), sent data is encrypted, preventing it from being intercepted, analyzed, or tampered with.

Creating and Installing the 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. 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.

The top page of Web Image Monitor appears.

3. Click [Login].

The network administrator can log on.

Enter the login user name and login password.

4. Click [Configuration], and then click [Device Certificate] under "Security".**5. Check the radio button next to the number of the certificate you want to create.****6. Click [Create].****7. Make the necessary settings.****8. Click [OK].**

The setting is changed.

9. Click [OK].

A security warning dialog box appears.

10. Check the details, and then click [OK].

"Installed" appears under "Certificate Status" to show that a device certificate for the machine has been installed.

11. Click [Logout].**↓ 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. 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.

The top page of Web Image Monitor appears.

3. Click [Login].

The network administrator can log on.

Enter the login user name and login password.

4. Click [Configuration], and then click [Device Certificate] under "Security".

The Device Certificate page appears.

5. Check the radio button next to the number of the certificate you want to request.**6. Click [Request].****7. Make the necessary settings.****8. Click [OK].**

The setting is changed.

9. Click [OK].

"Requesting" appears for "Certificate Status".

10. Click [Logout].**11. 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. 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.

The top page of Web Image Monitor appears.

3. Click [Login].

The network administrator can log on.

Enter the login user name and login password.

4. Click [Configuration], and then click [Device Certificate] under "Security".

The Device Certificate page appears.

5. Check the radio button next to the number of the certificate you want to install.

6. Click [Install].

7. Enter the contents of the device certificate.

In the "Certificate Request" box, enter the contents of the device certificate received from the certificate authority.

8. Click [OK].

9. Click [OK].

"Installed" appears under "Certificate Status" to show that a device certificate for the machine has been installed.

10. Click [Logout].

Enabling SSL

After installing the device certificate in the machine, enable the SSL setting.

This procedure is used for a self-signed certificate or a certificate issued by a certificate authority.

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.

The top page of Web Image Monitor appears.

3. Click [Login].

The network administrator can log on.

Enter the login user name and login password.

4. Click [Configuration], and then click [SSL/TLS] under "Security".

The SSL/TLS page appears.

5. Click [Active] for the protocol version used in "SSL/TLS".

6. Select the encryption communication mode for "Permit SSL/TLS Communication".

7. Click [OK].

The SSL setting is enabled.

8. Click [OK].

9. Click [Logout].

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.

User Settings for SSL (Secure Sockets Layer)

If you have installed a device certificate using a self-signed certificate and enabled Secure Sockets Layer (SSL), a warning message may appear when you access the machine using Web Image Monitor or IPP. To stop this message appearing, install the certificate using the procedure for your particular browser. If you are the network administrator, tell your users they must install the certificate to stop the warning message appearing.

Note

- Take the appropriate steps when you receive a user's inquiry concerning problems such as an expired certificate.
- For details about how to install the certificate and about where to store the certificate when accessing the machine using IPP, see Web Image Monitor Help.
- If a certificate issued by a certificate authority is installed in the machine, confirm the certificate store location with the certificate authority.

7

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.

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.

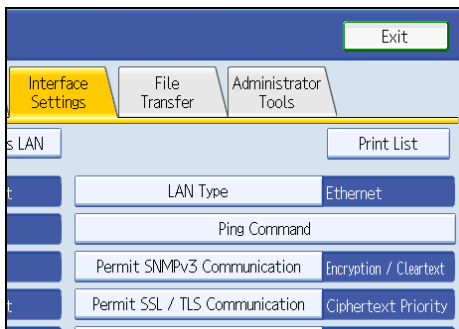
Specifying the SSL/TLS Encryption Mode

This can be specified by the network administrator.

After installing the device certificate, specify the SSL/TLS encrypted communication mode. By making this setting, you can change the security level.

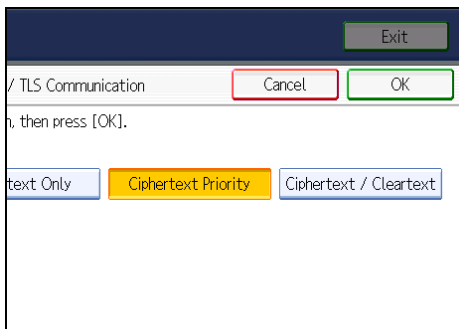
For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

1. Press the [User Tools] key.
2. Press [System Settings].
3. Press [Interface Settings].
4. Press [Permit SSL / TLS Communication].



If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

5. Select the encrypted communication mode.



Select [Ciphertext Only], [Ciphertext Priority], or [Ciphertext / Cleartext] as the encrypted communication mode.

6. Press [OK].
7. Press the [User Tools] key.

Note

- The SSL/TLS encrypted communication mode can also be specified using Web Image Monitor. For details, see Web Image Monitor Help.

Reference

- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"

SNMPv3 Encryption

This can be specified by the network administrator.

When using SmartDeviceMonitor for Admin or another application to make various settings, you can encrypt the data transmitted.

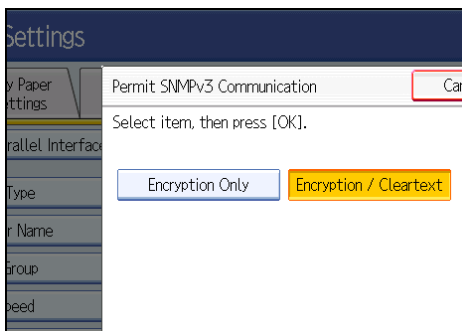
By making this setting, you can protect data from being tampered with.

For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

1. Press the [User Tools] key.
2. Press [System Settings].
3. Press [Interface Settings].
4. Press [Permit SNMPv3 Communication].

If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

5. Press [Encryption Only].



6. Press [OK].
7. Press the [User Tools] key.

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 "Registering the Administrator".

Reference

- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"
- p.30 "Registering the Administrator"

Transmission Using IPsec

This can be specified by the network administrator.

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", Network and System Settings Guide.
- IPsec is not applied to data obtained through DHCP, DNS, or WINS.
- IPsec compatible operating systems are Windows XP SP2, Windows Vista, Mac OSX 10.4 and later, RedHat Linux Enterprise 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 security 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.	<ul style="list-style-type: none"> Active Inactive
Exclude HTTPS Communication	Specify whether to enable IPsec for HTTPS transmission.	<ul style="list-style-type: none"> Active Inactive Specify "Active" if you do not want to use IPsec for HTTPS transmission.
Encryption Key Manual Settings	Specify whether to enable Encryption Key Manual Settings, or use Encryption Key Auto Exchange Settings only.	<ul style="list-style-type: none"> Active Inactive Specify "Active" if you want to use "Encryption Key Manual Settings".

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	SHA1
Phase 1 Encryption Algorithm	DES	3DES	3DES
Phase 1 Diffie-Hellman Group	2	2	2

Setting	Authentication Only	Authentication and Low Level Encryption	Authentication and High Level Encryption
Phase 2 Security Protocol	AH	ESP	ESP
Phase 2 Authentication Algorithm	HMAC-MD5-96/ HMAC-SHA1-96	HMAC-MD5-96/ HMAC-SHA1-96	HMAC-SHA1-96
Phase 2 Encryption Algorithm	Cleartext (NULL encryption)	DES/3DES/ AES-128/AES-192/ AES-256	3DES/AES-128/ AES-192/AES-256
Phase 2 PFS	Inactive	Inactive	2

Encryption Key Auto Exchange Setting 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".

7

Setting	Description	Setting Value
Address Type	Specify the address type for which IPsec transmission is used.	<ul style="list-style-type: none"> Inactive IPv4 IPv6 IPv4/IPv6 (Default Settings only)
Local Address	Specify the machine's address. If you are using multiple addresses in IPv6, you can also specify an address range.	The machine's IPv4 or IPv6 address. If you are not setting an address range, enter 32 after an IPv4 address, or enter 128 after an IPv6 address.

Setting	Description	Setting Value
Remote Address	Specify the address of the IPsec transmission partner. You can also specify an address range.	The IPsec transmission partner's IPv4 or IPv6 address. If you are not setting an address range, enter 32 after an IPv4 address, or enter 128 after an IPv6 address.
Security Policy	Specify how IPsec is handled.	<ul style="list-style-type: none"> • Apply • Bypass • Discard
Encapsulation Mode	Specify the encapsulation mode. (auto setting)	<ul style="list-style-type: none"> • Transport • Tunnel (Tunnel beginning address - Tunnel ending address) 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)	<ul style="list-style-type: none"> • Use When Possible • Always Require
Authentication Method	Specify the method for authenticating transmission partners. (auto setting)	<ul style="list-style-type: none"> • PSK • Certificate If you specify "PSK", you must then set the PSK text (using ASCII characters). If you specify "Certificate", the certificate for IPsec must be installed and specified before it can be used.

Setting	Description	Setting Value
PSK Text	Specify the pre-shared key for PSK authentication.	Enter the pre-shared key required for PSK authentication.
Phase 1 Hash Algorithm	Specify the Hash algorithm to be used in phase 1. (auto setting)	<ul style="list-style-type: none"> • MD5 • SHA1
Phase 1 Encryption Algorithm	Specify the encryption algorithm to be used in phase 1. (auto setting)	<ul style="list-style-type: none"> • DES • 3DES
Phase 1 Diffie-Hellman Group	Select the Diffie-Hellman group number used for IKE encryption key generation. (auto setting)	<ul style="list-style-type: none"> • 1 • 2 • 14
Phase 1 Validity Period	Specify the time period for which the SA settings in phase 1 are valid.	Set in seconds from 300 sec. (5 min.) to 172800 sec. (48 hrs.).
Phase 2 Security Protocol	Specify the security protocol to be used in Phase 2. To apply both encryption and authentication to sent data, specify "ESP" or "ESP+AH". To apply authentication data only, specify "AH". (auto setting)	<ul style="list-style-type: none"> • ESP • AH • ESP+AH
Phase 2 Authentication Algorithm	Specify the authentication algorithm to be used in phase 2. (auto setting)	<ul style="list-style-type: none"> • HMAC-MD5-96 • HMAC-SHA1-96

Setting	Description	Setting Value
Phase 2 Encryption Algorithm Permissions	Specify the encryption algorithm to be used in phase 2. (auto setting)	<ul style="list-style-type: none"> • Cleartext (NULL encryption) • DES • 3DES • AES-128 • AES-192 • AES-256
Phase 2 PFS	Specify whether to activate PFS. Then, if PFS is activated, select the Diffie-Hellman group. (auto setting)	<ul style="list-style-type: none"> • Inactive • 1 • 2 • 14
Phase 2 Validity Period	Specify the time period for which the SA settings in phase 2 are valid.	Specify a period (in seconds) from 300 (5min.) to 172800 (48 hrs.).

Encryption Key Manual Settings Items

7

Setting	Description	Setting Value
Address Type	Specify the address type for which IPsec transmission is used.	<ul style="list-style-type: none"> • Inactive • IPv4 • IPv6 • IPv4/IPv6 (Default Settings only)
Local Address	Specify the machine's address. If you are using multiple 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.

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.
Encapsulation Mode	Select the encapsulation mode.	<ul style="list-style-type: none"> • 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
Security Protocol	To apply both encryption and authentication to sent data, specify "ESP" or "ESP+AH". To apply authentication data only, specify "AH".	<ul style="list-style-type: none"> • ESP • AH • ESP+AH
Authentication Algorithm	Specify the authentication algorithm.	<ul style="list-style-type: none"> • HMAC-MD5-96 • HMAC-SHA1-96

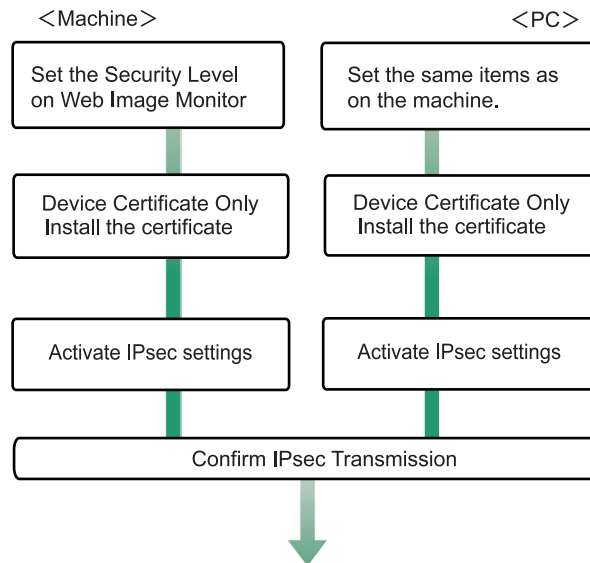
Setting	Description	Setting Value
Authentication Key	Specify the key for the authentication algorithm.	<p>Specify a value within the ranges shown below, according to the encryption algorithm.</p> <p>Hexadecimal value 0-9, a-f, A-F</p> <ul style="list-style-type: none"> • If HMAC-MD5-96, set 32 digits • If HMAC-SHA1-96, set 40 digits <p>ASCII</p> <ul style="list-style-type: none"> • If HMAC-MD5-96, set 16 characters • If HMAC-SHA1-96, set 20 characters
Encryption Algorithm	Specify the encryption algorithm.	<ul style="list-style-type: none"> • Cleartext (NULL encryption) • DES • 3DES • AES-128 • AES-192 • AES-256

Setting	Description	Setting Value
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 <ul style="list-style-type: none"> • DES, set 16 digits • 3DES, set 48 digits • AES-128, set 32 digits • AES-192, set 48 digits • AES-256, set 64 digits ASCII <ul style="list-style-type: none"> • 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

This section explains the procedure for specifying Encryption Key Auto Exchange Settings.

This can be specified by the network administrator.



BBD004S

↓ 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.

7

Specifying Encryption Key Auto Exchange Settings

This can be specified 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.

The top page of Web Image Monitor appears.

3. **Click [Login].**

The network administrator can log on.

Enter the login user name and login password.

4. **Click [Configuration], and then click [IPsec] under "Security".**

The IPsec settings page appears.

5. Click **[Edit]** under **"Encryption Key Auto Exchange Settings"**.
6. Make encryption key auto exchange 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"**.
9. Set **"Exclude HTTPS Communication"** to **[Active]** if you do not want to use IPsec for HTTPS transmission.
10. Click **[OK]**.
11. Click **[OK]**.
12. Click **[Logout]**.

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 "Using S/MIME to Protect E-mail Transmission".

Reference

- p.119 "Using S/MIME to Protect E-mail Transmission"

7

Selecting the Certificate for IPsec

This can be specified by the network administrator.

Using Web Image Monitor, select the certificate to be used for IPsec. You must install the certificate before it can be used.

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.
The top page of Web Image Monitor appears.
3. **Click [Login].**
The network administrator can log on.
Enter the login user name and login password.
4. **Click [Configuration], and then click [Device Certificate] under "Security".**
The Device Certificate page appears.
5. **Select the certificate to be used for IPsec from the drop down box in "IPsec" under "Certification".**

6. Click [OK].

The certificate for IPsec is specified.

7. Click [OK].**8. Click [Logout].**

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 XP when the Authentication and Low Level Encryption Security level is selected.

1. On the [Start] menu, click [Control Panel], click [Performance and Maintenance], and then click [Administrative Tools].**2. Click [Local Security Policy].****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 [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 combination of hash algorithm (on Windows XP, "Integrity"), the encryption algorithm (on Windows XP, "Encryption"), and the Diffie-Hellman group settings in "Security method preference order" match the settings specified on the machine in Encryption Key Auto Exchange Settings Phase 1.****12. If the settings are not displayed, click [Add].****13. Click [OK] twice.****14. Click [Add] in the "Rules" Tab.**

The Security Rule Wizard appears.

15. Click [Next].**16. Select "This rule does not specify a tunnel", and then click [Next].****17. Select the type of network for IPsec, and then click [Next].**

18. Select the "initial authentication method", and then click [Next].
19. 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.
20. Click [Add] in the IP Filter List.
21. In [Name], enter an IP Filter name, and then click [Add].
The IP Filter Wizard appears.
22. Click [Next].
23. Select "My IP Address" in "Source Address", and then click [Next].
24. Select "A specific IP address" in "Destination Address", enter the machine's IP address, and then click [Next].
25. Select the protocol type for IPsec, and then click [Next].
26. Click [Finish].
27. Click [OK].
28. Select the IP filter that was just created, and then click [Next].
29. Select the IPsec security filter, and then click [Edit].
30. Click [Add], select the "Custom" check box, and then click [Settings].
31. In "Integrity algorithm", select the authentication algorithm that was specified on the machine in Encryption Key Auto Exchange Settings Phase 2.
32. In "Encryption algorithm", select the encryption algorithm that specified on the machine in Encryption Key Auto Exchange Settings Phase 2.
33. 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.
34. Click [OK] three times.
35. Click [Next].
36. Click [Finish].
37. Click [OK].
38. Click [Close].

The new IP security policy (IPsec settings) is specified.

39. Select the security policy that was just created, right click, and then click [Assign].

IPsec settings on the computer are enabled.

 **Note**

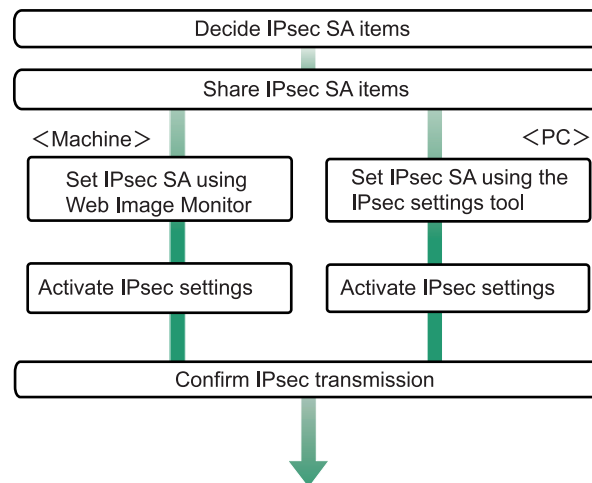
- To disable the computer's IPsec settings, select the security policy, right click, and then click [Un-assign].

- If you specify the "Authentication and High Level Encryption" security level in encryption key auto exchange settings, also select the "Master key perfect forward secrecy (PFS)" check box in the Security Filter Properties screen (which appears in step 29). If using PFS in Windows XP, 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.

Encryption Key Manual Settings Configuration Flow

This section explains the procedure for specifying encryption key manual settings.

This can be specified by the network administrator.



BBD003S

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

This can be specified 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.

The top page of Web Image Monitor appears.

3. Click [Login].

The network administrator can log on.

Enter the login user name and login password.

4. Click [Configuration], and then click [IPsec] under "Security".

The IPsec settings page appears.

5. Select [Active] for "Encryption Key Manual Settings".**6. Click [Edit] under "Encryption Key Manual Settings".****7. Set items for encryption key manual settings in [Settings 1].**

If you want to make multiple settings, select the settings number and add settings.

8. Click [OK].**9. Select [Active] for "IPsec:" in "IPsec".****10. Set "Exclude HTTPS Communication" to [Active] if you do not want to use IPsec for HTTPS communication.****11. Click [OK].****12. Click [Logout].****7**

telnet Setting Commands

You can use telnet to confirm IPsec settings and make setting changes. This section explains telnet commands for IPsec. To log on as an administrator using telnet, the default login user name is "admin", and the password is blank. For details about logging on to telnet and telnet operations, see "Using telnet", Network and System Settings Guide.

★ 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.

7**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.

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} 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 settings.

Authentication algorithm and authentication key settings

```
msh> ipsec manual {1|2|3|4|default} auth {hmac-md5|hmac-sha1} 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.

7**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 that IPsec can be applied to 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}
```

- Enter the separate setting number [1-4] or [default] and specify the ISAKMP SA (phase 1) hash algorithm.
- To use MD5, enter [md5]. To use SHA1, enter [sha1].
- 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}
```

- Enter the separate setting number [1-4] or [default] and specify the ISAKMP SA (phase 1) encryption algorithm.
- To use DES, enter [des]. To use 3DES, enter [3des].
- 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}
```

- 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.

Authentication by telnet

This section explains Authentication by telnet. When using telnet, the default login name for administrator login is "admin" and the password is blank. For details on how to login to telnet, see "Using telnet", Network and System Settings Guide.

"authfree" Command

Use the "authfree" command to display and configure authentication exclusion control settings. If you use the "authfree" command in telnet, you can exclude printer job authentication and specify an IP address range. The authentication exclusion control display and setting methods are explained below.

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 enable authfree, specify "on". To disable authfree, specify "off".
- Always specify the interface.

Authentication exclusion control initialization

```
msh> authfree flush
```

Note

- In both IPv4 and IPv6 environments, up to five access ranges can be registered and selected.

Authentication by IEEE802.1X

IEEE802.1X enables authentication in an Ethernet or wireless LAN environment. For details, see "Using telnet", Network and System Settings Guide.

8. Specifying the Extended Security Functions

This chapter describes the machine's extended security features and how to specify them.

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. If you need extended security, specify the machine's extended security functions before using the machine.

This section outlines the extended security functions and how to specify them.

For details about when to use each function, see the corresponding chapters.

Changing the Extended Security Functions

This section describes how to change the Extended Security Functions.

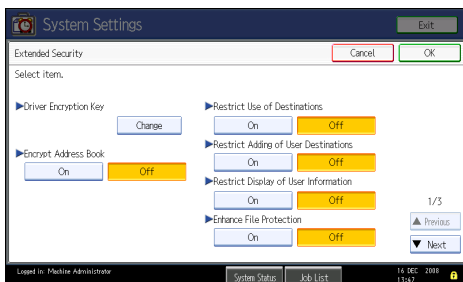
Administrators can change the extended security functions according to their role. For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

To change the extended security functions, display the extended security screen as follows.

1. Press the [User Tools] key.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [Extended Security].

If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

5. Press the setting you want to change, and change the setting.



6. Press [OK].

7. Press the [User Tools] key.

Reference

- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"

Extended Security Settings

Default settings are shown in **bold type**.

Driver Encryption Key

This can be specified by the network administrator. Encrypt the password transmitted when specifying user authentication. If you register the encryption key specified with the machine in the driver, passwords are encrypted. For details, see the printer driver Help, LAN Fax driver Help, or TWAIN driver Help.

Encrypt Address Book

This can be specified by the user administrator. Encrypt the data in the machine's Address Book. For details on protecting data in the Address Book, see "Protecting the Address Book".

- On
- **Off**

Restrict Use of Destinations

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 you specify the setting to receive e-mails via SMTP, you cannot use "Restrict Use of Destinations".

The destinations searched by "Search LDAP" can be used.

For details about preventing unauthorized transmission, see "Preventing Information Leakage Due to Unauthorized Transmission".

- On
- **Off**

Restrict Adding of User Destinations

This can be specified by the user administrator.

When "Restrict Use of Destinations" is set to [Off], after entering a fax or scanner destination directly, you can register it in the Address Book by pressing [Prg. Dest.]. If [On] is selected for this setting, [Prg. Dest.] does not appear. If you set "Restrict Adding of User Destinations" to [On], users can specify destinations directly, but cannot use [Prg. Dest.] to register data in the Address Book. When this setting

is made, only the user administrator can change the Address Book. If this setting is made, only the user administrator can register new users in the Address Book. Also, only the user administrator can change passwords and other user information that is registered in the Address Book.

- On
- **Off**

Restrict Display of User Information


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.

- On
- **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 "Enhance File Protection" is specified,  appears in the lower right corner of the screen.

When files are locked, you cannot select them even if the correct password is entered.

- On
- **Off**

Settings by SNMPv1 and 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.

- Prohibit
- **Do not Prohibit**

Restrict Use of Simple Encryption

This can be specified by the network administrator. When a sophisticated encryption method cannot be enabled, simple encryption will be applied. For example, when using User Management Tool and

Address Management in Smart Device Monitor for Admin to edit the Address Book, or DeskTopBinder and ScanRouter delivery software and SSL/TLS cannot be enabled, make this setting [Off] to enable simple encryption. When SSL/TLS can be enabled, make this setting [On].

For details about specifying SSL/TLS, see "Setting the SSL/TLS Encryption Mode".

If you select [On], specify the encryption setting using the printer driver.

- On
- **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.

- Prohibit
- **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

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 on to the machine before [Login Privilege] was selected.

If you select [Access Privilege], users who canceled a copy or print job in progress and the machine administrator can operate the machine.

Even if you select [Login Privilege] and log on to the machine, you cannot cancel a copy or print job in progress if you are not authorized to use the copy and printer functions.

You can specify [Authenticate Current Job] only if [User Authentication Management] was specified.

- Login Privilege
- Access Privilege
- **Off**

Password Policy

This can be specified by the user administrator.

The password policy setting is effective only if [Basic Auth.] is specified.

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 #.

- Level 2
- Level 1
- **Off**
- Minimum Character No. (0)

@Remote Service

Communication via HTTPS for @Remote Service is disabled if you select [Prohibit].

- Prohibit
- **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.

- Prohibit
- **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 on.

When Change Firmware Structure is set to [Prohibit], administrator authentication must be enabled.

After [Prohibit] is specified, turn off administrator authentication once, and the next time administrator authentication is specified, the setting will return to the default, [Do not Prohibit].

If you select [Do not Prohibit], firmware structure change detection is disabled.

- Prohibit
- **Do not Prohibit**

Reference

- p.127 "Protecting the Address Book"
- p.117 "Preventing Information Leakage Due to Unauthorized Transmission"
- p.190 "Setting the SSL/TLS Encryption Mode"

Other Security Functions

This section explains settings for preventing information leaks, and functions that you can restrict to further increase security.

Fax Function

Not Displaying Destinations and Senders in Reports and Lists

In [Facsimile Features], you can specify whether to display destinations and sender names by setting "Switch 4, Bit No. 4" and "Switch 4, 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 about "Not Displaying Destinations and Senders in Reports and Lists", see "Facsimile Features", Facsimile Reference.

Stored RX File User Setting

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 [Initial 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 about Stored RX File User Setting, see "Facsimile Features", Facsimile Reference.

Printing the Journal

When making authentication settings for users, to prevent personal information in transmission history being printed, set the Journal to not be printed. 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], go to [Initial Settings], [Parameter Setting] "Switch 03, Bit 7", and change the setting for automatically printing the Journal.
- In [Facsimile Features], go to [Initial Settings], [Parameter Setting] "Switch 21, Bit 4", and set "Transmit Journal by E-mail" to ON.

Scanner Function

Print & Delete Scanner Journal

To prevent personal information in the transmission/delivery history being printed automatically, set user authentication and the journal will specify [Do not Print: Disable Send] automatically. If you do this, 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 [On] for "Print & Delete Scanner Journal". For details, see "Scanner Features", Scanner Reference.

WSD scanner function

WSD scanner function is automatically disabled when user authentication is specified. Even if automatically disabled, it can be enabled from the initial settings available in Web Image Monitor. For instructions on how to configure this function, see "Before Sending Scan Files Using WSD", Scanner Reference.

Weekly Timer Code

This can be specified by the machine administrator.

For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

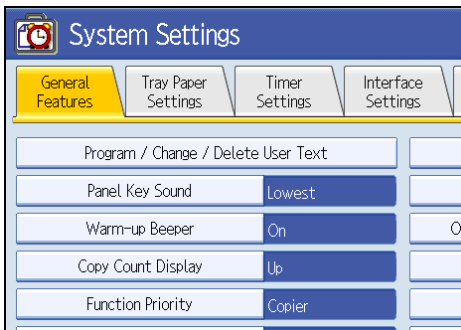
If the weekly timer is enabled and [Weekly Timer Code] is set to [On], you must enter the weekly timer code to turn the power back on after the timer has turned it off.

Reference

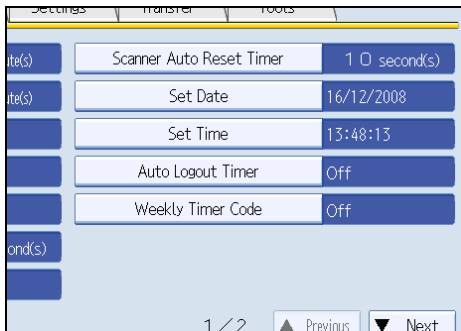
- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"

Specifying Weekly Timer Code

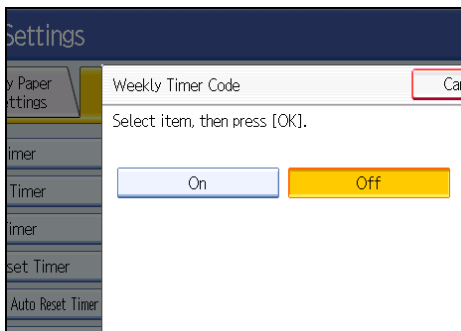
1. Press the [User Tools] key.
2. Press [System Settings].
3. Press [Timer Settings].



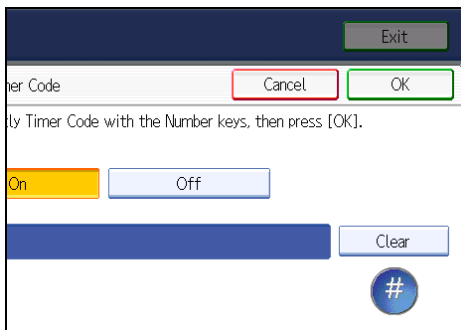
4. Press [Weekly Timer Code].



5. Press [On].



6. Using the number keys, enter the weekly timer code.



The weekly timer code must be one to eight digits long.

7. Press [OK].

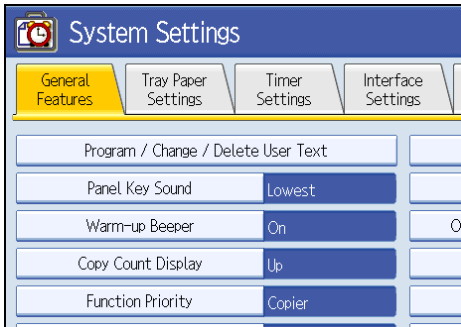
8. Press the [User Tools] key.

Canceling Weekly Timer Code

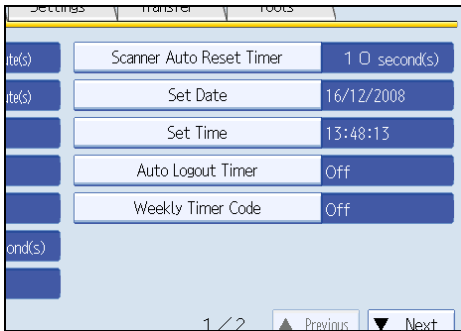
1. Press the [User Tools] key.

2. Press [System Settings].

3. Press [Timer Settings].

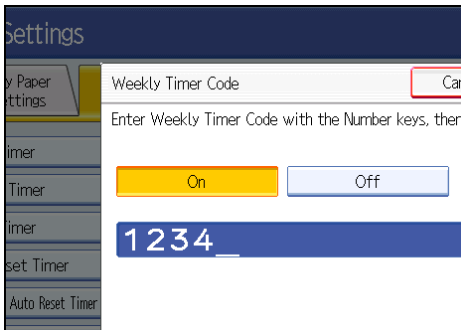


4. Press [Weekly Timer Code].



5. Press [Off] and then [OK].

8



6. Press the [User Tools] key.

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.

Use the following settings.

- Service Mode Lock

Settings

This can be specified by the machine administrator.

For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

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 the 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.

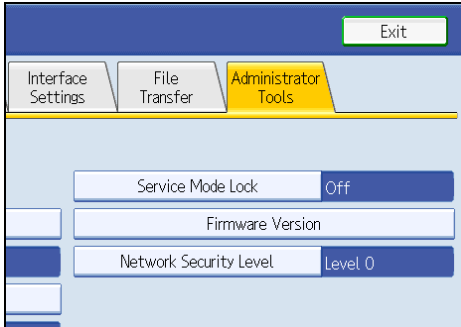
Reference

- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"

Specifying Service Mode Lock

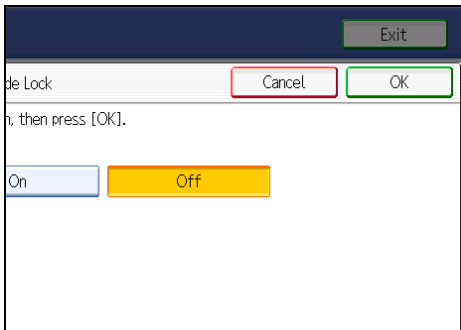
1. Press the [User Tools] key.
2. Press [System Settings].
3. Press [Administrator Tools].

4. Press [Service Mode Lock].



If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

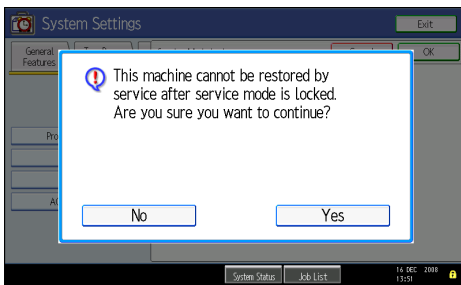
5. Press [On], and then press [OK].



8

A confirmation message appears.

6. Press [Yes].



7. Press the [User Tools] key.

Canceling Service Mode Lock

To enable a service representative to inspect or repair this machine, the machine administrator must log on and cancel the service mode lock beforehand.

1. Press the [User Tools] key.

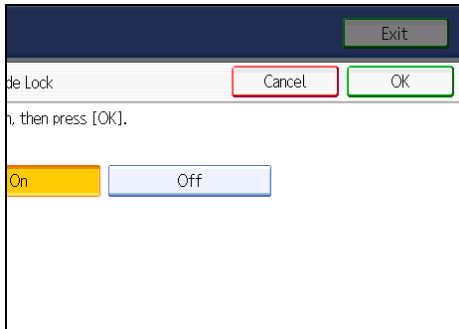
2. Press [System Settings].

3. Press [Administrator Tools].

4. Press [Service Mode Lock].

If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

5. Press [Off], and then press [OK].



6. Press the [User Tools] key.

The service representative can switch to service mode.

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.

Menu

System Settings

Tab	Item	Setting
Timer Settings	Auto Logout Timer	[On]: 180 seconds or less. You cannot change the Web Image Monitor auto logout time. See "Auto Logout".
Administrator Tools	User Authentication Management	Select [Basic Auth.], and then set "Printer Job Authentication" to [Entire]. See "Basic Authentication".
Administrator Tools	Administrator Authentication Management/User Management	Select [On], and then select [Administrator Tools] for "Available Settings". See "Enabling Administrator Authentication".
Administrator Tools	Administrator Authentication Management/Machine Management	Select [On], and then select [Timer Settings], [Interface Settings], [File Transfer], and [Administrator Tools] for "Available Settings". See "Enabling Administrator Authentication".
Administrator Tools	Administrator Authentication Management/Network Management	Select [On], and then select [Interface Settings], [File Transfer], and [Administrator Tools] for "Available Settings". See "Enabling Administrator Authentication".
Administrator Tools	Administrator Authentication Management/File Management	Select [On], and then select [Administrator Tools] for "Available Settings". See "Enabling Administrator Authentication".

Tab	Item	Setting
Administrator Tools	Extended Security/Settings by SNMPv1 and v2	[Prohibit] See "Specifying the Extended Security Functions".
Administrator Tools	Extended Security/Restrict Use of Simple Encryption	[On] See "Specifying the Extended Security Functions".
Administrator Tools	Extended Security/Authenticate Current Job	[Access Privilege] See "Specifying the Extended Security Functions".
Administrator Tools	Extended Security/Password Policy	"Complexity Setting": [Level 1] or higher, "Minimum Character No.": 6 or higher See "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 "Specifying Network Security Level".
Administrator Tools	Service Mode Lock	[On] See "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), or format all data." See "Encrypting Data on the Hard Disk".

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 "Other Security Functions".

Tab	Item	Setting
Initial Settings	Menu Protect	[Level 2] See "Menu Protect".

Note

- For details about SNMP setting, see Web Image Monitor Help.
- For details about the stored reception file user setting, see "Other Security Functions" or "Facsimile Features", Facsimile Reference.

Reference

- p.88 "Auto Logout"
- p.46 "Basic Authentication"
- p.27 "Enabling Administrator Authentication"
- p.221 "Specifying the Extended Security Functions"
- p.176 "Specifying Network Security Level"
- p.231 "Limiting Machine Operations to Customers Only"
- p.131 "Encrypting Data on the Hard Disk"
- p.227 "Other Security Functions"
- p.147 "Menu Protect"

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
Security/User Lockout Policy	Number of Attempts before Lockout	5 times or less. See "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. See "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. See "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.
Network/Network Security	FTP	Inactive Before specifying this setting, set "Network Security Level" to [Level 2] on the control panel.

↓ Note

- For details about the collect log setting and SNMPv3 setting, see Web Image Monitor Help.

📖 Reference

- p.86 "User Lockout Function"

Settings You Can Configure When IPsec Is Available/Unavailable

IPsec encrypts all the data traveling on your network.

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.

System Settings (Control panel)

Tab	Item	Setting
Interface Settings	IPsec	[Active]
Interface Settings	Permit SSL / TLS Communication	[Ciphertext Only]

Web Image Monitor settings

Category	Item	Setting
Security/SSL/TLS	Permit SSL/TLS Communication	If you set "Exclude HTTPS Communication" to Active, you must also set "Permit SSL/TLS Communication" to Ciphertext Priority.
Security/IPsec	Encryption Key Manual Settings	Inactive
Security/IPsec	Encryption Key Auto Exchange Settings/ Security Level	Authentication and High Level Encryption

Note

- You can set "Permit SSL/TLS Communication" using either Web Image Monitor or the machine's control panel.

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.

System Settings (Control panel)

Tab	Item	Setting
Interface Settings	IPsec	[Inactive]
Interface Settings	Permit SSL / TLS Communication	[Ciphertext Only]

Web Image Monitor settings

Category	Item	Setting
Security	S/MIME	"Encryption Algorithm": 3DES-168 bit You must register the user certificate in order to use S/MIME.
Address Book/E-mail	User Certificate	You must register the user certificate in order to use S/MIME.

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

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", Facsimile Reference.

- Printer

To use the printer functions, specify "SFTP" as the protocol, or specify "IPP" and select "Active" for "SSL".

For details about SFTP, see "Special Operations under Windows", Network and System Settings.

For details about IPP settings, see "Installing the Printer Driver", Printer Reference.

For details about SSL settings, see "Setting the SSL/TLS Encryption Mode".

- Scanner

Send the URL of scanned files to destinations by configuring [Send Settings] in [Scanner Features], instead of sending the actual scanned files. Use Web Image Monitor through your network to view, delete, send, and download scanned files.

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 "Sending Scan Files by E-mail", Scanner Reference.

↓ Note

- For details about enabling and disabling IPsec using the control panel, see "System Settings", Network and System Settings Guide.
- For details about Permit SSL/TLS Communication settings and IPsec settings using Web Image Monitor, see "Protection Using Encryption" and "Transmission Using IPsec".

- For Encryption Algorithm settings and how to specify User Certificate, see "Using S/MIME to Protect Email Transmission".

Reference

- p.185 "Protection Using Encryption"
- p.190 "Setting the SSL/TLS Encryption Mode"
- p.194 "Transmission Using IPsec"
- p.119 "Using S/MIME to Protect E-mail Transmission"

9. 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.

The most common messages are explained. If some other message appears, deal with the problem according to the information contained in the message.

Messages	Cause	Solutions
"You do not have the privileges to use this function."	The authority to use the function is not specified.	<ul style="list-style-type: none">• 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 authorize use of the function and then assign the authority.• 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 authorize use of the function.

Messages	Cause	Solutions
"Failed to obtain URL."	The machine cannot connect to the server or cannot establish communication.	Make sure the server's settings, such as the IP address and host name, are specified correctly on the machine. Make sure the host name of the UA Server is specified correctly.
"Failed to obtain URL."	The machine is connected to the server, but the UA service is not responding properly.	Make sure the UA service is specified correctly.
"Failed to obtain URL."	SSL is not specified correctly on the server.	Specify SSL using Authentication Manager.
"Failed to obtain URL."	Server authentication failed.	Make sure server authentication is specified correctly on the machine.
"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.

Messages	Cause	Solutions
"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 about authentication settings, see "Configuring User Authentication".
"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 file creator (owner) or file administrator. To delete a file which you are not authorized to delete, contact the file creator (owner).

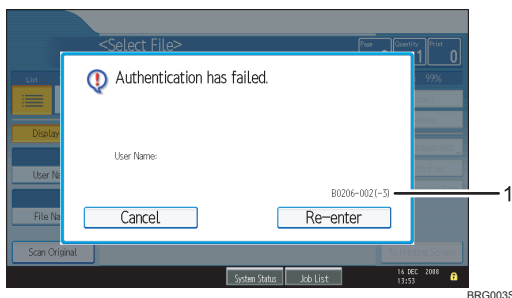
Reference

- p.39 "Configuring User Authentication"

If an Error Code is Displayed

When authentication fails, the message "Authentication has failed." appears with an error code. The following tables list the error codes, likely causes of the problems they indicate, and what you can do to resolve those problems. If the error code that appears is not on this table, take a note and contact your service representative.

Error Code Display Position



BRG003S

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.	<p>1. A password error occurred. Make sure the password is entered correctly.</p> <p>2. "Restrict Use of Simple Encryption" is enabled. The administrator has restricted use of simple encryption. You can use the encryption key if it has been specified in the driver.</p> <p>3. A driver encryption key error occurred. Make sure that the encryption key is correctly specified on the driver.</p>
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 on.
B0206-002	2. The user attempted authentication from an application on the "System Settings" screen, where only the administrator has authentication ability.	<p>Only the administrator has login privileges on this screen.</p> <p>Log on as a general user from the application's login screen.</p>

Error Code	Cause	Solution
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 on again.
B0207-001	An authentication error occurred because the Address Book is being used at another location.	Wait a few minutes and then try again.
B0208-000	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 on to the machine, and then try again.
W0104-000	Failed to encrypt password.	<ol style="list-style-type: none"> 1. A password error occurred. Make sure the password is entered correctly. 2. "Restrict Use of Simple Encryption" is enabled. 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.

Error Code	Cause	Solution
W0105-000	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 on as a general user from the application's login screen.
W0206-003	An authentication error occurred because the user name contains a space, colon (:), or quotation mark (").	Recreate the account if the account name contains any of these prohibited characters. If the account name was entered incorrectly, enter it correctly and log on 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.

Error Code	Cause	Solution
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.
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".

Error Code	Cause	Solution
W0406-104	4. Cannot resolve the domain name.	<p>Specify the IP address in the domain name and confirm that authentication is successful.</p> <p>If authentication was unsuccessful:</p> <ol style="list-style-type: none"> 1. Make sure that Restrict LM/NTLM is not set in either "Domain Controller Security Policy" or "Domain Security Policy". Authentication is rejected because NTLMv2 is not supported. 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. <p>If you are using a Windows firewall, open "Network Connection Properties". Then click detail settings, Windows firewall settings, permit exceptions settings. Click the exceptions tab and specify numbers 137, 139 as the exceptions.</p> <p>In "Network Connection" properties, 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".</p>

Error Code	Cause	Solution
W0406-104	5. Kerberos authentication failed.	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>

Error Code	Cause	Solution
W0400-105	<p>1. The UserPrincipalName (user@domainname.xxx.com) form is being used for the login user name.</p>	<p>The user group cannot be obtained if the UserPrincipalName (user@domainname.xxx.com) form is used. Use "sAMAccountName (user)" to log on, because this account allows you to obtain the user group.</p>
W0400-105	<p>2. Current settings do not allow group retrieval.</p>	<p>Make sure the user group's group scope is set to "Global Group" and the group type is set to "Security" in group properties.</p> <p>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.</p> <p>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.</p>
W0400-106	<p>The domain name cannot be resolved.</p>	<p>Make sure that DNS/WINS is specified in the domain name in "Interface Settings".</p>
W0400-200	<p>Due to the high number of authentication attempts, all resources are busy.</p>	<p>Wait a few minutes and then try again.</p>

Error Code	Cause	Solution
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 on.	If a user enters sAMAccountName as the login user name, ldap_bind fails in a parent/subdomain environment. Use UserPrincipalName for the login name instead.
W0406-003	An authentication error occurred because the user name contains a space, colon (:), or quotation mark (").	Recreate the account if the account name contains any of these prohibited characters. If the account name was entered incorrectly, enter it correctly and log on again.
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.

Error Code	Cause	Solution
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 on to the machine, and then try again.
L0104-000	Failed to encrypt password.	<ol style="list-style-type: none"> 1. A password error occurred. Make sure the password is entered correctly. 2. "Restrict Use of Simple Encryption" is enabled. 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.

Error Code	Cause	Solution
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 on 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 on 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.
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".

Error Code	Cause	Solution
<p>L0406-202 L0406-203</p>	<p>1. There is an error in the LDAP authentication settings, LDAP server, or network configuration.</p>	<p>1. Make sure that a connection test is successful with the current LDAP server configuration.</p> <p>If connection is not successful, there might be an error in the network settings. Check the domain name or DNS settings in "Interface Settings".</p> <p>2. Make sure the LDAP server is specified correctly in the LDAP authentication settings.</p> <p>3. Make sure the login name attribute is entered correctly in the LDAP authentication settings.</p> <p>4. Make sure the SSL settings are supported by the LDAP server.</p>
<p>L0406-202 L0406-203</p>	<p>2. A login user name or password error occurred.</p>	<p>1. Make sure the login user name and password are entered correctly.</p> <p>2. Make sure a usable login name is registered on the machine.</p> <p>Authentication will fail in the following cases:</p> <p>If the login user name contains a space, colon (:), or quotation mark (").</p> <p>If the login user name exceeds 128 bytes.</p>

Error Code	Cause	Solution
L0406-202 L0406-203	3. There is an error in the simple encryption method.	<p>1. Authentication will fail if the password is left blank in simple authentication mode. To allow blank passwords, contact your service representative.</p> <p>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.</p>
L0406-204	Kerberos authentication failed.	<p>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.</p> <p>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.</p> <p>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.</p>

Error Code	Cause	Solution
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 on 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.
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.)	<ol style="list-style-type: none"> 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.

Error Code	Cause	Solution
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 on to the machine, and then try again.
I0104-000	Failed to decrypt password.	<ol style="list-style-type: none"> 1. A password error occurred. Make sure the password is entered correctly. 2. "Restrict Use of Simple Encryption" is enabled. 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. <p>Make sure that the encryption key is correctly specified on the driver.</p>
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.	<p>Only the administrator has login privileges on this screen.</p> <p>Log on as a general user from the application's login screen.</p>

Error Code	Cause	Solution
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 on 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.
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 on 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.

Error Code	Cause	Solution
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.)	<ol style="list-style-type: none"> 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.
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
<p>Cannot perform the following:</p> <ul style="list-style-type: none"> • Print with the printer driver • Connect with the TWAIN driver • Send or print with the LAN-Fax driver 	<p>User authentication has been rejected.</p>	<p>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.</p> <p>Confirm with the user administrator if using basic authentication.</p>
<p>Cannot perform the following:</p> <ul style="list-style-type: none"> • Print with the printer driver • Connect with the TWAIN driver • Send or print with the LAN-Fax driver 	<p>The encryption key specified in the driver does not match the machine's driver encryption key.</p>	<p>Specify the driver encryption key registered in the machine.</p> <p>See "Specifying a Driver Encryption Key".</p>
<p>Cannot perform the following:</p> <ul style="list-style-type: none"> • Print with the printer driver • Connect with the TWAIN driver • Send or print with the LAN-Fax driver 	<p>The SNMPv3 account, password, and encryption algorithm do not match settings specified on this machine.</p>	<p>Specify the account, password and the encryption algorithm of SNMPv3 registered in the machine using network connection tools.</p>
<p>Cannot authenticate using the TWAIN driver.</p>	<p>Another user is logging on to the machine.</p>	<p>Wait for the user to log off.</p>
<p>Cannot authenticate using the TWAIN driver.</p>	<p>Authentication is taking time because of operating conditions.</p>	<p>Make sure the LDAP server setting is correct.</p> <p>Make sure the network settings are correct.</p>
<p>Cannot authenticate using the TWAIN driver.</p>	<p>Authentication is not possible while the machine is editing the Address Book data.</p>	<p>Wait until editing of the Address Book data is complete.</p>

Condition	Cause	Solution
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.	"Restrict Use of Simple Encryption" is not set correctly. Alternatively, "SSL/TLS" has been enabled although the required certificate is not installed in the computer.	Set "Restrict Use of Simple Encryption" to [On]. Alternatively, enable "SSL/TLS", install the server certificate in the machine, and then install the certificate in the computer. See "Setting the SSL/TLS Encryption Mode".
Cannot log on to the machine using [Document Server (MFP):Authentication/Encryption] in DeskTopBinder.	"Restrict Use of Simple Encryption" is not set correctly. Alternatively, "SSL/TLS" has been enabled although the required certificate is not installed in the computer.	Set "Restrict Use of Simple Encryption" to [On]. Alternatively, enable "SSL/TLS", install the server certificate in the machine, and then install the certificate in the computer. See "Setting the SSL/TLS Encryption Mode".
Cannot access the machine using ScanRouter EX Professional V3 / ScanRouter EX Enterprise V2.	"Restrict Use of Simple Encryption" is not set correctly. Alternatively, "SSL/TLS" has been enabled although the required certificate is not installed in the computer.	Set "Restrict Use of Simple Encryption" to [On]. Alternatively, enable "SSL/TLS", install the server certificate in the machine, and then install the certificate in the computer. See "Setting the SSL/TLS Encryption Mode".
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 off 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 off.

Condition	Cause	Solution
"Prg. Dest." does not appear on the fax or scanner screen for specifying destinations.	"Restrict Adding of User Destinations" is set to [Off] in "Restrict Use of Destinations" in "Extended Security", so only the user administrator can register destinations in the Address Book.	Registration must be done by the user administrator.
User authentication is enabled, yet stored files do not appear.	User authentication may have been disabled while [All Users] is not specified.	Re-enable user authentication, and then enable [All Users] for the files that did not appear. For details about enabling [All Users], see "Configuring Access Permissions for Stored Files".
User authentication is enabled, yet destinations specified using the machine do not appear.	User authentication may have been disabled while [All Users] is not specified.	Re-enable user authentication, and then enable [All Users] for the destinations that did not appear. For details about enabling [All Users], see "Protecting the Address Book".
Cannot print when user authentication has been specified.	User authentication may not be specified in the printer driver.	Specify user authentication in the printer driver. For details, see the printer driver Help.
If you try to interrupt a job while copying or scanning, an authentication screen appears.	With this machine, you can log off while copying or scanning. If you try to interrupt copying or scanning after logging off, 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 "Encrypt Address Book", the "Exit" message does not appear.	The hard disk may be faulty. The file may be corrupt.	Contact your service representative.

Reference

- p.180 "Specifying a Driver Encryption Key"
- p.190 "Setting the SSL/TLS Encryption Mode"

- p.105 "Configuring Access Permissions for Stored Files"
- p.127 "Protecting the Address Book"

10. Appendix

Supervisor Operations

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 on using the supervisor's user name and password, you cannot use normal functions or specify defaults.

Log on as the supervisor only to change an administrator's password.

★ Important

- The default login user name is "supervisor" and the login password is blank. We recommend changing the login user name and login password.
- When registering login user names and login passwords, you can specify up to 32 alphanumeric characters and symbols. Keep in mind that user names and passwords are case-sensitive.
- 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 on as the supervisor and delete an administrator's password or specify a new one.

Logging on as the Supervisor

If administrator authentication has been specified, log on using the supervisor login user name and login password. This section describes how to log on.

1. Press the [User Tools] key.
2. Press the [Login/Logout] key.
3. Press [Login].
4. Enter a login user name, and then press [OK].

When you assign the administrator for the first time, enter "supervisor".

5. Enter a login password, and then press [OK].

The message, "Authenticating... Please wait." appears.

Logging off as the Supervisor

If administrator authentication has been specified, be sure to log off after completing settings. This section describes how to log off after completing settings.

1. Press the [Login/Logout] key.
2. Press [Yes].

Changing the Supervisor

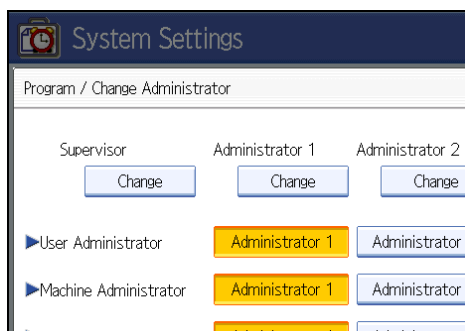
This section describes how to change the supervisor's login name and password.

To do this, you must enable the user administrator's privileges through the settings under "Administrator Authentication Management". For details, see "Specifying Administrator Privileges".

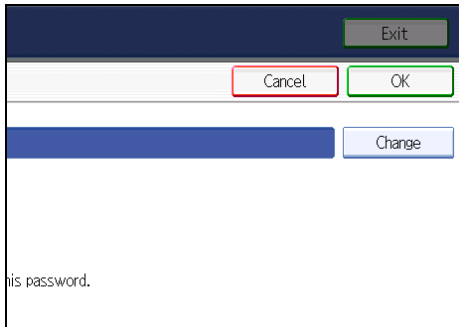
1. Press the [User Tools] key.
2. Press the [Login/Logout] key.
3. Log on as the supervisor.
You can log on in the same way as an administrator.
4. Press [System Settings].
5. Press [Administrator Tools].
6. Press [Program / Change Administrator].

If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

7. Under "Supervisor", press [Change].



8. Press [Change] for the login user name.



9. Enter the login user name, and then press [OK].

10. Press [Change] for the login password.

11. Enter the login password, and then press [OK].

12. If a password reentry screen appears, enter the login password, and then press [OK].

13. Press [OK] twice.

You will be automatically logged off.

14. Press the [User Tools] key.

Reference

- p.27 "Specifying Administrator Privileges"
- p.265 "Supervisor Operations"

Resetting the Administrator's Password

This section describes how to reset the administrators' passwords.

For details about logging on and logging off as the supervisor, see "Supervisor Operations".

1. Press the [User Tools] key.

2. Press the [Login/Logout] key.

3. Log on as the supervisor.

You can log on in the same way as an administrator.

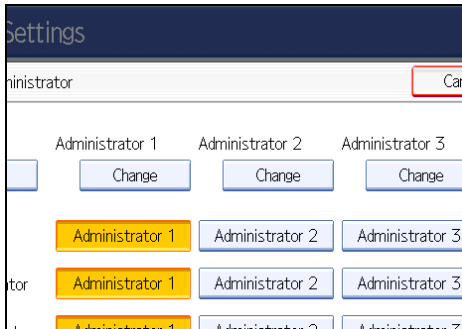
4. Press [System Settings].

5. Press [Administrator Tools].

6. Press [Program / Change Administrator].

If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

7. Press [Change] for the administrator you wish to reset.



8. Press [Change] for the login password.

9. Enter the login password, and then press [OK].

10. If a password reentry screen appears, enter the login password, and then press [OK].

11. Press [OK] twice.

You will be automatically logged off.

12. Press the [User Tools] key.

Reference

- p.265 "Supervisor Operations"

Machine Administrator Settings

The machine administrator settings that can be specified are as follows:

System Settings

The following settings can be specified.

General Features

All the settings can be specified.

Tray Paper Settings

All the settings can be specified.

Timer Settings

All the settings can be specified.

Interface Settings

The following settings can be specified.

- Parallel Interface

All the settings can be specified.

File Transfer

The following settings can be specified.

- Delivery Option
- Fax RX File Transmission
- Capture Server IPv4 Address
- SMTP Authentication

SMTP Authentication

User Name

E-mail Address

Password

Encryption

- POP before SMTP

Wait Time after Authent.

User Name

E-mail Address

Password

- Reception Protocol

- POP3 / IMAP4 Settings
 - Server Name
 - Encryption
 - Connection Test
- Administrator's E-mail Address
- Default User Name / Password (Send)
 - SMB User Name / SMB Password
 - FTP User Name / FTP Password
 - NCP User Name / NCP Password
- Program / Change / Delete E-mail Message
- Fax E-mail Account

Administrator Tools

The following settings can be specified.

- Address Book Management
 - Search
 - Switch Title
- Address Book: Program / Change / Delete Group
 - Search
 - Switch Title
- Display / Print Counter
 - Print Counter List
- Display / Clear / Print Counter per User
 - Print Counter List All Users
 - Print Counter List Per User
- User Authentication Management
 - You can specify which authentication to use.
 - You can also edit the settings for each function.
- Administrator Authentication Management
 - Machine Management
- Program / Change Administrator
 - Machine Administrator
 - You can change the user name and the full-control user's authority.
- Key Counter Management

- Extended Security
 - Restrict Display of User Information
 - Transfer to Fax Receiver
 - Authenticate Current Job
 - @Remote Service
 - Update Firmware
 - Change Firmware Structure
- Program / Change / Delete LDAP Server
 - Name
 - Server Name
 - Search Base
 - Port Number
 - Use Secure Connection (SSL)
 - Authentication
 - User Name
 - Password
 - Realm Name
 - Connection Test
 - Search Conditions
 - Search Options
- LDAP Search
- Program / Change / Delete Realm
- AOF (Always On)
- Capture Priority
- Capture: Delete All Unsent Files
- Capture: Ownership
- Capture: Public Priority
- Capture: Owner Defaults
- Service Mode Lock
- Auto Erase Memory Setting
- Erase All Memory
- Delete All Logs
- Transfer Log Setting

- Data Security for Copying
- Print Backup: Delete All Files
- Print Backup: Compression
- Print Backup: Default Format
- Print Backup: Default Resolution
- Fixed USB Port
- Machine Data Encryption Settings

Note

- The "Capture Server IPv4 Address" setting is available only if the optional File Format Converter is installed.
- The "Data Security for Copying" setting is available only if the optional Copy Data Security Unit is installed.
- "Machine Data Encryption Settings" are available only if the optional HDD Encryption Unit is installed.
- The following settings are available only if the optional File Format Converter is installed: "Capture Priority", "Capture: Delete All Unsent Files", "Capture: Ownership", "Capture: Public Priority", "Capture: Owner Defaults", "Print Backup: Delete All Files", "Print Backup: Delete All Files", "Print Backup: Compression", "Print Backup: Default User Name", "Print Backup: Default Format", "Print Backup: Default Resolution".
- "Auto Erase Memory Setting" and the "Erase All Memory" setting are available only if the optional Data Overwrite Security Unit is installed.

Copier / Document Server Features

The following settings can be specified.

General Features

All the settings can be specified.

Reproduction Ratio

All the settings can be specified.

Edit

All the settings can be specified.

Stamp

All the settings can be specified.

Input / Output

All the settings can be specified.

Administrator Tools

All the settings can be specified.

Facsimile Features

The following settings can be specified.

General Settings

All the settings can be specified.

Scan Settings

All the settings can be specified.

Send Settings

The following settings can be specified.

- Program / Change / Delete Standard Message
- Backup File TX Setting

Reception Settings

The following settings can be specified.

- Switch Reception Mode
- Program Special Sender
- Program Special Sender: Print List
- Forwarding
- Reception File Setting
- SMTP RX File Delivery Settings
- 2 Sided Print
- Checkered Mark
- Centre Mark
- Print Reception Time
- Reception File Print Quantity
- Paper Tray
- Specify Tray for Lines
- Folder Transfer Result Report
- Memory Lock Reception

Initial Settings

The following settings can be specified.

- Parameter Setting

- Parameter Setting: Print List
- Program Closed Network Code
- Program Memory Lock ID
- Internet Fax Setting
- Select Dial/Push Phone
- Program Fax Information
- Menu Protect
- E-mail Setting
- Folder Setting

Printer Features

The following settings can be specified.

List / Test Print

All the settings can be specified.

Maintenance

The following settings can be specified.

- Menu Protect
- List / Test Print Lock
- Reset IPDS Fonts

System

The following settings can be specified.

- Print Error Report
- Auto Continue
- Memory Overflow
- Job Separation
- Rotate by 180 Degrees
- Initial Print Job List
- Print Compressed Data
- Memory Usage
- Duplex
- Copies
- Blank Page Print
- Edge Smoothing

- Toner Saving
- Spool Image
- Reserved Job Waiting Time
- Printer Language
- Sub Paper Size
- Page Size
- Letterhead Setting
- Bypass Tray Setting Priority
- Edge to Edge Print
- Default Printer Language
- Tray Switching
- Extended Auto Tray Switching

Host Interface

All the settings can be specified.

PCL Menu

All the settings can be specified.

PS Menu

All the settings can be specified.

PDF Menu

All the settings can be specified.

IPDS Menu

All the settings can be specified.

Note

- The "Reset IPDS Fonts" setting is available only if the optional IPDS Unit is installed.
- PS or PDF menu settings are available only if the optional PostScript 3 Unit is required.
- IPDS menu settings are available only if the optional IPDS Unit is installed.

Scanner Features

The following settings can be specified.

General Settings

All the settings can be specified.

Scan Settings

All the settings can be specified.

Send Settings

The following settings can be specified.

- Compression (Black & White)
- Compression (Gray Scale/Full Color)
- High Compression PDF Level
- Insert Additional E-mail Info
- No. of Digits for Single Page Files
- Stored File E-mail Method
- Default E-mail Subject

Initial Settings

All the settings can be specified.

Settings via Web Image Monitor

The following settings can be specified.

Top Page

- Reset Device
- Reset Printer Job

Device Settings

- System
 - Spool Printing
 - Protect Printer Display Panel
 - Print Priority
 - Function Reset Timer
 - Permit Firmware Update
 - Permit Firmware Structure Change
 - Display IP Address on Device Display Panel
 - Output Tray
 - Paper Tray Priority
 - Front Cover Sheet Tray
 - Back Cover Sheet Tray
 - Slip Sheet Tray

Designation Sheet 1 Tray

Designation Sheet 2 Tray

- Paper
 - All the settings can be specified.
- Date/Time
 - All the settings can be specified.
- Timer
 - All the settings can be specified.
- Logs
 - All the settings can be specified.
- Download Logs
- E-mail
 - All the settings can be specified.
- Auto E-mail Notification
 - All the settings can be specified.
- On-demand E-mail Notification
 - All the settings can be specified.
- File Transfer
 - All the settings can be specified.
- User Authentication Management
 - All the settings can be specified.
- Administrator Authentication Management
 - Machine Administrator Authentication
 - Available Settings for Machine Administrator
- Program/Change Administrator
 - You can specify the following administrator settings for the machine administrator.
 - Login User Name
 - Login Password
 - Encryption Password
- LDAP Server
 - All the settings can be specified.
- Firmware Update
 - All the settings can be specified.

- Program/Change Realm
All the settings can be specified.

Printer

- System
All the settings can be specified except the following.
Auto Delete Temporary Print Jobs
Auto Delete Stored Print Jobs
- Host Interface
All the settings can be specified.
- PCL Menu
All the settings can be specified.
- PS Menu
All the settings can be specified.
- PDF Menu
All the settings can be specified.
- Tray Parameters (PCL)
All the settings can be specified.
- Tray Parameters (PS)
All the settings can be specified.
- Virtual Printer Settings
All the settings can be specified.
- IPDS Form Settings
All the settings can be specified.
- Reset IPDS Fonts
All the settings can be specified.
- IPDS Job Capture Settings
All the settings can be specified.
- PDF Group Password
All the settings can be specified.
- PDF Fixed Password
All the settings can be specified.

Fax

- Initial Settings

All the settings can be specified.

- Send / Reception Settings

All the settings can be specified.

- Parameter Settings

All the settings can be specified.

Scanner

- General Settings

All the settings can be specified.

- Scan Settings

All the settings can be specified.

- Send Settings

All the settings can be specified except the following.

Max.E-mail Size

Divide & Send E-mail

- Initial Settings

All the settings can be specified.

- Default Settings for Normal Screens on Device

Store File

Preview

Scan Type

Resolution

Auto Density

Send File Type

- Default Settings for Simplified Screens on Device

All the settings can be specified.

Interface Settings

- USB

- Parallel Interface

Parallel Timing

Parallel Communication Speed

Selection Signal Status

Input Prime

Bidirectional Communication

Signal Control

Network

- SNMPv3

Security

- User Lockout Policy
- All the settings can be specified.

RC Gate

- Setup RC Gate
Request No.
- Update RC Gate Firmware
- RC Gate Proxy Server

Webpage

- Webpage
Download Help File

Extended Feature Settings

- Startup Settings
- Extended Feature Info
- Install
- Uninstall
- Change Allocation
- Administrator Tools
- Additional Program Startup Setting
- Install Additional Program
- Uninstall Additional Program
- Copy Extended Features
- Copy Card Save Data

Note

- The following settings are available only if the optional IPDS Unit is installed: "IPDS Form Settings", "Reset IPDS Fonts", and "IPDS Job Capture Settings".
- The following settings are available only if the optional PostScript 3 Unit is installed: "PS Menu", "PDF Menu", "Tray Parameters (PCL)", "Tray Parameters (PS)", "Virtual Printer Settings", "PDF Group Password", and "PDF Fixed Password".

Settings via SmartDeviceMonitor for Admin

The following settings can be specified.

Device Properties

- Reset Device
- Reset Current Job
- Reset All Jobs

User Management Tool

- Export User Statistics List
- Edit CSV File Format of the User Statistics List
- Open CSV File with Program
- Restrict Access To Device
- Find User

Network Administrator Settings

The network administrator settings that can be specified are as follows:

System Settings

The following settings can be specified.

Interface Settings

If DHCP is set to On, the settings that are automatically obtained via DHCP cannot be specified.

- Print List
- Network
All the settings can be specified.
- Wireless LAN
Communication Mode
SSID Setting
Ad-hoc Channel
Security Method
Restore Factory Defaults

File Transfer

- SMTP Server
Server Name
Port No.
Connection Test
- E-mail Communication Port
All the settings can be specified.
- E-mail Reception Interval
- Max. Reception E-mail Size
- E-mail Storage in Server
- Auto Specify Sender Name
- Scanner Resend Interval Time
- Number of Scanner Resends

Administrator Tools

- Address Book Management
Search

- Switch Title
- Address Book: Program / Change / Delete Group
 - Search
 - Switch Title
- Administrator Authentication Management
 - Network Management
- Program / Change Administrator
 - Network Administrator
 - You can specify the user name and change the full-control user's authority.
- Extended Security
 - Driver Encryption Key
 - Settings by SNMP V1 and V2
 - Restrict Use of Simple Encryption
- Network Security Level

 **Note**

- The "Wireless LAN" setting is available only if the wireless LAN interface is installed.

Facsimile Features

The following settings can be specified.

Send Settings

- Max. E-mail Size

Initial Settings

- Enable H.323
- Enable SIP
- H.323 Settings
- SIP Settings
- Program / Change / Delete Gateway

10

Printer Features

The following settings can be specified.

System

- Print Compressed Data

Scanner Features

The following settings can be specified.

Send Settings

- Max. E-mail Size
- Divide & Send E-mail

Settings via Web Image Monitor

The following settings can be specified.

Device Settings

- System
 - Device Name
 - Comment
 - Location
- E-mail
 - Reception
 - SMTP
 - E-mail Communication Port
- Auto E-mail Notification
 - You can select groups to notify.
- Administrator Authentication Management
 - Network Administrator Authentication
 - Available Settings for Network Administrator
- Program/Change Administrator
 - You can specify the following administrator settings for the network administrator.
 - Login User Name
 - Login Password
 - Encryption Password

Printer

- System
 - Print Compressed Data

Fax

- Send / Reception Settings

Maximum E-mail Size

E-mail Size

- IP-Fax Settings
All the settings can be specified.
- IP-Fax Gateway Settings
All the settings can be specified.

Scanner

- Send Settings
Max. E-mail Size
Divide & Send E-mail

Interface Settings

- Ethernet Security
- Ethernet Speed
- Wireless LAN Settings
LAN Type
Communication Mode
SSID
Channel
Security Method
WEP Settings
WPA Settings
- Bluetooth
Operation Mode

Network

- IPv4
All the settings can be specified.
- IPv6
All the settings can be specified.
- NetWare
All the settings can be specified.
- AppleTalk
All the settings can be specified.
- SMB

All the settings can be specified.

- SNMP

All the settings can be specified.

- SNMPv3

All the settings can be specified.

- SSDP

All the settings can be specified.

- Bonjour

All the settings can be specified.

Security

- Network Security

All the settings can be specified.

- Access Control

All the settings can be specified.

- IPP Authentication

All the settings can be specified.

- SSL/TLS

All the settings can be specified.

- ssh

All the settings can be specified.

- Site Certificate

All the settings can be specified.

- Device Certificate

All the settings can be specified.

- IPsec

All the settings can be specified.

- IEEE 802.1X (WPA/WPA2)

All the settings can be specified.

- S/MIME

All the settings can be specified.

Webpage

All the settings can be specified.

Note

- "Wireless LAN Settings" are available only if the wireless LAN interface is installed.
- The "Bluetooth" setting is available only if the Bluetooth interface is installed.

Settings via SmartDeviceMonitor for Admin

The following settings can be specified.

NIB Setup Tool

All the settings can be specified.

File Administrator Settings

The file administrator settings that can be specified are as follows:

System Settings

The following settings can be specified.

Administrator Tools

- Address Book Management
 - Search
 - Switch Title
- Address Book: Program / Change / Delete Group
 - Search
 - Switch Title
- Administrator Authentication Management
 - File Management
- Program / Change Administrator
 - File Administrator
- Extended Security
 - Enhance File Protection
- Auto Delete File in Document Server
- Delete All Files in Document Server

Facsimile Features

The following settings can be specified.

Reception Settings

- Stored Reception File User Setting

Printer Features

The following settings can be specified.

Maintenance

- Delete All Temporary Print Jobs

- Delete All Stored Print Jobs

System

- Auto Delete Temporary Print Jobs
- Auto Delete Stored Print Jobs

Settings via Web Image Monitor

The following settings can be specified.

Document Server

All the settings can be specified.

Printer: Print Jobs

The file administrator can Edit/Delete the Print Job List and Unlock the print job.

Device Settings

- Auto E-mail Notification
You can select groups to notify.
- Administrator Authentication Management
File Administrator Authentication
Available Settings for File Administrator
- Program/Change Administrator
You can specify the following administrator settings for the file administrator.
Login User Name
Login Password
Encryption Password

Printer

- System
Auto Delete Temporary Print Jobs
Auto Delete Stored Print Jobs

Webpage

- Webpage
Download Help File

User Administrator Settings

The user administrator settings that can be specified are as follows:

System Settings

The following settings can be specified.

Administrator Tools

- Address Book Management
- Address Book: Program / Change / Delete Group
- Address Book: Change Order
- Print Address Book: Destination List
- Address Book: Edit Title
- Address Book: Switch Title
- Back Up / Restore Address Book
- Data Carry-over Setting for Address Book Auto-program
- Display / Clear / Print Counter per User
 - Clear All Users
 - Clear Per User
- Administrator Authentication Management
 - User Management
- Program / Change Administrator
 - User Administrator
- Extended Security
 - Encrypt Address Book
 - Encryption Key
 - Restrict Use of Destinations
 - Restrict Adding of User Destinations
 - Password Policy

Settings via Web Image Monitor

The following settings can be specified.

Address Book

All the settings can be specified.

Device Settings

- Auto E-mail Notification
You can select groups to notify.
- Administrator Authentication Management
User Administrator Authentication
Available Settings for User Administrator
- Program/Change Administrator
You can specify the following administrator settings for the user administrator.
Login User Name
Login Password
Encryption Password

Webpage

- Webpage
Download Help File

Settings via SmartDeviceMonitor for Admin

The following settings can be specified.

Address Management Tool

All the settings can be specified.

User Management Tool

- Export User Statistics List
- Edit CSV File Format of the User Statistics List
- Open CSV File with Program
- Export User Information
- Import User Information
- Restrict Access To Device
- Find User
- Add New User
- Delete User
- User Properties
User Code

Name

Document Server File Permissions

The authorities for using the files stored in Document Server are as follows.

The authority designations in the list indicate users with the following authorities.

- Read-only
This is a user assigned "Read-only" authority.
- Edit
This is a user assigned "Edit" authority.
- Edit / Delete
This is a user assigned "Edit / Delete" authority.
- Full Control
This is a user granted full control.
- Owner
This is a user who can store files in the machine and authorize other users to view, edit, or delete those files.
- File Administrator
This is the file administrator.

A =Granted authority to operate.

- =Not granted authority to operate.

Settings	Read-only	Edit	Edit / Delete	Full Control	Owner	File Admin.
Viewing Details About Stored Files	A	A	A	A	A *1	A
Viewing Thumbnails	A	A	A	A	A *1	A
Print/Transmission	A	A	A	A	A *1	-
Changing Information About Stored Files	-	A	A	A	A *1	-
Deleting Files	-	-	A	A	A *1	A
Specifying File Password	-	-	-	-	A	A
Specifying Permissions for Users/Groups	-	-	-	A	A	A

Settings	Read-only	Edit	Edit / Delete	Full Control	Owner	File Admin.
Unlocking Files	-	-	-	-	-	A

* 1 The owner can change the authorities for these settings as necessary.

The Privilege for User Account Settings in the Address Book

The authorities for using the Address Book are as follows:

The authority designations in the list indicate users with the following authorities.

- Abbreviations in the table heads

Read-only (User) = This is a user assigned "Read-only" authority.

Edit (User) = This is a user assigned "Edit" authority.

Edit / Delete (User) = This is a user assigned "Edit / Delete" authority.

User Admin. = This is the user administrator.

Registered User = This is a user that has personal information registered in the Address Book and has a login password and user name.

Full Control = This is a user granted full control.

- Abbreviations in the table columns

R/W (Read and Write) = Both reading and modifying the setting are available.

R (Read) = Reading only.

N/A (Not Applicable) = Neither reading nor modifying the setting is available.

Tab Name: Names

Settings	Read-only (User)	Edit (User)	Edit / Delete (User)	Full Control	Registered User	User Admin.
Registration No.	R	R/W	R/W	R/W	R/W	R/W
Key Display	R	R/W	R/W	R/W	R/W	R/W
Name	R	R/W	R/W	R/W	R/W	R/W
Select Title	R	R/W	R/W	R/W	R/W	R/W

Tab Name: Auth. Info

Settings	Read-only (User)	Edit (User)	Edit / Delete (User)	Full Control	Registered User	User Admin.
User Code	N/A	N/A	N/A	N/A	N/A	R/W

Settings	Read-only (User)	Edit (User)	Edit / Delete (User)	Full Control	Registered User	User Admin.
Login User Name	N/A	N/A	N/A	N/A	R	R/W
Login Password	N/A	N/A	N/A	N/A	R/W* ¹	R/W* ¹
SMTP Authentication	N/A	N/A	N/A	N/A	R/W* ¹	R/W* ¹
Folder Authentication	R	R/W* ¹	R/W* ¹	R/W* ¹	R/W* ¹	R/W* ¹
LDAP Authentication	N/A	N/A	N/A	N/A	R/W* ¹	R/W* ¹
Available Functions	N/A	N/A	N/A	N/A	R	R/W

*1 The password for "Login Password", "SMTP Authentication", or "LDAP Authentication" can be entered or changed but not displayed.

Tab Name: Protection

Settings	Read-only (User)	Edit (User)	Edit / Delete (User)	Full Control	Registered User	User Admin.
Use Name as	R	R/W	R/W	R/W	R/W	R/W
Protection Code	N/A	N/A	N/A	R/W* ²	R/W* ²	R/W* ²
Protection Object	N/A	R/W	R/W	R/W	R/W	R/W
Protect Destination: Permissions for Users/Groups	N/A	N/A	N/A	R/W	R/W	R/W
Protect File(s): Permissions for Users / Groups	N/A	N/A	N/A	R/W	R/W	R/W

*2 The code for "Protection Code" can be entered or changed but not displayed.

Tab Name: Fax. Dest

Settings	Read-only (User)	Edit (User)	Edit / Delete (User)	Full Control	Registered User	User Admin.
Fax Destination	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

Tab Name: E-mail

Settings	Read-only (User)	Edit (User)	Edit / Delete (User)	Full Control	Registered User	User Admin.
E-mail Address	R	R/W	R/W	R/W	R/W	R/W
Use E-mail Address for	R	R/W	R/W	R/W	R/W	R/W
Send via SMTP Server	R	R/W	R/W	R/W	R/W	R/W

Tab Name: Folder

Settings	Read-only (User)	Edit (User)	Edit / Delete (User)	Full Control	Registered User	User Admin.
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

Settings	Read-only (User)	Edit (User)	Edit / Delete (User)	Full Control	Registered User	User Admin.
NCP: Connection Type	R	R/W	R/W	R/W	R/W	R/W

User Settings - Control Panel Settings

This section explains which functions and system settings are available to users when administrator authentication is specified. The administrator's configuration of Menu Protect and Available Settings determines which functions and system settings are available to users. If user authentication is specified, system settings and functions are available to authorized users only, who must log on to access them.

Copier / Document Server Features

When administrator authentication is enabled, the administrator's configuration of Menu Protect determines which functions and settings are available to users.

User privileges are as follows:

- Abbreviations in the table columns

R/W (Read and Write) = Both reading and modifying the setting are available.

R (Read) = Reading only.

N/A (Not Applicable) = Neither reading nor modifying the setting is available.

When [Menu Protect] is set to [Off], all the following settings can be viewed and modified.

General Features

Settings	Level 1	Level 2
Auto Image Density Priority	R	R
Original Photo Type Priority	R	R
Original Type Display	R	R
Paper Display	R	R
Original Orientation in Duplex Mode	R	R
Copy Orientation in Duplex Mode	R	R
Max. Copy Quantity	R	R
Auto Tray Switching	R	R
Alert Sound: Original left on Exposure Glass	R	R
Job End Call	R	R
Switch Original Counter Display	R	R
Customize Function: Copier	R/W	R
Customize Function: Document Server Storage	R/W	R
Customize Function: Document Server Print	R/W	R

Reproduction Ratio

Settings	Level 1	Level 2
Shortcut Reduce/Enlarge	R	R
Reproduction Ratio	R	R
Reduce/Enlarge Ratio Priority	R	R
Ratio for Create Margin	R	R

Edit

Settings	Level 1	Level 2
Front Margin: Left / Right	R	R
Back Margin: Left / Right	R	R
Front Margin: Top / Bottom	R	R
Back Margin: Top / Bottom	R	R
1 Sided → 2 Sided Auto Margin: T to T	R	R
1 Sided → 2 Sided Auto Margin: T to B	R	R
Erase Border Width	R	R
Erase Original Shadow in Combine	R/W	R
Erase Center Width	R	R
Front Cover Copy in Combine	R/W	R
Copy Order in Combine	R/W	R
Orientation: Booklet, Magazine	R/W	R
Copy on Designating Page in Combine	R/W	R
Image Repeat Separation Line	R/W	R
Double Copies Separation Line	R/W	R
Separation Line in Combine	R/W	R
Copy Back Cover	R/W	R

Stamp

Background Numbering

Settings	Level 1	Level 2
Size	R/W	R
Density	R/W	R

Preset Stamp

Settings	Level 1	Level 2
Stamp Language	R/W	R
Stamp Priority	R	R
Stamp Format: COPY	R/W	R
Stamp Format: URGENT	R/W	R
Stamp Format: PRIORITY	R/W	R
Stamp Format: For Your Info.	R/W	R
Stamp Format: PRELIMINARY	R/W	R
Stamp Format: For Internal Use Only	R/W	R
Stamp Format: CONFIDENTIAL	R/W	R
Stamp Format: DRAFT	R/W	R

10

If you select Level 1 Stamp Format, you can only specify "Adjust Stamp Position".

User Stamp

Settings	Level 1	Level 2
Program / Delete Stamp	R/W	R
Stamp Format: 1	R/W	R
Stamp Format: 2	R/W	R
Stamp Format: 3	R/W	R
Stamp Format: 4	R/W	R

Date Stamp

Settings	Level 1	Level 2
Format	R	R
Font	R/W	R
Size	R/W	R
Superimpose	R/W	R
Stamp Setting	R/W	R

If you select Level 1 in Stamp Setting, you can only specify "Adjust Stamp Position".

Page Numbering

Settings	Level 1	Level 2
Stamp Format	R	R
Font	R/W	R
Size	R/W	R
Duplex Back Page Stamping Position	R/W	R
Page Numbering in Combine	R/W	R
Stamp on Designating Slip Sheet	R/W	R
Stamp Position: P1, P2...	R/W	R
Stamp Position: 1/5, 2/5...	R/W	R
Stamp Position: -1-, -2-...	R/W	R
Stamp Position: P.1, P.2...	R/W	R
Stamp Position: 1, 2...	R/W	R
Stamp Position: 1-1, 1-2...	R/W	R
Superimpose	R/W	R
Page Numbering Initial Letter	R/W	R

If you select Level 1 in Stamp Position, you can only specify "Adjust Stamp Position".

Stamp Text

Settings	Level 1	Level 2
Font	R/W	R
Size	R/W	R
Superimpose	R/W	R
Stamp Setting	R/W	R

Input / Output

Settings	Level 1	Level 2
Switch to Batch	R/W	R
SADF Auto Reset	R	R
Rotate Sort: Auto Paper Continue	R	R
Copy Eject Face Method in Glass Mode	R	R
Copy Eject Face Method in Bypass Mode	R	R
Memory Full Auto Scan Restart	R	R
Letterhead Setting	R	R
Staple Position	R/W	R
Punch Type	R/W	R
Simplified Screen: Finishing Types	R/W	R

Note

- The default for Menu Protect is [Level 2].
- Settings that are not in the list can only be viewed, regardless of the menu protect level setting.

Printer Functions

When administrator authentication is enabled, the administrator's configuration of Menu Protect determines which functions and settings are available to users.

User privileges are as follows:

- Abbreviations in the table columns
 - R/W (Read and Write) = Both reading and modifying the setting are available.
 - R (Read) = Reading only.
 - N/A (Not Applicable) = Neither reading nor modifying the setting is available.

When [Menu Protect] is set to [Off], all the following settings can be viewed and modified.

Normal Printer Screen

Functions	Level 1	Level 2
Print Jobs	R/W	R/W
Spooling Job List	R/W	R/W

Note

- The default for Menu Protect is [Level 2].
- Settings that are not in the list can only be viewed, regardless of the menu protect level setting.

Printer Features

When administrator authentication is enabled, the administrator's configuration of Menu Protect determines which functions and settings are available to users.

User privileges are as follows:

- Abbreviations in the table columns

R/W (Read and Write) = Both reading and modifying the setting are available.

R (Read) = Reading only.

N/A (Not Applicable) = Neither reading nor modifying the setting is available.

When [Menu Protect] is set to [Off], all the following settings can be viewed and modified.

List / Test Print

Settings	Level 1	Level 2
Multiple Lists	R/W	R/W
Configuration Page	R/W	R/W
Error Log	R/W	R/W
Menu List	R/W	R/W
IPDS Font List	R/W	R/W
PCL Configuration / Font Page	R/W	R/W
PS Configuration / Font Page	R/W	R/W
PDF Configuration / Font Page	R/W	R/W
Hex Dump	R/W	R/W

The "IPDS Font List" can be printed only if the optional IPDS Unit is installed.

The "PS Configuration / Font Page" and the "PDF Configuration / Font Page" can be printed only if the optional PostScript 3 Unit is installed.

System

Settings	Level 1	Level 2
Print Error Report	R	R
Auto Continue	R	R

Settings	Level 1	Level 2
Memory Overflow	R	R
Job Separation	R	R
Rotate by 180 Degrees	R	R
Auto Delete Temporary Print Jobs	R	R
Auto Delete Stored Print Jobs	R	R
Initial Print Job List	R	R
Print Compressed Data	R	R
Memory Usage	R	R
Duplex	R	R
Copies	R	R
Blank Page Print	R	R
Edge Smoothing	R	R
Toner Saving	R	R
Spool Image	R	R
Reserved Job Waiting Time	R	R
Printer Language	R	R
Sub Paper Size	R	R
Page Size	R/W	R
Letterhead Setting	R	R
Bypass Tray Setting Priority	R	R
Edge to Edge Print	R	R
Default Printer Language	R	R
Tray Switching	R	R
Extended Auto Tray Switching	R	R

Host Interface

Settings	Level 1	Level 2
I/O Buffer	R	R
I/O Timeout	R	R

PCL Menu

Settings	Level 1	Level 2
Orientation	R	R
Form Lines	R	R
Font Source	R	R
Font Number	R	R
Point Size	R	R
Font Pitch	R	R
Symbol Set	R	R
Courier Font	R	R
Extend A4 Width	R	R
Append CR to LF	R	R
Resolution	R	R

PS Menu

Settings	Level 1	Level 2
Job Timeout	R	R
Wait Timeout	R	R
Data Format	R	R
Resolution	R	R
Orientation Auto Detect	R	R

PS menu settings are available only if the optional PostScript 3 Unit is installed.

PDF Menu

Settings	Level 1	Level 2
Change PDF Password	R	R
PDF Group Password	R	R
Resolution	R	R
Orientation Auto Detect	R	R

PDF menu settings are available only if the optional PostScript 3 Unit is installed.

IPDS Menu

Settings	Level 1	Level 2
Tray Form	R/W	R
Emulation Mode	R/W	R
Print Mode	R/W	R
Default Code Page	R/W	R
Default FGID	R/W	R
Characters Per Inch	R/W	R
Valid Printable Area Check	R/W	R
Page	R/W	R
Edge to Edge	R/W	R
Font Substitution	R/W	R
Caching	R/W	R
Font Capture	R/W	R
Resolution	R/W	R
Graphic Character String	R/W	R
Bar Code	R/W	R
Box Draw	R/W	R

Settings	Level 1	Level 2
Color Simulation	R/W	R
Text Color Simulation	R/W	R
Suppress Staple Count Nacks	R/W	R
Suppress Punch Nacks	R/W	R
Tray Mapping	R/W	R
Corner Staple Angle	R/W	R
Offset	R/W	R
Default Punch Pattern	R/W	R

IPDS menu settings are available only if the optional IPDS Unit is installed.

Note

- The default for Menu Protect is [Level 2].
- Settings that are not in the list can only be viewed, regardless of the menu protect level setting.

Scanner Features

When administrator authentication is enabled, the administrator's configuration of Menu Protect determines which functions and settings are available to users.

User privileges are as follows:

- Abbreviations in the table columns
 - R/W (Read and Write) = Both reading and modifying the setting are available.
 - R (Read) = Reading only.
 - N/A (Not Applicable) = Neither reading nor modifying the setting is available.

When [Menu Protect] is set to [Off], all the following settings can be viewed and modified.

General Settings

Settings	Level 1	Level 2
Switch Title	R	R
Update Delivery Server Destination List	R/W	R
Search Destination	R	R
TWAIN Standby Time	R	R
Destination List Display Priority 1	R	R
Destination List Display Priority 2	R	R
Print & Delete Scanner Journal	R	R
Print Scanner Journal	N/A	N/A
Delete Scanner Journal	N/A	N/A

Scan Settings

Settings	Level 1	Level 2
A.C.S. Sensitivity Level	R	R
Wait Time for Next Orig.: Exposure Glass	R	R
Wait Time for Next Original(s): SADF	R	R
Background Density of ADS (Full Color)	R	R

Send Settings

Settings	Level 1	Level 2
Compression (Black & White)	R/W	R
Compression (Gray Scale / Full Color)	R/W	R
High Compression PDF Level	R/W	R
Insert Additional E-mail Info	R/W	R
No. of Digits for Single Page Files	R/W	R
Stored File E-mail Method	R/W	R
Default E-mail Subject	R	R

Note

- The default for Menu Protect is [Level 2].
- Settings that are not in the list can only be viewed, regardless of the menu protect level setting.

Facsimile Features

When administrator authentication is specified, the administrator's configuration of Menu Protect determines which functions and settings are available to users. If user authentication is specified, functions and settings are available to authorized users only, who must log in to access them.

The following settings can be specified by someone who is not an administrator.

- Abbreviations in the table columns
R/W (Read and Write) = Both reading and modifying the setting are available.
R (Read) = Reading only.
N/A (Not Applicable) = Neither reading nor modifying the setting is available.

Note

- Settings that are not in the list can only be viewed, regardless of the menu protect level setting.

The default for [Menu Protect] is [Off].

General Settings

Settings	Level 1	Level 2
Quick Operation key 1-3	R/W	R
Switch Title	R/W	R
Search Destination	R/W	R
Adjust Sound Volume	R/W	R
Box Setting	R	N/A
Box Setting: Print List	R/W	N/A
On Hook Mode Release Time	R/W	R

Scan Settings

Settings	Level 1	Level 2
Program / Change / Delete Scan Size	R/W	R

Send Settings

Settings	Level 1	Level 2
Max. E-mail Size	R	R

Settings	Level 1	Level 2
Program / Change / Delete Standard Message	R	R
Backup File TX Setting	R	R

Reception Settings

Settings	Level 1	Level 2
Switch Reception Mode	R	R
Program Special Sender	N/A	N/A
Program Special Sender: Print List	N/A	N/A
Forwarding	R	R
Reception File Setting	R	R
Stored Reception File User Setting	R	R
SMTP RX File Delivery Settings	R	R
2 Sided Print	R/W	R
Checkered Mark	R/W	R
Centre Mark	R/W	R
Print Reception Time	R/W	R
Reception File Print Quantity	R/W	R
Paper Tray	R/W	R
Specify Tray for Lines	R/W	R
Folder Transfer Result Report	R	R
Memory Lock Reception	R	R

Initial Settings

Settings	Level 1	Level 2
Parameter Setting	R	R
Parameter Setting: Print List	R/W	N/A

Settings	Level 1	Level 2
Program Closed Network Code	R	N/A
Program Memory Lock ID	R	N/A
Internet Fax Setting	R	R
Select Dial / Push Phone	R	R
Program Fax Information	R	R
Enable H.323	R	R
Enable SIP	R	R
H.323 Settings	R	R
SIP Settings	R	R
Program / Change / Delete Gateway	R	R
E-mail Setting	R	R
Folder Setting	R	R

System Settings

When administrator authentication is enabled, the administrator's configuration of Available Settings determines which system settings are available to users. If user authentication is specified, no settings are accessible to unauthorized users or authorized users before logging in.

User privileges are as follows:

- Abbreviations in the table heads

Not Specified = Authorized user when "Available Settings" have not been specified.

Specified = Authorized user when "Available Settings" have been specified.

- Abbreviations in the table columns

R/W (Read and Write) = Both reading and modifying the setting are available.

R (Read) = Reading only.

N/A (Not Applicable) = Neither reading nor modifying the setting is available.

General Features

Settings	Not Specified	Specified
Program / Change / Delete User Text	R/W	R
Panel Key Sound	R/W	R
Warm-up Beeper	R/W	R
Copy Count Display	R/W	R
Function Priority	R/W	R
Print Priority	R/W	R
Function Reset Timer	R/W	R
Interleave Print	R/W	R
Output: Copier	R/W	R
Output: Document Server	R/W	R
Output: Facsimile	R/W	R
Output: Printer	R/W	R
ADF Original Table Elevation	R/W	R

Settings	Not Specified	Specified
System Status / Job List Display Time	R/W	R
Time Interval between Printing Jobs	R/W	R
Key Repeat	R/W	R
Z-fold Position	R/W	R
Half Fold Position	R/W	R
Letter Fold-out Position	R/W	R
Letter Fold-in Position	R/W	R
Double Parallel Fold Position	R/W	R
Gate Fold Position	R/W	R

The following settings are available only if the optional Multi-Folding Unit is installed: "Z-fold Position", "Half Fold Position", "Letter Fold-out Position", "Letter Fold-in Position", "Double Parallel Fold Position", and "Gate Fold Position".

Tray Paper Settings

Settings	Not Specified	Specified
Paper Tray Priority: Copier	R/W	R
Paper Tray Priority: Facsimile	R/W	R
Paper Tray Priority: Printer	R/W	R
Tray Paper Size: Tray 2-3	R/W	R
Printer Bypass Paper Size	R/W	R
Paper Type: Bypass Tray	R/W	R
Paper Type: Tray 1-3	R/W	R
Paper Type: LCT	R/W	R
Front Cover Sheet Tray	R/W	R
Back Cover Sheet Tray	R/W	R

Settings	Not Specified	Specified
Slip Sheet Tray	R/W	R
Designation Sheet 1 Tray	R/W	R
Designation Sheet 2 Tray	R/W	R

The " Paper Type: LCT" setting is available only if the optional large capacity tray is installed.

Timer Settings

Settings	Not Specified	Specified
Auto Off Timer	R/W	R
Energy Saver Timer	R/W	R
Panel Off Timer	R/W	R
System Auto Reset Timer	R/W	R
Copier / Document Server Auto Reset Timer	R/W	R
Facsimile Auto Reset Timer	R/W	R
Printer Auto Reset Timer	R/W	R
Scanner Auto Reset Timer	R/W	R
Set Date	R/W	R
Set Time	R/W	R
Auto Logout Timer	R/W	R
Weekly Timer Code	R/W	R
Weekly Timer: Monday-Sunday	R/W	R

Interface Settings

Settings	Not Specified	Specified
Print List	R/W	N/A

Network

Settings	Not Specified	Specified
Machine IPv4 Address	R/W	R
IPv4 Gateway Address	R/W	R
Machine IPv6 Address	R/W	R
IPv6 Gateway Address	R/W	R
IPv6 Stateless Address Autoconfiguration	R/W	R
DNS Configuration	R/W	R
DDNS Configuration	R/W	R
IPsec	R/W	R
Domain Name	R/W	R
WINS Configuration	R/W	R
Effective Protocol	R/W	R
NCP Delivery Protocol	R/W	R
NW Frame Type	R/W	R
SMB Computer Name	R/W	R
SMB Work Group	R/W	R
Ethernet Speed	R/W	R
IEEE 802.1X Authentication for Ethernet	R/W	R
Restore IEEE 802.1X Authentication to Defaults	R/W	N/A
LAN Type	R/W	R
Ping Command	R/W	R
Permit SNMPv3 Communication	R/W	R
Permit SSL / TLS Communication	R/W	R
Host Name	R/W	R

Settings	Not Specified	Specified
Machine Name	R/W	R

If you set "Machine IPv4 Address", "Machine IPv6 Address", "DNS Configuration", "Domain Name", or "WINS Configuration" to "Auto-Obtain (DHCP)", you can only display the settings.

Parallel Interface

Settings	Not Specified	Specified
Parallel Timing	R/W	R
Parallel Communication Speed	R/W	R
Selection Signal Status	R/W	R
Input Prime	R/W	R
Bidirectional Communication	R/W	R
Signal Control	R/W	R

"Parallel Interface" settings are available only if the optional IEEE 1284 interface unit is installed.

Wireless LAN

Settings	Not Specified	Specified
Communication Mode	R/W	R
SSID Setting	R/W	R
Ad-hoc Channel	R/W	R
Security Method	R/W	R
Restore Factory Defaults	R/W	N/A

"Wireless LAN" settings are available only if the optional Wireless LAN interface unit is installed.

File Transfer

Settings	Not Specified	Specified
Delivery Option	R/W	R
Capture Server IPv4 Address	R/W	R
Fax RX File Transmission	R/W	R
SMTP Server	R/W	R
SMTP Authentication	R/W	R
POP before SMTP	R/W	R
Reception Protocol	R/W	R
POP3 / IMAP4 Settings	R/W	R
Administrator's E-mail Address	R/W	R
E-mail Communication Port	R/W	R
E-mail Reception Interval	R/W	R
Max. Reception E-mail Size	R/W	R
E-mail Storage in Server	R/W	R
Default User Name / Password (Send)	R/W	R
Program / Change / Delete E-mail Message	R/W	R/W
Auto Specify Sender Name	R/W	R
Fax E-mail Account	R/W	R
Scanner Resend Interval Time	R/W	R
Number of Scanner Resends	R/W	R

The settings made for "Main Delivery Server IPv4 Address" and "Sub Delivery Server IPv4 Address" in "Delivery Option" can only be displayed, not changed.

The "Capture Server IPv4 Address" setting is available only if the optional File Format Converter is installed.

The passwords for "SMTP Authentication" and "Default User Name / Password (Send)" can be entered or changed but not displayed.

Administrator Tools

Settings	Not Specified	Specified
Address Book Management	R/W	R/W
Address Book: Program / Change / Delete Group	R/W	R/W
Address Book: Change Order	R/W	N/A
Print Address Book: Destination List	R/W	R/W
Address Book: Edit Title	R/W	N/A
Address Book: Switch Title	R/W	N/A
Back Up / Restore Address Book	R/W	N/A
Data Carry-over Setting for Address Book Auto-program	R/W	R
Display / Print Counter	R/W	R/W
Display / Clear / Print Counter per User	R/W	N/A
User Authentication Management	R/W	R
Administrator Authentication Management	R/W	N/A
Key Counter Management	R/W	R
Extended Security	R/W	R
Auto Delete File in Document Server	R/W	R
Delete All Files in Document Server	R/W	N/A
Program / Change / Delete LDAP Server	R/W	R
LDAP Search	R/W	R
Program / Change / Delete Realm	R/W	R
AOF (Always On)	R/W	R
Capture Priority	R/W	R
Capture: Delete All Unsent Files	R/W	R
Capture: Ownership	R/W	R

Settings	Not Specified	Specified
Capture: Public Priority	R/W	R
Capture: Owner Defaults	R/W	R
Service Mode Lock	R/W	R
Auto Erase Memory Setting	R/W	R
Erase All Memory	R/W	R
Delete All Logs	R/W	N/A
Transfer Log Setting	R/W	N/A
Data Security for Copying	R/W	R
Print Backup: Delete All Files	R/W	R
Print Backup: Compression	R/W	R
Print Backup: Default Format	R/W	R
Print Backup: Default Resolution	R/W	R
Fixed USB Port	R/W	R
Data Security for Copying	R/W	R

The password for "Program / Change / Delete LDAP Server" can be entered or changed but not displayed.

The following settings are available only if the File Format Converter is installed: "Capture Priority", "Capture: Delete All Unsent Files", "Capture: Ownership", "Capture: Public Priority", "Capture: Owner Defaults", "Print Backup: Delete All Files", "Print Backup: Delete All Files", "Print Backup: Compression", "Print Backup: Default User Name", "Print Backup: Default Format", "Print Backup: Default Resolution".

The "Data Security for Copying" setting is available only if the Copy Data Security Unit is installed.

The "Auto Erase Memory Setting" and "Erase All Memory" settings are available only if the optional DataOverwriteSecurity Unit is installed.

User Settings - Web Image Monitor Settings

This section displays the user settings that can be specified on Web Image Monitor when user authentication is specified. Settings that can be specified by the user vary according to the menu protect level and available settings specifications.

Device Settings

The settings available to the user depend on whether or not administrator authentication is enabled.

If administrator authentication is enabled, the settings available to the user depend on whether or not "Available Settings" has been specified.

User privileges are as follows:

- Abbreviations in the table heads

Not Specified = Authorized user when "Available Settings" have not been specified.

Specified = Authorized user when "Available Settings" have been specified.

- Abbreviations in the table columns

R/W (Read and Write) = Both reading and modifying the setting are available.

R (Read) = Reading only.

N/A (Not Applicable) = Neither reading nor modifying the setting is available.

System

Settings	Not Specified	Specified
General Settings : Device Name	R/W	R
General Settings : Comment	R/W	R
General Settings : Location	R/W	R
General Settings : Spool Printing	R/W	R
Output Tray : Copier	R/W	R
Output Tray : Fax	R/W	R
Output Tray : Printer	R/W	R
Output Tray : Document Server	R/W	R
Paper Tray Priority : Copier	R/W	R
Paper Tray Priority : Fax	R/W	R
Paper Tray Priority : Printer	R/W	R
Front Cover Sheet Tray : Tray to set	R/W	R
Front Cover Sheet Tray : Apply Duplex	R/W	R

Settings	Not Specified	Specified
Front Cover Sheet Tray : Display Time	R/W	R
Back Cover Sheet Tray : Tray to set	R/W	R
Back Cover Sheet Tray : Apply Duplex	R/W	R
Back Cover Sheet Tray : Display Time	R/W	R
Slip Sheet Tray : Tray to set	R/W	R
Slip Sheet Tray : Apply Duplex	R/W	R
Slip Sheet Tray : Display Time	R/W	R
Designation Sheet 1-2 Tray: Tray to set	R/W	R
Designation Sheet 1-2 Tray: Apply Duplex	R/W	R
Designation Sheet 1-2 Tray: Display Time	R/W	R

Paper

Settings	Not Specified	Specified
Tray 1 : Paper Type	R/W	R
Tray 1 : Paper Thickness	R/W	R
Tray 1: Apply Auto Paper Select	R/W	R
Tray 1: Apply Duplex	R/W	R
Tray 2: Paper Size	R/W	R
Tray 2: Custom Paper Size	R/W	R
Tray 2: Paper Type	R/W	R
Tray 2: Paper Thickness	R/W	R
Tray 2: Apply Auto Paper Select	R/W	R
Tray 2: Apply Duplex	R/W	R
Tray 3: Paper Size	R/W	R

Settings	Not Specified	Specified
Tray 3: Custom Paper Size	R/W	R
Tray 3: Paper Type	R/W	R
Tray 3: Paper Thickness	R/W	R
Tray 3: Apply Auto Paper Select	R/W	R
Tray 3: Apply Duplex	R/W	R
Large Capacity Tray : Paper Type	R/W	R
Large Capacity Tray: Paper Thickness	R/W	R
Large Capacity Tray: Apply Auto Paper Select	R/W	R
Large Capacity Tray: Apply Duplex	R/W	R
Bypass Tray : Paper Size	R/W	R
Bypass Tray : Custom Paper Size	R/W	R
Bypass Tray : Paper Type	R/W	R
Bypass Tray : Paper Thickness	R/W	R

Date/Time

Settings	Not Specified	Specified
Set Date	R/W	R
Set Time	R/W	R
SNTP Server Name	R/W	R
SNTP Polling Interval	R/W	R
Time Zone	R/W	R

Timer

Settings	Not Specified	Specified
Auto Off Timer	R/W	R
Energy Saver Timer	R/W	R
Panel Off Timer	R/W	R
System Auto Reset Timer	R/W	R
Copier/Document Server Auto Reset Timer	R/W	R
Facsimile Auto Reset Timer	R/W	R
Scanner Auto Reset Timer	R/W	R
Printer Auto Reset Timer	R/W	R
Auto Logout Timer	R/W	R
Weekly Timer Code	R/W	R
Weekly Timer: Monday Sunday	R/W	R

Logs

Settings	Not Specified	Specified
Collect Job Logs	R/W	R
Job Log Collect Level	R/W	R
Collect Access Logs	R/W	R
Access Log Collect Level	R/W	R
Transfer Logs	R	R
Encrypt Logs	R/W	R
Classification Code	R/W	R
Delete All Logs	R/W	N/A

E-mail

Settings	Not Specified	Specified
Administrator E-mail Address	R/W	R
Reception Protocol	R/W	R
E-mail Reception Interval	R/W	R
Max. Reception E-mail Size	R/W	R
E-mail Storage in Server	R/W	R
SMTP Server Name	R/W	R
SMTP Port No.	R/W	R
SMTP Authentication	R/W	R
SMTP Auth. E-mail Address	R/W	R
SMTP Auth. User Name	R/W	N/A
SMTP Auth. Password	R/W	N/A
SMTP Auth. Encryption	R/W	R
POP before SMTP	R/W	R
POP E-mail Address	R/W	R
POP User Name	R/W	N/A
POP Password	R/W	N/A
Timeout setting after POP Auth.	R/W	R
POP3/IMAP4 Server Name	R/W	R
POP3/IMAP4 Encryption	R/W	R
POP3 Reception Port No.	R/W	R
IMAP4 Reception Port No.	R/W	R
Fax E-mail Address	R/W	R
Receive Fax E-mail	R/W	N/A

Settings	Not Specified	Specified
Fax E-mail User Name	R/W	N/A
Fax E-mail Password	R/W	N/A
E-mail Notification E-mail Address	R/W	R
Receive E-mail Notification	R/W	N/A
E-mail Notification User Name	R/W	N/A
E-mail Notification Password	R/W	N/A

Auto E-mail Notification

Settings	Not Specified	Specified
Groups to Notify: Address List	R/W	R/W

File Transfer

Settings	Not Specified	Specified
SMB User Name	R/W	N/A
SMB Password	R/W	N/A
FTP User Name	R/W	N/A
FTP Password	R/W	N/A
NCP User Name	R/W	N/A
NCP Password	R/W	N/A

The passwords for "SMB Password", "FTP Password", and "NCP Password" can be entered or changed but not displayed.

User Authentication Management

Settings	Not Specified	Specified
User Authentication Management	R/W	R
User Code Authentication - Printer Job Authentication Settings	R/W	R
User Code Authentication - User Code Authentication Settings	R/W	R
Basic Authentication - Printer Job Authentication Settings	R/W	R
Basic Authentication - Basic Authentication Settings	R/W	R
Windows Authentication - Printer Job Authentication Settings	R/W	R
Windows Authentication - Windows Authentication Settings	R/W	R
Windows Authentication - Group Settings for Windows Authentication	R/W	R
LDAP Authentication - Printer Job Authentication Settings	R/W	R
LDAP Authentication - LDAP Authentication Settings	R/W	R
Integration Server Authentication - Printer Job Authentication Settings	R/W	R
Integration Server Authentication - Integration Server Authentication Settings	R/W	R
Integration Server Authentication - Group Settings for Integration Server Authentication	R/W	R

10

LDAP Server

Settings	Not Specified	Specified
LDAP Search	R/W	N/A
Program/Change/Delete	R/W	N/A

Printer

If you have enabled administrator authentication, the menu protection setting determines which functions and settings are available.

User privileges are as follows:

- Abbreviations in the table columns

R/W (Read and Write) = Both reading and modifying the setting are available.

R (Read) = Reading only.

N/A (Not Applicable) = Neither reading nor modifying the setting is available.

When [Menu Protect] is set to [Off], all the following settings can be viewed and modified.

Printer Basic Settings

System

Settings	Level 1	Level 2
Print Error Report	R	R
Auto Continue	R	R
Memory Overflow	R	R
Job Separation	R	R
Auto Delete Temporary Print Jobs	R	R
Auto Delete Stored Print Jobs	R	R
Initial Print Job List	R	R
Rotate by 180 Degrees	R	R
Print Compressed Data	R	R
Memory Usage	R	R
Duplex	R	R
Copies	R	R
Blank Page Print	R	R
Edge Smoothing	R	R
Toner Saving	R	R

Settings	Level 1	Level 2
Spool Image	R	R
Reserved Job Waiting Time	R	R
Printer Language	R	R
Sub Paper Size	R	R
Page Size	R/W	R
Letterhead Setting	R	R
Bypass Tray Setting Priority	R	R
Edge to Edge Print	R	R
Default Printer Language	R	R
Tray Switching	R	R
Extended Auto Tray Switching	R	R
Virtual Printer	R	R

Host Interface

Settings	Level 1	Level 2
I/O Buffer	R	R
I/O Timeout	R	R

PCL Menu

Settings	Level 1	Level 2
Orientation	R	R
Form Lines	R	R
Font Source	R	R
Font Number	R	R
Point Size	R	R
Font Pitch	R	R

Settings	Level 1	Level 2
Symbol Set	R	R
Courier Font	R	R
Extend A4 Width	R	R
Append CR to LF	R	R
Resolution	R	R

PS Menu

Settings	Level 1	Level 2
Job Timeout	R	R
Wait Timeout	R	R
Data Format	R	R
Resolution	R	R
Orientation Auto Detect	R	R

PS menu settings are available only if the optional PostScript 3 Unit is installed.

PDF Menu

Settings	Level 1	Level 2
Resolution	R	R
Orientation Auto Detect	R	R

PDF menu settings are available only if the optional PostScript 3 Unit is installed.

IPDS Menu

Settings	Level 1	Level 2
Emulation Mode	R/W	R
Print Mode	R/W	R
Default Code Page	R/W	R
Default FGID	R/W	R

Settings	Level 1	Level 2
Characters Per Inch	R/W	R
Valid Printable Area Check	R/W	R
Page	R/W	R
Edge to Edge	R/W	R
Font Substitution	R/W	R
Caching	R/W	R
Font Capture	R/W	R
Resolution	R/W	R
Graphic Character String	R/W	R
Bar Code	R/W	R
Box Draw	R/W	R
Color Simulation	R/W	R
Text Color Simulation	R/W	R
Suppress Staple Count Nacks	R/W	R
Suppress Punch Nacks	R/W	R
Tray Mapping	R/W	R
IPDS Form Allocation	R/W	R
Corner Staple Angle	R/W	R
Offset	R/W	R
Default Punch Pattern	R/W	R

IPDS menu settings are available only if the optional IPDS Unit is installed.

Virtual Printer Settings

System

Settings	Level 1	Level 2
Print Error Report	R	R

Settings	Level 1	Level 2
Job Separation	R	R
Rotate by 180 Degrees	R	R
Memory Usage	R	R
Duplex	R	R
Copies	R	R
Blank Page Print	R	R
Edge Smoothing	R	R
Toner Saving	R	R
Sub Paper Size	R	R
Input Tray	R/W	R/W
Page Size	R/W	R
Paper Type	R/W	R/W
Output Tray	R/W	R/W
Letterhead Setting	R	R
Edge to Edge Print	R	R

PCL Menu

Settings	Level 1	Level 2
Orientation	R	R
Form Lines	R	R
Font Source	R	R
Font Number	R	R
Point Size	R	R
Font Pitch	R	R
Symbol Set	R	R

Settings	Level 1	Level 2
Courier Font	R	R
Extend A4 Width	R	R
Append CR to LF	R	R
Resolution	R	R

PS Menu

Settings	Level 1	Level 2
Job Timeout	R	R
Wait Timeout	R	R
Data Format	R	R
Resolution	R	R
Orientation Auto Detect	R	R

PS menu settings are available only if the optional PostScript 3 Unit is installed.

PDF Menu

Settings	Level 1	Level 2
Resolution	R	R
Orientation Auto Detect	R	R

PDF menu settings are available only if the optional PostScript 3 Unit is installed.

RHPP Settings

Settings	Level 1	Level 2
After Errors Are Solved	R/W	R/W
When Errors Occur	R/W	R/W
RHPP Timeout	R/W	R/W
After Misfed Paper Is Removed	R/W	R/W

IPDS Form Settings

Settings	Level 1	Level 2
Form Name	R	R
Description	R	R
Media Size	R	R
Custom Size Units	R	R
Cross Feed Dimension	R	R
Feed Dimension	R	R
Media Type	R	R
Media Orientation	R	R
Media Type Component ID	R	R
Edge Sensitive	R	R
Side Sensitive	R	R
Simplex Only	R	R
Simplex Adjust Cross Feed	R	R
Simplex Adjust Feed	R	R
Front Duplex Adjust Cross Feed	R	R
Front Duplex Adjust Feed	R	R
Back Duplex Adjust Cross Feed	R	R
Back Duplex Adjust Feed	R	R

IPDS Form Settings are available only if the optional IPDS Unit is installed.

PDF Temporary Password

Settings	Level 1	Level 2
PDF Temporary Password	R/W	R/W
Confirm Password	R/W	R/W

"PDF Temporary Password" settings are available only if the optional PostScript 3 Unit is installed.

PDF Group Password

Settings	Level 1	Level 2
Current PDF Group Password	N/A	N/A
New PDF Group Password	N/A	N/A
Confirm PDF Group Password	N/A	N/A

"PDF Group Password" settings are available only if the optional PostScript 3 Unit is installed.

PDF Fixed Password

Settings	Level 1	Level 2
Current PDF Fixed Password	N/A	N/A
New PDF Fixed Password	N/A	N/A
Confirm Password	N/A	N/A

"PDF Fixed Password" settings are available only if the optional PostScript 3 Unit is installed.

↓ Note

- The default for Menu Protect is [Level 2].
- Settings that are not in the list can only be viewed, regardless of the menu protect level setting.

Scanner

If you have enabled administrator authentication, the menu protection setting determines which functions and settings are available.

User privileges are as follows:

- Abbreviations in the table columns
 - R/W (Read and Write) = Both reading and modifying the setting are available.
 - R (Read) = Reading only.
 - N/A (Not Applicable) = Neither reading nor modifying the setting is available.

When [Menu Protect] is set to [Off], all the following settings can be viewed and modified.

General Settings

Settings	Level 1	Level 2
Switch Title	R	R
Search Destination	R	R
TWAIN Standby Time	R	R
Destination List Display Priority 1	R	R
Destination List Display Priority 2	R	R
Print & Delete Scanner Journal	R	R

Scan Settings

Settings	Level 1	Level 2
A.C.S. Sensitivity Level	R	R
Wait Time for Next Original(s): Exposure Glass	R	R
Wait Time for Next Original(s): SADF	R	R
Background Density of ADS (Full Color)	R	R

Send Settings

Settings	Level 1	Level 2
Compression (Black & White)	R/W	R

Settings	Level 1	Level 2
Compression (Gray Scale/Full Color)	R/W	R
High Compression PDF Level	R/W	R
Max. E-mail Size	R	R
Divide & Send E-mail	R	R
Insert Additional E-mail Info	R/W	R
No. of Digits for Single Page Files	R/W	R
Stored File E-mail Method	R/W	R
Default E-mail Subject	R	R

Default Settings for Normal Screens on Device

Settings	Level 1	Level 2
Store File	R	R
Preview	R	R
Scan Type	R	R
Resolution	R	R
Auto Density	R	R
Dropout Color	R	R
Send File Type	R	R

10

Default Settings for Simplified Screens on Device

Settings	Level 1	Level 2
Scan Type	R	R
Resolution	R	R
Send File Type	R	R

↓ Note

- The default for Menu Protect is [Level 2].

- Settings that are not in the list can only be viewed, regardless of the menu protect level setting.

Fax

If you have specified administrator authentication, the available functions and settings depend on the menu protect setting.

The following settings can be specified by someone who is not an administrator.

- Abbreviations in the table columns

R/W (Read and Write) = Both reading and modifying the setting are available.

R (Read) = Reading only.

N/A (Not Applicable) = Neither reading nor modifying the setting is available.

The default for [Menu Protect] is [Off].

Initial Settings

Settings	Level 1	Level 2
Closed Network Code	N/A	N/A
Internet Fax	N/A	N/A
Program Memory Lock ID	N/A	N/A
Fax Information: Fax Header	N/A	N/A
Fax Information: Own Name	N/A	N/A
Fax Information: Own Fax Number	N/A	N/A
Select Dial/Push Phone	N/A	N/A

Send / Reception Settings

Settings	Level 1	Level 2
Maximum E-mail Size	N/A	N/A
Switch Reception Mode	N/A	N/A
SMTP RX File Delivery Settings	N/A	N/A
Duplex Print	N/A	N/A
Checkered Mark	N/A	N/A
Center Mark	N/A	N/A
Print Reception Time	N/A	N/A

Settings	Level 1	Level 2
Reception File Print Quantity	N/A	N/A
Paper Tray	N/A	N/A
Memory Lock Reception	N/A	N/A

IP-Fax Settings

Settings	Level 1	Level 2
Enable H.323	N/A	N/A
Enable IP-Fax Gatekeeper	N/A	N/A
Gatekeeper Address (Main)	N/A	N/A
Gatekeeper Address (Sub)	N/A	N/A
Own Fax No.	N/A	N/A
Enable SIP	N/A	N/A
Enable Server	N/A	N/A
User Name	N/A	N/A
Server IP Address: Proxy Server Addr. (Main)	N/A	N/A
Server IP Address: Proxy Server Addr. (Sub)	N/A	N/A
Server IP Address: Redirect Svr. Addr. (Main)	N/A	N/A
Server IP Address: Redirect Svr. Addr. (Sub)	N/A	N/A
Server IP Address: Registrar Address (Main)	N/A	N/A
Server IP Address: Registrar Address (Sub)	N/A	N/A
Digest Authentication	N/A	N/A

IP-Fax Gateway Settings

Settings	Level 1	Level 2
Prefix 1-50	N/A	N/A
Protocol 1-50	N/A	N/A

Settings	Level 1	Level 2
Gateway Address 1-50	N/A	N/A

Parameter Settings

Settings	Level 1	Level 2
Just Size Printing	N/A	N/A
Combine 2 Originals	N/A	N/A
Convert to PDF When Transferring to Folder	N/A	N/A
Journal	N/A	N/A
Immediate Transmission Result Report	N/A	N/A
Communication Result Report	N/A	N/A
Memory Storage Report	N/A	N/A
SEP Code RX Result Report	N/A	N/A
SEP Code RX Reserve Report	N/A	N/A
Confidential File Report	N/A	N/A
LAN-Fax Result Report	N/A	N/A
Inclusion of Part of Image	N/A	N/A
Error E-mail Notification	N/A	N/A
Display Network Errors	N/A	N/A
Journal Notification by E-mail	N/A	N/A
Response to RX Notice Request	N/A	N/A
Select Destination Type Priority	N/A	N/A

Interface

The settings available to the user depend on whether or not administrator authentication is enabled.

If administrator authentication is enabled, the settings available to the user depend on whether or not "Available Settings" has been specified.

User privileges are as follows:

- Abbreviations in the table heads

Not Specified = Authorized user when "Available Settings" have not been specified.

Specified = Authorized user when "Available Settings" have been specified.

- Abbreviations in the table columns

R/W (Read and Write) = Both reading and modifying the setting are available.

R (Read) = Reading only.

N/A (Not Applicable) = Neither reading nor modifying the setting is available.

Interface Settings

Settings	Not Specified	Specified
Ethernet : Ethernet Security	R/W	R
Ethernet : Ethernet Speed	R/W	R
Bluetooth : Bluetooth	R/W	R
Bluetooth : Operation Mode	R/W	R
USB	R/W	R
Parallel Interface	R/W	R
Parallel Timing	R/W	R
Parallel Communication Speed	R/W	R
Selection Signal Status	R/W	R
Input Prime	R/W	R
Bidirectional Communication	R/W	R

The following settings are available only if the optional IEEE 1284 interface board is installed: "Parallel Interface", "Parallel Timing", "Parallel Communication Speed", "Selection Signal Status", "Input Prime", and "Bidirectional Communication".

The "Bluetooth" setting is available only if the Bluetooth interface unit is installed.

Wireless LAN Settings

Settings	Not Specified	Specified
LAN Type	R/W	N/A
Communication Mode	R/W	R
SSID	R/W	R
Channel	R/W	R
Security Method	R/W	R
WEP Authentication	R/W	N/A
WEP Key Number	R/W	R
WEP Key	R/W	R
WPA Encryption Method	R/W	R
WPA Authentication Method	R/W	R
WPA-PSK/WPA2-PSK	R/W	R

"Wireless LAN Settings" are available only if the Wireless LAN interface unit is installed.

Network

The settings available to the user depend on whether or not administrator authentication is enabled.

If administrator authentication is enabled, the settings available to the user depend on whether or not "Available Settings" has been specified.

User privileges are as follows:

- Abbreviations in the table heads

Not Specified = Authorized user when "Available Settings" have not been specified.

Specified = Authorized user when "Available Settings" have been specified.

- Abbreviations in the table columns

R/W (Read and Write) = Both reading and modifying the setting are available.

R (Read) = Reading only.

N/A (Not Applicable) = Neither reading nor modifying the setting is available.

IPv4

Settings	Not Specified	Specified
Host Name	R/W	R
DHCP	R/W	R
Domain Name	R/W	R
IPv4 Address	R/W	R
Subnet Mask	R/W	R
DDNS	R/W	R
WINS	R/W	R
Primary WINS Server	R/W	R
Secondary WINS Server	R/W	R
Scope ID	R/W	R
Default Gateway Address	R/W	R
DNS Server	R/W	R
LPR	R/W	R
RSH/RCP	R/W	R

Settings	Not Specified	Specified
DIPRINT	R/W	R
FTP	R/W	R
sftp	R/W	R
WSD (Device)	R/W	R
WSD (Printer)	R/W	R
WSD (Scanner)	R/W	R
IPP	R/W	R
WSD (Printer)/IPP Timeout	R/W	R
IPDS	R/W	R
IPDS Port Number	R/W	R
RHPP	R/W	R

IPv6

Settings	Not Specified	Specified
IPv6	R/W	R
Host Name	R/W	R
Domain Name	R/W	R
Stateless Address	R/W	R
Manual Configuration Address	R/W	R
DHCPv6-lite	R/W	R
DDNS	R/W	R
Default Gateway Address	R/W	R
DNS Server	R/W	R
LPR	R/W	R

Settings	Not Specified	Specified
RSH/RCP	R/W	R
DIPRINT	R/W	R
FTP	R/W	R
sftp	R/W	R
WSD (Device)	R/W	R
WSD (Printer)	R/W	R
WSD (Scanner)	R/W	R
IPP	R/W	R
WSD (Printer)/IPP Timeout	R/W	R
RHPP	R/W	R

NetWare

Settings	Not Specified	Specified
NetWare	R/W	R
Print Server Name	R/W	R
Logon Mode	R/W	R
File Server Name	R/W	R
NDS Tree	R/W	N/A
NDS Context Name	R/W	R
Operation Mode	R/W	R
Remote Printer No.	R/W	N/A
Job Timeout	R/W	N/A
Frame Type	R/W	R
Print Server Protocol	R/W	R

Settings	Not Specified	Specified
NCP Delivery Protocol	R/W	R

AppleTalk

Settings	Not Specified	Specified
AppleTalk	R/W	R
Printer Name	R/W	R
Zone Name	R/W	R

SMB

Settings	Not Specified	Specified
SMB	R/W	R
Workgroup Name	R/W	R
Computer Name	R/W	R
Comment	R/W	R
Notify Print Completion	R/W	R

Bonjour

Settings	Not Specified	Specified
Bonjour	R/W	R
Computer Name	R/W	R
Location	R/W	R
DIPRINT	R/W	R
LPR	R/W	R
IPP	R/W	R

Webpage

The settings available to the user depend on whether or not administrator authentication is enabled.

If administrator authentication is enabled, the settings available to the user depend on whether or not "Available Settings" has been specified.

User privileges are as follows:

- Abbreviations in the table heads

Not Specified = Authorized user when "Available Settings" have not been specified.

Specified = Authorized user when "Available Settings" have been specified.

- Abbreviations in the table columns

R/W (Read and Write) = Both reading and modifying the setting are available.

R (Read) = Reading only.

N/A (Not Applicable) = Neither reading nor modifying the setting is available.

Webpage

Settings	Not Specified	Specified
Language 1	R/W	R
Language 2	R/W	R
URL1	R/W	R
URL2	R/W	R
Set Help URL Target	R/W	R
WSD/UPnP Setting	R/W	R
Download Help File	R/W	R/W

Functions That Require Options

The following functions require certain options and additional functions.

- Hard Disk overwrite erase function
DataOverwriteSecurity Unit
- Data security for copying function
Copy Data Security Unit
- PDF Direct Print function
PostScript 3 Unit
- Hard Disk data encryption function
HDD Encryption Unit

Trademarks

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

Adobe, Acrobat, Acrobat Reader, PostScript, 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.

NetWare is a registered trademark of Novell, Inc.

UPnP™ is a trademark of the UPnP™ Implementers Corporation.

PCL® is a registered trademark of Hewlett-Packard Company.

Apple, AppleTalk, Bonjour, Macintosh, and Mac OS are trademarks of Apple Inc., registered in the U.S. and other countries.

Monotype is a registered trademark of Monotype Imaging, Inc.

Solaris is a trademark or registered trademark of Sun Microsystems, Inc. in the United States and other countries.

LINUX® is the registered trademark of Linus Torvalds in the U.S. and other countries.

RED HAT is a registered trademark of Red Hat, Inc.

PowerPC® is a trademark of International Business Machines Corporation in the United States, other countries, or both.

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 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

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® Enterprise

Microsoft® Windows Vista® Business

Microsoft® Windows Vista® Home Premium

Microsoft® Windows Vista® Home Basic

* 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

INDEX

A

Access Control.....	167
Access Permission.....	105
Address Book Access Permission.....	127
Address Book Privileges.....	295
Administrator.....	17
Administrator Authentication.....	17, 25, 27
Administrator Privileges.....	27
AH Protocol.....	195
AH Protocol + ESP Protocol.....	195
Authenticate Current Job.....	224
Authentication and Access Limits.....	16
authfree.....	218
Auto Erase Memory Setting.....	138
Auto Logout.....	88
Available Functions.....	152

B

Basic Authentication.....	46
---------------------------	----

C

Canceling Weekly Timer Code.....	229
Change Firmware Structure.....	225
Copier / Document Server Features.....	300
Creating the Device Certificate (Certificate Issued by a Certificate Authority).....	187

D

Data Security for Copying.....	94
Device Settings.....	325
Document Server File Permissions.....	293
Driver Encryption Key.....	180, 222

E

E-mail Encryption.....	119
Edit.....	293, 295
Edit / Delete.....	293, 295
Electronic Signature.....	121
Enabling/Disabling Protocols.....	168
Encrypt Address Book.....	222
Encrypting Data on the Hard Disk.....	131
Encrypting the Data in the Address Book.....	128
Encryption Key Auto Exchange / Manual Settings - Shared Settings.....	196

Encryption Key Auto Exchange Security Level.....	196
Encryption Key Auto Exchange Setting Items.....	198
Encryption Key Auto Exchange Settings Configuration Flow.....	204
Encryption Key Manual Settings Configuration Flow.....	209
Encryption Key Manual Settings Items.....	201
Encryption Technology.....	16
Enhance File Protection.....	223
Erase All Memory.....	142
Error Code.....	243
Error Message.....	241
ESP Protocol.....	194
Extended Security Functions.....	221

F

Facsimile Features.....	313
Fax.....	343
File Administrator.....	24, 293
File Administrator Settings.....	288
File Creator (Owner).....	17
Full Control.....	293, 295

G

Group Password for PDF files.....	181
Guarding Against Unauthorized Copying.....	93

H

Hard Disk Data Encryption Settings.....	131
How to read this manual.....	11

I

If User Authentication is Specified.....	83
Important.....	10
Installing the Device Certificate (Certificate Issued by a Certificate Authority).....	188
Integration Server Authentication.....	73
Interface.....	346
IP Address.....	11
IPP Authentication Password.....	183
IPsec.....	194
IPsec Settings.....	196
IPsec telnet Setting Commands.....	210

L

LDAP Authentication.....	65
LDAP Authentication - Operational Requirements for LDAP Authentication.....	65
Legal Prohibition.....	12
Locked Print.....	99
Log off (Administrator).....	34
Log on (Administrator).....	33
Login.....	17
Logout.....	17

M

Machine Administrator.....	24
Machine Administrator Settings.....	269
Menu Protect.....	145

N

Network Administrator.....	24
Network Administrator Settings.....	282
Network Security Level.....	176
Notice.....	10

O

Operational Issues.....	259
Overwriting Data on the Hard Disk.....	137
Owner.....	293

P

Password for Stored Files.....	105
Password Policy.....	225
Print & Delete Scanner Journal.....	227
Printer.....	332
Printer Functions.....	305
Printer Job Authentication.....	80
Printer Job Authentication Levels.....	80
Printer Job Types.....	81
Printing the Encryption Key.....	133

R

Read-only.....	293, 295
Registered User.....	17, 295
Registering the Administrator.....	30
Remote Service.....	225
Restrict Adding of User Destinations.....	222

Restrict Display of User Information.....	223
Restrict Use of Destinations.....	222
Restrict Use of Simple Encryption.....	223
Restricting Destinations.....	117

S

S/MIME.....	119
Scanner.....	340
Scanner Features.....	311
Security Functions.....	227
Self-Signed Certificate.....	186
Service Mode Lock.....	231
Settings by SNMP v1 and v2.....	223
SNMPv3.....	192
Specifying Login Details.....	51
Specifying Weekly Timer Code.....	228
SSL.....	189
SSL (Secure Sockets Layer).....	185
SSL / TLS Encryption.....	190
Stored RX File User Setting.....	227
Supervisor.....	24, 265
Symbols.....	11
System Settings.....	316

T

telnet.....	218
Transfer Log Setting.....	155
Transfer to Fax Receiver.....	224
Transmitted Passwords.....	180
Type of Administrator.....	145

U

Unauthorized Copy Prevention.....	93
Update Firmware.....	225
User.....	17, 37
User Administrator.....	295
User Administrator Settings.....	290
User Authentication.....	17, 38, 41
User Code Authentication.....	42
User Lockout Function.....	86
User Settings - Control Panel Settings.....	299
User Settings - Web Image Monitor Settings.....	324

W

Weekly Timer Code.....	228
Windows Authentication.....	53
Windows Authentication - Operational Requirements for Kerberos Authentication.....	53
Windows Authentication - Operational Requirements for NTLM Authentication.....	53
WSD scanner function.....	228

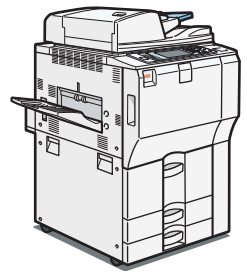
MEMO



Type for 9060/MP 6001/LD360/Aficio MP 6001
Type for 9070/MP 7001/LD370/Aficio MP 7001
Type for 9080/MP 8001/LD380/Aficio MP 8001
Type for 9090/MP 9001/LD390/Aficio MP 9001



PostScript 3 Supplement



-
- 1** Windows Configuration
 - 2** Mac OS Configuration
 - 3** Using PostScript 3
 - 4** Printer Utility for Mac
 - 5** Appendix

TABLE OF CONTENTS

Manuals for This Machine.....	5
Notice.....	7
Important.....	7
How to Read This Manual.....	8
Symbols.....	8
Notes.....	8
About IP Address.....	8
Laws and Regulations.....	9
Legal Prohibition.....	9

1. Windows Configuration

Using the DeskTop Binder-SmartDeviceMonitor for Client.....	11
Installing DeskTop Binder-SmartDeviceMonitor for Client.....	11
Installing the PostScript 3 Printer Driver (Windows 2000 - TCP/IP).....	12
Installing the PostScript 3 Printer Driver (Windows 2000 - IPP).....	13
Installing the PostScript 3 Printer Driver (Windows XP, Windows Server 2003 / 2003 R2 - TCP/IP).....	14
Installing the PostScript 3 Printer Driver (Windows XP, Windows Server 2003 / 2003 R2 - IPP).....	16
Installing the PostScript 3 Printer Driver (Windows Vista, Windows Server 2008 - TCP/IP).....	17
Installing the PostScript 3 Printer Driver (Windows Vista, Windows Server 2008 - IPP).....	19
Changing the Port Settings DeskTop Binder-SmartDeviceMonitor for Client.....	20
Using the Standard TCP/IP Port.....	22
Installing the PostScript 3 Printer Driver (Windows 2000).....	22
Installing the PostScript 3 Printer Driver (Windows XP, Windows Server 2003 / 2003 R2).....	23
Installing the PostScript 3 Printer Driver (Windows Vista, Windows Server 2008).....	24
Using the LPR Port.....	26
Installing the PostScript 3 Printer Driver (Windows 2000).....	26
Installing the PostScript 3 Printer Driver (Windows XP, Windows Server 2003 / 2003 R2).....	27
Installing the PostScript 3 Printer Driver (Windows Vista, Windows Server 2008).....	28
Using as the Windows Network Printer.....	30
Installing the PostScript 3 Printer Driver (Windows 2000).....	30
Installing the PostScript 3 Printer Driver (Windows XP, Windows Server 2003 / 2003 R2).....	31
Installing the PostScript 3 Printer Driver (Windows Vista, Windows Server 2008).....	32
Using the WSD port.....	33

Using as the NetWare Print Server / Remote Printer.....	35
When using the PostScript 3 Printer Driver.....	35
Installing the Printer Driver Using USB.....	36
Windows 2000 - USB.....	36
Windows XP, Windows Server 2003 / 2003 R2 - USB.....	37
Windows Vista, Windows Server 2008 - USB.....	38
Troubleshooting for using USB.....	39
Printing with Parallel Connection.....	40
Installing the PostScript 3 printer driver (Windows 2000).....	40
Installing the PostScript 3 Printer Driver (Windows XP, Windows Server 2003 / 2003 R2).....	41
Installing the PostScript 3 Printer Driver (Windows Vista, Windows Server 2008).....	42
Printing with Bluetooth Connection.....	44
Supported Profiles.....	44
Adding a Bluetooth Printer.....	44
If a Message Appears during Installation.....	47
Making Option Settings for the Printer.....	49
Setting Up the Printer Driver.....	50
Windows 2000 - Accessing the Printer.....	50
Windows XP, Windows Server 2003 / 2003 R2 - Accessing the Printer Properties.....	51
Windows Vista, Windows Server 2008 - Accessing the Printer Properties.....	53

2. Mac OS Configuration

Mac OS.....	55
Installing the PostScript 3 Printer Driver and PPD File.....	55
Setting Up PPD Files.....	56
Setting Up Options.....	56
Installing Adobe Type Manager.....	57
Installing Screen fonts.....	57
Changing to EtherTalk.....	58
Mac OS X.....	59
Installing the PPD Files.....	59
Setting Up the PPD File.....	59
Setting Up Options.....	60
Using USB Interface.....	61

Using Bonjour.....	61
Changing to EtherTalk.....	62
Configuring the Printer.....	64

3. Using PostScript 3

Setting Up Options.....	65
Printing a Document.....	67
Job Type.....	67
User Code.....	82
Paper Size.....	82
Fit to Paper.....	83
Input Slot.....	83
Resolution.....	84
Orientation.....	84
Rotate by 180 degrees.....	85
Copies.....	85
Orientation Override.....	85
Print Mode.....	86
Duplex Printing.....	87
Pages per Sheet.....	88
Pages per Sheet Layout.....	88
Draw Border.....	89
Collate.....	89
Paper Type.....	89
Destination Tray.....	90
Staple.....	90
Punch.....	91
Fold Type.....	92
Z-fold.....	93
Multi-sheet Fold.....	94
Reduce/Enlarge.....	94
Watermark.....	95
Watermark Text.....	96
Watermark Font.....	96

Watermark Size.....	96
Watermark Angle.....	97
Watermark Style.....	97
Dithering.....	97
Image Smoothing.....	98

4. Printer Utility for Mac

Installing Printer Utility for Mac.....	101
Starting Printer Utility for Mac.....	102
Mac OS.....	102
Mac OS X.....	102
Printer Utility for Mac Functions.....	103
Downloading PS Fonts.....	104
Displaying Printer's Fonts.....	104
Deleting Fonts.....	105
Initializing the Printer Disk.....	105
Page Setup.....	106
Printing Fonts Catalog.....	106
Printing Fonts Sample.....	106
Renaming the Printer.....	106
Restarting the Printer.....	107
Downloading PostScript Files.....	107
Selecting the Zone.....	108
Displaying the Printer Status.....	109
Launching the Dialogue Console.....	109

5. Appendix

Trademarks.....	111
INDEX	113

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.
- The printed and electronic versions of a manual have the same contents.
- 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.

About This Machine

Before using the machine, be sure to read the section of this manual entitled Safety Information.

This manual introduces the machine's various functions. It also explains the control panel, preparation procedures for using the machine, how to enter text, how to install the CD-ROMs provided, and how to replace paper, toner, staples, and other consumables.

Troubleshooting

Provides a guide for resolving common usage-related problems.

Copy and Document Server Reference

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

Facsimile Reference

Explains Facsimile functions and operations.

Printer Reference

Explains Printer functions and operations.

Scanner Reference

Explains Scanner functions and operations.

Network and System Settings Guide

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

Security Reference

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 "Setting Up the Machine", Security Reference.

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

PostScript 3 Supplement

Explains how to set up and use PostScript 3.

Other manuals

- UNIX Supplement
- Quick Reference Copy Guide
- Quick Reference Printer Guide
- Quick Reference Fax Guide
- Quick Reference Scanner Guide
- Manuals for DeskTopBinder Lite
 - DeskTopBinder Lite Setup Guide
 - DeskTopBinder Introduction Guide
 - Auto Document Link Guide

↓ Note

- Manuals provided are specific to machine types.
- 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.
- The following software products are referred to using general names:

Product Name	General name
DeskTopBinder Lite and DeskTopBinder Professional *1	DeskTopBinder

*1 Optional

Notice

Important

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.

For good copy quality, the supplier recommends that you use genuine toner from the supplier.

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

How to Read This Manual

Symbols

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 that appear on the machine's display panel.

[]

Indicates the names of keys on the machine's control panel.

Notes

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

Two kinds of size notation are employed in this manual.

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

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.

This machine comes in four models which vary in copy/print speed.

About IP Address

In this manual, "IP address" covers both IPv4 and IPv6 environments. Read the instructions that are relevant to the environment you are using.

Laws and Regulations

Legal Prohibition

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.



1. Windows Configuration

Using the DeskTop Binder-SmartDeviceMonitor for Client Port

1

Installing DeskTop Binder-SmartDeviceMonitor for Client

★ Important

- To install DeskTop Binder-SmartDeviceMonitor for Client under Windows 2000 / XP Professional / Vista and Windows Server 2003 / 2003 R2 / 2008, you must have an account that has Manage Printers permission. Log on as an Administrator.
 - Install DeskTop Binder-SmartDeviceMonitor for Client before installing the printer driver when using the DeskTop Binder-SmartDeviceMonitor for Client port.
1. Quit all applications currently running.
 2. Insert the CD-ROM into the CD-ROM drive.
The installer starts.
 3. Select an interface language, and then click [OK].
 4. Click [DeskTopBinder - SmartDeviceMonitor for Client].
 5. Select an interface language, and then click [Next >].
 6. The message to quit all other applications appears. Quit all applications, and then click [Next >].
 7. The software license agreement appears in the [License Agreement] dialog box. After reading through its contents, click [Yes].
 8. Click [Full install] or [Custom install].
[Full install] installs all required applications: DeskTopBinder Lite and SmartDeviceMonitor for Client.
[Custom install] installs selected applications.
 9. Follow the instructions on the display and click [Next >] to proceed to the next step.
 10. After the installation is completed, select one of the options to restart the computer either now or later, and click [Complete].
Restart the computer to complete installation.

Note

- Depending on your computer's operating system, the [AutoPlay] dialog box may appear. If this happens, click [Run SETUP.EXE]. If the [User Account Control] dialog box appears, click [Continue] to allow the auto play program to run.
- To stop installation of the selected software, click [Cancel] before installation is complete.
- Auto Run may not work with certain operating system settings. In that case, launch "Setup.exe" on the CD-ROM root directory.

Installing the PostScript 3 Printer Driver (Windows 2000 - TCP/IP)

★ Important

- **Installing this printer driver requires Administrators permission. Log on using an account that has Administrators permission.**

1. **Quit all applications currently running.**
2. **Insert the CD-ROM into the CD-ROM drive.**

The installer starts.

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

The printer driver with the selected language will be installed. The English printer driver is installed when the following language is selected: Suomi, Magyar, Cestina, Polski, Portugues, Russian, Catala, Turkce.

4. **Click [PostScript 3 Printer Driver].**

Add Printer Wizard starts.

5. **Click [Next >].**

6. **Click [Local printer], and then click [Next >].**

7. **Click [Create a new port:].**

8. **Click [DeskTop Binder - SmartDeviceMonitor], and then click [Next >].**

9. **Click [TCP/IP], and then click [Search].**

A list of machines using TCP/IP appears.

10. **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.

11. **Check that the name of the machine whose driver you want to install is selected, and then click [Next >].**

12. **Change the machine name if you want, and then click [Next >].**

Select the [Yes] check box to configure the machine as default.

13. Specify whether or not to share the machine, and then click [Next >].
14. Specify whether or not to print a test page, and then click [Next >].
15. Click [Finish].

The printer driver installation starts.

↓ Note

- A user code can be set after the printer driver installation. For information about user code, see the printer driver Help.
- Auto Run may not work with certain operating system settings. In that case, launch "Setup.exe" on the CD-ROM root directory.

Installing the PostScript 3 Printer Driver (Windows 2000 - IPP)

★ Important

- Installing this printer driver requires Administrators permission. Log on using an account that has Administrators permission.
1. Quit all applications currently running.
 2. Insert the CD-ROM into the CD-ROM drive.
The installer starts.
 3. Select an interface language, and then click [OK].
The printer driver with the selected language will be installed. The English printer driver is installed when the following language is selected: Suomi, Magyar, Cestina, Polski, Portugues, Russian, Catala, Turkce.
 4. Click [PostScript 3 Printer Driver].
Add Printer Wizard starts.
 5. Click [Next >].
 6. Click [Local printer attached to this computer], and then click [Next >].
 7. Click [Create a new port:].
 8. Click [DeskTop Binder - SmartDeviceMonitor], and then click [Next >].
 9. Click [IPP].
 10. In the [Printer URL] box, enter "http://(machine's IP address or host name)/printer" as the machine's address.
If the server authentication is issued, to enable SSL (a protocol for encrypted communication), enter "https://(machine's IP address or host name)/printer" (Internet Explorer 5.01, or a higher version must be installed).
(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 or host name/ipp" as the machine's address.

If the address is "192.168.001.010", you must enter it as "192.168.1.10" to connect to the machine.

- 11. Enter a name for identifying the machine in [IPP Port Name]. Use a name different from the name of any existing port.**

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

- 12. Click [Detailed Settings] to configure proxy server, the IPP user name and other settings. Specify the necessary settings, and then click [OK].**

For information about the settings, see DeskTop Binder-SmartDeviceMonitor for Client Help.

- 13. Click [OK].**

- 14. Check that the name of the machine whose driver you want to install is selected, and then click [Next >].**

- 15. Change the machine name if you want, and then click [Next >].**

Select the [Yes] check box to configure the machine as default.

- 16. Specify whether or not to share the machine, and then click [Next >].**

- 17. Specify whether or not to print a test page, and then click [Next >].**

- 18. Click [Finish].**

The printer driver installation starts.

Note

- A user code can be set after the printer driver installation. For information about user code, see the printer driver Help.
- Auto Run may not work with certain operating system settings. In that case, launch "Setup.exe" on the CD-ROM root directory.

Installing the PostScript 3 Printer Driver (Windows XP, Windows Server 2003 / 2003 R2 - TCP/IP)

Important

- Installing this printer driver requires Administrators permission. Log on using an account that has Administrators permission.
- You can install the printer driver from the CD-ROM provided with this machine or download it from the supplier's Web site.

- If your operating system is Windows XP Professional x64, Windows Server 2003 / 2003 R2 x64, you must download the printer driver from the manufacturer's Web site. Select this machine and the operating system you are using, and then download it.

1. Quit all applications currently running.

2. Insert the CD-ROM into the CD-ROM drive.

The installer starts.

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

The printer driver with the selected language will be installed. The English printer driver is installed when the following language is selected: Suomi, Magyar, Cestina, Polski, Portugues, Russian, Catala, Turkce.

4. Click [PostScript 3 Printer Driver].

Add Printer Wizard starts.

5. Click [Next >].

6. Click [Local printer attached to this computer.], and then click [Next >].

7. Click [Create a new port:].

8. Click [DeskTop Binder - SmartDeviceMonitor], and then click [Next >].

9. Click [TCP/IP], and then click [Search].

A list of machines using TCP/IP appears.

10. 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.

11. Check that the name of the machine whose driver you want to install is selected, and then click [Next >].

12. Change the machine name if you want, and then click [Next >].

Select the [Yes] check box to configure the machine as default.

13. Specify whether or not to share the machine, and then click [Next >].

14. Specify whether or not to print a test page, and then click [Next >].

15. Click [Finish].

The printer driver installation starts.

Note

- A user code can be set after the printer driver installation. For information about user code, see the printer driver Help.
- Auto Run may not work with certain operating system settings. In that case, launch "Setup.exe" on the CD-ROM root directory.

Installing the PostScript 3 Printer Driver (Windows XP, Windows Server 2003 / 2003 R2 - IPP)

1

★ Important

- Installing this printer driver requires Administrators permission. Log on using an account that has Administrators permission.
- You can install the printer driver from the CD-ROM provided with this machine or download it from the supplier's Web site.
- If your operating system is Windows XP Professional x64, Windows Server 2003 / 2003 R2 x64, you must download the printer driver from the manufacturer's Web site. Select this machine and the operating system you are using, and then download it.

1. Quit all applications currently running.

2. Insert the CD-ROM into the CD-ROM drive.

The installer starts.

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

The printer driver with the selected language will be installed. The English printer driver is installed when the following language is selected: Suomi, Magyar, Cestina, Polski, Portugues, Russian, Catala, Turkce.

4. Click [PostScript 3 Printer Driver].

Add Printer Wizard starts.

5. Click [Next >].

6. Click [Local printer attached to this computer.], and then click [Next >].

7. Click [Create a new port:].

8. Click [DeskTop Binder - SmartDeviceMonitor], and then click [Next >].

9. Click [IPP].

10. In the [Printer URL] box, enter "http://(machine's IP address or host name)/printer" as the machine's address.

If the server authentication is issued, to enable SSL (a protocol for encrypted communication), enter "https://(machine's IP address or host name)/printer" (Internet Explorer 5.01, or a higher version must be installed).

(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 or host name/ipp" as the machine's address.

If the address is "192.168.001.010", you must enter it as "192.168.1.10" to connect to the machine.

11. Enter a name for identifying the machine in [IPP Port Name]. Use a name different from the one of any existing port.

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

12. Click [Detailed Settings] to make necessary settings.

For information about the settings, see DeskTop Binder-SmartDeviceMonitor for Client Help.

13. Click [OK].

14. Check that the name of the printer driver you want to install is selected, and then click [OK].

15. Change the name of the machine if you want, and then click [Next >].

Select the [Yes] check box to configure the machine as default.

16. Specify whether or not to share the machine, and then click [Next >].

17. Specify whether or not to print a test page, and then click [Next >].

18. Click [Finish].

The printer driver installation starts.

↓ Note

- A user code can be set after the printer driver installation. For information about user code, see the printer driver Help.
- Auto Run may not work with certain operating system settings. In that case, launch "Setup.exe" on the CD-ROM root directory.

Installing the PostScript 3 Printer Driver (Windows Vista, Windows Server 2008 - TCP/IP)

★ Important

- Installing this printer driver requires Administrators permission. Log on using an account that has Administrators permission.
- You can install the printer driver from the CD-ROM provided with this machine or download it from the supplier's Web site.
- If your operating system is Windows Vista x64, Windows Server 2008 x64, you must download the printer driver from the manufacturer's Web site. Select this machine and the operating system you are using, and then download it.

1. Quit all applications currently running.
2. Insert the CD-ROM into the CD-ROM drive.

The installer starts.

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

The printer driver with the selected language will be installed. The English printer driver is installed when the following language is selected: Suomi, Magyar, Cestina, Polski, Portugues, Russian, Catala, Turkce.

4. Click [PostScript 3 Printer Driver].

Add Printer Wizard starts.

5. Click [Add a local printer].

6. Click [Create a new port:], and then select [DeskTop Binder - SmartDeviceMonitor] in [Type of port].

7. Click [Next >].

8. Click [TCP/IP], and then click [Search].

A list of printers using TCP/IP appears.

9. Select the printer you want to use, and then click [OK].

Only printers 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.

10. Select that the name of the machine whose driver you want to install is selected, and then click [Next >].

11. Change the machine name if you want, and then click [Next >].

Check the checkbox to configure the machine as default.

12. Specify whether or not to share the machine, and then click [Next >].

13. Specify whether or not to print a test page, and then click [Finish].

The printer driver installation starts.

Note

- Depending on your computer's operating system, the [AutoPlay] dialog box may appear. If this happens, click [Run SETUP.EXE]. If the [User Account Control] dialog box appears, click [Continue] to allow the auto play program to run.
- A user code can be set after the printer driver installation. For information about user code, see the printer driver Help.
- Auto Run may not work with certain operating system settings. In that case, launch "Setup.exe" on the CD-ROM root directory.

Installing the PostScript 3 Printer Driver (Windows Vista, Windows Server 2008 - IPP)

★ Important

- Installing this printer driver requires Administrators permission. Log on using an account that has Administrators permission.
- You can install the printer driver from the CD-ROM provided with this machine or download it from the supplier's Web site.
- If your operating system is Windows Vista x64, Windows Server 2008 x64, you must download the printer driver from the manufacturer's Web site. Select this machine and the operating system you are using, and then download it.

1. Quit all applications currently running.
2. Insert the CD-ROM into the CD-ROM drive.

The installer starts.

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

The printer driver with the selected language will be installed. The English printer driver is installed when the following language is selected: Suomi, Magyar, Cestina, Polski, Portugues, Russian, Catala, Turkce.

4. Click [PostScript 3 Printer Driver].

Add Printer Wizard starts.

5. Click [Add a local printer].

6. Click [Create a new port:], and then select [DeskTop Binder - SmartDeviceMonitor] in [Type of port].

7. Click [Next >].

8. Click [IPP].

9. In the [Printer URL] box, enter "http://(machine's IP address or host name)/printer" as the machine's address.

If the server authentication is issued, to enable SSL (a protocol for encrypted communication), enter "https://(machine's IP address or host name)/printer" (Internet Explorer 5.01, or a higher version must be installed).

(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 or host name/ipp" as the machine's address.

If the address is "192.168.001.010", you must enter it as "192.168.1.10" to connect to the machine.

- 10. Enter a name for identifying the machine in [IPP Port Name]. Use a name different from the one of any existing port.**

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

- 11. Click [Detailed Settings] to make necessary settings.**

For information about the settings, see DeskTop Binder-SmartDeviceMonitor for Client Help.

- 12. Click [OK].**

- 13. Click [OK].**

- 14. Check that the name of the printer driver you want to install is selected, and then click [Next >].**

- 15. Change the name of the machine if you want, and then click [Next >].**

Select the [Yes] check box to configure the machine as default.

- 16. Specify whether or not to share the machine, and then click [Next >].**

- 17. Specify whether or not to print a test page, and then click [Finish].**

The printer driver installation starts.

Note

- Depending on your computer's operating system, the [AutoPlay] dialog box may appear. If this happens, click [Run SETUP.EXE]. If the [User Account Control] dialog box appears, click [Continue] to allow the auto play program to run.
- user code can be set after the printer driver installation. For information about user code, see the printer driver Help.
- Auto Run may not work with certain operating system settings. In that case, launch "Setup.exe" on the CD-ROM root directory.

Changing the Port Settings DeskTop Binder-SmartDeviceMonitor for Client

Follow the procedure below to change the DeskTop Binder-SmartDeviceMonitor for Client settings, such as TCP/IP timeout, recovery/parallel printing, and printer groups.

Windows 2000:

- 1. Open the [Printers] window from the [Start] menu.**
- 2. Click the icon of the machine you want to use. On the [File] menu, click [Properties].**

The printer properties appear.

- 3. On the [Ports] tab, click [Configure Port...].**

The [Port Configuration] dialog box appears.

Windows XP, Windows Server 2003 / 2003 R2:

1. Open the [Printers and Faxes] window from the [Start] menu.

The [Printers and Faxes] window appears.

2. Click the icon of the machine you want to use. On the [File] menu, click [Properties].

The printer properties appear.

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

The [Port Configuration] dialog box appears.

- For TCP/IP, timeout setting can be configured.
- User, proxy, and timeout settings can be configured for IPP.

↓ Note

- For information about these settings, see DeskTop Binder-SmartDevice-Monitor for Client Help.

Windows Vista, Windows Server 2008:

1. Open the [Printers] window from [Control Panel] on the [Start] menu.

The [Printers] window appears.

2. Right - click the icon of the machine you want to use, and then click the [Properties].

The printer properties appear.

3. Click the [Port] tab, and then click [Configure Port].

The [Port Configuration] dialog box appears.

- For TCP/IP, timeout setting can be configured.
- User, proxy, and timeout settings can be configured for IPP.

↓ Note

- For information about these settings, see DeskTop Binder-SmartDevice-Monitor for Client Help.

How to enable Recovery/Parallel Printing

If no settings on the [Recovery/Parallel Printing] tab are available, follow the procedure below.

1. Start DeskTop Binder-SmartDeviceMonitor for Client, and then right-click the DeskTop Binder-SmartDeviceMonitor for Client icon on the taskbar.
2. Click [Extended Features Settings], and then select the [Set Recovery/Parallel Printing for each port] check box.
3. Click [OK] to close the [Extended Features Settings] dialog box.

Using the Standard TCP/IP Port

1

Installing the PostScript 3 Printer Driver (Windows 2000)

★ Important

- Installing this printer driver requires Administrators permission. Log on using an account that has Administrators permission.
- In an IPv6 environment, you cannot use the Standard TCP/IP Port. Use the DeskTop Binder-SmartDeviceMonitor port.

1. Quit all applications currently running.

2. Insert the CD-ROM into the CD-ROM drive.

The installer starts.

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

The printer driver with the selected language will be installed. The English printer driver is installed when the following language is selected: Suomi, Magyar, Cestina, Polski, Portugues, Russian, Catala, Turkce.

4. Click [PostScript 3 Printer Driver].

Add Printer Wizard starts.

5. Click [Next >].

6. Click [Local printer], and then click [Next >].

7. Click [Create a new port:].

8. Click [Standard TCP/IP Port], and then click [Next >].

9. Click [Next >] in the [Add Standard TCP/IP Printer Port Wizard] dialog box.

10. Enter the machine name or IP address in the [Printer Name or IP Address] box.

The [Port Name] text box automatically obtains a port name. Change this name if necessary.

When screen for Device selection appears, select "RICOH NetworkPrinter Driver C Model".

11. Click [Next >].

12. Click [Finish] in the [Add Standard TCP/IP Printer Port Wizard-dialog box].

13. Check that the name of the machine whose driver you want to install is selected, and then click [Next >].

14. Change the machine name if you want, and then click [Next >].

Select the [Yes] check box to configure the machine as default.

15. Click [Next >].

16. Specify whether or not to share the machine, and then click [Next >].

17. Specify whether or not to print a test page, and then click [Next >].

18. Click [Finish].

The printer driver installation starts.

↓ Note

- A user code can be set after the printer driver installation. For information about user code, see the printer driver Help.
- Auto Run may not work with certain operating system settings. In that case, launch "Setup.exe" on the CD-ROM root directory.

Installing the PostScript 3 Printer Driver (Windows XP, Windows Server 2003 / 2003 R2)

★ Important

- Installing this printer driver requires Administrators permission. Log on using an account that has Administrators permission.
- In an IPv6 environment, you cannot use the Standard TCP/IP Port. Use the DeskTop Binder-SmartDeviceMonitor port.
- You can install the printer driver from the CD-ROM provided with this machine or download it from the supplier's Web site.
- If your operating system is Windows XP Professional x64, Windows Server 2003 / 2003 R2 x64, you must download the printer driver from the manufacturer's Web site. Select this machine and the operating system you are using, and then download it.

1. Quit all applications currently running.
2. Insert the CD-ROM into the CD-ROM drive.

The installer starts.

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

The printer driver with the selected language will be installed. The English printer driver is installed when the following language is selected: Suomi, Magyar, Cestina, Polski, Portugues, Russian, Catala, Turkce.

4. Click [PostScript 3 Printer Driver].

Add Printer Wizard starts.

5. Click [Next >].
6. Click [Local printer attached to this computer], and then click [Next >].
7. Click [Create a new port:].
8. Click [Standard TCP/IP Port] in [Create a new port], and then click [Next >].

9. Click **[Next >]** in the **[Add Standard TCP/IP Printer Port Wizard]** dialog box.
10. Enter the machine name or IP address in the **[Printer Name or IP Address]** box.
The **[Port Name]** text box automatically obtains a port name. Change this name if necessary.
When screen for Device selection appears, select "RICOH NetworkPrinter Driver C Model".
11. Click **[Next >]**.
12. Click **[Next >]**.
13. Click **[Finish]** in the **[Add Standard TCP/IP Printer Port Wizard]** dialog box.
14. Check that the name of the machine whose driver you want to install is selected, and then click **[Next >]**.
15. Change the machine name if you want, and then click **[Next >]**.
Select the **[Yes]** check box to configure the machine as default.
16. Specify whether or not to share the machine, and then click **[Next >]**.
17. Specify whether or not to print a test page, and then click **[Next >]**.
18. Click **[Finish]**.
The printer driver installation starts.

 **Note**

- A user code can be set after the printer driver installation. For information about user code, see the printer driver Help.
- Auto Run may not work with certain operating system settings. In that case, launch "Setup.exe" on the CD-ROM root directory.

Installing the PostScript 3 Printer Driver (Windows Vista, Windows Server 2008)

 **Important**

- Installing this printer driver requires Administrators permission. Log on using an account that has Administrators permission.
- In an IPv6 environment, you cannot use the Standard TCP/IP Port. Use the DeskTop Binder-SmartDeviceMonitor port.

1. Quit all applications currently running.
2. Insert the CD-ROM into the CD-ROM drive.

The installer starts.

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

The printer driver with the selected language will be installed. The English printer driver is installed when the following language is selected: Suomi, Magyar, Cestina, Polski, Portugues, Russian, Catala, Turkce.

4. Click [PostScript 3 Printer Driver].

Add Printer Wizard starts.

5. Click [Add a local printer].**6. Click [Create a new port:], and then select [Standard TCP/IP Port] in [Type of port].****7. Click [Next].****8. Select [TCP/IP Device] in [Device Type].****9. Enter the machine's IP address in [Hostname or IP Address], and then click [Next>].**

The [Port name] text box automatically obtains a port name. Change this name if necessary.

A printer driver installation screen appears when TCP/IP port is detected.

When screen for Device selection appears, select "RICOH NetworkPrinter Driver C Model".

10. Select that the name of the machine whose driver you want to install is selected, and then click [Next >].**11. Change the machine name if you want, and then click [Next >].**

Check the checkbox to configure the machine as default.

12. Specify whether or not to share the machine, and then click [Next >].**13. Specify whether or not to print a test page, and then click [Finish].**

The printer driver installation starts.

Note

- Depending on your computer's operating system, the [AutoPlay] dialog box may appear. If this happens, click [Run SETUP.EXE]. If the [User Account Control] dialog box appears, click [Continue] to allow the auto play program to run.
- A user code can be set after the printer driver installation. For information about user code, see the printer driver Help.
- Auto Run may not work with certain operating system settings. In that case, launch "Setup.exe" on the CD-ROM root directory.

Using the LPR Port

1 Installing the PostScript 3 Printer Driver (Windows 2000)

★ Important

- Installing this printer driver requires Administrators permission. Log on using an account that has Administrators permission.

1. Quit all applications currently running.
2. Insert the CD-ROM into the CD-ROM drive.

The installer starts.

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

The printer driver with the selected language will be installed. The English printer driver is installed when the following language is selected: Suomi, Magyar, Cestina, Polski, Portugues, Russian, Catala, Turkce,

4. Click [PostScript 3 Printer Driver].

Add Printer Wizard starts.

5. Click [Next >].

6. Click [Local printer], and then click [Next >].

7. Click [Create a new port:].

8. Click [LPR Port], and then click [Next >].

9. Enter the machine's IP address in the [Name or address of server providing lpd] box.

10. Enter "lp" in the [Name of printer or print queue on that server] box, and then click [OK].

11. Check that the name of the machine whose driver you want to install is selected, and then click [Next >].

12. Change the machine name if you want, and then click [Next >].

Select the [Yes] check box to configure the machine as default.

13. Specify whether or not to share the machine, and then click [Next >].

14. Specify whether or not to print a test page, and then click [Next >].

15. Click [Finish].

The printer driver installation starts.

↓ Note

- A user code can be set after the printer driver installation. For information about user code, see the printer driver Help.

- Auto Run may not work with certain operating system settings. In that case, launch "Setup.exe" on the CD-ROM root directory.

Installing the PostScript 3 Printer Driver (Windows XP, Windows Server 2003 / 2003 R2)

1

★ Important

- Installing this printer driver requires Administrators permission. Log on using an account that has Administrators permission.
- In an IPv6 environment, you cannot use the LPR Port. Use the DeskTop Binder-SmartDeviceMonitor port.
- You can install the printer driver from the CD-ROM provided with this machine or download it from the supplier's Web site.
- If your operating system is Windows XP Professional x64, Windows Server 2003 / 2003 R2 x64, you must download the printer driver from the manufacturer's Web site. Select this machine and the operating system you are using, and then download it.

1. Quit all applications currently running.
2. Insert the CD-ROM into the CD-ROM drive.

The installer starts.

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

The printer driver with the selected language will be installed. The English printer driver is installed when the following language is selected: Suomi, Magyar, Cestina, Polski, Portugues, Russian, Catala, Turkce.

4. Click [PostScript 3 Printer Driver].
Add Printer Wizard starts.
5. Click [Next >].
6. Click [Local Printer attached to this computer.], and then click [Next >].
7. Click [Create a new port:].
8. Click [LPR Port] in [Create a new port], and then click [Next >].
9. Enter the machine's IP address in the [Name or address of server providing lpd] box.
10. Enter "lp" in the [Name of printer or print queue on that server box], and then click [OK].
11. Check that the name of the machine whose driver you want to install is selected, and then click [Next >].
12. Change the machine name if you want, and then click [Next >].
Select the [Yes] check box to configure the machine as default.

13. Specify whether or not to share the machine, and then click [Next >].
14. Specify whether or not to print a test page, and then click [Next >].
15. Click [Finish].

The printer driver installation starts.

Note

- A user code can be set after the printer driver installation. For information about user code, see the printer driver Help.
- Auto Run may not work with certain operating system settings. In that case, launch "Setup.exe" on the CD-ROM root directory.

Installing the PostScript 3 Printer Driver (Windows Vista, Windows Server 2008)

Important

- Installing this printer driver requires Administrators permission. Log on using an account that has Administrators permission.
 - In an IPv6 environment, you cannot use the LPR Port. Use the DeskTop Binder-SmartDeviceMonitor port.
1. Quit all applications currently running.
 2. Insert the CD-ROM into the CD-ROM drive.
The installer starts.
 3. Select an interface language, and then click [OK].
The printer driver with the selected language will be installed. The English printer driver is installed when the following language is selected: Suomi, Magyar, Cestina, Polski, Portugues, Russian, Catala, Turkce.
 4. Click [PostScript 3 Printer Driver].
Add Printer Wizard starts.
 5. Click [Add a local printer].
 6. Click [Create a new port:], and then click [LPR Port] in [Create a new port].
 7. Click [Next >].
 8. Enter the machine's IP address in [Name or address of server providing lpd].
 9. Enter "lp" in [Name of printer or print queue on that server], and then click [OK].
 10. Select that the name of the machine whose driver you want to install is selected, and then click [Next >].
 11. Change the machine name if you want, and then click [Next >].
Check the checkbox to configure the machine as default.

12. Specify whether or not to print a test page, and then click [Finish].

The printer driver installation starts.

↓ Note

- Depending on your computer's operating system, the [AutoPlay] dialog box may appear. If this happens, click [Run SETUP.EXE]. If the [User Account Control] dialog box appears, click [Continue] to allow the auto play program to run.
- A user code can be set after the printer driver installation. For information about user code, see the printer driver Help.
- Auto Run may not work with certain operating system settings. In that case, launch "Setup.exe" on the CD-ROM root directory.

Using as the Windows Network Printer

1 Installing the PostScript 3 Printer Driver (Windows 2000)

★ Important

- Installing a printer driver requires Administrators permission. Log on using an account that has Administrators permission.
- If you print from a print server connected to the machine using the DeskTop Binder-SmartDeviceMonitor port, the client cannot use Recovery Printing and Parallel Printing.

1. Quit all applications currently running.
2. Insert the CD-ROM into the CD-ROM drive.

The installer starts.

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

The printer driver with the selected language will be installed. The English printer driver is installed when the following language is selected: Suomi, Magyar, Cestina, Polski, Portugues, Russian, Catala, Turkce.

4. Click [PostScript 3 Printer Driver].

Add Printer Wizard starts.

5. Click [Next >].

6. Click [Network printer], and then click [Next >].

7. Select the location method from the [Locate Your Printer] screen, and then click [Next >].

8. Double-click the computer name you want to use as a print server in the [Shared printers] window.

9. Select the machine you want to use, and then click [Next >].

10. The printer driver installation starts.

11. Click [Next >].

Select the [Yes] check box to configure the machine as default.

12. Click [Finish].

Restart the computer to complete installation.

↓ Note

- A user code can be set after the printer driver installation. For information about user code, see the printer driver Help.
- Auto Run may not work with certain operating system settings. In that case, launch "Setup.exe" on the CD-ROM root directory.

Installing the PostScript 3 Printer Driver (Windows XP, Windows Server 2003 / 2003 R2)

★ Important

- Installing this printer driver requires Administrators permission. Log on using an account that has Administrators permission.
 - If you print from a print server connected to the machine using the DeskTop Binder-SmartDeviceMonitor port, the client cannot use Recovery Printing and Parallel Printing.
 - If you print with a Windows XP or Windows Server 2003 / 2003 R2 print server, DeskTop Binder-SmartDeviceMonitor notification functions may not be possible for the client.
 - You can install the printer driver from the CD-ROM provided with this machine or download it from the supplier's Web site.
 - If your operating system is Windows XP Professional x64, Windows Server 2003 / 2003 R2 x64, you must download the printer driver from the manufacturer's Web site. Select this machine and the operating system you are using, and then download it.
1. Quit all applications currently running.
 2. Insert the CD-ROM into the CD-ROM drive.
The installer starts.
 3. Select an interface language, and then click [OK].
The printer driver with the selected language will be installed. The English printer driver is installed when the following language is selected: Suomi, Magyar, Cestina, Polski, Portugues, Russian, Catala, Turkce.
 4. Click [PostScript 3 Printer Driver].
Add Printer Wizard starts.
 5. Click [Next >].
 6. Click [A network printer, or a printer attached to another computer] and then click [Next >].
 7. Select [Browse for a printer], and then click [Next >].
 8. Double-click the computer name you want to use as a print server in the [Shared printers] window.
 9. Select the machine you want to use, and then click [Next >].
 10. The printer driver installation starts.
 11. Click [Next >].
Select the [Yes] check box to configure the machine as default.
 12. Click [Finish].
Restart the computer to complete installation.

Note

- A user code can be set after the printer driver installation. For information about user code, see the printer driver Help.
- Auto Run may not work with certain operating system settings. In that case, launch "Setup.exe" on the CD-ROM root directory.

Installing the PostScript 3 Printer Driver (Windows Vista, Windows Server 2008)

Important

- Installing this printer driver requires Administrators permission. Log on using an account that has Administrators permission.
- If you print from a print server connected to the machine using the DeskTop Binder-SmartDeviceMonitor port, the client cannot use Recovery Printing and Parallel Printing.
- If you print with a Windows Vista or Windows Server 2008 print server, DeskTop Binder-SmartDeviceMonitor notification functions may not be possible for the client.
- You can install the printer driver from the CD-ROM provided with this machine or download it from the supplier's Web site.
- If your operating system is Windows Vista x64, Windows Server 2008 x64, you must download the printer driver from the manufacturer's Web site. Select this machine and the operating system you are using, and then download it.

1. Quit all applications currently running.

2. Insert the CD-ROM into the CD-ROM drive.

The installer starts.

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

The printer driver with the selected language will be installed. The English printer driver is installed when the following language is selected: Suomi, Magyar, Cestina, Polski, Portugues, Russian, Catala, Turkce.

4. Click [PostScript 3 Printer Driver].

Add Printer Wizard starts.

5. Click [Add a network, wireless or Bluetooth printer].

6. Select your machine, and then click [Next >].

7. Select that the name of the machine whose driver you want to install is selected, and then click [Next >].

8. Change the machine name if you want, and then click [Next >].

The printer driver installation starts.

9. Click [Next >].

Select the [Yes] check box to configure the machine as default.

10. Specify whether or not to share the machine, and then click [Next >].**11. Click [Finish].**

Restart the computer to complete installation.

↓ Note

- Depending on your computer's operating system, the [AutoPlay] dialog box may appear. If this happens, click [Run SETUP.EXE]. If the [User Account Control] dialog box appears, click [Continue] to allow the auto play program to run.
- A user code can be set after the printer driver installation. For information about user code, see the printer driver Help.
- Auto Run may not work with certain operating system settings. In that case, launch "Setup.exe" on the CD-ROM root directory.

Using the WSD port

This section explains installation when using the WSD port.

★ Important

- **The WSD Port can be used under Windows Vista or Windows Server 2008.**
- **To install under Windows Vista or Windows Server 2008, you must have an account that has Manage Printers permission. Log on as an Administrator.**
- **If the machine is connected using the WSD port, bi-directional communication is not possible. For details about bi-directional communication, see "Making Option Settings for the Printer".**
- **You can connect to the machine only if both the machine and computer are on the same network segment, or "Network discovery" is enabled. For details, see Windows Help.**

1. Quit all applications currently running.**2. Click [Start], and then click [Network].**

The [Network] window appears, and the device search begins automatically.

3. Using as the NetWare Print Server / Remote Printer

If the [User Account Control] dialog box appears, click [Continue].

The [Found New Hardware] dialog box appears.

4. Click [Locate and install driver software (Recommended)].

If the [User Account Control] dialog box appears, click [Continue].

The [Found New Hardware] window appears.

5. Click [Don't search online].

6. Click [Browse my computer for driver software (advanced)].

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

If the [AutoPlay] dialog box appears, click the [close] button and then proceed to step 8.

8. Click [Browse...], and then specify a location for the printer driver.

If the CD-ROM drive letter is D, the printer driver's source files are stored in "D:\DRIVERS\PS\
(Language) \XP_VISTA\DISK1".

9. Click [Next].

If the [Windows can't verify the publisher of this driver software] message appears, click [Install this driver software anyway].

10. Click [Close].

If installation is successful, the icon of the machine connected to the "WSD" port is added to the [Printers] window.

Note

- Depending on your computer's operating system, the [AutoPlay] dialog box may appear. If this happens, click [Run SETUP.EXE]. If the [User Account Control] dialog box appears, click [Continue] to allow the auto play program to run.
- 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 machine's icon in the [Network] window, and then click [Uninstall].

Reference

- p.49 "Making Option Settings for the Printer"

Using as the NetWare Print Server / Remote Printer

1

When using the PostScript 3 Printer Driver

Important

- In an IPv6 environment, Netware servers cannot be used.

Follow the procedure below to set up the PostScript 3 printer driver.

1. In the [Printers] or [Printers and Faxes] window, open the printer properties.
2. Click the [Device Settings] tab.
3. Select a [No] on the [Send CTRL+D before job] and [Send CTRL+D after job], and then click [OK].
4. Click [OK] to close the printer properties dialog box.

Installing the Printer Driver Using USB

This section explains how to install printer drivers using USB.

1

★ Important

- Make sure that machine is connected to the computer's USB ports using the USB interface cable.
- Before installing, check that only the operating system is running on the computer and no print jobs are in progress.
- The printer drivers can be installed from the CD-ROM provided with this machine.
- You can install the printer driver from the CD-ROM provided with this machine or download it from the supplier's Web site.
- If your operating system is Windows XP Professional x64, Windows Vista x64, or Windows Server 2003 / 2003 R2 / 2008 x64, you must download the printer driver from the manufacturer's Web site. Select this machine and the operating system you are using, and then download it.

Windows 2000 - USB

★ Important

- Installing a printer driver requires Administrators permission. Log on using an account that has Administrators permission.

If the printer driver has already been installed, plug and play is enabled, and the icon of the machine connected to the "USB" port is added to the [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.

1. **Connect the machine to the computer using the USB cable.**
Connect the USB cable firmly.
2. **In the Found New Hardware Wizard display, click [Search for a suitable driver for my device [recommended]], and then click [Next >].**
3. **Select the [Specify location] check box, and then click [Next >].**
4. **Insert the CD-ROM into the CD-ROM drive.**
5. **When Auto Run starts, click [Exit].**

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.

6. **Specify the location where the source files of the printer driver is stored.**

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

- PostScript 3

D:\DRIVERS\PS\XP_VISTA\Language\DISK1

7. Check the printer driver location, and then click [OK].
8. Click [Next >].
9. Click [Finish].

If the printer driver has already been installed, plug and play is enabled, and the icon of the machine connected to the "USB001" port is added to the [Printers] window.

↓ Note

- When Auto Run starts, click [Exit].
- 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.
- The number after "USB" varies depending on the number of machines connected.

Windows XP, Windows Server 2003 / 2003 R2 - USB

★ Important

- **Installing a printer driver requires Administrators permission. Log on using an account that has Administrators permission.**

If the printer driver has already been installed, plug and play is enabled, and the icon of the machine connected to the "USB" port is added to the [Printers] window.

The printer drivers can be installed from the CD-ROM provided with this machine.

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.

1. **Connect the machine to the computer using the USB cable.**

Connect the USB cable firmly.

2. **In the Found New Hardware Wizard display, click Install the software automatically (Recommended), and then click [Next >].**

3. **Insert the CD-ROM into the CD-ROM drive.**

If Auto Run starts, click [Cancel], and then [Exit].

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.

4. **Select the [Include this location in the search] check box under [Search for the best driver in these location], and then click [Browse] to select the printer driver location.**

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

- PostScript 3

D:\DRIVERS\PS\XP_VISTA\Language\DISK1

5. Check the printer driver location, and then click [Next >].
6. Click [Continue].
7. Click [Finish].

If installation is successful, the icon of the machine connected to the "USB001" port is added to the [Printers] window.

Note

- If Auto Run starts, click [Cancel], and then [Exit].
- The number after "USB" varies depending on the number of machines connected.

Windows Vista, Windows Server 2008 - USB

Important

- **Installing a printer driver requires Administrators permission. Log on using an account that has Administrators permission.**

If the printer driver has already been installed, plug and play is enabled, and the icon of the machine connected to the "USB" port is added to the [Printers] window.

The printer drivers can be installed from the supplied CD-ROM provided with this machine.

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.

1. Connect the machine to the computer using the USB cable.

Connect the USB cable firmly.

2. In the Found New Hardware display, select [Locate and install driver software (Recommended)].

Click [Continue] if the [User Account Control] window appears.

3. When a message prompting insertion of the CD-ROM, insert the CD-ROM into the CD-ROM drive.

Installation of the printer driver is automatically started.

If "Windows can't verify the publisher of this software" display appears in the installation, select the [Install this driver software anyway].

4. Click [Exit].

If installation is successful, the icon of this machine is added to the [Printers] window.

Note

- Depending on your computer's operating system, the [AutoPlay] dialog box may appear. If this happens, click [Run SETUP.EXE]. If the [User Account Control] dialog box appears, click [Continue] to allow the auto play program to run.

- When a printer driver meeting this machine is found on a network, a message prompting insertion of the CD-ROM is not displayed.
- The number after "USB" varies depending on the number of machines connected.

Troubleshooting for using USB

Problems	Solutions
The machine is not automatically recognized.	Turn off the power of the machine, reconnect the USB cable, and then turn it on again.
Windows has already configured the USB settings.	Open Windows' Device Manager, and then, under [Universal Serial Bus controllers], remove any conflicting devices. Conflicting devices have a yellow [!] or [?] icon by them. Take care not to accidentally remove required devices. For details, see Windows Help.

↓ Note

- When using Windows 2000 / XP / Vista or Windows Server 2003 / 2003 R2 / 2008, an erroneous device is displayed under [USB Controller] in the [Device Manager] dialog box.

Printing with Parallel Connection

To use a machine connected using a parallel interface, click [LPT1] when installing the printer driver.

1

Installing the PostScript 3 printer driver (Windows 2000)

★ Important

- Installing this printer driver requires Administrators permission. Log on using an account that has Administrators permission.

1. Quit all applications currently running.
2. Insert the CD-ROM into the CD-ROM drive.

The installer starts.

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

The printer driver with the selected language will be installed. The English printer driver is installed when the following language is selected: Suomi, Magyar, Cestina, Polski, Portugues, Russian, Catala, Turkce.

4. Click [PostScript 3 Printer Driver].

Add Printer Wizard starts.

5. Click [Next >].

6. Click [Local printer], and then click [Next >].

A dialog box for selecting the machine manufacturer and model name appears.

7. Select [LPT1] at the [Printer Port] dialog box, and then click [Next >].

8. Select whether or not to share the machine, and then click [Next >].

9. Select the name of the machine whose driver you want to install, and then click [Next >].

10. Select whether or not you want to print a test page, and then click [Finish].

The printer driver installation starts.

11. Restart the computer to complete installation if necessary.

↓ Note

- A user code can be set after the printer driver installation. For information about user code, see the printer driver Help.
- Auto Run may not work with certain operating system settings. In that case, launch "Setup.exe" on the CD-ROM root directory.

Installing the PostScript 3 Printer Driver (Windows XP, Windows Server 2003 / 2003 R2)

★ Important

- Installing this printer driver requires Administrators permission. Log on using an account that has Administrators permission.
- You can install the printer driver from the CD-ROM provided with this machine or download it from the supplier's Web site.
- If your operating system is Windows XP Professional x64, Windows Server 2003 / 2003 R2 x64, you must download the printer driver from the manufacturer's Web site. Select this machine and the operating system you are using, and then download it.

1. Quit all applications currently running.
2. Insert the CD-ROM into the CD-ROM drive.

The installer starts.

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

The printer driver with the selected language will be installed. The English printer driver is installed when the following language is selected: Suomi, Magyar, Cestina, Polski, Portugues, Russian, Catala, Turkce.

4. Click [PostScript 3 Printer Driver].

Add Printer Wizard starts.

5. Click [Next >].

6. Click [Local printer attached to this computer], and then click [Next >].

7. Select the port you want to use, and then click [Next >].

A dialog box for selecting the machine manufacturer and model name appears.

8. Select the name of the machine whose driver you want to install, and then click [Next >].

9. Click [Close] to close the [Printer Port] dialog box.

10. Click [Next >].

11. Change the machine name if you want, and then click [Next >].

12. Select whether or not to share the machine, and then click [Next >].

13. Specify whether or not to print a test page, and then click [Finish].

The printer driver installation starts.

14. Restart the computer to complete installation.

↓ Note

- A user code can be set after the printer driver installation. For information about user code, see the printer driver Help.

- Auto Run may not work with certain operating system settings. In that case, launch "Setup.exe" on the CD-ROM root directory.

1

Installing the PostScript 3 Printer Driver (Windows Vista, Windows Server 2008)

Important

- Installing this printer driver requires Administrators permission. Log on using an account that has Administrators permission.
- You can install the printer driver from the CD-ROM provided with this machine or download it from the supplier's Web site.
- If your operating system is Windows Vista x64, Windows Server 2008 x64, you must download the printer driver from the manufacturer's Web site. Select this machine and the operating system you are using, and then download it.

1. Quit all applications currently running.
2. Insert the CD-ROM into the CD-ROM drive.

The installer starts.

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

The printer driver with the selected language will be installed. The English printer driver is installed when the following language is selected: Suomi, Magyar, Cestina, Polski, Portugues, Russian, Catala, Turkce.

4. Click [PostScript 3 Printer Driver].

Add Printer Wizard starts.

5. Click [Add a local printer].

6. Select the port you want to use, and then click [Next >].

A dialog box for selecting the machine manufacturer and model name appears.

7. Select the name of the machine whose driver you want to install, and then click [Next >].

8. Change the machine name if you want, and then click [Next >].

9. Specify whether or not to print a test page, and then click [Finish].

The printer driver installation starts.

10. Restart the computer to complete installation.

Note

- Depending on your computer's operating system, the [AutoPlay] dialog box may appear. If this happens, click [Run SETUP.EXE]. If the [User Account Control] dialog box appears, click [Continue] to allow the auto play program to run.

- A user code can be set after the printer driver installation. For information about user code, see the printer driver Help.
- Auto Run may not work with certain operating system settings. In that case, launch "Setup.exe" on the CD-ROM root directory.

Printing with Bluetooth Connection

This describes how to print with Bluetooth devices.

1

Supported Profiles

The following profiles are supported:

- SPP (Serial Port Profile)
- HCRP (Hardcopy Cable 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.

Restrictions on BIP

- For BIP connection, a module including PostScript 3 must be installed in the machine.
- 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

The following procedures explain how to install a Bluetooth printer on a computer that is running Windows XP or Windows Vista.

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 perform a machine installation, your account must have Manage Printers permission. Log on as an Administrators group member.
- To connect to a Bluetooth printer, your computer must have a Bluetooth device installed. Make sure a Bluetooth device is installed on your computer.

1

Windows XP

1. On the [Start] menu, click [Printers and Faxes].

The [Printers and Faxes] window appears.

2. Click [Add a printer].

The [Add Printer Wizard] window opens.

3. Click [Next >].

4. 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.

5. Click [No, I will not connect], and then click [Next >].

6. Click [Install from a list or specific location (Advanced)], and then click [Next >].

7. 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 >].

8. If the [Hardware Installation] window appears, click [Continue].

9. If the installation was successful, click [Finish].

10. Select [Test Print], and then click [Next >].

11. 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

★ Important

- To perform a machine installation, your account must have **Manage Printers** permission. Log on as an **Administrators** group member.

1. On the [Start] menu, click [Control Panel].
2. In the "Hardware and Sound" area, click [Printers].
3. In the top part of the window, click [Add a printer].
4. 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.

5. From the list of discovered devices, select the printer 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 printer you select is a Bluetooth printer.

6. 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.
7. In the [Found New Hardware] window, select the printer driver you want to use, and then click [Next].

The printer driver installation starts.

8. If the [Windows Security] window appears, click [Install this driver software anyway].
9. Click [Close].
10. If you want to change the machine name, enter the new name in the [Printer Name Settings] window.
11. If you want to print a test page, click [Printing Test Page] on the "Test Print" page.

Otherwise, click [Finish].

↓ Note

- Depending on your computer's operating system, the [AutoPlay] dialog box may appear. If this happens, click [Run SETUP.EXE]. If the [User Account Control] dialog box appears, click [Continue] to allow the auto play program to run.
- 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.

If a Message Appears during Installation

Message number 58 or 34 indicates the printer driver cannot be installed using Auto Run. Install the printer driver using [Add Printer] or [Install Printer].

For Windows 2000:

1. On the [Start] menu, point to [Settings], and then click [Printers].
2. Double-click the Add Printer icon.
3. Follow the instructions in Add Printer Wizard.

If the printer driver is on a CD-ROM, the location of the PostScript 3 printer driver is D:\DRIVERS\PS\XP_VISTA\Language\DISK1.

For Windows XP Professional and Windows Server 2003 / 2003 R2:

1. On the [Start] menu, click [Printers and Faxes].
2. Click [Add a printer].
3. Follow the instructions in Add Printer Wizard.

If the printer driver is on a CD-ROM, the location of the PostScript 3 printer driver is D:\DRIVERS\PS\XP_VISTA\Language\DISK1.

For Windows XP Home Editions:

1. On the [Start] menu, click [Control Panel].
2. Click [Printers and Other Hardware].
3. Click [Printers and Faxes].
4. Click [Install Printer].
5. Follow the instructions in Add Printer Wizard.

If the printer driver is on a CD-ROM, the location of the PostScript 3 printer driver is D:\DRIVERS\PS\XP_VISTA\Language\DISK1.

For Windows Vista and Windows Server 2008:

1. On the [Start] menu, click [Control Panel].
The [Control Panel] window appears.
2. Click [Printer] in "Hardware and Sound".
3. Click [Install Printer].
4. Follow the instructions in Add Printer Wizard.

If the printer driver is on a CD-ROM, the location of the PostScript 3 printer driver is D:\DRIVERS\PS\XP_VISTA\Language\DISK1.

 **Note**

- If the installer starts, click [Cancel] to quit.

Making Option Settings for the Printer

Make option settings for the machine using the printer driver when bidirectional communication is disabled.

Set up option settings when bidirectional communications are disabled.

★ Important

- Under Windows 2000 / XP / Vista and Windows Server 2003 / 2003 R2 / 2008, Manage Printers permission is required to change the printer properties in the [Printers] folder. Log on as an Administrators group member.

1. On the [Start] menu, click [Printers and Faxes] or [Printers].

The [Printers and Faxes] or [Printers] window appears.

2. Click the icon of the printer you want to use.

3. On the [File] menu, click [Properties].

Under Windows Vista, Windows Server 2008, Right - click the icon of the machine you want to use, and then click the [Properties].

4. Click the [Device Settings] tab.

5. Select options installed from the [Install Options] area, and then make the necessary settings.

6. Click [Apply], and then click [OK] to close the printer properties dialog box.

↓ Note

- For details about making option settings for the printer using a Mac OS, see "Setting Up Options".

📖 Reference

- p.56 "Setting Up Options"
- p.60 "Setting Up Options"

Setting Up the Printer Driver

1

Windows 2000 - Accessing the Printer

Making printer default settings - the printer properties

★ Important

- To change the printer default settings including option configuration settings, log on using an account that has Manage Printers permission. Members of the Administrators group have Manage Printers permission by default.
- You cannot change the printer default settings for each user. Settings made in the printer properties dialog box are applied to all users.

1. On the [Start] menu, point to [Settings], and then click [Printers].

The [Printers] window appears.

2. Click the icon of the printer you want to use.

3. On the [File] menu, click [Properties].

The printer properties dialog box appears.

4. Make the necessary settings, and then click [OK].

↓ Note

- Settings you make here are used as the default settings for all applications.
- Do not make a setting for [Form to Tray Assignment].
- For details, see the printer driver Help.

Making printer default settings - Printing Preferences

★ Important

- You cannot change the printer default settings for each user. Settings made in the printer properties dialog box are applied to all users.

1. On the [Start] menu, point to [Settings], and then click [Printers].

The [Printers] window appears.

2. Click the icon of the printer you want to use.

3. On the [File] menu, click [Printing Preferences...].

The [Printing Preferences] dialog box appears.

4. Make the necessary settings, and then click [OK].

Note

- Settings you make here are used as the default settings for all applications.
- For details, see the printer driver Help.

Making printer settings from an application

You can make printer settings for a specific application.

To make printer settings for a specific application, open the [Printing Preferences] dialog box from that application.

The following explains how to make settings for the WordPad application provided with Windows 2000.

1. **Open the application.**
2. **On the [File] menu, click [Print...].**
The [Print] dialog box appears.
3. **Select the printer you want to use in the [Select Printer] list, and then click the tab for the settings you want to change.**
4. **Make the necessary settings, and then click [Apply].**
5. **Click [Print].**

Note

- The procedure to open the [Printing Preferences] dialog box may vary depending on the application. For details, see the manuals provided with the application you use.
- Any settings you make in the following procedure are valid for the current application only.
- General users can change the properties displayed in the [Print] dialog box of an application. Settings made here are used as defaults when printing from this application.
- For details, see the printer driver Help.

Windows XP, Windows Server 2003 / 2003 R2 - Accessing the Printer Properties

Making printer default settings - the printer properties

Important

- To change the printer default settings including option configuration settings, log on using an account that has Manage Printers permission. Members of the Administrators group have Manage Printers permission by default.
- You cannot change the printer default settings for each user. Settings made in the printer properties dialog box are applied to all users.

1. On the [Start] menu, click [Printers and Faxes].

The [Printers and Faxes] window appears.

2. Click the icon of the printer you want to use.

3. On the [File] menu, click [Properties].

The printer properties dialog box appears.

4. Make the necessary settings, and then click [OK].

↓ Note

- Settings you make here are used as the default settings for all applications.
- Do not make a setting for [Form to Tray Assignment].
- For details, see the printer driver Help.

Making printer default settings - Printing Preferences

★ Important

- You cannot change the printer default settings for each user. Settings made in the printer properties dialog box are applied to all users.

1. On the [Start] menu, click [Printers and Faxes].

The [Printers and Faxes] window appears.

2. Click the icon of the printer you want to use.

3. On the [File] menu, click [Printing Preferences...].

The [Printing Preferences] dialog box appears.

4. Make the necessary settings, and then click [OK].

↓ Note

- Settings you make here are used as the default settings for all applications.
- For details, see the printer driver Help.

Making printer settings from an application

You can make printer settings for a specific application.

To make printer settings for a specific application, open the [Printing Preferences] dialog box from that application. The following explains how to make settings for the WordPad application provided with Windows XP.

1. On the [File] menu, click [Print...].

The [Print] dialog box appears.

2. Select the printer you want to use in the [Select Printer] list, and then click [Preferences].
3. Make the necessary settings, and then click [OK].

↓ Note

- The procedure to open the [Printing Preferences] dialog box may vary depending on the application. For details, see the manuals provided with the application you use
- Any settings you make in the following procedure are valid for the current application only.
- General users can change the properties displayed in the [Print] dialog box of an application. Settings made here are used as defaults when printing from this application.
- For details, see the printer driver Help.

1

Windows Vista, Windows Server 2008 - Accessing the Printer Properties

Making printer default settings - the printer properties

★ Important

- To change the printer default settings including option configuration settings, log on using an account that has Manage Printers permission. Members of the Administrators group have Manage Printers permission by default.
- You cannot change the printer default settings for each user. Settings made in the printer properties dialog box are applied to all users.

1. On the [Start] menu, click [Control Panel].

The [Control Panel] window appears.

2. Click [Printer] in "Hardware and Sound".
3. Right - click the icon of the printer you want to use, and then click the [Properties].
4. Make the necessary settings, and then click [OK].

↓ Note

- Settings you make here are used as the default settings for all applications.
- Do not make a setting for [Form to Tray Assignment].
- For details, see the printer driver Help.

Making printer default settings - Printing Preferences

★ Important

- You cannot change the printer default settings for each user. Settings made in the printer properties dialog box are applied to all users.

1. On the [Start] menu, click [Control Panel].

The [Control Panel] window appears.

2. Click [Printer] in "Hardware and Sound".

3. Right - click the icon of the printer you want to use, and then click the [Printing Preferences...].

The [Printing Preferences] dialog box appears.

4. Make the necessary settings, and then click [OK].

↓ Note

- Settings you make here are used as the default settings for all applications.
- For details, see the printer driver Help.

Making printer settings from an application

You can make printer settings for a specific application.

To make printer settings for a specific application, open the [Printing Preferences] dialog box from that application. The following explains how to make settings for the WordPad application provided with Windows XP.

1. On the [File] menu, click [Print...].

The [Print] dialog box appears.

2. Select the printer you want to use in the [Select Printer] list, and then click [Preferences].

3. Make the necessary settings, and then click [OK].

↓ Note

- The procedure to open the [Printing Preferences] dialog box may vary depending on the application. For details, see the manuals provided with the application you use
- Any settings you make in the following procedure are valid for the current application only.
- General users can change the properties displayed in the [Print] dialog box of an application. Settings made here are used as defaults when printing from this application.
- For details, see the printer driver Help.

2. Mac OS Configuration

Mac OS

This section explains how to configure a Mac OS to use EtherTalk and USB.

The following explains how to configure Mac OS 9.2. If you are not using Mac OS 9.2, see the manual of the Mac OS you are using for details.

★ Important

- For Mac OS 8.6 and higher. (Mac OS X Classic environment is supported.)

↓ Note

- The PostScript 3 printer driver is stored in the following folder on the CD-ROM.
Mac OS 8 and 9:PS Driver:(language):Disk1

Installing the PostScript 3 Printer Driver and PPD File

It is necessary to install a printer driver and PostScript Printer Description (PPD) files to print from a Mac OS.

Follow the procedure below to install a printer driver and a PPD file into a Mac OS using Mac OS 8.6 and higher.

PostScript 3 Printer Driver

1. Insert the CD-ROM into the CD-ROM drive.
2. Double-click the CD-ROM drive icon.
3. Double-click the [Mac OS 8 and 9] folder.
4. Double-click the [PS Driver] folder.
5. Double-click the folder of the language you use.
6. Open [Disk1], and then double-click the installer icon.
7. Follow the instructions on the screen.

PPD Files

1. Double-click the CD-ROM drive icon.
2. Double-click the [Mac OS 8 and 9] folder.
3. Double-click the [Printer Descriptions] folder.
4. Double-click the folder of the language you are using.
5. Open the [DISK1] folder.

6. Drag the PPD file and the plugin file into [Printer Descriptions] in [Extensions] under [System Folder].
7. Restart the Mac OS.

Setting Up PPD Files

2

★ Important

- Make sure that the printers are connected to an AppleTalk network before performing the following procedure.
1. On the [Apple] menu, click [Chooser].
 2. Click the Adobe PS icon.
 3. In the [Select a PostScript Printer:] list, click the name of the printer you want to use.
 4. Click [Create].
 5. Click the printer you want to use, and then click [Setup...].

A PPD file is set up and the Adobe PS icon appears at the left of the machine name in the list. Follow the procedure on Setting Up Options to make option settings; otherwise close the [Chooser] dialog box.

Setting Up Options

1. On the [Apple] menu, click [Chooser].
2. Click the Adobe PS icon.
3. In the [Select a PostScript Printer:] list, click the name of the printer you want to use, and then click [Setup].
4. Click [Configure].
A list of options appears.
5. Select the option you want to set up, and then select an appropriate setting for it.
6. Click [OK].
The list of options closes.
7. Click [OK].
The [Chooser] dialog box appears.
8. Close the [Chooser] dialog box.

↓ 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.

Installing Adobe Type Manager

★ Important

- Quit all applications currently running before installation. Install ATM after you restart the computer.
1. Start a Mac OS.
 2. Insert the CD-ROM into the CD-ROM drive.
 3. Double-click the CD-ROM drive icon.
 4. Double-click the [Mac OS 8 and 9] folder.
 5. Double-click the [ATM] folder.
 6. Double-click the ATM 4.6.2 installer icon.
 7. Follow the instructions on the screen.
 8. When the procedure is complete, restart the computer. ATM will be completely installed only after restarting.
 9. On the [Apple] menu, open [Control Panel], and then click [~ ATM].
 10. The ATM control panel opens.

↓ Note

- For details about installation, see the operating instructions in the ATM folder.

Installing Screen fonts

Follow the procedure below to install screen fonts.

The screen fonts described below can be found in the [Fonts] folder on the CD-ROM.

1. Start a Mac OS.
2. Insert the CD-ROM into the CD-ROM drive.
The CD-ROM drive icon appears.
3. Double-click the CD-ROM drive icon.
The contents of the CD-ROM appear.
4. Double-click the [Mac OS 8 and 9] folder.
5. Double-click the [Fonts] folder.
6. Double-click the [Screen font] folder.
7. Double-click the [TrueType] or [Type 1] folder.
Select the font type you want to use.

8. Drag and drop the fonts you want to install to the [Fonts] folder under [System Folder].

A confirmation message appears.

9. Close the [Fonts] folder.

The fonts are installed.

10. Restart the Mac OS.

2

Changing to EtherTalk

Follow the procedure below to configure to a Mac OS to use EtherTalk.

1. Open [Control Panels], and then click the AppleTalk icon.
2. On the [Connect via:] pop-up menu, click [Ethernet].
3. If you change zones, select a name on the [Current zone:] pop-up menu.
4. Close the AppleTalk control panel.
5. Restart the computer.

↓ Note

- The procedures used to configure Mac OS may vary depending on the Mac OS version. The following describes how to configure Mac OS 9.1. If you are using a different version of Mac OS, use the following procedures as a reference and see the manuals for your Mac OS version.
- Confirm the Connection to the Printer with TCP/IP.
- For information about installing applications required for EtherTalk, see the Mac OS manuals.

Mac OS X

This section explains how to configure a Mac OS X to use EtherTalk, USB and TCP/IP.

Follow the procedure below to configure Mac OS X 10.3.8. If you are not using Mac OS X 10.3.8, see the manual of the Mac OS X you are using for details.

★ Important

- For Mac OS X 10.1 or higher.

↓ Note

- The PPD files are stored in the following folder on the CD-ROM.

Mac OS X: MacOSX PPD Installer

Installing the PPD Files

Follow the procedure below to install a PPD file to print from Mac OS X.

★ Important

- You need an administrator name and a password (phrase). For details, consult your network administrator.
1. Insert the CD-ROM into the CD-ROM drive.
 2. Double-click the CD-ROM drive icon.
 3. Double-click the [Mac OS X] folder.
 4. Double-click the [MacOSX PPD Installer] folder.
 5. Double-click the [MAC OSX 10.1 or later] or [MAC OSX 10.5 or later] folder, depending on your operating system.
 6. Double-click the installer icon.
 7. Double-click the package file icon.
 8. Follow the instructions on the screen.

Setting Up the PPD File

1. Start Printer Setup Utility.

Under Mac OS X 10.5, start System Preferences and click [Print & FAX].

2. Click [Add] or [+] button.

Mac OS X 10.5

Click [Default]. If the machine name is not displayed, select the icon that corresponds to your network environment (AppleTalk, etc.).

If several AppleTalk zones exist on the network, select the zone the printer belongs to.

Mac OS X 10.4

Click [More Printers...]. Then select the zone from the second pop-up menu.

Other Mac OS X

Click [AppleTalk] on the first pop-up menu.

If the zone is set, select the zone from the second pop-up menu.

3. Select the printer, and then select its manufacturer from the [Printer Model:] pop-up menu.

Under Mac OS X 10.4, select the printer you are using from the [Print Using] popup menu.

Under Mac OS X 10.5, select the printer you are using from the [Printer Name] list.

4. Select the PPD file for the model you are using, and then click [Add].

5. Quit Printer Setup Utility or System Preferences.

Setting Up Options

1. Start System Preferences.

2. Click [Utilities], and then double-click [Print Center] or [Printer Setup Utility].

Mac OS X 10.5

Click [Print& Fax].

The printer list dialog box appears.

3. Select the machine you are using, and then click [Show Info].

Mac OS X 10.5

Select the machine you are using, and then click [Options & Supplies...].

4. Select [Installable Options] in the drop-down menu, and then configure settings as needed.

Mac OS X 10.5

Click [Driver], and then configure settings as needed.

5. Click [Apply Changes].

Mac OS X 10.5

Click [OK].

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.

Using USB Interface

2

Follow the procedure below to set up USB connection.

1. Start Printer Setup Utility.

Under Mac OS X 10.5, start System Preferences and click [Print & FAX].

2. Click [Add] or [+] button.**Mac OS X 10.5**

Click [Default].

Mac OS X 10.4

Click a printer that has "USB" indicated in the "Connection" column.

Other Mac OS X

Click [USB] on the pop-up menu.

The connected printer appears.

3. Select the printer, and then select its manufacturer from the [Printer Model:] pop-up menu.

Under Mac OS X 10.4, select the printer you are using from the [Print Using] pop-up menu.

A list of printer types appears.

Under Mac OS X 10.5, select the printer you are using from the [Printer Name] list, and [kind] of USB.

4. Select the connected printer from the list of printer models, and then click [Add].**5. Quit Printer Setup Utility or System Preferences.****Note**

- When printing with a USB connection to a Macintosh computer, printer language does not change automatically. Use the control panel on this machine to change printer language to [Auto Detect] or [PS] before printing.
- USB2.0 can be used only with Mac OS X 10.3.3 or higher.

Using Bonjour

Follow the procedure below to print using Bonjour under Mac OS X 10.2.3 or higher. Ethernet, wireless LAN connections can also be used.

1. Start Printer Setup Utility.

Under Mac OS X 10.5, start System Preferences and click [Print & FAX].

2. Click [Add] or [+] button.

Mac OS X 10.5

Click [Default]. If the machine name is not displayed, select the icon that corresponds to your network environment (AppleTalk, etc.).

If several AppleTalk zones exist on the network, select the zone the printer belongs to.

Mac OS X 10.4

Click a printer that has "Bonjour" indicated in the "Connection" column.

Other Mac OS X

Click [Rendezvous] on the pop-up menu.

3. Select the name of the connected printer from the list of printer models, and then click [Add].

Under Mac OS X 10.4, Installable Options window appears. Select the option you want to set up, and then select an appropriate setting for it, and then [Continue].

Under Mac OS X 10.5, select the printer you are using from the [Printer Name] list, and [kind] of Bonjour.

4. Quit Printer Setup Utility or System Preferences.

When printing with a Rendezvous connection to a Macintosh computer, printer language does not change automatically. Use the control panel on this machine to change printer language to [Auto Detect] or [PS] before printing.

Note

- When printing with a Rendezvous connection to a Macintosh computer, printer language does not change automatically. Use the control panel on this machine to change printer language to [Auto Detect] or [PS] before printing.

Changing to EtherTalk

Follow the procedure below to configure a Mac OS X to use EtherTalk.

Important

- You need an administrator name and a password (phrase). For details, consult your network administrator.

1. Open [System Preferences], and then click the Network icon.

2. Click [Built-in Ethernet] in the [Show:] list box.

Mac OS X 10.5

Click [Ethernet], and then click [Advanced...] to open the Ethernet window.

3. Click the [AppleTalk] tab.
4. Select the [Make AppleTalk Active] check box.
5. To change AppleTalk zones, select a name from the [AppleTalk Zone:] pop-up menu.
6. When the settings are made, click [Apply Now].

Mac OS X 10.5

Click [OK], and then click [Apply].

↓ Note

- For information about installing applications required for EtherTalk, see the Mac OS manuals.

Configuring the Printer

Use the control panel to enable AppleTalk. (The default is active.)

3. Using PostScript 3

Setting Up Options

To use installed options correctly, first set up the printer driver. If the options are not recognized, you cannot use them, even though they are physically installed.

The procedure to set up a printer driver varies depending on the operating system.

Windows XP, Mac OS 9.2, and Mac OS X 10.5 are used as examples of their respective operating system families.

★ Important

- If your system is Windows 2000, Windows XP Professional, Windows Vista, or Windows Server 2003 / 2003 R2 / 2008, changing printer driver settings requires Manage Printers permission. Members of Administrators group have Manage Printers permission by default. When you change printer driver settings, log on with an account that has Manage Printers permission.
- If you are using Adobe PageMaker 6.0, 6.5, or 7.0, you have to set up options in Adobe PageMaker's print dialog box.

Windows

You can set up any of the options using the following tabs.

Windows	[Installable Options] on the [Device Settings] tab.
---------	---

Mac OS

You can set up all options using the [Chooser] dialog box.

Mac OS	For Ethernet, [Chooser] on the Apple Menu. For USB, [Change Setup] from the [Printing] menu to open the Desktop printer.
Mac OS X	[Options & Supplies...] in [Print & Fax] to open the System Preferences.

↓ Note

- To set up options, access the printer driver from Windows. You cannot set up options if you access the printer driver from an application.
- See, "Making Option Settings for the Printer", "Setting Up Options" or "Setting Up Options" for the installation method appropriate to your printing environment.

 **Reference**

- p.49 "Making Option Settings for the Printer"
- p.56 "Setting Up Options"
- p.60 "Setting Up Options"

Printing a Document

This documentation describes the specific printer functions and menus that are added by installing the PPD file.

Windows XP, Mac OS 9.2, and Mac OS X 10.5 are used as examples of their respective operating system families. Procedures for other versions of these operating systems may vary slightly.

★ Important

- On a Macintosh, Mac OS 8.6 or higher (Mac OS X Classic environment is supported.), or Mac OS X 10.1 or higher is required.
- If you are using Mac OS X 10.1.x, the following functions cannot be used:
 - Sample Print
 - Locked Print
 - Hold Print
 - Stored Print
 - Store and Print
 - Document Server
 - User Code
- Applications, such as PageMaker, that have their own drivers do not support the following functions:
 - Sample Print
 - Locked Print
 - Hold Print
 - Stored Print
 - Store and Print
 - Document Server
 - User Code

↓ Note

- If you are using Mac OS X 10.2.x or higher, the Job Type function can be used.
- "Mac OS X" in the tables below refers to Mac OS X 10.2.3. Depending on the version, [Features x] is displayed as [Set x] (x is a number). Make adjustments according to the version you use.

Job Type

Use this to select the type of print job.

The following table shows the tabs or menus where you can select this function.

Windows	[Job Type:] is displayed on the [Job/Log] tab in the Printing Preferences dialog box.
Mac OS	[Job Type:] is displayed on [Job Log] in the print dialog box.
Mac OS X	[Job Type:] is displayed on [Job Log] in the print dialog box.

3

You can select the following items:

Normal Print

Select this for normal printing. The print job starts immediately after the print command is given.

Sample Print

Use this function to print only one set of a multiple print jobs.

The other sets are saved in the machine. The saved job can be printed from the machine's control panel. You can also delete the saved job.

The "User ID" can contain up to eight alphanumeric (a-z, A-Z, 0-9) characters.

Entering the "User ID" helps you distinguish your print job from others.

For details about how to use Sample Print, see "How to Use Sample Print".

Locked Print

Use this function to save documents in the machine memory with a password, and then edit and print them as you want.

The "User ID" can contain to eight alphanumeric (a-z, A-Z, 0-9) characters. The "Password" must be 4-8 digits.

Entering the "User ID" helps you distinguish your print job from others.

For details about how to use Locked Print, see "How to Use Locked Print".

Hold Print

Use this function to temporarily hold a file in the machine, and print it from the computer or the machine's control panel later.

The "User ID" can contain up to eight alphanumeric (a-z, A-Z, 0-9) characters.

The "File Name" can contain to 16 alphanumeric (a-z, A-Z, 0-9) characters.

Entering the "User ID" helps you distinguish your print job from others.

For details about how to use Hold Print, see "How to Use Hold Print".

Stored Print

Use this function to store a file in the machine, and then print it from the computer or the machine's control panel later.

The "User ID" can contain up to eight alphanumeric (a-z, A-Z, 0-9) characters. The "Password" must be 4-8 digits.

The File Name can contain to 16 alphanumeric (a-z, A-Z, 0-9) characters.

You can assign a password to a saved document, but password assignment is not mandatory.

Entering the "User ID" helps you distinguish your print job from others.

For details about how to use Stored Print, see "How to Use Stored Print/Store and Print".

Store and Normal Print

Use this function to print the file at once and also store the file in the printer.

The "User ID" can contain up to eight alphanumeric (a-z, A-Z, 0-9) characters. The "Password" must be 4-8 digits.

The "File Name" can contain to 16 alphanumeric (a-z, A-Z, 0-9) characters.

You can assign a password to a saved document, but password assignment is not mandatory.

Entering the "User ID" helps you distinguish your print job from others.

For details about how to use Stored Print, see "How to Use Stored Print/Store and Print".

Send to Document Server

Use this function to store documents that you want to print in the printer, as well as documents you might want to later combine or process for printing.

The "File Name" can contain to 16 alphanumeric (a-z, A-Z, 0-9) characters.

For details about the Document Server function, see "Accessing the Document Server", Printer Reference.

Reference

- p.69 "How to Use Sample Print"
- p.72 "How to Use Locked Print"
- p.75 "How to Use Hold Print"
- p.77 "How to Use Stored Print/Store and Print"

How to Use Sample Print

Follow the procedure below to print a document using the Sample Print function.

Windows

1. In the application, on the [File] menu, click [Print].

The [Print] dialog box appears.

2. Select the printer, and then click [Preferences].

3. Click the [Job/Log] tab.

4. In the [Job Type:] list, click [Sample Print].
5. In the [User ID:] box, enter a user ID using up to eight alphanumeric (a-z, A-Z, 0-9) characters.

The user ID associates the user with his / her jobs.

6. Click [OK] to close the printer properties dialog box.
7. Set the number of copies to two or more, and then start the printing from the application's [Print] dialog box.

The sample print job is sent to the machine, and one set is printed.

8. Check the printed output to make sure the settings are correct.

If the settings are correct, perform the following steps to print the remaining sets.

If you want to delete a saved job, see "Deleting a Sample Print File".

9. On the machine's control panel, press the [Printer] key to display the printer screen.
10. Press [Print Jobs].
11. Press [Sample Print Job List].

A list of sample print files stored in the machine appears.

[User ID], [Date / Time] and [File Name] also appear.

12. Select the file you want to print by pressing it.

A list of print files stored in the machine appears.

13. Press [Print] to change the number of sets to be printed.

14. Enter the new number of sets using the number keys.

If you do not want to change the set quantity, perform the following steps.

You can enter up to 999 sets.

Press the [Clear/Stop] key to correct any entry mistakes.

When multiple files are selected without setting a quantity, 1 page less than the minimum number of all settings is applied.

15. Press [Yes].

The remaining sets are printed.

If the application has a collate option, make sure it is not selected before sending a print job. The printer driver automatically collates Sample Print jobs by default. If the collate option is selected in the application's [Print] dialog box, there may be more prints than required.

Mac OS / Mac OS X

1. In the application, on the [File] menu, click [Print].

The [Print] dialog box appears.

2. Set the number of copies to two or more.

The sample print job is sent to the machine, and one set is printed.

3. In the pop-up menu, click [Job Log].**4. On the [Job Type:] pop-up menu, select [Sample Print].****5. In the [User ID:] box, enter a user ID using up to eight alphanumeric (a-z, A-Z, 0-9) characters.**

The user ID associates the user with his / her jobs.

6. Check the printed output to make sure the settings are correct.

If the settings are correct, perform the following steps to print the remaining sets.

If you want to delete a saved job, see "Deleting a Sample Print File".

7. On the machine's control panel, press the [Printer] key to display the printer screen.**8. Press [Print Jobs].****9. Press [Sample Print Job List].**

A list of sample print files stored in the machine appears.

[User ID], [Date / Time] and [File Name] also appear.

10. Select the file you want to print by pressing it.

A list of print files stored in the machine appears.

11. Press [Print] to change the number of sets to be printed.**12. Enter the new number of sets using the number keys.**

If you do not want to change the set quantity, perform the following steps.

You can enter up to 999 sets.

Press the [Clear/Stop] key to correct any entry mistakes.

When multiple files are selected without setting a quantity, 1 page less than the minimum number of all settings is applied.

13. Press [Yes].

The remaining sets are printed.

Note

- Press [Stop] to cancel printing.
- When printing finishes, the stored file is deleted.
- To cancel printing, press [Exit]. Then, press [Job Reset]. After it has started, the file is deleted.
- If there is a print job outstanding, this is printed before the sample print job.

Reference

- p.72 "Deleting a Sample Print File"

Deleting a Sample Print File

If the printed document is no longer required, you can delete the Sample Print file.

This procedure uses Windows XP as an example.

1. On the machine's control panel, press the [Printer] key to display the printer screen.

2. Press [Print Jobs].

A list of print files stored in the machine appears.

3. Press [Sample Print Job List].

A list of sample print files stored in the machine appears.

4. Select the file you want to delete by pressing it.

To cancel a selection, press the highlighted jobs again.

Only one file can be selected at a time.

5. Press [Delete].

A confirmation screen appears.

6. Press [Yes] to delete the file.

After the file is deleted the printer screen reappears.

Press [No] to cancel the delete request.

3

How to Use Locked Print

Follow the procedure below to print a document using the Locked Print function.

Windows

1. In the application, on the [File] menu, click [Print].

The [Print] dialog box appears.

2. Select the printer, and then click [Preferences].

3. Click the [Job/Log] tab.

4. In the [Job Type:] list, click [Locked Print].

5. In the [User ID:] box, enter a user ID using up to eight alphanumeric (a-z, A-Z, 0-9) characters, and then enter a 4-8 digit password in the [Password:] box.

The user ID associates user with his / her jobs.

6. Click [OK] to close the printer properties dialog box.

7. Start the printing from the application's [Print] dialog box.

The document file is saved in the machine.

To print the document, perform the following steps.

To delete the document, see "Deleting a Locked Print File".

8. On the machine's control panel, press the [Printer] key to display the printer screen.

9. Press [Print Jobs].

A list of print files stored in the machine appears.

10. Press [Locked Print Job List].

A list of locked print files stored in the machine appears.

[User ID], [Date / Time] and [File Name] also appear.

11. Select the file you want to print by pressing it.

12. Press [Print].

The password screen appears.

13. Enter the password using the number keys, and then press [OK].

A confirmation screen appears.

A confirmation screen will appear if the password is not entered correctly. Press [OK] to enter the password again.

When multiple print files are selected, the machine prints only files that correspond to the entered password. The number of files is displayed on the confirmation screen.

14. Press [Yes].

The locked file is printed.

If the application has a collate option, make sure it is not selected before sending a print job. The printer driver automatically collates Locked Print jobs by default. If the collate option is selected in the application's [Print] dialog box, there may be more prints than required.

Mac OS / Mac OS X

1. In the application, click [Print] on the [File] menu.

The [Print] dialog box appears.

2. In the pop-up menu, click [Job Log].

3. On the [Job Type:] pop-up menu, click [Locked Print].

4. In the [User ID:] box, enter a user ID using up to eight alphanumeric (a-z, A-Z, 0-9) characters, and then enter a 4-8 digit password in the [Password:] box.

The user ID associates the user with his / her jobs.

5. After making the necessary settings, click [Print].

The document file is saved in the machine.

To print the document, perform the following steps.

To delete the document, see "Deleting a Locked Print File".

6. On the machine's control panel, press the [Printer] key to display the printer screen.

7. Press [Print Jobs].

A list of print files stored in the machine appears.

8. Press [Locked Print Job List].

A list of locked print files stored in the machine appears.
[User ID], [Date / Time] and [File Name] also appear.

9. Select the file you want to print by pressing it.

10. Press [Print].

The password screen appears.

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

A confirmation screen appears.

A confirmation screen will appear if the password is not entered correctly. Press [OK] to enter the password again.

When multiple print files are selected, the machine prints only files that correspond to the entered password. The number of files is displayed on the confirmation screen.

12. Press [Yes].

The locked file is printed.

Note

- Press [Stop] to cancel printing.
- To cancel printing, press [Exit]. Then, press [Job Reset]. After it has started, the file is deleted.

Reference

- p.74 "Deleting a Locked Print File"

Deleting a Locked Print File

If the printed document is no longer required, you can delete the Locked Print file.

This procedures use Windows XP as an example.

1. On the machine's control panel, press the [Printer] key to display the printer screen.

2. Press [Print Jobs].

A list of print files stored in the machine appears.

3. Press [Locked Print Job List].

A list of locked print files stored in the machine appears.

4. Select the file you want to delete by pressing it.

To cancel a selection, press the highlighted job again.

Only one file can be selected at a time.

5. Press [Delete].

A password screen appears.

6. Enter the password using the number keys, and then press [OK].

A confirmation screen appears.

A confirmation screen will reappear if the password was entered incorrectly. Press [OK] to enter the password again.

When multiple files are selected, the machine deletes only files that correspond to the entered password. The number of files to be deleted is displayed on the confirmation screen.

7. Press [Yes].

After the file is deleted, the printer screen reappears.

Note

- Press [No] to cancel the delete request.

How to Use Hold Print

Follow the procedure below to print a document using the Hold Print function.

Windows

1. In the application, on the [File] menu, click [Print].

The [Print] dialog box appears.

2. Select the printer, and then click [Preferences].**3. Click the [Job/Log] tab.****4. In the [Job Type:] list, click [Hold Print].****5. In the [User ID:] box, enter a user ID using up to eight alphanumeric (a-z, A-Z, 0-9) characters. [File Name] can also be entered optionally.**

The user ID associates the user with his / her jobs.

6. Click [OK] to close the printer properties dialog box.**7. Start the printing from the application's [Print] dialog box.**

The document file is saved in the machine.

To print the document, perform the following steps.

To delete the document, see "Deleting a Hold Print File".

8. On the machine's control panel, press the [Printer] key to display the printer screen.**9. Press [Print Jobs].**

A list of print files stored in the machine appears.

10. Press [Hold Print Job List].

A list of hold print files stored in the machine appears.

[User ID], [Date / Time] and [File Name] also appear.

Depending on the security settings, certain print jobs may not be displayed.

11. Select the file you want to print by pressing it.

12. Press [Print].

13. A confirmation screen appears.

14. Press [Yes].

The hold print file is printed.

If the application has a collate option, make sure it is not selected before sending a print job. The printer driver automatically collates Hold Print files by default. If a collate option is selected from the application's Print dialog box, there may be more prints than required.

Mac OS / Mac OS X

1. From an application, on the [File] menu, click [Print].

The [Print] dialog box appears.

2. In the pop-up menu, click [Job Log].

3. On the [Job Type:] pop-up menu, click [Hold Print].

4. In the [User ID:] box, enter the user ID using up to eight alphanumeric (a-z, A-Z, 0-9) characters. [File Name] can also be set.

The user ID associates the user with his / her jobs.

5. After making the necessary settings, click [Print].

The document file is saved in the machine.

To print the document, perform the following steps.

To delete the document, see "Deleting a Hold Print File".

6. On the machine's control panel, press the [Printer] key to display the printer screen.

7. Press [Print Jobs].

A list of print files stored in the machine appears.

8. Press [Hold Print Job List].

A list of hold print files stored in the machine appears.

[User ID], [Date / Time] and [File Name] also appear.

Depending on the security settings, certain print jobs may not be displayed.

9. Select the file you want to print by pressing it.

10. Press [Print].

A confirmation screen appears.

11. Press [Yes].

The hold print file is printed.

Note

- Press [Stop] to cancel printing.
- To cancel printing, press [Exit]. Then, press [Job Reset]. After it has started, the file is deleted.
- When printing is completed, the stored file is deleted.

Reference

- p.77 "Deleting a Hold Print File"

Deleting a Hold Print File

If the printed document is no longer required, you can delete the Hold Print file.

This procedure uses Windows XP as an example.

1. On the machine's control panel, press the [Printer] key to display the printer screen.**2. Press [Print Jobs].**

A list of the print files stored in the machine appears.

3. Press [Hold Print Job List].

A list of Hold Print files stored in the machine appears.

Depending on the security settings, certain print jobs may not be displayed.

4. Select the file you want to delete by pressing it.**5. Press [Delete].**

A confirmation screen appears.

6. Press [Yes].

After the file is deleted, the printer screen reappears.

Note

- Press [No] to cancel the delete request.

How to Use Stored Print/Store and Print

Follow the procedure below to print a document using the Stored Print function.

Windows

- 1. In the application, on the [File] menu, click [Print].**

The [Print] dialog box appears.

- 2. Select the printer, and then click [Preferences].**

- 3. Click the [Job/Log] tab.**

- 4. In the [Job Type:] list, click [Stored Print] or [Store and Normal Print].**

- [Stored Print]

Stores the file in the printer and print it later using the control panel.

- [Store and Normal Print]

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

- 5. In the [User ID:] box, enter a user ID using up to eight alphanumeric (a-z, A-Z, 0-9) characters. A file name and password can also be entered optionally.**

The user ID associates the user with his / her job.

You can assign a password to a saved document, but password assignment is not mandatory.

The same password must be entered when printing or deleting.

- 6. Click [OK] to close the printer properties dialog box.**

- 7. Start the printing from the application's [Print] dialog box.**

The document file is saved in the machine.

To print the document, perform the following steps.

To delete the document, see "Deleting a Stored Print File".

- 8. On the machine's control panel, press the [Printer] key to display the printer screen.**

- 9. Press [Print Jobs].**

A list of print files stored in the machine appears.

- 10. Press [Stored Print Job List].**

A list of stored print files stored in the machine appears.

[User ID], [Date / Time] and [File Name] also appear.

Depending on the security settings, certain print jobs may not be displayed.

- 11. Select the file you want to print by pressing it.**

- 12. Press [Print].**

A confirmation screen appears.

If you have already set a password, proceed to the following step.

13. Enter a password using the number keys on the password screen, and then press [OK].

A confirmation screen will appear if the password is not entered correctly. Press [OK] to enter the password again.

If you have not set the password, proceed to the following step.

14. Press [Yes].

The stored file is printed.

If the application has a collate option, make sure it is not selected before sending a print job. The printer driver automatically collates Stored Print files by default. If a collate option is selected from the application's Print dialog box, there may be more prints than required.

Mac OS / Mac OS X**1. In the application, on the [File] menu, click [Print].**

The [Print] dialog box appears.

2. In the pop-up menu, click [Job Log].**3. On the [Job Type:] pop-up menu, click [Stored Print] or [Store and Print].**

- [Stored Print]

Stores the file in the printer and print it later using the control panel.

- [Store and Print]

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

4. In the [User ID:] box, enter a user ID using up to eight alphanumeric (a-z, A-Z, 0-9) characters, and then enter a 4-8 digit password in the [Password:] box. [File Name] can also be set.

The user ID associates the user with his / her jobs.

You can assign a password to a saved document, but password assignment is not mandatory.

The password must be entered when printing or deleting.

5. After making the necessary settings, click [Print].

The document file is saved in the machine.

To print the document, perform the following steps.

To delete the document, see "Deleting a Stored Print File".

6. On the machine's control panel, press the [Printer] key to display the printer screen.**7. Press [Print Jobs].**

A list of print files stored in the machine appears.

8. Press [Stored Print Job List].

A list of stored print files stored in the machine appears.

[User ID], [Date / Time] and [File Name] also appear.

Depending on the security settings, certain print jobs may not be displayed.

9. Select the file you want to print by pressing it.

10. Press [Print].

A confirmation screen appears.

If you have already set a password, proceed to the following step.

11. Enter a password using the number keys on the password screen, and then press [OK].

A confirmation screen will appear if the password is not entered correctly. Press [OK] to enter the password again.

If you have not set the password, proceed to the following step.

12. Press [Yes].

The stored file is printed.

Note

- Press [Stop] to cancel printing.
- To cancel printing, press [Exit]. Then, press [Job Reset]. After it has started, the file is deleted.
- Stored Print file sent to the machine is not deleted unless you delete them in the machine or select [Auto Delete Stored Print Jobs] (see "System", Printer Reference). For details, see "Deleting a Stored Print File".

Reference

- p.80 "Deleting a Stored Print File"

Deleting a Stored Print File

If the printed document is no longer required, you can delete the Stored Print file.

This procedures use Windows XP as an example.

1. On the machine's control panel, press the [Printer] key to display the printer screen.

2. Press [Print Jobs].

A list of print files stored in the machine appears.

3. Press [Stored Print Job List].

A list of stored print files stored in the machine appears.

4. Select the file you want to delete by pressing it.

To cancel a selection, press the highlighted job again.

5. Press [Delete].

A confirmation screen appears.

6. Press [Yes].

After the file is deleted, the printer screen reappears.

Note

- Press [No] to cancel the delete request.
- If you have already set a password in the printer driver, enter it to delete.

How to Use Document Server

Follow the procedure below to print a document using the Document Server function.

Important

- An optional hard disk drive is required to use the Document Server function.
- If you are using Mac OS X 10.1.x, this function cannot be used
- If you are using Mac OS X 10.2.x or higher, the Job Type function can be used.

Windows**1. In the application, on the [File] menu, click [Print].**

The [Print] dialog box appears.

2. Select the printer, and then click [Preferences].**3. Click the [Job/Log] tab.****4. In the [Job Type:] list, click [Send to Document Server].****5. In the [User name] box, enter a user ID in the dialog box that appears. A file name and password can also be entered optionally.**

The user ID associates the user with his / her job.

You can assign a password to a saved document, but password assignment is not mandatory.

The same password must be entered when printing or deleting.

6. Click [OK].**7. Start the printing from the application's [Print] dialog box.****Mac OS X****1. In the application, on the [File] menu, click [Print].**

The [Print] dialog box appears.

2. In the pop-up menu, click [Job Log].**3. On the [Job Type:] pop-up menu, click [Document Server].****4. Enter a user ID, file name, and password in the dialog box that appears. The file name and password are optional.**

5. Start the printing from the application's [Print] dialog box.

User Code

Use this to set a user code for print logging.

Enter a user code using up to eight digits. A user code identifies a group of users and allows you to check the number of sheets printed under each code with SmartDeviceMonitor for Admin.

The following table shows the tabs or menus where you can select this function.

Windows	Select [Enabled] on [Log], and then enter a user code in the [User Code:] box on the [Job/Log] tab in the Printing Preferences dialog box.
Mac OS	Select the [Enable User Code] check box, and then enter a user code in the [User Code] box on [Job Log] in the print dialog box.
Mac OS X	Select the [Enable User Code] check box, and then enter a user code in the [User Code] box on [Job Log] in the print dialog box.

↓ Note

- For details about using SmartDeviceMonitor for Admin, see SmartDeviceMonitor for Admin Help.

Paper Size

Use this to select the size of paper you want to use.

The following table shows the tabs or menus where you can select this function.

Windows	[Paper Size:] is displayed on [Paper Options] on the [Paper/Quality] tab in the Printing Preference dialog box.
Mac OS	[Paper:] is displayed on the [Page Attributes] tab in the Page Setup dialog box.
Mac OS X	[Paper Size:] is displayed in the Page Setup dialog box.

↓ Note

- For details about the paper sizes supported by this machine, see General Setting Guide.

Fit to Paper

When the size of the document and paper size differ, set whether or not to print according to paper size.

Windows	[Fit to Paper] is displayed on [Document Options] on the [Advanced] tab in the Printing Preferences dialog box.
Mac OS	[Fit to Paper] is displayed on [Printer Specific Options] in the print dialog box.
Mac OS X	[Fit to Paper] is displayed under [General 1] in the [Feature Sets] list on [Printer Features] in the print dialog box.

3

[Prompt User]

Print is performed with the size of document to be printed unchanged.

[Nearest Size and Scale]

If the paper size is smaller than the selected paper size, the driver reduces the print size.

If the paper size is larger than the size of document to be printed, print is not to fit the paper size.

[Nearest Size and Crop]

When the paper size is smaller than the size of document to be printed, print is adjusted to meet the paper size.

Input Slot

Use this to select the paper sources.

The following table shows the tabs or menus where you can select this function.

Windows	[Paper Size:] is displayed on [Paper Options] on the [Paper/Quality] tab in the Printing Preference dialog box.
Mac OS	[Paper Source:] is displayed on [General] in the print dialog box.
Mac OS X	[All Pages from:] is displayed on [Paper Feed] in the print dialog box.

Note

- For details about the paper sources, see Printer Reference.

Resolution

Use this to set the resolution types.

The following table shows the tabs or menus where you can select this function.

3

Windows	[Resolutions:] is displayed on [Print Quality] on the [Paper/Quality] tab in the Printing Preferences dialog box.
Mac OS	[Resolution:] is displayed on [Printer Specific Options] in the print dialog box.
Mac OS X	[Resolution] is displayed under [General 1] in the [Feature Sets] list on [Printer Features] in the print dialog box.

Note

- For more information about the resolution types, see Printer Reference.

Orientation

Use this to set the paper orientation.

The following table shows the tabs or menus where you can select this function.

Windows	[Orientation] is displayed on the [Paper/Quality] tab in the Printing Preferences dialog box.
Mac OS	[Orientation] is displayed on the [Page Attributes] tab in the Page Setup dialog box.
Mac OS X	[Orientation] is displayed in the Page Setup dialog box.

You can select the following items:

- [Landscape]
- [Portrait]
- [Rotated Landscape]

Note

- If you are using a Mac OS or Mac OS X, click to select the button that means "Landscape" or "Portrait".
- Under Mac OS, "Rotated Landscape" cannot be selected.

Rotate by 180 degrees

Use this to rotate the print image by 180 degrees.

The following table shows where you can select this function.

Windows	Check the [Rotate by 180 degrees] checkbox on [Orientation] on the [Paper/Quality] tab in the Printing Preference dialog box.
Mac OS	[Rotate by 180 degrees:] is displayed in [Printer Specific Options] in the print dialog box.
Mac OS X	[Rotate by 180 degrees] is displayed under [General 3] in the [Feature Sets] list on [Printer Features] in the print dialog box.

3

Copies

Use this function to specify the number of copies to print.

The following table shows the tabs or menus where you can select this function.

Windows	[Copies] is displayed on the [Paper/Quality] tab in the Printing Preferences dialog box.
Mac OS	[Copies:] is displayed on [General] in the print dialog box.
Mac OS X	[Copies:] is displayed in the print dialog box.

Orientation Override

Use this to set the paper orientation.

The following table shows the tabs or menus where you can select this function.

Windows	[Orientation Override] is displayed on [Document Options] on the [Advanced] tab in the Printing Preferences dialog box.
Mac OS	[Orientation Override:] is displayed on [Printer Specific Options] in the print dialog box.
Mac OS X	[Orientation Override] is displayed under [General 3] in the [Feature Sets] list on [Printer Features] in the print dialog box.

You can select the following items:

- [Off]
- [Landscape]
- [Portrait]

Print Mode

Use this to select the print mode.

The following table shows the tabs or menus where you can select this function.

Windows	[Print Mode] is displayed on [Paper/Quality] tab in the Printing Preferences dialog box.
Mac OS	[Print Mode:] is displayed on [Printer Specific Options] in the print dialog box.
Mac OS X	[Print Mode:] is displayed under [General 1] in the [Feature Sets] list on [Printer Features] in the print dialog box.

You can select the following items:

Through

Disables print mode.

Edge Smoothing

Smooths jagged lines in text and graphics to produce a finer image.

Toner Saving

Reduces the amount of toner used when printing.

Duplex Printing

Use this function to select duplex printing.

★ Important

- To use this function, the optional duplex unit must be installed on the machine.

The following table shows the tabs or menus where you can select this function.

Windows	[Print on Both Sides] is displayed on the [Finishing] tab in the Printing Preferences dialog box.
Mac OS	[Print on Both Sides] is displayed on [Layout] in the print dialog box.
Mac OS X	<ul style="list-style-type: none"> • 10.3 or higher The [Two-Sided:] check box is displayed on [Layout] in the print dialog box. • Other Mac OS X The [Print on both Sides] is displayed check box on [Duplex] in the print dialog box.

3

The following items may vary depending on the operating system you are using.

Windows 2000 / XP / Vista, Windows Server 2003 / 2003 R2 / 2008, Mac OS

Off

Disables Duplex Printing.

Long Edge

Prints output so that you can open it to the long edge when bound along the long edge.

Short Edge

Prints output so that you can open it to the short edge when bound along the short edge.

↓ Note

- If you are using a Mac OS, click to select the button that means "Flip on Long Edge" or "Flip on Short Edge".

Mac OS X

The following functions are selectable under Mac OS X 10.3 or higher.

Off

Disables Duplex Printing.

Long-Edge Binding

Prints output so that you can open it to the long edge when bound along the long edge.

Short-Edge Binding

Prints output so that you can open it to the short edge when bound along the short edge.

Note

- If you are using Mac OS X 10.2 or earlier, see "Windows 2000 / XP / Vista, Windows Server 2003 / 2003 R2 / 2008, Mac OS".

Reference

- p.87 "Windows 2000 / XP / Vista, Windows Server 2003 / 2003 R2 / 2008, Mac OS"

Pages per Sheet

Use this function to specify the number of pages to be printed on a single sheet of paper.

The following table shows the tabs or menus where you can select this function.

Windows	[Pages per Sheet] is displayed on [Finishing] tab in the Printing Preferences dialog box.
Mac OS	[Pages per Sheet:] is displayed on [Layout] in the print dialog box.
Mac OS X	[Pages per Sheet:] is displayed on [Layout] in the print dialog box.

Pages per Sheet Layout

Use this function to specify the layout when printing multiple pages onto a single sheet of paper.

The following table shows the tabs or menus where you can select this function.

Windows	[Pages per Sheet Layout] is displayed on [Finishing] tab in the Printing Preferences dialog box.
Mac OS	[Layout Direction:] is displayed on [Layout] in the print dialog box.
Mac OS X	[Layout Direction:] is displayed on [Layout] in the print dialog box.

Note

- If you are using a Mac OS or Mac OS X, click to select the button.

Draw Border

Use this function to specify whether or not to draw a page border on each page.

The following table shows the tabs or menus where you can select this function.

Windows	Check the [Draw Border] checkbox on [Finishing] tab in the Printing Preferences dialog box.
Mac OS	[Border:] is displayed on [Layout] in the print dialog box.
Mac OS X	[Border:] is displayed on [Layout] in the print dialog box.

3

Collate

Use this function to enable collation. With this feature, the machine can efficiently print collated sets of multiple-page documents.

Important

- **To use this function, a memory unit of at least 192 MB or hard disk drive must be installed on the machine.**

The following table shows the tabs or menus where you can select this function.

Windows	Set the number of copies to two or more, and then click the [Collate] checkbox on the [Paper/Quality] tab in the Printing Preference dialog box.
Mac OS	[Collated:] is displayed under on [Printer Specific Options] in the print dialog box.
Mac OS X	Check the [Collated] checkbox in the printer dialog box.

Paper Type

Use this to select the paper type.

The following table shows the tabs or menus where you can select this function.

Windows	[Media Type] is displayed on [Paper Options] on the [Paper/Quality] tab in the Printing Preference dialog box.
Mac OS	[Paper Type:] is displayed on [Printer Specific Options] in the print dialog box.
Mac OS X	[Paper Type:] is displayed under [General 1] in the [Feature Sets] list on [Printer Features] in the print dialog box.

↓ Note

- For details about the media type supported by this machine, see General Setting Guide.

Destination Tray

Use this to select the destination tray.

The following table shows where you can select this function.

Windows	[Destination] is displayed on [Output Tray] on the [Finishing] tab in the Printing Preference dialog box.
Mac OS	[Destination:] is displayed in [Printer Specific Options] in the print dialog box.
Mac OS X	[Destination:] is displayed under [General 1] in the [Feature Sets] list on [Printer Features] in the print dialog box.

↓ Note

- For details about the destination tray supported by this machine, see Network and System Settings Guide.

Staple

Use this function to staple sheets of printed paper together.

★ Important

- When stapling, use the finisher option. See General Setting Guide or Printer Reference.

The following table shows where you can select this function.

Windows	[Staple] is displayed on [Print Job] on the [Finishing] tab in the Printing Preference dialog box.
Mac OS	[Staple:] is displayed in [Printer Specific Options] in the print dialog box.
Mac OS X	[Staple:] is displayed under [General 2] in the [Feature Sets] list on [Printer Features] in the print dialog box.

3

↓ Note

- The stapling location might differ depending on the orientation of the machine set in the printer and the orientation of the data to be printed. For details, see Printer Reference.

Punch

Use this function to punch holes in the printed documents.

★ Important

- **When punching holes, use the finisher option. See Printer Reference.**

The following table shows where you can select this function.

Windows	[Punch] is displayed on [Print Job] on the [Finishing] tab in the Printing Preference dialog box.
Mac OS	[Punch:] is displayed in [Printer Specific Options] in the print dialog box.
Mac OS X	[Punch:] is displayed under [General 2] in the [Feature Sets] list on [Printer Features] in the print dialog box.

↓ Note

- Punch positions and the number of punch holes that are available will change depending on the type of finisher, the original's orientation, and the printing paper size and orientation. For details, see Printer Reference.

Fold Type

Use this function to select a fold type for your printed documents.

★ Important

- **This function requires the optional folding finisher unit. See Printer Reference.**

The following table shows where you can select this function.

Windows	[Fold Type:] is displayed on [Document Options] on the [Advanced] tab in the Printing Preference dialog box.
Mac OS	[Fold Type:] is displayed in [Printer Specific Options] in the print dialog box.
Mac OS X	[Fold Type:] is displayed under [General 2] in the [Feature Sets] list on [Printer Features] in the print dialog box.

You can select the following fold types:

None

Disables fold.

Half Fold

Folds prints in half along their long edge.

Letter Fold-in

Folds prints into thirds with their two end segments folded one on top of the other.

Letter Fold-out

Folds prints into thirds with their two end segments folded in opposite directions.

Double Parallel Fold

Folds prints in half and then in half again with all folding edges aligned parallel to each other.

Gate Fold

Folds prints into four segments, with their two end segments folded inward.

You can have the print appear on the inside or outside of the sheets' folds.

Inside printing

In the print dialog box, specify only the type of fold that you require. By default, the print will appear on the inside of the folds.

If you want the folded sheets to open to the left or top, you must also select [Rotate by 180 degrees] in the print dialog box.

Outside printing

If you want the print to appear on the outside of the folds, in the print dialog box you must select [Letter Fold-out] for the type of fold. When this fold is selected, the print appears on the outside of the folds by default. If you select any other type of fold, the print will appear on the inside of the folds.

If you want the folded sheets to open to the left or top, you must also select [Rotate by 180 degrees] in the print dialog box.

If you want to specify other types of fold, use one of the following procedures.

- When one-sided printing is enabled

In the print dialog box, select the fold type you require and set [Eject Face-up:] to [On].

If you want the folded sheets to open to the left or top, you must also select [Rotate by 180 degrees] in the print dialog box.

- When duplex printing is enabled

Windows

In the print dialog box, select the fold type you require and set [Page Output Order] to [Back to Front].

If you want the folded sheets to open to the left or top, you must also select [Rotate by 180 degrees] in the print dialog box.

Mac OS X

In the print dialog box, select the fold type you require and set [Page Order] to [Reverse].

If you want the folded sheets to open to the left or top, you must also select [Rotate by 180 degrees] in the print dialog box.

Note

- In some applications, changing the [Orientation:] setting to [Landscape] can result in folded sheets opening in the opposite direction to that specified in the print dialog box.
- The reverse order printing function might not work from some applications. If this is the case, specify reverse order printing using the application's settings.
- [Page Order] can be set to [Reverse] only under Mac OS 10.3 and later.
- For details about how output of sheets varies according to the type of fold, see Printer Reference.

Z-fold

Use this function to specify the position of the folds when using Z-fold function.

Important

- **This function requires the optional folding finisher unit. See Printer Reference.**

The following table shows where you can select this function.

Windows	[Z-fold] is displayed on [Print Job] on the [Finishing] tab in the Printing Preference dialog box.
Mac OS	[Z-fold:] is displayed in [Printer Specific Options] in the print dialog box.
Mac OS X	[Z-fold:] is displayed under [General 2] in the [Feature Sets] list on [Printer Features] in the print dialog box.

3

You can select the following items:

Off

Disables Z-fold.

Bottom Fold

Folds prints so that their bottom end segment is on top.

Right Fold

Folds prints so that their rightmost segment is on top.

Left Fold

Folds prints so that their leftmost segment is on top.

Multi-sheet Fold

Use this function to specify multi-sheet fold.

The following table shows where you can select this function.

Windows	[Multi-sheet Fold:] is displayed on [Document Options] on the [Advanced] tab in the Printing Preference dialog box.
Mac OS	[Multi-sheet Fold:] is displayed in [Printer Specific Options] in the print dialog box.
Mac OS X	[Multi-sheet Fold:] is displayed under [General 2] in the [Feature Sets] list on [Printer Features] in the print dialog box.

Reduce/Enlarge

Use this function to specify a scaling mode for reducing or enlarging the print size of documents.

The following table shows the tabs or menus where you can select this function.

Windows	[Reduce/Enlarge] is displayed on [Effects] tab in the Printing Preferences dialog box.
MacOS X	[Scale:] is displayed on [Preview].

You can select the following items for Windows:

Full Size

Prints the document at its original size.

Print on

Prints the document by scaling it up or down to fit the specified paper size.

Scale To Fit

Prints the document at the specified reproduction ratio.

You can select the following items for MacOS X:

Scale

Prints the document at the specified reproduction ratio.

Scale To Fit

Select whether to scale the image so that the entire image fits on one page or scale the image so that it covers the entire page.

Watermark

Set the Watermark function.

Windows	[Watermark] is displayed on [Document Option] on the [Advanced] tab in the Printing Preferences dialog box.
MacOS X	[Watermark:] is displayed under [General 3] in the [Feature Sets] list on [Printer Features] in the print dialog box.

↓ Note

- When using this function under Mac OS, see the printer driver Help.

Watermark Text

Select the Watermark Text type.

Windows	[Watermark Text] is displayed on the [Advanced] tab in the Printing Preferences dialog box.
MacOS X	[Watermark Text:] is displayed under [General 3] in the [Feature Sets] list on [Printer Features] in the print dialog box.

↓ Note

- When using this function under Mac OS, see the printer driver Help.

Watermark Font

Select the Watermark Font type.

Windows	[Watermark Font] is displayed on the [Advanced] tab in the Printing Preferences dialog box.
MacOS X	[Watermark Font:] is displayed under [General 3] in the [Feature Sets] list on [Printer Features] in the print dialog box.

↓ Note

- When using this function under Mac OS, see the printer driver Help.

Watermark Size

Select the Watermark size.

Windows	[Watermark Size] is displayed on the [Advanced] tab in the Printing Preferences dialog box.
MacOS X	[Watermark Size:] is displayed under [General 4] in the [Feature Sets] list on [Printer Features] in the print dialog box.

Note

- When using this function under Mac OS, see the printer driver Help.

Watermark Angle

Select the Watermark angle.

Windows	[Watermark Angle] is displayed on the [Advanced] tab in the Printing Preferences dialog box.
MacOS X	[Watermark Angle:] is displayed under [General 4] in the [Feature Sets] list on [Printer Features] in the print dialog box.

Note

- When using this function under Mac OS, see the printer driver Help.

Watermark Style

Select the Watermark style.

Windows	[Watermark Style] is displayed on the [Advanced] tab in the Printing Preferences dialog box.
MacOS X	[Watermark Style:] is displayed under [General 4] in the [Feature Sets] list on [Printer Features] in the print dialog box.

Note

- When using this function under Mac OS, see the printer driver Help.

Dithering

Use this to set the Image Rendering mode.

The following table shows the tabs or menus where you can select this function.

Windows	[Dithering] is displayed on [Document Options] on the [Advanced] tab in the Printing Preferences dialog box.
---------	--

Mac OS	[Dithering:] is displayed on [Printer Specific Options] in the print dialog box.
Mac OS X	[Dithering:] is displayed under [General 2] in the [Feature Sets] list on [Printer Features] in the print dialog box.

You can select the following items:

3

Auto

Use this setting to configure the best dithering method automatically depending on the appearance of the document to be printed.

Photographic

Performs dithering using an appropriate pattern for photographs.

Text

Performs dithering using an appropriate pattern for text.

User Setting

Use this setting to print images set in half tone in your application.

Image Smoothing

Use this to select the image smoothing type.

The following table shows the tabs or menus where you can select this function.

Windows	[Image Smoothing] is displayed on [Document Options] on the [Advanced] tab in the Printing Preferences dialog box.
Mac OS	[Image Smoothing:] is displayed on [Printer Specific Options] in the print dialog box.
Mac OS X	[Image Smoothing:] is displayed under [General 1] in the [Feature sets] tab on [Printer Features] in the print dialog box.

You can select the following items:

Off

Disables image smoothing.

On

Performs image smoothing unconditionally.

Auto

Performs image smoothing automatically for images that have a resolution less than 25% of supported printer resolution.

Less than 90 ppi - Less than 300 ppi

Performs image smoothing only when the image has an image resolution (pixels per inch) less than the respective value you have selected in the list.

↓ Note

- When [Auto] is selected, data processing may take a long time.
- When Image Smoothing is used for a mask image, this function may have an undesired effect on the print result.

4. Printer Utility for Mac

Installing Printer Utility for Mac

Follow these steps to install Printer Utility for Mac on the machine.

★ Important

- If a Macintosh and printer are connected by USB, you cannot use Printer Utility for Mac.

1. Start the Mac OS.

2. Insert the CD-ROM into the CD-ROM drive.

The CD-ROM icon appears.

3. Double-click the CD-ROM icon.

The contents of the CD-ROM appear.

4. Double-click the [Mac OS] folder.

Under Mac OS X, double-click the [Mac OS X] folder.

5. Double-click the [PS Utility] folder on the CD-ROM, and then drag the [Printer Utility for Mac] file, and then drop it into the Macintosh hard disk.

6. Drag the CD-ROM icon and drop it into [Trash] to eject the CD-ROM.

Printer Utility for Mac is installed.

↓ Note

- Printer Utility for Mac is included on the CD-ROM labeled "Printer Drivers and Utilities".
- Printer Utility for Mac requires Mac OS 8.1 or higher. (Mac OS X Classic environment is supported.)
- Printer Utility for Mac cannot use Mac OS X (native mode).

Starting Printer Utility for Mac

The following instructions describe how to start Printer Utility for Mac.

Mac OS

★ Important

- Before starting Printer Utility for Mac, make sure the printer is selected in [Chooser] on the Apple menu.

4

1. Double-click the **Printer Utility for Mac** icon.

The [Printer Utility for Mac] dialog box appears.

2. Click [OK].

Printer Utility for Mac will take a few seconds to start.

Mac OS X

1. Double-click the **Printer Utility for Mac** icon.

The [Printer Utility for Mac] dialog box appears.

2. Click [OK].

3. In the [Available Printers:] box, select the printer you want to use.

If you change zones, select a name from [Available Network Zones:].

Click [Choose Printer...] on the Printer Utility for Mac menu if you want to change the printer.

4. Select the printer you want to use.

Printer Utility for Mac will take a few seconds to start.

5. Click [Choose].

Printer Utility for Mac Functions

Printer Utility for Mac functions are described below.

File menu

- [Download PS Fonts...]
Download fonts (PostScript Type 1) to the printer. See Downloading PS Fonts.
- [Display Printer's Fonts...]
Display and delete the fonts in printer memory and the printer's hard disk drive.
See Displaying Printer's Fonts.
- [Initialize Printer's Disk...]
Initialize the printer's hard disk drive. See Initializing the Printer Disk.
- [Page Setup...]
Set up the paper size to print "Printer Font Catalog" and "Printer Font Sample".
See Page Setup.
- [Print Fonts Catalog...]
Print the names of available fonts. See Printing Fonts Catalog.
- [Print Fonts Sample...]
Print a sample of fonts. See Printing Fonts Sample.
- [Rename Printer...]
Change the printer's name when viewed via AppleTalk. See Renaming the Printer.
- [Restart Printer]
Restart the printer. See Restarting the Printer.

Utility menu

- [Download PostScript File...]
Download a PostScript file. See Downloading PostScript Files.
- [Select Zone...]
Change the zone to which the printer belongs to via AppleTalk. See Selecting the Zone.
- [Display Printer Status...]
Display the status of the printer. See Displaying the Printer Status.
- [Launch Dialogue Console...]
Create and edit a PostScript file, and then download it to the printer. See Launching the Dialogue Console.

Downloading PS Fonts

You can download the PS fonts to the printer's memory or hard disk drive.

★ Important

- The following procedures to download the fonts assume that you are a system administrator. If you are not, be sure to consult your system administrator.
- If the printer restarts, all the printer settings return to their defaults.
- Confirm that a Mac OS and the printer are connected with AppleTalk.
- During the download, do not turn off the power switch, operate the panel or open or close the cover.

4

1. Select [Download PS Fonts...] on the [File] menu.

2. Click [Add to list].

The dialog box to select fonts appears.

3. Click to select the desired font files, and then click [Open].

The list of selectable font names appears.

4. After adding all the fonts you want to download, click [OK].

The dialog box of selected fonts to download appears.

5. Click [Download].

The fonts begin to download, and the download status is shown.

6. When the completion message appears, click [OK].

7. Click [Cancel].

↓ Note

- Some fonts cannot be downloaded.
- Before downloading, read the documentation about the fonts you want to use.

Displaying Printer's Fonts

You can display the available fonts currently downloaded to the printer. Fonts in the printer's memory and hard disk drive can be displayed.

1. Select [Display Printer's Fonts...] on the [File] menu.

A dialog box appears.

2. Select [Printer's memory] or [Printer's disk].

3. Click [OK].

Note

- The fonts displayed in italics are the default fonts.

Deleting Fonts

You can delete fonts from the printer's memory or hard disk drive.

Important

- You cannot delete the fonts displayed in italic.
1. Select [Display Printer's fonts] on the [File] menu.
A dialog box appears.
 2. Select [Printer's memory] or [Printer's disk].
 3. Select the fonts you want to delete.
 4. Click [Delete].
A confirmation message appears.
 5. Confirm the fonts you want to delete and the machine name from which you want to delete the fonts.
 6. Click [Continue], and then click [OK].
 7. Click [OK].

Initializing the Printer Disk

When initializing the printer's hard disk drive, all the fonts downloaded to the printer's hard disk drive are deleted. Before initializing, be sure to check the fonts on the hard disk drive.

Important

- When initializing the printer's hard disk drive from the operation panel, all of the data on the printer's hard disk drive is deleted. Before initializing, be sure to check the data on the hard disk drive.
 - Do not turn off the power switch until initializing is completed, otherwise the hard disk drive might be damaged.
1. Select [Initialize Printer's Disk...] on the [File] menu.
The confirmation message appears.
To cancel initialization, click [Cancel].
 2. Click [Execute].
Initialization starts.
 3. When the completion message appears, click [OK].

Page Setup

You can set the paper size on which to print "Print Fonts Catalogue" and "Prints Fonts Sample".

1. Select [Page Setup...] on the [File] menu.
2. Choose the paper size.
3. Click [OK].

Printing Fonts Catalog

Print the names of fonts available on the printer.

1. Select [Print Fonts Catalog...] on the [File] menu.
2. Click [Print].

 **Note**

- The paper selected under [Page Setup] is used.

Printing Fonts Sample

You can print samples of fonts downloaded to the hard disk drive or memory.

1. Select [Print Fonts Sample...] on the [File] menu.
2. Click [Print].

 **Note**

- Print by using the paper selected on [Page Setup].

Renaming the Printer

You can change the machine name displayed under AppleTalk. If you connect several printers on the network, assign different names so you can identify them. If several machines have the same name, a digit appears next to the machine name in [Chooser].

 **Important**

- You can enter up to 31 digits and letters.
- Do not use symbols, for example "*", ":", "=", "@", "~".

Mac OS

1. On the [File] menu, click [Rename Printer...].

2. In the [New Name:] field enter a new name.
3. Click [Rename].

The machine name is changed.
4. Click [OK].
5. On the Apple menu, click [Chooser].
6. Click the [AdobePS] icon.
7. Select the printer whose name you changed, and then close the [Chooser] dialog box.

If there are several AppleTalk zones, select the zone the machine belongs to.

Mac OS X

1. On the [File] menu, click [Rename Printer...].
2. In the [New Name:] field enter a new name.
3. Click [Rename].

The machine name is changed.
4. Click [OK].
5. On the Printer Utility for Mac menu, click [Choose Printer...].
6. In the [Available Network Zones:] list, select the zone for the Macintosh in use.
7. In the [Available Printers:] list, select the printer whose name you changed, and then click [Choose].

Restarting the Printer

You can restart the printer.

1. Select [Restart Printer] on the [File] menu.
2. Confirm the message that appears on the screen, and then click [Restart].

The printer restarts.

The fonts that you downloaded in the printer's memory will be deleted.

If the printer restarts, all the printer settings return to their defaults.

Downloading PostScript Files

You can download a Postscript file to the printer.

1. Select [Download PostScript File...] on the [Utility] menu.
2. Select the file name to download and click the file name, and then click [Open].

3. Type the log file name, and then click [Save...].

The selected file is downloaded.

Errors are recorded in the log file.

Selecting the Zone

You can change the zone to which the printer belongs under AppleTalk.

★ Important

- Confirm that a Macintosh and printer are connected with AppleTalk.

4

Mac OS

1. On the [Utility] menu, click [Select Zone...].

The zone to which the printer belongs and the available zone list appears.

2. Select the zone in which you want to locate the printer, and then click [Change].

A confirmation message appears.

3. Click [Continue].

A confirmation message appears.

4. Click [OK].

5. On the Apple menu, click [Chooser].

6. Click the [AdobePS] icon.

7. In the [AppleTalk zone:] list, select the zone you changed.

8. In the [Select a PostScript Printer:] list, select the printer you want to use.

9. Close the [Chooser] dialog box.

Mac OS X

1. On the [Utility] menu, click [Select Zone...].

The zone to which the printer belongs and the available zone list appears.

2. Select the zone which you want to locate the printer in, and then click [Change].

A confirmation message appears.

3. Click [Continue].

A confirmation message appears.

4. Click [OK].

5. On the [Printer Utility for Mac] menu, click [Choose Printer...].

6. In the [Available Network Zones:] list, select the zone you changed.

7. In the [Available Printers:] list, select the model of printer in use, and then click [Choose].

Displaying the Printer Status

You can display and confirm the current status of the printer.

1. Select [Display Printer Status...] on the [Utility] menu.

The current status of the printer appears.

2. Confirm the current status of the printer.

You can confirm the memory capacity, the VM (Virtual Memory) space, the hard disk drive status and available space on the hard disk drive. You can also confirm the zone to which the printer belongs to.

3. Click [OK].

Launching the Dialogue Console

You can create and edit a PostScript file for printing, and then download it to the printer.

★ Important

- "Launch Dialogue Console" is recommended for users with an understanding of PostScript.
- Do not download any file other than PostScript files to the printer.
- "Launch Dialogue Console" must be used at your own responsibility.

1. Select [Launch Dialogue Console...] on the [Utility] menu.

Open the editing screen. The Dialogue Console menu bar appears.

2. Type the PostScript command in the editor screen.

To edit a PostScript file, select [Open] on the [File] menu to open it.

You can search or replace a character string by using the [Search] menu.

3. After editing the PostScript file, select [Download Top Window] on [Console] menu to start printing.

The PostScript file is sent to the printer.

The [Reply from Printer] box opens, depending on the PostScript file you sent.

4. Select [Return To Main Menu] on the [Console] menu to close the PostScript file.

5. Appendix

Trademarks

- Adobe, Acrobat, Acrobat Reader, Adobe Type Manager, PageMaker, PostScript, and Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.
- Apple, AppleTalk, Bonjour, EtherTalk, Macintosh, Mac OS, and TrueType are registered trademarks of Apple Inc., registered in the United States and other countries.
- The Bluetooth® word mark and logos are owned by the Bluetooth SIG, Inc. and any use of such marks by Ricoh Company, Ltd. is under license.
- Other product names used herein are for identification purposes only and might be trademarks of their respective companies. We disclaim any and all rights to those marks.
- Microsoft®, Windows®, Windows Server®, and Windows Vista® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

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
 - 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 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

INDEX

A

About This Machine.....5

B

Bluetooth.....44
 Adding a Printer.....44

C

Changing to EtherTalk.....62
 Mac OS.....58
Collate.....89
Copies.....85
Copy and Document Server Reference.....5

D

Deleting a Hold Print File.....77
Deleting a Locked Print File.....74
Deleting a Sample Print File.....72
Deleting a Stored Print File.....80
Deleting Fonts.....105
Destination Tray.....90
Displaying Printer's Fonts.....104
Displaying the Printer Status.....109
Dithering.....97
Document Server.....81
Downloading PostScript Files.....107
Downloading PS Fonts.....104
Draw Border.....89
Duplex Printing.....87

F

Fit to Paper.....83
Fold Type.....92
Functions
 Printer Utility for Mac.....103

H

How to Read This Manual.....8

I

Image Smoothing.....98
Initializing Printer Disk.....105
Input Slot.....83
Installing
 Printer Utility for Mac.....101

Installing Adobe Type Manager
 Mac OS.....57

Installing Screen fonts
 Mac OS.....57

Installing the PostScript 3 Printer Driver and PPD File
 Mac OS.....55

Installing the PPD Files
 Mac OS X.....59

Installing the Printer Driver Using USB
 Windows 2000.....36
 Windows Me.....36
 Windows Vista.....36
 Windows XP/2003/2003 R2.....36

J

Job Type.....67

L

Launching the Dialogue Console.....109

M

Mac OS X.....59
Multi-sheet Fold.....94

N

Network and System Settings Guide.....5

O

Orientation.....84
Other manuals.....5

P

Page Setup.....106
Pages per Sheet.....88
Pages per Sheet Layout.....88
Paper Size.....82
Paper Type.....89
PostScript 3 Supplement.....5
Print Mode.....86
Printer Reference.....5
Printer Utility for Mac.....101, 106, 108
 Functions.....103
Printing Fonts Catalog.....106
Printing Fonts Sample.....106
Printing with Parallel Connection
 Windows 2000.....40

Punch.....91

R

Reduce/Enlarge.....94

Renaming the Printer.....106

Resolution.....84

Restarting the Printer.....107

Rotate by 180 degrees.....85

S

Scanner Reference.....5

Security Reference.....5

Selecting the Zone.....108

Setting Up Options.....65

 Mac OS.....56

 Mac OS X.....60

Setting Up PPD Files

 Mac OS.....56

Setting Up the PPD File

 Mac OS X.....59

Staple.....90

T

Troubleshooting.....5

U

User Code.....82

Using Bonjour

 Mac OS X.....61

Using USB Interface

 Mac OS X.....61

W

Watermark.....95

Watermark Angle.....97

Watermark Font.....96

Watermark Size.....96

Watermark Style.....97

Watermark Text.....96

Windows 2000

 printer properties, PostScript 3.....50

Windows Server 2003

 printer properties, PostScript 3.....51

Windows Vista

 printer properties, PostScript 3.....53

Windows XP

 printer properties, PostScript 3.....51

Z

Z-fold.....93

MEMO

MEMO

