

*MP 171F/MP 171SPF*  
**Aficio™ MP 171F/171SPF**  
**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.....                       | 7  |
| Notice.....   | 9  |
| Important.....                                      | 9  |
| How to Read This Manual.....                        | 10 |
| Symbols.....  | 10 |
| Display.....  | 10 |
| IP Address.....                                     | 11 |
| Note.....   | 11 |
| Laws and Regulations.....                           | 12 |
| Legal Prohibition.....                              | 12 |
| <b>1. Getting Started</b>                           |    |
| 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.....                     | 20 |
| <b>2. Configuring Administrator Authentication</b>  |    |
| Administrators.....                                 | 21 |
| User Administrator.....                             | 21 |
| Machine Administrator.....                          | 22 |
| Network Administrator.....                          | 22 |
| File Administrator.....                             | 22 |
| Supervisor.....                                     | 22 |
| About Administrator Authentication.....             | 23 |
| Enabling Administrator Authentication.....          | 25 |
| Specifying Administrator Privileges.....            | 25 |
| Registering the Administrator.....                  | 27 |
| Logging on Using Administrator Authentication.....  | 32 |
| Logging off Using Administrator Authentication..... | 33 |

---

|  |    |
|--|----|
| Changing the Administrator.....  | 33 |
| 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.....  | 48 |
| Specifying Basic Authentication.....   | 48 |
| Authentication Information Stored in the Address Book.....                     | 53 |
| Specifying Login User Names and Passwords.....                                 | 53 |
| Specifying Login Details.....  | 56 |
| Windows Authentication.....  | 60 |
| Specifying Windows Authentication.....   | 61 |
| Installing Internet Information Services (IIS) and Certificate Services.....   | 67 |
| Creating the Server Certificate.....   | 67 |
| If the fax number cannot be obtained.....                                      | 68 |
| Installing the Device Certificate (Issued by a Certificate Authority).....     | 68 |
| LDAP Authentication.....   | 70 |
| Specifying LDAP Authentication.....  | 71 |
| Integration Server Authentication.....   | 78 |
| Specifying Integration Server Authentication.....                              | 78 |
| Printer Job Authentication.....  | 87 |
| If User Authentication is Specified.....                                       | 90 |
| If User Code Authentication is Specified.....                                  | 90 |
| If Basic, Windows, LDAP or Integration Server Authentication is Specified..... | 91 |
| User Lockout Function.....   | 93 |
| Auto Logout.....   | 95 |
| Authentication Using an External Device.....                                   | 97 |

### 4. Protecting Data from Information Leaks

---

|                                       |    |
|---------------------------------------|----|
| 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.....                | 104 |

## 5. Securing Information Sent over the Network or Stored on Hard Disk

---

|  |     |
|--|-----|
| Preventing Information Leakage Due to Unauthorized Transmission..... | 107 |
| Restricting Destinations.....  | 107 |
| Using S/MIME to Protect E-mail Transmission.....                     | 110 |
| E-mail Encryption.....   | 110 |
| Attaching an Electronic Signature.....                               | 112 |
| Protecting the Address Book.....                                     | 118 |
| Configuring Address Book Access Permissions.....                     | 118 |
| Encrypting Data in the Address Book.....                             | 120 |
| Encrypting Data on the Hard Disk.....                                | 124 |
| Enabling the Encryption Settings.....                                | 124 |
| Printing the Encryption Key.....                                     | 126 |
| Updating the Encryption Key.....                                     | 127 |
| Canceling Data Encryption.....                                       | 129 |
| Deleting Data on the Hard Disk.....                                  | 132 |
| Auto Erase Memory.....   | 132 |
| Erase All Memory.....  | 136 |

## 6. Managing Access to the Machine

---

|   |     |
|---|-----|
| Preventing Changes to Machine Settings.....               | 141 |
| Menu Protect.....   | 143 |
| Specifying Menu Protect.....                              | 143 |
| Limiting Available Functions.....                         | 147 |
| Specifying Which Functions are Available.....             | 147 |
| Managing Log Files.....                                   | 150 |
| Using the Control Panel to Specify Log File Settings..... | 150 |
| Using Web SmartDeviceMonitor to Manage Log Files.....     | 153 |
| Using Web Image Monitor to Manage Log Files.....          | 153 |
| Logs that can be Managed Using Web Image Monitor.....     | 157 |

---

## 7. Enhanced Network Security

---

|   |     |
|---|-----|
| Preventing Unauthorized Access.....   | 163 |
| Access Control.....   | 163 |
| Enabling and Disabling Protocols.....   | 164 |
| Specifying Network Security Level.....  | 172 |
| Encrypting Transmitted Passwords.....   | 176 |
| Specifying a Driver Encryption Key.....                                       | 176 |
| Specifying a Group Password for PDF Files.....                                | 178 |
| Specifying an IPP Authentication Password.....                                | 179 |
| Protection Using Encryption.....  | 181 |
| SSL (Secure Sockets Layer) Encryption.....                                    | 181 |
| User Settings for SSL (Secure Sockets Layer).....                             | 186 |
| Setting the SSL/TLS Encryption Mode.....                                      | 186 |
| SNMPv3 Encryption.....  | 188 |
| Transmission Using IPsec.....   | 190 |
| Encryption and Authentication by IPsec.....                                   | 190 |
| Encryption Key Auto Exchange Settings and Encryption Key Manual Settings..... | 191 |
| IPsec Settings.....   | 192 |
| Encryption Key Auto Exchange Settings Configuration Flow.....                 | 200 |
| Encryption Key Manual Settings Configuration Flow.....                        | 205 |
| telnet Setting Commands.....  | 206 |
| Authentication by telnet.....   | 214 |
| "authfree" Command.....   | 214 |
| Authentication by IEEE802.1X.....   | 215 |

## 8. Specifying the Extended Security Functions

---

|  |     |
|--|-----|
| Specifying the Extended Security Functions.....    | 217 |
| Changing the Extended Security Functions.....      | 217 |
| Extended Security Settings.....                    | 218 |
| Other Security Functions.....                      | 223 |
| Fax Function.....                                  | 223 |
| Scanner Function.....                              | 224 |
| Limiting Machine Operations to Customers Only..... | 225 |
| Settings.....                                      | 225 |

---

|   |     |
|---|-----|
| Additional Information for Enhanced Security.....                   | 228 |
| Settings you can Configure Using the Control Panel.....             | 228 |
| Settings you can Configure Using Web Image Monitor.....             | 230 |
| Settings you can Configure when IPsec is Available/Unavailable..... | 231 |

## 9. Troubleshooting

---

|  |     |
|--|-----|
| If Authentication Fails.....           | 235 |
| If a Message is Displayed.....         | 235 |
| If the Machine Cannot Be Operated..... | 237 |

## 10. Appendix

---

|  |     |
|--|-----|
| Supervisor Operations.....                     | 241 |
| Logging on as the Supervisor.....              | 241 |
| Logging off as the Supervisor.....             | 242 |
| Changing the Supervisor.....                   | 242 |
| Resetting the Administrator's Password.....    | 245 |
| Machine Administrator Settings.....            | 248 |
| System Settings.....                           | 248 |
| Copier Features.....                           | 250 |
| Fax Features.....                              | 250 |
| Printer Features.....                          | 251 |
| Scanner Features.....                          | 252 |
| Settings via Web Image Monitor.....            | 253 |
| Settings via SmartDeviceMonitor for Admin..... | 257 |
| Network Administrator Settings.....            | 258 |
| System Settings.....                           | 258 |
| Fax Features.....                              | 259 |
| Printer Features.....                          | 259 |
| Scanner Features.....                          | 259 |
| Settings via Web Image Monitor.....            | 260 |
| Settings via SmartDeviceMonitor for Admin..... | 262 |
| File Administrator Settings.....               | 263 |
| System Settings.....                           | 263 |
| Fax Features.....                              | 263 |
| Printer Features.....                          | 263 |

---

|  |     |
|--|-----|
| Settings via Web Image Monitor.....                              | 264 |
| User Administrator Settings.....                                 | 265 |
| System Settings.....   | 265 |
| Settings via Web Image Monitor.....                              | 265 |
| Settings via SmartDeviceMonitor for Admin.....                   | 266 |
| The Privilege for User Account Settings in the Address Book..... | 267 |
| User Settings - Control Panel Settings.....                      | 270 |
| Copier Features.....   | 271 |
| Printer Features.....  | 272 |
| Scanner Features.....  | 276 |
| Fax Features.....  | 278 |
| System Settings.....   | 281 |
| User Settings - Web Image Monitor Settings.....                  | 287 |
| Device Settings.....   | 288 |
| Printer.....   | 294 |
| Scanner.....   | 300 |
| Fax.....   | 302 |
| Interface.....   | 305 |
| Network.....   | 307 |
| Webpage.....   | 311 |
| Functions That Require Options.....                              | 312 |
| Trademarks.....  | 313 |
| <b>INDEX</b> .....   | 315 |

---

# 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, and other consumables.

## Troubleshooting

Provides a guide for resolving common usage-related problems.

## Copy Reference

Explains Copier 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 Fax Guide
- Quick Reference Printer 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 <sup>*1</sup>  | DeskTopBinder                    |
| ScanRouter EX Professional <sup>*1</sup> and ScanRouter EX Enterprise <sup>*1</sup>                    | the ScanRouter delivery software |
| Web SmartDeviceMonitor Professional IS <sup>*1</sup> and Web SmartDeviceMonitor Standard <sup>*1</sup> | 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.

---

## Display

---

The display panel shows machine status, error messages, and function menus.

When you select or specify an item on the display panel, it is highlighted like **100%**.

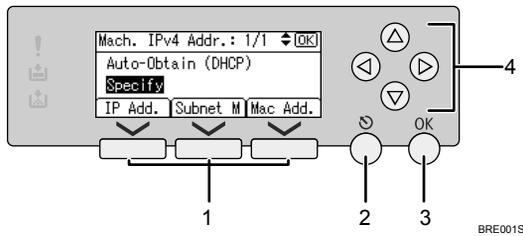
The copy display is set as the default screen when the machine is turned on.



---

## Reading the Display and Using Keys

---



### 1. Selection keys

Correspond to items at the bottom line on the display.

- When the instruction "press [IP Addr.]" appears in this manual, press the left selection key.
- When the instruction "press [Subnet M]" appears in this manual, press the center selection key.
- When the instruction "press [Mac Add.]" appears in this manual, press the right selection key.

### 2. [Escape] key

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

### 3. [OK] key

Press to set a selected item or entered numeric value.

### 4. Scroll keys

Press to move the cursor to each direction one by one.

When [▲][▼][▶], or [◀] key appears in this manual, press the scroll key of the same direction.

---

## 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.

---

## Note

---

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

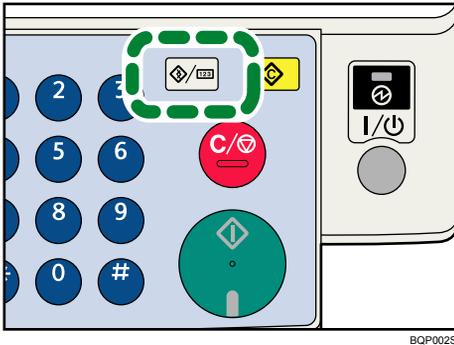
### ★ Important

- **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.

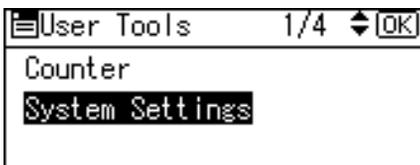
# Setting Up the Machine

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/Counter] key.



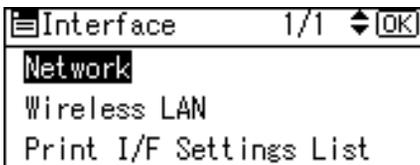
3. Press [System Settings] using [▲] or [▼], and then press the [OK] key.



4. Press [Interface Settings] using [▲] or [▼], and then press the [OK] key.



5. Select [Network] using [▲] or [▼], and then press the [OK] key.



6. Specify IPv4 Address.

For details on how to specify the IPv4 address, see "Interface Settings", Network and System Settings Guide.

7. Connect the machine to the network.

**8. 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".

**9. Install the device certificate.**

For information on how to install the device certificate, see "Protection Using Encryption".

**10. Enable secure sockets layer (SSL).****11. 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 7 to 10. 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 7.

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.181 "Protection Using Encryption"
- p.27 "Registering the Administrator"
- p.242 "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.21 "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.

## 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. 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.48 "Basic Authentication"
- p.147 "Limiting Available Functions"

---

## Ensuring Information Security

---

### 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".

### 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 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.99 "Printing a Confidential Document"
- p.107 "Preventing Information Leakage Due to Unauthorized Transmission"
- p.110 "Using S/MIME to Protect E-mail Transmission"
- p.118 "Protecting the Address Book"
- p.150 "Managing Log Files"
- p.124 "Encrypting Data on the Hard Disk"
- p.132 "Deleting Data on the Hard Disk"

---

## Limiting and Controlling Access

---

### 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.141 "Preventing Changes to Machine Settings"
- p.147 "Limiting Available Functions"

---

## Enhancing Network Security

---

### Preventing Unauthorized Access

You can limit IP addresses or disable ports to prevent unauthorized access over the network and protect the Address Book, 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.163 "Preventing Unauthorized Access"
- p.176 "Encrypting Transmitted Passwords"
- p.181 "Protection Using Encryption"
- p.190 "Transmission Using IPsec"

# 2. Configuring Administrator Authentication

This chapter explains 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 access limitations and other 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.27 "Registering the Administrator"
- p.241 "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 files. The file administrator can carry out such tasks as deleting Locked Print files and changing passwords.

---

## Supervisor

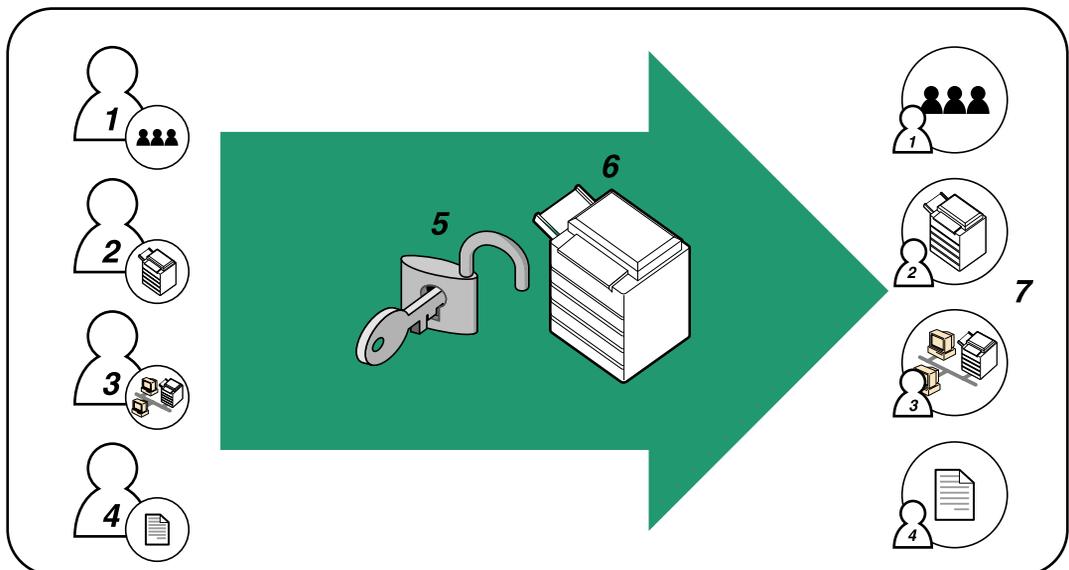
---

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 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 is the administrator who manages files. The file administrator can carry out such tasks as deleting Locked Print files and changing passwords.

## 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.21 "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.27 "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.

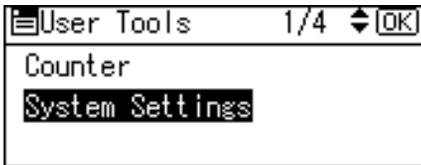
The defaults are "admin" for the login name and blank for the password. For details about changing the administrator password using the supervisor's authority, see "Supervisor Operations".

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/Counter] key.
2. Press [System Settings] using [▲] or [▼], and then press the [OK] key.



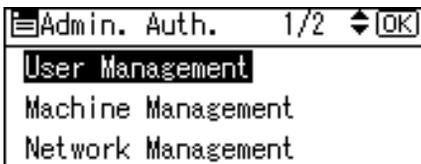
3. Select [Administrator Tools] using [▲] or [▼], and then press the [OK] key.



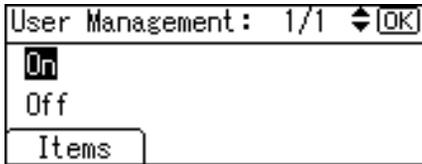
4. Press [Admin. Auth. Management] using [▲] or [▼], and then press the [OK] key.



5. Select [User Management], [Machine Management], [Network Management], or [File Management] using [▲] or [▼], and then press the [OK] key.

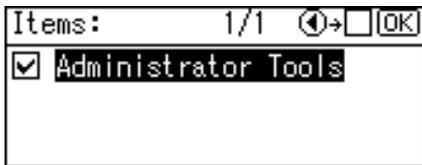


6. Select [On] using [▲] or [▼], and then press the [OK] key.



[Items] appears.

7. Select the settings to manage from [Items] using [▶], and then press the [OK] key.



The selected settings will be unavailable to users.

[Items] varies depending on the administrator.

For details about "Items", see "Limiting Available Functions".

The box next to a selected item is checked. To deselect the item, press [◀].

To specify administrator authentication for more than one category, repeat steps 5 to 7.

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

#### Reference

- p.241 "Supervisor Operations"
- p.32 "Logging on Using Administrator Authentication"
- p.33 "Logging off Using Administrator Authentication"
- p.147 "Limiting Available Functions"

## Registering the Administrator

If administrator authentication has been specified, we recommend only one person take each administrator role.

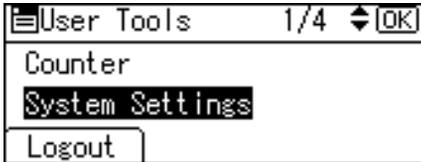
The sharing of administrator tasks eases the burden on individual administrators while also limiting unauthorized operation by a single administrator. You can register up to four login user names (Administrators 1-4) to which you can grant administrator privileges.

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".

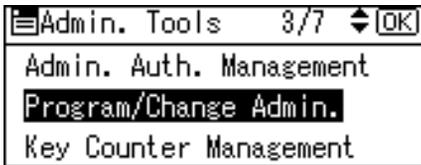
1. Press the [User Tools/Counter] key.
2. Select [System Settings] using [▲] or [▼], and then press the [OK] key.



3. Select [Administrator Tools] using [▲] or [▼], and then press the [OK] key.



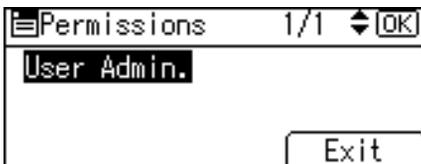
4. Select [Program/Change Admin.] using [▲] or [▼], and then press the [OK] key.



5. Select [Permissions] using [▲] or [▼], and then press the [OK] key.



6. Select the administrator, and then press the [OK] key.



7. Select [Administrator 1], [Administrator 2], [Administrator 3] or [Administrator 4] using [▲] or [▼], and then press the [▶] key.

User Admin.: 1/2 ◀▶◂◃ [OK]

Administrator1

Administrator2

Administrator3

The box next to a selected item is checked. To deselect the item, press [◀].

8. Press the [OK] key.

User Admin.: 2/2 ◀▶◂◃ [OK]

Administrator4

9. Press [Exit].

Permissions 1/1 ◀▶ [OK]

User Admin.

Exit

10. Select [Admin. Detailed Settings] using [▲] or [▼], and then press the [OK] key.

Prog/Chge Admin 1/1 ◀▶ [OK]

Admin. Detailed Settings

Permissions

Exit

11. Select the setting you want to specify, and then press the [OK] key.

Admin. Settings 1/1 ◀▶ [OK]

Administrator1

Exit

12. Select [Login User Name] using [▲] or [▼], and then press the [OK] key.

Administrator1 1/2 ◀▶ [OK]

Login User Name

Login Password

Exit

13. Enter the login user name, and then press the [OK] key.

|                  |       |
|------------------|-------|
| Login User Name: | [OK]  |
| Enter user name. |       |
| abc              | admin |
|                  |       |

14. Select [Login Password] using [▲] or [▼], and then press the [OK] key.

|                    |        |
|--------------------|--------|
| Administrator1 1/2 | ◆ [OK] |
| Login User Name    |        |
| Login Password     |        |
| Exit               |        |

15. Enter the login password, and then press the [OK] key.

|                 |      |
|-----------------|------|
| Login Password: | [OK] |
| Enter password. |      |
| abc             |      |
|                 |      |

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".

16. If a password reentry screen appears, enter the login password, and then press the [OK] key.

|                           |      |
|---------------------------|------|
| Confirm Password:         | [OK] |
| Please re-enter password. |      |
| abc                       | _    |
|                           |      |

17. Select [Encryption Password] using [▲] or [▼], and then press the [OK] key.

|                     |        |
|---------------------|--------|
| Administrator1 2/2  | ◆ [OK] |
| Encryption Password |        |
| Exit                |        |

18. Enter the encryption password, and then press the [OK] key.

|                      |      |
|----------------------|------|
| Encryption Password: | [OK] |
| Enter password.      |      |
| abc                  | _    |
|                      |      |

19. If a password reentry screen appears, enter the encryption password, and then press the [OK] key.

|                           |      |
|---------------------------|------|
| Confirm Enchr.Password:   | [OK] |
| Please re-enter password. |      |
| abc                       |      |
|                           |      |

20. Press [Exit] three times.

|                     |      |
|---------------------|------|
| Administrator1 2/2  | [OK] |
| Encryption Password |      |
|                     |      |
| Exit                |      |

You will be automatically logged off.

21. Press the [User Tools/Counter] 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.32 "Logging on Using Administrator Authentication"
- p.33 "Logging off Using Administrator Authentication"
- p.217 "Specifying the Extended Security Functions"

## Logging on Using Administrator Authentication

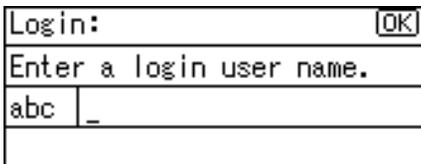
If administrator authentication has been specified, log on using an administrator's user name and password. This section describes how to log on. When you log on with a user name that has multiple administrator authorities, one of the authorities associated with that name is displayed.

2

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

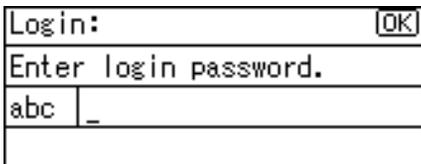


3. Enter the login user name, and then press the [OK] key.



When you log on to the machine for the first time as the administrator, enter "admin".

4. Enter the login password, and then press the [OK] key.



If assigning the administrator for the first time, press the [OK] key without entering login password.

"Authenticating... Please wait." appears, followed by the screen for specifying the default. To log on as an administrator, enter the administrator's login user name and login password.

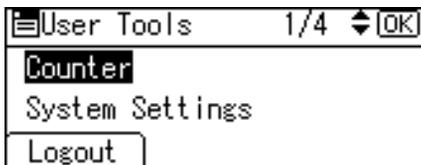
### Note

- If you try to log on from an operating screen, "Privileges are required. Administrator-login is limited to setting changes only." appears. Press the [User Tools/Counter] key to change the default.
- If user authentication has already been specified, a screen for authentication appears.
- 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.

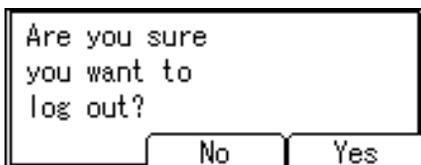
## Logging off Using Administrator Authentication

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 [Logout].



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".

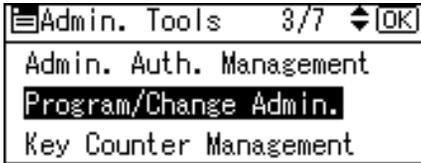
1. Press the [User Tools/Counter] key.
2. Select [System Settings] using [▲] or [▼], and then press the [OK] key.



3. Select [Administrator Tools] using [▲] or [▼], and then press the [OK] key.



4. Select [Program/Change Admin.] using [▲] or [▼], and then press the [OK] key.



5. Select [Permissions] using [▲] or [▼], and then press the [OK] key.



6. Select the administrator, and then press the [OK] key.



7. Select [Administrator 1], [Administrator 2], [Administrator 3] or [Administrator 4] using [▲] or [▼], and then press the [▶] key.

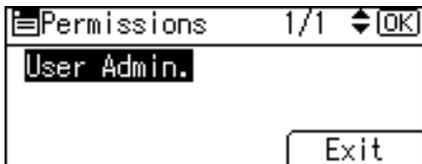


The box next to a selected item is checked. To deselect the item, press [◀].

8. Press the [OK] key.



9. Press [Exit].



10. Select [Admin. Detailed Settings] using [▲] or [▼], and then press the [OK] key.



11. Select the administrator you want to change settings using [▲] or [▼], and then press the [OK] key, and re-enter the setting.



12. Press [Exit] three times.

You are logged off automatically.

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

### Reference

- p.32 "Logging on Using Administrator Authentication"
- p.33 "Logging off Using Administrator Authentication"

## Using Web Image Monitor to Configure Administrator Authentication

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 explains what a user can do, how to specify user authentication, and how to log on to 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.

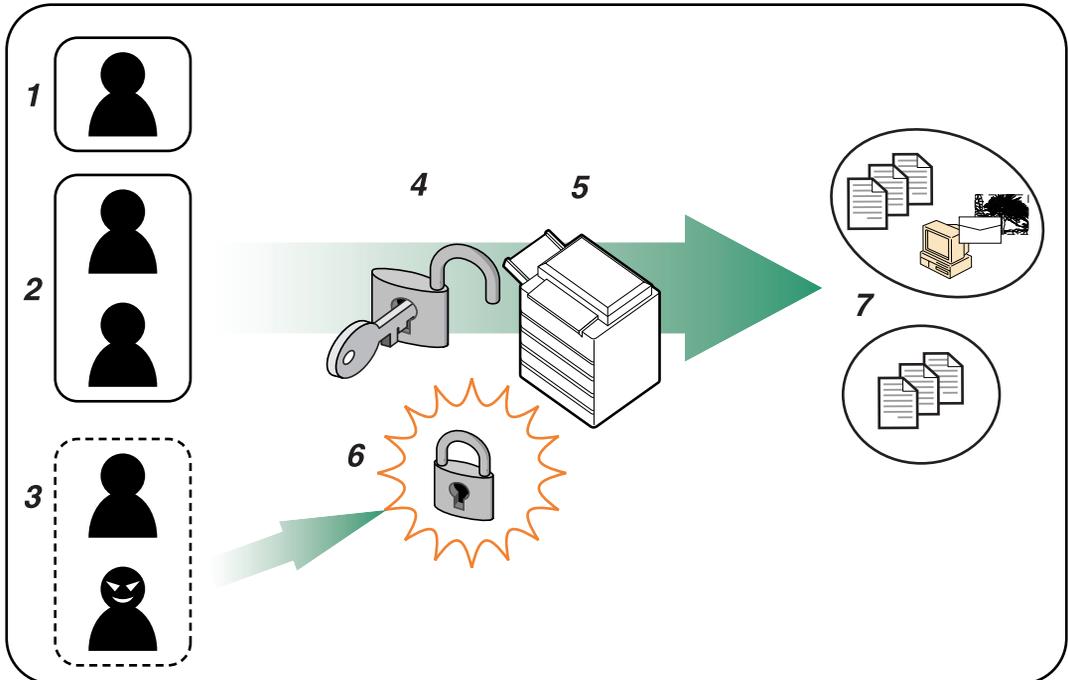
### 📖 Reference

- p.21 "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<br/>See "Enabling Administrator Authentication".</p> | <p>Specifying Administrator Privileges<br/>See "Specifying Administrator Privileges".<br/>Registering the Administrator<br/>See "Registering the Administrator".</p>   |
| <p>User Authentication<br/>See "Enabling User Authentication".</p>                   | <p>Specifying User Authentication<br/><b>Authentication that requires only the machine:</b></p> <ul style="list-style-type: none"> <li>• User Code Authentication<br/>See "User Code Authentication".</li> <li>• Basic Authentication<br/>See "Basic Authentication".</li> </ul> <p><b>Authentication that requires external devices:</b></p> <ul style="list-style-type: none"> <li>• Windows Authentication<br/>See "Windows Authentication".</li> <li>• LDAP Authentication<br/>See "LDAP Authentication".</li> <li>• Integration Server Authentication<br/>See "Integration Server Authentication".</li> </ul> |

3

## ↓ 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.25 "Enabling Administrator Authentication"
- p.41 "Enabling User Authentication"
- p.25 "Specifying Administrator Privileges"
- p.27 "Registering the Administrator"
- p.42 "User Code Authentication"
- p.48 "Basic Authentication"

- p.60 "Windows Authentication"
- p.70 "LDAP Authentication"
- p.78 "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.53 "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

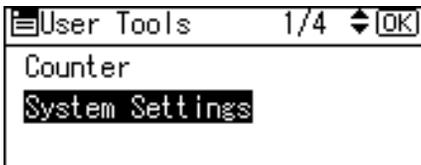
### ★ Important

- 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.

1. Press the [User Tools/Counter] key.
2. Select [System Settings] using [▲] or [▼], and then press the [OK] key.



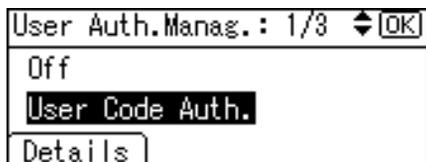
3. Select [Administrator Tools] using [▲] or [▼], and then press the [OK] key.



4. Select [User Auth. Management] using [▲] or [▼], and then press the [OK] key.

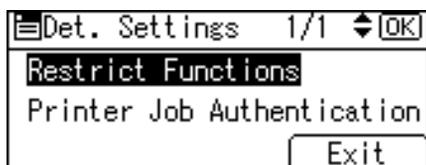


5. Select [User Code Auth.] using [▲] or [▼], and then press [Details].

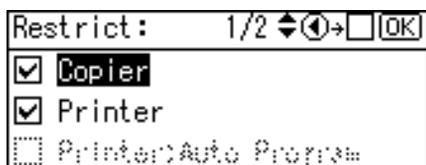


If you do not want to use user authentication management, select [Off].

6. Select [Restrict Functions] using [▲] or [▼], and then press the [OK] key.



7. Select which of the machine's functions you want to limit using [▲] or [▼], and then press the [▶] key.

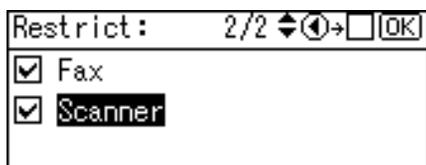


The box next to a selected item is checked. To deselect the item, press [◀].

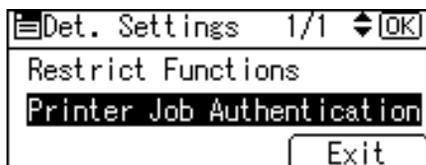
The selected settings will be unavailable to users.

For details about limiting available functions for individuals or groups, see "Limiting Available Functions".

8. Press the [OK] key.



9. Select [Printer Job Authentication] using [▲] or [▼], and then press the [OK] key.



10. 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.147 "Limiting Available Functions"
- p.44 "Selecting Entire or Simple (All)"
- p.45 "Selecting Simple (Limitation)"
- p.87 "Printer Job Authentication"

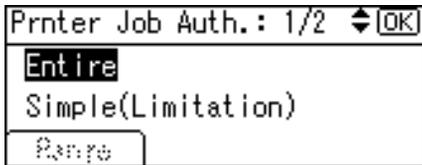
## 3

### 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.

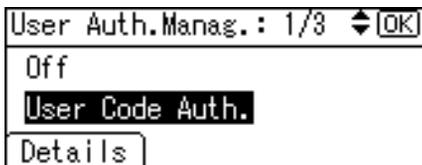
1. Select [Entire] or [Simple(All)] using [▲] or [▼], and then press the [OK] key.



2. Press [Exit].



3. Press the [OK] key.



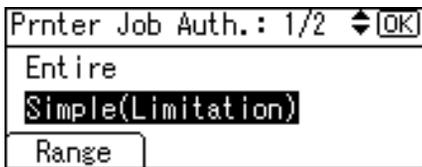
4. Press the [User Tools/Counter] key.

## Selecting Simple (Limitation)

If you select [Simple(Limitation)], you can specify clients for which printer job authentication is not required. Specify [Parallel Interface(Sim.)], [USB(Sim.)] 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. Select [Simple(Limitation)] using [▲] or [▼], and then press [Range].



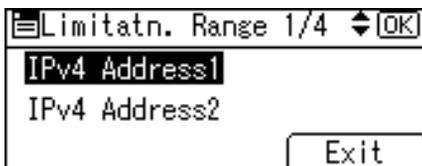
Specify the range in which [Simple(Limitation)] is applied to Printer Job Authentication.

If you specify IPv4 address range, proceed to step 2.

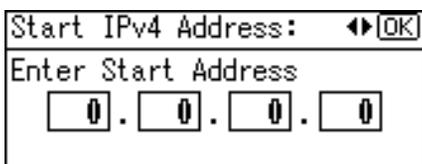
If you specify [Parallel Interface(Sim.)], proceed to step 5.

If you specify [USB(Sim.)], proceed to step 7.

2. Select [IPv4 Address 1], [IPv4 Address 2], [IPv4 Address 3], [IPv4 Address 4] or [IPv4 Address 5] using [▲] or [▼], and then press the [OK] key.



3. Enter the Start IPv4 Address, and then press the [OK] key.



You can specify the IPv4 address range to which this setting is applied.

4. Enter the End IPv4 Address, and then press the [OK] key.

Be sure the number you enter for End IPv4 Address is larger than that for Start IPv4 Address.

5. Select [Parallel Interface(Sim.)] using [▲] or [▼], and then press the [OK] key.

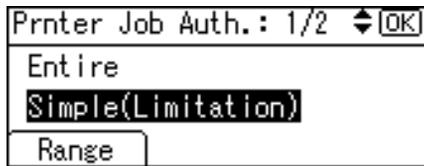
6. Select [Apply] using [▲] or [▼], and then press the [OK] key.

7. Select [USB(Sim.)] using [▲] or [▼], and then press the [OK] key.

8. Select [Apply] using [▲] or [▼], and then press the [OK] key.

9. Press [Exit].

10. Press the [OK] key.



11. Press the [User Tools/Counter] 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 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 "Admin. Auth. 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/Counter] key.
2. Select [System Settings] using [▲] or [▼], and then press the [OK] key.



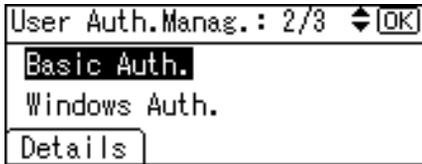
3. Select [Administrator Tools] using [▲] or [▼], and then press the [OK] key.



4. Select [User Auth. Management] using [▲] or [▼], and then press the [OK] key.



5. Select [Basic Auth.] using [▲] or [▼], and then press [Details].

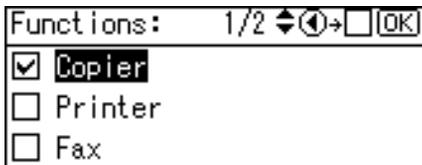


If you do not want to use user authentication management, select [Off].

6. Select [Function Permissions] using [▲] or [▼], and then press the [OK] key.



7. Select which of the machine's functions you want to permit using [▲] or [▼], and then press the [▶] key.

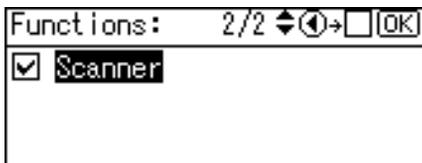


The box next to a selected item is checked. To deselect the item, press [◀].

The functions you select here become the default Basic Authentication settings that will be assigned to all new users of the Address Book.

For details about specifying available functions for individuals or groups, see "Limiting Available Functions".

8. Press the [OK] key.



9. Select [Printer Job Authentication] using [▲] or [▼], and then press the [OK] key.



10. 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.32 "Logging on Using Administrator Authentication"
- p.33 "Logging off Using Administrator Authentication"
- p.147 "Limiting Available Functions"
- p.50 "Selecting Entire or Simple (All)"
- p.51 "Selecting Simple (Limitation)"
- p.87 "Printer Job Authentication"

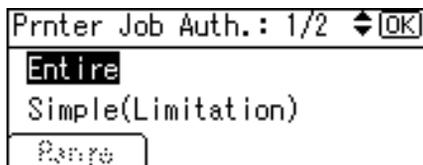
## 3

### 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.

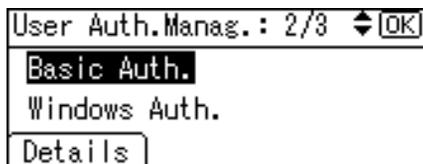
1. Select [Entire] or [Simple(All)] using [▲] or [▼], and then press the [OK] key.



2. Press [Exit].



3. Press the [OK] key.



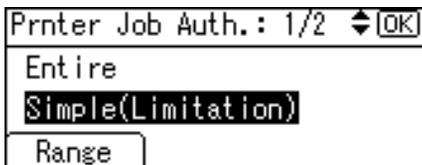
4. Press the [User Tools/Counter] key.

## Selecting Simple (Limitation)

If you select [Simple(Limitation)], you can specify clients for which printer job authentication is not required. Specify [Parallel Interface(Sim.)], [USB(Sim.)] 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. Select [Simple(Limitation)] using [▲] or [▼], and then press [Range].



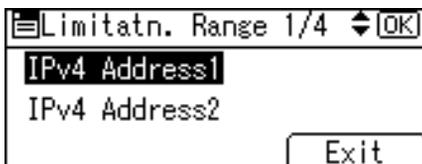
Specify the range in which [Simple(Limitation)] is applied to Printer Job Authentication.

If you specify IPv4 address range, proceed to step 2.

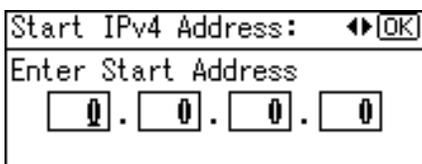
If you specify [Parallel Interface(Sim.)], proceed to step 5.

If you specify [USB(Sim.)], proceed to step 7.

2. Select [IPv4 Address 1], [IPv4 Address 2], [IPv4 Address 3], [IPv4 Address 4] or [IPv4 Address 5] using [▲] or [▼], and then press the [OK] key.

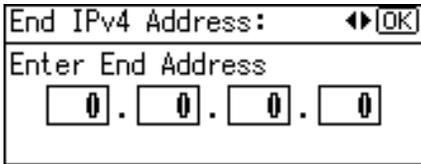


3. Enter the Start IPv4 Address, and then press the [OK] key.



You can specify the IPv4 address range to which this setting is applied.

4. Enter the End IPv4 Address, and then press the [OK] key.



Be sure the number you enter for End IPv4 Address is larger than that for Start IPv4 Address.

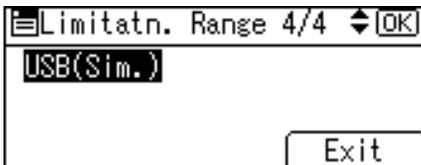
5. Select [Parallel Interface(Sim.)] using [▲] or [▼], and then press the [OK] key.



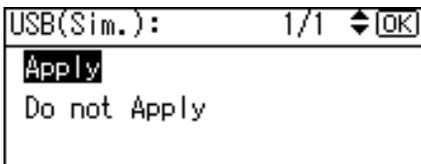
6. Select [Apply] using [▲] or [▼], and then press the [OK] key.



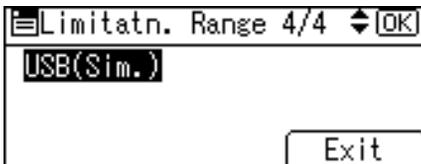
7. Select [USB(Sim.)] using [▲] or [▼], and then press the [OK] key.



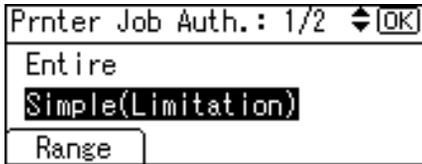
8. Select [Apply] using [▲] or [▼], and then press the [OK] key.



9. Press [Exit].



10. Press the [OK] key.



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

## Authentication Information Stored in the Address Book

3

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

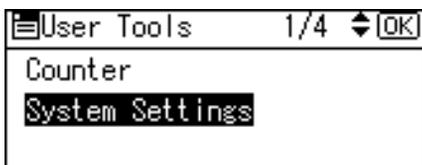
- p.32 "Logging on Using Administrator Authentication"
- p.33 "Logging off Using Administrator Authentication"

## 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.

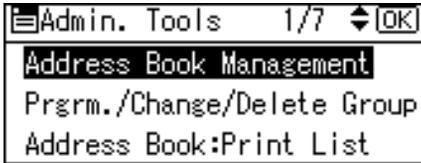
1. Press the [User Tools/Counter] key.
2. Select [System Settings] using [▲] or [▼], and then press the [OK] key.



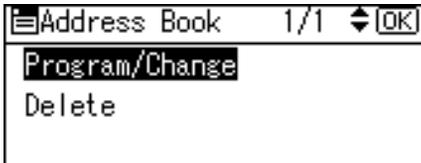
3. Select [Administrator Tools] using [▲] or [▼], and then press the [OK] key.



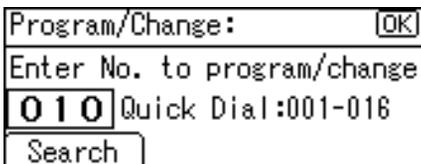
4. Select [Address Book Management] using [▲] or [▼], and then press the [OK] key.



5. Select [Program/Change] using [▲] or [▼], and then press the [OK] key.

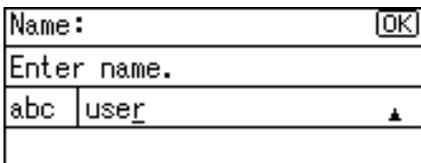


6. Enter the registration number you want to program using the number keys or the Quick Dial keys, and then press the [OK] key.

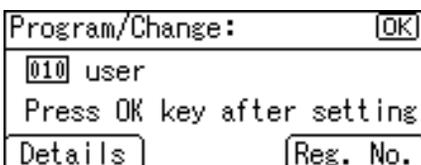


By pressing [Search], you can search by Name, Display Destination List, Registration No., User Code and Fax Destination.

7. Press the [OK] key.



8. Press [Details].



9. Select [Auth. Info] using [▲] or [▼], and then press the [OK] key.

|               |     |   |     |
|---------------|-----|---|-----|
| Det. Settings | 1/3 | ◆ | OK  |
| Auth. Info    |     |   |     |
| Auth. Protect |     |   |     |
|               |     |   | End |

10. Select [Login Authent.Info] using [▲] or [▼], and then press the [OK] key.

|                       |     |   |    |
|-----------------------|-----|---|----|
| Auth. Info            | 1/2 | ◆ | OK |
| Login Authent.Info    |     |   |    |
| SMTP Authentication   |     |   |    |
| Folder Authentication |     |   |    |

11. Select [Login User Name] using [▲] or [▼], and then press the [OK] key.

|                 |     |   |    |
|-----------------|-----|---|----|
| Login Auth.Info | 1/1 | ◆ | OK |
| Login User Name |     |   |    |
| Login Password  |     |   |    |

12. Enter the login name, and then press the [OK] key.

|                  |      |
|------------------|------|
| Login User Name: | OK   |
| Enter user name. |      |
| abc              | 1234 |
|                  |      |

13. Select [Login Password] using [▲] or [▼], and then press the [OK] key.

|                 |     |   |    |
|-----------------|-----|---|----|
| Login Auth.Info | 1/1 | ◆ | OK |
| Login User Name |     |   |    |
| Login Password  |     |   |    |

14. Enter the login password, and then press the [OK] key.

|                 |    |
|-----------------|----|
| Login Password: | OK |
| Enter password. |    |
| abc             | _  |
|                 |    |

15. Re-enter the login password, and then press the [OK] key.

|                           |      |
|---------------------------|------|
| Confirm Password:         | [OK] |
| Please re-enter password. |      |
| abc                       | _    |
|                           |      |

16. Press the [Escape] key two times.  
17. Press [End].

|               |     |      |
|---------------|-----|------|
| Det. Settings | 1/3 | [OK] |
| Auth. Info    |     |      |
| Auth. Protect |     |      |
|               |     | End  |

18. Press the [OK] key.

|                            |          |
|----------------------------|----------|
| Program/Change:            | [OK]     |
| [010] user                 |          |
| Press OK key after setting |          |
| Details                    | Reg. No. |

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

2. Select [System Settings] using [▲] or [▼], and then press the [OK] key.

|                 |     |        |
|-----------------|-----|--------|
| ☰ User Tools    | 1/4 | ◆ [OK] |
| Counter         |     |        |
| System Settings |     |        |
| Logout          |     |        |

3. Select [Administrator Tools] using [▲] or [▼], and then press the [OK] key.

|                     |     |        |
|---------------------|-----|--------|
| ☰ System Settings   | 2/2 | ◆ [OK] |
| Interface Settings  |     |        |
| File Transfer       |     |        |
| Administrator Tools |     |        |

4. Select [Address Book Management] using [▲] or [▼], and then press the [OK] key.

|                            |     |        |
|----------------------------|-----|--------|
| ☰ Admin. Tools             | 1/7 | ◆ [OK] |
| Address Book Management    |     |        |
| Prgrm./Change/Delete Group |     |        |
| Address Book:Print List    |     |        |

5. Select [Program/Change] using [▲] or [▼], and then press the [OK] key.

|                |     |        |
|----------------|-----|--------|
| ☰ Address Book | 1/1 | ◆ [OK] |
| Program/Change |     |        |
| Delete         |     |        |

6. Enter the registration number you want to program using the number keys or the Quick Dial keys, and then press the [OK] key.

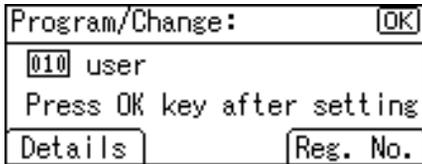
|                             |                    |
|-----------------------------|--------------------|
| Program/Change:             | [OK]               |
| Enter No. to program/change |                    |
| 010                         | Quick Dial:001-016 |
| Search                      |                    |

By pressing [Search], you can search by Name, Display Destination List, Registration No., User Code and Fax Destination.

7. Press the [OK] key.

|             |        |
|-------------|--------|
| Name:       | [OK]   |
| Enter name. |        |
| abc         | user ▲ |
|             |        |

- Press [Details].



- Select [Auth. Info] using [▲] or [▼], and then press the [OK] key.



- Select [LDAP Authentication] using [▲] or [▼], and then press the [OK] key.



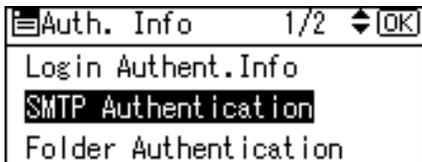
- Select [Use Auth. Info at Login] using [▲] or [▼], and then press the [OK] key.



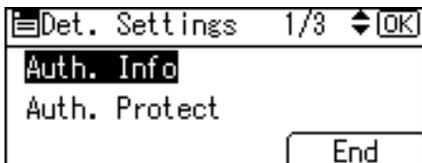
For folder authentication, select [Use Auth. Info at Login] in "Folder Authentication".

For SMTP authentication, select [Use Auth. Info at Login] in "SMTP Authentication".

- Press the [Escape] key.



- Press [End].



14. Press the [OK] key.

|                            |          |
|----------------------------|----------|
| Program/Change:            | [OK]     |
| [010] user                 |          |
| Press OK key after setting |          |
| Details                    | Reg. No. |

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

#### **E** Reference

- p.53 "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.

## 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

- 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.
- Under Windows Authentication, you can select whether or not to use secure sockets layer (SSL) authentication.
- 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 "Admin. Auth. 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/Counter] key.
2. Select [System Settings] using [▲] or [▼], and then press the [OK] key.



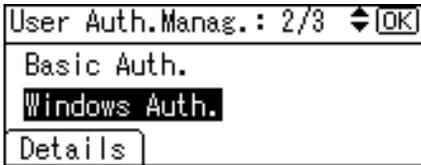
3. Select [Administrator Tools] using [▲] or [▼], and then press the [OK] key.



4. Select [User Auth. Management] using [▲] or [▼], and then press the [OK] key.



5. Select [Windows Auth.] using [▲] or [▼], and then press [Details].



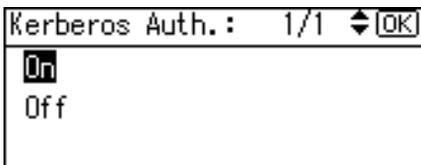
If you do not want to use user authentication management, select [Off].

6. Select [Kerberos Authentication] using [▲] or [▼], and then press the [OK] key.

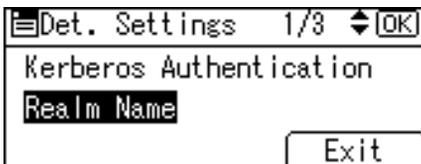


If you want to use NTLM authentication, proceed to step 10.

7. Select [On] using [▲] or [▼], and then press the [OK] key.



8. Select [Realm Name] using [▲] or [▼], and then press the [OK] key.



9. Select the realm using [▲] or [▼], and then press the [OK] key.

|                    |     |    |
|--------------------|-----|----|
| Realm Name:        | 1/2 | OK |
| 1: REALM1          |     |    |
| 2: *Not Programmed |     |    |
| 3: *Not Programmed |     |    |

10. Select [Domain Name] using [▲] or [▼], and then press the [OK] key.

|                         |     |      |
|-------------------------|-----|------|
| Det. Settings           | 1/3 | OK   |
| Kerberos Authentication |     |      |
| Domain Name             |     |      |
|                         |     | Exit |

To display [Domain Name], set [Kerberos Authentication] to [Off].

11. Enter the name of the domain controller to be authenticated, and then press the [OK] key.

|                    |    |
|--------------------|----|
| Domain Name:       | OK |
| Enter domain name. |    |
| abc                | _  |

12. Select [Printer Job Authentication] using [▲] or [▼], and then press the [OK] key.

|                            |     |      |
|----------------------------|-----|------|
| Det. Settings              | 2/3 | OK   |
| Printer Job Authentication |     |      |
| Prgrm./Change/Delete Group |     |      |
|                            |     | Exit |

13. 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

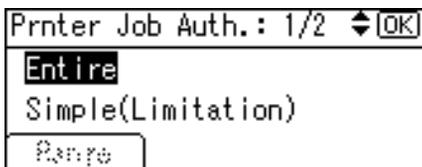
- p.32 "Logging on Using Administrator Authentication"
- p.33 "Logging off Using Administrator Authentication"
- p.64 "Selecting Entire or Simple (All)"
- p.64 "Selecting Simple (Limitation)"
- p.87 "Printer Job Authentication"

## 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.

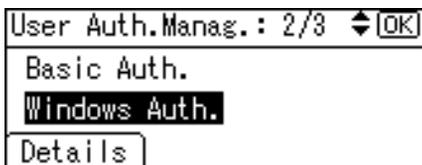
1. Select [Entire] or [Simple(All)] using [▲] or [▼], and then press the [OK] key.



2. Press [Exit].



3. Press the [OK] key.



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

### Note

- 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.

## Selecting Simple (Limitation)

If you select [Simple(Limitation)], you can specify clients for which printer job authentication is not required. Specify [Parallel Interface(Sim.)], [USB(Sim.)] 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. Select [Simple(Limitation)] using [▲] or [▼], and then press [Range].

Specify the range in which [Simple(Limitation)] is applied to Printer Job Authentication.

If you specify IPv4 address range, proceed to step 2.

If you specify [Parallel Interface(Sim.)], proceed to step 5.

If you specify [USB(Sim.)], proceed to step 7.

2. Select [IPv4 Address 1], [IPv4 Address 2], [IPv4 Address 3], [IPv4 Address 4] or [IPv4 Address 5] using [▲] or [▼], and then press the [OK] key.

3. Enter the Start IPv4 Address, and then press the [OK] key.

You can specify the IPv4 address range to which this setting is applied.

4. Enter the End IPv4 Address, and then press the [OK] key.

Be sure the number you enter for End IPv4 Address is larger than that for Start IPv4 Address.

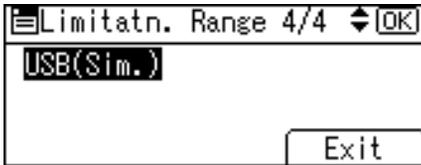
5. Select [Parallel Interface(Sim.)] using [▲] or [▼], and then press the [OK] key.



6. Select [Apply] using [▲] or [▼], and then press the [OK] key.



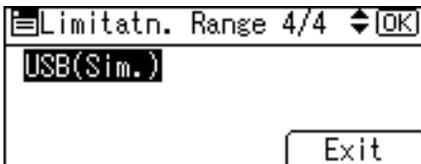
7. Select [USB(Sim.)] using [▲] or [▼], and then press the [OK] key.



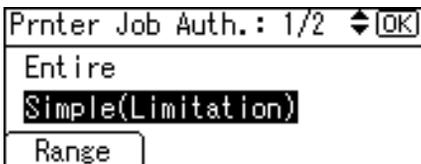
8. Select [Apply] using [▲] or [▼], and then press the [OK] key.



9. Press [Exit].



10. Press the [OK] key.



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

**Note**

- 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.

## Installing Internet Information Services (IIS) and Certificate Services

3

Specify this setting if you want the machine to automatically obtain e-mail addresses registered in Active Directory.

We recommend you install Internet Information Services (IIS) and Certificate services as the Windows components.

Install the components, and then create the server certificate.

If they are not installed, install them as follows:

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

---

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 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.

### 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

---

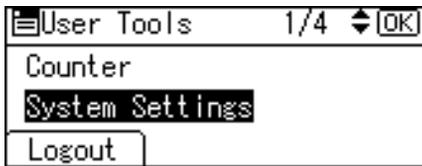
Before beginning to configure the machine, make sure that administrator authentication is properly configured under "Admin. Auth. Management".

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/Counter] key.

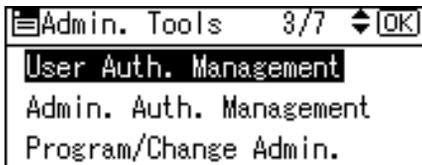
2. Select [System Settings] using [▲] or [▼], and then press the [OK] key.



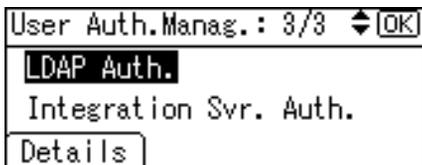
3. Select [Administrator Tools] using [▲] or [▼], and then press the [OK] key.



4. Select [User Auth. Management] using [▲] or [▼], and then press the [OK] key.



5. Select [LDAP Auth.] using [▲] or [▼], and then press [Details].



If you do not want to use user authentication management, select [Off].

6. Select [Select LDAP Server] using [▲] or [▼], and then press the [OK] key.



7. Select the LDAP server to be used for LDAP authentication using [▲] or [▼], and then press the [▶] key.



The box next to a selected item is checked. To deselect the item, press [◀].

8. Press the [OK] key.

```
LDAP Server: 2/2 [OK]
 4: *Not Programmed
 5: *Not Programmed
```

9. Select [Login Name Attribute] using [▲] or [▼], and then press the [OK] key.

```
Det. Settings 2/3 [OK]
Login Name Attribute
Unique Attribute
Exit
```

10. Enter the login name attribute, and then press the [OK] key.

```
Login Name Attribute: [OK]
Enter attribute.
abc
```

You can 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. The method for selecting the user name depends on the server environment. Check the server environment and enter the user name accordingly.

11. Select [Unique Attribute] using [▲] or [▼], and then press the [OK] key.

```
Det. Settings 2/3 [OK]
Login Name Attribute
Unique Attribute
Exit
```

12. Enter the unique attribute, and then press the [OK] key.

```
Unique Attribute: [OK]
Enter attribute.
abc _
```

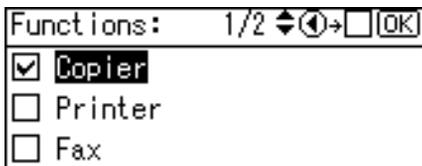
Specify Unique Attribute on the machine to match the user information in the LDAP server with that in the machine. By doing this, if the Unique Attribute of a user registered in the LDAP server matches that of a user registered in the machine, the two instances are treated as referring to the same user. 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.

13. Select [Function Permissions] using [▲] or [▼], and then press the [OK] key.



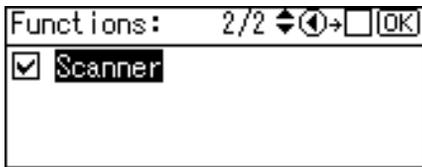
14. Select which of the machine's functions you want to permit using [▲] or [▼], and then press the [►] key.



The box next to a selected item is checked. To deselect the item, press [◀].

LDAP Authentication will be applied to the selected functions. Users can use the selected functions only.

15. Press the [OK] key.



16. Select [Printer Job Authentication] using [▲] or [▼], and then press the [OK] key.



17. 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.32 "Logging on Using Administrator Authentication"
- p.33 "Logging off Using Administrator Authentication"
- p.75 "Selecting Entire or Simple (All)"

- p.75 "Selecting Simple (Limitation)"
- p.87 "Printer Job Authentication"

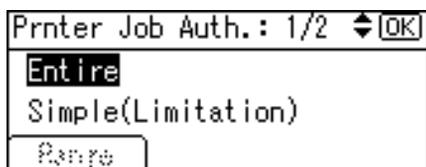
## Selecting Entire or Simple (All)

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

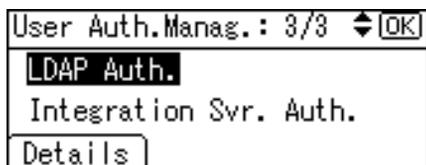
1. Select [Entire] or [Simple(All)] using [▲] or [▼], and then press the [OK] key.



2. Press [Exit].



3. Press the [OK] key.



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

## Selecting Simple (Limitation)

If you select [Simple(Limitation)], you can specify clients for which printer job authentication is not required. Specify [Parallel Interface(Sim.)], [USB(Sim.)] 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. Select [Simple(Limitation)] using [▲] or [▼], and then press [Range].

Printer Job Auth.: 1/2 [OK]

Entire

**Simple(Limitation)**

Range

Specify the range in which [Simple(Limitation)] is applied to Printer Job Authentication.

If you specify IPv4 address range, proceed to step 2.

If you specify [Parallel Interface(Sim.)], proceed to step 5.

If you specify [USB(Sim.)], proceed to step 7.

2. Select [IPv4 Address 1], [IPv4 Address 2], [IPv4 Address 3], [IPv4 Address 4] or [IPv4 Address 5] using [▲] or [▼], and then press the [OK] key.

Limitatn. Range 1/4 [OK]

**IPv4 Address 1**

IPv4 Address2

Exit

3. Enter the Start IPv4 Address, and then press the [OK] key.

Start IPv4 Address: [OK]

Enter Start Address

[0] . [0] . [0] . [0]

You can specify the IPv4 address range to which this setting is applied.

4. Enter the End IPv4 Address, and then press the [OK] key.

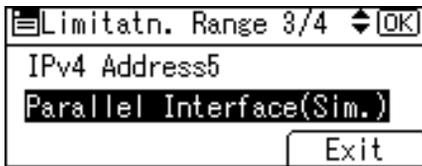
End IPv4 Address: [OK]

Enter End Address

[0] . [0] . [0] . [0]

Be sure the number you enter for End IPv4 Address is larger than that for Start IPv4 Address.

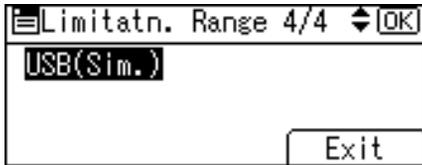
5. Select [Parallel Interface(Sim.)] using [▲] or [▼], and then press the [OK] key.



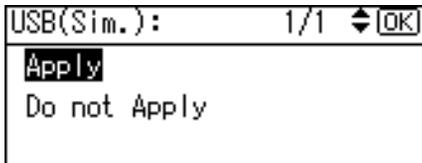
6. Select [Apply] using [▲] or [▼], and then press the [OK] key.



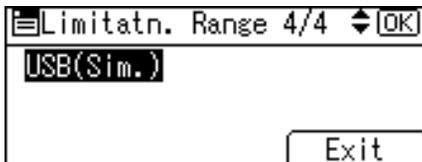
7. Select [USB(Sim.)] using [▲] or [▼], and then press the [OK] key.



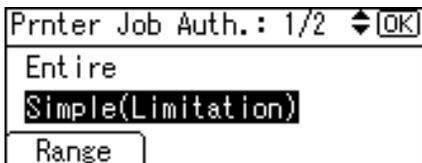
8. Select [Apply] using [▲] or [▼], and then press the [OK] key.



9. Press [Exit].



10. Press the [OK] key.



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

## 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.

3

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 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 "Admin. Auth. 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/Counter] key.

2. Select [System Settings] using [▲] or [▼], and then press the [OK] key.

|                 |     |        |
|-----------------|-----|--------|
| ☰ User Tools    | 1/4 | ◆ [OK] |
| Counter         |     |        |
| System Settings |     |        |
| Logout          |     |        |

3. Select [Administrator Tools] using [▲] or [▼], and then press the [OK] key.

|                     |     |        |
|---------------------|-----|--------|
| ☰ System Settings   | 2/2 | ◆ [OK] |
| Interface Settings  |     |        |
| File Transfer       |     |        |
| Administrator Tools |     |        |

4. Select [User Auth. Management] using [▲] or [▼], and then press the [OK] key.

|                         |     |        |
|-------------------------|-----|--------|
| ☰ Admin. Tools          | 3/7 | ◆ [OK] |
| User Auth. Management   |     |        |
| Admin. Auth. Management |     |        |
| Program/Change Admin.   |     |        |

5. Select [Integration Svr. Auth.] using [▲] or [▼], and then press [Details].

|                        |     |        |
|------------------------|-----|--------|
| User Auth. Manag. :    | 3/3 | ◆ [OK] |
| LDAP Auth.             |     |        |
| Integration Svr. Auth. |     |        |
| Details                |     |        |

If you do not want to use User Authentication Management, select [Off].

6. Select [Server Name] using [▲] or [▼], and then press the [OK] key.

|                     |     |        |
|---------------------|-----|--------|
| ☰ Det. Settings     | 1/4 | ◆ [OK] |
| Server Name         |     |        |
| Authentication Type |     |        |
| Exit                |     |        |

Specify the name of the server for external authentication.

7. Enter the server name, and then press the [OK] key.

|                    |      |
|--------------------|------|
| Server Name:       | [OK] |
| Enter server name. |      |
| abc                | _    |
|                    |      |

Enter the IPv4 address or host name.

8. Select [Authentication Type] using [▲] or [▼], and then press the [OK] key.

|                        |      |
|------------------------|------|
| Det. Settings 1/4 [OK] |      |
| Server Name            |      |
| Authentication Type    |      |
|                        | Exit |

9. Select the authentication system for external authentication using [▲] or [▼], and then press the [OK] key.

|                        |
|------------------------|
| Auth. Type: 1/2 [OK]   |
| Default                |
| Windows (Native)       |
| Windows(NT Compatible) |

Select an available authentication system.

10. Select [Domain Name] using [▲] or [▼], and then press the [OK] key.

|                        |      |
|------------------------|------|
| Det. Settings 2/4 [OK] |      |
| Domain Name            |      |
| Obtain URL             |      |
|                        | Exit |

11. Enter the domain name, and then press the [OK] key.

|                    |
|--------------------|
| Domain Name: [OK]  |
| Enter domain name. |
| abc                |

You cannot specify a domain name under an authentication system that does not support domain login.

12. Select [Obtain URL] using [▲] or [▼], and then press the [OK] key.

|                        |      |
|------------------------|------|
| Det. Settings 2/4 [OK] |      |
| Domain Name            |      |
| Obtain URL             |      |
|                        | Exit |

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" will be not obtained.

If you set "Authentication Type" to "Windows", 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. Select [Prgrm./Change/Delete Group] using [▲] or [▼], and then press the [OK] key.

Det. Settings 3/4 [OK]

Prgrm./Change/Delete Group

Printer Job Authentication

Exit

14. Select [Program/Change] using [▲] or [▼], and then press the [OK] key.

Group 1/1 [OK]

Program/Change

Delete

15. Select [\*Not Programmed] using [▲] or [▼], and then press the [OK] key.

Group 1/4 [OK]

1: \*Default Group

2: \*Not Programmed

3: \*Not Programmed

16. Enter the group name, and then press the [OK] key.

Group 2 Name: [OK]

Enter name.

abc

17. Select which of the machine's functions you want to permit using [▲] or [▼], and then press the [▶] key.

Functions: 1/2 [OK]

Copier

Printer

Fax

The box next to a selected item is checked. To deselect the item, press [◀].

Authentication will be applied to the selected functions.

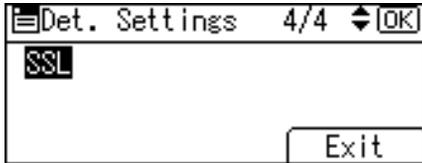
Users can use the selected functions only.

For details about specifying available functions for individuals or groups, see "Limiting Available Functions".

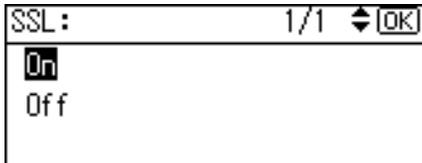
18. Press the [OK] key, and then press the [Escape] key twice.



19. Select [SSL] using [▲] or [▼], and then press the [OK] key.



20. Select [On] using [▲] or [▼], and then press the [OK] key.

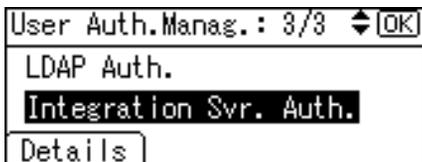


To not use secure sockets layer (SSL) for authentication, press [Off].

21. Press [Exit].



22. Select [Integration Svr. Auth.] using [▲] or [▼], and then press [Details].



23. Select [Printer Job Authentication] using [▲] or [▼], and then press the [OK] key.



24. 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

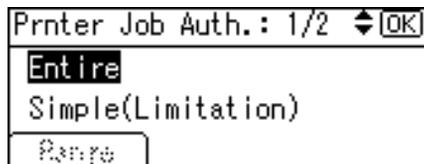
- p.32 "Logging on Using Administrator Authentication"
- p.33 "Logging off Using Administrator Authentication"
- p.147 "Limiting Available Functions"
- p.83 "Selecting Entire or Simple (All)"
- p.84 "Selecting Simple (Limitation)"
- p.87 "Printer Job Authentication"

## 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.

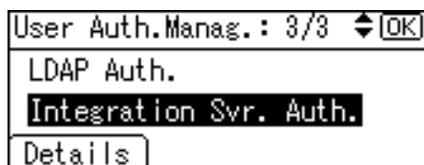
1. Select [Entire] or [Simple(All)] using [▲] or [▼], and then press the [OK] key.



2. Press [Exit].



3. Press the [OK] key.



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

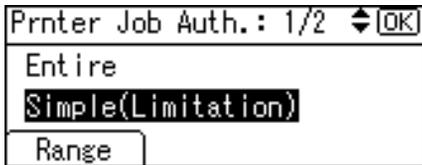
## Selecting Simple (Limitation)

If you select [Simple(Limitation)], you can specify clients for which printer job authentication is not required. Specify [Parallel Interface(Sim.)], [USB(Sim.)] 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. Select [Simple(Limitation)] using [▲] or [▼], and then press [Range].



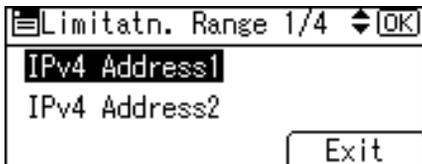
Specify the range in which [Simple(Limitation)] is applied to Printer Job Authentication.

If you specify IPv4 address range, proceed to step 2.

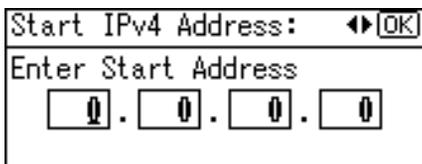
If you specify [Parallel Interface(Sim.)], proceed to step 5.

If you specify [USB(Sim.)], proceed to step 7.

2. Select [IPv4 Address 1], [IPv4 Address 2], [IPv4 Address 3], [IPv4 Address 4] or [IPv4 Address 5] using [▲] or [▼], and then press the [OK] key.



3. Enter the Start IPv4 Address, and then press the [OK] key.



You can specify the IPv4 address range to which this setting is applied.

4. Enter the End IPv4 Address, and then press the [OK] key.

Be sure the number you enter for End IPv4 Address is larger than that for Start IPv4 Address.

5. Select [Parallel Interface(Sim.)] using [▲] or [▼], and then press the [OK] key.

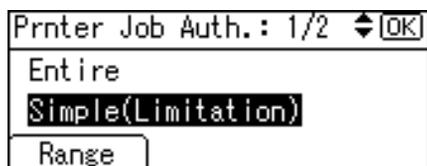
6. Select [Apply] using [▲] or [▼], and then press the [OK] key.

7. Select [USB(Sim.)] using [▲] or [▼], and then press the [OK] key.

8. Select [Apply] using [▲] or [▼], and then press the [OK] key.

9. Press [Exit].

10. Press the [OK] key.



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

# 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 PCL printer driver.

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 Auth. Management]      | Specified      | Specified      | Specified | Specified |
|------------------------------|----------------|----------------|-----------|-----------|
| [Printer Job Authentication] | [Simple (All)] | [Simple (All)] | [Entire]  | [Entire]  |
| [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(Sim.)], [USB(Sim.)], and the client's IPv4 address.

3

### Printer Job Types

1. 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 "Simple Encryption", see "Specifying the Extended Security Functions".

2. 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 "Simple Encryption" and allowing the use of simple encryption, see "Specifying the Extended Security Functions".

3. 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 a 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 a 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.217 "Specifying the Extended Security Functions"

3

## 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**

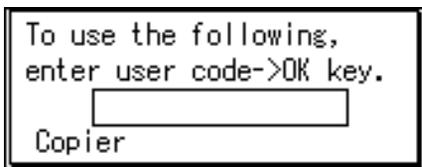
- p.97 "Authentication Using an External Device"

---

## If User Code Authentication is Specified

---

When User Code Authentication is set, the following screen appears.



Enter your user code.

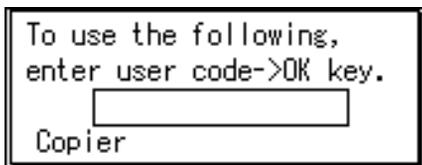
---

## 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 the [OK] key.



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 [Clear/Stop] key and the [Reset] key at the same time.

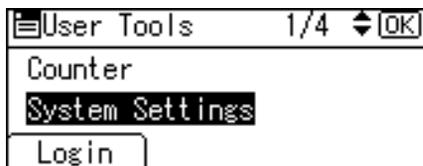
## Logging on Using the Printer Driver

When User Code Authentication is set, specify a user code in printer properties on the printer driver. For details, see the printer driver Help.

3

## 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.

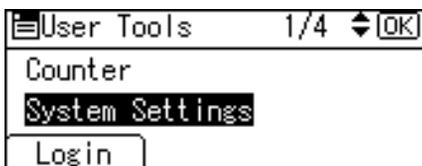


Enter your login user name and password.

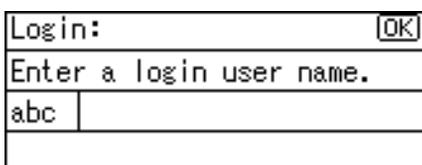
## Logging on Using the Control Panel

Use the following procedure to log on when Basic Authentication, Windows Authentication, LDAP Authentication, or Integration Server Authentication is enabled.

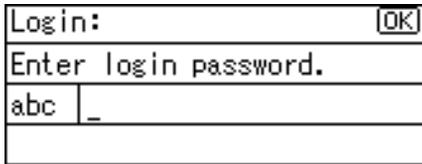
1. Press [Login].



2. Enter a login user name, and then press the [OK] key.



3. Enter a login password, and then press the [OK] key.



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

### 3

## Logging off Using the Control Panel

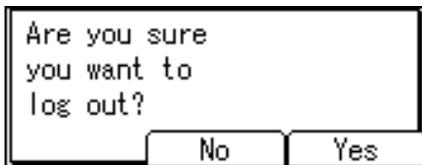
---

Follow the procedure below to log off when Basic Authentication, Windows Authentication, LDAP Authentication, or Integration Server Authentication is set.

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



3. Press [Yes].



## 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 the 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 "User Name", and then click [Login].

## Logging off Using Web Image Monitor

### 1. Click [Logout] to log off.

### ↓ Note

- Delete the cache memory in the Web Image Monitor after logging off.

3

## User Lockout Function

If an incorrect password is entered several times, the User Lockout function prevents further login attempts under the same user name. Even if the locked out user enters the correct password later, authentication will fail and the machine cannot be used until the lockout period elapses or an administrator or supervisor disables the lockout.

To use the lockout function for user authentication, the authentication method must be set to Basic authentication. Under other authentication methods, the lockout function protects supervisor and administrator accounts only, not general user accounts.

### Lockout setting items

The lockout function settings can be made using Web Image Monitor.

| Setting Item                      | Description   | Setting Values   | Default Setting  |
|-----------------------------------|---|--|--|
| Lockout                           | Specify whether or not to enable the lockout function.                          | <ul style="list-style-type: none"> <li>• Active</li> <li>• Inactive</li> </ul> | <ul style="list-style-type: none"> <li>• Inactive</li> </ul> |
| 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"> <li>• Active</li> <li>• Inactive</li> </ul> | <ul style="list-style-type: none"> <li>• Inactive</li> </ul> |

| Setting Item      | Description  | Setting Values | Default Setting |
|-------------------|--|----------------|-----------------|
| 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.

3

| Locked out User  | Unlocking administrator |
|--|-------------------------|
| general user   | user administrator      |
| user administrator, network administrator, file administrator, machine administrator | supervisor              |
| 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 [OK].
11. 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. **Select the "Lockout" to [Inactive] under "Authentication Information".**
8. **Click [OK].**
9. **Click [Logout].**

## Auto Logout

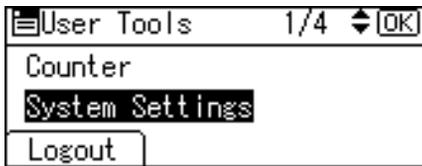
This can be specified by the machine administrator.

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.

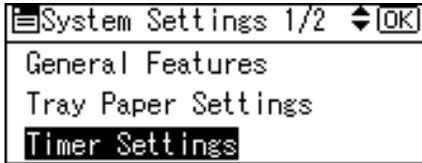
For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

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

2. Select [System Settings] using [▲] or [▼], and then press the [OK] key.



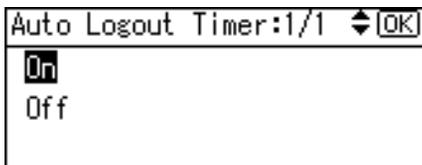
3. Select [Timer Settings] using [▲] or [▼], and then press the [OK] key.



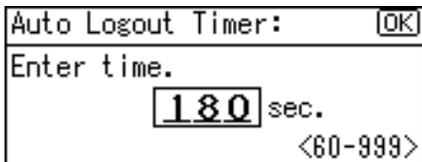
4. Select [Auto Logout Timer] using [▲] or [▼], and then press the [OK] key.



5. Select [On] using [▲] or [▼], and then press the [OK] key.



6. Enter "60" to "999" (seconds) using the number keys, and then press the [OK] key.



If you do not want to specify [Auto Logout Timer], select [Off].

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

#### ↓ 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.32 "Logging on Using Administrator Authentication"
- p.33 "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.

## 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 [Stored Print (Shared)], you can also share these files.

## 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 "One Click Presets" 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. Print the locked document.**

## Printing a Locked Print File

**4**

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".

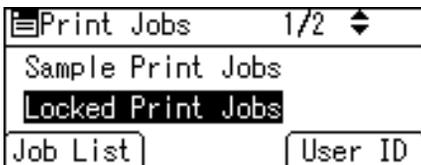
This can also be specified via Web Image Monitor. For details, see Web Image Monitor Help.

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

**2. Press [Prt.Jobs].**

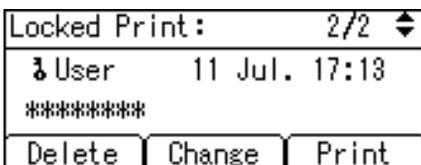


**3. Select [Locked Print Jobs] using [▲] or [▼], and then press [Job List].**



Only Locked Print files belonging to the user who has logged on appear.

**4. Select the Locked Print file using [▲] or [▼], and then press [Print].**

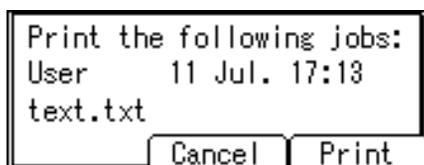


5. Enter the password for the stored file, and then press the [OK] key.



Enter the password specified in step 4 of "Specifying a Locked Print File".

6. Press [Print].



### Reference

- p.90 "If User Authentication is Specified"

## Deleting Locked Print Files

This can be specified by the file creator (owner).

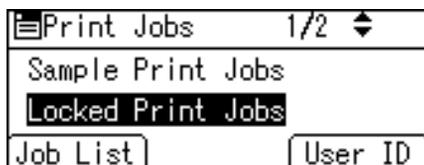
To delete Locked Print files, you must enter the password for the files. If the password has been forgotten, ask the file administrator to change the password.

This can also be specified via Web Image Monitor. For details, see Web Image Monitor Help.

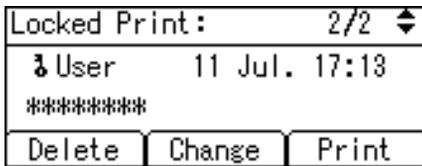
1. Press the [Printer] key.
2. Press [Prt.Jobs].



3. Select [Locked Print Jobs] using [▲] or [▼], and then press [Job List].



4. Select the Locked Print file using [▲] or [▼], and then press [Delete].



5. Enter the password for the stored file, and then press the [OK] key.



6. Press [Delete].



**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 [Prt.Jobs].



3. Select [Locked Print Jobs] using [▲] or [▼], and then press [Job List].

|                   |     |         |
|-------------------|-----|---------|
| Print Jobs        | 1/2 | ◆       |
| Sample Print Jobs |     |         |
| Locked Print Jobs |     |         |
| Job List          |     | User ID |

4. Select the Locked Print file using [▲] or [▼], and then press [Change].

|               |               |       |
|---------------|---------------|-------|
| Locked Print: | 2/2           | ◆     |
| ⌂ User        | 11 Jul. 17:13 |       |
| *****         |               |       |
| Delete        | Change        | Print |

5. Enter the password for the stored file, and then press the [OK] key.

|                                      |
|--------------------------------------|
| Enter the password<br>then press OK. |
| <input type="text"/>                 |

The file administrator does not need to enter the password.

6. Press the [OK] key.

|                 |     |   |
|-----------------|-----|---|
| Locked Print:   | 1/1 | ◆ |
| Change Password |     |   |

7. Enter the new password for the stored file, and then press the [OK] key.

|  |
|--|
| Enter the new password<br>then press OK. |
| <input type="text"/>                     |

8. If a password reentry screen appears, enter the login password, and then press the [OK] key.

|  |
|--|
| Enter the confirmation<br>password, then press OK. |
| <input type="text"/>                               |

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".

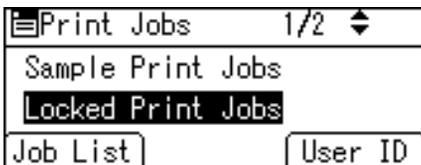
This can also be specified via Web Image Monitor. For details, see Web Image Monitor Help.

### 4

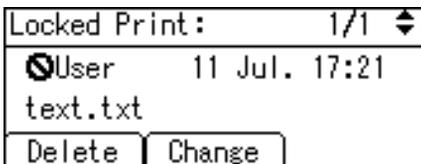
1. Press the [Printer] key.
2. Press [Prt.Jobs].



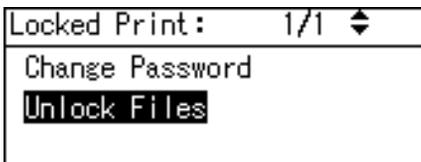
3. Select [Locked Print Jobs] using [▲] or [▼], and then press [Job List].

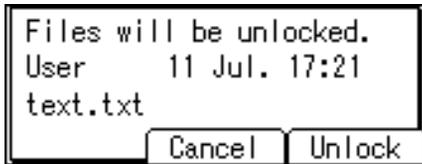


4. Select the Locked Print file using [▲] or [▼], and then press [Change].



5. Select [Unlock Files] using [▲] or [▼], and then press the [OK] key.



**6. Press [Unlock].****Note**

- You can use the same procedure to unlock stored print files also.

**Reference**

- p.217 "Specifying the Extended Security Functions"
- p.32 "Logging on Using Administrator Authentication"
- p.33 "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 and phone numbers 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 Dest. Use(Fax)" to [On], you can prohibit users from directly entering telephone numbers, e-mail addresses, or Folder Path on the fax screen in order to send files. If you set "Rstrct Dest. Use(Scanner)" to [On], you can prohibit users from directly entering telephone numbers, e-mail addresses, or Folder Path on the scanner screen in order to send files.

If you set "Restrict Dest. Use(Fax)" to [Off], "Rstrct Dest. Add.(Fax)" appears. If you set "Rstrct Dest. Use(Scanner)" to [Off], "Rstrct Dest. Add.(Scanner)" appears.

In "Rstrct Dest. Add.(Fax)", you can restrict users from registering data in the Address Book on the fax screen. In "Rstrct Dest. Add.(Scanner)", you can restrict users from registering data in the Address Book on the scanner screen.

If you set "Rstrct Dest. Add.(Fax)" to [Off], users can directly enter destination telephone numbers, e-mail addresses, and Folder Path in "Program" on the fax screen. If you set "Rstrct Dest. Add.(Scanner)" to [Off], users can directly enter destination telephone numbers, e-mail addresses, and Folder Path in "Program" on the scanner screen.

If you set "Rstrct Dest. Add.(Fax)" to [On], users can enter destinations directly, but cannot use "Program" to register data in the Address Book on the fax screen. If you set "Rstrct Dest. Add.(Scanner)" to [On], users

can enter destinations directly, but cannot use "Program" to register data in the Address Book on the scanner screen.

When this setting is made, only the user administrator can change the Address Book. "Restrict Dest. Use (Fax)", "Rstrct Dest. Use(Scanner)", "Rstrct Dest. Add.(Fax)", and "Rstrct Dest. Add.(Scanner)" 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/Counter] key.
2. Select [System Settings] using [▲] or [▼], and then press the [OK] key.



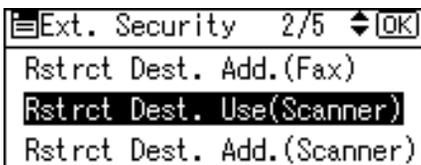
3. Select [Administrator Tools] using [▲] or [▼], and then press the [OK] key.



4. Select [Extended Security] using [▲] or [▼], and then press the [OK] key.

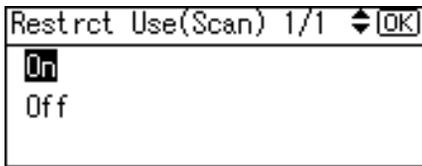


5. Select [Rstrct Dest. Use(Scanner)] using [▲] or [▼], and then press the [OK] key.



To restrict the use of fax destinations, select [Restrict Dest. Use(Fax)].

6. Select [On] using [▲] or [▼], and then press the [OK] key.



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

#### **Reference**

- p.217 "Specifying the Extended Security Functions"
- p.32 "Logging on Using Administrator Authentication"
- p.33 "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.

### 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.

## Specifying the User Certificate

## 5

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 [OK].**

**8. Click [Logout].**

5

---

## 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.

- 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)

- Creating and installing the device certificate.  
Create and install the device certificate using Web Image Monitor.
- Make certificate settings.  
Make settings for the certificate to be used for S/MIME using Web Image Monitor.
- Make electronic signature settings.  
Make settings for the electronic signature using Web Image Monitor.

### Configuration flow (certificate issued by a certificate authority)

- 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.
- Install the device certificate.  
Install the device certificate using Web Image Monitor.
- Make certificate settings.  
Make settings for the certificate to be used for S/MIME using Web Image Monitor.
- Make electronic signature settings.  
Make settings for the electronic signature using Web Image Monitor.

5

## 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.

- Open a Web browser.**
- 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.

- 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].**

"Requesting" appears for Certificate Status in the "Certificates" area.

**9. Click [Logout].****10. Apply to the certificate authority for the device certificate.**

The application procedure depends on the certificate authority. For details, contact the certificate authority.

For application details, click the Web Image Monitor Details icon and use the information shown 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)**

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].**

"Installed" appears under [Certificate Status] to show that a device certificate for the machine has been installed.

**9. Click [Logout].**

## 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.

5

**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 logon.

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 logon.

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 stored documents next to "When Transferring Files Stored in Document Server (Utility)" under "Signature".****8. Click [OK].**

The settings for the S/MIME electronic signature are enabled.

**9. Click [OK].****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

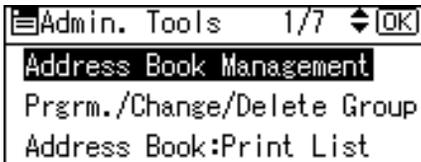
1. Press the [User Tools/Counter] key.
2. Select [System Settings] using [▲] or [▼], and then press the [OK] key.



3. Select [Administrator Tools] using [▲] or [▼], and then press the [OK] key.



4. Press [Address Book Management] using [▲] or [▼], and then press the [OK] key.



5. Select [Program/Change] using [▲] or [▼], and then press the [OK] key.

|                |     |   |    |
|----------------|-----|---|----|
| Address Book   | 1/1 | ◆ | OK |
| Program/Change |     |   |    |
| Delete         |     |   |    |

6. Enter the registration number you want to program using the number keys or the Quick Dial keys, and then press the [OK] key.

|                             |                    |
|-----------------------------|--------------------|
| Program/Change:             | OK                 |
| Enter No. to program/change |                    |
| 001                         | Quick Dial:001-016 |
| Search                      |                    |

By pressing [Search], you can search by Name, Display Destination List, Registration No., User Code and Fax Destination.

7. Press the [OK] key.

|             |      |
|-------------|------|
| Name:       | OK   |
| Enter name. |      |
| abc         | test |
|             |      |

8. Press [Details].

|                            |          |
|----------------------------|----------|
| Program/Change:            | OK       |
| 001 test                   |          |
| Press OK key after setting |          |
| Details                    | Reg. No. |

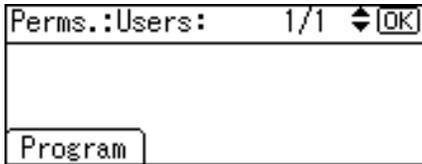
9. Select [Auth. Protect] using [▲] or [▼], and then press the [OK] key.

|               |     |   |     |
|---------------|-----|---|-----|
| Det. Settings | 1/3 | ◆ | OK  |
| Auth. Info    |     |   |     |
| Auth. Protect |     |   |     |
|               |     |   | End |

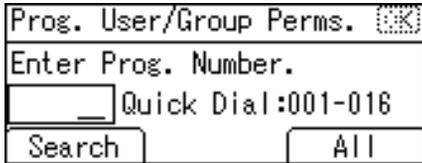
10. Select [Dest.Protect:Permissions] using [▲] or [▼], and then press the [OK] key.

|                          |     |   |    |
|--------------------------|-----|---|----|
| Auth.Protect             | 1/1 | ◆ | OK |
| Register as              |     |   |    |
| Dest.Protect Obj.        |     |   |    |
| Dest.Protect:Permissions |     |   |    |

11. Press [Program].

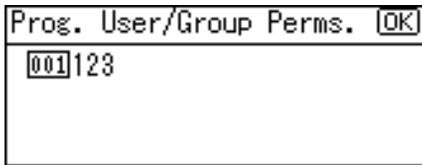


12. Select the users or groups to register.



You can select more than one user.  
By pressing [All], you can select all the users.

13. Press the [OK] key.



14. Select the permission, and then press the [OK] key.

Select the permission, from [Read-only], [Edit], [Edit/Delete], or [Full Control].  
To register multiple users, repeat steps 12 to 14.



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

**Reference**

- p.32 "Logging on Using Administrator Authentication"
- p.33 "Logging off Using Administrator Authentication"

---

## Encrypting Data in the Address Book

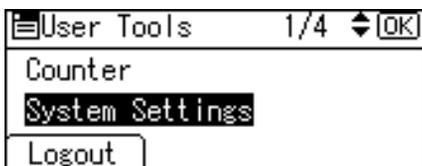
---

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/Counter] key.
2. Select [System Settings] using [▲] or [▼], and then press the [OK] key.



3. Select [Administrator Tools] using [▲] or [▼], and then press the [OK] key.



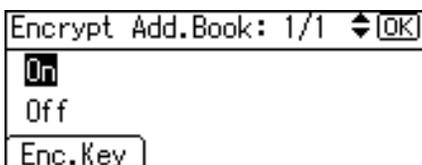
4. Select [Extended Security] using [▲] or [▼], and then press the [OK] key.



5. Select [Encrypt Address Book] using [▲] or [▼], and then press the [OK] key.



6. Select the setting you want to change using [▲] or [▼], and then press [Enc.Key].



- 7. Enter the encryption key, and then press the [OK] key.

|                       |      |      |
|-----------------------|------|------|
| Encryption Key:       |      | [OK] |
| Enter Encryption Key: |      |      |
| abc                   | **** |      |
|                       |      |      |

Enter the encryption key using up to 32 alphanumeric characters.

- 8. Re-enter the encryption key, and then press the [OK] key.

|                          |   |      |
|--------------------------|---|------|
| Confirm Encryption Key:  |   | [OK] |
| Re-enter Encryption key. |   |      |
| abc                      | _ |      |
|                          |   |      |

- 9. Press the [OK] key.

|                                     |     |   |      |
|-------------------------------------|-----|---|------|
| Encrypt Add.Book: 1/1               |     | ↕ | [OK] |
| <input checked="" type="checkbox"/> | On  |   |      |
| <input type="checkbox"/>            | Off |   |      |
| Enc.Key                             |     |   |      |

- 10. Press [OK].

|  |    |
|--|----|
| Encryption/Decryption<br>will start. This may<br>take some time. |    |
| Cancel   | OK |

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, [Exit] appears.

If you press [Stop] during encryption, the data is not encrypted.

If you press [Stop] during decryption, the data stays encrypted.

- 11. Press [Exit].

|   |  |
|---|--|
| Encryption/Decryption<br>completed. Press Exit. |  |
| Exit  |  |

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

### Note

- If you register additional users after encrypting the data in the Address Book, those users are also encrypted.

### Reference

- p.32 "Logging on Using Administrator Authentication"
- p.33 "Logging off Using Administrator Authentication"
- p.217 "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

5

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
- Temporary stored documents
- Logs
- Network I/F setting information
- System settings information

### Reference

- p.32 "Logging on Using Administrator Authentication"
- p.33 "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.

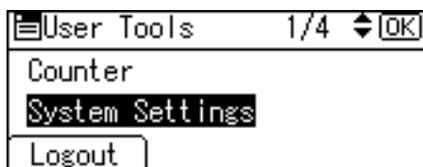
### ★ Important

- **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. If there is unencrypted data on the hard disk that must be both transferred and encrypted, rebooting will take about three hours. If there is encrypted data on the hard disk that must be re-encrypted, rebooting will take about five 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.

- 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 five hours. If you specify re-encryption of encrypted data, the entire process will take about seven hours.
- Rebooting will be faster if there is no data to carry over to the hard disk and if encryption is set to [Format], 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.

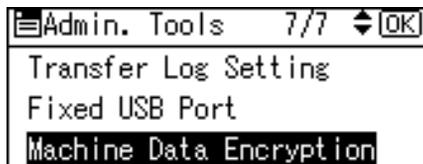
1. Press the [User Tools/Counter] key.
2. Select [System Settings] using [▲] or [▼], and then press the [OK] key.



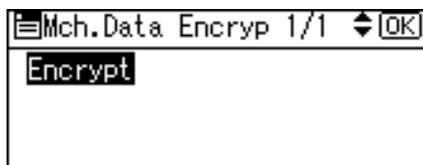
3. Select [Administrator Tools] using [▲] or [▼], and then press the [OK] key.



4. Select [Machine Data Encryption] using [▲] or [▼], and then press the [OK] key.



5. Select [Encrypt] using [▲] or [▼], and then press the [OK] key.



6. Select the data to be carried over to the hard disk and not be reset.



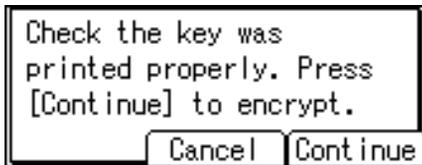
To carry all of the data over to the hard disk, select [All Data]. To carry over only the machine settings data, select [File Sys]. To reset all of the data, select [Format].

7. Press [Print].

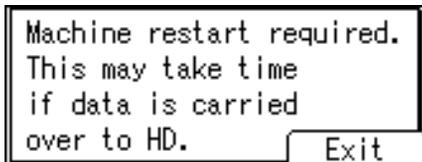


The encryption key for backup data is printed.

8. Press [Continue].



9. Press [Exit].



10. Press the [User Tools/Counter] 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.

---

## 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.

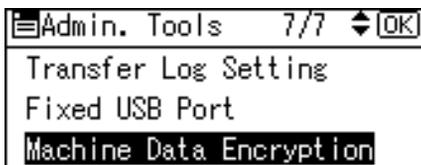
1. Press the [User Tools/Counter] key.
2. Select [System Settings] using [▲] or [▼], and then press the [OK] key.



3. Select [Administrator Tools] using [▲] or [▼], and then press the [OK] key.



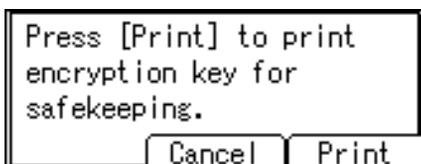
4. Select [Machine Data Encryption] using [▲] or [▼], and then press the [OK] key.



5. Select [Print Encryption Key] using [▲] or [▼], and then press the [OK] key.



6. Press [Print].



The encryption key for backup data is printed.

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

## 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.

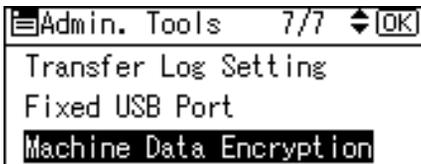
1. Press the [User Tools/Counter] key.
2. Select [System Settings] using [▲] or [▼], and then press the [OK] key.



3. Select [Administrator Tools] using [▲] or [▼], and then press the [OK] key.



4. Select [Machine Data Encryption] using [▲] or [▼], and then press the [OK] key.



5. Select [Update Encryption Key] using [▲] or [▼], and then press the [OK] key.



6. Select the data to be carried over to the hard disk and not be reset.



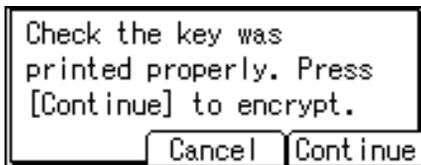
To carry all of the data over to the hard disk, select [All Data]. To carry over only the machine settings data, select [File Sys]. To reset all of the data, select [Format].

7. Press [Print].

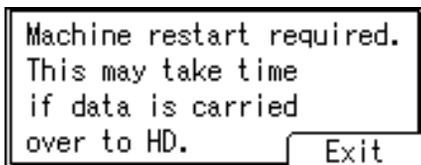


The encryption key for retrieving the backup data is printed.

8. Press [Continue].



9. Press [Exit].



10. Press the [User Tools/Counter] 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.

---

## Canceling Data Encryption

---

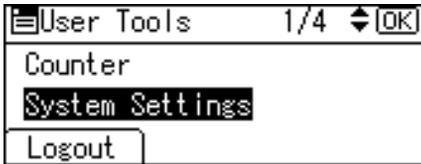
Use the following procedure to cancel the encryption settings when encryption is no longer necessary.

**★ 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] is selected and encryption is canceled, data stored on the hard disk is not erased.

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

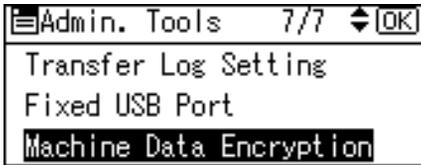
2. Select [System Settings] using [▲] or [▼], and then press the [OK] key.



3. Select [Administrator Tools] using [▲] or [▼], and then press the [OK] key.



4. Select [Machine Data Encryption] using [▲] or [▼], and then press the [OK] key.



5. Select [Cancel Encryption] using [▲] or [▼], and then press the [OK] key.

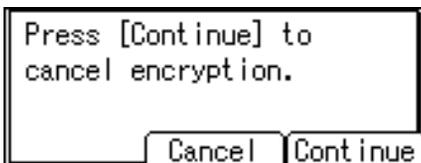


6. Select the data to be carried over to the hard disk and not be reset.

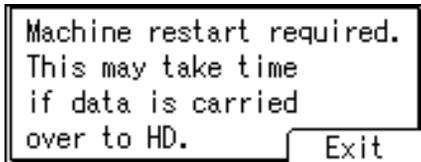


To carry all of the data over to the hard disk, select [All Data]. To carry over only the machine settings data, select [File Sys]. To reset all of the data, select [Format].

7. Press [Continue].



8. Press [Exit].



9. Press the [User Tools/Counter] key.
10. 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, fax, and scanner functions. It also stores the data of users' 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.

---

## 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.

---

## 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

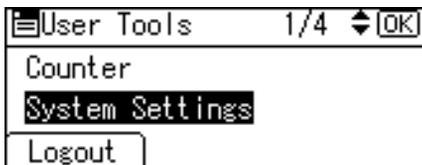
This can be specified by the machine administrator.

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 "Off" might not be overwritten.

1. Press the [User Tools/Counter] key.
2. Select [System Settings] using [▲] or [▼], and then press the [OK] key.



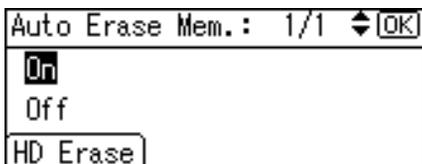
3. Select [Administrator Tools] using [▲] or [▼], and then press the [OK] key.



4. Select [Auto Erase Memory Setting] using [▲] or [▼], and then press the [OK] key.



5. Select [On] using [▲] or [▼], and then press [HD Erase].



Select the method of erasing the data from [NSA], [DoD], or [Random Numbers].

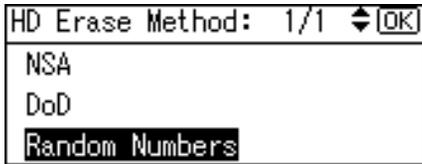
If you select [Random Numbers], proceed to step 6.

If you select [NSA] proceed to step 8.

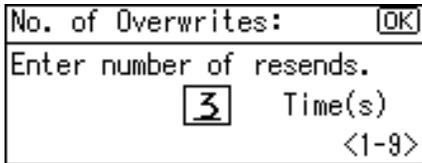
If you select [DoD], proceed to step 9.

For details about the methods of overwriting, see "Methods of Overwriting".

6. Select [Random Numbers] using [▲] or [▼], and then press the [OK] key.

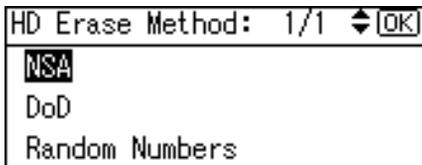


7. Enter the number of times that you want to overwrite using the number keys, and then press the [OK] key.



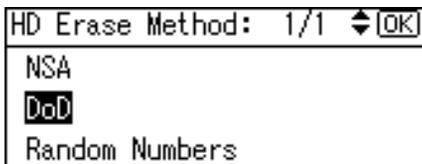
Auto Erase Memory is set.

8. Select [NSA] using [▲] or [▼], and then press the [OK] key.



Auto Erase Memory is set.

9. Select [DoD] using [▲] or [▼], and then press the [OK] key.



Auto Erase Memory is set.

**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.32 "Logging on Using Administrator Authentication"
- p.33 "Logging off Using Administrator Authentication"
- p.132 "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 4 in "Auto Erase Memory Setting".
2. Select [Off] using [▲] or [▼], and then press the [OK] key.

Auto Erase Memory is disabled.

### Note

- To set Auto Erase Memory to "On" again, repeat the procedure in "Using Auto Erase Memory".

### Reference

- p.32 "Logging on Using Administrator Authentication"
- p.33 "Logging off Using Administrator Authentication"

## Types of Data that Can or Cannot Be Overwritten

The following table shows 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

### Data Not Overwritten by Auto Erase Memory

- 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
- Image overlay data

Image overlay data is overwritten after it is deleted.

#### Reference

- p.118 "Protecting the Address Book"

## 5

---

### 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.

#### Important

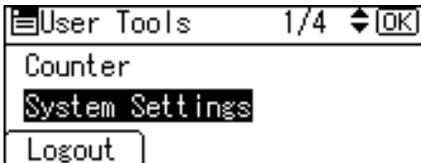
- If you select "Erase All Memory", the following are also deleted: user codes, counters under each user code, user stamps, data stored in the Address Book, printer fonts downloaded by users, applications using Embedded Software Architecture, SSL server certificates, and the machine's network settings.
- 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 hours.

#### Reference

- p.32 "Logging on Using Administrator Authentication"
- p.33 "Logging off Using Administrator Authentication"

## Using Erase All Memory

1. Disconnect communication cables connected to the machine.
2. Press the [User Tools/Counter] key.
3. Select [System Settings] using [▲] or [▼], and then press the [OK] key.



4. Select [Administrator Tools] using [▲] or [▼], and then press the [OK] key.



5. Select [Erase All Memory] using [▲] or [▼], and then press the [OK] key.



6. Select the method of erasing the data.

Select the method of erasing the data from [NSA], [DoD], or [Random Numbers].

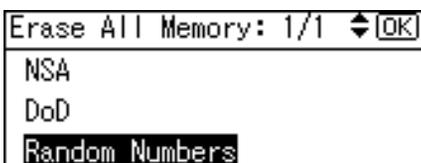
If you select [Random Numbers], proceed to step 7.

If you select [NSA] proceed to step 9.

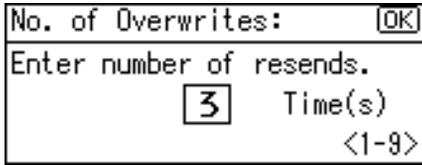
If you select [DoD], proceed to step 10.

For details about the methods of overwriting, see "Methods of Overwriting".

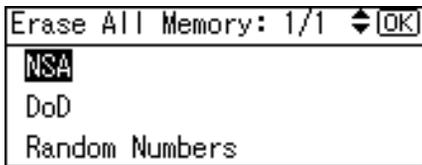
7. Select [Random Numbers] using [▲] or [▼], and then press the [OK] key.



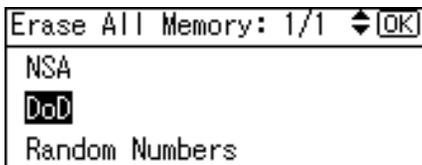
- Enter the number of times that you want to overwrite using the number keys, and then press the [OK] key.



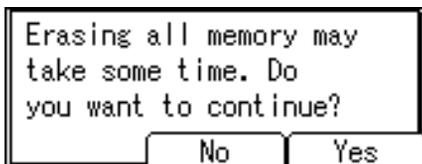
- Select [NSA] using [▲] or [▼], and then press the [OK] key.



- Select [DoD] using [▲] or [▼], and then press the [OK] key.



- Press [Yes].



- When overwriting is completed, press [Exit], and then turn off the power.

**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 you specify to both overwrite and encrypt the data, the data will all be encrypted.
- If an error occurs before overwriting is completed, turn off the main power. Turn it on again, and then repeat from step 2.

**Reference**

- p.132 "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 canceled.
  3. Turn off the main power.

**↓ 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 "Items" under "Admin. Auth. 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 [Items] in "Admin. Auth. Management" 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 Features
- Fax 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.21 "Administrators"
- p.27 "Registering the Administrator"
- p.265 "User Administrator Settings"
- p.248 "Machine Administrator Settings"
- p.258 "Network Administrator Settings"
- p.263 "File Administrator Settings"
- p.270 "User Settings - Control Panel Settings"
- p.287 "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.270 "User Settings - Control Panel Settings"
- p.287 "User Settings - Web Image Monitor Settings"

## Specifying Menu Protect

This can be specified by the machine administrator. 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].

For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

### Reference

- p.32 "Logging on Using Administrator Authentication"
- p.33 "Logging off Using Administrator Authentication"

## Copy Function

To specify "Menu Protect" in "Copier Features", set "Machine Management" to [On] in "Admin. Auth. Management" in "Administrator Tools" in "System Settings".

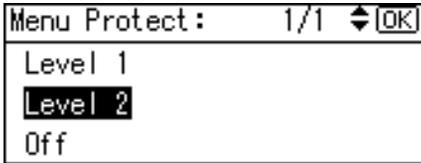
1. Press the [User Tools/Counter] key.
2. Select [Copier Features] using [▲] or [▼], and then press the [OK] key.



3. Select [Menu Protect] using [▲] or [▼], and then press the [OK] key.



4. Select the menu protect level using [▲] or [▼], and then press the [OK] key.



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

## Fax Function

---

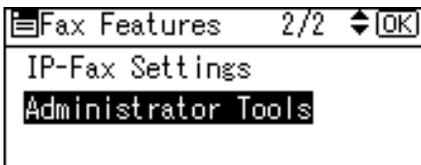
### 6

To specify "Menu Protect" in "Fax Features", set "Machine Management" to [On] in "Admin. Auth. Management" in "Administrator Tools" in "System Settings".

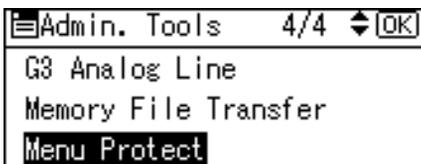
1. Press the [User Tools/Counter] key.
2. Select [Fax Features] using [▲] or [▼], and then press the [OK] key.



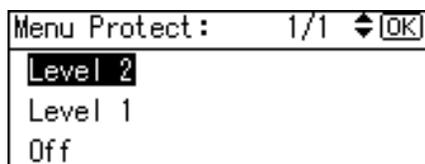
3. Select [Administrator Tools] using [▲] or [▼], and then press the [OK] key.



4. Select [Menu Protect] using [▲] or [▼], and then press the [OK] key.



5. Select the menu protect level using [▲] or [▼], and then press the [OK] key.



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

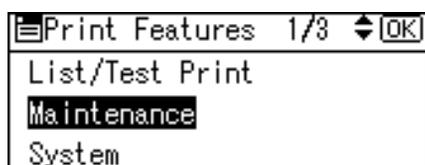
## Printer Function

To specify "Menu Protect" in "Printer Features", set "Machine Management" to [On] in "Admin. Auth. Management" in "Administrator Tools" in "System Settings".

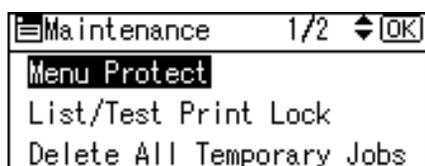
1. Press the [User Tools/Counter] key.
2. Select [Printer Features] using [▲] or [▼], and then press the [OK] key.



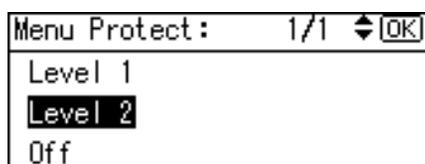
3. Select [Maintenance] using [▲] or [▼], and then press the [OK] key.



4. Select [Menu Protect] using [▲] or [▼], and then press the [OK] key.



5. Select the menu protect level using [▲] or [▼], and then press the [OK] key.



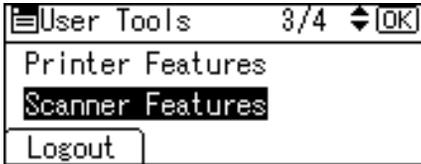
6. Press the [User Tools/Counter] key.

## Scanner Function

---

To specify "Menu Protect" in "Scanner Features", set "Machine Management" to [On] in "Admin. Auth. Management" in "Administrator Tools" in "System Settings".

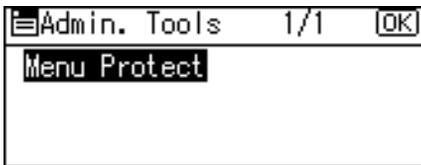
1. Press the [User Tools/Counter] key.
2. Select [Scanner Features] using [▲] or [▼], and then press the [OK] key.



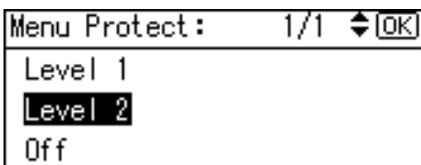
3. Select [Administrator Tools] using [▲] or [▼], and then press the [OK] key.



4. Select [Menu Protect], and then press the [OK] key.



5. Select the menu protect level using [▲] or [▼], and then press the [OK] key.



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

# Limiting Available Functions

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

## Available Functions

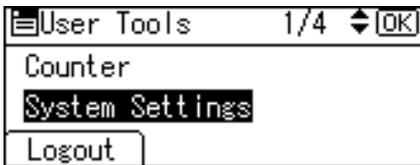
Specify the available functions from the copier, fax, scanner, and printer functions.

## 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".

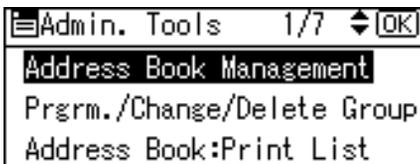
1. Press the [User Tools/Counter] key.
2. Select [System Settings] using [▲] or [▼], and then press the [OK] key.



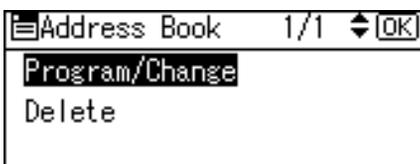
3. Select [Administrator Tools] using [▲] or [▼], and then press the [OK] key.



4. Select [Address Book Management] using [▲] or [▼], and then press the [OK] key.



5. Select [Program/Change] using [▲] or [▼], and then press the [OK] key.



6. Enter the registration number you want to program using the number keys or the Quick Dial keys, and then press the [OK] key.

|                             |                    |
|-----------------------------|--------------------|
| Program/Change:             | [OK]               |
| Enter No. to program/change |                    |
| 010                         | Quick Dial:001-016 |
| Search                      |                    |

By pressing [Search], you can search by Name, Display Destination List, Registration No., User Code and Fax Destination.

7. Press the [OK] key.

|             |      |
|-------------|------|
| Name:       | [OK] |
| Enter name. |      |
| abc         | user |

8. Press [Details].

|                            |          |
|----------------------------|----------|
| Program/Change:            | [OK]     |
| 010                        | user     |
| Press OK key after setting |          |
| Details                    | Reg. No. |

9. Select [Auth. Info] using [▲] or [▼], and then press the [OK] key.

|               |     |      |
|---------------|-----|------|
| Det. Settings | 1/3 | [OK] |
| Auth. Info    |     |      |
| Auth. Protect |     |      |
| End           |     |      |

10. Select [Function Permissions] using [▲] or [▼], and then press the [OK] key.

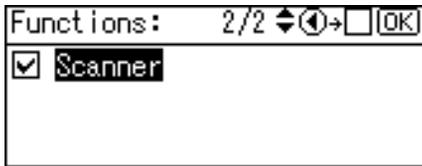
|                      |     |      |
|----------------------|-----|------|
| Auth. Info           | 2/2 | [OK] |
| LDAP Authentication  |     |      |
| Function Permissions |     |      |

11. Select which of the machine's functions you want to permit using [▲] or [▼], and then press the [▶] key.

|  |     |      |
|--|-----|------|
| Functions:                                 | 1/2 | [OK] |
| <input checked="" type="checkbox"/> Copier |     |      |
| <input type="checkbox"/> Printer           |     |      |
| <input type="checkbox"/> Fax               |     |      |

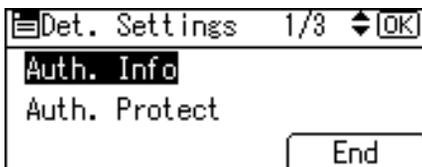
The box next to a selected item is checked. To deselect the item, press [◀].

12. Press the [OK] key.



13. Press the [Escape] key.

14. Press [End].



15. Press the [OK] key.

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

#### Reference

- p.32 "Logging on Using Administrator Authentication"
- p.33 "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 faxing, and control panel operations such as sending scan files and printing reports (the configuration list, for example).

- Access Log

Stores details of login/logout activity, service engineer operations such as hard disk formatting, system operations such as viewing the results of log transfers, 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

---

You can specify settings such as whether or not to transfer logs to Web SmartDeviceMonitor and whether or not to delete all logs.

### Disabling Log Transfer to Web SmartDeviceMonitor

---

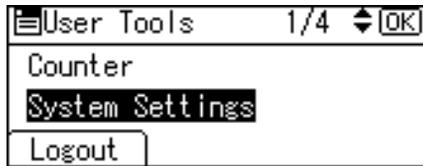
This can be specified by the machine administrator. For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

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/Counter] key.
2. Select [System Settings] using [▲] or [▼], and then press the [OK] key.



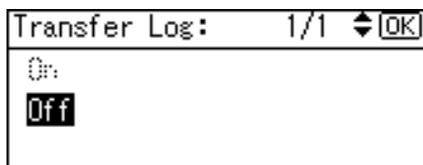
3. Select [Administrator Tools] using [▲] or [▼], and then press the [OK] key.



4. Select [Transfer Log Setting] using [▲] or [▼], and then press the [OK] key.



5. Press the [OK] key.



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

#### Reference

- p.32 "Logging on Using Administrator Authentication"
- p.33 "Logging off Using Administrator Authentication"

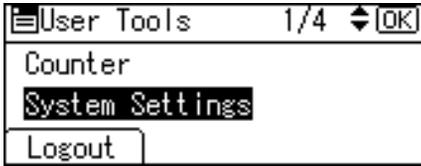
## Specifying Delete All Logs

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".

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/Counter] key.
2. Select [System Settings] using [▲] or [▼], and then press the [OK] key.



3. Select [Administrator Tools] using [▲] or [▼], and then press the [OK] key.

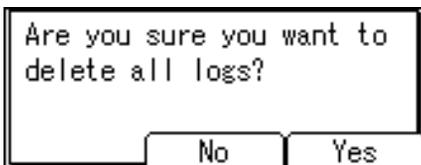


4. Select [Delete All Logs] using [▲] or [▼], and then press the [OK] key.



6

5. Press [Yes].



6. Press [Exit].



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

**Reference**

- p.32 "Logging on Using Administrator Authentication"
- p.33 "Logging off Using Administrator Authentication"

---

## 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.

### Reference

- p.32 "Logging on Using Administrator Authentication"
- p.33 "Logging off Using Administrator Authentication"

---

## Specify Log Collect Settings

---

Specify collection log settings. The collection log 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 Level" or "Access Log Collect Level" 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

---

**6**

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].

**6. Click [OK].**

The log is encrypted. If other changes have been made in related log settings, they will occur at the same time.

**7. 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] under "Device Settings".**
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.160 "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 Web Image Monitor Help.

#### Job Log Information Items

| Job Log Item                       | Content  |
|------------------------------------|--|
| Copier: Copying                    | Details of normal and Sample Copy jobs.  |
| Scanner: Sending                   | Details of sent scan files.  |
| 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.   |

| Job Log Item                     | Content   |
|----------------------------------|---|
| 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.  |
| Report Printing                  | Details of reports printed from the control panel.  |
| Result Report Printing/E-mailing | Details of sent e-mail notifications and printouts of reports such as the Communication Result Report and Error Report.                             |
| Scanner: TWAIN Driver Scanning   | Details of stored scan files that were sent using Network TWAIN Scanner.  |
| Fax: Sending                     | Details of sent fax files.  |
| Fax: LAN-Fax Sending             | Details of sent LAN-Fax files.  |
| Fax: Storing                     | Details of stored fax files.  |
| Fax: Stored File Printing        | Details of printing of fax files waiting be sent.   |
| Fax: Receiving                   | Details of received fax files.  |
| Fax: Receiving and Delivering    | Details of forwarding of received fax files.  |
| Fax: Receiving and Storing       | Details of storage of received fax files.   |

### 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. |
| HDD Format         | Details of hard disk formatting.                  |
| All Logs Deletion  | Details of deletions of all logs.                 |
| Log Setting Change | Details of changes made to log settings.          |
| Transfer Log Error | Details of log transfer errors.                   |

| Access Log Item                      | Content  |
|--------------------------------------|--|
| Log Collection Item Change           | Details of changes to job log collection levels, access log collection levels, and types of log collected.                       |
| Collect Encrypted Communication Logs | Details of communications that were encrypted using utilities, Web Image Monitor, or external devices.                           |
| 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.   |
| File Access Privilege Change         | Details of changes made to access privileges for 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; "Received File" indicates a stored file; "Printer" indicates a printer driver job; "Report" indicates a printed report. |
| Start Date/Time | Dates and times "Scan File", "Received File" and "Printer" operations started.  |

| Item                | Content  |
|---------------------|--|
| End Date/Time       | Dates and times "Scan File", "Received File" and "Report" operations ended.  |
| Stored File ID      | ID assigned to stored "Stored File" files.   |
| Stored File Name    | Names of "Stored File" files.  |
| 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, e-mail address or fax number 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

| Item                                  | Content  |
|---------------------------------------|--|
| Access Log Type                       | Type of access log.  |
| Authentication Server                 | The name of the authentication server accessed last (Windows/LDAP Authentication only).  |
| No. of Authentication Server Switches | The number of authentication server switches due to server failure (LDAP Authentication only).   |
| 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. |

| Item                   | Content   |
|------------------------|---|
| 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.  |
| File Location          | Region of all file deletion. "Fax Memory" 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.157 "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, 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 [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"> <li>Control Panel</li> <li>Web Image Monitor</li> <li>telnet</li> <li>SmartDeviceMonitor for Admin</li> <li>Web SmartDeviceMonitor</li> </ul> | <p>All applications that operate over IPv4 cannot be used.</p> <p>IPv4 cannot be disabled from Web Image Monitor when using IPv4 transmission.</p> |
| IPv6     | -    | <ul style="list-style-type: none"> <li>Control Panel</li> <li>Web Image Monitor</li> <li>telnet</li> <li>SmartDeviceMonitor for Admin</li> <li>Web SmartDeviceMonitor</li> </ul> | <p>All applications that operate over IPv6 cannot be used.</p>   |
| IPsec    | -    | <ul style="list-style-type: none"> <li>Control Panel</li> <li>Web Image Monitor</li> <li>telnet</li> </ul>   | <p>Encrypted transmission using IPsec is disabled.</p>   |

| Protocol | Port                 | Setting Method   | When Disabled  |
|----------|----------------------|--|--|
| FTP      | TCP:21               | <ul style="list-style-type: none"> <li>• Web Image Monitor</li> <li>• telnet</li> <li>• SmartDeviceMonitor for Admin</li> <li>• Web SmartDeviceMonitor</li> </ul>        | <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"> <li>• Web Image Monitor</li> <li>• telnet</li> <li>• SmartDeviceMonitor for Admin</li> <li>• Web SmartDeviceMonitor</li> </ul>        | <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"> <li>• Web Image Monitor</li> </ul>  | <p>Commands using telnet are disabled.</p>   |
| SMTP     | TCP:25<br>(variable) | <ul style="list-style-type: none"> <li>• Control Panel</li> <li>• Web Image Monitor</li> <li>• SmartDeviceMonitor for Admin</li> <li>• Web SmartDeviceMonitor</li> </ul> | <p>Internet Fax or e-mail notification functions that require SMTP reception cannot be used.</p>   |
| HTTP     | TCP:80               | <ul style="list-style-type: none"> <li>• Web Image Monitor</li> <li>• telnet</li> </ul>  | <p>Functions that require HTTP cannot be used.</p> <p>Cannot print using IPP on port 80.</p>   |

| Protocol  | Port               | Setting Method   | When Disabled   |
|-----------|--------------------|--|---|
| HTTPS     | TCP:443            | <ul style="list-style-type: none"> <li>• Web Image Monitor</li> <li>• telnet</li> </ul>  | <p>Functions that require HTTPS cannot be used.</p> <p>@Remote cannot be used.</p> <p>You can also make settings to require SSL transmission using the control panel or Web Image Monitor.</p>      |
| SMB       | TCP:139            | <ul style="list-style-type: none"> <li>• Control Panel</li> <li>• Web Image Monitor</li> <li>• telnet</li> <li>• SmartDeviceMonitor for Admin</li> <li>• Web SmartDeviceMonitor</li> </ul> | SMB printing functions cannot be used.  |
| NBT       | UDP:137<br>UDP:138 | <ul style="list-style-type: none"> <li>• telnet</li> </ul>   | SMB printing functions via TCP/IP, as well as NetBIOS designated functions on the WINS server cannot be used.   |
| SNMPv1,v2 | UDP:161            | <ul style="list-style-type: none"> <li>• Web Image Monitor</li> <li>• telnet</li> <li>• SmartDeviceMonitor for Admin</li> <li>• Web SmartDeviceMonitor</li> </ul>                          | <p>Functions that require SNMPv1, v2 cannot be used.</p> <p>Using the control panel, Web Image Monitor or telnet, you can specify that SNMPv1, v2 settings are read-only, and cannot be edited.</p> |

| Protocol | Port    | Setting Method  | When Disabled   |
|----------|---------|---|---|
| SNMPv3   | UDP:161 | <ul style="list-style-type: none"> <li>• Web Image Monitor</li> <li>• telnet</li> <li>• SmartDeviceMonitor for Admin</li> <li>• Web SmartDeviceMonitor</li> </ul> | <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"> <li>• Web Image Monitor</li> <li>• telnet</li> <li>• SmartDeviceMonitor for Admin</li> <li>• Web SmartDeviceMonitor</li> </ul> | <p>Functions that require RSH and network TWAIN functions cannot be used.</p> <p>You can restrict personal information from being displayed by making settings on the control panel using "Restrict Display of User Information".</p>     |
| LPR      | TCP:515 | <ul style="list-style-type: none"> <li>• Web Image Monitor</li> <li>• telnet</li> <li>• SmartDeviceMonitor for Admin</li> <li>• Web SmartDeviceMonitor</li> </ul> | <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>  |

| Protocol | Port  | Setting Method   | When Disabled   |
|----------|---|--|---|
| IPP      | TCP:631   | <ul style="list-style-type: none"> <li>• Web Image Monitor</li> <li>• telnet</li> <li>• SmartDeviceMonitor for Admin</li> <li>• Web SmartDeviceMonitor</li> </ul>        | IPP functions cannot be used.   |
| IP-Fax   | TCP:1720 (H.323)<br>UDP:1719 (Gatekeeper)<br>TCP/UDP:5060 (SIP)<br>TCP:5000 (H.245)<br>UDP:5004, 5005 (Voice)<br>TCP/UDP:49152 (T.38) | <ul style="list-style-type: none"> <li>• Control Panel</li> <li>• Web Image Monitor</li> <li>• SmartDeviceMonitor for Admin</li> <li>• Web SmartDeviceMonitor</li> </ul> | IP-Fax connecting functions using H.323, SIP and T.38 cannot be used. |
| SSDP     | UDP:1900  | <ul style="list-style-type: none"> <li>• Web Image Monitor</li> <li>• telnet</li> </ul>  | Device discovery using UPnP from Windows cannot be used.              |
| Bonjour  | UDP:5353  | <ul style="list-style-type: none"> <li>• Web Image Monitor</li> <li>• telnet</li> <li>• SmartDeviceMonitor for Admin</li> <li>• Web SmartDeviceMonitor</li> </ul>        | Bonjour functions cannot be used.                                     |
| @Remote  | TCP:7443<br>TCP:7444  | <ul style="list-style-type: none"> <li>• telnet</li> </ul>   | @Remote cannot be used.   |
| DIPRINT  | TCP:9100  | <ul style="list-style-type: none"> <li>• Web Image Monitor</li> <li>• telnet</li> <li>• SmartDeviceMonitor for Admin</li> <li>• Web SmartDeviceMonitor</li> </ul>        | DIPRINT functions cannot be used.                                     |

| Protocol      | Port                    | Setting Method   | When Disabled   |
|---------------|-------------------------|--|---|
| RFU           | TCP:10021               | <ul style="list-style-type: none"> <li>telnet</li> </ul>   | You can attempt to update firmware via FTP.                 |
| NetWare       | (IPX/SPX)               | <ul style="list-style-type: none"> <li>Control Panel</li> <li>Web Image Monitor</li> <li>telnet</li> <li>SmartDeviceMonitor for Admin</li> <li>Web SmartDeviceMonitor</li> </ul> | Cannot print with NetWare.<br>SNMP over IPX cannot be used. |
| AppleTalk     | (PAP)                   | <ul style="list-style-type: none"> <li>Control Panel</li> <li>Web Image Monitor</li> <li>telnet</li> </ul>   | Cannot print with AppleTalk.                                |
| WSD (Device)  | TCP:53000<br>(variable) | <ul style="list-style-type: none"> <li>Web Image Monitor</li> <li>telnet</li> <li>SmartDeviceMonitor for Admin</li> <li>Web SmartDeviceMonitor</li> </ul>                        | WSD (Device) functions cannot be used.                      |
| WSD (Printer) | TCP:53001<br>(variable) | <ul style="list-style-type: none"> <li>Web Image Monitor</li> <li>telnet</li> <li>SmartDeviceMonitor for Admin</li> <li>Web SmartDeviceMonitor</li> </ul>                        | WSD (Printer) functions cannot be used.                     |
| WSD (Scanner) | TCP:53002<br>(variable) | <ul style="list-style-type: none"> <li>Web Image Monitor</li> <li>telnet</li> <li>SmartDeviceMonitor for Admin</li> <li>Web SmartDeviceMonitor</li> </ul>                        | WSD (Scanner) functions cannot be used.                     |

| Protocol     | Port         | Setting Method   | When Disabled  |
|--------------|--------------|--|--|
| WS-Discovery | UDP/TCP:3702 | <ul style="list-style-type: none"> <li>telnet</li> <li>Web SmartDeviceMonitor</li> </ul> | WSD (Device, Printer, Scanner) search function cannot be used. |
| RHPP         | TCP:59100    | <ul style="list-style-type: none"> <li>Web Image Monitor</li> <li>telnet</li> </ul>      | 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".

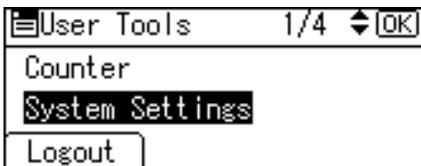
**Reference**

- p.32 "Logging on Using Administrator Authentication"
- p.33 "Logging off Using Administrator Authentication"
- p.217 "Specifying the Extended Security Functions"

**7**

**Enabling and Disabling Protocols Using the Control Panel**

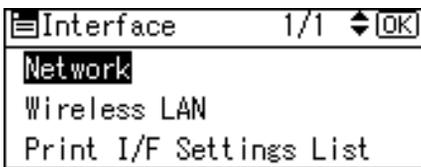
1. Press the [User Tools/Counter] key.
2. Select [System Settings] using [▲] or [▼], and then press the [OK] key.



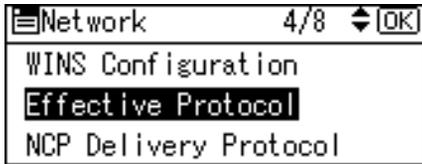
3. Select [Interface Settings] using [▲] or [▼], and then press the [OK] key.



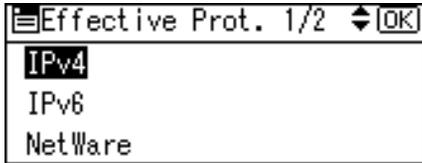
4. Select [Network] using [▲] or [▼], and then press the [OK] key.



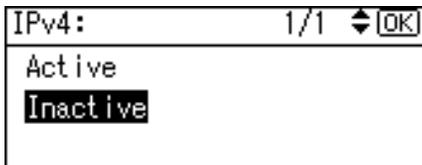
5. Select [Effective Protocol] using [▲] or [▼], and then press the [OK] key.



6. Select the protocol you want to specify, and then press the [OK] key.



7. Select [Inactive] using [▲] or [▼], and then press the [OK] key.



8. Press the [User Tools/Counter] 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**

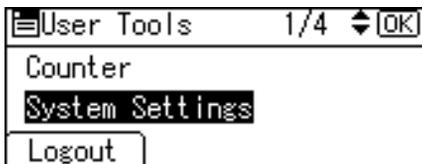
- p.32 "Logging on Using Administrator Authentication"
- p.33 "Logging off Using Administrator Authentication"

---

## Specifying Network Security Level Using the Control Panel

---

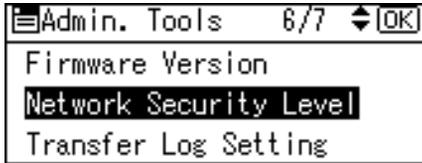
1. Press the [User Tools/Counter] key.
2. Select [System Settings] using [▲] or [▼], and then press the [OK] key.



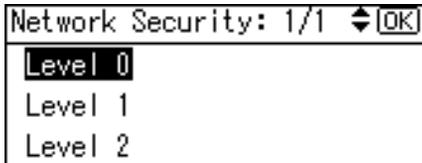
3. Select [Administrator Tools] using [▲] or [▼], and then press the [OK] key.



4. Select [Network Security Level] using [▲] or [▼], and then press the [OK] key.



5. Select the network security level using [▲] or [▼], and then press the [OK] key.



Select [Level 0], [Level 1], or [Level 2].

6. Press the [User Tools/Counter] 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 |
| SSL/TLS> Certificate Status           | None                | None                | None            |
| 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        |
| WSD (Printer)                         | Active              | Active              | Inactive        |
| WSD (Scanner)                         | 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 /<br>Cleartext | Encryption /<br>Cleartext | Encryption<br>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

---

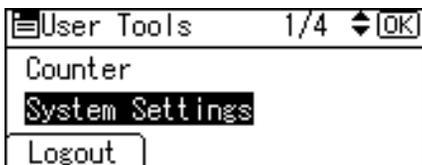
This can be specified by the network administrator.

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/Counter] key.
2. Select [System Settings] using [▲] or [▼], and then press the [OK] key.



3. Select [Administrator Tools] using [▲] or [▼], and then press the [OK] key.



4. Select [Extended Security] using [▲] or [▼], and then press the [OK] key.

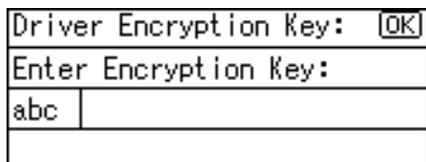


5. Select [Driver Encryption Key] using [▲] or [▼], and then press the [OK] key.



"Driver Encryption Key" is one of the extended security functions. For details about this and other security functions, see "Specifying the Extended Security Functions".

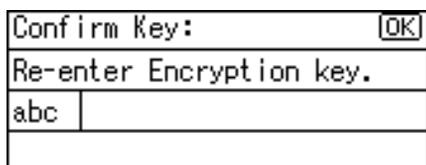
6. Enter the driver encryption key, and then press the [OK] key.



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. Re-enter the encryption key, and then press the [OK] key.



8. Press the [User Tools/Counter] 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.32 "Logging on Using Administrator Authentication"
- p.33 "Logging off Using Administrator Authentication"
- p.217 "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.

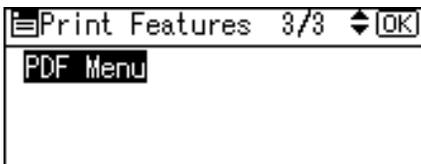
By using a PDF group password, you can enhance security and so protect passwords from being analyzed.

For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

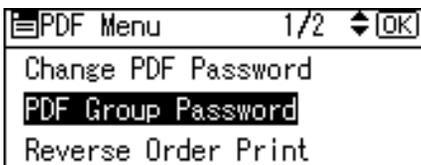
1. Press the [User Tools/Counter] key.
2. Select [Printer Features] using [▲] or [▼], and then press the [OK] key.



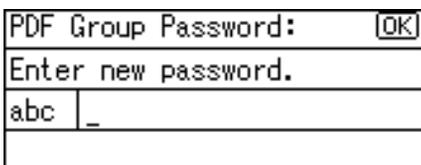
3. Select [PDF Menu] using [▲] or [▼], and then press the [OK] key.



4. Select [PDF Group Password] using [▲] or [▼], and then press the [OK] key.



5. Enter the new PDF Group password, and then press the [OK] key.



6. Re-enter the PDF Group password, and then press the [OK] key.

|                             |      |
|-----------------------------|------|
| PDF Group Password:         | [OK] |
| Enter Confirmation password |      |
| abc                         | _    |
|                             |      |

7. Press the [Escape] key two times.
8. Press the [User Tools/Counter] 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.32 "Logging on Using Administrator Authentication"
- p.33 "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] under "Security", and then click [IPP Authentication].  
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 [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.

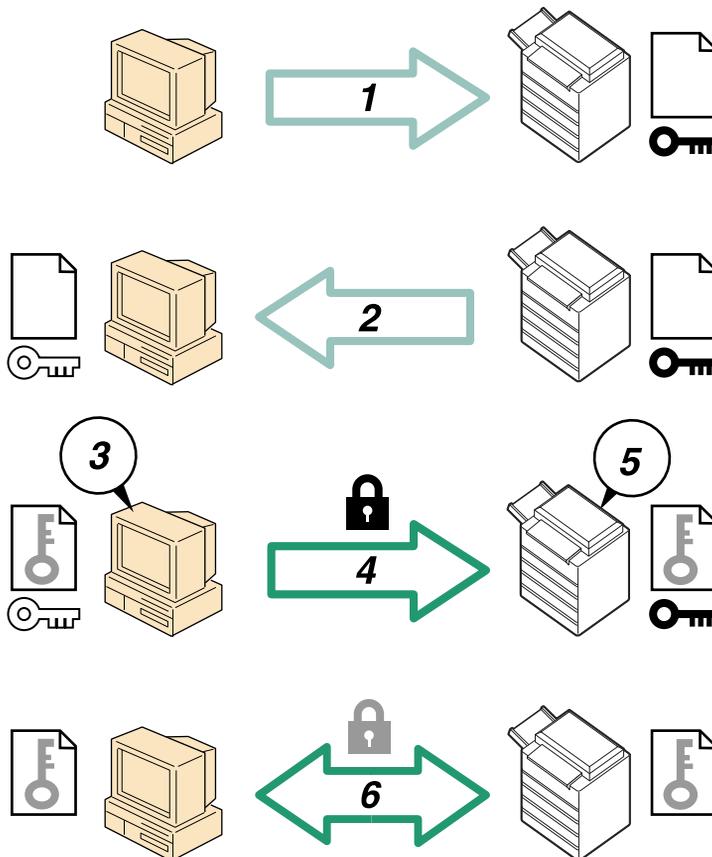
## SSL (Secure Sockets Layer) Encryption

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].**

"Requesting" appears for "Certificate Status" in the "Certificates" area.

**9. Click [Logout].**

**10. Apply to the certificate authority for the device certificate.**

The application procedure depends on the certificate authority. For details, contact the certificate authority.

For the application, click Web Image Monitor Details icon and use the information that appears in "Certificate Details".

**Note**

- The issuing location may not be displayed if you request two certificates at the same time. When you install a certificate, be sure to check the certificate destination and installation procedure.
- Using Web Image Monitor, you can create the contents of the device certificate but you cannot send the certificate application.
- Click [Cancel Request] to cancel the request for the device certificate.

**7**

### **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].**

"Installed" appears under "Certificate Status" to show that a device certificate for the machine has been installed.

**9. 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 appears whenever 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.

## Setting the SSL/TLS Encryption Mode

By specifying the SSL/TLS encrypted communication mode, you can change the security level.

### 7

#### Encrypted Communication Mode

Using the encrypted communication mode, you can specify encrypted communication.

|                      |  |
|----------------------|--|
| Ciphertext Only      | Allows encrypted communication only.<br>If encryption is not possible, the machine does not communicate.                           |
| Ciphertext Priority  | Performs encrypted communication if encryption is possible.<br>If encryption is not possible, the machine communicates without it. |
| Ciphertext/Cleartext | Communicates with or without encryption, according to the setting.   |

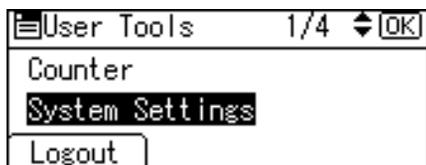
#### Specifying the SSL/TLS Encryption Mode

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/Counter] key.
2. Select [System Settings] using [▲] or [▼], and then press the [OK] key.



3. Select [Interface Settings] using [▲] or [▼], and then press the [OK] key.



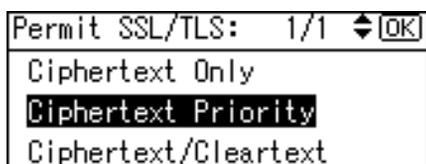
4. Select [Network] using [▲] or [▼], and then press the [OK] key.



5. Select [Permit SSL/TLS Comm.] using [▲] or [▼], and then press the [OK] key.



6. Select the encrypted communication mode using [▲] or [▼], and then press the [OK] key.



Select [Ciphertext Only], [Ciphertext Priority], or [Ciphertext/Cleartext] as the encrypted communication mode.

7. Press the [User Tools/Counter] 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.32 "Logging on Using Administrator Authentication"
- p.33 "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".

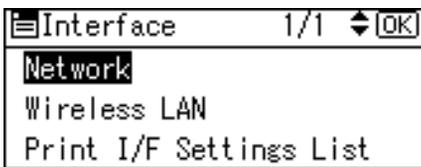
1. Press the [User Tools/Counter] key.
2. Select [System Settings] using [▲] or [▼], and then press the [OK] key.



3. Select [Interface Settings] using [▲] or [▼], and then press the [OK] key.



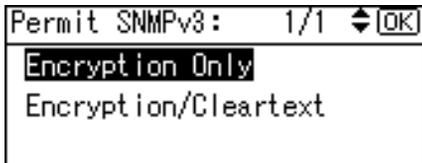
4. Select [Network] using [▲] or [▼], and then press the [OK] key.



5. Select [Permit SNMPv3 Communictn.] using [▲] or [▼], and then press the [OK] key.



6. Select [Encryption Only] using [▲] or [▼], and then press the [OK] key.



7. Press the [User Tools/Counter] 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 Key] in [SNMP Authentication Information] in SmartDeviceMonitor for Admin, in addition to specifying [Permit SNMPv3 Communictn.] on the machine. For details about specifying [Encryption Key] 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.32 "Logging on Using Administrator Authentication"
- p.33 "Logging off Using Administrator Authentication"
- p.27 "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 Communication 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"> <li>Active</li> <li>Inactive</li> </ul>  |
| Exclude HTTPS Communication    | Specify whether to enable IPsec for HTTPS transmission.  | <ul style="list-style-type: none"> <li>Active</li> <li>Inactive</li> </ul> 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"> <li>Active</li> <li>Inactive</li> </ul> Specify "Active" if you want to use "Encryption Key Manual Exchange 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.<br><br>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/<br>HMAC-SHA1-96 | HMAC-MD5-96/<br>HMAC-SHA1-96             | HMAC-SHA1-96                             |
| Phase 2 Encryption Algorithm     | Cleartext (NULL encryption)  | DES/3DES/<br>AES-128/AES-192/<br>AES-256 | 3DES/AES-128/<br>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"> <li>Inactive</li> <li>IPv4</li> <li>IPv6</li> <li>IPv4/IPv6 (Default Settings only)</li> </ul>                       |
| 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.<br><br>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.<br>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"> <li>• apply</li> <li>• bypass</li> <li>• discarded</li> </ul>   |
| Encapsulation Mode      | Specify the encapsulation mode.<br>(auto setting)  | <ul style="list-style-type: none"> <li>• Transport</li> <li>• Tunnel</li> </ul> (Tunnel beginning address - Tunnel ending address)<br>If you specify "Tunnel", you must then specify the "Tunnel End Points", 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.<br>(auto setting) | <ul style="list-style-type: none"> <li>• Use When Possible</li> <li>• Always Require</li> </ul>  |
| Authentication Method   | Specify the method for authenticating transmission partners.<br>(auto setting)   | <ul style="list-style-type: none"> <li>• PSK</li> <li>• Certificate</li> </ul> If you specify PSK, you must then set the PSK text (using ASCII characters).<br>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<br>HASH Algorithm           | Specify the HASH algorithm to be used in phase 1.<br>(auto setting)  | <ul style="list-style-type: none"> <li>• MD5</li> <li>• SHA1</li> </ul>                 |
| Phase 1<br>Encryption Algorithm     | Specify the encryption algorithm to be used in phase 1.<br>(auto setting)  | <ul style="list-style-type: none"> <li>• DES</li> <li>• 3DES</li> </ul>                 |
| Phase 1<br>Diffie-Hellman Group     | Select the Diffie-Hellman group number used for IKE encryption key generation.<br>(auto setting)   | <ul style="list-style-type: none"> <li>• 1</li> <li>• 2</li> <li>• 14</li> </ul>        |
| Phase 1<br>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<br>Security Protocol        | Specify the security protocol to be used in Phase 2.<br><br>To apply both encryption and authentication to sent data, specify ESP or ESP+AH.<br><br>To apply authentication data only, specify AH.<br>(auto setting) | <ul style="list-style-type: none"> <li>• ESP</li> <li>• AH</li> <li>• ESP+AH</li> </ul> |
| Phase 2<br>Authentication Algorithm | Specify the authentication algorithm to be used in phase 2.<br>(auto setting)  | <ul style="list-style-type: none"> <li>• HMAC-MD5-96</li> <li>• HMAC-SHA1-96</li> </ul> |

| Setting  | Description  | Setting Value   |
|--|--|---|
| Phase 2<br>Encryption Algorithm<br>Permissions | Specify the encryption algorithm to be used in phase 2.<br><br>(auto setting)                                      | <ul style="list-style-type: none"> <li>• Cleartext (NULL encryption)</li> <li>• DES</li> <li>• 3DES</li> <li>• AES-128</li> <li>• AES-192</li> <li>• AES-256</li> </ul> |
| Phase 2<br>PFS                                 | Specify whether to activate PFS. Then, if PFS is activated, select the Diffie-Hellman group.<br><br>(auto setting) | <ul style="list-style-type: none"> <li>• Inactive</li> <li>• 1</li> <li>• 2</li> <li>• 14</li> </ul>  |
| Phase 2<br>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"> <li>• Inactive</li> <li>• IPv4</li> <li>• IPv6</li> <li>• IPv4/IPv6 (Default Settings only)</li> </ul>               |
| 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.<br><br>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.<br>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"> <li>• Transport</li> <li>• Tunnel</li> </ul> (Tunnel beginning address - Tunnel ending address)<br>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 AH + ESP.<br><br>To apply authentication data only, specify AH. | <ul style="list-style-type: none"> <li>• ESP</li> <li>• AH</li> <li>• ESP + AH</li> </ul>   |
| Authentication Algorithm | Specify the authentication algorithm.  | <ul style="list-style-type: none"> <li>• HMAC-MD5-96</li> <li>• HMAC-SHA1-96</li> </ul>   |

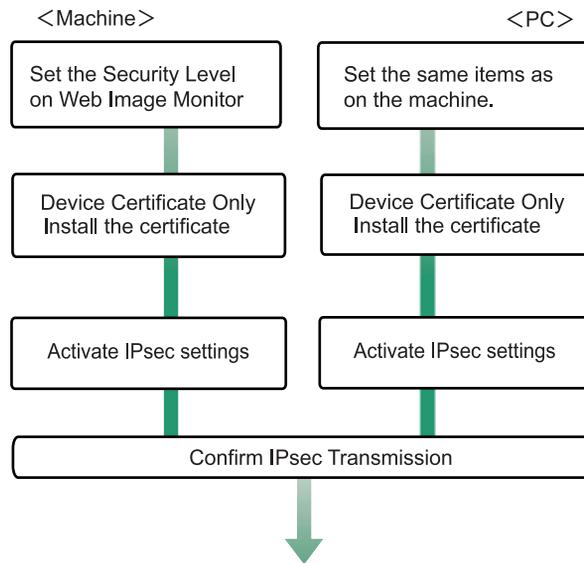
| Setting              | Description                                       | Setting Value  |
|----------------------|---|--|
| Authentication Key   | Specify the key for the authentication algorithm. | <p>Specify a value within the ranges shown below, according to the encryption algorithm.</p> <p>Hexadecimal value<br/>0-9, a-f, A-F</p> <ul style="list-style-type: none"> <li>• If HMAC-MD5-96, set 32 digits</li> <li>• If HMAC-SHA1-96, set 40 digits</li> </ul> <p>ASCII</p> <ul style="list-style-type: none"> <li>• If HMAC-MD5-96, set 16 characters</li> <li>• If HMAC-SHA1-96, set 20 characters</li> </ul> |
| Encryption Algorithm | Specify the encryption algorithm.                 | <ul style="list-style-type: none"> <li>• Cleartext (NULL encryption)</li> <li>• DES</li> <li>• 3DES</li> <li>• AES-128</li> <li>• AES-192</li> <li>• AES-256</li> </ul>  |

| 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.<br>hexadecimal value<br>0-9, a-f, A-F <ul style="list-style-type: none"> <li>• DES, set 16 digits</li> <li>• 3DES, set 48 digits</li> <li>• AES-128, set 32 digits</li> <li>• AES-192, set 48 digits</li> <li>• AES-256, set 64 digits</li> </ul> ASCII <ul style="list-style-type: none"> <li>• DES, set 8 characters</li> <li>• 3DES, set 24 characters</li> <li>• AES-128, set 16 characters</li> <li>• AES-192, set 24 characters</li> <li>• AES-256, set 32 characters</li> </ul> |

7

**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 **[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.110 "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] settings page appears.
5. **Select the certificate to be used for IPsec from the drop down box in "IPsec" under "Certificate".**
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 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.

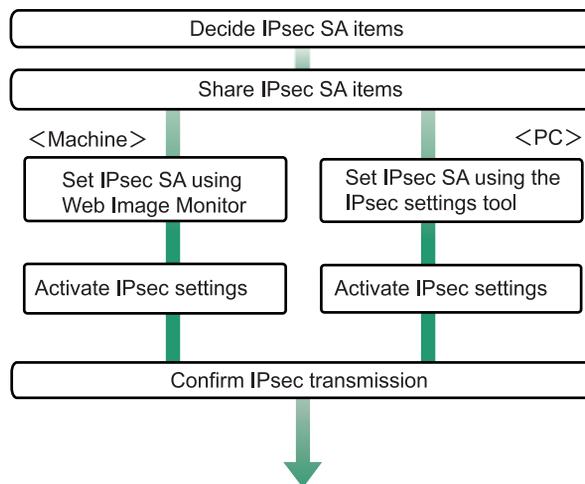
 **Note**

- To disable the computer's IPsec settings, select the security policy, right click, and then click [Unassign].

- 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] or [default] 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 ike {1|2|3|4|default} disable
```

- To disable the settings 1-4, specify the number [1-4].
- To disable the default settings, specify [default].

**Specify the local/remote address for settings 1-4**

```
msh> ipsec ike {1|2|3|4} {ipv4|ipv6} local address remote address
```

- Enter the separate setting number [1-4], and the address type to specify local and remote address.
- To set the local or remote address values, specify masklen by entering [/] and an integer 0-32 when settings an IPv4 address. When setting an IPv6 address, specify masklen by entering [/] and an integer 0-128.
- Not specifying an address value displays the current setting.

**7****Specify the address type in default setting**

```
msh> ipsec ike default {ipv4|ipv6|any}
```

- Specify the address type for the default setting.
- To specify both ipv4 and ipv6, enter [any].

**Security policy setting**

```
msh> ipsec ike {1|2|3|4|default} proc {apply|bypass|discard}
```

- Enter the separate setting number [1-4] or [default] and specify the security policy for the address specified in the selected setting.
- To apply IPsec to the relevant packets, specify [apply]. To not apply IPsec, specify [bypass].
- If you specify [discard], any packets 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

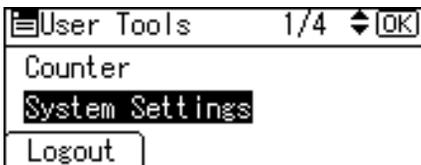
To change the extended security functions, display the extended security screen as follows.

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".

This section describes how to Change the Extended Security Functions.

1. Press the [User Tools/Counter] key.
2. Select [System Settings] using [▲] or [▼], and then press the [OK] key.



3. Select [Administrator Tools] using [▲] or [▼], and then press the [OK] key.



4. Select [Extended Security] using [▲] or [▼], and then press the [OK] key.



5. Press the setting you want to change using [▲] or [▼], and then press the [OK] key.



6. Change the setting, and then press the [OK] key.

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

### Reference

- p.32 "Logging on Using Administrator Authentication"
- p.33 "Logging off Using Administrator Authentication"

## Extended Security Settings

### 8

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 Dest. Use(Fax), Rstrct Dest. Use(Scanner)

This can be specified by the user administrator.

The available fax and scanner destinations are limited to the destinations registered in the Address Book.

A user cannot directly enter the destinations for transmission.

If [Rstrct Dest. Use(Scanner)] is set to [On], you can register fax numbers only.

If you have selected e-mail reception via SMTP, you cannot use "Restrict Dest. Use(Fax)" and "Rstrct Dest. Use(Scanner)".

The destinations searched by "LDAP Search" can be used.

For details about preventing unauthorized transmission, see "Preventing Information Leakage Due to Unauthorized Transmission".

- On
- Off

### **Rstrct Dest. Add.(Fax), Rstrct Dest. Add.(Scanner)**

This can be specified by the user administrator.

When "Restrict Dest. Use(Fax)" is set to [Off], after entering a destination directly on the fax screen, you can register it in the Address Book by pressing [Add Dest]. When "Rstrct Dest. Use(Scanner)" is set to [Off], after entering a destination directly on the scanner screen, you can register it in the Address Book by pressing [Add Dest].

If [On] is selected for this setting, [Add Dest] does not appear.

If you set "Rstrct Dest. Add.(Fax)" to [On], users can specify destinations directly on the fax screen, but cannot use [Add Dest] to register data in the Address Book. If you set "Rstrct Dest. Add.(Scanner)" to [On], users can specify destinations directly on the scanner screen, but cannot use [Add Dest] to register data in the Address Book. When this setting is made, only the user administrator can change the Address Book.

- On
- Off

### **Restrict User Info.Display**

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**

### 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 [Do not Restrict] to enable simple encryption. When SSL/TLS can be enabled, make this setting [Restrict].

For details about specifying SSL/TLS, see "Setting the SSL / TSL Encryption Mode".

If you select [Restrict], specify the encryption setting using the printer driver.

- Restrict
- **Do not Restrict**

### Transfer to Fax Receiver

This can be specified by the machine administrator.

If you use [Forwarding] 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
- Delivery of Mail Received via SMTP

- Routing Received Documents

### Remote Diags.(Fax)

This setting is not available if [Admin. Auth. Management] and [User Auth. Management] have been specified.

- Prohibit
- **Do not prohibit**

### 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 Auth. 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 1
- Level 2
- **Do not Restrict**
- Minimum Character No. (0)

### @Remote Service

This can be specified by the machine administrator.

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.118 "Protecting the Address Book"
- p.107 "Preventing Information Leakage Due to Unauthorized Transmission"
- p.186 "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 [Fax 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 [Administrator Tools]. 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 "Parameter Settings", see "Fax Features", Facsimile Reference.

### Stored Reception File User Setting

In [Fax Features], you can specify which users can manage fax files stored on the hard disk by setting [Stored Recept.File User Set] to [Set], under [Reception Settings]. To access the machine over the network, specified users must enter their user codes or login user names and passwords. Only authorized users can manage fax files stored on the hard disk. For details about "Reception Settings", see "Fax 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 [Fax Features], go to [Administrator Tools], [Parameter Setting] "Switch 03, Bit 7", and change the setting for automatically printing the Journal.
- In [Fax Features], go to [Administrator Tools], [Parameter Setting] "Switch 21, Bit 4", and set "Journal Notification by E-mail" to ON.

### Specifying Automatic Deletion of Incoming Faxes when an Error Occurs

This can be specified by the machine administrator.

In [Fax Features], you can configure the machine to automatically delete incoming faxes by setting Bit 07 of Switch 10 in [Parameter Setting] under [Administrator Tools]. If you make this setting, the machine will delete every incoming fax when an error occurs, even if you have configured the machine to only store incoming faxes. Errors can be caused by corruption of the hard disk, memory overload, or lack of storage for incoming faxes. Each deletion is recorded and will appear on the incoming fax deletion report. By preventing incoming faxes printing out unexpectedly, this function makes fax reception more secure.

---

## 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".

### 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 the Web Image Monitor. For instructions on how to configure this function, see "Before Sending Scan Files Using WSD", Scanner Reference.

# 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 setting.

- Service Mode Lock

## Settings

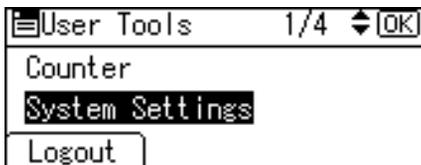
### Service Mode Lock

This can be specified by the machine administrator. Service mode is used by a service representative for inspection or repair. If you set 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.

### Specifying Service Mode Lock

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/Counter] key.
2. Select [System Settings] using [▲] or [▼], and then press the [OK] key.



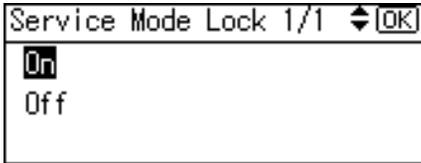
3. Select [Administrator Tools] using [▲] or [▼], and then press the [OK] key.



4. Select [Service Mode Lock] using [▲] or [▼], and then press the [OK] key.

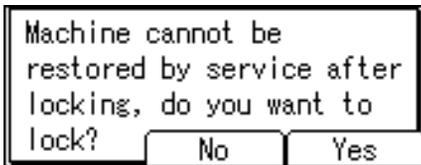


5. Select [On] using [▲] or [▼], and then press the [OK] key.



A confirmation message appears.

6. Press [Yes].



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

#### Reference

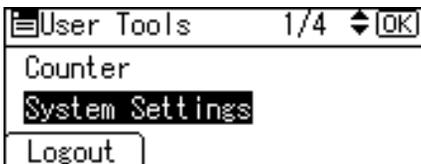
- p.32 "Logging on Using Administrator Authentication"
- p.33 "Logging off Using Administrator Authentication"

## 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.

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/Counter] key.
2. Select [System Settings] using [▲] or [▼], and then press the [OK] key.



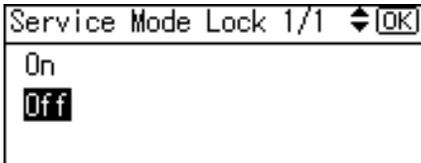
3. Select [Administrator Tools] using [▲] or [▼], and then press the [OK] key.



4. Select [Service Mode Lock] using [▲] or [▼], and then press the [OK] key.



5. Select [Off] using [▲] or [▼], and then press the [OK] key.



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

The service representative can switch to service mode.

#### **Reference**

- p.32 "Logging on Using Administrator Authentication"
- p.33 "Logging off Using Administrator Authentication"

# 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.<br>You cannot change the Web Image Monitor auto logout time.<br>See "Auto Logout".   |
| Administrator Tools | User Auth. Management                        | Select [Basic Auth.], and then set "Printer Job Authentication" to [Entire].<br>See "Basic Authentication".   |
| Administrator Tools | Admin. Auth. Management / User Management    | Select [On], and then select [Administrator Tools] for "Items".<br>See "Enabling Administrator Authentication".   |
| Administrator Tools | Admin. Auth. Management / Machine Management | Select [On], and then select [General Features], [Tray Paper Settings], [Timer Settings], [Interface Settings], [File Transfer], and [Administrator Tools] for "Items".<br>See "Enabling Administrator Authentication". |
| Administrator Tools | Admin. Auth. Management / Network Management | Select [On], and then select [Interface Settings], [File Transfer], and [Administrator Tools] for "Items".<br>See "Enabling Administrator Authentication".  |
| Administrator Tools | Admin. Auth. Management / File Management    | Select [On], and then select [Administrator Tools] for "Items".<br>See "Enabling Administrator Authentication".   |

| Tab                 | Item  | Setting  |
|---------------------|---|--|
| Administrator Tools | Extended Security/Settings by SNMPv1 and v2 | [Prohibit]<br>See "Specifying the Extended Security Functions".  |
| Administrator Tools | Extended Security / Simple Encryption       | [Do not Restrict]<br>See "Specifying the Extended Security Functions".   |
| Administrator Tools | Extended Security/ Authenticate Current Job | [Access Privilege]<br>See "Specifying the Extended Security Functions".  |
| Administrator Tools | Extended Security/ Password Policy          | "Complexity Setting": [Level 1] or higher,<br>"Minimum Character No.": 6 or higher<br>See "Specifying the Extended Security Functions".  |
| Administrator Tools | Network Security Level                      | [Level 2]<br>To acquire the machine status through printer driver or Web Image Monitor, set "SNMP" to Active on Web Image Monitor.<br>See "Specifying Network Security Level". |
| Administrator Tools | Service Mode Lock                           | [On]<br>See "Limiting Machine Operations to Customers Only".   |
| Administrator Tools | Machine Data Encryption                     | Select [Encrypt], and then select [All Data] for "Carry over to HD All Data, File Sys only or Format all."<br>See "Encrypting Data on the Hard Disk".                          |

## Fax Features

| Tab                | Item                       | Setting  |
|--------------------|----------------------------|--|
| Reception Settings | Stored Recpt.File User Set | Select [Set], and then specify the recipient user or group.<br>See "Other Security Functions". |

| Tab                 | Item         | Setting                          |
|---------------------|--------------|----------------------------------|
| Administrator Tools | Menu Protect | [Level 2]<br>See "Menu Protect". |

**Note**

- For details about SNMP setting, see Web Image Monitor Help.

**Reference**

- p.95 "Auto Logout"
- p.48 "Basic Authentication"
- p.25 "Enabling Administrator Authentication"
- p.217 "Specifying the Extended Security Functions"
- p.172 "Specifying Network Security Level"
- p.225 "Limiting Machine Operations to Customers Only"
- p.124 "Encrypting Data on the Hard Disk"
- p.223 "Other Security Functions"
- p.143 "Menu Protect"

## 8 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/<br>Logs        | Collect Job Logs                     | Active  |
| Device Settings/<br>Logs        | Collect Access Logs                  | Active  |
| Security/User<br>Lockout Policy | Lockout                              | Active  |
| Security/User<br>Lockout Policy | Number of Attempts before<br>Lockout | 5 times or less.<br>See "User Lockout Function".  |
| Security/User<br>Lockout Policy | Lockout Release Timer                | Set to Active or Inactive. When setting to Active, set the Lockout release timer to 60 minutes or more.<br>See "User Lockout Function". |

| Category                     | Item              | Setting   |
|------------------------------|-------------------|---|
| 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.<br>See "User Lockout Function".  |
| Network/SNMPv3               | SNMPv3 Function   | Inactive<br>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<br>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.93 "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 | Network / IPsec      | [Active]          |
| Interface Settings | Permit SSL/TLS Comm. | [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 | Network / IPsec      | [Inactive]        |
| Interface Settings | Permit SSL/TLS Comm. | [Ciphertext Only] |

**Web Image Monitor settings**

| Category            | Item             | Setting  |
|---------------------|------------------|--|
| Security            | S/MIME           | "Encryption Algorithm": 3DES-168 bit<br>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 or e-mail address. Do not specify destinations by IP-Fax destination. For details about specifying fax destinations, 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 Guide.

For details about IPP settings, see "Installing the Printer Driver", Printer Reference.

For details about SSL settings, see "Protection Using Encryption".

- 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.

### Reference

- p.181 "Protection Using Encryption"



# 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 privileges to use this function." | The authority to use the function is not specified. | <ul style="list-style-type: none"><li>• 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.</li><li>• 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.</li></ul> |

| 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 failed." | The entered login user name or login password is incorrect.   | Ask the user administrator for the correct login user name and login password.  |
| "Authentication 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.  |
| "Authentication 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.   |

| Messages   | Cause   | Solutions  |
|--|---|--|
| "Set User Management in Admin. Auth. to On to use this setting." | 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.<br><br>For details about authentication settings, see "Configuring User Authentication". |

### Reference

- p.39 "Configuring User Authentication"

## If the Machine Cannot Be Operated

If the following conditions arise while users are operating the machine, provide the instructions on how to deal with them.

| Condition  | Cause  | Solution  |
|--|--|---|
| Cannot perform the following: <ul style="list-style-type: none"> <li>• Print with the printer driver</li> <li>• Connect with the TWAIN driver</li> </ul> Send or print with the LAN-Fax driver | User authentication has been rejected.   | Confirm the user name and login name with the administrator of the network in use if using Windows Authentication, LDAP Authentication, or Integration Server Authentication.<br><br>Confirm with the user administrator if using basic authentication. |
| Cannot perform the following: <ul style="list-style-type: none"> <li>• Print with the printer driver</li> <li>• Connect with the TWAIN driver</li> </ul> Send or print with the LAN-Fax driver | The encryption key specified in the driver does not match the machine's driver encryption key. | Specify the driver encryption key registered in the machine.<br><br>See "Specifying a Driver Encryption Key".   |

| Condition  | Cause   | Solution  |
|--|---|---|
| <p>Cannot perform the following:</p> <ul style="list-style-type: none"> <li>• Print with the printer driver</li> <li>• Connect with the TWAIN driver</li> </ul> <p>Send or print with the LAN-Fax driver</p>             | The SNMPv3 account, password, and encryption algorithm do not match settings specified on this machine.   | Specify the account, password and the encryption algorithm of SNMPv3 registered in the machine using network connection tools.  |
| Cannot authenticate using the TWAIN driver.  | Another user is logging on to the machine.  | Wait for the user to log off.   |
| Cannot authenticate using the TWAIN driver.  | Authentication is taking time because of operating conditions.  | <p>Make sure the LDAP server setting is correct.</p> <p>Make sure the network settings are correct.</p>   |
| Cannot authenticate using the TWAIN driver.  | Authentication is not possible while the machine is editing the Address Book data.  | Wait until editing of the Address Book data is complete.  |
| After starting "User Management Tool" or "Address Management Tool" in SmartDeviceMonitor for Admin and entering the correct login user name and password, a message that an incorrect password has been entered appears. | "Simple Encryption" is not set correctly. Alternatively, "SSL/TLS" has been enabled although the required certificate is not installed in the computer. | <p>Set "Simple Encryption" to [On]. Alternatively, enable "SSL/TLS", install the server certificate in the machine, and then install the certificate in the computer.</p> <p>See "Setting the SSL / TLS Encryption Mode".</p> |
| Cannot access the machine using ScanRouter EX Professional V3 / ScanRouter EX Enterprise V2.   | "Simple Encryption" is not set correctly. Alternatively, "SSL/TLS" has been enabled although the required certificate is not installed in the computer. | <p>Set "Simple Encryption" to [On]. Alternatively, enable "SSL/TLS", install the server certificate in the machine, and then install the certificate in the computer.</p> <p>See "Setting the SSL / TLS Encryption Mode".</p> |
| 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.   |

| Condition   | Cause  | Solution  |
|---|--|---|
| 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 the [#] key, remove the original, and then log off.  |
| "Program" does not appear on the fax or scanner screen for specifying destinations.         | <p>"Rstrct Dest. Add.(Fax)" is set to [Off] in "Restrict Dest. Use(Fax)" under "Extended Security", so only the user administrator can register destinations in the Address Book on the fax screen.</p> <p>"Rstrct Dest. Add.(Scanner)" is set to [Off] in "Restrict Dest. Use (Scanner)" under "Extended Security", so only the user administrator can register destinations in the Address Book on the scanner screen.</p> | Registration must be done by the user administrator.  |
| 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.   | <p>Re-enable user authentication, and then enable [All Users] for the destinations that did not appear.</p> <p>For details about enabling [All Users], see "Protecting the Address Book".</p> |
| Cannot print when user authentication has been specified.                                   | User authentication may not be specified in the printer driver.  | <p>Specify user authentication in the printer driver.</p> <p>For details, see the printer driver Help.</p>  |

| Condition  | Cause  | Solution  |
|--|--|---|
| 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.<br>The file may be corrupt.   | Contact your service representative.  |

**Reference**

- p.176 "Specifying a Driver Encryption Key"
- p.186 "Setting the SSL/TLS Encryption Mode"
- p.118 "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.

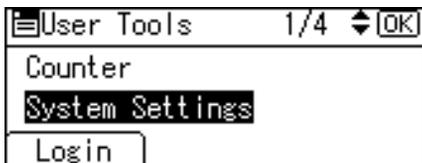
---

## 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/Counter] key.
2. Press [Login].



3. Enter a login user name, and then press the [OK] key.

|  |            |
|--|------------|
| Login: <span style="float: right;">[OK]</span> |            |
| Enter a login user name.                       |            |
| abc  | supervisor |
|  |            |

When you assign the administrator for the first time, enter "supervisor".

4. Enter a login password, and then press the [OK] key.

|  |  |
|--|--|
| Login: <span style="float: right;">[OK]</span> |  |
| Enter login password.                          |  |
| abc  |  |
|  |  |

When you assign the administrator for the first time, press the [OK] key without entering login password.

## 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 [Logout].

|                 |     |      |
|-----------------|-----|------|
| User Tools      | 1/4 | [OK] |
| Counter         |     |      |
| System Settings |     |      |
| Logout          |     |      |

2. Press [Yes].

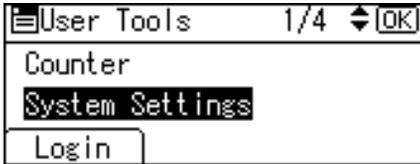
|   |     |
|---|-----|
| Are you sure<br>you want to<br>log out? |     |
| No                                      | Yes |

## 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 [Admin. Auth. Management]. For details, see "Specifying Administrator Privileges".

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



3. Log on as the supervisor.  
You can log on in the same way as an administrator.

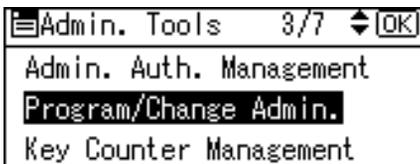
4. Select [System Settings] using [▲] or [▼], and then press the [OK] key.



5. Select [Administrator Tools] using [▲] or [▼], and then press the [OK] key.



6. Select [Program/Change Admin.] using [▲] or [▼], and then press the [OK] key.



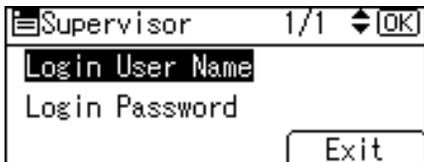
7. Select [Admin. Detailed Settings] using [▲] or [▼], and then press the [OK] key.



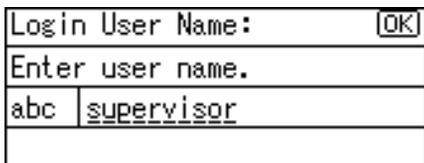
8. Select [Supervisor] using [▲] or [▼], and then press the [OK] key.



9. Select [Login User Name] using [▲] or [▼], and then press the [OK] key.



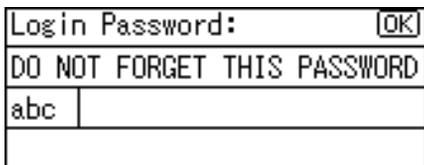
10. Enter the login user name, and then press the [OK] key.



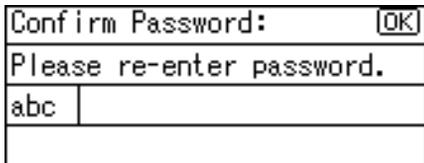
11. Select [Login Password] using [▲] or [▼], and then press the [OK] key.



12. Enter the login password, and then press the [OK] key.



13. If a password reentry screen appears, enter the login password, and then press the [OK] key.



14. Press [Exit] three times.



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

## Reference

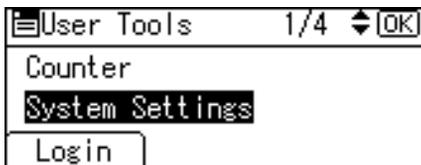
- p.25 "Specifying Administrator Privileges"

## 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".

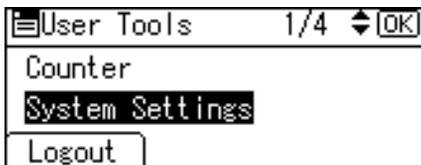
1. Press the [User Tools/Counter] key.
2. Press [Login].



3. Log on as the supervisor.

You can log on in the same way as an administrator.

4. Select [System Settings] using [▲] or [▼], and then press the [OK] key.



5. Select [Administrator Tools] using [▲] or [▼], and then press the [OK] key.



6. Select [Program/Change Admin.] using [▲] or [▼], and then press the [OK] key.



7. Select [Admin. Detailed Settings] using [▲] or [▼], and then press the [OK] key.

|                          |      |
|--------------------------|------|
| Prog/Chge Admin 1/1      | OK   |
| Admin. Detailed Settings |      |
| Permissions              |      |
|                          | Exit |

8. Select the administrator you wish to reset using [▲] or [▼], and then press the [OK] key.

|                     |      |
|---------------------|------|
| Admin. Settings 1/3 | OK   |
| Administrator1      |      |
| Administrator2      |      |
|                     | Exit |

9. Select [Login Password] using [▲] or [▼], and then press the [OK] key.

|                    |      |
|--------------------|------|
| Administrator1 1/2 | OK   |
| Login User Name    |      |
| Login Password     |      |
|                    | Exit |

10. Enter the login password, and then press the [OK] key.

|                 |    |
|-----------------|----|
| Login Password: | OK |
| Enter password. |    |
| abc             |    |
|                 |    |

11. If a password reentry screen appears, enter the login password, and then press the [OK] key.

|                           |    |
|---------------------------|----|
| Confirm Password:         | OK |
| Please re-enter password. |    |
| abc                       | _  |
|                           |    |

12. Press [Exit] three times.

|                    |      |
|--------------------|------|
| Administrator1 1/2 | OK   |
| Login User Name    |      |
| Login Password     |      |
|                    | Exit |

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

 **Reference**

- p.241 "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
- SMTP Authentication

User Name

E-mail Address

Password

Encrypt

- POP before SMTP

Wait Time after Auth.

User Name

E-mail Address

Password

- Reception Protocol
- POP3 / IMAP4 Settings

Server Name

Encryption

- Admin.E- mail Address
- Default User Name/PW(Send)
  - SMB User Name / SMB Password
  - FTP User Name / FTP Password
  - NCP User Name / NCP Password
- Fax E-mail Account

### Administrator Tools

The following settings can be specified.

- Address Book Management
- Prgrm./Change/Delete Group
- Display / Print Counter
  - Print
- Disp./Print User Counter
- User Auth. Management
  - You can specify which authentication to use.
  - You can also edit the settings for each function.
- Admin. Auth. Management
  - Machine Management
- Program/Change Admin.
  - Machine Administrator
  - You can change the user name and the full-control user's authority.
- Key Counter Management
- Extended Security
  - Encrypt Address Book
  - Restrict User Info.Display
  - Transfer to Fax Receiver
  - Authenticate Current Job
  - @Remote Service
  - Update Firmware
  - Change Firmware Structure
- Prog/Chnge/Del LDAP Server
- LDAP Search
- Prog./Change/Delete Realm

- AOF (Always On)
- Service Mode Lock
- Firmware Version
- Auto Erase Memory Setting
- Erase All Memory
- Delete All Logs
- Transfer Log Setting
- Fixed USB Port
- Machine Data Encryption

**Note**

- "Machine Data Encryption" are available only if the optional HDD Encryption Unit is installed.
- "Auto Erase Memory Setting" and the "Erase All Memory" setting are available only if the optional Data Overwrite Security Unit is installed.

---

## Copier Features

---

All the settings can be specified.

---

## Fax Features

---

The following settings can be specified.

### General Settings/Adjust

All the settings can be specified.

### Reception Settings

The following settings can be specified.

- Switch Reception Mode
- RX Mode Auto Switch Time
- Authorized Reception
- Checkered Mark
- Center Mark
- Print Reception Time
- 2 Sided Print
- Reception File Setting

## E-mail Settings

The following settings can be specified.

- Internet Fax Setting
- SMTP RX File Delivery

## Administrator Tools

The following settings can be specified.

- Print Journal
- Print TX Standby File List
- Communication Page Count
- Forwarding
- Folder TX Result Report
- Parameter Setting
- Program Special Sender
- Program Memory Lock ID
- G3 Analog Line
- Memory File Transfer
- Menu Protect

---

## 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

### System

The following settings can be specified.

- Print Error Report
- Auto Continue
- Memory Overflow
- Rotate by 180 Degrees
- Print Compressed Data

- Memory Usage
- Duplex
- Copies
- Blank Page Print
- Edge Smoothing
- Toner Saving
- Printer Language
- Sub Paper Size
- Page Size
- Letterhead Setting
- Bypass Tray Setting Priority
- Edge to Edge Print
- Default Printer Lang.
- Tray Switching
- RAM Disk
- 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.

#### **Note**

- PS or PDF menu settings are available only if the optional PostScript 3 Unit is installed.

---

## **Scanner Features**

---

The following settings can be specified.

### **Scan Settings**

All the settings can be specified.

**Destination List Settings**

All the settings can be specified.

**Send Settings**

The following settings can be specified.

- PC Scan Command Stdby Time
- File Type Priority
- Compression (B&W)
- Compress. (Gray/FullClr)
- Print&Del. Scanner Journal
- Print Scanner Journal
- Delete Scanner Journal
- Insert Addit. E-mail Info
- Default E-mail Subject

**Administrator Tools**

All the settings can be specified.

---

**Settings via Web Image Monitor**


---

The following settings can be specified.

**Status**

- 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
  - Paper Tray Priority
- 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.
- 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**

- Basic Settings  
Print Error Report

Auto Continue  
Memory Overflow  
Rotate by 180 Degrees  
Print Compressed Data  
Memory Usage  
Duplex  
Copies  
Blank Page Print  
Edge Smoothing  
Toner Saving  
Printer Language  
Sub Paper Size  
Page Size  
Letterhead Setting  
Bypass Tray Setting Priority  
Edge to Edge Print  
Default Printer Language  
Tray Switching  
List/Test Print Lock  
Extended Auto Tray Switching  
Virtual Printer  
Host Interface  
PCL Menu  
PS Menu  
PDF Menu

- 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.
- PDF Group Password  
All the settings can be specified.

- PDF Fixed Password  
All the settings can be specified.

### **Fax**

- General Settings  
All the settings can be specified.
- Administrator Tools  
All the settings can be specified.
- E-mail Settings  
Internet Fax  
SMTP RX File Delivery  
Settings Authorized E-mail Address
- Parameter Settings  
All the settings can be specified.

### **Scanner**

- Scan Settings  
All the settings can be specified.
- Destination List Settings  
All the settings can be specified.
- Send Settings  
All the settings can be specified.
- Administrator Tools  
All the settings can be specified.

### **Interface**

- Interface Settings  
USB

### **Network**

- SNMPv3

### **Security**

- User Lockout Policy  
All the settings can be specified.

### **RC Gate**

- Setup RC Gate  
Request No.

- Update RC Gate Firmware  
All the settings can be specified.
- RC Gate Proxy Server  
All the settings can be specified.

### Webpage

- Webpage  
Download Help File

### Extended Feature Settings

- Install  
All the settings can be specified.
- Administrator Tools  
All the settings can be specified.
- Copy Extended Features  
All the settings can be specified.

#### Note

- The following settings are available only if the optional PostScript 3 Unit is installed: "PS Menu", "PDF Menu", "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 Current Job
- Reset All Jobs
- Reset Device
- Refresh

### User Management Tool

The following settings can be specified.

- User Counter Information
- Access Control List

# 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.

- Network  
All the settings can be specified.
- Wireless LAN  
Communication Mode  
SSID Setting  
Channel  
Security Method  
Restore Defaults
- Print I/F Settings List

### File Transfer

- SMTP Server  
Server Name  
Port No.
- E-mail Communication Port
- E-mail Recept. Interval
- Max. Recept. E-mail Size
- E-mail Storage in Server
- Auto Specify Sender Name

### Administrator Tools

- Address Book Management
- Prgrm./Change/Delete Group
- Disp./Print User Counter  
Display
- Admin. Auth. Management  
Network Management

- Program/Change Admin.  
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  
Simple Encryption
- Network Security Level

**Note**

- The "Wireless LAN" setting is available only if the wireless LAN interface is installed.

---

## Fax Features

---

The following settings can be specified.

### E-mail Settings

- Maximum E- mail Size

### IP-Fax Settings

All the settings can be specified.

---

## 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
  - All the settings can be specified.
- Auto E-mail Notification
  - 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

- Basic Settings
  - Print Compressed Data

### Fax

- E-mail Settings
  - Maximum 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

- Interface Settings
  - LAN Type
  - Ethernet Security
  - Ethernet Speed
- Wireless LAN Settings
  - LAN Type
  - Communication Mode
  - SSID
  - Channel
  - Security Method
    - WEP Settings
    - WPA Settings

## 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.

---

## 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
- Prgrm./Change/Delete Group
- Disp./Print User Counter  
Display
- Admin.Auth.Management  
File Management
- Program/Change Admin.  
File Administrator
- Extended Security  
Enhance File Protection

---

## Fax Features

---

The following settings can be specified.

### Reception Settings

- Stored Recept.File User Set

---

## Printer Features

---

The following settings can be specified.

### Maintenance

- Delete All Temporary Jobs
- Delete All Stored Jobs

### System

- Auto Delete Temporary Jobs
- Auto Delete Stored Jobs

---

## Settings via Web Image Monitor

---

The following 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

- Basic Settings  
Auto Delete Temporary Print Jobs  
Auto Delete Stored Print Jobs

### 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
- Prgrm. / Change / Delete Group
- Address Book: Print List
- Display/Print Counter
- Disp./Print User Counter
  - Display
  - Clear
- Admin.Auth. Management
  - User Management
- Program / Change Admin.
  - User Administrator
- Extended Security
  - Encrypt Address Book
  - Rstrict Dest. Use(Fax)
  - Rstrct Dest. Add.(Fax)
  - Rstrct Dest. Use(Scanner)
  - Rstrct Dest. Add.(Scanner)
  - 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

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**

- 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**

- Reset User Counters
- Add New User
- Delete User
- User Properties

# 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.

| Settings | Read-only (User) | Edit (User) | Edit / Delete (User) | Full Control | Registered User | User Admin. |
|----------|------------------|-------------|----------------------|--------------|-----------------|-------------|
| Name     | R                | R/W         | R/W                  | R/W          | R/W             | R/W         |
| Reg.No.  | 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               |
| Login User Name     | N/A              | N/A         | N/A                  | N/A          | R/W               | R/W               |
| Login Password      | N/A              | N/A         | N/A                  | N/A          | R/W* <sup>1</sup> | R/W* <sup>1</sup> |
| SMTP Authentication | N/A              | N/A         | N/A                  | N/A          | R/W* <sup>1</sup> | R/W* <sup>1</sup> |

| Settings              | Read-only (User) | Edit (User) | Edit / Delete (User) | Full Control | Registered User   | User Admin.       |
|-----------------------|------------------|-------------|----------------------|--------------|-------------------|-------------------|
| Folder Authentication | R                | R/W         | R/W                  | R/W          | R/W               | R/W               |
| LDAP Authentication   | N/A              | N/A         | N/A                  | N/A          | R/W* <sup>1</sup> | R/W* <sup>1</sup> |
| Function Permissions  | 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: Auth.Protect**

| Settings                 | Read-only (User) | Edit (User) | Edit / Delete (User) | Full Control      | Registered User   | User Admin.       |
|--------------------------|------------------|-------------|----------------------|-------------------|-------------------|-------------------|
| Register as              | R                | R/W         | R/W                  | R/W               | R/W               | R/W               |
| Dest.Protect Code        | N/A              | N/A         | N/A                  | R/W* <sup>2</sup> | R/W* <sup>2</sup> | R/W* <sup>2</sup> |
| Dest.Protect Obj.        | N/A              | R/W         | R/W                  | R/W               | R/W               | R/W               |
| Dest.Protect:Permissions | 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 Settings**

| Settings              | Read-only (User) | Edit (User) | Edit / Delete (User) | Full Control | Registered User | User Admin. |
|-----------------------|------------------|-------------|----------------------|--------------|-----------------|-------------|
| Fax Dest.             | R                | R/W         | R/W                  | R/W          | R/W             | R/W         |
| SUB Code              | R                | R/W         | R/W                  | R/W          | R/W             | R/W         |
| SEP Code              | R                | R/W         | R/W                  | R/W          | R/W             | R/W         |
| International TX Mode | N/A              | R/W         | R/W                  | R/W          | R/W             | R/W         |
| Label Insertion       | N/A              | R/W         | R/W                  | R/W          | R/W             | R/W         |

**Tab Name: E-mail Settings**

| 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         |
| E-mail/Internet Fax Dest. | N/A              | R/W         | R/W                  | R/W          | R/W             | R/W         |
| Internet Fax Dest. only   | N/A              | R/W         | R/W                  | R/W          | R/W             | R/W         |

**Tab Name: Folder Info**

| 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: Port No.              | 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         |
| NCP: Path (NDS or Bindery) | 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 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 Tray Switching    | R       | R       |
| Original Type Setting  | R/W     | R       |
| Duplex Mode Priority   | R       | R       |
| Orientation            | R/W     | R       |
| Max. Number of Sets    | R       | R       |
| Original Count Display | R       | R       |
| Reproduction Ratio     | R       | R       |
| Preset R/E Priority    | R       | R       |
| Duplex Margin          | R/W     | R       |
| Letterhead Setting     | R       | R       |
| Menu Protect           | 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.

## 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.

### Normal Printer Screen

| Functions | Level 1 | Level 2 |
|-----------|---------|---------|
| Prt.Jobs  | R/W     | R/W     |

### List / Test Print

| Settings              | Level 1 | Level 2 |
|-----------------------|---------|---------|
| Multiple Lists        | R/W     | R/W     |
| Config. Page          | R/W     | R/W     |
| Error Log             | R/W     | R/W     |
| Menu List             | R/W     | R/W     |
| PCL Config./Font Page | R/W     | R/W     |
| PS Config./Font Page  | R/W     | R/W     |
| PDF Config./Font Page | R/W     | R/W     |
| Hex Dump              | R/W     | R/W     |

The "PS Config./Font Page" and the "PDF Config./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       |

| Settings                   | Level 1 | Level 2 |
|----------------------------|---------|---------|
| Auto Continue              | R       | R       |
| Memory Overflow            | R       | R       |
| Rotate by 180 Degrees      | R       | R       |
| Auto Delete Temporary Jobs | R       | R       |
| Auto Delete Stored Jobs    | 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       |
| Printer Language           | R       | R       |
| Sub Paper Size             | R       | R       |
| Page Size                  | R/W     | R       |
| Letterhead Setting         | R       | R       |
| Bypass Tray Priority       | R       | R       |
| Edge to Edge Print         | R       | R       |
| Default Printer Lang.      | R       | R       |
| Tray Switching             | R       | R       |
| RAM Disk                   | R       | R       |
| Extend 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       |
| RAM Disk        | 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       |
| Reverse Order Print     | R       | R       |
| Resolution              | R       | R       |
| Orientation Auto Detect | R       | R       |

PDF menu 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 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.

### Scan Settings

| Settings                   | Level 1 | Level 2 |
|----------------------------|---------|---------|
| Default Scan Settings      | R       | R       |
| Original Setting           | R       | R       |
| Orig. Orientation Priority | R       | R       |
| Original Type Setting      | R/W     | R       |
| Color Mode Priority        | R       | R       |
| Blank Page Detect          | R       | R       |

### Destination List Settings

| Settings              | Level 1 | Level 2 |
|-----------------------|---------|---------|
| Dest. List Priority 2 | R       | R       |

### Send Settings

| Settings                    | Level 1 | Level 2 |
|-----------------------------|---------|---------|
| PC Scan Command Stdbby Time | R       | R       |
| File Type Priority          | R       | R       |
| Compression (B&W)           | R/W     | R       |
| Compress. (Gray/Full Clr)   | R/W     | R       |

| Settings                   | Level 1 | Level 2 |
|----------------------------|---------|---------|
| Print&Del. Scanner Journal | R       | R       |
| Print Scanner Journal      | R       | R       |
| Delete Scanner Journal     | R       | R       |
| Max. E-mail Size           | R       | R       |
| Divide & Send E-mail       | R       | R       |
| Insert Addit. E-mail Info  | R/W     | R       |
| Default E-mail Subject     | R       | R       |

### Administrator Tools

| Settings     | Level 1 | Level 2 |
|--------------|---------|---------|
| Menu Protect | 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 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/Adjust

| Settings                | Level 1 | Level 2 |
|-------------------------|---------|---------|
| Adjust Sound Volume     | R/W     | R       |
| Program Fax Information | R       | R       |
| On Hook Release Time    | R/W     | R       |
| Set User Function Key   | R/W     | R       |

### Reception Settings

| Settings                    | Level 1 | Level 2 |
|-----------------------------|---------|---------|
| Switch Reception Mode       | R       | R       |
| RX Mode Auto Switch Time    | R       | R       |
| Authorized Reception        | R       | R       |
| Checked Mark                | R/W     | R       |
| Center Mark                 | R/W     | R       |
| Print Reception Time        | R/W     | R       |
| 2 Sided Print               | R/W     | R       |
| Reception File Setting      | R       | R       |
| Stored Recpt. File User Set | R       | R       |

**E-mail Settings**

| Settings              | Level 1 | Level 2 |
|-----------------------|---------|---------|
| Internet Fax Settings | R       | R       |
| Maximum E-mail Size   | R       | R       |
| SMTP RX File Delivery | R       | R       |

**IP-Fax Settings**

| Settings         | Level 1 | Level 2 |
|------------------|---------|---------|
| Enable H.323     | R       | R       |
| Enable SIP       | R       | R       |
| H.323 Settings   | R       | R       |
| SIP Settings     | R       | R       |
| Gateway Settings | R       | R       |

**Administrator Tools**

| Settings                   | Level 1 | Level 2 |
|----------------------------|---------|---------|
| Print Journal              | R       | N/A     |
| Print TX Standby File List | R       | R       |
| Communication Page Count   | R       | R       |
| Memory Lock                | R       | R       |
| Forwarding                 | R       | R       |
| Folder TX Result Report    | R       | R       |
| Parameter Settings         | R       | R       |
| Program Special Sender     | R       | R       |
| Program Memory Lock ID     | R       | R       |
| G3 Analog line             | R       | R       |
| Memory File Transfer       | R       | R       |

| Settings     | Level 1 | Level 2 |
|--------------|---------|---------|
| Menu Protect | 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.

# System Settings

When administrator authentication is enabled, the administrator's configuration of Available Settings determines which system settings are available to users.

User privileges are as follows:

- Abbreviations in the table heads  
Not Specified = Authorized user when "Items" have not been specified.  
Specified = Authorized user when "Items" 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         |
| Display Contrast                    | R/W           | R         |
| Key Repeat                          | R/W           | R         |
| Measurement Unit                    | R/W           | R         |

10

## Tray Paper Settings

| Settings           | Not Specified | Specified |
|--------------------|---------------|-----------|
| Paper Size:Tray1-3 | R/W           | R         |

| Settings                  | Not Specified | Specified |
|---------------------------|---------------|-----------|
| Printer Bypass Paper Size | R/W           | R         |
| Paper Type: Bypass Tray   | R/W           | R         |
| Paper Type: Tray 1-3      | R/W           | R         |
| Ppr Tray Priority:Copier  | R/W           | R         |
| Ppr Tray Priority:Fax     | R/W           | R         |
| Ppr Tray Priority:Printer | R/W           | R         |

### Timer Settings

| Settings                   | Not Specified | Specified |
|----------------------------|---------------|-----------|
| Auto Off Timer             | R/W           | R         |
| Energy Saver Timer         | R/W           | R         |
| System Auto Reset Timer    | R/W           | R         |
| Copier 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         |

### Interface Settings

| Settings                | Not Specified | Specified |
|-------------------------|---------------|-----------|
| Print I/F Settings List | R/W           | R         |

### 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 Settings    | 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           | N/A       |
| SMB Work Group             | R/W           | N/A       |
| Ethernet Speed             | R/W           | R         |
| IEEE802.1X Auth.(Ethernet) | R/W           | R         |
| Restr.IEEE802.1X Auth.Def. | R/W           | R         |
| Ping Command               | R/W           | R         |
| Permit SNMPv3 Communictn.  | R/W           | R         |
| Permit SSL / TLS Comm.     | R/W           | R         |
| Host Name                  | R/W           | N/A       |
| Machine Name               | R/W           | N/A       |

If you set "Machine IPv4 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 Comm. Speed    | R/W           | R         |
| Selection Signal Status | R/W           | R         |
| Input Prime             | R/W           | R         |
| Bidirectional Comm.     | 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 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         |
| SMTP Server         | R/W           | R         |
| SMTP Authentication | R/W           | R         |
| POP before SMTP     | R/W           | R         |

| Settings                      | Not Specified | Specified |
|-------------------------------|---------------|-----------|
| Reception Protocol            | R/W           | R         |
| POP3 / IMAP4 Settings         | R/W           | R         |
| Admin. E-mail Address         | R/W           | N/A       |
| E-mail Communication Port     | R/W           | R         |
| E-mail Recept. Interval       | R/W           | R         |
| Max. Recept. E-mail Size      | R/W           | R         |
| E-mail Storage in Server      | R/W           | R         |
| Default User Name / PW (Send) | R/W           | R         |
| Auto Specify Sender name      | R/W           | R         |
| Fax E-mail Account            | R/W           | R         |
| Scanner Resend Time           | R/W           | R         |
| Scanner Resend                | R/W           | R         |

The settings made for "Main Delivery Server IP Address" and "Sub Delivery Server IP Address" in "Delivery Option" can only be displayed, not changed.

The passwords for "SMTP Authentication" and "Default User Name / PW (Send)" can be entered or changed but not displayed.

### Administrator Tools

| Settings                  | Not Specified | Specified |
|---------------------------|---------------|-----------|
| Address Book Management   | R/W           | R/W       |
| Prgm./Change/Delete Group | R/W           | R/W       |
| Address Book:Print List   | R/W           | R/W       |
| Display / Print Counter   | R/W           | R/W       |
| Disp./Print User Counter  | R/W           | R/W       |
| User Auth. Management     | R/W           | R         |
| Admin. Auth Management    | R/W           | R         |

| Settings                        | Not Specified | Specified |
|---------------------------------|---------------|-----------|
| Key Counter Management          | R/W           | R         |
| Extended Security               | R/W           | R         |
| Prog / Change / Del LDAP Server | R/W           | R         |
| LDAP Search                     | R/W           | R         |
| Prog./ Change / Delete Realm    | R/W           | R         |
| AOF(Always On)                  | R/W           | R         |
| Service Mode Lock               | R/W           | R         |
| Firmware Version                | R             | R         |
| Delete All Logs                 | R/W           | R         |
| Transfer log Setting            | R/W           | N/A       |
| Fixed USB Port                  | R/W           | R         |

The password for "Program / Change / Delete LDAP Server" can be entered or changed but not displayed.

## 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 "Items" has been specified.

User privileges are as follows:

- Abbreviations in the table heads

Not Specified = Authorized user when "Items" have not been specified.

Specified = Authorized user when "Items" 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         |
| Spool Printing                 | R/W           | N/A       |
| Paper Tray Priority : Copier   | R/W           | R         |
| Paper Tray Priority : Fax      | R/W           | R         |
| Paper Tray Priority : Printer  | R/W           | R         |

### Paper

| Settings                        | Not Specified | Specified |
|---------------------------------|---------------|-----------|
| Tray1 : Paper Size              | R/W           | R         |
| Tray1 : Paper Type              | R/W           | R         |
| Tray1 : Apply Auto Paper Select | R/W           | R         |

| Settings                        | Not Specified | Specified |
|---------------------------------|---------------|-----------|
| Tray1 : Apply Duplex            | R/W           | R         |
| Tray2 : Paper Size              | R/W           | R         |
| Tray2 : Paper Type              | R/W           | R         |
| Tray2 : Apply Auto Paper Select | R/W           | R         |
| Tray2 : Apply Duplex            | R/W           | R         |
| Tray3 : Paper Size              | R/W           | R         |
| Tray3 : Paper Type              | R/W           | R         |
| Tray3 : Apply Auto Paper Select | R/W           | R         |
| Tray3 : 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         |

### 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         |

| Settings                   | Not Specified | Specified |
|----------------------------|---------------|-----------|
| Energy Saver Timer         | R/W           | R         |
| System Auto Reset Timer    | R/W           | R         |
| Copier 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         |

### 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         |

| Settings                           | Not Specified | Specified |
|------------------------------------|---------------|-----------|
| 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       |
| 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       |

| Settings                      | Not Specified | Specified |
|-------------------------------|---------------|-----------|
| E-mail Notification User Name | R/W           | N/A       |
| E-mail Notification Password  | R/W           | N/A       |

### 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 | R/W           | R         |
| User Code Authentication - Available Function         | R/W           | R         |
| Basic Authentication - Printer Job Authentication     | R/W           | R         |
| Basic Authentication - Available Function             | R/W           | R         |
| Windows Authentication - Printer Job Authentication   | R/W           | R         |
| Windows Authentication - SSL                          | R/W           | R         |
| Windows Authentication - Kerberos Authentication      | R/W           | R         |

| Settings   | Not Specified | Specified |
|--|---------------|-----------|
| Windows Authentication - Domain Name   | R/W           | R         |
| Windows Authentication - Realm Name  | R/W           | R         |
| Windows Authentication - Group Settings for Windows Authentication                       | R/W           | R         |
| LDAP Authentication - Printer Job Authentication   | R/W           | R         |
| LDAP Authentication - LDAP Authentication  | R/W           | R         |
| LDAP Authentication - Login Name Attribute   | R/W           | R         |
| LDAP Authentication - Unique Attribute   | R/W           | R         |
| LDAP Authentication - Available Function   | R/W           | R         |
| Integration Server Authentication - Printer Job Authentication                           | R/W           | R         |
| Integration Server Authentication - SSL  | R/W           | R         |
| Integration Server Authentication - Integration Server Name                              | R/W           | R         |
| Integration Server Authentication - Authentication Type                                  | R/W           | R         |
| Integration Server Authentication - Domain Name  | R/W           | R         |
| Integration Server Authentication - Group Settings for Integration Server Authentication | R/W           | R         |

### Auto E-mail Notification

10

| Settings     | Not Specified | Specified |
|--------------|---------------|-----------|
| Address List | R/W           | R/W       |

### 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       |
| 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       |
| Printer Language             | R       | R       |
| Sub Paper Size               | R       | R       |
| Letterhead Setting           | R       | R       |
| Bypass Tray Setting Priority | R       | R       |

| Settings                     | Level 1 | Level 2 |
|------------------------------|---------|---------|
| 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       |
| 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 |
|-------------------------|---------|---------|
| Reverse Order Print     | R       | R       |
| Resolution              | R       | R       |
| Orientation Auto Detect | R       | R       |

PDF menu settings are available only if the optional PostScript 3 Unit is installed.

#### Virtual Printer Settings

##### System

| Settings              | Level 1 | Level 2 |
|-----------------------|---------|---------|
| Print Error Report    | R       | R       |
| 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       |

| Settings           | Level 1 | Level 2 |
|--------------------|---------|---------|
| Sub Paper Size     | R       | R       |
| Input Tray         | R/W     | R/W     |
| Page Size          | R/W     | R/W     |
| 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       |
| 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       |

| Settings                | Level 1 | Level 2 |
|-------------------------|---------|---------|
| 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     |

#### 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     |

| Settings                   | Level 1 | Level 2 |
|----------------------------|---------|---------|
| 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.

## Scan Settings

| Settings  | Level 1 | Level 2 |
|---|---------|---------|
| Scan Settings: Original Type (Full Color: Text)   | R/W     | R       |
| Scan Settings: Original Type (Full Color: Photo)  | R/W     | R       |
| Scan Settings: Original Type (Black&White: Text)  | R/W     | R       |
| Scan Settings: Original Type (Black&White: Photo) | R/W     | R       |
| Scan Settings: Resolution                         | R       | R       |
| Scan Settings: Scan Size                          | R       | R       |
| Scan Size   | R       | R       |
| Original Setting                                  | R       | R       |
| Original Orientation Priority                     | R       | R       |
| A.C.S. Sensitivity Level                          | R/W     | R       |
| Blank Page Detect                                 | R       | R       |

## Destination List Settings

| Settings                            | Level 1 | Level 2 |
|-------------------------------------|---------|---------|
| Destination List Display Priority 1 | R       | R       |
| Destination List Display Priority 2 | R       | R       |

## Send Settings

| Settings                            | Level 1 | Level 2 |
|-------------------------------------|---------|---------|
| PC Scan Command Standby Time        | R       | R       |
| Send File Type                      | R       | R       |
| Compression (Black & White)         | R/W     | R       |
| Compression (Gray Scale/Full Color) | R/W     | R       |
| Print & Delete Scanner Journal      | R/W     | R       |
| Max. E-mail Size                    | R       | R       |
| Divide & Send E-mail                | R       | R       |
| Insert Additional E-mail Info       | R/W     | R       |
| Default E-mail Subject              | R       | R       |

## Administrator Tools

| Settings                     | Level 1 | Level 2 |
|------------------------------|---------|---------|
| Display WSD Destination List | R       | R       |
| Prohibit WSD Scan Command    | 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 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.

## Fax General Settings

| Settings              | Level 1 | Level 2 |
|-----------------------|---------|---------|
| Fax Header            | N/A     | N/A     |
| Own Name              | N/A     | N/A     |
| Own Fax Number        | N/A     | N/A     |
| Switch Reception Mode | N/A     | N/A     |
| 2 Sided Print         | R/W     | N/A     |
| Checkered Mark        | R/W     | N/A     |
| Center Mark           | R/W     | N/A     |
| Print Reception Time  | R/W     | N/A     |
| Paper Tray            | R/W     | N/A     |

## Administrator Tools

| Settings                  | Level 1 | Level 2 |
|---------------------------|---------|---------|
| Memory Lock Reception     | N/A     | N/A     |
| Program Memory Lock ID    | N/A     | N/A     |
| Select Dial/Push Phone    | N/A     | N/A     |
| Select Extension/ Outside | N/A     | N/A     |
| Outside Access No.        | N/A     | N/A     |

### Fax E-mail Settings

| Settings                       | Level 1 | Level 2 |
|--------------------------------|---------|---------|
| Internet Fax                   | N/A     | N/A     |
| Maximum E-mail Size            | N/A     | N/A     |
| SMTP RX File Delivery Settings | 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 Address (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 1-10 | N/A     | N/A     |

| Settings             | Level 1 | Level 2 |
|----------------------|---------|---------|
| Select Protocol 1-10 | N/A     | N/A     |
| Gateway Address 1-10 | 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     |
| 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     |

#### ↓ 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.

# 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 "Items" has been specified.

User privileges are as follows:

- Abbreviations in the table heads  
Not Specified = Authorized user when "Items" have not been specified.  
Specified = Authorized user when "Items" 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         |
| USB                          | R/W           | R         |

## 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           | N/A       |
| Security Method    | R/W           | R         |
| WEP Authentication | R/W           | N/A       |
| WEP Key Number     | R/W           | R         |

| Settings                  | Not Specified | Specified |
|---------------------------|---------------|-----------|
| WEP Key                   | R/W           | R         |
| WPA Encryption Method     | R/W           | R         |
| WPA Authentication Method | R/W           | R         |
| WPA-PSK/WPA2-PSK          | R/W           | R         |
| WPA/WPA2 Settings         | 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 "Items" has been specified.

User privileges are as follows:

- Abbreviations in the table heads

Not Specified = Authorized user when "Items" have not been specified.

Specified = Authorized user when "Items" 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         |

| 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         |

## 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         |
| 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         |
| 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         |
| 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 "Items" has been specified.

User privileges are as follows:

- Abbreviations in the table heads

Not Specified = Authorized user when "Items" have not been specified.

Specified = Authorized user when "Items" 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         |
| URL 1               | R/W           | R         |
| URL 2               | 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
- PDF Direct Print function  
PostScript 3 Unit
- Hard Disk data encryption function  
HDD Encryption Unit

# Trademarks

Microsoft®, Windows®, Windows Server®, Windows Vista®, and Outlook® 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.

Netscape, and Netscape Messenger are either registered trademarks or trademarks of Netscape Communications Corporation in the United States and/or other countries.

Lotus, and Lotus Notes are either registered trademarks or trademarks of IBM Corporation in the United States and/or other countries.

Netware, IPX, IPX/SPX are either registered trademarks or trademarks of Novell, Inc.

UPnP™ is a trademark of the UPnP™ Implementers Corporation.

PCL® is a registered trademark of Hewlett-Packard Company.

Monotype is a registered trademark of Monotype Imaging, Inc.

Apple, AppleTalk, Bonjour, Macintosh, and Mac OS are trademarks of Apple Inc., registered in the U.S. and other countries.

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.

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® 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

Microsoft® Windows Server® 2003 Web Edition

Microsoft® Windows Server® 2003 Datacenter 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

Microsoft® Windows Server® 2003 R2 Datacenter 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

# INDEX

## A

|  |            |
|--|------------|
| Access Control.....                          | 163        |
| Address Book Privileges.....                 | 267        |
| Administrator.....                           | 17         |
| Administrator Authentication.....            | 17, 23, 25 |
| Administrator Privileges.....                | 25         |
| AH Protocol.....                             | 191        |
| AH Protocol + ESP Protocol.....              | 191        |
| Authenticate Current Job.....                | 221        |
| Authentication and Access Limits.....        | 16         |
| Authentication by IEEE802.1X.....            | 215        |
| Authentication Using an External Device..... | 97         |
| authfree.....                                | 214        |
| Auto Erase Memory.....                       | 132        |
| Auto Logout.....                             | 95         |
| Available Functions.....                     | 147        |

## B

|                           |    |
|---------------------------|----|
| Basic Authentication..... | 48 |
|---------------------------|----|

## C

|  |     |
|--|-----|
| Change Firmware Structure.....   | 222 |
| Configuring Address Book Access Permissions.....                         | 118 |
| Configuring User Authentication.....                                     | 39  |
| Copier Features.....   | 271 |
| Creating the Device Certificate (Issued by a Certificate Authority)..... | 183 |

## D

|   |          |
|---|----------|
| Device Settings.....                                  | 288      |
| Disabling Log Transfer to Web SmartDeviceMonitor..... | 150      |
| Display.....  | 10       |
| Driver Encryption Key.....                            | 176, 218 |

## E

|                                       |     |
|---------------------------------------|-----|
| E-mail Encryption.....                | 110 |
| Edit.....                             | 267 |
| Edit / Delete.....                    | 267 |
| Electronic Signature.....             | 112 |
| Enabling and Disabling Protocols..... | 164 |
| Enabling the Encryption Settings..... | 124 |
| Encrypt Address Book.....             | 218 |
| Encrypting Data on the Hard Disk..... | 124 |

|   |     |
|---|-----|
| Encrypting the Data in the Address Book.....                          | 120 |
| Encryption Key Auto Exchange / Manual Settings - Shared Settings..... | 192 |
| Encryption Key Auto Exchange Security Level.....                      | 192 |
| Encryption Key Auto Exchange Setting Items.....                       | 194 |
| Encryption Key Auto Exchange Settings Configuration Flow.....         | 200 |
| Encryption Key Manual Settings Configuration Flow.....                | 205 |
| Encryption Key Manual Settings Items.....                             | 197 |
| Encryption Technology.....  | 16  |
| Enhance File Protection.....  | 219 |
| Enhanced Security.....  | 228 |
| ESP Protocol.....   | 190 |
| Extended Security Functions.....                                      | 217 |

## F

|                                  |     |
|----------------------------------|-----|
| Fax.....                         | 302 |
| Fax Features.....                | 278 |
| File Administrator.....          | 22  |
| File Administrator Settings..... | 263 |
| Full Control.....                | 267 |

## I

|  |     |
|--|-----|
| If User Authentication is Specified.....                                   | 90  |
| Installing the Device Certificate (Issued by a Certificate Authority)..... | 184 |
| Integration Server Authentication.....                                     | 78  |
| Interface.....   | 305 |
| IP Address.....  | 11  |
| IPsec.....   | 190 |
| IPsec Settings.....  | 192 |
| IPsec telnet Setting Commands.....   | 206 |

## L

|   |    |
|---|----|
| Laws and Regulations.....   | 12 |
| LDAP Authentication.....  | 70 |
| LDAP Authentication - Operational Requirements for LDAP Authentication..... | 70 |
| Locked Print.....   | 99 |
| Log off (Administrator).....  | 33 |
| Log on (Administrator).....   | 32 |
| Login.....  | 17 |
| Logout.....   | 17 |

---

## M

|                                     |     |
|-------------------------------------|-----|
| Machine Administrator.....          | 22  |
| Machine Administrator Settings..... | 248 |
| Menu Protect.....                   | 141 |
| Message.....                        | 235 |

## N

|                                     |     |
|-------------------------------------|-----|
| Network.....                        | 307 |
| Network Administrator.....          | 22  |
| Network Administrator Settings..... | 258 |
| Network Security Level.....         | 172 |
| Note.....                           | 11  |
| Notice.....                         | 9   |

## O

|                         |     |
|-------------------------|-----|
| Operational Issues..... | 237 |
| Options.....            | 312 |

## P

|  |     |
|--|-----|
| Password Policy.....                   | 221 |
| Preventing information leaks.....      | 223 |
| Printer.....                           | 294 |
| Printer Features.....                  | 272 |
| Printer Job Authentication.....        | 87  |
| Printer Job Authentication Levels..... | 87  |
| Printer Job Types.....                 | 88  |
| Printing the Encryption Key.....       | 126 |

## R

|                                    |         |
|------------------------------------|---------|
| Read-only.....                     | 267     |
| Registered User.....               | 17, 267 |
| Registering the Administrator..... | 27      |
| Remote Diagns.(Fax).....           | 221     |
| Remote Service.....                | 221     |
| Restrict Adding User Dest.....     | 219     |
| Restrict Use of Dest.....          | 218     |
| Restrict User Info.Display.....    | 219     |
| Restricting Destinations.....      | 107     |

## S

|                         |     |
|-------------------------|-----|
| S/MIME.....             | 110 |
| Scanner.....            | 300 |
| Scanner Features.....   | 276 |
| Security Functions..... | 13  |

|  |         |
|--|---------|
| Security Measures.....                         | 18      |
| Self-Signed Certificate.....                   | 182     |
| Service Mode Lock.....                         | 225     |
| Setting Up the Machine.....                    | 14      |
| Settings SNMPv1 and v2.....                    | 220     |
| Simple Encryption.....                         | 220     |
| SNMPv3.....                                    | 188     |
| Specifying a Group Password for PDF Files..... | 178     |
| Specifying an IPP Authentication Password..... | 179     |
| Specifying Login Details.....                  | 56      |
| Specifying Menu Protect.....                   | 143     |
| SSL.....                                       | 185     |
| SSL (Secure Sockets Layer).....                | 181     |
| SSL/TLS Encryption.....                        | 186     |
| Supervisor.....                                | 22, 241 |
| Symbols.....                                   | 10      |
| System Settings.....                           | 281     |

## T

|                               |     |
|-------------------------------|-----|
| telnet.....                   | 214 |
| Trademarks.....               | 313 |
| Transfer to Fax Receiver..... | 220 |
| Transmitted Passwords.....    | 176 |
| Type of Administrator.....    | 141 |

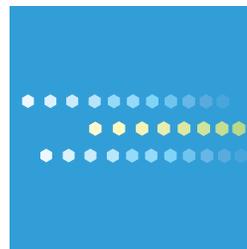
## U

|   |            |
|---|------------|
| Update Firmware.....                        | 222        |
| User.....                                   | 17, 37     |
| User Administrator.....                     | 267        |
| User Administrator Settings.....            | 265        |
| User Authentication.....                    | 17, 38, 41 |
| User Code Authentication.....               | 42         |
| User Lockout Function.....                  | 93         |
| User Settings - Control Panel Settings..... | 270        |

## W

|  |     |
|--|-----|
| Web Image Monitor Settings.....  | 287 |
| Webpage.....   | 311 |
| Windows Authentication.....  | 60  |
| Windows Authentication - Operational Requirements for Kerberos Authentication..... | 60  |
| Windows Authentication - Operational Requirements for NTLM Authentication.....     | 60  |





Type for MP 171F/Aficio MP 171F  
Type for MP 171SPF/Aficio MP 171SPF