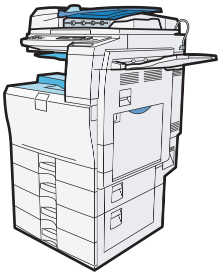
MP C2030/C2530
MP C2030/C2530
Aficio™ MP C2030/C2530

Operating Instructions

Security Reference



1 Getting Started

2 Administrators/Authentication and its Application

3 Users/Authentication and its Application

4 Protecting Document Data Information from Leaks

5 Managing Access to the Machine

6 Enhanced Network Security

7 Specifying the Extended Security Functions

8 Troubleshooting

9 Appendix

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

Manuals for This Machine

Read this manual carefully before you use this machine.

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

Important

- **Media differ according to manual.**
- **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.**

Reference

- p.14 "Setting Up the Machine"

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 and Scanner Reference

Explains functions and operations for the machine's printer and scanner unit.

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.

Other manuals

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

Note

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

Product name	General name
DeskTopBinder Lite and DeskTopBinder Professional * 1	DeskTopBinder
Web SmartDeviceMonitor Professional IS * 1 and Web SmartDeviceMonitor Standard * 1	Web SmartDeviceMonitor

*1 Optional

TABLE OF CONTENTS

Manuals for This Machine.....1

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

1. Getting Started

Before Using the Security Functions.....13

Setting Up the Machine.....14

Enhanced Security.....16

Glossary.....17

Security Measures Provided by this Machine.....18

Using Authentication and Managing Users.....18

Ensuring Information Security.....18

Limiting and Controlling Access.....19

Enhanced Network Security.....20

2. Administrators/Authentication and Its Application

Administrators.....21

User Administrator.....21

Machine Administrator.....22

Network Administrator.....22

File Administrator.....22

Supervisor.....22

About Administrator Authentication.....23

Enabling Administrator Authentication.....24

Specifying Administrator Privileges.....24

Registering the Administrator.....26

Logging on Using Administrator Authentication.....30

Logging off Using Administrator Authentication.....31

Changing the Administrator....32

Using Web Image Monitor....34

3. Users/Authentication and Its Application

Users....35

About User Authentication....36

Authentication Setting Procedure....37

Enabling User Authentication....39

User Code Authentication....40

Specifying User Code Authentication....40

Basic Authentication....46

Specifying Basic Authentication....46

Authentication Information Stored in the Address Book....51

Specifying Login User Name and Login Password....51

Specifying Authentication Information to Log on....54

Windows Authentication....58

Specifying Windows Authentication....59

LDAP Authentication....69

Specifying LDAP Authentication....70

Integration Server Authentication....78

Specifying Integration Server Authentication....78

Printer Job Authentication....87

If User Authentication is Specified....89

User Code Authentication (Using the Control Panel)....89

User Code Authentication (Using a Printer Driver)....89

Login (Using the Control Panel)....90

Log Off (Using the Control Panel)....90

Login (Using a Printer Driver)....91

Login (Using Web Image Monitor)....91

Log Off (Using Web Image Monitor)....91

User Lockout Function....91

Auto Logout....94

Authentication Using an External Device....96

4. Protecting Document Data Information from Leaks

Preventing Unauthorized Copying....97

Unauthorized Copy Prevention....98

Data Security for Copying....99

Printing Limitations....100

Notice....100

Printing with Unauthorized Copy Prevention and Data Security for Copying....101

Preventing Data Leaks Due to Unauthorized Transmission....103

Restrictions on Destinations....103

Protecting the Address Book....105

Address Book Access Permission....105

Encrypting Data in the Address Book....108

5. Managing Access to the Machine

Preventing Modification of Machine Settings....111

Menu Protect....113

Set up Menu Protect....113

Limiting Available Functions....117

Specifying Which Functions are Available....117

Managing Log Files....120

Using the Control Panel to Specify Log File Settings....120

Using Web SmartDeviceMonitor to Manage Log Files....123

Using Web Image Monitor to Manage Log Files....123

6. Enhanced Network Security

Preventing Unauthorized Access....127

Access Control....127

Enabling/Disabling Protocols....128

Specifying Network Security Level....135

Encrypting Transmitted Passwords....139

Driver Encryption Key....139

IPP Authentication Password....141

Protection Using Encryption....142

SSL (Secure Sockets Layer) Encryption....142

User Settings for SSL (Secure Sockets Layer)....147

Setting the SSL / TLS Encryption Mode....147
SNMPv3 Encryption....149
Transmission Using IPsec....152
Encryption and Authentication by IPsec....152
Encryption Key Auto Exchange Settings and Encryption Key Manual Settings....153
IPsec Settings....154
Encryption Key Auto Exchange Settings Configuration Flow....161
Encryption Key Manual Settings Configuration Flow....166
telnet Setting Commands....167
Authentication by telnet....175
"authfree" Command....175
Authentication by IEEE802.1X....176

7. Specifying the Extended Security Functions

Specifying the Extended Security Functions....177
Changing the Extended Security Functions....177
Procedure for Changing the Extended Security Functions....177
Settings....178
Other Security Functions....183
Fax Function....183
Limiting Machine Operation to Customers Only....184
Settings....184
Specifying Service Mode Lock Preparation....184
Canceling Service Mode Lock....185

8. Troubleshooting

Authentication Does Not Work Properly....187
A Message Appears....187
Machine Cannot Be Operated....189

9. Appendix

Supervisor Operations....193
Logging on as the Supervisor....193
Logging off as the Supervisor....194
Changing the Supervisor....194
Resetting an Administrator's Password....197

Machine Administrator Settings....200

System Settings....200

Copier Features....201

Facsimile Features....202

Printer Features....202

Settings via Web Image Monitor....203

Settings via SmartDeviceMonitor for Admin....206

Network Administrator Settings....207

System Settings....207

Settings via Web Image Monitor....207

Settings via SmartDeviceMonitor for Admin....209

File Administrator Settings....210

System Settings....210

Settings via Web Image Monitor....210

User Administrator Settings....211

System Settings....211

Settings via Web Image Monitor....211

Settings via SmartDeviceMonitor for Admin....212

The Privilege for User Account Settings in the Address Book....213

User Settings - Control Panel Settings....215

Copier Features....216

Printer Features....217

Facsimile Features....220

System Settings....222

User Settings - Web Image Monitor Settings....226

Device Settings....227

Printer....232

Fax....234

Interface....236

Network....237

Webpage....241

Functions That Require Options....242

Trademarks....243

INDEX......245

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.

[ ]

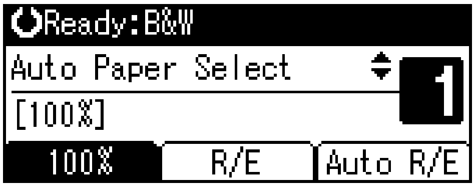
Indicates the names of keys on the machine's control panel.

Display

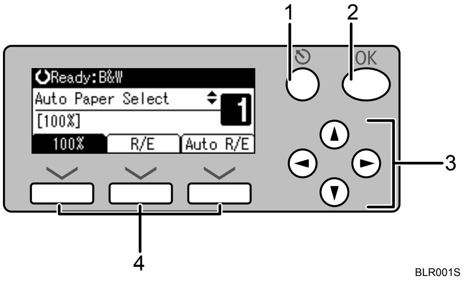
The display panel shows machine status, error messages, and function menus.

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. **[Escape] key**

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

2. **[OK] key**

   Press to set a selected item or entered numeric value.

3. **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.

4. **Selection keys**

   Correspond to items at the bottom line on the display.

   Example: initial copy display

   - When the instruction "press [100%]" appears in this manual, press the left selection key.
   - When the instruction "press [R/E]" appears in this manual, press the center selection key.

   When the instruction "press [Auto R/E]" appears in this manual, press the right selection key.

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.

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

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.

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

1. Getting Started

This chapter describes the machine's security features and how to specify initial security settings.

Before Using the Security Functions

Important

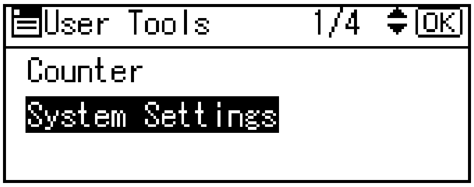
- **If the security settings are not specified, the machine may be damaged by malicious attackers.**

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. If the administrator 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.

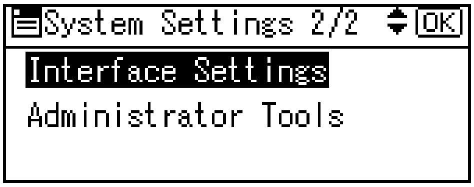
Setting Up the Machine

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.

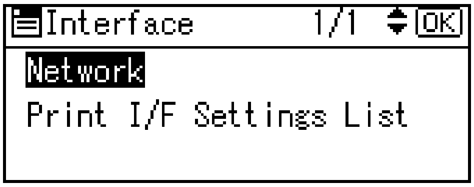
1. **Turn the machine on.**
2. **Press the [User Tools/Counter] key.**
3. **Press [System Settings] using [▲] or [▼], and then press the [OK] key.**



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 IP Address.**
7. **Connect the machine to the network.**
8. **Start Web Image Monitor, and then log on to the machine as the administrator.**
9. **Install the device certificate.**
10. **Enable secure sockets layer (SSL).**
11. **Enter the administrator's user name and password.**

    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 between steps 1 and 7.

Reference

- p.34 "Using Web Image Monitor"
- p.142 "Protection Using Encryption"
- p.26 "Registering the Administrator"

Enhanced Security

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.35 "Users"

Glossary

Administrator

There are four types of administrators according to administrative function: machine administrator, network administrator, file administrator, and user administrator. We recommend that only one person takes 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, 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

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 "Authentication Setting Procedure".

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.37 "Authentication Setting Procedure"
- p.46 "Basic Authentication"
- p.117 "Limiting Available Functions"

Ensuring Information Security

Preventing Unauthorized Copying (Unauthorized Copy Prevention)

Using the printer driver, you can embed a mask and pattern in the printed document. For details about preventing unauthorized copying, see "Preventing Unauthorized Copying". For information on how to specify Unauthorized Copy Prevention, see "Printing with Unauthorized Copy Prevention and Data Security for Copying".

Preventing Unauthorized Copying (Data Security for Copying)

Using the printer driver to enable data security for the copying function, you can print a document with an embedded pattern of hidden text.

To gray out the copy of a copy-guarded document, the optional security module is required. For details about Data Security for Copying, see "Data Security for Copying".

Preventing Data Leaks Due to Unauthorized Transmission

You can specify in the Address Book which users are allowed to send files using the 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 Data Leaks Due to Unauthorized 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".

Reference

- p.97 "Preventing Unauthorized Copying"
- p.101 "Printing with Unauthorized Copy Prevention and Data Security for Copying"
- p.99 "Data Security for Copying"
- p.103 "Preventing Data Leaks Due to Unauthorized Transmission"
- p.105 "Protecting the Address Book"
- p.120 "Managing Log Files"

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 Modification of 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.111 "Preventing Modification of Machine Settings"

- p.117 "Limiting Available Functions"

Enhanced 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 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.127 "Preventing Unauthorized Access"
- p.139 "Encrypting Transmitted Passwords"
- p.142 "Protection Using Encryption"
- p.152 "Transmission Using IPsec"

2. Administrators/Authentication and Its Application

Administrators

Administrators manage user access to the machine and various other important functions and settings.

When an administrator controls limited access and settings, first select the machine's administrator, enable the authentication function, and then use 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 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.26 "Registering the Administrator"
- p.193 "Supervisor Operations"
- p.35 "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 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 administrator can confirm the printer log information.

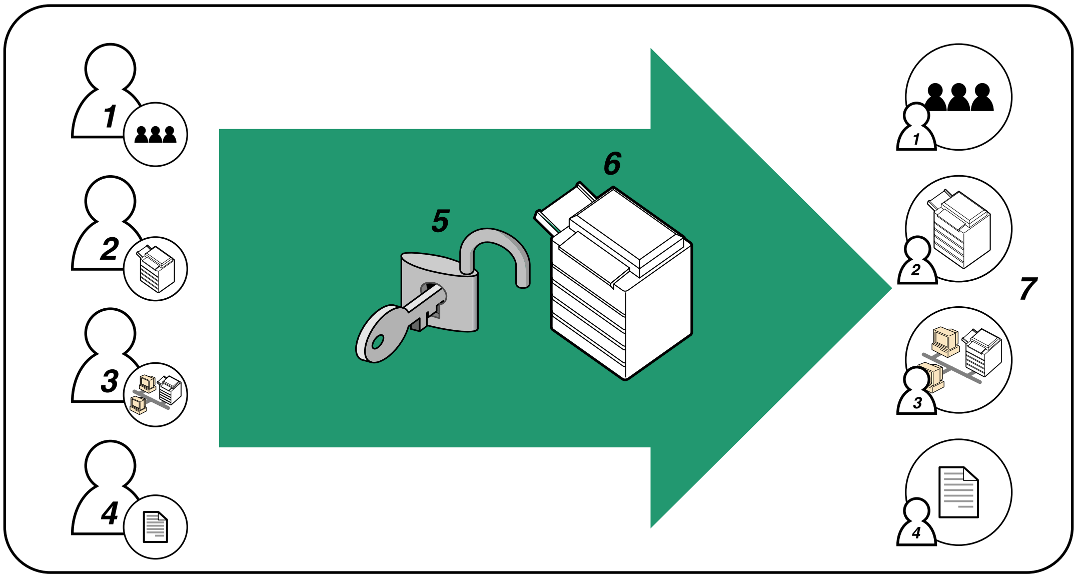
Supervisor

The supervisor can delete an administrator's password and specify a new one. The supervisor cannot specify defaults or use normal functions. However, if any of the administrators forget their password and cannot access the machine, the supervisor can provide support.

About Administrator Authentication

There are four types of administrators: user administrator, machine administrator, network administrator, and file administrator.

For details about each administrator, see "Administrators".



BBC005S

1. **User Administrator**

   This administrator manages personal information in the Address Book. You can register/delete users in the Address Book or change users' personal information.

2. **Machine Administrator**

   This administrator manages the machine's default settings. It is possible to enable only the machine administrator to set data security for copying, log deletion and other defaults.

3. **Network Administrator**

   This administrator manages the network settings. You can set the machine so that network settings such as the IP address can be specified by the network administrator only.

4. **File Administrator**

   This administrator can confirm the printer log information.

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 "Authentication Setting Procedure".

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.26 "Registering the Administrator"
- p.37 "Authentication Setting Procedure"

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.

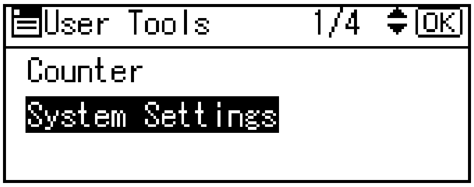
The defaults are "admin" for the login name and blank for the password. For details about changing the administrator password using the supervisor's authority, see "Supervisor Operations".

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

Important

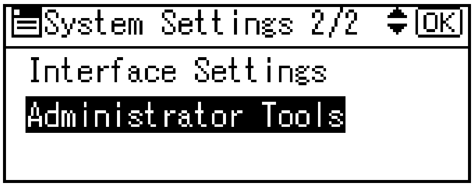
- If you have enabled Administrator Authentication Management, make sure not to forget the administrator login user name and login password. If an administrator login user name or login password is forgotten, a new password must be specified using the supervisor's authority. For instructions on registering 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 and the service call may not be free of charge.

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



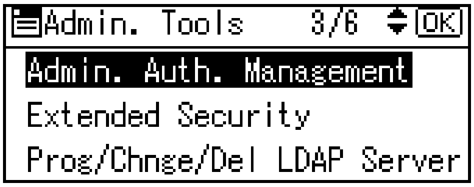
User Tools 1/4 ⇕ OK
Counter
System Settings

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



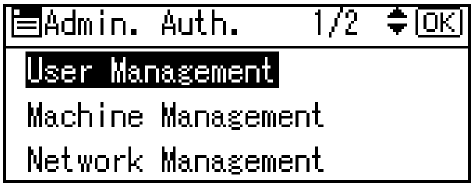
System Settings 2/2 ⇕ OK
Interface Settings
Administrator Tools

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



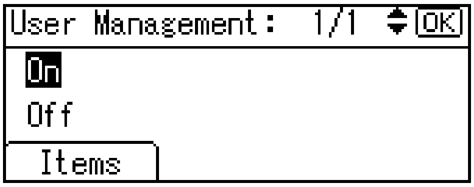
Admin. Tools 3/6 ⇕ OK
Admin. Auth. Management
Extended Security
Prog/Chnge/Del LDAP Server

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



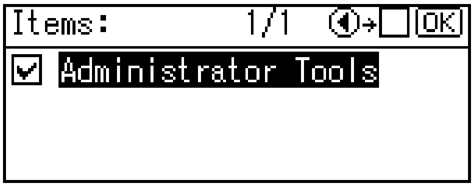
Admin. Auth. 1/2 ⇕ OK
User Management
Machine Management
Network Management

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.

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.193 "Supervisor Operations"
- p.30 "Logging on Using Administrator Authentication"
- p.31 "Logging off Using Administrator Authentication"
- p.111 "Managing Access to the Machine"

Registering the Administrator

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

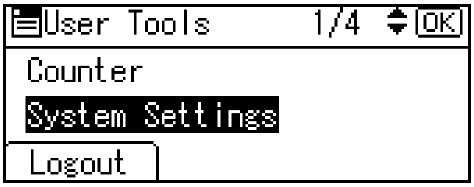
The sharing of administrator tasks eases the burden on individual administrators while also limiting unauthorized operation by a single administrator. You can register up to four login user names (Administrators 1-4) to which you can grant administrator privileges.

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.

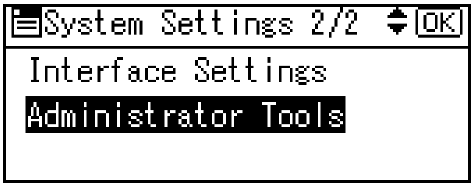
For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

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



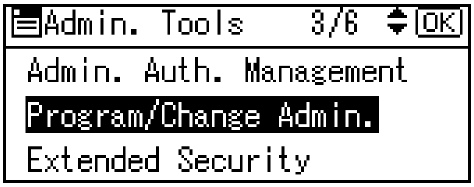
User Tools 1/4 ⬍ OK
Counter
System Settings
Logout

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



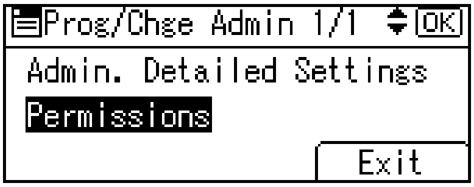
System Settings 2/2 ⬍ OK
Interface Settings
Administrator Tools

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



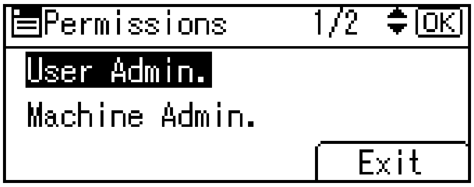
Admin. Tools 3/6 ⬍ OK
Admin. Auth. Management
Program/Change Admin.
Extended Security

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



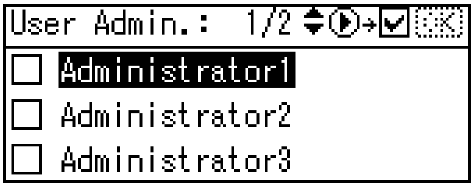
Prog/Chge Admin 1/1 ⬍ OK
Admin. Detailed Settings
Permissions
Exit

6. **Press [▲] or [▼] to scroll to the administrator whose access privileges you want to specify, and then press the [OK] key.**

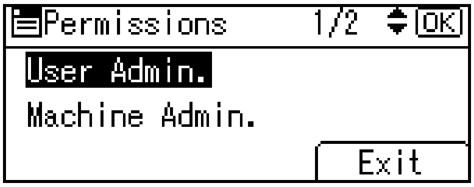


Permissions 1/2 ⬍ OK
User Admin.
Machine Admin.
Exit

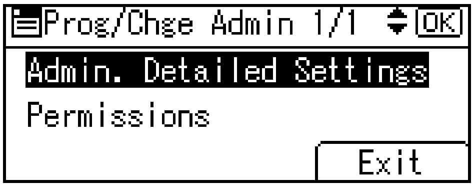
7. Select [Administrator 1], [Administrator 2], [Administrator 3] or [Administrator 4] using [▲] or [▼], and then press the [OK] key.



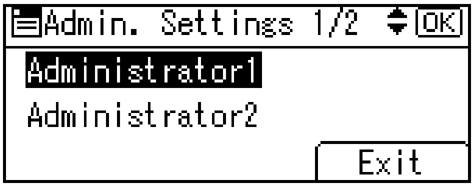
8. Press [Exit].



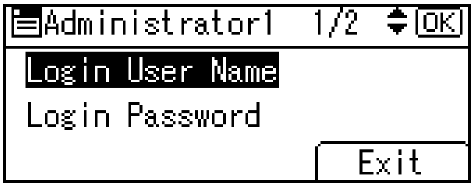
9. Select [Admin. Detailed Settings] using [▲] or [▼], and then press the [OK] key.



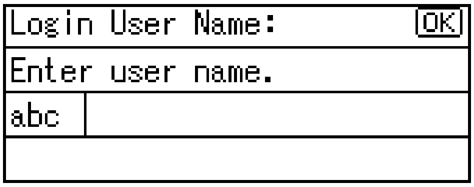
10. Select the setting you want to specify using [▲] or [▼], and then press the [OK] key.



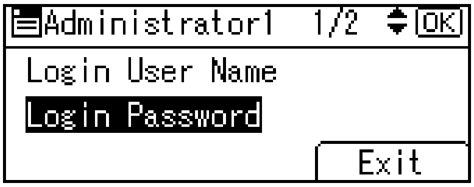
11. Select [Login User Name] using [▲] or [▼], and then press the [OK] key.



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



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



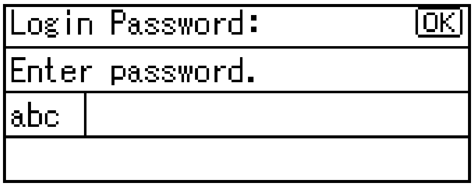
Administrator1 1/2 ⬍ OK

Login User Name

Login Password

Exit

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



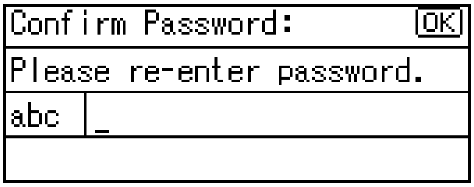
Login Password: OK

Enter password.

abc

Follow the password policy to make the login password more secure.

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

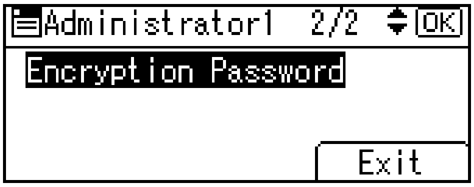


Confirm Password: OK

Please re-enter password.

abc _

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

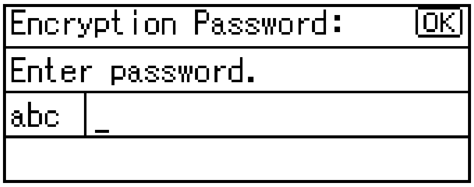


Administrator1 2/2 ⬍ OK

Encryption Password

Exit

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

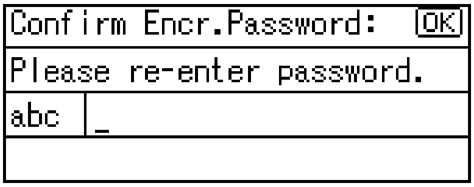


Encryption Password: OK

Enter password.

abc _

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

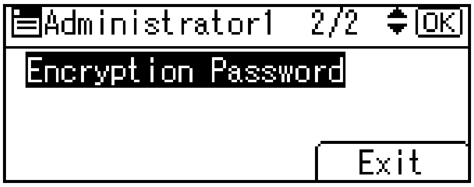


Confirm Encr.Password: OK

Please re-enter password.

abc _

19. **Press [Exit] three times.**



Administrator1 2/2 OK

Encryption Password

Exit

You will be automatically logged off.

20. **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

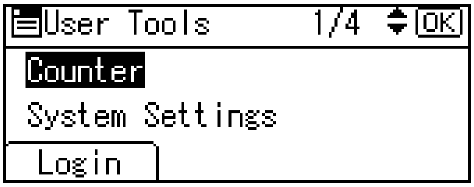
- p.30 "Logging on Using Administrator Authentication"
- p.31 "Logging off Using Administrator Authentication"
- p.177 "Specifying the Extended Security Functions"

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.

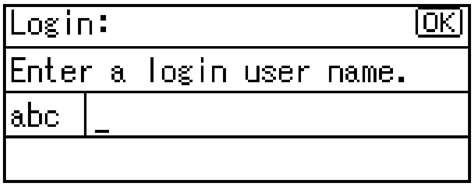
1. **Press the [User Tools/Counter] key.**

2. **Press [Login].**



```
User Tools          1/4  ⇕ OK
 Counter
 System Settings
 Login
```

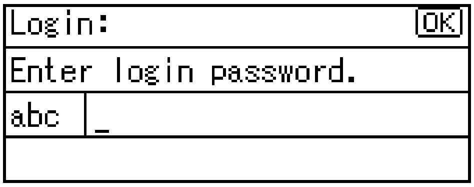
3. **Enter the login user name, and then press the [OK] key.**



```
Login:                      OK
Enter a login user name.
abc | _
```

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.**



```
Login:                      OK
Enter login password.
abc | _
```

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

To log on as an administrator, enter the administrator's login user name and login password.

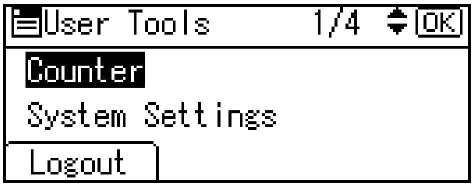
Note

- 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.

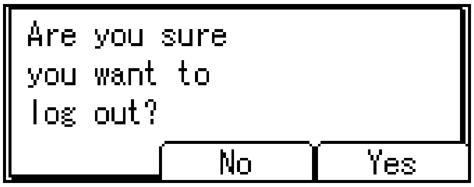
Logging off Using Administrator Authentication

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].**


Are you sure you want to log out?

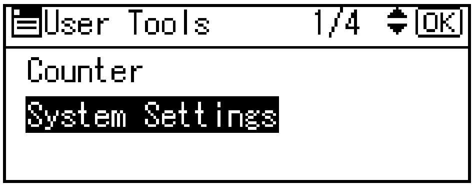
Changing the Administrator

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.

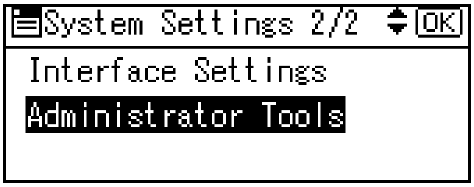
For example, to assign machine administrator authority and user administrator authority to [Administrator 1], press [Administrator 1] in the lines for the machine administrator and the user administrator.

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

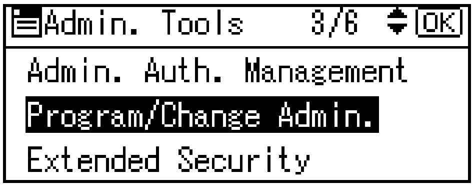
1. **Press the [User Tools/Counter] key.**
2. **Select [System Settings] using [▲] or [▼], and then press the [OK] key.**



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

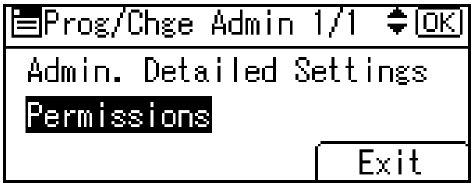


4. Select [Program/Change Admin.] using [▲] or [▼], and then press the [OK] key.



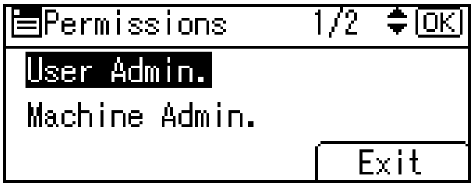
```
Admin. Tools      3/6  ⇕ OK
 Admin. Auth. Management
 Program/Change Admin.
 Extended Security
```

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



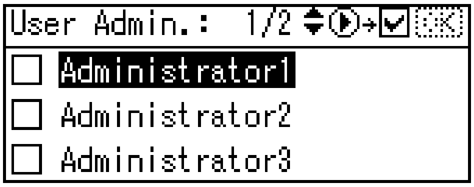
```
Prog/Chge Admin 1/1  ⇕ OK
 Admin. Detailed Settings
 Permissions
                      Exit
```

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



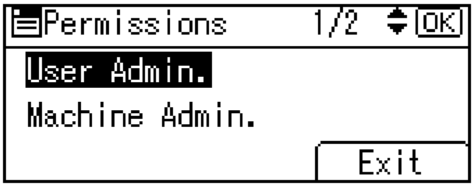
```
Permissions       1/2  ⇕ OK
 User Admin.
 Machine Admin.
                      Exit
```

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



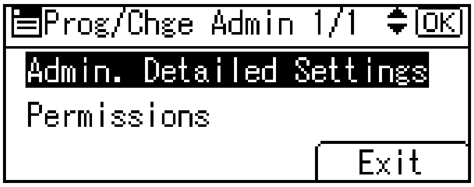
```
User Admin.:  1/2 ⇕ ▶→☑ OK
□ Administrator1
□ Administrator2
□ Administrator3
```

8. Press [Exit].



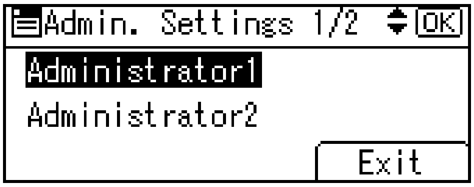
```
Permissions       1/2  ⇕ OK
 User Admin.
 Machine Admin.
                      Exit
```

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



```
Prog/Chge Admin 1/1  ⇕ OK
 Admin. Detailed Settings
 Permissions
                      Exit
```

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



Admin. Settings 1/2 ⬍ OK

Administrator1

Administrator2

Exit

11. **Press [Exit] three times.**

    You will be automatically logged off.

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

Reference

- p.30 "Logging on Using Administrator Authentication"
- p.31 "Logging off Using Administrator Authentication"

Using Web Image Monitor

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. Users/Authentication and Its Application

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", General Settings Guide, SmartDeviceMonitor for Admin Help, or Web Image Monitor Help.

Important

- **If user authentication is not possible because of a problem with the 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.**

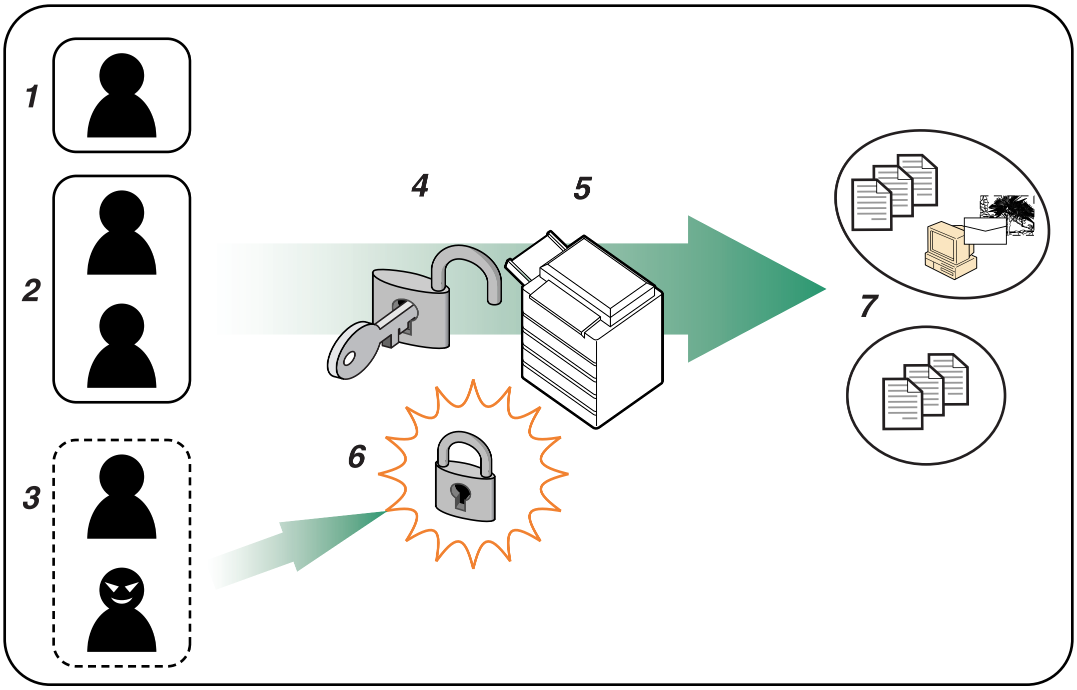
Reference

- 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.**

Authentication Setting Procedure

Specify administrator authentication and user authentication according to the following chart:

Administrator Authentication See "Enabling Administrator Authentication".	Specifying Administrator Privileges See "Specifying Administrator Privileges". Registering the Administrator See "Registering the Administrator".
User Authentication See "Enabling User Authentication".	Specifying User Authentication **Authentication that requires only the machine:** • User Code Authentication See "User Code Authentication". • Basic Authentication See "Basic Authentication". **Authentication that requires external devices:** • Windows Authentication See "Windows Authentication". • LDAP Authentication See "LDAP Authentication". • Integration Server Authentication See "Integration Server Authentication".

Note

- To specify Basic Authentication, Windows Authentication, LDAP Authentication, or Integration Server Authentication, you must first specify administrator authentication.
- You can specify User Code Authentication without specifying administrator authentication.

Reference

- p.24 "Enabling Administrator Authentication"
- p.39 "Enabling User Authentication"
- p.24 "Specifying Administrator Privileges"
- p.26 "Registering the Administrator"
- p.40 "User Code Authentication"
- p.46 "Basic Authentication"
- p.58 "Windows Authentication"

- p.69 "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", General Settings Guide. For details about changing passwords, see "Specifying Login User Name and Login Password".
- 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.51 "Specifying Login User Name and Login Password"

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", General Settings Guide.

For details about specifying the user code for the printer driver, see Printer and Scanner Reference or the printer driver Help.

For details about specifying the TWAIN driver user code, see the TWAIN driver Help.

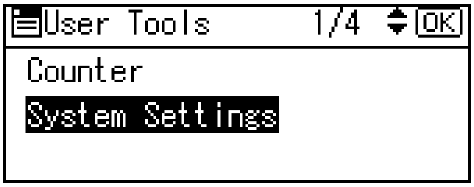
Important

- **To control the use of DeskTopBinder for the delivery of files stored in the machine, select Basic Authentication, Windows Authentication, LDAP Authentication, or Integration Server Authentication.**

Specifying User Code Authentication

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.**

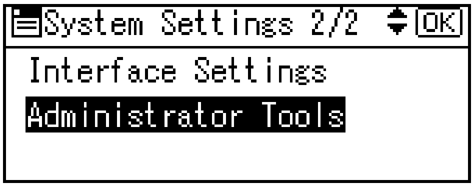


User Tools 1/4 ⇕ OK

Counter

System Settings

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

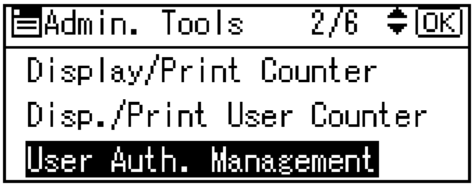


System Settings 2/2 ⇕ OK

Interface Settings

Administrator Tools

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



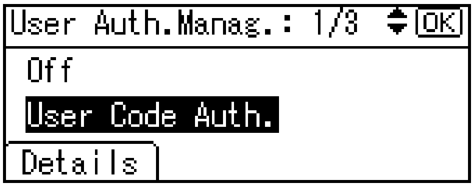
Admin. Tools 2/6 ⇕ OK

Display/Print Counter

Disp./Print User Counter

User Auth. Management

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



User Auth.Manag.: 1/3 ⬍ [OK]

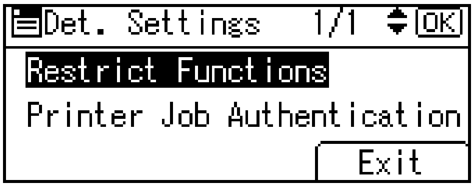
Off

User Code Auth.

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.**



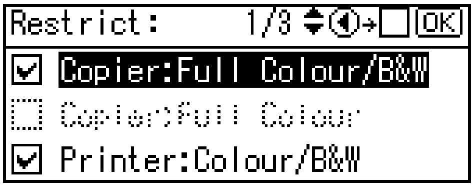
Det. Settings 1/1 ⬍ [OK]

Restrict Functions

Printer Job Authentication

Exit

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



Restrict: 1/3 ⬍ ◀→□ [OK]

☑ Copier:Full Colour/B&W

□ Copier:Full Colour

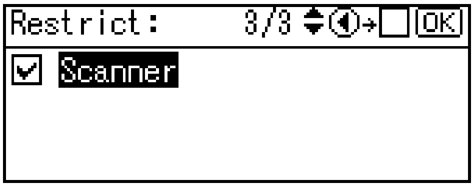
☑ Printer:Colour/B&W

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

User Code Authentication will be applied to the selected functions.

Unselected functions will not be affected.

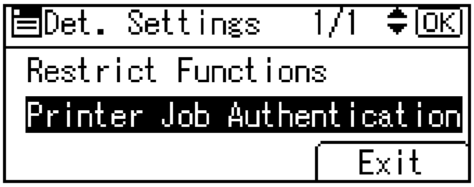
8. **Press the [OK] key.**



Restrict: 3/3 ⬍ ◀→□ [OK]

☑ Scanner

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



Det. Settings 1/1 ⬍ [OK]

Restrict Functions

Printer Job Authentication

Exit

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)".

Reference

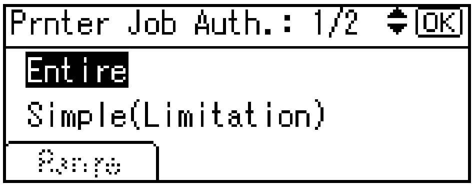
- p.117 "Limiting Available Functions"
- p.42 "Selecting Entire or Simple (All)"
- p.43 "Selecting Simple (Limitation)"
- p.87 "Printer Job Authentication"

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)].

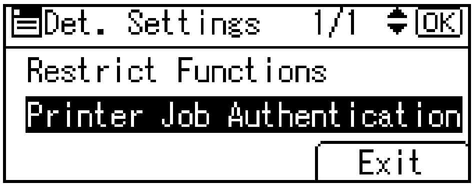
If you select [Simple (All)], you can print even with unauthenticated printer drivers or devices. Specify this setting if you want to print with a printer driver or device that cannot be identified by the machine or if you do not require authentication for printing. However, note that, because the machine does not require authentication in this case, it may be used by unauthorized users.

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



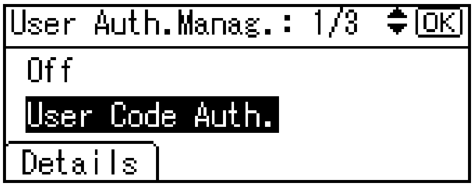
Prnter Job Auth.: 1/2 ⬍ OK
Entire
Simple(Limitation)
Range

2. **Press [Exit].**



Det. Settings 1/1 ⬍ OK
Restrict Functions
Printer Job Authentication
Exit

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



User Auth.Manag.: 1/3 ⬍ OK
Off
User Code Auth.
Details

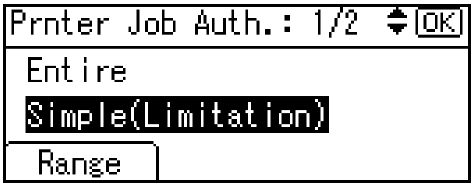
4. **Press the [User Tools/Counter] key.**

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 the [Range] key.**



```
Prnter Job Auth.: 1/2 ⇕ OK
 Entire
 Simple(Limitation)
 Range
```

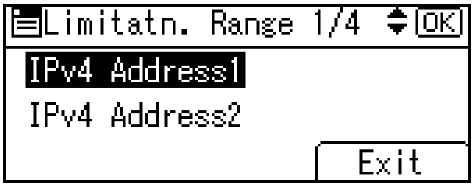
Specify the range in which [Simple (Limitation)] is applied to Printer Job Authentication.

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

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

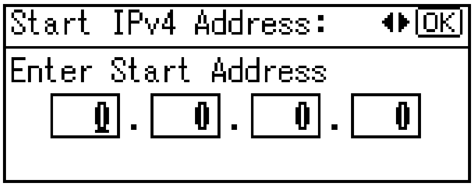
If you specify [USB (Sim.)], proceed to step 7.

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 Address1
 IPv4 Address2
                 Exit
```

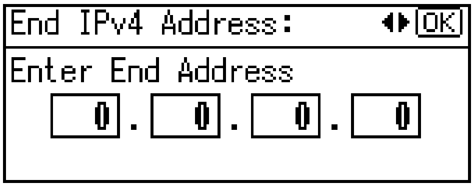
3. **Enter the Start IPv4 Address, and then press the [OK] key.**



```
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.**



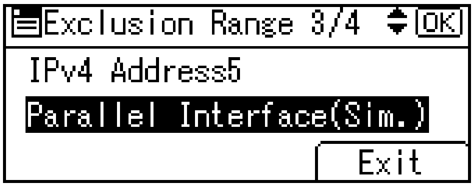
End IPv4 Address: ◀▶ OK

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.**



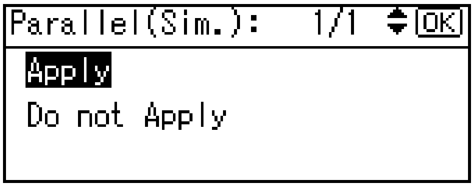
Exclusion Range 3/4 ⬍ OK

IPv4 Address5

Parallel Interface(Sim.)

Exit

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

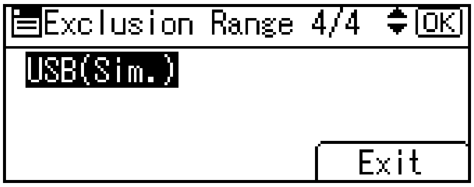


Parallel(Sim.): 1/1 ⬍ OK

Apply

Do not Apply

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

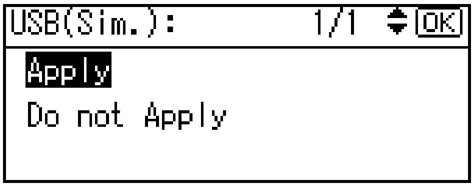


Exclusion Range 4/4 ⬍ OK

USB(Sim.)

Exit

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

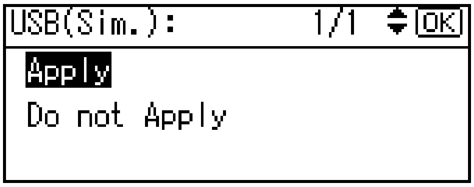


USB(Sim.): 1/1 ⬍ OK

Apply

Do not Apply

9. Press [Exit].

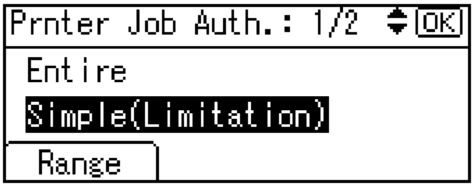


USB(Sim.): 1/1 ⬍ OK

Apply

Do not Apply

10. Press the [OK] key.



Prnter Job Auth.: 1/2 ⬍ OK

Entire

Simple(Limitation)

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.

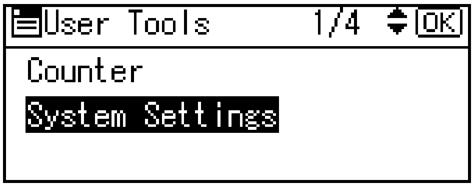
Specifying Basic Authentication

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

This can be specified by the machine administrator.

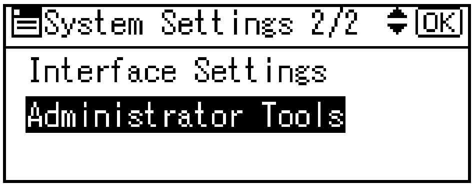
For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

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



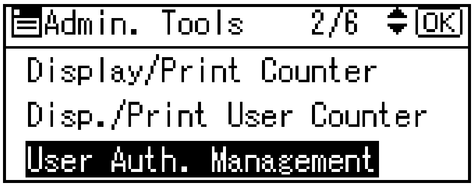
```
User Tools        1/4  ⬍ OK
Counter
System Settings
```

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



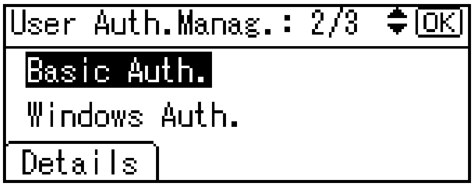
```
System Settings 2/2  ⬍ OK
Interface Settings
Administrator Tools
```

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



```
Admin. Tools      2/6  ⬍ OK
Display/Print Counter
Disp./Print User Counter
User Auth. Management
```

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



User Auth.Manag.: 2/3 ⬍ OK

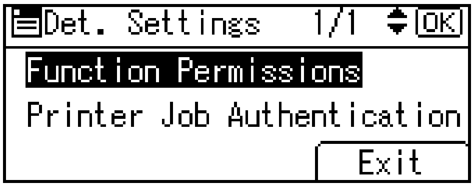
Basic Auth.

Windows Auth.

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.**



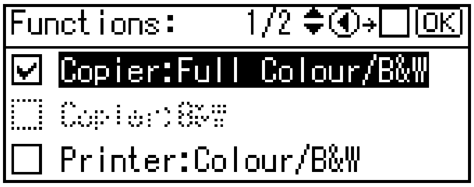
Det. Settings 1/1 ⬍ OK

Function Permissions

Printer Job Authentication

Exit

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



Functions: 1/2 ⬍ ◀→□ OK

☑ Copier:Full Colour/B&W

□ Copier:B&W

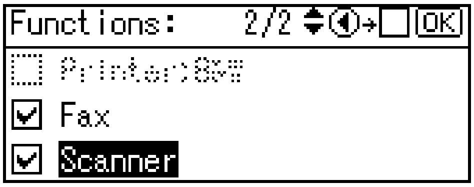
□ Printer:Colour/B&W

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

Basic Authentication will be applied to the selected functions.

Users can use the selected functions only.

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



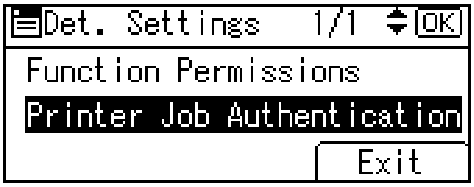
Functions: 2/2 ⬍ ◀→□ OK

□ Printer:B&W

☑ Fax

☑ Scanner

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



Det. Settings 1/1 ⬍ OK

Function Permissions

Printer Job Authentication

Exit

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)".

Reference

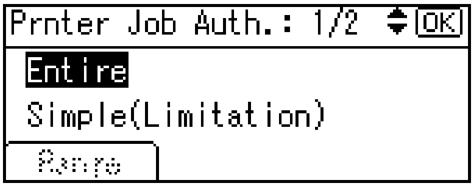
- p.30 "Logging on Using Administrator Authentication"
- p.31 "Logging off Using Administrator Authentication"
- p.117 "Limiting Available Functions"
- p.48 "Selecting Entire or Simple (All)"
- p.49 "Selecting Simple (Limitation)"

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)].

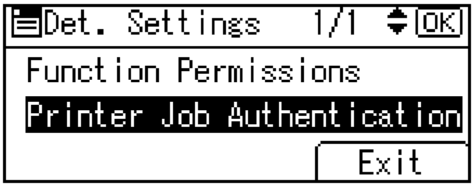
If you select [Simple (All)], you can print even with unauthenticated printer drivers or devices. Specify this setting if you want to print with a printer driver or device that cannot be identified by the machine or if you do not require authentication for printing. However, note that, because the machine 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.**



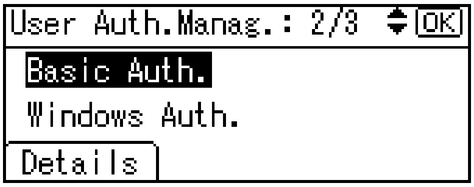
Prnter Job Auth.: 1/2 ⬍ OK
Entire
Simple(Limitation)
Range

2. **Press [Exit].**



Det. Settings 1/1 ⬍ OK
Function Permissions
Printer Job Authentication
Exit

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



User Auth.Manag.: 2/3 ⬍ OK
Basic Auth.
Windows Auth.
Details

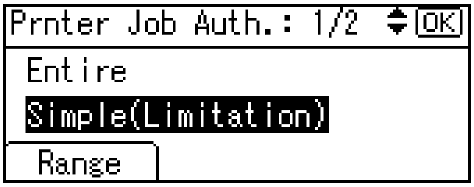
4. **Press the [User Tools/Counter] key.**

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 the [Range] key.**



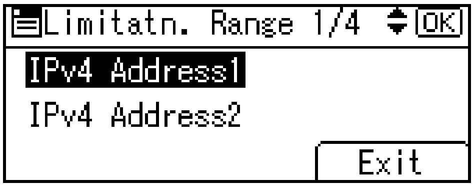
Specify the range in which [Simple (Limitation)] is applied to Printer Job Authentication.

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

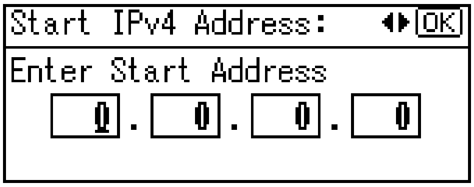
If you specify [Parallel Interface (Sim.)], proceed to step 5.

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.**

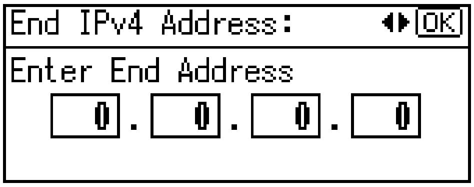


3. **Enter the Start IPv4 Address, and then press the [OK] key.**



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.**



End IPv4 Address: ◀▶ OK

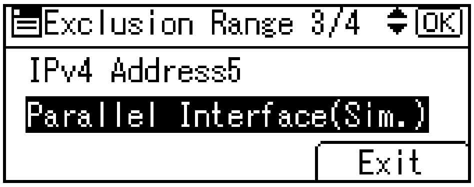
Enter End Address

0 . 0 . 0 . 0

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

Select

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



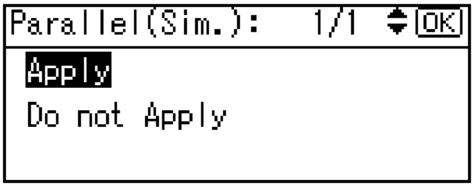
Exclusion Range 3/4 ▲▼ OK

IPv4 Address5

Parallel Interface(Sim.)

Exit

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

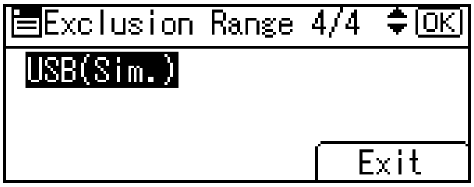


Parallel(Sim.): 1/1 ▲▼ OK

Apply

Do not Apply

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

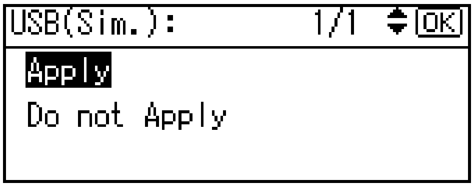


Exclusion Range 4/4 ▲▼ OK

USB(Sim.)

Exit

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

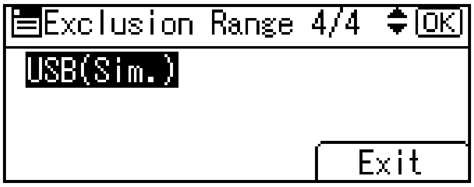


USB(Sim.): 1/1 ▲▼ OK

Apply

Do not Apply

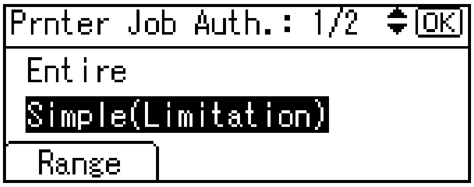
9. **Press [Exit].**



```
Exclusion Range 4/4  ⇕ OK
USB(Sim.)

                      Exit
```

10. **Press the [OK] key.**



```
Prnter Job Auth.: 1/2  ⇕ OK
 Entire
 Simple(Limitation)
 Range
```

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

Authentication Information Stored in the Address Book

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

If you have specified User Authentication, you can specify access limits for individual users and groups of users. Specify the setting in the Address Book for each user.

Users must have a registered account in the Address Book in order to use the machine when User Authentication is specified. For details about user registration, see "Registering Names", General Settings Guide.

User authentication can also be specified via SmartDeviceMonitor for Admin or Web Image Monitor.

Reference

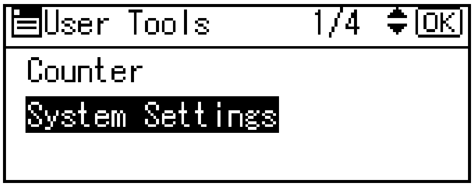
- p.30 "Logging on Using Administrator Authentication"
- p.31 "Logging off Using Administrator Authentication"

Specifying Login User Name and Login Password

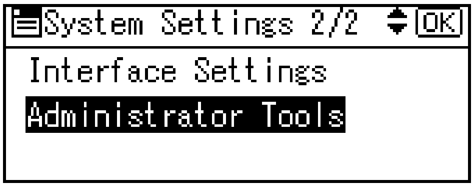
In [Address Book Management], specify the login user name and login password to be used for User Authentication Management.

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

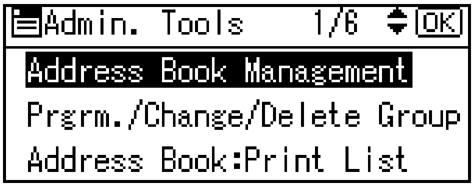
2. **Select [System Settings] using [▲] or [▼], and then press the [OK] key.**



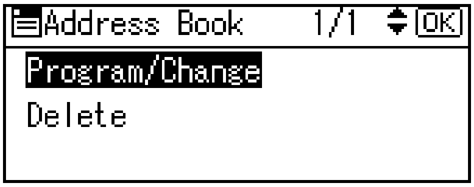
3. **Select [Administrator Tools] using [▲] or [▼], and then press the [OK] key.**



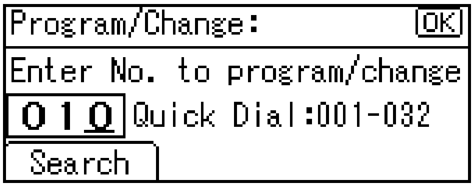
4. **Select [Address Book Management] using [▲] or [▼], and then press the [OK] key.**



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

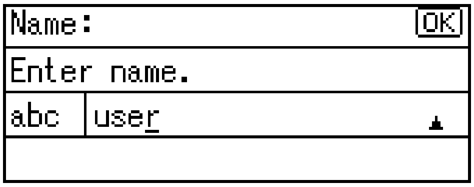


6. **Enter the registration number you want to program using the number keys or the Quick Dial keys, and then press the [OK] key.**



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

7. Press the [OK] key.

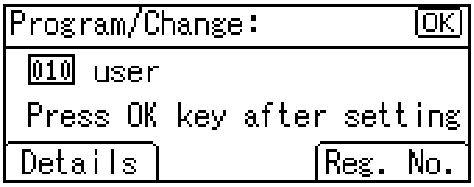


Name: [OK]

Enter name.

abc | user

8. Press [Details].



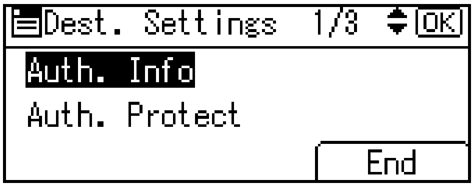
Program/Change: [OK]

010 user

Press OK key after setting

Details | Reg. No.

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



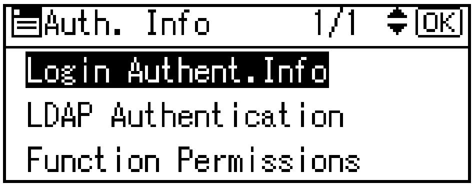
Dest. Settings 1/3 ⬍ [OK]

Auth. Info

Auth. Protect

End

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



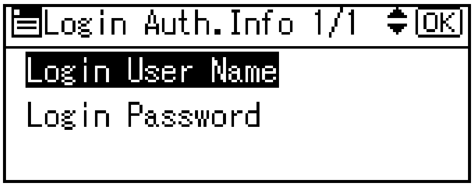
Auth. Info 1/1 ⬍ [OK]

Login Authent.Info

LDAP Authentication

Function Permissions

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

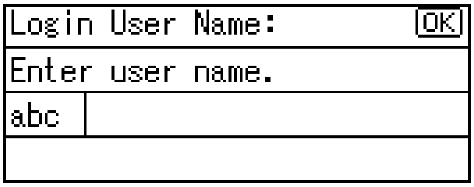


Login Auth.Info 1/1 ⬍ [OK]

Login User Name

Login Password

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

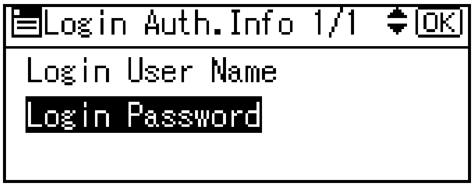


Login User Name: [OK]

Enter user name.

abc |

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

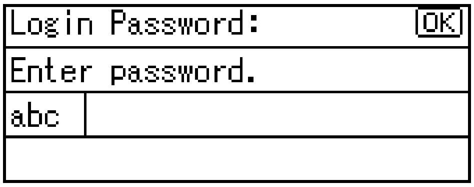


Login Auth.Info 1/1 ⬍ OK

Login User Name

Login Password

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

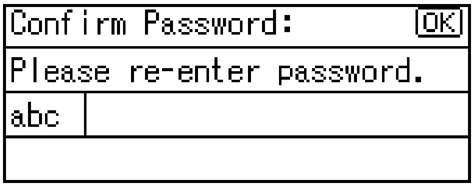


Login Password: OK

Enter password.

abc

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



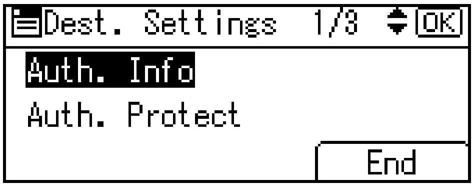
Confirm Password: OK

Please re-enter password.

abc

16. Press the [Escape] key two times.

17. Press [End].



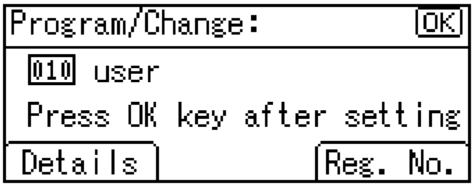
Dest. Settings 1/3 ⬍ OK

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 Authentication Information to Log on

The login user name and password specified in [Address Book Management] can be used as the login information for "Folder Authentication" and "LDAP Authentication".

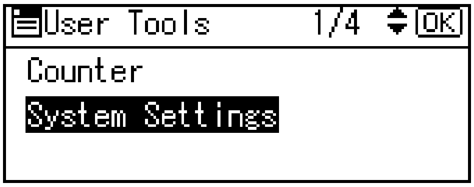
If you do not want to use the login user name and password specified in [Address Book Management] for "Folder Authentication", or "LDAP Authentication", see "Address Book" General Settings Guide.

For details about specifying login user name and login password, see "Specifying Login User Name and Login Password".

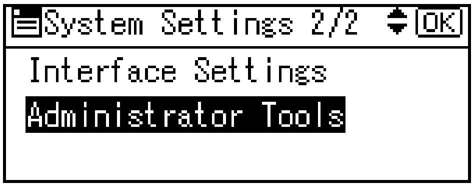
Important

- **When using [Use Auth. Info at Login] for "Folder Authentication" or "LDAP Authentication", a user name other than "other", "admin", "supervisor" or "HIDE***" must be specified. The symbol "***" represents any character.**

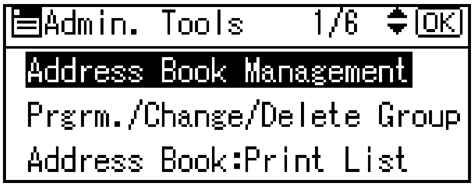
1. **Press the [User Tools/Counter] key.**
2. **Select [System Settings] using [▲] or [▼], and then press the [OK] key.**



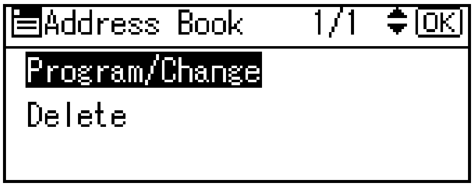
3. **Select [Administrator Tools] using [▲] or [▼], and then press the [OK] key.**



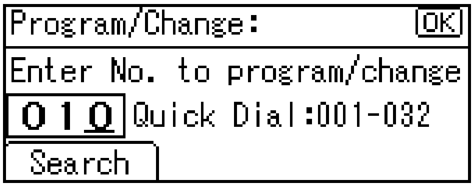
4. **Select [Address Book Management] using [▲] or [▼], and then press the [OK] key.**



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



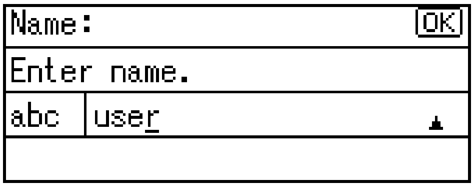
6. **Enter the registration number you want to program using the number keys or the Quick Dial keys, and then press the [OK] key.**



```
Program/Change:                 OK
Enter No. to program/change
010 Quick Dial:001-032
Search
```

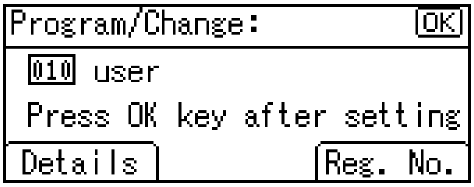
By pressing [Search], you can search by Name, Display Destination List, Registration No., User Code and Fax Destination.

7. **Press the [OK] key.**



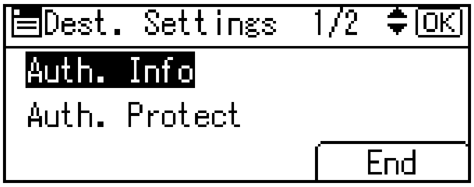
```
Name:                           OK
Enter name.
abc  user
```

8. **Press [Details].**



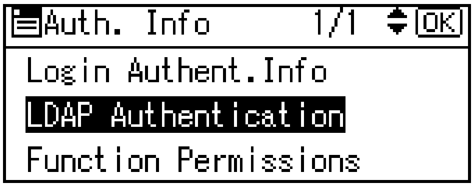
```
Program/Change:                 OK
 010 user
 Press OK key after setting
Details                  Reg. No.
```

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



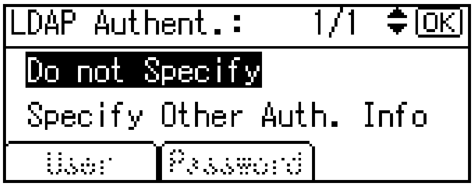
```
Dest. Settings  1/2  ⬍ OK
 Auth. Info
 Auth. Protect
                       End
```

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



```
Auth. Info      1/1  ⬍ OK
 Login Authent.Info
 LDAP Authentication
 Function Permissions
```

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



LDAP Authent.: 1/1 ⇕ OK

Do not Specify

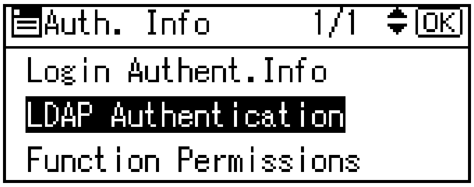
Specify Other Auth. Info

User Password

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

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

12. **Press the [Escape] key.**



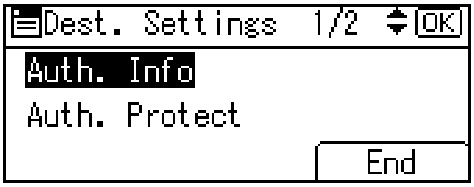
Auth. Info 1/1 ⇕ OK

Login Authent.Info

LDAP Authentication

Function Permissions

13. **Press [End].**



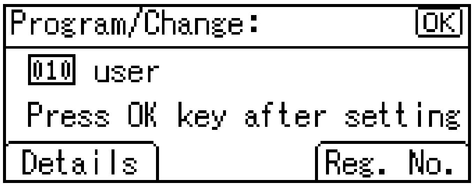
Dest. Settings 1/2 ⇕ OK

Auth. Info

Auth. Protect

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.**

Note

- When using [Use Auth. Info at Login] for "Folder Authentication" or "LDAP Authentication", a user name other than "other" , "admin" , "supervisor" or "HIDE* * *" must be specified. The symbol "* * *" represents any character.

Reference

- p.51 "Specifying Login User Name and Login Password"

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.

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 NT 4.0 Server
  - 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 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.**

- **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.**

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.
- A user registered in two or more global groups can use all the functions available to members of those groups.
- If the "Guest" account on the Windows server is enabled, even users not registered in the domain controller can be authenticated. When this account is enabled, users are registered in the Address Book and can use the functions available under [*Default Group].

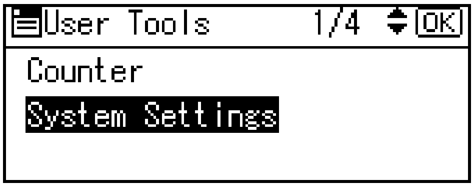
Specifying Windows Authentication

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

This can be specified by the machine administrator.

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

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

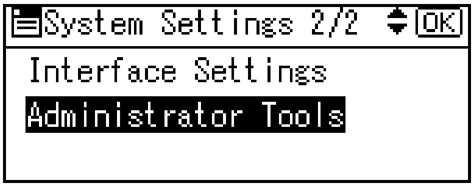


User Tools 1/4 ⬍ OK

Counter

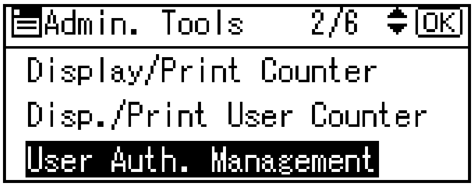
System Settings

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



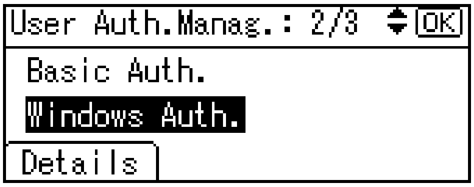
```
System Settings 2/2  ⬍ OK
Interface Settings
Administrator Tools
```

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



```
Admin. Tools     2/6  ⬍ OK
Display/Print Counter
Disp./Print User Counter
User Auth. Management
```

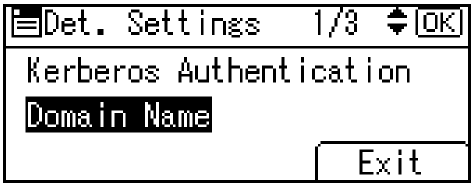
5. **Select [Windows Auth.] using [▲] or [▼], and then press [Details].**



```
User Auth.Manag.: 2/3  ⬍ OK
Basic Auth.
Windows Auth.
Details
```

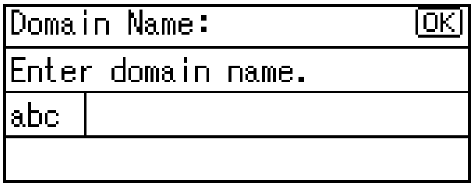
If you do not want to use user authentication management, select [Off].

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



```
Det. Settings    1/3  ⬍ OK
Kerberos Authentication
Domain Name
                      Exit
```

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



```
Domain Name:             OK
Enter domain name.
abc
```

If global groups have not been registered, proceed to step 15.

If global groups have been registered, proceed to step 8.

If global groups have been registered under Windows server, you can limit the use of functions for each global group.

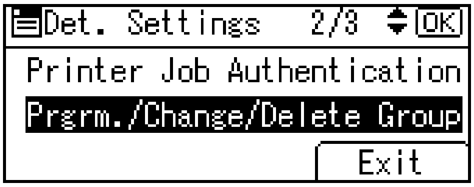
You need to create global groups in the Windows server in advance and register in each group the users to be authenticated.

You also need to register in the machine the functions available to the global group members.

Create global groups in the machine by entering the names of the global groups registered in the Windows Server. (Keep in mind that group names are case sensitive.) Then specify the machine functions available to each group.

If global groups are not specified, users can use the available functions specified in [*Default Group]. If global groups are specified, users not registered in global groups can use the available functions specified in [*Default Group]. By default, all functions are available to [*Default Group] members. Specify the limitation on available functions according to user needs.

8. **Select [Prgrm./Change/Delete Group] using [▲] or [▼], and then press the [OK] key.**



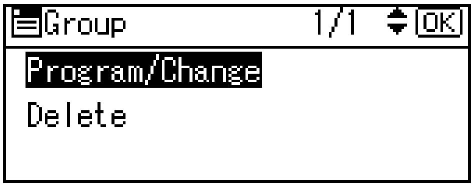
Det. Settings 2/3 ⬍ OK

Printer Job Authentication

Prgrm./Change/Delete Group

Exit

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

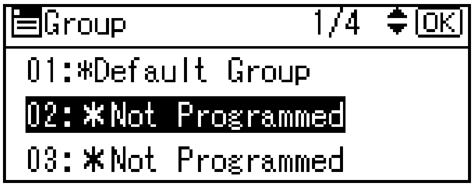


Group 1/1 ⬍ OK

Program/Change

Delete

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



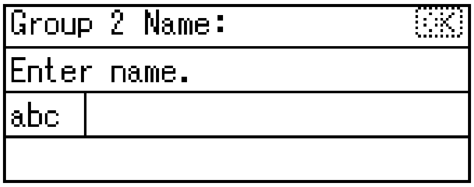
Group 1/4 ⬍ OK

01:*Default Group

02:*Not Programmed

03:*Not Programmed

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

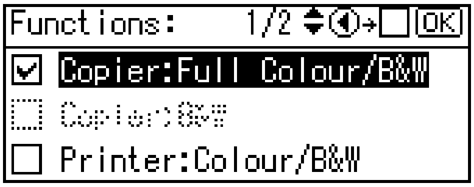


Group 2 Name: OK

Enter name.

abc

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



Functions: 1/2 OK

☑ Copier:Full Colour/B&W

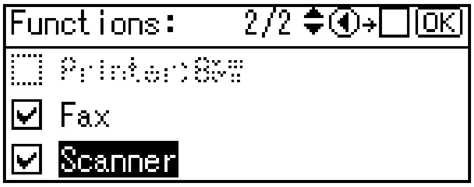
□ Copier:B&W

□ Printer:Colour/B&W

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

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

13. **Press the [OK] key.**



Functions: 2/2 OK

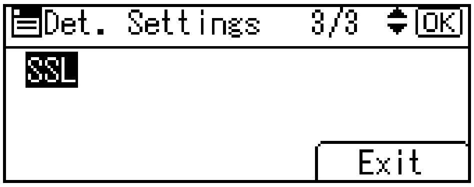
□ Printer:B&W

☑ Fax

☑ Scanner

14. **Press the [Escape] key twice.**

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

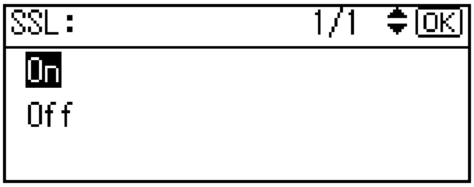


Det. Settings 3/3 OK

SSL

Exit

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



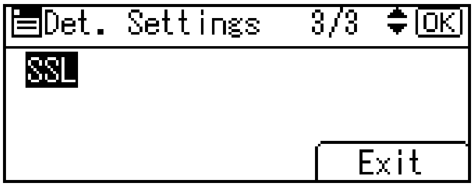
SSL: 1/1 OK

On

Off

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

17. **Press [Exit].**

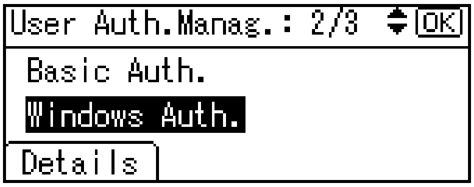


Det. Settings 3/3 OK

SSL

Exit

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

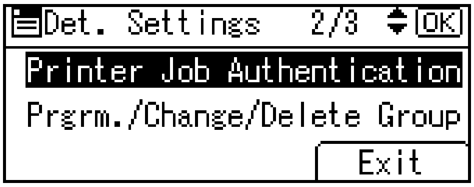


User Auth.Manag.: 2/3 ⇕ OK

Basic Auth.

Windows Auth.

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



Det. Settings 2/3 ⇕ OK

Printer Job Authentication

Prgrm./Change/Delete Group

20. **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

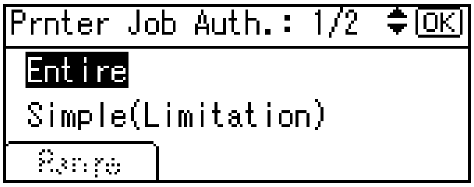
- p.30 "Logging on Using Administrator Authentication"
- p.31 "Logging off Using Administrator Authentication"
- p.117 "Limiting Available Functions"
- p.63 "Selecting Entire or Simple (All)"
- p.64 "Selecting Simple (Limitation)"
- p.87 "Printer Job Authentication"

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.**



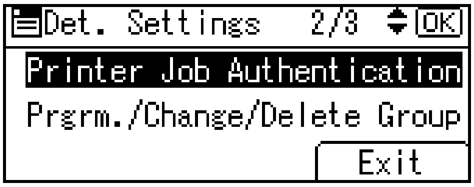
Prnter Job Auth.: 1/2 ⇕ OK

Entire

Simple(Limitation)

Range

2. **Press [Exit].**



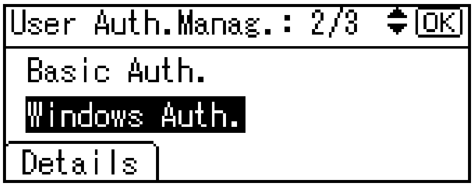
Det. Settings 2/3 ⇕ OK

Printer Job Authentication

Prgrm./Change/Delete Group

Exit

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



User Auth.Manag.: 2/3 ⇕ OK

Basic Auth.

Windows Auth.

Details

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

Note

- Under Windows Authentication, you can select whether or not to use secure sockets layer (SSL) authentication.
- To automatically register user information such as fax numbers 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 using SSL.

Reference

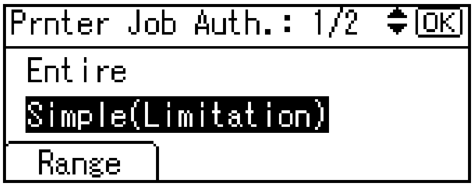
- p.117 "Limiting Available Functions"

Selecting Simple (Limitation)

If you select [Simple (Limitation)], you can specify clients for which printer job authentication is not required. Specify [Parallel Interface (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 the [Range] key.**



Prnter Job Auth.: 1/2 ⬍ OK

Entire

Simple(Limitation)

Range

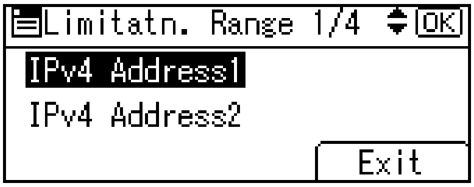
Specify the range in which [Simple (Limitation)] is applied to Printer Job Authentication.

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.**



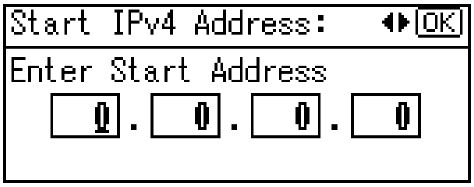
Limitatn. Range 1/4 ⬍ OK

IPv4 Address1

IPv4 Address2

Exit

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



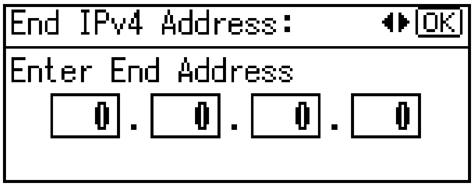
Start IPv4 Address: ◀▶ OK

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.**



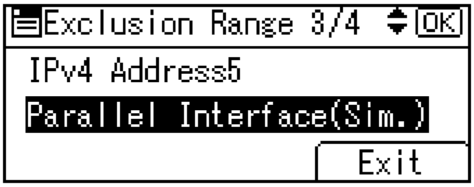
End IPv4 Address: ◀▶ OK

Enter End Address

0 . 0 . 0 . 0

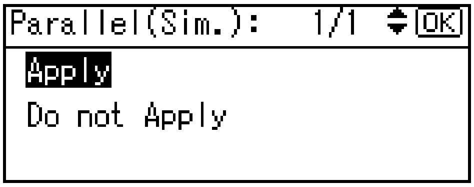
Be sure the number you enter for End IPv4 Address is larger than that for Start IPv4 Address.

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



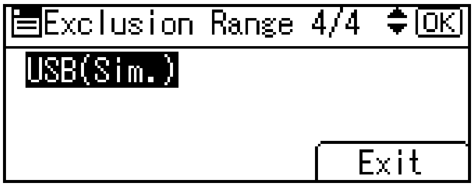
Exclusion Range 3/4 ⬍ OK
IPv4 Address5
Parallel Interface(Sim.)
Exit

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



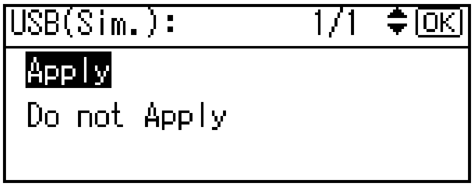
Parallel(Sim.): 1/1 ⬍ OK
Apply
Do not Apply

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



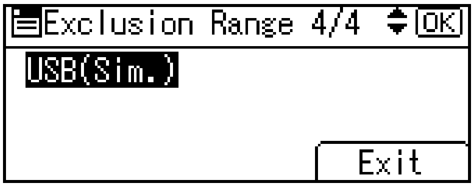
Exclusion Range 4/4 ⬍ OK
USB(Sim.)
Exit

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



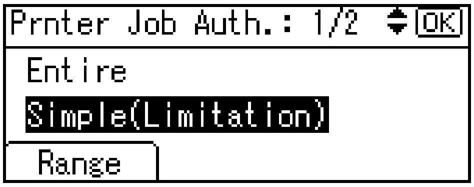
USB(Sim.): 1/1 ⬍ OK
Apply
Do not Apply

9. Press [Exit].



Exclusion Range 4/4 ⬍ OK
USB(Sim.)
Exit

10. Press the [OK] key.



Prnter Job Auth.: 1/2 ⬍ OK
Entire
Simple(Limitation)
Range

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

Note

- Under Windows Authentication, you can select whether or not to use secure sockets layer (SSL) authentication.
- To automatically register user information such as fax numbers 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 using SSL.

Reference

- p.117 "Limiting Available Functions"

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 (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", General Settings Guide.
- The reference function is not available for SSL servers when a search for LDAP is in progress.

Specifying LDAP Authentication

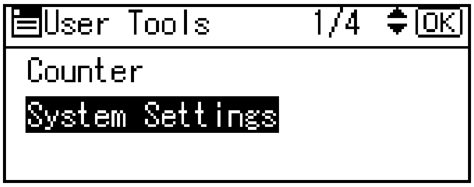
Before beginning to configure the machine, make sure that administrator authentication is properly configured under "Administrator Authentication Management".

This can be specified by the machine administrator.

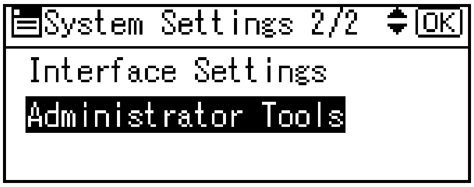
For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

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

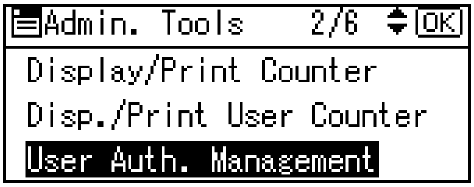
2. Select [System Settings] using [▲] or [▼], and then press the [OK] key.



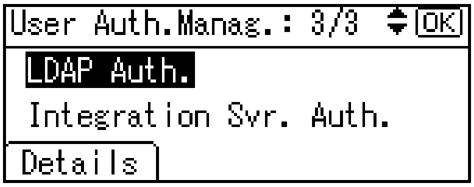
3. Select [Administrator Tools] using [▲] or [▼], and then press the [OK] key.



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

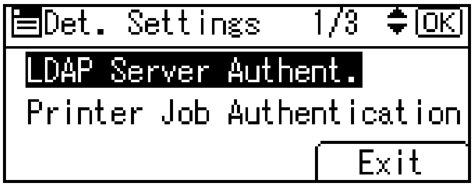


5. Select [LDAP Auth.] using [▲] or [▼], and then press [Details].

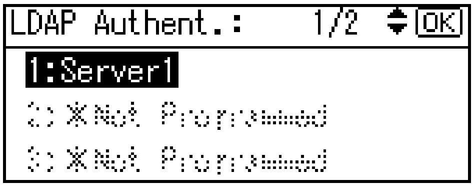


If you do not want to use user authentication management, select [Off].

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

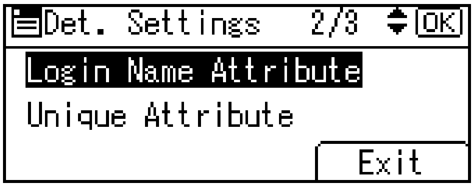


7. **Select the LDAP server to be used for LDAP authentication using [▲] or [▼], and then press the [OK] key.**



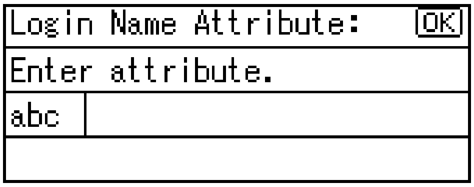
```
LDAP Authent.:      1/2 ⇕ OK
 1:Server1
 2:※Not Programmed
 3:※Not Programmed
```

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



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

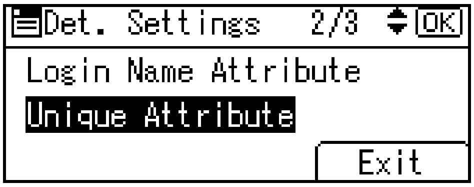
9. **Enter the login name attribute, and then press the [OK] key.**



```
Login Name Attribute:     OK
Enter attribute.
abc |
```

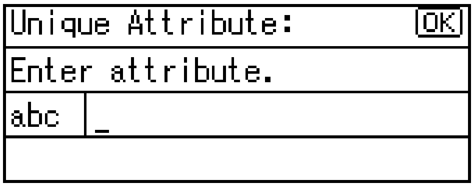
You can use the Login Name Attribute as a search criterion to obtain information about an authenticated user. You can create a search filter based on the Login Name Attribute, select a user, and then retrieve the user information from the LDAP server so it is transferred to the machine's address book. The method for selecting the user name depends on the server environment. Check the server environment and enter the user name accordingly.

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



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

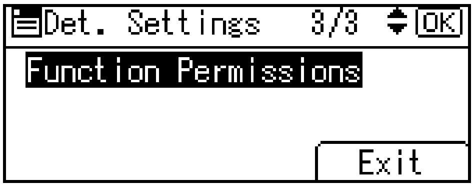
11. **Enter the unique attribute, and then press the [OK] key.**



```
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.

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

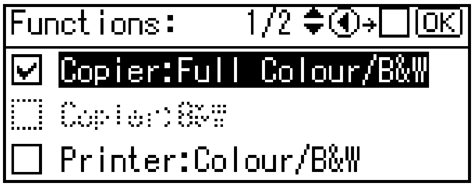


Det. Settings 3/3 OK

Function Permissions

Exit

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



Functions: 1/2 OK

☑ Copier:Full Colour/B&W

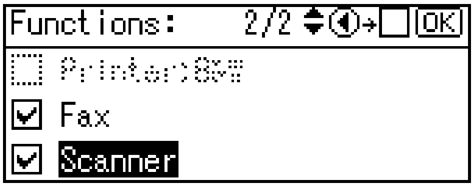
□ Copier:B&W

□ Printer:Colour/B&W

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.

14. **Press the [OK] key.**



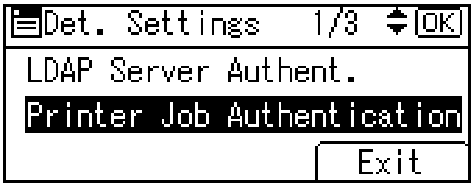
Functions: 2/2 OK

□ Printer:B&W

☑ Fax

☑ Scanner

15. **Select [Printer Job Authentication] using [▲] or [▼], and then press the [▶] key.**



Det. Settings 1/3 OK

LDAP Server Authent.

Printer Job Authentication

Exit

16. **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

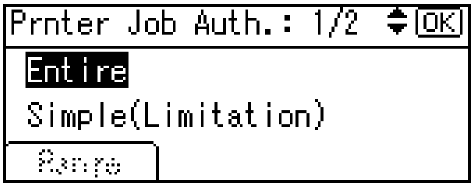
- p.30 "Logging on Using Administrator Authentication"
- p.31 "Logging off Using Administrator Authentication"
- p.74 "Selecting Entire or Simple (All)"
- p.75 "Selecting Simple (Limitation)"
- p.87 "Printer Job Authentication"

Selecting Entire or Simple (All)

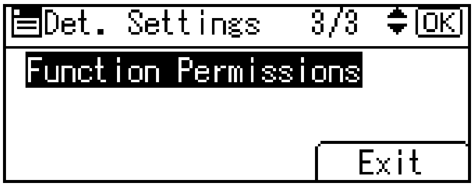
If you select [Entire], you cannot print using a printer driver or a device that does not support authentication. To print under an environment that does not support authentication, select [Simple (All)] or [Simple (Limitation)].

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.

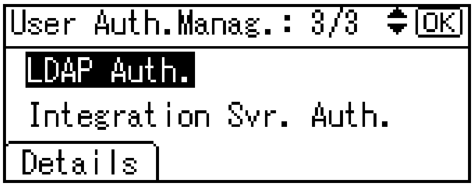
1. **Select [Entire] or [Simple (All)] using [▲] or [▼], and then press the [OK] key.**



2. **Press [Exit].**



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



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

Reference

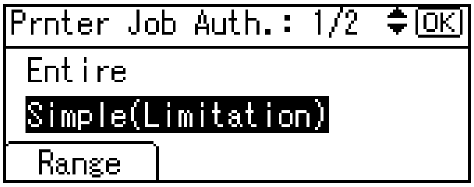
- p.117 "Limiting Available Functions"

Selecting Simple (Limitation)

If you select [Simple (Limitation)], you can specify clients for which printer job authentication is not required. Specify [Parallel Interface (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 the [Range] key.**



Prnter Job Auth.: 1/2 ⬍ OK

Entire

Simple(Limitation)

Range

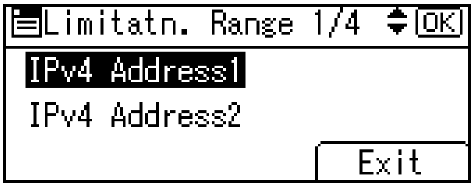
Specify the range in which [Simple (Limitation)] is applied to Printer Job Authentication.

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.**



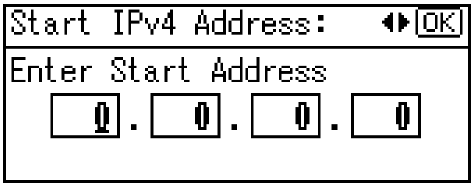
Limitatn. Range 1/4 ⬍ OK

IPv4 Address1

IPv4 Address2

Exit

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



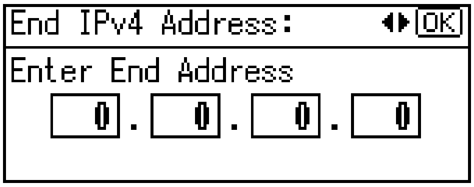
Start IPv4 Address: ◀▶ OK

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.**



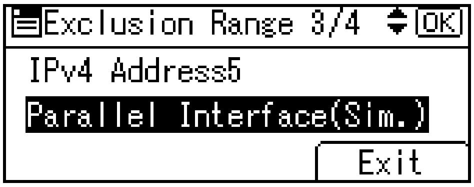
End IPv4 Address: ◀▶ OK

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.**



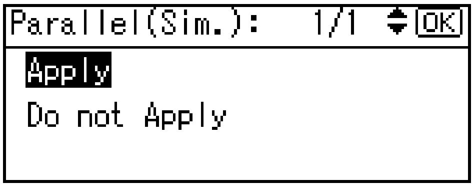
Exclusion Range 3/4 ▲▼ OK

IPv4 Address5

Parallel Interface(Sim.)

Exit

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

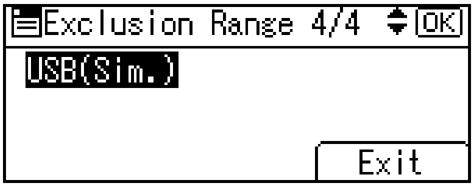


Parallel(Sim.): 1/1 ▲▼ OK

Apply

Do not Apply

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

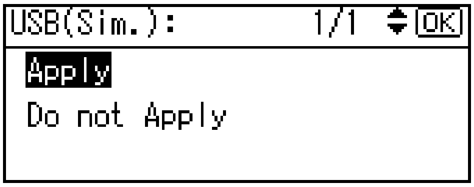


Exclusion Range 4/4 ▲▼ OK

USB(Sim.)

Exit

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

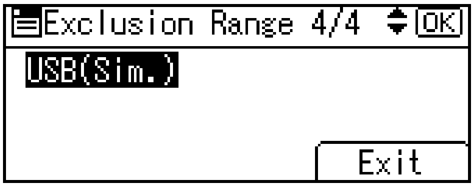


USB(Sim.): 1/1 ▲▼ OK

Apply

Do not Apply

9. **Press [Exit].**

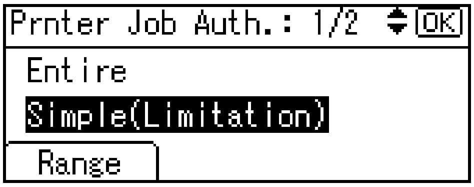


Exclusion Range 4/4 ▲▼ OK

USB(Sim.)

Exit

10. **Press the [OK] key.**



```
Prnter Job Auth.: 1/2  ⬍ OK
 Entire
 Simple(Limitation)
  Range
```

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

Reference

- p.117 "Limiting Available Functions"

Integration Server Authentication

To use Integration Server authentication, you need a server on which ScanRouter software that supports authentication is installed.

For external authentication, the Integration Server authentication collectively authenticates users accessing the server over the network, providing a server-independent, centralized user authentication system that is safe and convenient.

For example, if the delivery server and the machine share the same Integration Server authentication, single sign-on is possible using DeskTopBinder.

To use Integration Server authentication, access to a server on which ScanRouter System or Web SmartDeviceMonitor and Authentication Manager are installed, other than the machine, is required. For details about the software, contact your sales representative.

Using Web Image Monitor, you can specify that the server reliability and site certificate are checked every time you access the SSL server. For details about specifying SSL using Web Image Monitor, see Web Image Monitor Help.

Important

- **During Integration Server Authentication, the data registered in the server is automatically registered in the machine.**
- **If user information on the server is changed, information registered in the machine may be overwritten when authentication is performed.**

Note

- The default administrator name for ScanRouter System or Web SmartDeviceMonitor, "Admin," differs from the server, "admin".

Specifying Integration Server Authentication

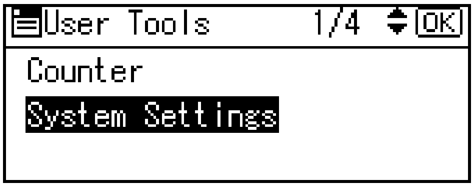
Before beginning to configure the machine, make sure that administrator authentication is properly configured under "Administrator Authentication Management".

This can be specified by the machine administrator.

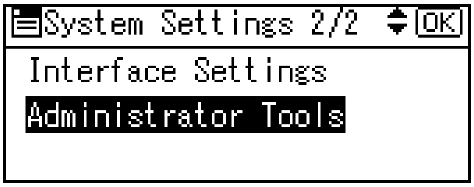
For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

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

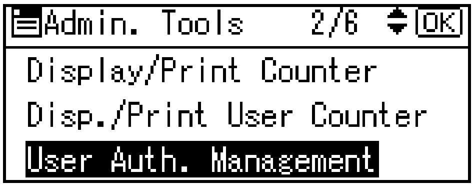
2. **Select [System Settings] using [▲] or [▼], and then press the [OK] key.**



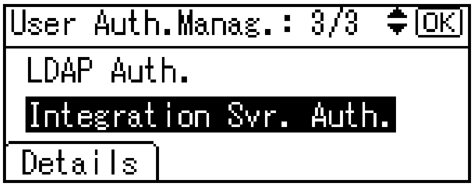
3. **Select [Administrator Tools] using [▲] or [▼], and then press the [OK] key.**



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

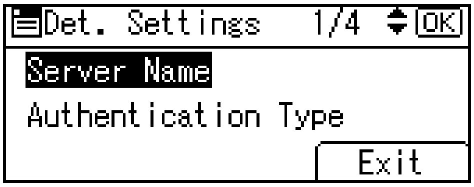


5. **Select [Integration Svr. Auth.] using [▲] or [▼], and then press [Details].**



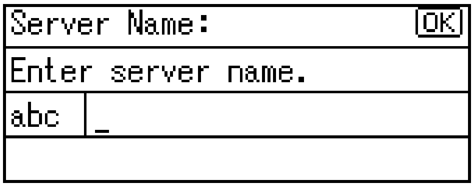
If you do not want to use User Authentication Management, select [Off].

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



Specify the name of the server for external authentication.

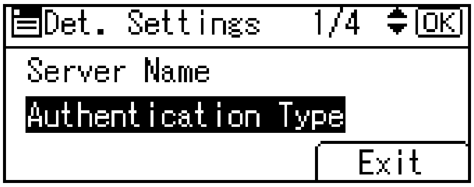
7. **Enter the server name, and then press the [OK] key.**



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

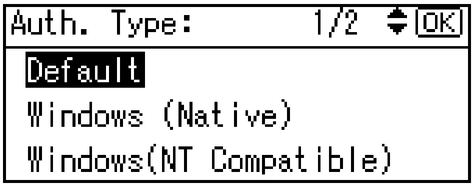
Enter the IPv4 address or host name.

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



```
Det. Settings    1/4 ⬍ [OK]
 Server Name
 Authentication Type
                   Exit
```

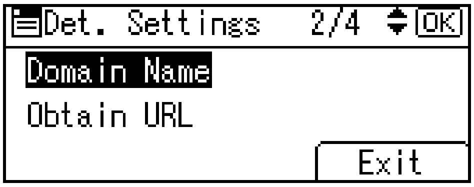
9. **Select the authentication system for external authentication using [▲] or [▼], and then press the [OK] key.**



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

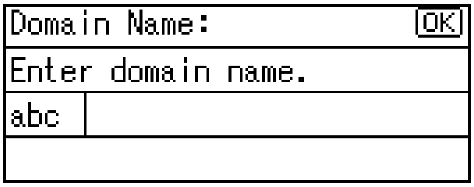
Select an available authentication system.

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



```
Det. Settings    2/4 ⬍ [OK]
 Domain Name
 Obtain URL
                   Exit
```

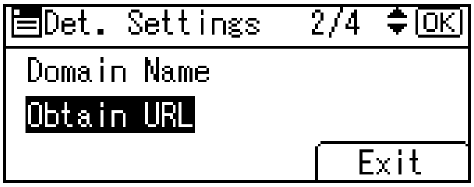
11. **Enter the domain name, and then press the [OK] key.**



```
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

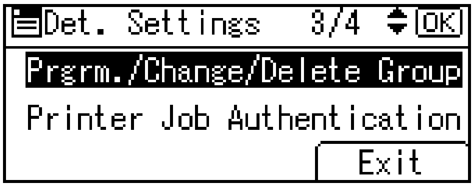
The machine obtains the URL of the server specified in "Server Name".

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.**



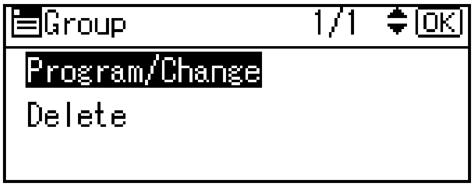
Det. Settings 3/4 ⇕ OK

Prgrm./Change/Delete Group

Printer Job Authentication

Exit

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

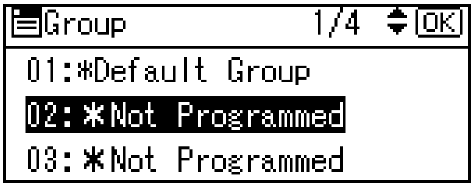


Group 1/1 ⇕ OK

Program/Change

Delete

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



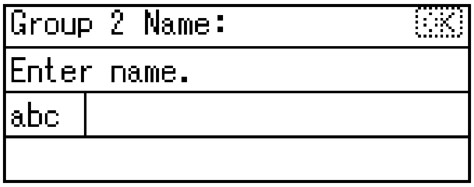
Group 1/4 ⇕ OK

01:*Default Group

02:*Not Programmed

03:*Not Programmed

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

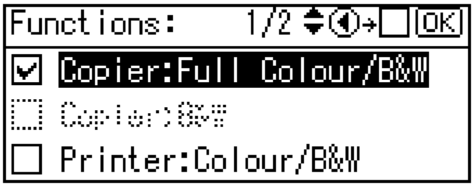


Group 2 Name: OK

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:Full Colour/B&W

⬚ Copier:B&W

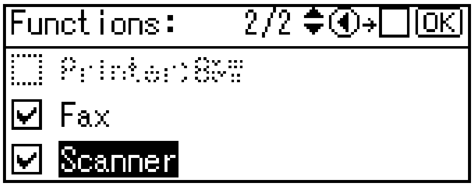
□ Printer:Colour/B&W

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

Integration Server Authentication will be applied to the selected functions.

Users can use the selected functions only.

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



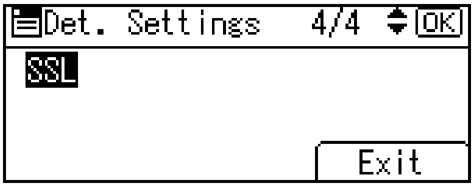
Functions: 2/2 ⇕ ◀▶☐ OK

⬚ Printer:B&W

☑ Fax

☑ Scanner

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

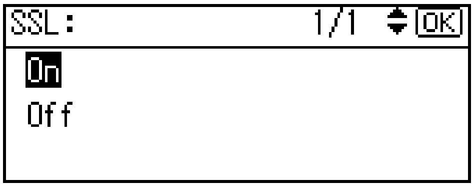


Det. Settings 4/4 ⇕ OK

SSL

Exit

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



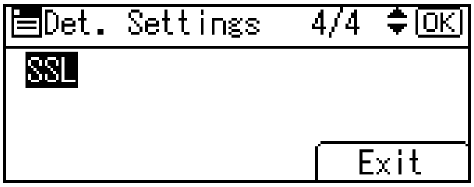
SSL: 1/1 ⇕ OK

On

Off

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

21. **Press [Exit].**

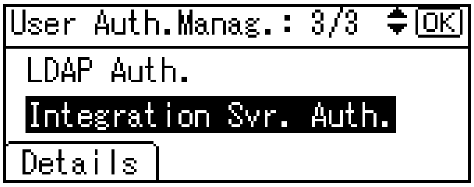


Det. Settings 4/4 ⇕ OK

SSL

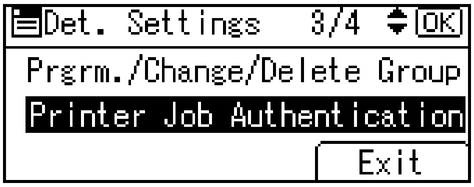
Exit

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



User Auth.Manag.: 3/3 ⇕ OK
LDAP Auth.
Integration Svr. Auth.
Details

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



Det. Settings 3/4 ⇕ OK
Prgrm./Change/Delete Group
Printer Job Authentication
Exit

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) ".

Reference

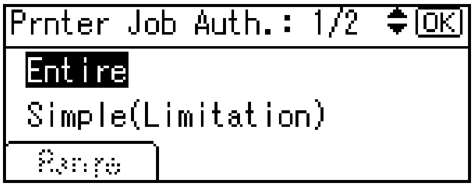
- p.30 "Logging on Using Administrator Authentication"
- p.31 "Logging off Using Administrator Authentication"
- p.117 "Limiting Available Functions"
- p.83 "Selecting Entire or Simple (All)"
- p.84 "Selecting Simple (Limitation)"
- p.87 "Printer Job Authentication"

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)].

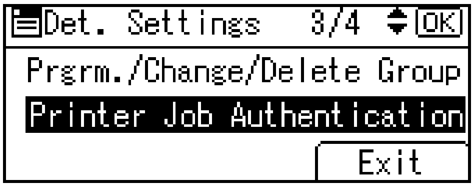
If you select [Simple (All)], you can print even with unauthenticated printer drivers or devices. Specify this setting if you want to print with a printer driver or device that cannot be identified by the machine or if you do not require authentication for printing. However, note that, because the machine 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.**



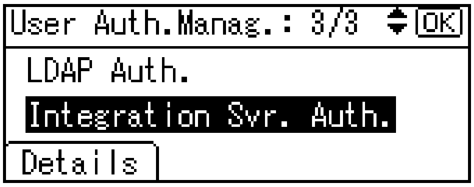
Prnter Job Auth.: 1/2 ⇕ OK
Entire
Simple(Limitation)
Range

2. **Press [Exit].**



Det. Settings 3/4 ⬍ OK
Prgrm./Change/Delete Group
Printer Job Authentication
Exit

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



User Auth.Manag.: 3/3 ⬍ OK
LDAP Auth.
Integration Svr. Auth.
Details

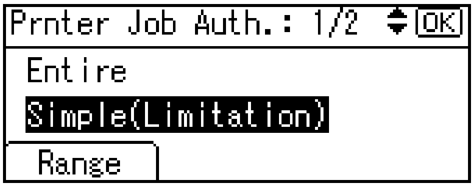
4. **Press the [User Tools/Counter] key.**

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 the [Range] key.**



Prnter Job Auth.: 1/2 ⬍ OK
Entire
Simple(Limitation)
Range

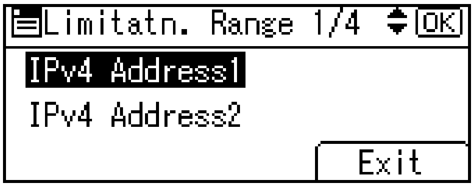
Specify the range in which [Simple (Limitation)] is applied to Printer Job Authentication.

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.**



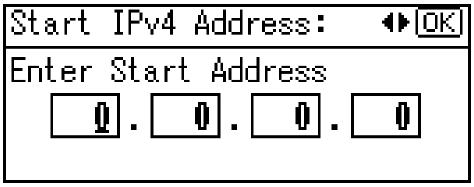
Limitatn. Range 1/4 OK

IPv4 Address1

IPv4 Address2

Exit

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



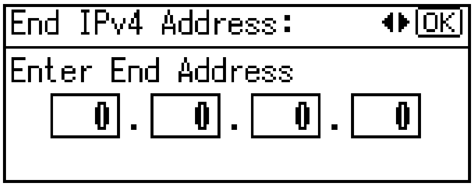
Start IPv4 Address: OK

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

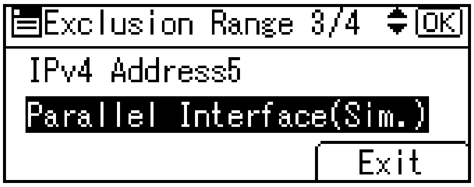
Enter End Address

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.**



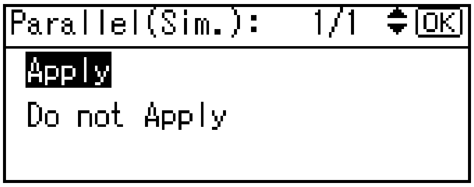
Exclusion Range 3/4 OK

IPv4 Address5

Parallel Interface(Sim.)

Exit

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

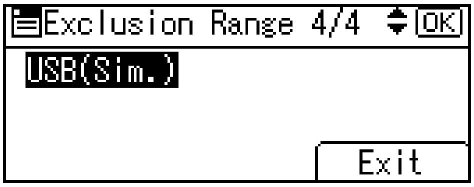


Parallel(Sim.): 1/1 OK

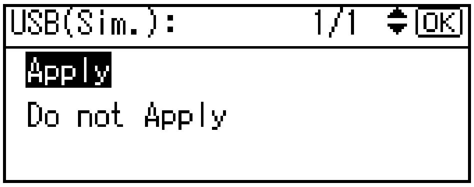
Apply

Do not Apply

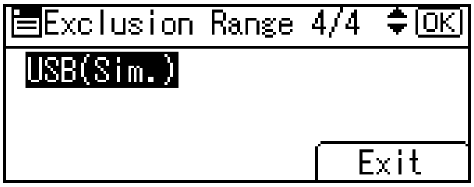
7. Select [USB (Sim.)] using [▲] or [▼], and then press the [OK] key.



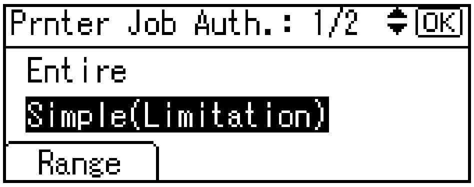
8. Select [Apply] using [▲] or [▼], and then press the [OK] key.



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 RPCS and PCL printer drivers.

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	[Off]
[Printer Job Authentication]	[Simple (All)]	[Simple (All)]	[Entire]	[Entire]	-
[Simple Encryption]	[Off]	[On]	[Off]	[On]	-
Printer Job Type 1	C	C	C	C	A
Printer Job Type 2	B	X	B	X	A
Printer Job Type 3	X	X	X	X	A
Printer Job Type 4	A	A	B	B	A
Printer Job Type 5	A	A	X	X	A
Printer Job Type 6	A	A	X	X	A
Printer Job Type 7	B	B	B	B	A

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.

Printer Job Types

1. In the RPCS printer driver dialog box, the "Confirm authentication information when printing" and "Encrypt" check boxes are selected. In the PCL printer driver dialog box, the "User Authentication" and "Encrypt" check boxes are selected. Personal authentication information is added to the printer job. The printer driver applies advanced encryption to the login passwords. The printer driver encryption key enables driver encryption and prevents the login password from being stolen.

   For details about prohibiting the use of simple encryption using "Restrict Use of Simple Encryption", see "Specifying the Extended Security Functions".

2. In the RPCS printer driver dialog box, the "Confirm authentication information when printing" check box is selected. In the PCL printer driver dialog box, the "User Authentication" and "Encrypt" check boxes are selected. Personal authentication information is added to the printer job. The printer driver applies simple encryption to login passwords.

   For details about turning off "Restrict Use of Simple Encryption" and allowing the use of simple encryption, see "Specifying the Extended Security Functions".

3. In the RPCS printer driver dialog box, the "Confirm authentication information when printing" check box is not selected. In the PCL printer driver dialog box, the "User Authentication" check box is not selected. Personal authentication information is added to the printer job and is disabled.

4. A printer job 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.

5. 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.177 "Specifying the Extended Security Functions"

If User Authentication is Specified

When user authentication (User Code Authentication, Basic Authentication, Windows Authentication, LDAP Authentication, or Integration Server Authentication) is set, the authentication screen is displayed. Unless a valid user name and password are entered, operations are not possible with the machine. Log on to operate the machine, and log off when you are finished operations. Be sure to log off to prevent unauthorized users from using the machine. When auto logout timer is specified, the machine automatically logs you off if you do not use the control panel within a given time. Additionally, you can authenticate using an external device. For details about using an external device for user authentication, see "Authentication Using an External Device".

Note

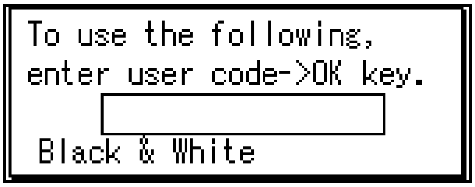
- Consult the User Administrator about your login user name, password, and user code.
- For user code authentication, enter a number registered in the Address Book as [User Code].

Reference

- p.96 "Authentication Using an External Device"

User Code Authentication (Using the Control Panel)

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



```
To use the following,
enter user code->OK key.

 Black & White
```

Enter a user code (up to 8 digits), and then press the [OK] key.

Note

- To log off, do one of the following:
    - Press the Operation switch.
    - Press the [Energy Saver] key after jobs are completed.
    - Press the [Clear/Stop] key and the [Reset] key at the same time.

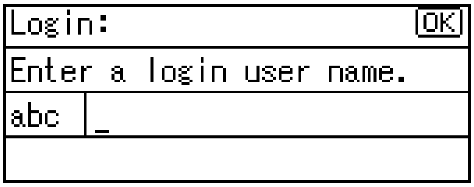
User Code Authentication (Using a Printer Driver)

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

Login (Using the Control Panel)

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

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

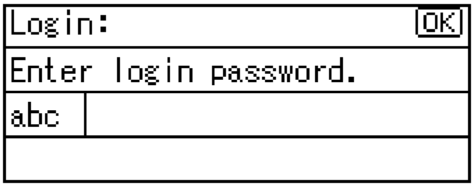


Login: OK

Enter a login user name.

abc _

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



Login: OK

Enter login password.

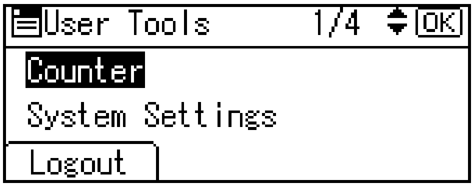
abc

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

Log Off (Using the Control Panel)

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

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



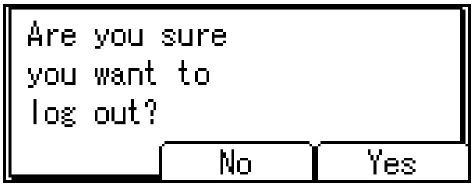
User Tools 1/4 ⇕ OK

Counter

System Settings

Logout

3. **Press [Yes].**



Are you sure you want to log out?

No Yes

Login (Using a Printer Driver)

When Basic Authentication, Windows Authentication, or LDAP 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.

Login (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].

Log Off (Using Web Image Monitor)

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

Note

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

User Lockout Function

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

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

Lockout setting items

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

Setting Item	Description	Setting Values	Default Setting
Lockout	Specify whether or not to enable the lockout function.	• Active • Inactive	• Inactive
Number of Attempts Before Lockout	Specify the number of authentication attempts to allow before applying lockout.	1-10	5
Lockout Release Timer	Specify whether or not to cancel lockout after a specified period elapses.	• Active • Inactive	• Inactive
Lock Out User for	Specify the number of minutes after which lockout is canceled.	1-9999 min.	60 min.

Lockout release privileges

Administrators with unlocking privileges are as follows.

Locked out User	Unlocking administrator
general user	user administrator
user administrator, network administrator, file administrator, machine administrator	supervisor
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 "Cancel Lockout" check box under "Authentication Information".**
8. **Click [OK].**
9. **Click [Logout].**

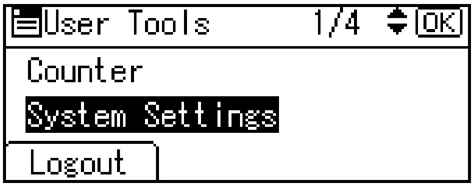
Auto Logout

This can be specified by the machine administrator.

When using user authentication management, 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.

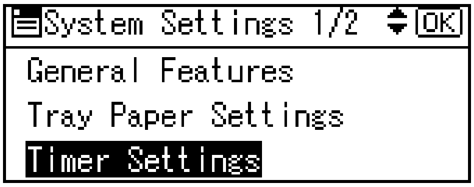
For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

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



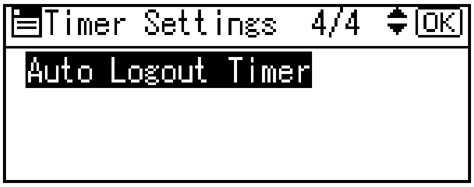
User Tools 1/4 ⬍ OK
Counter
System Settings
Logout

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



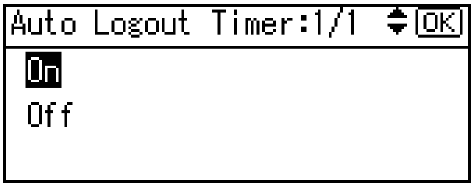
System Settings 1/2 ⬍ OK
General Features
Tray Paper Settings
Timer Settings

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



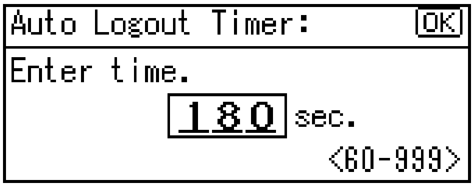
Timer Settings 4/4 ⬍ OK
Auto Logout Timer

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



Auto Logout Timer:1/1 ⬍ OK
On
Off

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



```
Auto Logout Timer:      [OK]
Enter time.
            180 sec.
                 <60-999>
```

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.30 "Logging on Using Administrator Authentication"
- p.31 "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 Document Data Information from Leaks

This chapter describes how to protect document data and information transmitted through the network from unauthorized viewing and modification.

Preventing Unauthorized Copying

In Printer Features, using the printer driver, you can embed a pattern in the printed copy to discourage or prevent unauthorized copying.

The unauthorized copy prevention function prevents unauthorized copies of documents by embedding a text pattern (for instance, a warning such as "No Copying") that you can set on the print driver (which will appear on printed copies).

Data security for copying prevents document information leaks by graying out copies of documents that were printed with the data security for copying pattern enabled in the printer driver.

However, in order to gray out the security pattern, the Copy Data Security Unit is required for the copier or multi-function printer.

For more information, see the information below.

Unauthorized Copy Prevention

1. Using the printer driver, specify the printer settings for unauthorized copy prevention. For details on how to specify settings for unauthorized copy prevention, see "Specifying Printer Settings for Unauthorized Copy Prevention (Printer Driver Setting)".

Data Security for Copying

1. Using the printer driver, specify the printer settings for data security for copying. For details on how to specify settings on the printer driver, see "Specifying Printer Settings for Data Security for Copying (Printer Driver Setting)".
2. Set the data security for copying function to appear gray when documents with the function are copied or scanned. For details on how to specify settings on the machine, see "Specifying Data Security for Copying (Machine Setting)".

Reference

- p.101 "Specifying Printer Settings for Unauthorized Copy Prevention (Printer Driver Setting)"
- p.101 "Specifying Printer Settings for Data Security for Copying (Printer Driver Setting)"
- p.102 "Specifying Data Security for Copying (Machine Setting)"

Unauthorized Copy Prevention

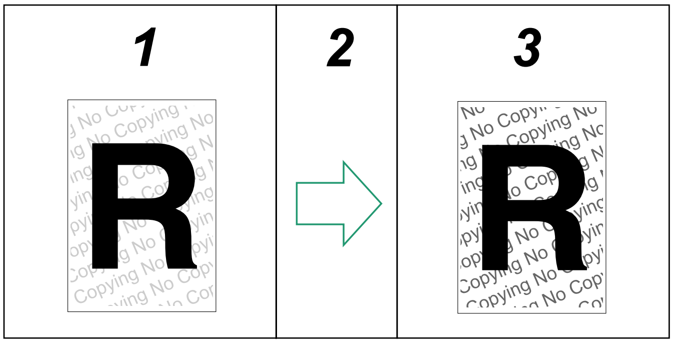
Using the printer driver, you can embed mask and pattern (for instance, a warning such as "No Copying") in the printed document.

If the document is copied, faxed or scanned by a copier or multifunction printer, the embedded pattern appears clearly on the copy, discouraging unauthorized copying.

To use the printer function when User Authentication is enabled, you must enter the login user name and password for the printer driver. For details, see the printer driver Help.

Important

- **Unauthorized copy prevention discourages unauthorized copying, but will not necessarily stop information leaks.**
- **The embedded pattern cannot be guaranteed to be copied, faxed or scanned properly.**
- **Depending on the machine and scanner settings, the embedded pattern may not be copied, scanned or faxed.**



1. **Printed Documents**

   Using the printer driver, you can embed background images and pattern in a printed document for Unauthorized Copy Prevention.

2. **The document is copied, faxed or scanned.**
3. **Printed Copies**

   The embedded pattern (for instance, a warning such as "No Copying") in a printed document appears clearly in printed copies.

Note

- To make the embedded pattern clear, set the character size to at least 50 pt (preferably 70 to 80 pt) and character angle to between 30 and 40 degrees.

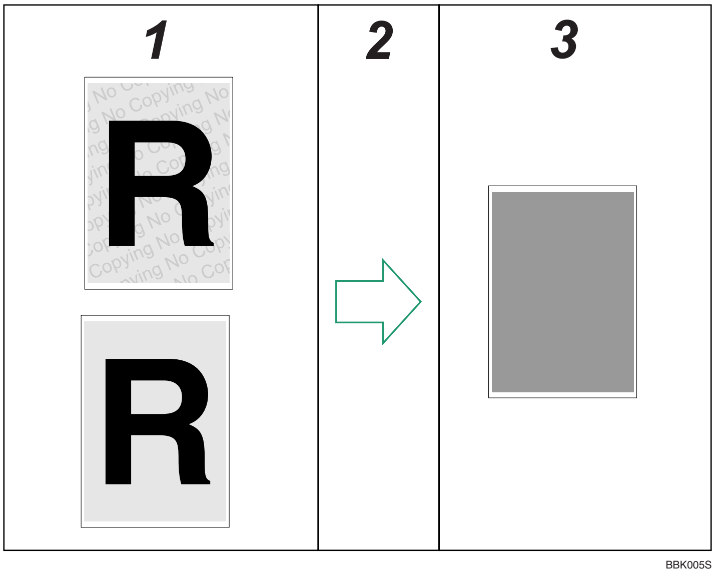
Data Security for Copying

Using the printer driver to enable the data security for copying function, you can print a document with an embedded pattern of hidden text. Such a document is called a data security for copying document.

If a data security for copying document is copied using a copier or multi-function printer with the Copy Data Security Unit, protected pages are grayed out in the copy, preventing confidential information from being copied. Also if a document with embedded pattern is detected, the machine beeps. An unauthorized copy log is also stored. To gray out copies of data security for copying documents when they are copied, faxed or scanned, the optional Copy Data Security Unit must be installed in the machine.

Important

- **If a document with embedded pattern for data security for copying is copied, faxed or scanned by a copier or multi-function printer without the Copy Data Security Unit, the embedded pattern appears conspicuously in the copy. However, character relief may differ depending on the copier or multifunction printer model in use or document scan setting.**
- **The machine does not beep with a data security for copying document is detected while using the network TWAIN scanner.**



1. **Documents with data security for copying**
2. **The document is copied, faxed or scanned.**
3. **Printed Copies**

   Text and images in the document are grayed out in printed copies.

Note

- You can also embed pattern in a document protected by data security for copying. However, if such a document is copied using a copier or multi-function printer with the Copy Data Security Unit, the copy is grayed out, so the embedded pattern does not appear on the copy.
- If misdetection occurs, contact your service representative.
- If a document with embedded pattern for data security for copying is copied, faxed or scanned using a copier or multi-function printer without the Copy Data Security Unit, the embedded pattern appears clearly on the copy.
- If a data security for copying document is detected, the machine beeps.
- If the scanned data security for copying document is registered as a user stamp, the machine does not beep. The file registered as a user stamp is grayed out, and no entry is added to the unauthorized copying log.

Printing Limitations

The following is a list of limitations on printing with unauthorized copy prevention and data security for copying.

Unauthorized copy prevention / Data security for copying

You can print using only the RPCS printer driver.

You cannot print at 200 dpi resolution.

You cannot partially embed pattern in the printed document.

You can only embed pattern that is entered in the text box of the printer driver.

Printing with embedding takes longer than normal printing.

Data security for copying Only

Select 182 × 257 mm / 7.2 × 10.1 inches or larger as the paper size.

Select a paper type of Plain or Recycled with a brightness of 70% or more.

If you select Duplex, the data security for copying function may not work properly due to printing on the back of sheets.

Notice

1. The supplier does not guarantee that unauthorized copy prevention and data security for copying will always work. Depending on the paper, the model of the copier or multi-function printer, and the copier or printer settings, unauthorized copy prevention and data security for copying may not work properly.

2. The supplier is not liable for any damage caused by using or not being able to use unauthorized copy prevention and data security for copying.

Printing with Unauthorized Copy Prevention and Data Security for Copying

This section describes Printing with Unauthorized Copy Prevention and Data Security for Copying.

Specifying Printer Settings for Unauthorized Copy Prevention (Printer Driver Setting)

Using the printer driver, specify the printer settings for unauthorized copy prevention.

To use the printer function when User Authentication is enabled, you must enter the login user name and password for the printer driver. For details about logging in, see the printer driver Help.

For details about specifying data security for copying using the printer driver, see the printer driver Help.

1. **Open the printer driver dialog box.**
2. **On the Edit tab, select the [Unauthorized copy...] check box.**
3. **Click [Control Settings...].**
4. **In the text box in the [Unauthorized copy prevention: Pattern] group, enter the text to be embedded in the printed document.**

   Also, specify [Font:], [Font style:], and Size.
5. **Click [OK].**

Specifying Printer Settings for Data Security for Copying (Printer Driver Setting)

If a printed document using this function is copied by a copier or multi-function printer, the copy is grayed out.

Using the printer driver, specify the printer settings for data security for copying.

To use the printer function when User Authentication is enabled, you must enter the login user name and password for the printer driver. For details about logging in, see the printer driver Help.

For details about specifying data security for copying using the printer driver, see the printer driver Help.

1. **Open the printer driver dialog box.**
2. **On the Edit tab, select the "Unauthorized copy..." check box.**
3. **Click [Control Settings...].**
4. **Check the [Data security for copying] check box in the [Unauthorized copy prevention: Pattern] group.**
5. **Click [OK].**

Specifying Data Security for Copying (Machine Setting)

This can be specified by the machine administrator.

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

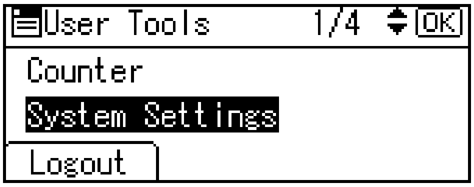
To use this function, the Copy Data Security Unit must be installed.

If a document printed is copied, faxed or scanned, the copy is grayed out.

Important

- **If a document that is not copy-guarded is copied, faxed or scanned, the copy or stored file is not grayed out.**

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



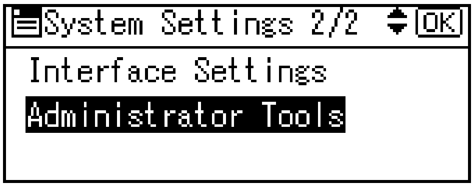
User Tools 1/4 ⇕ OK

Counter

System Settings

Logout

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

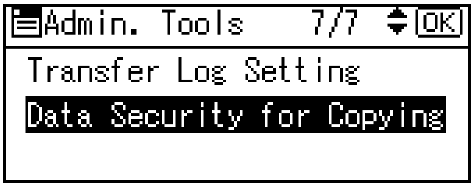


System Settings 2/2 ⇕ OK

Interface Settings

Administrator Tools

4. **Select [Data Security for Copying] using [▲] or [▼], and then press the [OK] key.**



Admin. Tools 7/7 ⇕ OK

Transfer Log Setting

Data Security for Copying

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

   If you do not want to specify [Data Security for Copying], select [Off].

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

Reference

- p.30 "Logging on Using Administrator Authentication"
- p.31 "Logging off Using Administrator Authentication"

Preventing Data Leaks 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.

Restrictions on Destinations

This can be specified by the user administrator.

Make the setting to disable the direct entry of phone numbers under the fax functions.

By making this setting, the destinations are restricted to addresses registered in the Address Book.

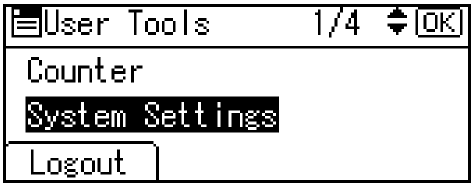
If you set "Restrict Use of Destinations" to [On], you can prohibit users from directly entering telephone numbers in order to send files. If you set "Restrict Use of Destinations" to [Off], "Restrict Adding of User Destinations" appears. In "Restrict Adding of User Destinations", you can restrict users from registering data in the Address Book.

If you set "Restrict Adding of User Destinations" to [Off], users can directly enter destination telephone numbers in "Program Dest." on the fax screens. If you set "Restrict Adding of User Destinations" to [On], users can specify destinations directly, but cannot use "Program Dest." to register data in the Address Book. When this setting is made, only the user administrator can change the Address Book. "Restrict Use of Destinations" and "Restrict Adding of User Destinations" are extended security functions. For more information about these and the extended security functions, see "Specifying the Extended Security Functions".

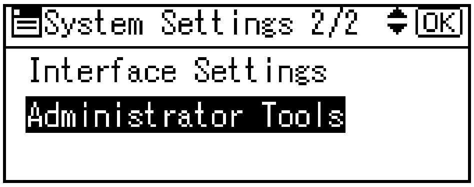
"Restrictions on Destinations" can also be specified using Web Image Monitor or SmartDeviceMonitor for Admin. For details, see the Help for these applications.

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.**

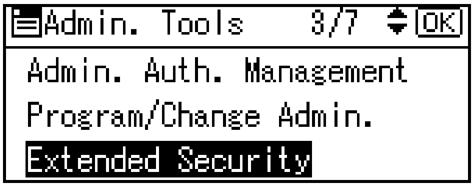


3. Select [Administrator Tools] using [▲] or [▼], and then press the [OK] key.



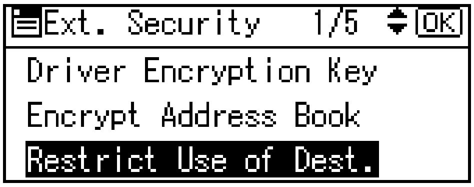
```
System Settings 2/2  ⬍ OK
 Interface Settings
 Administrator Tools
```

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



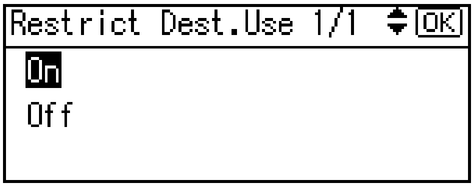
```
Admin. Tools     3/7  ⬍ OK
 Admin. Auth. Management
 Program/Change Admin.
 Extended Security
```

5. Select [Restrict Use of Dest.] using [▲] or [▼], and then press the [OK] key.



```
Ext. Security    1/5  ⬍ OK
 Driver Encryption Key
 Encrypt Address Book
 Restrict Use of Dest.
```

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



```
Restrict Dest.Use 1/1 ⬍ OK
 On
 Off
```

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

Reference

- p.177 "Specifying the Extended Security Functions"
- p.30 "Logging on Using Administrator Authentication"
- p.31 "Logging off Using Administrator Authentication"

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.

Address Book Access Permission

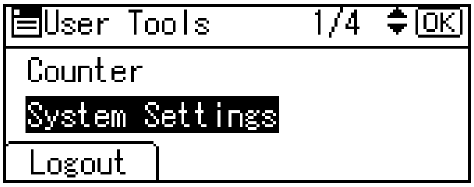
This can be specified by the registered user. Access permission can also be specified by a user granted full control or the user administrator.

You can specify who is allowed to access the data in the Address Book.

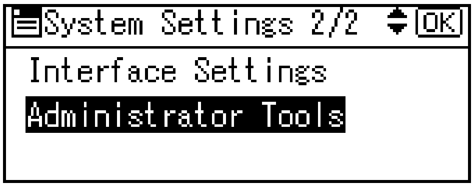
By making this setting, you can prevent the data in the Address Book being used by unregistered users.

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

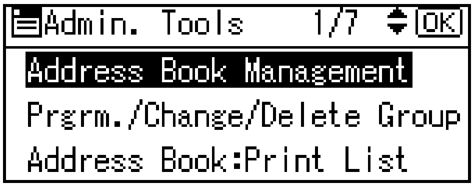
1. **Press the [User Tools/Counter] key.**
2. **Select [System Settings] using [▲] or [▼], and then press the [OK] key.**



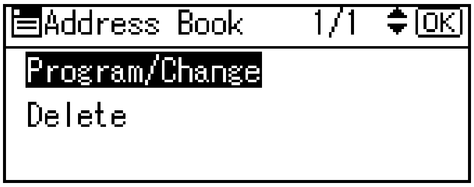
3. **Select [Administrator Tools] using [▲] or [▼], and then press the [OK] key.**



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.**

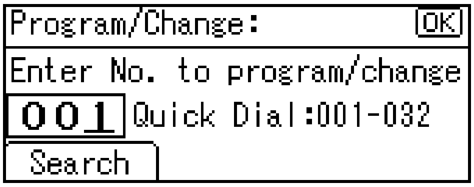


Address Book 1/1 ⇕ OK

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

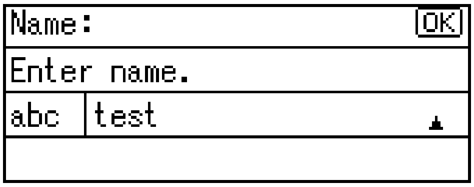
Enter No. to program/change

001 Quick Dial:001-032

Search

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

7. **Press the [OK] key.**

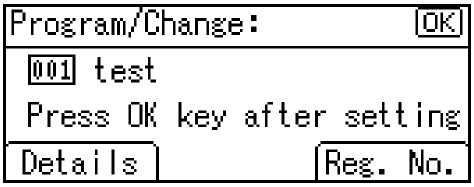


Name: OK

Enter name.

abc test

8. **Press [Details].**



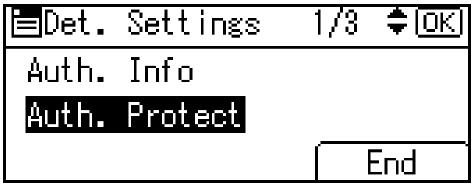
Program/Change: OK

001 test

Press OK key after setting

Details Reg. No.

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



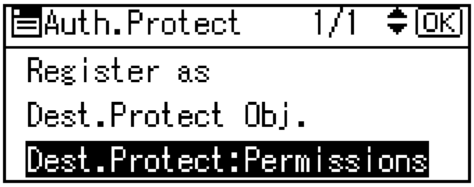
Det. Settings 1/3 ⇕ OK

Auth. Info

Auth. Protect

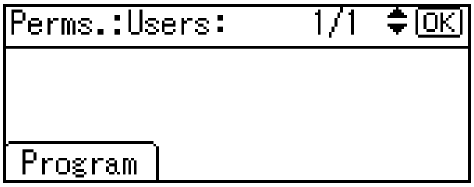
End

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].**

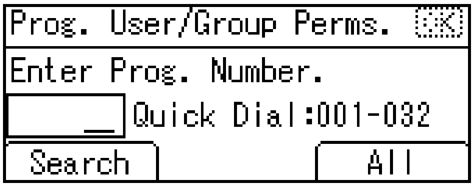


```
Perms.:Users:     1/1 ⇕ OK



 Program
```

12. **Select the users or groups to register.**

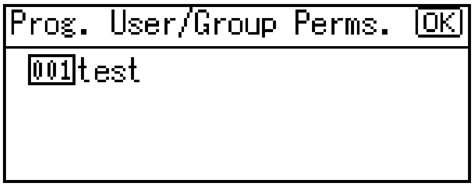


```
Prog. User/Group Perms. OK
Enter Prog. Number.
    _ Quick Dial:001-032
 Search              All
```

You can select more than one user.

By pressing [All], you can select all the users.

13. **Press the [OK] key.**

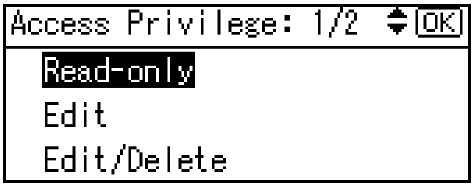


```
Prog. User/Group Perms. OK
 001 test
```

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.



```
Access Privilege: 1/2 ⇕ OK
  Read-only
  Edit
  Edit/Delete
```

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

Reference

- p.30 "Logging on Using Administrator Authentication"
- p.31 "Logging off Using Administrator Authentication"

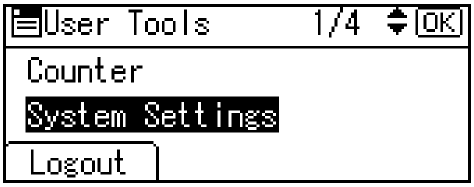
Encrypting Data in the Address Book

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".

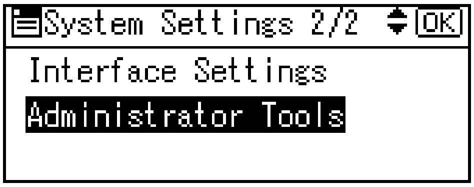
For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

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



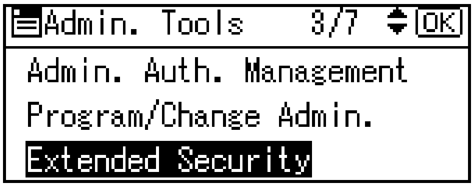
User Tools 1/4 ⬍ OK
Counter
System Settings
Logout

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



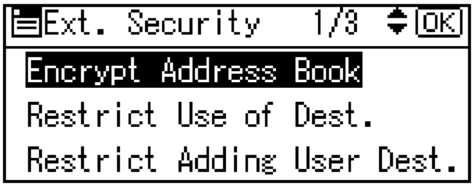
System Settings 2/2 ⬍ OK
Interface Settings
Administrator Tools

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



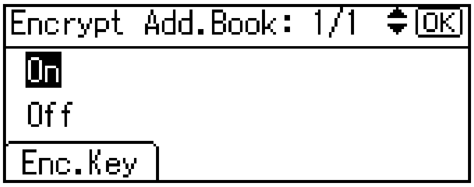
Admin. Tools 3/7 ⬍ OK
Admin. Auth. Management
Program/Change Admin.
Extended Security

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



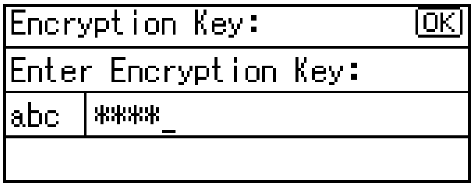
```
Ext. Security    1/3 ⇕ OK
Encrypt Address Book
Restrict Use of Dest.
Restrict Adding User Dest.
```

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



```
Encrypt Add.Book: 1/1 ⇕ OK
On
Off
Enc.Key
```

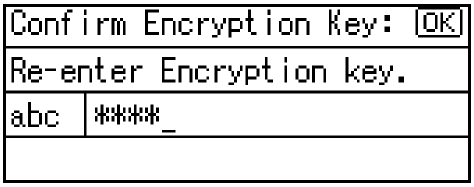
7. **Enter the encryption key, and then press the [OK] key.**



```
Encryption Key:          OK
Enter Encryption Key:
abc  ****_
```

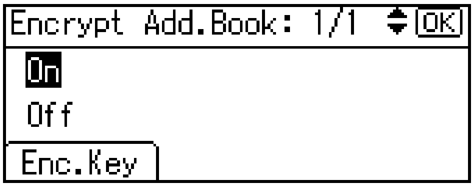
Enter the encryption key using up to 32 alphanumeric characters.

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



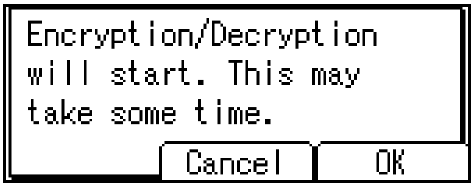
```
Confirm Encryption Key:  OK
Re-enter Encryption key.
abc  ****_
```

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



```
Encrypt Add.Book: 1/1 ⇕ OK
On
Off
Enc.Key
```

10. **Press [OK].**



```
Encryption/Decryption
will start. This may
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.

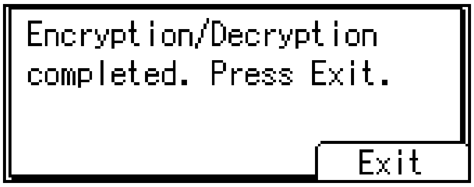
The machine cannot be used during encryption.

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 completed. Press 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.30 "Logging on Using Administrator Authentication"
- p.31 "Logging off Using Administrator Authentication"
- p.177 "Specifying the Extended Security Functions"

5. Managing Access to the Machine

This chapter describes how to prevent unauthorized access to and modification of the machine's settings.

Preventing Modification of 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 [Admin. Auth. management], [Items], 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
- Facsimile Features
- Printer 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.26 "Registering the Administrator"
- p.211 "User Administrator Settings"
- p.200 "Machine Administrator Settings"
- p.207 "Network Administrator Settings"
- p.210 "File Administrator Settings"
- p.215 "User Settings - Control Panel Settings"
- p.226 "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.215 "User Settings - Control Panel Settings"
- p.226 "User Settings - Web Image Monitor Settings"

Set up 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".

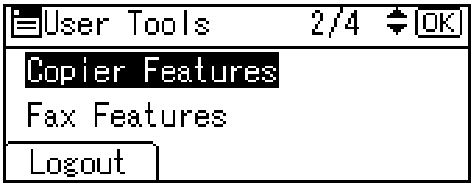
Reference

- p.30 "Logging on Using Administrator Authentication"
- p.31 "Logging off Using Administrator Authentication"

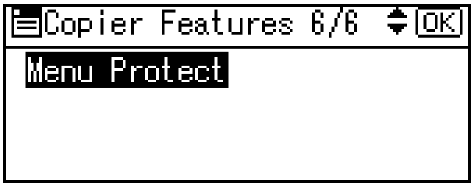
Copying Functions

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.**



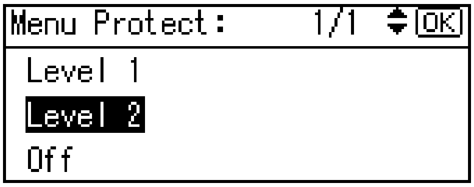
3. **Select [Menu Protect] using [▲] or [▼], and then press the [OK] key.**



Copier Features 6/6 ⬍ OK

Menu Protect

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



Menu Protect: 1/1 ⬍ OK

Level 1

Level 2

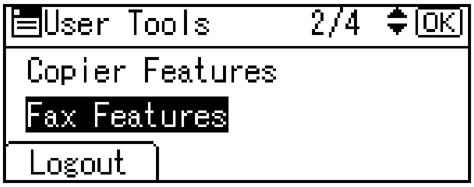
Off

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

Fax Functions

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.**



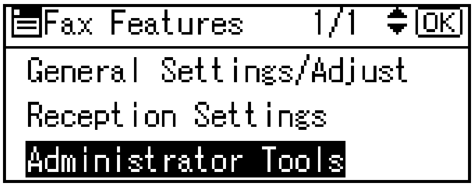
User Tools 2/4 ⬍ OK

Copier Features

Fax Features

Logout

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



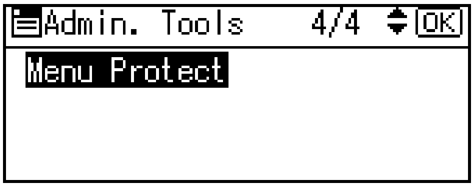
Fax Features 1/1 ⬍ OK

General Settings/Adjust

Reception Settings

Administrator Tools

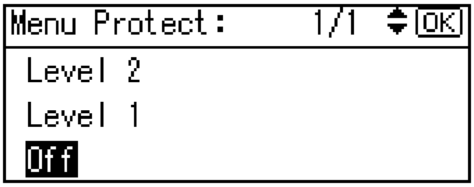
4. **Select [Menu Protect] using [▲] or [▼], and then press the [OK] key.**



Admin. Tools 4/4 ⬍ OK

Menu Protect

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

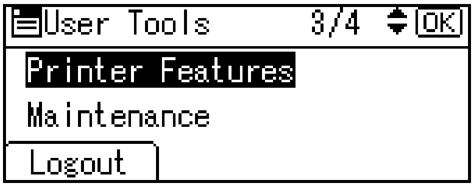


6. **Press the [User Tools/Counter] key.**

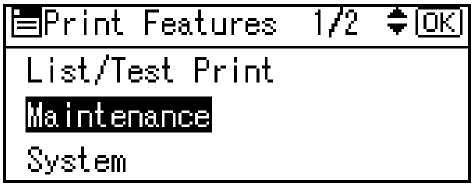
Printer Functions

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

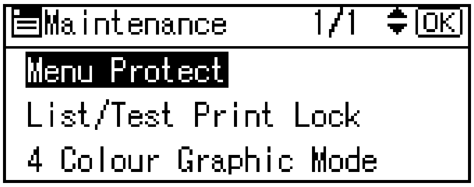
1. **Press the [User Tools/Counter] key.**
2. **Select [Printer Features] using [▲] or [▼], and then press the [OK] key.**



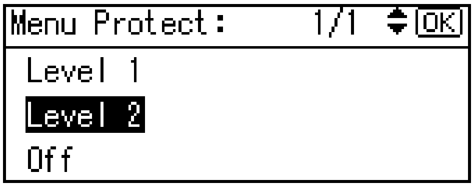
3. **Select [Maintenance] using [▲] or [▼], and then press the [OK] key.**



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.**

Limiting Available Functions

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

Available Functions

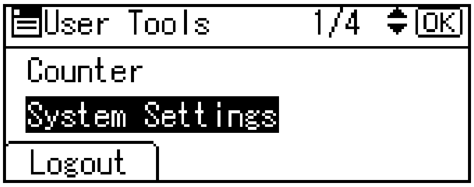
Specify the available functions from the copier, fax, scanner, and printer functions.

Specifying Which Functions are Available

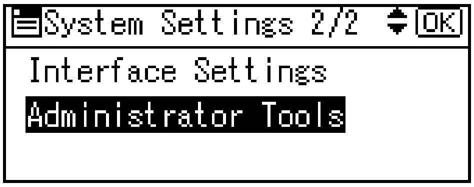
This can be specified by the user administrator. Specify the functions available to registered users. By making this setting, you can limit the functions available to users.

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

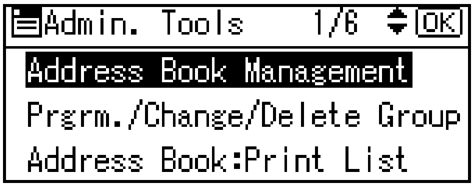
1. **Press the [User Tools/Counter] key.**
2. **Select [System Settings] using [▲] or [▼], and then press the [OK] key.**



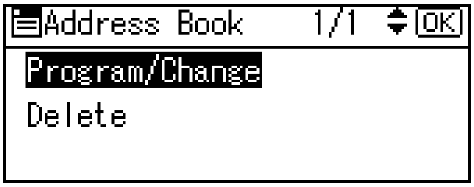
3. **Select [Administrator Tools] using [▲] or [▼], and then press the [OK] key.**



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.**

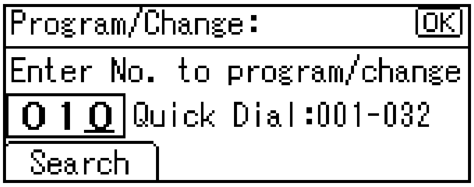


Address Book 1/1 ⬍ OK

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

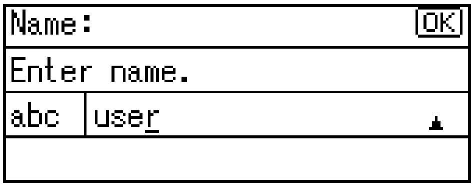
Enter No. to program/change

010 Quick Dial:001-032

Search

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

7. **Press the [OK] key.**

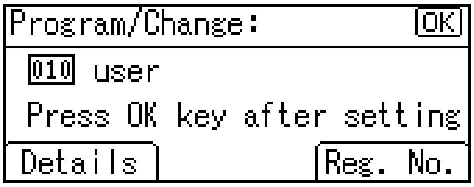


Name: OK

Enter name.

abc user

8. **Press [Details].**



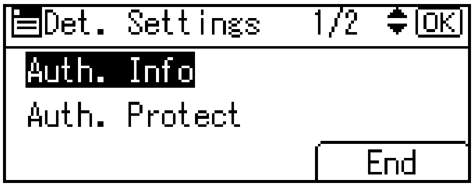
Program/Change: OK

010 user

Press OK key after setting

Details Reg. No.

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



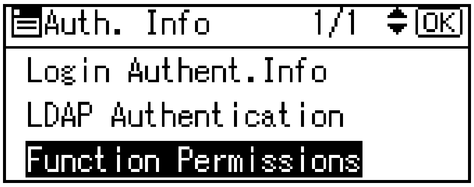
Det. Settings 1/2 ⬍ OK

Auth. Info

Auth. Protect

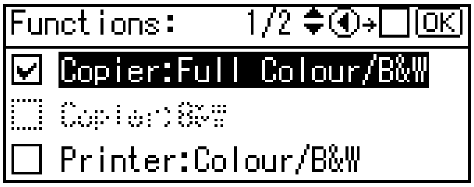
End

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



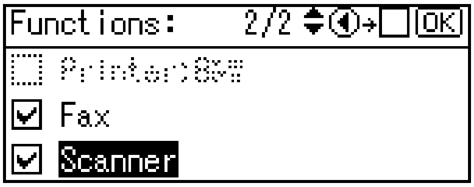
```
Auth. Info          1/1  ⇕[OK]
 Login Authent.Info
 LDAP Authentication
 Function Permissions
```

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



```
Functions:     1/2 ⇕◀▶□[OK]
☑ Copier:Full Colour/B&W
⬚ Copier:B&W
□ Printer:Colour/B&W
```

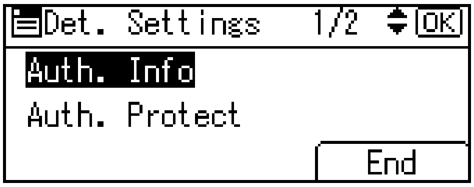
12. Press the [OK] key.



```
Functions:     2/2 ⇕◀▶□[OK]
⬚ Printer:B&W
☑ Fax
☑ Scanner
```

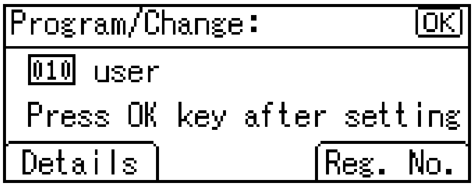
13. Press the [Escape] key.

14. Press [End].



```
Det. Settings       1/2  ⇕[OK]
 Auth. Info
 Auth. Protect
                     End
```

15. Press the [OK] key.



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

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

Reference

- p.30 "Logging on Using Administrator Authentication"
- p.31 "Logging off Using Administrator Authentication"

Managing Log Files

1. Log information

   To view the log, Web SmartDeviceMonitor is required.

   The following log information is stored in the machine's memory:

   - Job log

     Stores information about user file-related activities, such as copying, printing, sending and receiving faxes, and sending scanned files.

   - Access log

     Stores information about access, such as logging on and off, creating and deleting files, scanning invalid images, administrator procedures, changing the Date/Time using SNTP, and service representative procedures.

     Administrator procedures include changing the Date/Time settings, changing the Job Log function settings, changing the Access Log function settings, deleting all log information, and changing the Log Encryption settings.

     Service representative procedures include specifying whether or not to store job logs and access logs, and restoring encryption key.

2. Deleting log information

   By deleting the log stored in the machine, you can free up space on the hard disk.

3. Transferring log information

   You can transfer the log information, which indicates who tried to gain access and at what time.

   By transferring the log files, you can check the history data and identify unauthorized access.

Using the Control Panel to Specify Log File Settings

Transfer Log Setting

The machine administrator can select [On] from the log server only.

When using the machine's control panel, you can change the setting to [Off] only if it is set to [On].

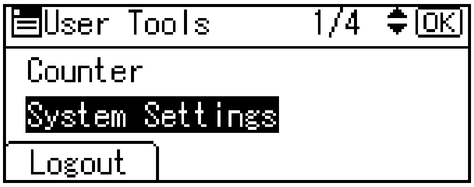
You can check and change the transfer log setting. This setting lets you transfer log files to the log server to check the history data and identify unauthorized access.

For details about Web SmartDeviceMonitor, contact your sales representative.

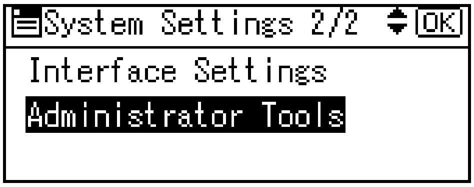
For details about the transfer log setting, see Web SmartDeviceMonitor manual.

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

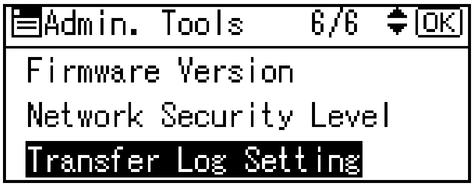
1. **Press the [User Tools/Counter] key.**
2. **Select [System Settings] using [▲] or [▼], and then press the [OK] key.**



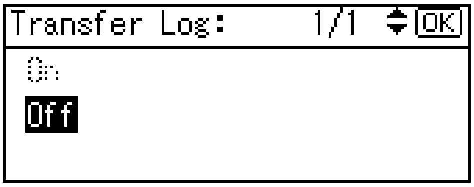
3. **Select [Administrator Tools] using [▲] or [▼], and then press the [OK] key.**



4. **Select [Transfer Log Setting] 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.**

Reference

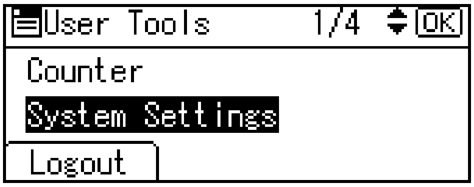
- p.30 "Logging on Using Administrator Authentication"
- p.31 "Logging off Using Administrator Authentication"

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".

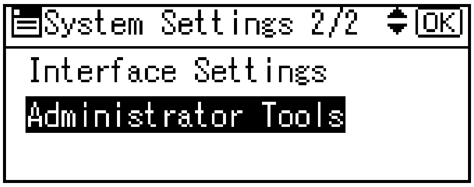
To delete all logs from the control panel, you must use Web SmartDeviceMonitor or enable the Job Log or Access Log collection settings using Web Image Monitor first.

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



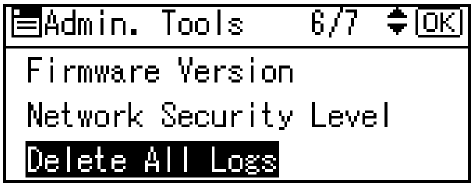
User Tools 1/4 ⇕ OK
Counter
System Settings
Logout

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



System Settings 2/2 ⇕ OK
Interface Settings
Administrator Tools

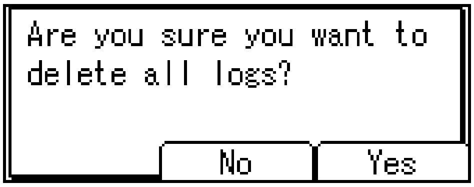
4. **Select [Delete All Logs] using [▲] or [▼], and then press the [OK] key.**



Admin. Tools 6/7 ⇕ OK
Firmware Version
Network Security Level
Delete All Logs

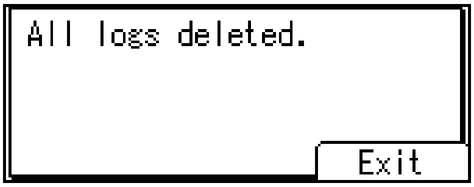
A confirmation screen appears.

5. **Press [Yes].**



Are you sure you want to delete all logs?
No Yes

6. **Press [Exit].**



All logs deleted.
Exit

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

Reference

- p.30 "Logging on Using Administrator Authentication"
- p.31 "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 type of log recording and collection level on the control panel, perform log encryption and also delete all logs.

Reference

- p.30 "Logging on Using Administrator Authentication"
- p.31 "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 Settings Listed by Function Type" or "Access Log Collect Settings Listed by Function Type" vary depending on the collection level selected.

   If you change the setting in the list, the setting for [Job Log Collect Level] or [Access Log Collect Level] automatically changes to [User Settings].
7. **Click [OK].**

   Changes are also reflected in related log settings.
8. **Click [Logout].**

Note

- The greater the Access Log Collect setting value, the more logs are collected.

Transfer Logs

Select to disable log transfer.

When log transfer is inactive, [Inactive] is displayed and this setting cannot be changed. When log transfer is active, log records can be transferred to the log collection system.

1. **Follow steps 1 to 4 in "Specify Log Collect Settings".**
2. **Select [Inactive] under "Transfer Logs".**
3. **Click [OK].**
4. **Click [Logout].**

Encrypt Logs

1. **Follow steps 1 to 4 in "Specify Log Collect Settings ".**
2. **Select [Active] under "Encrypt Logs."**

   To disable log encryption, select [Inactive].
3. **Click [OK].**

   The log is encrypted. If other changes have been made in related log settings, they will occur at the same time.
4. **Click [Logout].**

Note

- In order to enable encryption, either [Collect Job Logs] or [Collect Access Logs], or both must be set to [Active].

Delete All Logs

1. **Follow steps 1 to 4 in " Specify Log Collect Settings ".**
2. **Click [Delete] under "Delete All Logs".**
3. **Click [OK].**

   All job logs and device access log records are cleared.
4. **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].

6. 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), 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/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 Guide.

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	Disabled Condition
IPv4	-	• Control Panel • Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Web SmartDeviceMonitor	All applications that operate over IPv4 cannot be used. IPv4 cannot be disabled from Web Image Monitor when using IPv4 transmission.
IPv6	-	• Control Panel • Web Image Monitor • SmartDeviceMonitor for Admin • Web SmartDeviceMonitor	All applications that operate over IPv6 cannot be used.
IPsec	-	• Control Panel • Web Image Monitor • telnet	Encrypted transmission using IPsec is disabled.
FTP	TCP:21	• Web Image Monitor • telnet	Functions that require FTP cannot be used.

Protocol	Port	Setting Method	Disabled Condition
		• SmartDeviceMonitor for Admin • Web SmartDeviceMonitor	You can restrict personal information from being displayed by making settings on the control panel using "Restrict Display of User Information". * 1
sshd/sftpd	TCP:22	• Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Web SmartDeviceMonitor	Functions that require sftp cannot be used. You can restrict personal information from being displayed by making settings on the control panel using "Restrict Display of User Information". * 1
telnet	TCP:23	• Web Image Monitor	Commands using telnet are disabled.
HTTP	TCP:80	• Web Image Monitor • telnet	Functions that require HTTP cannot be used. Cannot print using IPP on port 80.
HTTPS	TCP:443	• Web Image Monitor • telnet	Functions that require HTTPS cannot be used. @Remote cannot be used. You can also make settings to require SSL transmission using the control panel or Web Image Monitor.
SMB	TCP:139	• Control Panel • Web Image Monitor • telnet • SmartDeviceMonitor for Admin	SMB printing functions cannot be used.

Protocol	Port	Setting Method	Disabled Condition
		• Web SmartDeviceMonitor	
NBT	UDP:137 UDP:138	• telnet	SMB printing functions via TCP/IP, as well as NetBIOS designated functions on the WINS server cannot be used.
SNMPv1,v2	UDP:161	• Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Web SmartDeviceMonitor	Functions that require SNMPv1, v2 cannot be used. Using the control panel, Web Image Monitor or telnet, you can specify that SNMPv1, v2 settings are read-only, and cannot be edited.
SNMPv3	UDP:161	• Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Web SmartDeviceMonitor	Functions that require SNMPv3 cannot be used. You can also make settings to require SNMPv3 encrypted transmission and restrict the use of other transmission methods using the control panel, Web Image Monitor, or telnet.
RSH/RCP	TCP:514	• Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Web SmartDeviceMonitor	Functions that require RSH and network TWAIN functions cannot be used. You can restrict personal information from being displayed by making settings on the control panel using

Protocol	Port	Setting Method	Disabled Condition
			"Restrict Display of User Information".*1
LPR	TCP:515	• Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Web SmartDeviceMonitor	LPR functions cannot be used. You can restrict personal information from being displayed by making settings on the control panel using "Restrict Display of User Information".*1
IPP	TCP:631	• Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Web SmartDeviceMonitor	IPP functions cannot be used.
SSDP	UDP:1900	• Web Image Monitor • telnet	Device discovery using UPnP from Windows cannot be used.
Bonjour	UDP:5353	• Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Web SmartDeviceMonitor	Bonjour functions cannot be used.
@Remote	TCP:7443 TCP:7444	• telnet	@Remote cannot be used.
DIPRINT	TCP:9100	• Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Web SmartDeviceMonitor	DIPRINT functions cannot be used.

Protocol	Port	Setting Method	Disabled Condition
RFU	TCP:10021	• telnet	You can attempt to update firmware via FTP.
NetWare	(IPX/SPX)	• Control Panel • Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Web SmartDeviceMonitor	Cannot print with NetWare. SNMP over IPX cannot be used.
WSD (Device)	TCP:53000 (variable)	• Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Web SmartDeviceMonitor	WSD (Device) functions cannot be used.
WSD (Printer)	TCP:53001 (variable)	• Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Web SmartDeviceMonitor	WSD (Printer) functions cannot be used.
WS-Discovery	UDP/TCP:3702	• Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Web SmartDeviceMonitor	WSD (Device, Printer) search function cannot be used.
RHPP	TCP:59100	• Web Image Monitor • telnet	Cannot print with RHPP.

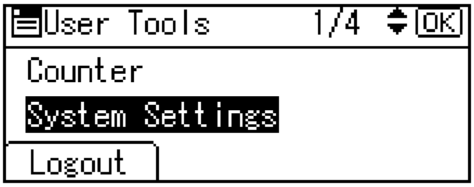
*1 "Restrict Display of User Information" is one of the Extended Security features. For details about making this setting, see "Specifying the Extended Security Functions".

Reference

- p.177 "Specifying the Extended Security Functions"
- p.30 "Logging on Using Administrator Authentication"
- p.31 "Logging off Using Administrator Authentication"

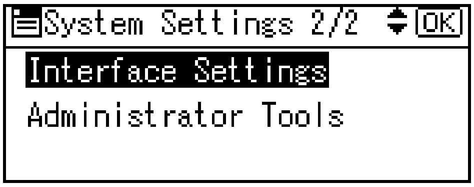
Making Settings Using the Control Panel

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



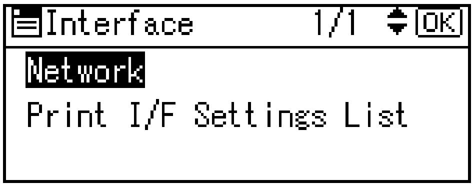
```
User Tools          1/4  ⇕ OK
 Counter
 System Settings
 Logout
```

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



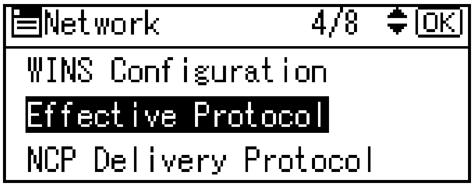
```
System Settings 2/2  ⇕ OK
 Interface Settings
 Administrator Tools
```

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



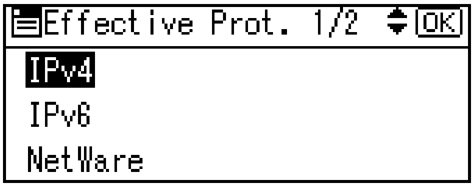
```
Interface           1/1  ⇕ OK
 Network
 Print I/F Settings List
```

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



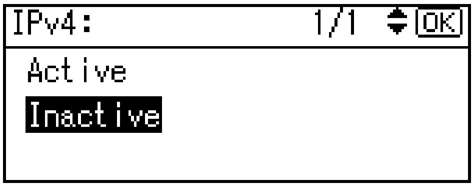
```
Network             4/8  ⇕ OK
 WINS Configuration
 Effective Protocol
 NCP Delivery Protocol
```

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



```
Effective Prot.  1/2  ⬍ OK
 IPv4
 IPv6
 NetWare
```

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



```
IPv4:            1/1  ⬍ OK
 Active
 Inactive
```

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

Making Settings 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

- For details about how to configure telnet, see "Using telnet", Network and System 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.

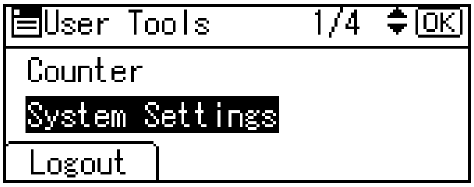
For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

Reference

- p.30 "Logging on Using Administrator Authentication"
- p.31 "Logging off Using Administrator Authentication"

Making Settings Using the Control Panel

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



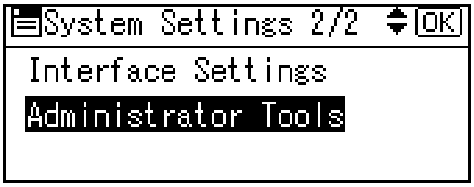
User Tools 1/4 ⇕ OK

Counter

System Settings

Logout

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

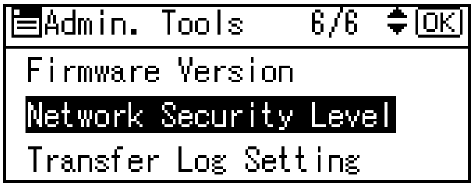


System Settings 2/2 ⇕ OK

Interface Settings

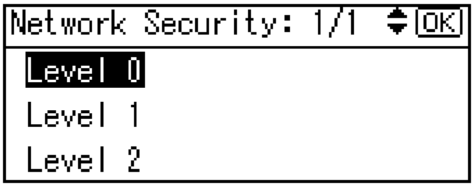
Administrator Tools

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



```
Admin. Tools     6/6  ⇕ OK
 Firmware Version
 Network Security Level
 Transfer Log Setting
```

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



```
Network Security: 1/1 ⇕ OK
 Level 0
 Level 1
 Level 2
```

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

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

Reference

- p.30 "Logging on Using Administrator Authentication"
- p.31 "Logging off Using Administrator Authentication"

Making Settings 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
RHPP	Active	Active	Inactive

Tab Name:NetWare

Function	Level 0	Level 1	Level 2
NetWare	Active	Active	Inactive

Tab Name:SNMP

Function	Level 0	Level 1	Level 2
SNMP	Active	Active	Active
Permit Settings by SNMPv1 and v2	On	Off	Off
SNMPv1 / v2 Function	Active	Active	Inactive
SNMPv3 Function	Active	Active	Active
Permit SNMPv3 Communication	Encryption / Cleartext	Encryption Only	Encryption Only

Encrypting Transmitted Passwords

Prevent login passwords 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.

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.

Driver Encryption Key

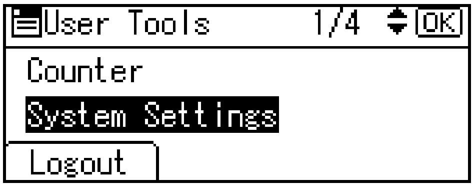
This can be specified by the network administrator.

Specify the driver encryption key on the machine.

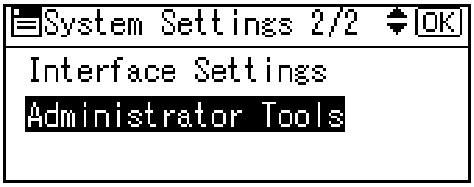
By making this setting, you can encrypt login passwords for transmission to prevent them from being analyzed.

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

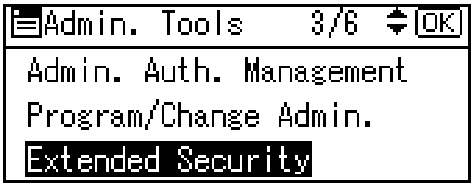
1. **Press the [User Tools/Counter] key.**
2. **Select [System Settings] using [▲] or [▼], and then press the [OK] key.**



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

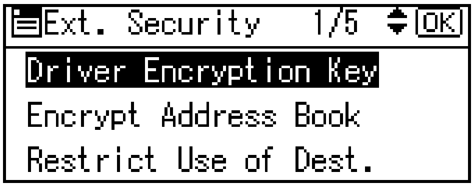


4. **Select [Extended Security] using [▲] or [▼], and then press the [OK] key.**



```
Admin. Tools      3/6  ⇕ OK
 Admin. Auth. Management
 Program/Change Admin.
 Extended Security
```

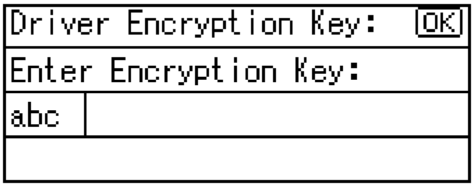
5. **Select [Driver Encryption Key] using [▲] or [▼], and then press the [OK] key.**



```
Ext. Security     1/5  ⇕ OK
 Driver Encryption Key
 Encrypt Address Book
 Restrict Use of Dest.
```

"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.**

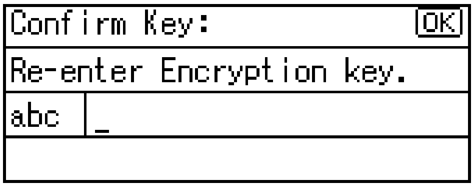


```
Driver Encryption Key:    OK
Enter Encryption Key:
abc |
```

Enter the driver encryption key using up to 32 alphanumeric characters.

The network administrator must give users the driver encryption key specified on the machine so they can register it on their computers. Make sure to enter the same driver encryption key as that is specified on the machine.

7. **Press the [OK] key.**



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

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.30 "Logging on Using Administrator Authentication"
- p.31 "Logging off Using Administrator Authentication"

- p.177 "Specifying the Extended Security Functions"

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 [Apply].**

   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.

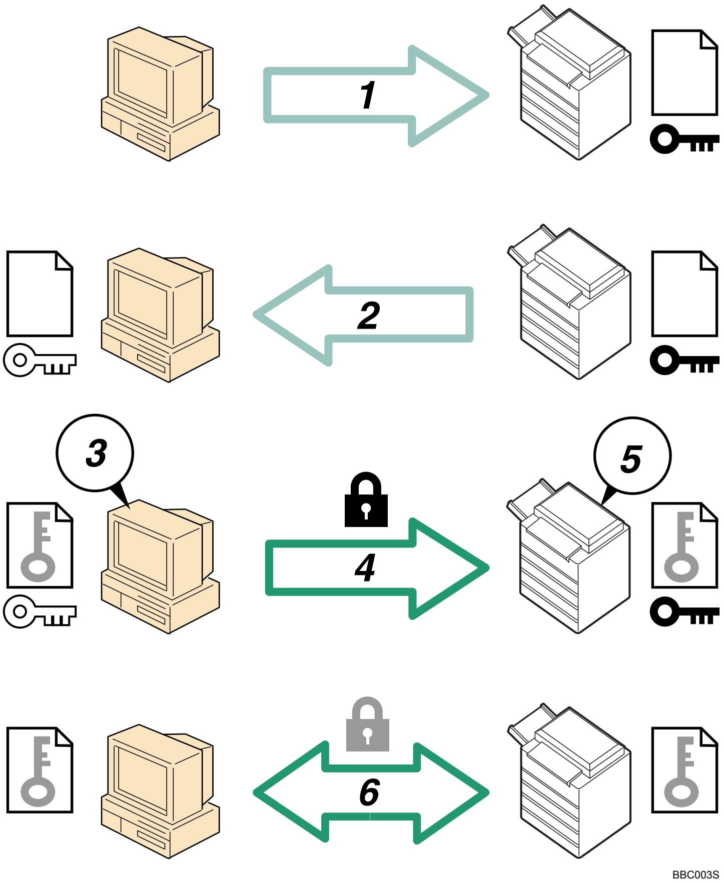
SSL (Secure Sockets Layer) Encryption

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)



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 (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.

Installing the Device Certificate (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 "http://(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 and enabled SSL (Secure Sockets Layer), you need to install the certificate on the user's computer.

The network administrator must explain the procedure for installing the certificate to users.

If a warning dialog box appears while accessing the machine using Web Image Monitor or IPP, start the Certificate Import Wizard and install a certificate.

1. **When the Security Alert dialog box appears, click [View Certificate].**

   The Certificate dialog box appears.

   To be able to respond to inquiries from users about such problems as expiry of the certificate, check the contents of the certificate.

2. **Click [Install Certificate...] on the "General" tab.**

   Certificate Import Wizard starts.

3. **Install the certificate by following the Certificate Import Wizard instructions.**

Note

- 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.

Encrypted Communication Mode

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

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

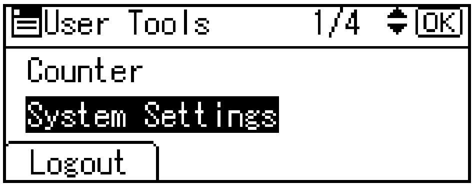
Setting the SSL / TLS Encryption Mode

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.

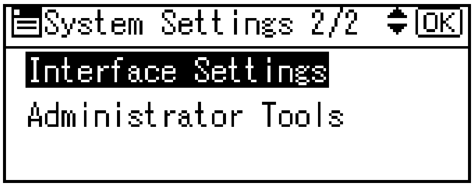
For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

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



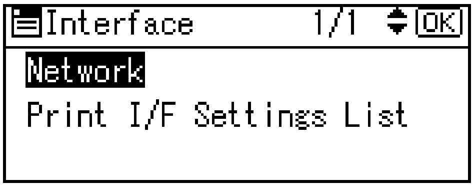
```
User Tools          1/4 ⬍ OK
 Counter
 System Settings
 Logout
```

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



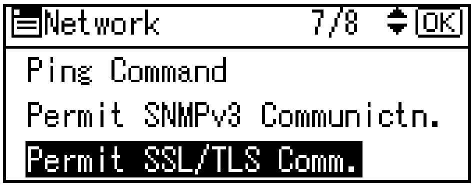
```
System Settings 2/2 ⬍ OK
 Interface Settings
 Administrator Tools
```

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



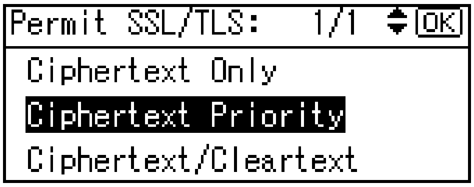
```
Interface           1/1 ⬍ OK
 Network
 Print I/F Settings List
```

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



```
Network             7/8 ⬍ OK
 Ping Command
 Permit SNMPv3 Communictn.
 Permit SSL/TLS Comm.
```

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



Permit SSL/TLS: 1/1 ⇕ OK
Ciphertext Only
Ciphertext Priority
Ciphertext/Cleartext

Select [Ciphertext Only], [Ciphertext Priority], or [Ciphertext / Clear Text] 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.30 "Logging on Using Administrator Authentication"
- p.31 "Logging off Using Administrator Authentication"

SNMPv3 Encryption

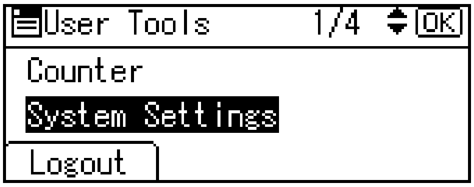
This can be specified by the network administrator.

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.

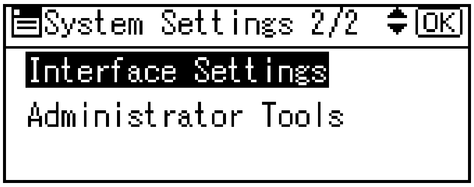
For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

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



User Tools 1/4 ⇕ OK
Counter
System Settings
Logout

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

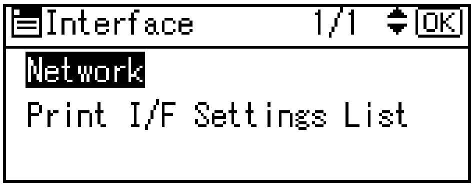


System Settings 2/2 ⬍ OK

Interface Settings

Administrator Tools

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

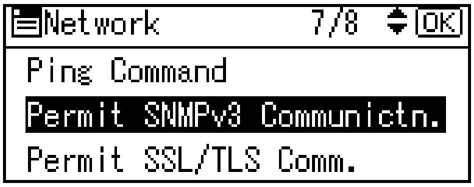


Interface 1/1 ⬍ OK

Network

Print I/F Settings List

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



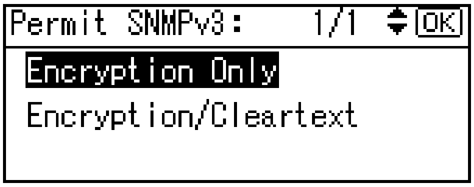
Network 7/8 ⬍ OK

Ping Command

Permit SNMPv3 Communictn.

Permit SSL/TLS Comm.

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



Permit SNMPv3: 1/1 ⬍ OK

Encryption Only

Encryption/Cleartext

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 Communication] 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.30 "Logging on Using Administrator Authentication"
- p.31 "Logging off Using Administrator Authentication"

- p.26 "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 Transmission", access to Web Image Monitor can be lost if the key settings are improperly configured. In order to prevent this, you can specify IPsec to exclude HTTPS transmission by selecting "Active". When you want to include HTTPS transmission, we recommend that you select "Inactive" for "Exclude HTTPS Transmission" after confirming that IPsec is properly configured. When "Active" is selected for "Exclude HTTPS Transmission", 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", General 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.	• Active • Inactive
Exclude HTTPS Transmission	Specify whether to enable IPsec for HTTPS transmission.	• Active • Inactive Specify "Active" if you do not want to use IPsec for HTTPS transmission.
Encryption Key Manual Settings	Specify whether to enable Encryption Key Manual Settings, or use Encryption Key Auto Exchange Settings only.	• Active • Inactive Specify "Active" if you want to use "Encryption Key Manual 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.

Security Level	Security Level Features
	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
Phase 2 Security Protocol	AH	ESP	ESP

Setting	Authentication Only	Authentication and Low Level Encryption	Authentication and High Level Encryption
Phase 2 Authentication Algorithm	HMAC-MD5-96/ HMAC-SHA1-96	HMAC-MD5-96/ HMAC-SHA1-96	HMAC-SHA1-96
Phase 2 Encryption Algorithm	Cleartext (NULL encryption)	DES/3DES/ AES-128/AES-192/ AES-256	3DES/AES-128/ AES-192/AES-256
Phase 2 PFS	Inactive	Inactive	2

Encryption Key Auto Exchange Setting Items

When you specify a security level, the corresponding security settings are automatically configured, but other settings, such as address type, local address, and remote address must still be configured manually.

After you specify a security level, you can still make changes to the auto configured settings. When you change an auto configured setting, the security level switches automatically to "User Setting".

Setting	Description	Setting Value
Address Type	Specify the address type for which IPsec transmission is used.	• Inactive • IPv4 • IPv6 • IPv4/IPv6 (Default Settings only)
Local Address	Specify the machine's address. If you are using multiple addresses in IPv6, you can also specify an address range.	The machine's IPv4 or IPv6 address. If you are not setting an address range, enter 32 after an IPv4 address, or enter 128 after an IPv6 address.
Remote Address	Specify the address of the IPsec transmission partner. You can also specify an address range.	The IPsec transmission partner's IPv4 or IPv6 address. If you are not setting an address range, enter 32 after an IPv4 address, or enter 128 after an IPv6 address.

Setting	Description	Setting Value
Security Policy	Specify how IPsec is handled.	• apply • bypass • discarded
Encapsulation Mode	Specify the encapsulation mode. (auto setting)	• Transport • Tunnel (Tunnel beginning address - Tunnel ending address) 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. (auto setting)	• Use When Possible • Always Require
Authentication Method	Specify the method for authenticating transmission partners. (auto setting)	• PSK • Certificate If you specify PSK, you must then set the PSK text (using ASCII characters). If you specify Certificate, the certificate for IPsec must be installed and specified before it can be used.
PSK Text	Specify the pre-shared key for PSK authentication.	Enter the pre-shared key required for PSK authentication.
Phase 1 HASH Algorithm	Specify the HASH algorithm to be used in phase 1. (auto setting)	• MD5 • SHA1

Setting	Description	Setting Value
Phase 1 Encryption Algorithm	Specify the encryption algorithm to be used in phase 1. (auto setting)	• DES • 3DES
Phase 1 Diffie-Hellman Group	Select the Diffie-Hellman group number used for IKE encryption key generation. (auto setting)	• 1 • 2 • 14
Phase 1 Validity Period	Specify the time period for which the SA settings in phase 1 are valid.	Set in seconds from 300 sec. (5 min.) to 172800 sec. (48 hrs.).
Phase 2 Security Protocol	Specify the security protocol to be used in Phase 2. To apply both encryption and authentication to sent data, specify ESP or AH + ESP. To apply authentication data only, specify AH. (auto setting)	• ESP • AH • AH + ESP
Phase 2 Authentication Algorithm	Specify the authentication algorithm to be used in phase 2. (auto setting)	• HMAC-MD5-96 • HMAC-SHA1-96
Phase 2 Encryption Algorithm Permissions	Specify the encryption algorithm to be used in phase 2. (auto setting)	• Cleartext (NULL encryption) • DES • 3DES • AES-128 • AES-192 • AES-256
Phase 2 PFS	Specify whether to activate PFS. Then, if PFS is activated, select the Diffie-Hellman group.	• Inactive • 1 • 2

Setting	Description	Setting Value
	(auto setting)	• 14
Phase 2 Validity Period	Specify the time period for which the SA settings in phase 2 are valid.	Specify a period (in seconds) from 300 (5min.) to 172800 (48 hrs.).

Encryption Key Manual Settings Items

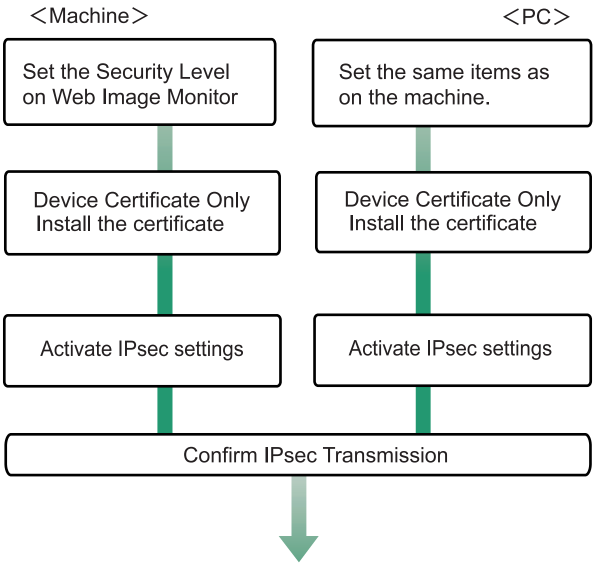
Setting	Description	Setting Value
Address Type	Specify the address type for which IPsec transmission is used.	• Inactive • IPv4 • IPv6 • IPv4/IPv6 (Default Settings only)
Local Address	Specify the machine's address. If you are using multiple IPv6 addresses, you can also specify an address range.	The machine's IPv4 or IPv6 address. If you are not setting an address range, enter 32 after an IPv4 address, or enter 128 after an IPv6 address.
Remote Address	Specify the address of the IPsec transmission partner. You can also specify an address range.	The IPsec transmission partner's IPv4 or IPv6 address. If you are not setting an address range, enter 32 after an IPv4 address, or enter 128 after an IPv6 address.
Encapsulation Mode	Select the encapsulation mode.	• Transport • Tunnel (Tunnel beginning address - Tunnel ending address) If you select "Tunnel", set the "Tunnel End Point", the beginning and ending IP addresses. In "Tunnel End Point", set the same address for

Setting	Description	Setting Value
		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. To apply authentication data only, specify AH.	• ESP • AH • AH + ESP
Authentication Algorithm	Specify the authentication algorithm.	• HMAC-MD5-96 • HMAC-SHA1-96
Authentication Key	Specify the key for the authentication algorithm.	Specify a value within the ranges shown below, according to the encryption algorithm. Hexadecimal value 0-9, a-f, A-F • If HMAC-MD5-96, set 32 digits • If HMAC-SHA1-96, set 40 digits ASCII • IF HMAC-MD5-96, set 16 characters • If HMAC-SHA1-96, set 20 characters
Encryption Algorithm	Specify the encryption algorithm.	• Cleartext (NULL encryption) • DES • 3DES

Setting	Description	Setting Value
		• AES-128 • AES-192 • AES-256
Encryption Key	Specify the key for the encryption algorithm.	Specify a value within the ranges shown below, according to the encryption algorithm. hexadecimal value 0-9, a-f, A-F • DES, set 16 digits • 3DES, set 48 digits • AES-128, set 32 digits • AES-192, set 48 digits • AES-256, set 64 digits ASCII • DES, set 8 characters • 3DES, set 24 characters • AES-128, set 16 characters • AES-192, set 24 characters • AES-256, set 32 characters

Encryption Key Auto Exchange Settings Configuration Flow

This section explains the procedure for specifying Encryption Key Auto Exchange Settings. This can be specified by the network administrator.



<Machine>
<PC>
Set the Security Level on Web Image Monitor
Set the same items as on the machine.
Device Certificate Only Install the certificate
Device Certificate Only Install the certificate
Activate IPsec settings
Activate IPsec settings
Confirm IPsec Transmission

BBD004S

6

Note

- To use a certificate to authenticate the transmission partner in encryption key auto exchange settings, a device certificate must be installed.
- After configuring IPsec, you can use "Ping" command to check if the connection is established correctly. However, you cannot use "Ping" command when ICMP is excluded from IPsec transmission on the computer side. Also, because the response is slow during initial key exchange, it may take some time to confirm that transmission has been established.

Specifying Encryption Key Auto Exchange Settings

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 Transmission" 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 "Creating and Installing the Self-Signed Certificate".

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.

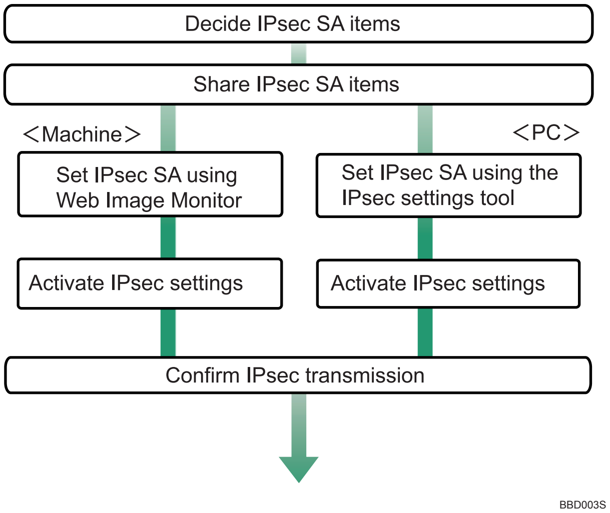
Note

- 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.



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 Transmission" to [Active] if you do not want to use IPsec for HTTPS communication.**
11. **Click [OK].**
12. **Click [Logout].**

telnet Setting Commands

You can use telnet to confirm IPsec settings and make setting changes. This section explains telnet commands for IPsec. To log in as an administrator using telnet, the default login user name is "admin", and the password is blank. For details about logging in to telnet and telnet operations, see "Using telnet", Network 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.

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} tunneladdar beginning IP address ending IP
address
```

- Enter the separate setting number [1-4] or [default] and specify the tunnel end point beginning and ending IP address.
- Not specifying either the beginning or ending address displays the current settings.

Authentication algorithm and authentication key settings

```
msh> ipsec manual {1|2|3|4|default} auth {hmac-md5|hmac-sha1} authentication key
```

- Enter the separate setting number [1-4] or [default] and specify the authentication algorithm, and then set the authentication key.
- If you are setting a hexadecimal number, attach 0x at the beginning.
- If you are setting an ASCII character string, enter it as is.
- Not specifying either the authentication algorithm or key displays the current setting. (The authentication key is not displayed.)

Encryption algorithm and encryption key setting

```
msh> ipsec manual {1|2|3|4|default} encrypt {null|des|3des|aes128|aes192|aes256}
encryption key
```

- Enter the separate setting number [1-4] or [default], specify the encryption algorithm, and then set the encryption key.
- If you are setting a hexadecimal number, attach 0x at the beginning. If you have set the encryption algorithm to [null], enter an encryption key of arbitrary numbers 2-64 digits long.
- If you are setting an ASCII character string, enter it as is. If you have set the encryption algorithm to [null], enter an encryption key of arbitrary numbers 1-32 digits long.
- Not specifying an encryption algorithm or key displays the current setting. (The encryption key is not displayed.)

Reset setting values

```
msh> ipsec manual {1|2|3|4|default|all} clear
```

- Enter the separate setting number [1-4] or [default] and reset the specified setting. Specifying [all] resets all of the settings, including default.

ipsec ike

To display or specify the encryption key auto exchange settings, use the "ipsec ike" command.

Display current settings

```
msh> ipsec ike {1|2|3|4|default}
```

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

- To display the default setting, specify [default].
- Not specifying any value displays all of the settings.

Disable settings

```
msh> ipsec manual {1|2|3|4|default} disable
```

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

Specify the local/remote address for settings 1-4

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

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

Specify the address type in default setting

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

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

Security policy setting

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

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

- Enter the separate setting number [1-4] or [default] and specify the tunnel end point beginning and ending IP address.
- Not specifying either the beginning or ending address displays the current 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 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
```

USB setting

```
msh> authfree [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 environment. For details, see "Using telnet", Network and System Settings Guide.

7. 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".

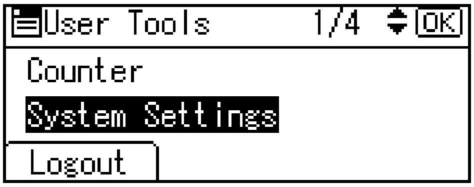
Reference

- p.30 "Logging on Using Administrator Authentication"
- p.31 "Logging off Using Administrator Authentication"

Procedure for Changing the Extended Security Functions

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.**



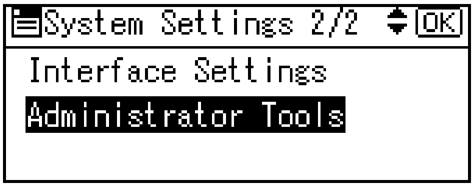
User Tools 1/4 ⬍ OK

Counter

System Settings

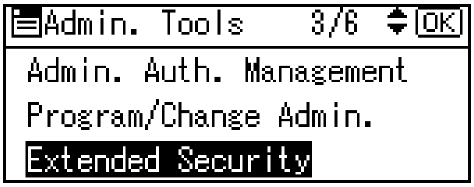
Logout

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



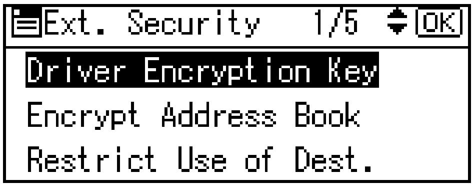
```
System Settings 2/2  ⬍ OK
 Interface Settings
 Administrator Tools
```

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



```
Admin. Tools    3/6  ⬍ OK
 Admin. Auth. Management
 Program/Change Admin.
 Extended Security
```

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



```
Ext. Security   1/5  ⬍ OK
 Driver Encryption Key
 Encrypt Address Book
 Restrict Use of Dest.
```

6. **Change the setting, and then press the [OK] key.**
7. **Press the [User Tools/Counter] key.**

Settings

Default settings are shown in **bold type**.

Driver Encryption Key

This can be specified by the network administrator. Encrypt the password transmitted when specifying user authentication. If you register the encryption key specified with the machine in the driver, passwords are encrypted. For details, see the printer driver Help, LAN Fax driver Help, or TWAIN driver Help.

Encrypt Address Book

This can be specified by the user administrator. Encrypt the data in the machine's Address Book.

For details on protecting data in the Address Book, see "Protecting the Address Book".

- On
- **Off**

Restrict Use of Destinations

This can be specified by the user administrator.

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

A user cannot directly enter the destinations for transmission.

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

For details about preventing unauthorized transmission, see "Preventing Data Leaks Due to Unauthorized Transmission".

- On
- **Off**

Restrict Adding of User Destinations

This can be specified by the user administrator.

When "Restrict Use of Destinations" is set to [Off], after entering a fax destination directly, 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 "Restrict Adding of User Destinations" to [On], users can specify destinations directly, 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 Display of User Information

This can be specified if user authentication is specified. When the job history is checked using a network connection for which authentication is not available, all personal information can be displayed as "*********". For example, when someone not authenticated as an administrator checks the job history using SNMP in SmartDeviceMonitor for Admin, personal information can be displayed as "*********" so that users cannot be identified. Because information identifying registered users cannot be viewed, unauthorized users are prevented from obtaining information about the registered files.

- On
- **Off**

Enhance File Protection

This can be specified by the file administrator. By specifying a password, you can limit operations such as printing, deleting, and sending files, and can prevent unauthorized people from accessing the files. However, it is still possible for the password to be cracked.

By specifying "Enhance File Protection", files are locked and so become inaccessible if an invalid password is entered ten times. This can protect the files from unauthorized access attempts in which a password is repeatedly guessed.

The locked files can only be unlocked by the file administrator. When "Enhance File Protection" is specified, (🔒) appears in the lower right corner of the screen.

When files are locked, you cannot select them even if the correct password is entered.

- On

- **Off**

Settings by SNMP v1 and v2

This can be specified by the network administrator. When the machine is accessed using the SNMPv1, v2 protocol, authentication cannot be performed, allowing machine administrator settings such as the paper setting to be changed. If you select [Prohibit], the setting can be viewed but not specified with SNMPv1, v2.

- Prohibit
- **Do not Prohibit**

Restrict Use of Simple Encryption

This can be specified by the network administrator. When a sophisticated encryption method cannot be enabled, simple encryption will be applied. For example, when using User Management Tool and Address Management in Smart Device Monitor for Admin to edit the Address Book, or DeskTopBinder and ScanRouter delivery software and SSL/TLS cannot be enabled, make this setting [Off] to enable simple encryption. When SSL/TLS can be enabled, make this setting [On].

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

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

- On
- **Off**

Transfer to Fax Receiver

This can be specified by the machine administrator.

If you use [Forwarding] 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 from Personal Box
- Information Box
- Routing Received Documents

Authenticate Current Job

This can be specified by the machine administrator. This setting lets you specify whether or not authentication is required for operations such as canceling jobs under the copier and printer functions.

If you select [Login Privilege], authorized users and the machine administrator can operate the machine. When this is selected, authentication is not required for users who logged on to the machine before [Login Privilege] was selected.

If you select [Access Privilege], users who canceled a copy or print job in progress and the machine administrator can operate the machine.

Even if you select [Login Privilege] and log on to the machine, you cannot cancel a copy or print job in progress if you are not authorized to use the copy and printer functions.

You can specify [Authenticate Current Job] only if [User 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 2
- Level 1
- **Off**
- Minimum Character No. (**0**)

@Remote Service

Communication via HTTPS for @Remote Service is disabled if you select [Prohibit].

- Prohibit
- **Do not Prohibit**

Update Firmware

This can be specified by the machine administrator.

Specify whether to allow firmware updates on the machine. Firmware update means having the service representative update the firmware or updating the firmware via the network.

If you select [Prohibit], firmware on the machine cannot be updated.

If you select [Do not Prohibit], there are no restrictions on firmware updates.

- Prohibit
- **Do not Prohibit**

Change Firmware Structure

This can be specified by the machine administrator.

Specify whether to prevent changes in the machine's firmware structure. The Change Firmware Structure function detects when the SD card is inserted, removed or replaced.

If you select [Prohibit], the machine stops during startup when a firmware structure change is detected and a message requesting administrator login is displayed. After the machine administrator logs in, the machine finishes startup with the updated firmware.

The administrator can confirm if the updated structure change is permissible or not by checking the firmware version displayed on the control panel screen. If the firmware structure change is not permissible, contact your service representative before logging in.

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.105 "Protecting the Address Book"
- p.103 "Preventing Data Leaks Due to Unauthorized Transmission"
- p.147 "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 "Not Displaying Destinations and Senders in Reports and Lists", see "Facsimile Settings", 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.

Limiting Machine Operation to Customers Only

The machine can be set so that operation is impossible without administrator authentication.

The machine can be set to prohibit operation without administrator authentication and also prohibit remote registration in the Address Book by a service representative.

We maintain strict security when handling customers' data. Administrator authentication prevents us from operating the machine without administrator permission.

Use the following settings.

- Service Mode Lock

Settings

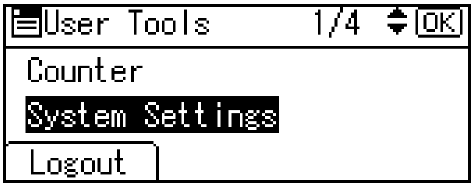
Service Mode Lock

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.

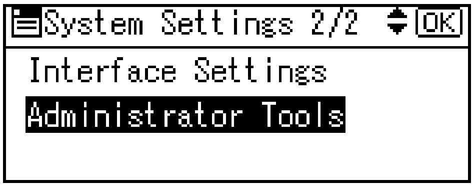
Specifying Service Mode Lock Preparation

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

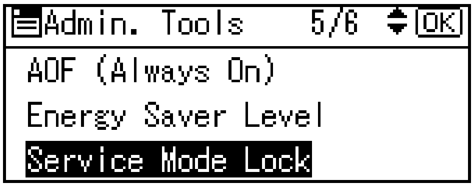
1. **Press the [User Tools/Counter] key.**
2. **Select [System Settings] using [▲] or [▼], and then press the [OK] key.**



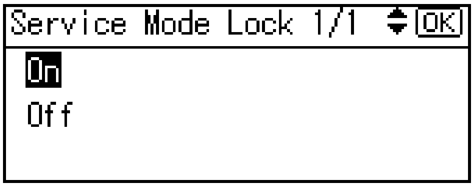
3. **Select [Administrator Tools] using [▲] or [▼], and then press the [OK] key.**



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

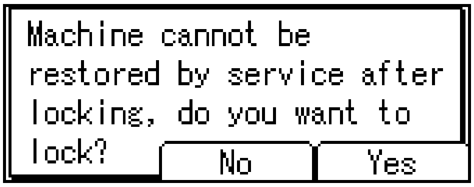


5. **Select [On] using [▲] or [▼], and then press the [OK] key.**



A confirmation message appears.

6. **Press [Yes].**


Machine cannot be restored by service after locking, do you want to lock?

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

Reference

- p.30 "Logging on Using Administrator Authentication"
- p.31 "Logging off Using Administrator Authentication"

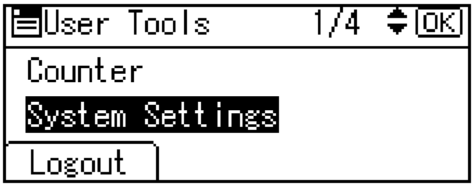
Canceling Service Mode Lock

For a service representative to carry out inspection or repair in service mode, the machine administrator must log on to the machine and cancel the 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".

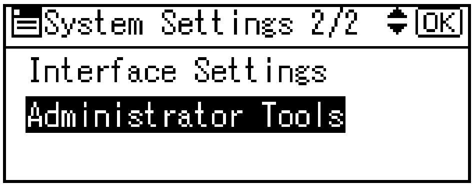
1. **Press the [User Tools/Counter] key.**

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



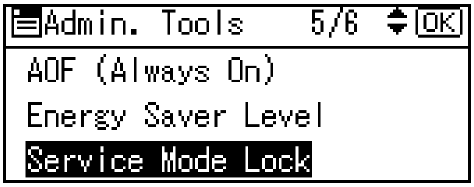
```
User Tools        1/4 ⬍ OK
Counter
System Settings
Logout
```

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



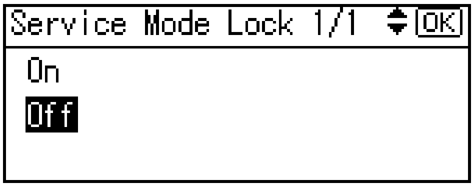
```
System Settings 2/2 ⬍ OK
Interface Settings
Administrator Tools
```

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



```
Admin. Tools      5/6 ⬍ OK
AOF (Always On)
Energy Saver Level
Service Mode Lock
```

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



```
Service Mode Lock 1/1 ⬍ OK
On
Off
```

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

   The service representative can switch to service mode.

Reference

- p.30 "Logging on Using Administrator Authentication"
- p.31 "Logging off Using Administrator Authentication"

8. Troubleshooting

This chapter describes what to do if the machine does not function properly.

Authentication Does Not Work Properly

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.

A Message Appears

This section explains how to deal with problems if a message appears on the screen during user authentication.

The most common messages are explained. If some other message appears, deal with the problem according to the information contained in the message.

Messages	Cause	Solutions
"You do not have the privileges to use this function."	The authority to use the function is not specified.	• If this appears when trying to use a function: The function is not specified in the Address Book management setting as being available. The user administrator must decide whether to authorize use of the function and then assign the authority. • If this appears when trying to specify a default setting: The administrator differs depending on the default settings you wish to specify. Using the list of settings, the administrator responsible must decide whether to authorize use of the function.

Messages	Cause	Solutions
"Failed to obtain URL."	The machine cannot connect to the server or cannot establish communication.	Make sure the server's settings, such as the IP address and host name, are specified correctly on the machine. Make sure the host name of the UA Server is specified correctly.
"Failed to obtain URL."	The machine is connected to the server, but the UA service is not responding properly.	Make sure the UA service is specified correctly.
"Failed to obtain URL."	SSL is not specified correctly on the server.	Specify SSL using Authentication Manager.
"Failed to obtain URL."	Server authentication failed.	Make sure server authentication is specified correctly on the machine.
"Authentication 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.
"Set User Management in Admin. Auth. to On to use this setting."	Admin. Authentication is not configured under "Administrator Authentication Management".	To specify Basic Authentication, Windows Authentication, LDAP Authentication, or Integration Server. Authentication, you must first specify administrator authentication. For details about authentication settings, see "Authentication Setting Procedure".

Reference

- p.37 "Authentication Setting Procedure"

Machine Cannot Be Operated

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

Condition	Cause	Solution
Cannot perform the following: • Print with the printer driver • Connect with the TWAIN driver Send with the LAN-Fax driver	User authentication has been rejected.	Confirm the user name and login name with the administrator of the network in use if using Windows Authentication, LDAP Authentication, or Integration Server Authentication. Confirm with the user administrator if using basic authentication.
Cannot perform the following: • Print with the printer driver • Connect with the TWAIN driver Send 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. See "Driver Encryption Key".
Cannot perform the following: • Print with the printer driver • Connect with the TWAIN driver Send with the LAN-Fax driver	The SNMPv3 account, password, and encryption algorithm do not match settings specified on this machine.	Specify the account, password and the encryption algorithm of SNMPv3 registered in the machine using network connection tools.
Cannot authenticate using the TWAIN driver.	Another user is logging 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.	Make sure the LDAP server setting is correct. Make sure the network settings are correct.

Condition	Cause	Solution
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.	"Restrict Use of Simple Encryption" is not set correctly. Alternatively, "SSL/TLS" has been enabled although the required certificate is not installed in the computer.	Set "Restrict Use of Simple Encryption" to [On]. Alternatively, enable "SSL/TLS", install the server certificate in the machine, and then install the certificate in the computer. See "Setting the SSL / TLS Encryption Mode".
Cannot access the machine using ScanRouter EX Professional V3 / ScanRouter EX Enterprise V2.	"Restrict Use of Simple Encryption" is not set correctly. Alternatively, "SSL/TLS" has been enabled although the required certificate is not installed in the computer.	Set "Restrict Use of Simple Encryption" to [On]. Alternatively, enable "SSL/TLS", install the server certificate in the machine, and then install the certificate in the computer. See "Setting the SSL / TLS Encryption Mode".
Cannot 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 functions.	The original has not been scanned completely.	When the original has been scanned completely, press [#], remove the original, and then log off.
"Program Dest." does not appear on the fax screen for specifying destinations.	"Restrict Adding of User Destinations" is set to [Off] in "Restrict Use of Destinations" in "Extended Security", so only the user administrator can register destinations in the Address Book.	Registration must be done by the user administrator.
User authentication is enabled, yet stored files do not appear.	User authentication may have been disabled while [All Users] is not specified.	Re-enable user authentication, and then enable [All Users] for the files that did not appear.

Condition	Cause	Solution
		For details about enabling [All Users], see "Specifying Access Permission for Stored Files".
User authentication is enabled, yet destinations specified using the machine do not appear.	User authentication may have been disabled while [All Users] is not specified.	Re-enable user authentication, and then enable [All Users] for the destinations that did not appear. For details about enabling [All Users], see "Protecting the Address Book".
Cannot print when user authentication has been specified.	User authentication may not be specified in the printer driver.	Specify user authentication in the printer driver. For details, see the printer driver Help.
If you try to interrupt a job while copying or scanning, an authentication screen appears.	With this machine, you can log off while copying or scanning. If you try to interrupt copying or scanning after logging off, an authentication screen appears.	Only the user who executed a copying or scanning job can interrupt it. Wait until the job has completed or consult an administrator or the user who executed the job.
After you execute "Encrypt Address Book", the "Exit" message does not appear.	The file may be corrupt.	Contact your service representative.

Reference

- p.139 "Driver Encryption Key"
- p.147 "Setting the SSL / TLS Encryption Mode"
- p.105 "Protecting the Address Book"

9. 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 to 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.**

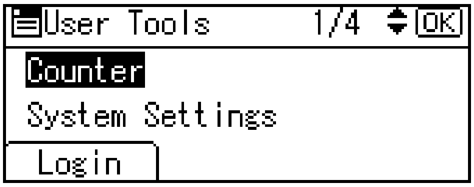
Note

- 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.

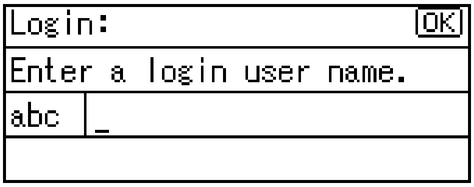
Logging on as the Supervisor

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].**



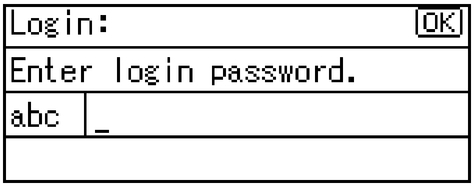
3. **Enter a login user name, and then press the [OK] key.**



Enter a login user name.

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

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



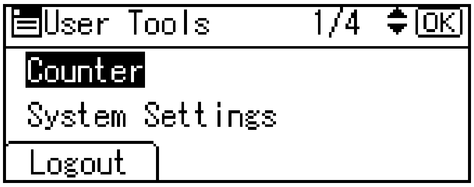
Enter login password.

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

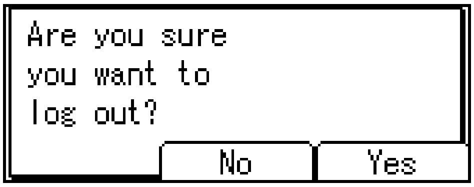
Logging off as the Supervisor

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].**



2. **Press [Yes].**



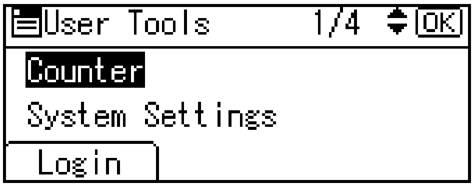
Are you sure you want to log out?

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".

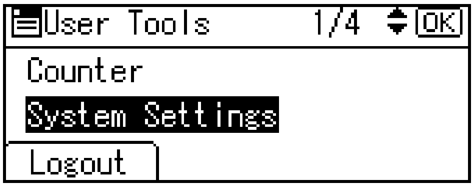
1. **Press the [User Tools/Counter] key.**
2. **Press [Login].**



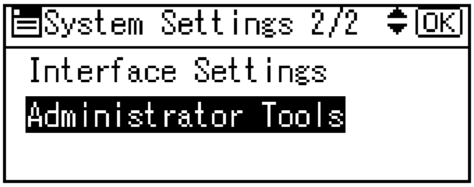
3. **Log on as the supervisor.**

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

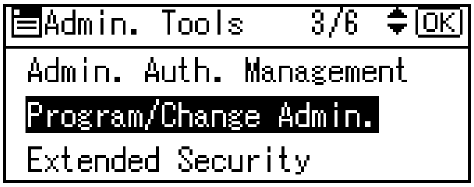
4. **Select [System Settings] using [▲] or [▼], and then press the [OK] key.**



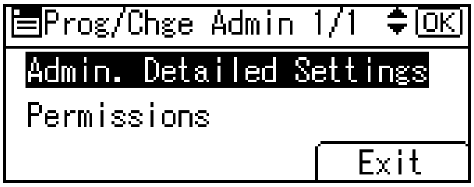
5. **Select [Administrator Tools] using [▲] or [▼], and then press the [OK] key.**



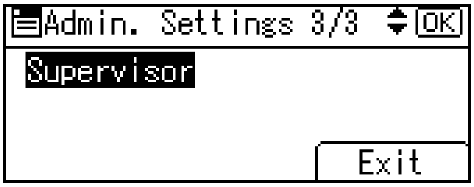
6. **Select [Program/Change Admin.] using [▲] or [▼], and then press the [OK] key.**



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



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

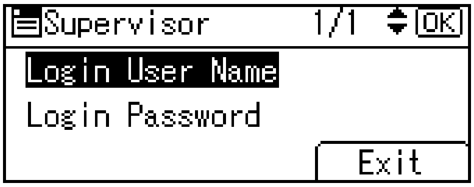


Admin. Settings 3/3 ⇕ OK

Supervisor

Exit

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



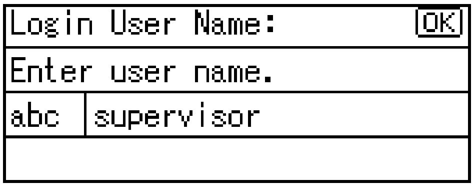
Supervisor 1/1 ⇕ OK

Login User Name

Login Password

Exit

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

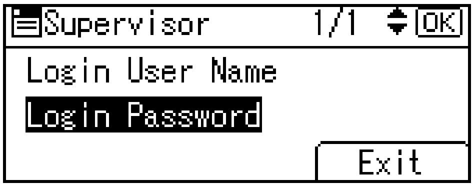


Login User Name: OK

Enter user name.

abc supervisor

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



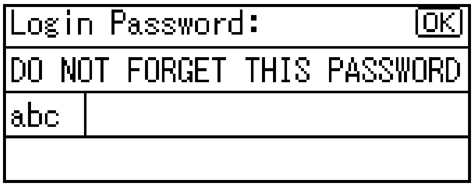
Supervisor 1/1 ⇕ OK

Login User Name

Login Password

Exit

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

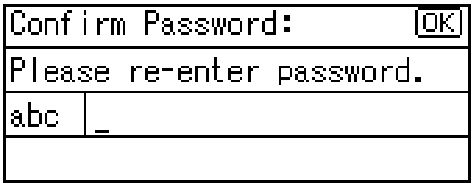


Login Password: OK

DO NOT FORGET THIS PASSWORD

abc

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

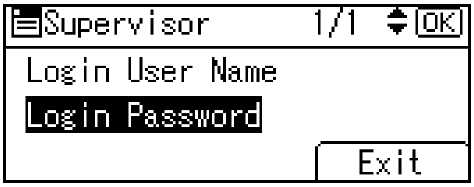


Confirm Password: OK

Please re-enter password.

abc _

14. **Press [Exit] three times.**



```
Supervisor          1/1 ⇕ OK
 Login User Name
 Login Password
                      Exit
```

You will be automatically logged off.

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

Reference

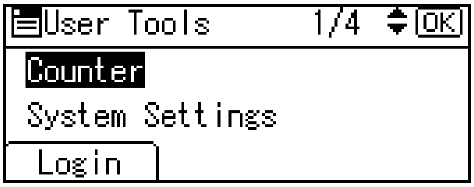
- p.24 "Specifying Administrator Privileges"
- p.193 "Supervisor Operations"

Resetting an 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].**

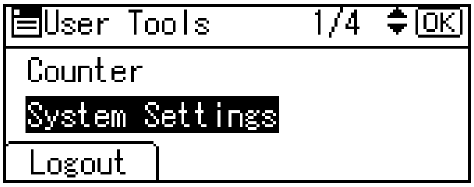


```
User Tools          1/4 ⇕ OK
 Counter
 System Settings
 Login
```

3. **Log on as the supervisor.**

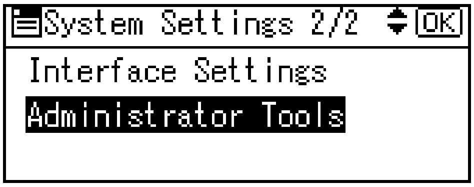
   You can log on in the same way as an administrator.

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



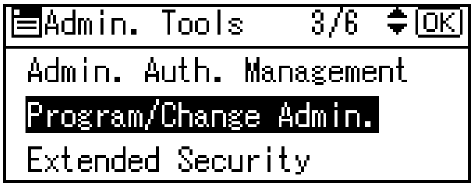
```
User Tools          1/4 ⇕ OK
 Counter
 System Settings
 Logout
```

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



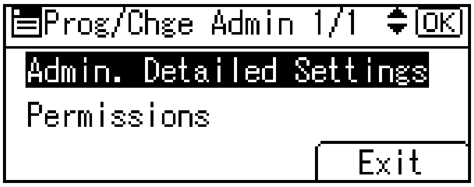
```
System Settings 2/2 ⇕ OK
 Interface Settings
 Administrator Tools
```

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



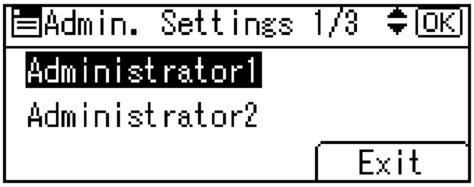
```
Admin. Tools     3/6 ⇕ OK
 Admin. Auth. Management
 Program/Change Admin.
 Extended Security
```

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



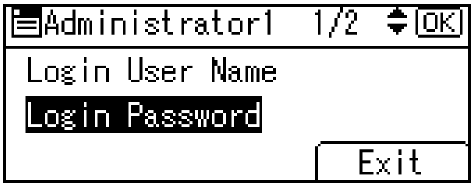
```
Prog/Chge Admin 1/1 ⇕ OK
 Admin. Detailed Settings
 Permissions
                   Exit
```

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



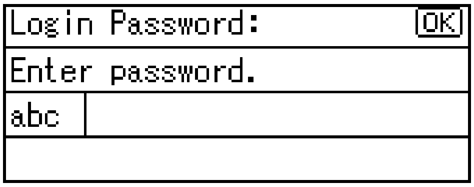
```
Admin. Settings 1/3 ⇕ OK
 Administrator1
 Administrator2
                   Exit
```

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



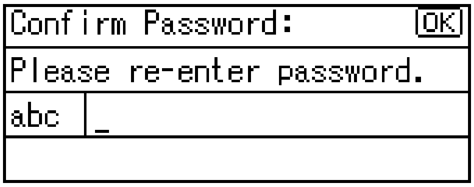
```
Administrator1  1/2 ⇕ OK
 Login User Name
 Login Password
                   Exit
```

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.**

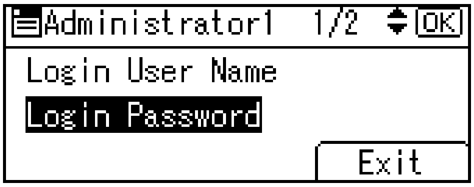


Confirm Password: OK

Please re-enter password.

abc _

12. **Press [Exit] three times.**



Administrator1 1/2 OK

Login User Name

Login Password

Exit

You will be automatically logged off.

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

Reference

- p.193 "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.

Administrator Tools

The following settings can be specified.

- Display / Print Counter

  Print Counter List

- Display / Clear / Print Counter per User

  Print Counter List

- User Authentication Management

  You can specify which authentication to use.

  You can also edit the settings for each function.

- Administrator Authentication Management

  Machine Management

- Program / Change Administrator

  Machine Administrator

  You can change the user name and the full-control user's authority.

- Key Counter Management
- Restrict Display of User Information
- Extended Security

  Transfer to Fax Receiver

  @Remote Service

  Update Firmware

  Change Firmware Structure

- Program / Change / Delete LDAP Server

  Name

  Server Name

  Search Base

  Port Number

  Use Secure Connection (SSL)

  Authentication

  User Name

  Password

  Connection Test

  Search Conditions

  Search Options
- LDAP Search
- Program / Change / Delete Realm
- AOF (Always On)
- Energy Saver Level
- Service Mode Lock
- Firmware Version
- Delete All Logs
- Transfer Log Setting
- Data Security for Copying *1
- Fixed USB Port

*1 The Copy Data Security Unit option must be installed.

Copier Features

The following settings can be specified.

General Features

All the settings can be specified.

Reproduction Ratio

All the settings can be specified.

Edit

All the settings can be specified.

Stamp

All the settings can be specified.

Input / Output

All the settings can be specified.

Adjust Colour Image

All the settings can be specified.

Administrator Tools

All the settings can be specified.

Facsimile Features

The following settings can be specified.

General Settings/Adjust

All the settings can be specified.

Reception Settings

All the settings can be specified.

Administrator Tools

The following settings can be specified.

- Print Journal
- Print TX Standby File List
- Forwarding
- Parameter Setting
- Program Special Sender
- Program Memory Lock ID
- G3 Analog Line
- 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
- 4 Colour Graphic Mode

System

The following settings can be specified.

- Print Error Report
- Auto Continue
- Memory Overflow
- Rotate by 180 Degrees
- Duplex
- Copies
- Blank Page Print
- Sub Paper Size
- Page Size
- Letterhead Setting
- Bypass Tray Setting Priority
- Edge To Edge Print
- Tray Switching
- Extended Auto Tray Switching

Host Interface

All the settings can be specified.

PCL Menu

All the settings can be specified.

Settings via Web Image Monitor

The following settings can be specified.

Top Page

- Reset Device
- Reset Printer Job

Device Settings

- System

  Device Name

  Comment

Location

Protect Printer Display Panel

Permit Firmware Update

Permit Firmware Structure Change

Display IP Address on Device Display Panel

Output Tray

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.

- User Authentication Management

  All the settings can be specified.

- Administrator Authentication Management

  Machine Administrator Authentication

  Available Settings for Machine Administrator

- Program/Change Administrator

  You can specify the following administrator settings for the machine administrator.

  Login User Name

  Login Password

  Encryption Password

- LDAP Server

  All the settings can be specified.

- Firmware Update

  All the settings can be specified.

- Program/Change Realm

  All the settings can be specified.

Printer

- System

All the settings can be specified.

- Host Interface

  All the settings can be specified.

- PCL Menu

  All the settings can be specified.

- Tray Parameters (PCL)

  All the settings can be specified.

- Virtual Printer Settings

  All the settings can be specified.

Fax

- General Settings

  All the settings can be specified.

- Administrator Tools

  All the settings can be specified.

- Parameter Settings

  All the settings can be specified.

Interface

- Interface Settings

  Ethernet Security

  USB

  Pict Bridge

Network

- SNMPv3

Security

- User Lockout Policy

  All the settings can be specified.

RC Gate

- Set up RC Gate

  Request No.

- Update RC Gate Firmware
- RC Gate Proxy Server

Webpage

- Download Help File

Settings via SmartDeviceMonitor for Admin

The following settings can be specified.

Device Properties

- Reset Device
- Reset Current Job
- 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.

Administrator Tools

- 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

Settings via Web Image Monitor

The following settings can be specified.

Device Settings

- System

  Device Name

  Comment

  Location

- 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

Interface Settings

- Ethernet Security

Network

- IPv4

  All the settings can be specified.

- IPv6

  All the settings can be specified.

- NetWare

  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.

- 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.

Webpage

All the settings can be specified.

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

- Administrator Authentication Management

  File Management

- Program / Change Administrator

  File Administrator

- Extended Security

  Enhance File Protection

Settings via Web Image Monitor

The following settings can be specified.

Device Settings

- 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

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
- Progrm./Change/Delete Group
- Address Book : Print List
- Admin. Auth.Management

  User Management
- Program Change/Admin.

  User Administrator
- Extended Security

  Encrypt Address Book

  Restrict User of Dest.

  Restrict Adding of User Dest.

Settings via Web Image Monitor

The following settings can be specified.

Address Book

All the settings can be specified.

Device Settings

- 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

- Restrict Access To Device
- 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

  A = You can view and change the setting.

  B = You can view the setting.

  C = You cannot view or specify the setting.

Settings	Read-only (User)	Edit (User)	Edit / Delete (User)	Full Control	Registered User	User Admin.
Regist. No.	B	A	A	A	A	A
Name	B	A	A	A	A	A

Auth. Info

Settings	Read-only (User)	Edit (User)	Edit / Delete (User)	Full Control	Registered User	User Admin.
Login User Name	C	C	C	C	A	A
Login Password	C	C	C	C	A*1	A*1
LDAP Authentication	C	C	C	C	A*1	A*1
Function Permissions	C	C	C	C	B	A

*1 You can only enter the password.

Auth. Protect

Settings	Read-only (User)	Edit (User)	Edit / Delete (User)	Full Control	Registered User	User Admin.
Register as	B	A	A	A	A	A
Dest. Protect Obj.	C	C	C	A	A	A
Dest. Protect: Permission	C	C	C	A	A	A

Fax Settings

Settings	Read-only (User)	Edit (User)	Edit / Delete (User)	Full Control	Registered User	User Admin.
Fax Dest.	B	A	A	A	A	A

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 in to access them.

Copier Features

When administrator authentication is specified, the administrator's configuration of Menu Protect determines which functions and settings are available to users. If user authentication is specified, functions and settings are available to authorized users only, who must log in to access them.

- Abbreviations in the table columns

  R/W (Read and Write) = Both reading and modifying the setting are available.

  R (Read) = Reading only.

  N/A (Not Applicable) = Neither reading nor modifying the setting is available.

Note

- Settings that are not in the list can only be viewed, regardless of the menu protect level setting.

The default for [Menu Protect] is [Level 2].

General Features

Settings	Off	Level 1	Level 2
APS/ Auto R/E Priority	R/W	R	R
Auto Tray Switching	R/W	R	R
Original Type Setting	R/W	R/W	R
Duplex Mode Priority	R/W	R	R
Orientation	R/W	R/W	R
Max. Number of Sets	R/W	R	R
Original Count Display	R/W	R	R
Colour Mode Priority	R/W	R	R
Reproduction Ratio	R/W	R	R
Preset R/E Priority	R/W	R	R
Duplex Margin	R/W	R/W	R
Rotate Sort	R/W	R/W	R
Rotate Sort:Auto Continue	R/W	R	R
Letterhead Setting	R/W	R	R
ADS Background	R/W	R/W	R

Printer Features

When administrator authentication is specified, the administrator's configuration of Menu Protect determines which functions and settings are available to users. If user authentication is specified, functions and settings are available to authorized users only, who must log in to access them.

The following settings can be specified by someone who is not an administrator.

- Abbreviations in the table columns

  R/W (Read and Write) = Both reading and modifying the setting are available.

  R (Read) = Reading only.

  N/A (Not Applicable) = Neither reading nor modifying the setting is available.

Note

- Settings that are not in the list can only be viewed, regardless of the menu protect level setting.

The default for [Menu Protect] is [Level 2].

List / Test Print

Settings	Off	Level 1	Level 2
Multiple Lists	R/W	R/W	R/W
Configuration Page	R/W	R/W	R/W
Error Log	R/W	R/W	R/W
Menu List	R/W	R/W	R/W
PCL Configuration / Font Page	R/W	R/W	R/W
Hex Dump	R/W	R/W	R/W

Maintenance

Settings	Off	Level 1	Level 2
4Colour Graphic Mode	R/W	R	R

System

Settings	Off	Level 1	Level 2
Print Error Report	R/W	R	R
Auto Continue	R/W	R	R

Settings	Off	Level 1	Level 2
Memory Overflow	R/W	R	R
Rotate by 180 Degrees	R/W	R	R
Duplex	R/W	R	R
Copies	R/W	R	R
Blank Page Print	R/W	R	R
Sub Paper Size	R/W	R	R
Page Size	R/W	R/W	R
Letterhead Setting	R/W	R	R
Bypass Tray Setting Priority	R/W	R	R
Edge to Edge Print	R/W	R	R
Tray Switching	R/W	R	R
Extended Auto Tray Switching	R/W	R	R

Host Interface

Settings	Off	Level 1	Level 2
I/O Buffer	R/W	R	R
I/O Timeout	R/W	R	R

PCL Menu

Settings	Off	Level 1	Level 2
Orientation	R/W	R	R
Form Lines	R/W	R	R
Font Source	R/W	R	R
Font Number	R/W	R	R
Point Size	R/W	R	R
Font Pitch	R/W	R	R

Settings	Off	Level 1	Level 2
Symbol Set	R/W	R	R
Courier Font	R/W	R	R
Extend A4 Width	R/W	R	R
Append CR to LF	R/W	R	R
Resolution	R/W	R	R

Facsimile Features

When administrator authentication is specified, the administrator's configuration of Menu Protect determines which functions and settings are available to users. If user authentication is specified, functions and settings are available to authorized users only, who must log in to access them.

The following settings can be specified by someone who is not an administrator.

- Abbreviations in the table columns

  R/W (Read and Write) = Both reading and modifying the setting are available.

  R (Read) = Reading only.

  N/A (Not Applicable) = Neither reading nor modifying the setting is available.

Note

- Settings that are not in the list can only be viewed, regardless of the menu protect level setting.

The default for [Menu Protect] is [Off].

General Settings / Adjust

Settings	Off	Level 1	Level 2
Adjust Sound Volume	R/W	R/W	R
Program Fax Information	R/W	R	R
On Hook Mode Release Time	R/W	R/W	R
Set User Function Key	R/W	R/W	R

Reception Settings

Settings	Off	Level 1	Level 2
Switch Reception Mode	R/W	R	R
Authorized Reception	R/W	R	R
Checkered Mark	R/W	R/W	R
Center Mark	R/W	R/W	R
Print Reception Time	R/W	R/W	R
FAX Print Colour	R/W	R/W	R

Administrator Tools

Settings	Off	Level 1	Level 2
Print Journal	R/W	R/W	R
Print TX Standby File List	R/W	R/W	R
Memory Lock	R/W	R/W	R
Forwarding	R/W	R	R
Parameter Setting	R/W	R	R
Program Special Sender	R/W	R	R
Program Memory Lock ID	R/W	R	R
Select Dial/Push Phone	R/W	R	R
G3 Analog Line	R/W	R	R

System Settings

When administrator authentication is specified, the administrator's configuration of Available Settings determines which system settings are available to users. If user authentication is specified, system settings are available to authorized users only, who must log in to access them.

- Abbreviations in the table heads

  A = Authorized user when Available Settings have not been specified.

  B = Authorized user when Available Settings have been specified.

  C = Unauthorized user.

- 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	A	B	C
Prog./Change/Del User Text	R/W	R	N/A
Panel Key Sound	R/W	R	N/A
Warm-up Beeper	R/W	R	N/A
Copy Count Display	R/W	R	N/A
Function Priority	R/W	R	N/A
Output: Copier	R/W	R	N/A
Output: Facsimile	R/W	R	N/A
Output: Printer	R/W	R	N/A
Display Contrast	R/W	R	N/A
Key Repeat	R/W	R	N/A
Measurement Unit	R/W	R	N/A
Copier/Printer Mem. Usage	R/W	R	N/A

Tray Paper Settings

Settings	A	B	C
Tray Paper Size: Tray 1-4	R/W	R	N/A
Printer Bypass Paper Size	R/W	R	N/A
Paper Type: Bypass Tray	R/W	R	N/A
Paper Type: Tray 1-4	R/W	R	N/A
Ppr Tray Priority:Copier	R/W	R	N/A
Ppr Tray Priority:Fax	R/W	R	N/A
Ppr Tray Priority:Printer	R/W	R	N/A

Timer Settings

Settings	A	B	C
Auto Off Timer	R/W	R	N/A
Panel Off Timer	R/W	R	N/A
System Auto Reset Timer	R/W	R	N/A
Copier Auto Reset Timer	R/W	R	N/A
Facsimile Auto Reset Timer	R/W	R	N/A
Printer Auto Reset Timer	R/W	R	N/A
Scanner Auto Reset Timer	R/W	R	N/A
Set Date	R/W	R	N/A
Set Time	R/W	R	N/A
Auto Logout Timer	R/W	R	N/A

Interface Settings

Settings	A	B	C
Print I/F Setting List	R/W	N/A	N/A

Network

Settings	A	B	C
Machine IPv4 Address*1	R/W	R	N/A
IPv4 Gateway Address	R/W	R	N/A
IPv6 Stateless Setting	R/W	R	N/A
DNS Configuration*1	R/W	R	N/A
DDNS Configuration	R/W	R	N/A
IPsec	R/W	R	N/A
Domain Name*1	R/W	R	N/A
WINS Configuration*1	R/W	R	N/A
Effective Protocol	R/W	R	N/A
NCP Delivery Protocol	R/W	R	N/A
NW Frame Type	R/W	R	N/A
SMB Computer Name	R/W	N/A	N/A
SMB Work Group	R/W	N/A	N/A
Ethernet Speed	R/W	R	N/A
IEEE 802.1X Auth.(Ethernet)	R/W	R	N/A
Restr. IEEE802.1X Auth.Def.	R/W	R	N/A
Ping Command	R/W	R	N/A
Permit SNMPv3 Communictn.	R/W	R	N/A
Permit SSL/TLS Comm.	R/W	R	N/A
Host Name	R/W	R	N/A
Machine Name	R/W	R	N/A

*1 If you select [Auto-Obtain (DHCP)], you can only read the setting.

Administrator Tools

Settings	A	B	C
Address Book Management	R/W	R/W	N/A
Prgrm. /Change/Delete Group	R/W	R/W	N/A
Address Book:Print List	R/W	R/W	N/A
Display / Print Counter	R/W	R/W	N/A
Disp./Print User Counter	R/W	N/A	N/A
User Auth. Management	R/W	R	N/A
Admin.Auth.Management	R/W	N/A	N/A
Key Counter Management	R/W	R	N/A
Extended Security	R/W	R	N/A
Prog/Chnge/Del LDAP Server *6	R/W	R	N/A
LDAP Search	R/W	R	N/A
Prog./Change/Delete Realm	R/W	R	N/A
AOF(Always On)	R/W	R	N/A
Energy Saver Level	R/W	R	N/A
Service Mode Lock	R/W	R	N/A
Delete All Logs	R/W	R	N/A
Transfer log Setting	R/W	N/A	N/A

*6 Only the password can be specified.

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 has been specified.

If administrator authentication has been specified, the settings available to the user depend on whether or not "Available Settings" has been specified.

- Abbreviations in the table heads

  A = Authorized user when Available functions have not been specified.

  B = Authorized user when Available functions have been specified.

  C = Unauthorized user.

- 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	A	B	C
General Settings : Device Name	R/W	R	N/A
General Settings : Comment	R/W	R	N/A
General Settings : Location	R/W	R	N/A
Paper Tray Priority : Copier	R/W	R	N/A
Paper Tray Priority : Fax	R/W	R	N/A
Paper Tray Priority : Printer	R/W	R	N/A

Paper

Settings	A	B	C
Tray1 : Paper Size	R/W	R	N/A
Tray1 : Custom Paper Size	R/W	R	N/A
Tray1 : Paper Type	R/W	R	N/A
Tray1 : Apply Auto Paper Select	R/W	R	N/A
Tray1 : Apply Duplex	R/W	R	N/A

Settings	A	B	C
Tray2 : Paper Size	R/W	R	N/A
Tray2 : Custom Paper Size	R/W	R	N/A
Tray2 : Paper Type	R/W	R	N/A
Tray2 : Apply Auto Paper Select	R/W	R	N/A
Tray2 : Apply Duplex	R/W	R	N/A
Tray3 : Paper Size	R/W	R	N/A
Tray3 : Custom Paper Size	R/W	R	N/A
Tray3 : Paper Type	R/W	R	N/A
Tray3 : Apply Auto Paper Select	R/W	R	N/A
Tray3 : Apply Duplex	R/W	R	N/A
Tray4 : Paper Size	R/W	R	N/A
Tray4 : Custom Paper Size	R/W	R	N/A
Tray4 : Paper Type	R/W	R	N/A
Tray4 : Apply Auto Paper Select	R/W	R	N/A
Tray4 : Apply Duplex	R/W	R	N/A
Bypass Tray : Paper Size	R/W	R	N/A
Bypass Tray : Custom Paper Size	R/W	R	N/A
Bypass Tray : Paper Type	R/W	R	N/A

Date/Time

Settings	A	B	C
Set Date	R/W	R	N/A
Set Time	R/W	R	N/A
SNTP Server NAME	R/W	R	N/A
SNTP Polling Interval	R/W	R	N/A

Settings	A	B	C
Time Zone	R/W	R	N/A

Timer

Settings	A	B	C
Auto Off Timer	R/W	R	N/A
Panel Off Timer	R/W	R	N/A
System Auto Reset Timer	R/W	R	N/A
Copier Auto Reset Timer	R/W	R	N/A
Facsimile Auto Reset Timer	R/W	R	N/A
Scanner Auto Reset Timer	R/W	R	N/A
Printer Auto Reset Timer	R/W	R	N/A
Auto Logout Timer	R/W	R	N/A

Logs

Settings	A	B	C
Collect Job Logs	R/W	R	N/A
Job Log Collect Level	R/W	R	N/A
Collect Access Logs	R/W	R	N/A
Access Log Collect Level	R/W	R	N/A
Transfer Logs	R	R	N/A
Encrypt Logs	R	R	N/A
Classification Code	R/W	R	N/A
Delete All Logs	R/W	N/A	N/A

User Authentication Management

Settings	A	B	C
User Authentication Management	R/W	R	N/A
User Code Authentication - Printer Job Authentication	R/W	R	N/A
User Code Authentication - Available Function	R/W	R	N/A
Basic Authentication - Printer Job Authentication	R/W	R	N/A
Basic Authentication - Available Function	R/W	R	N/A
Windows Authentication - Printer Job Authentication	R/W	R	N/A
Windows Authentication - SSL	R/W	R	N/A
Windows Authentication - Kerberos Authentication	R/W	R	N/A
Windows Authentication - Domain Name	R/W	R	N/A
Windows Authentication - Realm Name	R/W	R	N/A
Windows Authentication - Group Settings for Windows Authentication	R/W	R	N/A
LDAP Authentication - Printer Job Authentication	R/W	R	N/A
LDAP Authentication - LDAP Authentication	R/W	R	N/A
LDAP Authentication - Login Name Attribute	R/W	R	N/A
LDAP Authentication - Unique Attribute	R/W	R	N/A
LDAP Authentication - Available Function	R/W	R	N/A
Integration Server Authentication - Printer Job Authentication	R/W	R	N/A
Integration Server Authentication - SSL	R/W	R	N/A
Integration Server Authentication - Integration Server Name	R/W	R	N/A

Settings	A	B	C
Integration Server Authentication - Authentication Type	R/W	R	N/A
Integration Server Authentication - Domain Name	R/W	R	N/A
Integration Server Authentication - Group Settings for Integration Server Authentication	R/W	R	N/A

LDAP Server

Settings	A	B	C
LDAP Search	R/W	N/A	N/A
Program/Change/Delete	R/W	N/A	N/A

Printer

If you have specified administrator authentication, the available functions and settings depend on the menu protect setting.

The following settings can be specified by someone who is not an administrator.

- Abbreviations in the table columns

  R/W (Read and Write) = Both reading and modifying the setting are available.

  R (Read) = Reading only.

  N/A (Not Applicable) = Neither reading nor modifying the setting is available.

The default for [Menu Protect] is [Level 2].

Printer Basic Settings

System

Settings	Off	Level 1	Level 2
Print Error Report	R/W	R	N/A
Auto Continue	R/W	R	N/A
Memory Overflow	R/W	R	N/A
Rotate by 180 Degrees	R/W	R	N/A
Blank Page Print	R/W	R	N/A
Sub Paper Size	R/W	R	N/A
Letterhead Setting	R/W	R	N/A
Bypass Tray Setting Priority	R/W	R	N/A
Extended Auto Tray Switching	R/W	R	N/A
Virtual Printer	R/W	R	N/A

Host Interface

Settings	Off	Level 1	Level 2
I/O Buffer	R/W	R	R
I/O Timeout	R/W	R	R

PCL Menu

Settings	Off	Level 1	Level 2
Orientation	R/W	R	R
Form Lines	R/W	R	R
Font Source	R/W	R	R
Font Number	R/W	R	R
Point Size	R/W	R	R
Font Pitch	R/W	R	R
Symbol Set	R/W	R	R
Courier Font	R/W	R	R
Extend A4 Width	R/W	R	R
Append CR to LF	R/W	R	R
Resolution	R/W	R	R

Virtual Printer Settings

Settings	Off	Level 1	Level 2
Details	R/W	R	N/A
Select Virtual Printer	R/W	R/W	N/A

Fax

If you have specified administrator authentication, the available functions and settings depend on the menu protect setting.

The following settings can be specified by someone who is not an administrator.

- Abbreviations in the table columns

  R/W (Read and Write) = Both reading and modifying the setting are available.

  R (Read) = Reading only.

  N/A (Not Applicable) = Neither reading nor modifying the setting is available.

The default for [Menu Protect] is [Off].

Administrator Tools

Settings	Off	Level 1	Level 2
Memory Lock Reception	R/W	N/A	N/A
Program Memory Lock ID	R/W	N/A	N/A
Select Extension / Outside	R/W	N/A	N/A
Outside Access No.	R/W	N/A	N/A

General Settings

Settings	Off	Level 1	Level 2
Switch Reception Mode	R/W	N/A	N/A
Fax Header	R/W	N/A	N/A
Own Name	R/W	N/A	N/A
Own Fax Number	R/W	N/A	N/A
Switch Reception Mode	R/W	N/A	N/A
Paper Tray	R/W	R/W	N/A
FAX Print Color	R/W	R/W	N/A

Parameter Settings

Settings	Off	Level 1	Level 2
Just Size Printing	R/W	N/A	N/A
Combine 2 Originals	R/W	N/A	N/A
Journal	R/W	N/A	N/A
Immediate Transmission Result Report	R/W	N/A	N/A
Communication Result Report	R/W	N/A	N/A
Memory Storage Report	R/W	N/A	N/A
SEP Code RX Result Report	R/W	N/A	N/A
SEP Code RX Reserve Report	R/W	N/A	N/A
LAN-Fax Result Report	R/W	N/A	N/A
Inclusion of Part of Image	R/W	N/A	N/A

Interface

The settings available to the user depend on whether or not administrator authentication has been specified.

If administrator authentication has been specified, the settings available to the user depend on whether or not "Available Settings" has been specified.

- Abbreviations in the table heads

  A = Authorized user when Available functions have not been specified.

  B = Authorized user when Available functions have been specified.

  C = Unauthorized user.

- 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	A	B	C
Ethernet : Ethernet Security	R/W	R	N/A
USB	R/W	R	N/A
PictBridge	R/W	R	N/A

Network

The settings available to the user depend on whether or not administrator authentication has been specified.

If administrator authentication has been specified, the settings available to the user depend on whether or not "Available Settings" has been specified.

- Abbreviations in the table heads

  A = Authorized user when Available functions have not been specified.

  B = Authorized user when Available functions have been specified.

  C = Unauthorized user.

- 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	A	B	C
Host Name	R/W	R	N/A
DHCP	R/W	R	N/A
Domain Name	R/W	R	N/A
IPv4 Address	R/W	R	N/A
Subnet Mask	R/W	R	N/A
DDNS	R/W	R	N/A
WINS	R/W	R	N/A
Primary WINS Server	R/W	R	N/A
Secondary WINS Server	R/W	R	N/A
Scope ID	R/W	R	N/A
Default Gateway Address	R/W	R	N/A
DNS Server	R/W	R	N/A
LPR	R/W	R	N/A
RSH/RCP	R/W	R	N/A

Settings	A	B	C
DIPRINT	R/W	R	N/A
FTP	R/W	R	N/A
sftp	R/W	R	N/A
WSD (Device)	R/W	R	N/A
WSD (Printer)	R/W	R	N/A
IPP	R/W	R	N/A
WSD (Printer) / IPP Timeout	R/W	R	N/A
RHPP	R/W	R	N/A

IPv6

Settings	A	B	C
IPv6	R/W	R	N/A
Host Name	R/W	R	N/A
Domain Name	R/W	R	N/A
Stateless Address	R/W	R	N/A
Manual Configuration Address	R/W	R	N/A
DCHPv6-lite	R/W	R	N/A
DDNS	R/W	R	N/A
Default Gateway Address	R/W	R	N/A
DNS Server	R/W	R	N/A
LPR	R/W	R	N/A
RSH/RCP	R/W	R	N/A
DIPRINT	R/W	R	N/A
FTP	R/W	R	N/A
sftp	R/W	R	N/A

Settings	A	B	C
WSD (Device)	R/W	R	N/A
WSD (Printer)	R/W	R	N/A
IPP	R/W	R	N/A
WSD (Printer) / IPP Timeout	R/W	R	N/A
RHPP	R/W	R	N/A

NetWare

Settings	A	B	C
NetWare	R/W	R	N/A
Print Server Name	R/W	R	N/A
Logon Mode	R/W	R	N/A
File Server Name	R/W	R	N/A
NDS Tree	R/W	N/A	N/A
NDS Context Name	R/W	R	N/A
Operation Mode	R/W	R	N/A
Remote Printer No.	R/W	N/A	N/A
Job Timeout	R/W	N/A	N/A
Frame Type	R/W	R	N/A
Print Server Protocol	R/W	R	N/A
NCP Delivery Protocol	R/W	R	N/A

SMB

Settings	A	B	C
SMB	R/W	R	N/A
Workgroup Name	R/W	R	N/A
Computer Name	R/W	R	N/A

Settings	A	B	C
Comment	R/W	R	N/A
Notify Print Completion	R/W	R	N/A

Bonjour

Settings	A	B	C
Bonjour	R/W	R	N/A
Computer Name	R/W	R	N/A
Location	R/W	R	N/A
DIPRINT	R/W	R	N/A
LPR	R/W	R	N/A
IPP	R/W	R	N/A

Webpage

The settings available to the user depend on whether or not administrator authentication has been specified.

If administrator authentication has been specified, the settings available to the user depend on whether or not "Available Settings" has been specified.

- Abbreviations in the table heads

  A = Authorized user when Available functions have not been specified.

  B = Authorized user when Available functions have been specified.

  C = Unauthorized user.

- 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	A	B	C
Language 1	R/W	R	N/A
Language 2	R/W	R	N/A
URL 1	R/W	R	N/A
URL 2	R/W	R	N/A
Set Help URL Target	R/W	R	N/A
WSD (Device) / UPnP Setting	R/W	R	N/A
Download Help File	R/W	R/W	N/A

Functions That Require Options

The following functions require certain options and additional functions.

- Data security for copying function

  Copy Data Security Unit

Trademarks

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

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

NetWare is a registered trademark of Novell, Inc.

UPnP™ is a trademark of the UPnP™ Implementers Corporation.

PCL® is a registered trademark of Hewlett-Packard Company.

Apple, Bonjour, Macintosh, and Mac OS are trademarks of Apple Inc., registered in the U.S. and other countries.

Monotype is a registered trademark of Monotype Imaging, Inc.

Solaris is a trademark or registered trademark of Sun Microsystems, Inc. in the United States and other countries.

LINUX® is the registered trademark of Linus Torvalds in the U.S. and other countries.

RED HAT is a registered trademark of Red Hat, Inc.

PowerPC® is a trademark of International Business Machines Corporation in the United States, other countries, or both.

Other product names used herein are for identification purposes only and might be trademarks of their respective companies. We disclaim any and all rights to those marks.

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

* The product names of Windows 2000 are as follows:

Microsoft® Windows® 2000 Professional

Microsoft® Windows® 2000 Server

Microsoft® Windows® 2000 Advanced Server

* The product names of Windows XP are as follows:

Microsoft® Windows® XP Professional

Microsoft® Windows® XP Home Edition

Microsoft® Windows® XP Media Center Edition

Microsoft® Windows® XP Tablet PC Edition

* The product names of Windows Vista are as follows:

Microsoft® Windows Vista® Ultimate

Microsoft® Windows Vista® Enterprise

Microsoft® Windows Vista® Business

Microsoft® Windows Vista® Home Premium

Microsoft® Windows Vista® Home Basic

* The product names of Windows Server 2003 are as follows:

Microsoft® Windows Server® 2003 Standard Edition

Microsoft® Windows Server® 2003 Enterprise Edition

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

* The product names of Windows NT 4.0 are as follows:

Microsoft® Windows NT® Workstation 4.0

Microsoft® Windows NT® Server 4.0

INDEX

A

Access Control...127
Address Book Access Permission......................105
Address Book Privileges...................................213
Administrator...17
Administrator Authentication..................17, 23, 24
Administrator Privileges.......................................24
AH Protocol..153
AH Protocol + ESP Protocol..............................153
Authenticate Current Job..................................180
Authentication and Access Limits.........................16
Authentication Information..................................54
authfree...175
Auto Logout..94
Available Functions...117

B

Basic Authentication...46

C

Change Firmware Structure..............................182
Copier Features...216
Creating the Device Certificate (Certificate Issued by a Certificate Authority).................................144

D

Data Security for Copying...................................99
Device Settings..227
Display..10
Driver Encryption Key..............................139, 178

E

Edit...213
Edit / Delete...213
Enabling/Disabling Protocols...........................128
Encrypt Address Book.......................................178
Encrypting the Data in the Address Book..........108
Encryption Key Auto Exchange / Manual Settings - Shared Settings...154
Encryption Key Auto Exchange Security Level........ 154
Encryption Key Auto Exchange Setting Items.......... 156
Encryption Key Auto Exchange Settings Configuration Flow...161
Encryption Key Manual Settings Configuration Flow..166
Encryption Key Manual Settings Items.............159
Encryption Technology..16
Enhance File Protection....................................179
Error Message..187
ESP Protocol..152
Extended Security Functions.............................177
Extended Security Supplement.........................244

F

Facsimile Features..220
Fax...234
File Administrator...22
File Administrator Settings................................210
Full Control..213

G

Group Password for PDF files...........................141
Guarding Against Unauthorized Copying..........97

I

Installing the Device Certificate (Certificate Issued by a Certificate Authority)................................145
Integration Server Authentication........................78
Interface...236
IP Address..11
IPP Authentication Password............................141
IPsec...152
IPsec Settings...154
IPsec telnet Setting Commands.........................167

L

Laws and Regulations...12
LDAP Authentication..69
LDAP Authentication - Operational Requirements for LDAP Authentication.......................................69
Log off (Administrator)...31
Log on (Administrator)..30
Login...17
Logout...17

M

Machine Administrator...22
Machine Administrator Settings.........................200

Menu Protect..111, 113

N

Network Administrator..22
Network Administrator Settings.........................207
Network Security Level.....................................135

O

Operational Issues...189

P

Password Policy..181
Printer..232
Printer Job Authentication...................................87
Printer Job Authentication Levels.........................87
Printer Job Types..88

R

Read-only..213
Registered User...17, 213
Registering the Administrator...............................26
Remote Service..181
Restrict Adding of User Destinations.................179
Restrict Display of User Information..................179
Restrict Use of Destinations................................178
Restrict Use of Simple Encryption......................180
Restrictions on Destinations...............................103

S

Security Functions..183
Self-Signed Certificate...143
Service Mode Lock..184
Settings by SNMP v1 and v2..............................180
SNMPv3...149
SSL...146
SSL (Secure Sockets Layer)...............................142
SSL / TLS Encryption..147
Supervisor...22, 193
Symbols..10
System Settings...222

T

telnet...175
Transfer Log Setting..120
Transfer to Fax Receiver......................................180
Transmitted Passwords.......................................139
Type of Administrator...111

U

Unauthorized Copy Prevention............................98
Update Firmware...181
User...17, 35
User Administrator...213
User Administrator Settings...............................211
User Authentication...........................17, 36, 39, 89
User Code Authentication....................................40
User Lockout Function...91
User Settings - Control Panel Settings...............215
User Settings - Web Image Monitor Settings..........
....226

W

Windows Authentication.....................................58
Windows Authentication - Operational Requirements for Kerberos Authentication..........58
Windows Authentication - Operational Requirements for NTLM Authentication..............58

MEMO

MEMO

Operating Instructions Security Reference

Type for MP C2030/Aficio MP C2030
Type for MP C2530/Aficio MP C2530

AE AE D040-7762