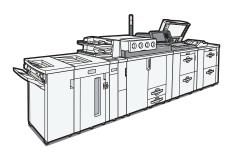


Pro C901s

Operating Instructions Security Reference



- 1 Getting Started
- 2 Authentication and its Application
- 3 Ensuring Information Security
- 4 Managing Access to the Machine
- 5 Enhanced Network Security
- 6 Specifying the Extended Security Functions
- 7 Troubleshooting
- 8 Appendix

TABLE OF CONTENTS

Manuals for This Machine	6
Notice	8
Important	8
How to Read This Manual	9
Symbols	9
Names of Major Items	9
IP Address	9
Notes	10
1. Getting Started	
Before Using the Security Functions	11
Setting Up the Machine	12
Enhanced Security	16
Glossary	17
Security Measures Provided by this Machine	19
Using Authentication and Managing Users	
Ensuring Information Security	19
Limiting and Controlling Access	
Enhanced Network Security	21
2. Authentication and its Application	
Administrators and Users	
Administrators	23
User	24
The Management Function	26
About Administrator Authentication	26
About User Authentication	27
Enabling Authentication	29
Authentication Setting Procedure	
Administrator Authentication	
Specifying Administrator Privileges	
Registering the Administrator	
Logging in Using Administrator Authentication	
Logging out Using Administrator Authentication	
Changing the Administrator	

Using Web Image Monitor to Configure Administrator Authentication	38
User Authentication	39
User Code Authentication.	40
Specifying User Code Authentication	40
Basic Authentication	42
Specifying Basic Authentication	42
Authentication Information Stored in the Address Book	43
Specifying Login User Name and Login Password	43
Specifying Authentication Information to Log in	46
Windows Authentication.	48
Specifying Windows Authentication	49
Installing Internet Information Services (IIS) and Certificate services	52
Creating the Server Certificate	52
Installing the Device Certificate (Certificate Issued by a Certificate Authority)	53
LDAP Authentication	55
Specifying LDAP Authentication	56
Integration Server Authentication.	60
Specifying Integration Server Authentication	60
If User Authentication is Specified	64
If User Code Authentication is Specified	64
If Basic, Windows, LDAP or Integration Server Authentication is Specified	65
Logging in Using Web Image Monitor	66
Logging out Using Web Image Monitor	66
Auto Logout	66
Authentication Using an External Device	69
3. Ensuring Information Security	
Specifying Access Permission for Stored Files	71
Assigning Users and Access Permission for Stored Files	72
Changing the Owner of a Document	74
Specifying Access Privileges for Files Stored using the Scanner Function	75
Assigning the User and the Access Permission for the User's Stored Files	79
Specifying Passwords for Stored Files	80
Unlocking Files.	82

Preventing Data Leaks Due to Unauthorized Transmission	84
Restrictions on Destinations	84
Using S/MIME to Protect E-mail Transmission	86
E-mail Encryption	86
Attaching an Electronic Signature	88
Protecting the Address Book	94
Address Book Access Permission	94
Encrypting Data in the Address Book	95
Deleting Data on the Hard Disk	98
Auto Erase Memory	98
Erase All Memory	102
4. Managing Access to the Machine	
Preventing Modification of Machine Settings	107
Menu Protect	109
Enabling Menu Protect	109
Disabling Menu Protect	109
Specifying Menu Protect	109
Limiting Available Functions	112
Specifying Which Functions are Available	112
5. Enhanced Network Security	
Preventing Unauthorized Access	
Access Control	115
Enabling/Disabling Protocols	116
Specifying Network Security Level	121
Encrypting Transmitted Passwords	125
Driver Encryption Key	125
Protection Using Encryption	
SSL (Secure Sockets Layer) Encryption	127
User Settings for SSL (Secure Sockets Layer)	132
Setting the SSL / TLS Encryption Mode	132
SNMPv3 Encryption	134
Transmission Using IPsec	136
Encryption and Authentication by IPsec	136

Encryption Key Auto Exchange Settings and Encryption Key Manual Settings	
IPsec Settings	138
Encryption Key Auto Exchange Settings Configuration Flow	146
Encryption Key Manual Settings Configuration Flow	151
telnet Setting Commands	152
6. Specifying the Extended Security Functions	
Specifying the Extended Security Functions	
Changing the Extended Security Functions	161
Extended Security Settings	162
Other Security Functions	165
Scanner Function	165
System Status	165
Weekly Timer Code	165
Limiting Machine Operation to Customers Only	168
Settings	168
7. Troubleshooting	
Authentication Does Not Work Properly	171
A Message Appears	171
An Error Code Appears	173
Machine Cannot Be Operated	188
8. Appendix	
Supervisor Operations	193
Logging in as the Supervisor	193
Logging out as the Supervisor	194
Changing the Supervisor	194
Resetting an Administrator's Password	195
Machine Administrator Settings	197
System Settings	197
Maintenance	199
Copier / Document Server Features	199
Scanner Features	200
Tray Paper Settings	200
Settings via Web Image Monitor	200

Network Administrator Settings	204
System Settings	204
Scanner Features	205
Settings via Web Image Monitor	205
File Administrator Settings	208
System Settings	208
Settings via Web Image Monitor	208
User Administrator Settings	210
System Settings	210
Settings via Web Image Monitor	211
Document Server File Permissions	212
The Privilege for User Account Settings in the Address Book	213
User Settings - Control Panel Settings	216
Copier / Document Server Features	217
Scanner Features.	224
System Settings	226
Maintenance	232
Tray Paper Settings	233
User Settings - Web Image Monitor Settings	234
Device Settings	235
Scanner	241
Network	243
Webpage	246
Functions That Require Options	247
Trademarks	248
INDEX	251

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.

Mportant !

- Media differ according to manual.
- The printed and electronic versions of a manual have the same contents.
- Adobe Acrobat Reader/Adobe Reader must be installed in order to view the manuals as PDF files.
- A Web browser must be installed in order to view the html manuals.
- For enhanced security, we recommend that you first make the following settings. For details, see
 "Setting Up the Machine".
 - Install the Device Certificate.
 - Enable SSL (Secure Sockets Layer) Encryption.
 - Change the user name and password of the administrator using Web Image Monitor.

About This Machine

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

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

Troubleshooting

Provides a guide to solving common usage-related problems, and explains how to replace paper, toner, staples, and other consumables.

Copy/Document Server Reference

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

Scanner Reference

Explains Scanner functions and operations.

Network Guide

Explains how to configure and operate the machine in a network environment.

General Settings Guide

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

Paper Settings Reference

Explains how to make paper settings.

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.



- In addition to the above, manuals are also provided for the Printer function.
- The following optional software products are referred to using general names:

Product name	General name
ScanRouter EX Professional and ScanRouter EX Enterprise	the ScanRouter delivery software

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 manufacturer recommends that you use genuine toner from the manufacturer.

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

How to Read This Manual

Symbols

This manual uses the following symbols:

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.

UNote

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

Reference

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

[]

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

Names of Major Items

Major items of this machine are referred to as follows in this manual:

- Auto Document Feeder → ADF
- Z-folding Unit ZF4000 (optional) → Z-folding unit
- Trimmer Unit TR5020 (optional) → Trimmer
- High Capacity Stacker SK5010 (optional) → Stacker
- Ring Binder RB5000 (optional) → Ring binder
- Perfect Binder GB5000 (optional) → Perfect binder
- Data OverWriteSecurity Unit Type H (optional) → DataOverwriteSecurity unit

IP Address

In this manual, "IP address" covers both IPv4 and IPv6 environments. Read the instructions that are relevant to the environment you are using.

Notes

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

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.

1. Getting Started

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

Before Using the Security Functions

- If the security settings are not configured, the data in the machine is vulnerable to attack.
- 1. To prevent this machine being stolen or willfully damaged, etc., install it in a secure location.
- 2. Purchasers of this machine must make sure that people who use it do so appropriately, in accordance with operations determined by the machine administrator and supervisor. If the administrator or supervisor does not make the required security settings, there is a risk of security breaches by users.
- 3. Before setting this machine's security features and to ensure appropriate operation by users, administrators must read the Security 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.

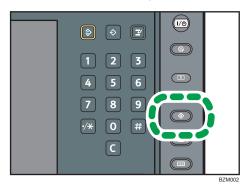
11

Setting Up the Machine

This section describes how to enable encryption of transmitted data and configure the administrator account. If you want a high level of security, make the following setting before using the machine.

Enabling security

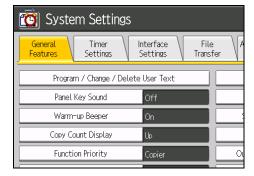
- 1. Turn the machine on.
- 2. Press the [User Tools] key.



3. Press [System Settings].



4. Press [Interface Settings].



1

5. Specify IPv4 Address.

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

- 6. Be sure to connect this machine to a network that only administrators can access.
- 7. Start Web Image Monitor, and then log in to the machine as the administrator.

For details about logging in to Web Image Monitor as an administrator, see "Using Web Image Monitor to Configure Administrator Authentication".

8. Click [Configuration], and then click [E-mail] under "Device Settings".

The E-mail page appears.

- 9. Enter the machine administrator's e-mail address in [Administrator E-mail Address], and then, click [OK].
- 10. Install the device certificate.

For details about installing the device certificate, see "Protection Using Encryption".

11. Enable secure sockets layer (SSL).

For details about enabling SSL, see "Enabling SSL".

12. Change the administrator's user name and password.

To enable higher security, proceed to step 2 in the following "Enabling enhanced security".

- 13. Log out, and then quit Web Image Monitor.
- 14. Disconnect the machine from the administrators-only network, and then connect it to the general use network.

Enabling enhanced security

- Configure the security settings for the machine by following steps 1 to 12 of the previous procedure ("Enabling Security").
- 2. Click [Configuration], and then click [Network Security] under "Security".

The Network Security page appears.

3. Set "Network Security" to [Level 2].

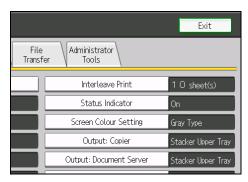
Only ports that have high security can be used. Note that some functions will be unavailable after you select [Level 2] for this setting. For details, see "Status of Functions under each Network Security Level" and "Enabling/Disabling Protocols".

Set both "FTP" with high security risk and "SNMPv3 Function" to [Inactive], and then click [OK] twice.

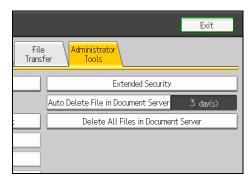
For details about the functions that will be unavailable if "FTP" and "SNMPv3" are set to [Inactive], see "Enabling/Disabling Protocols".

- 5. Log out, and then quit Web Image Monitor.
- 6. Press the [User Tools] key on the control panel.
- 7. Press [System Settings].

8. Press [Administrator Tools].

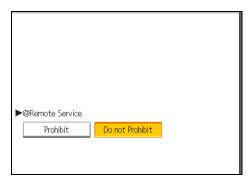


9. Press [Extended Security].



If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

10. Set [@Remote Service] to [Prohibit].



For details about "Update Firmware", see the following "Firmware Update Cautions".

- 11. Press [OK].
- 12. Press the [User Tools] key.
- 13. Disconnect the machine from the administrators-only network, and then connect it to the general use network.

Firmware Update Cautions

If "IPsec" is enabled, all information on the network will be encrypted. This allows you to perform firmware updates securely.

If "IPsec" is not enabled, the information on the network may not be encrypted depending on the protocol. If you want to perform a firmware update when "IPsec" is not enabled, be sure to do so only if your network environment is protected against electronic eavesdropping and similar security threats.

Reference

- p.38 "Using Web Image Monitor to Configure Administrator Authentication"
- p.116 "Enabling/Disabling Protocols"
- p.123 "Status of Functions under each Network Security Level"
- p.127 "Protection Using Encryption"
- p.131 "Enabling SSL"

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 manufacturer 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 data stored in the machine.

For details about the administrator and user roles, see "Administrators and Users".

Encryption Technology

This machine can establish secure communication paths by encrypting transmitted data and passwords.



• p.23 "Administrators and 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.

Supervisor

The supervisor can reset an administrator's password. This is required if an administrator's password is lost or revealed, or if an administrator is changed.

The supervisor can neither perform normal operations nor specify default settings.

User

A user performs normal operations on the machine.

File Creator (Owner)

This is a user who can store files in the machine and authorize other users to view, edit, or delete those files.

Registered User

Users with personal information registered in the address book who have a login password and user

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 are stored in the machine's address book. The personal information can be obtained from the Windows domain controller (Windows authentication), LDAP Server (LDAP authentication), or Integration Server (Integration Server authentication) connected to the machine via the network. The "Integration Server" is the computer on which Authentication Manager is installed.

Login

This action is required for administrator authentication and user authentication. Enter your login user name and login password on the machine's control panel. You might have to enter your login user name and password when accessing the machine over a network or using utilities such as Web Image Monitor.

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 "Enabling Authentication".

Specifying Authentication Information to Log in

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 in, 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.29 "Enabling Authentication"
- p.42 "Basic Authentication"
- p.112 "Limiting Available Functions"

Ensuring Information Security

Protecting Stored Files from Unauthorized Access

You can specify who is allowed to use and access scanned files and the files in Document Server.

You can prevent activities such as the printing of stored files by unauthorized users. For details about protecting stored files from unauthorized access, see "Specifying Access Permission for Stored Files".

Protecting Stored Files from Theft

You can specify who is allowed to use and access scanned files and the files in Document Server.

You can prevent activities such as the sending and downloading of stored files by unauthorized users.

For details about protecting stored files from theft, see "Specifying Access Permission for Stored Files".

Preventing Data Leaks Due to Unauthorized Transmission

You can specify in the Address Book which users are allowed to send files using the scanner 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".

Using S/MIME to Protect E-mail Transmission

When sending mail from the scanner to a user registered in the Address Book, you can use S/MIME to protect its contents from interception and alteration, and attach an electronic signature to guarantee the sender's identity. For details about using S/MIME to protect e-mail transmission, see "Using S/MIME to Protect E-mail Transmission".

Protecting Registered Information in the Address Book

You can specify who is allowed to access the data in the address book. You can prevent the data in the address book being used by unregistered users.

To protect the data from unauthorized reading, you can also encrypt the data in the address book. For details about protecting registered information in the address book, see "Protecting the Address Book".

Overwriting the Data on the Hard Disk

To prevent data leaks, you can set the machine to automatically overwrite temporary data. We recommend that before disposing of the machine, you overwrite all the data on the hard disk.

To overwrite the hard disk data, the DataOverwriteSecurity unit is required. For details about overwriting the data on the hard disk, see "Deleting Data on the Hard Disk".

Reference

- p.71 "Specifying Access Permission for Stored Files"
- p.84 "Preventing Data Leaks Due to Unauthorized Transmission"
- p.86 "Using S/MIME to Protect E-mail Transmission"
- p.94 "Protecting the Address Book"
- p.98 "Deleting Data on the Hard Disk"

Limiting and Controlling Access

Preventing Modification or Deletion of Stored Data

You can allow selected users to access stored scan files and files stored in Document Server.

You can permit selected users who are allowed to access stored files to modify or delete the files. For details about limiting and controlling access, see "Specifying Access Permission for Stored Files".

Preventing Modification of Machine Settings

The machine settings that can be modified depend on the type of administrator account.

Register the administrators so that users cannot change the administrator settings. For details about preventing modification of machine settings, see "Preventing 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.71 "Specifying Access Permission for Stored Files"
- p.107 "Preventing Modification of Machine Settings"
- p.112 "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, stored files, and default settings. For details about preventing unauthorized access, see "Preventing Unauthorized Access".

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.115 "Preventing Unauthorized Access"
- p.127 "Protection Using Encryption"
- p.136 "Transmission Using IPsec"

2. Authentication and its Application

This chapter describes how to register the administrator and specify the authentication methods. How to log in and log out once authentication is enabled is also described here.

Administrators and Users

When controlling access using the authentication method specified by an administrator, select the machine's administrator, enable the authentication function, and then use the machine.

The administrators manage access to the allocated functions, and users can use only the functions they are permitted to access. When the authentication function is enabled, the login user name and login password are required in order to use the machine.

Specify administrator authentication, and then specify user authentication.

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

Mportant !

• If user authentication is not possible because of a problem with the hard disk or network, you can use the machine by accessing it using administrator authentication and disabling user authentication. Do this if, for instance, you need to use the machine urgently.

Reference

• p.43 "Specifying Login User Name and Login Password"

Administrators

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. You can also specify a supervisor who can change each administrator's password. Administrators are limited to managing the machine's settings and controlling user access, so they cannot use functions such as copying and scanning. To use these functions, the administrator must register as a user in the Address Book and then be authenticated as the user.

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.

For instructions on registering the user administrator, see "Registering the Administrator".

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.

For instructions on registering the machine administrator, see "Registering the Administrator".

Network Administrator

This is the administrator who manages the network settings. You can set the machine so that network settings such as the IP address and settings for sending and receiving e-mail can only be specified by the network administrator.

By making this setting, you can prevent unauthorized users from changing the settings and disabling the machine, and thus ensure correct network operation.

For instructions on registering the network administrator, see "Registering the Administrator".

File Administrator

This is the administrator who manages permission to access stored files. You can specify passwords to allow only registered users with permission to view and edit files stored in Document Server. By making this setting, you can prevent data leaks and tampering due to unauthorized users viewing and using the registered data.

For instructions on registering the file administrator, see "Registering the Administrator".

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.

For instructions on registering the supervisor, see "Supervisor Operations".

Reference

- p.33 "Registering the Administrator"
- p.193 "Supervisor Operations"

User

Users are managed using the personal information 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.

2

For details about registering users in the address book, see "Registering Addresses and Users for Scanner Functions", General Settings Guide, or Web Image Monitor Help.

The Management Function

The machine has an authentication function requiring a login user name and login password. By using the authentication function, you can specify access limits for individual users and groups of users. Using access limits, you can not only limit the machine's available functions but also protect the machine settings and files and data stored in the machine. For instructions on changing the administrator's password, see "Supervisor Operations".



- 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.
- 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.

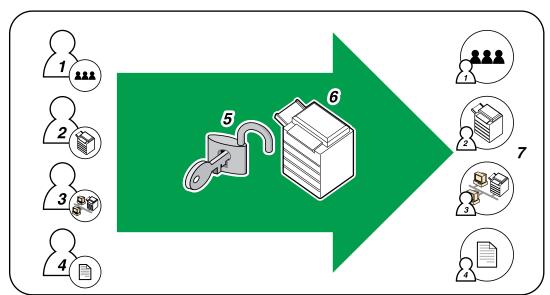
Reference

• p.193 "Supervisor Operations"

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 and Users".



BZM004

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. You can specify a security setting to allow only the machine administrator to configure system settings such as tray paper settings.

3. Network Administrator

This administrator manages the network settings. You can set the machine so that network settings such as the IP address and settings for sending and receiving e-mail can be specified by the network administrator only.

4. File Administrator

This is the administrator who manages permission to access stored files. You can specify passwords to allow only registered users with permission to view and edit files stored in Document Server. By making this setting, you can prevent data leaks and tampering due to unauthorized users viewing and using the registered data.

5. Authentication

Administrators must enter their login user name and password to be authenticated.

6. This machine

7. Administrators manage the machine's settings and access limits.

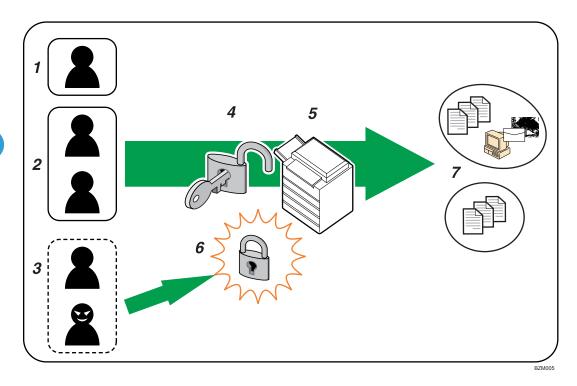
Reference

• p.23 "Administrators and Users"

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.



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.

Enabling Authentication

To control administrators' and users' access to the machine, perform administrator or user authentication using login user names and passwords. To perform authentication, the authentication function must be enabled. To specify authentication, you need to register administrators.

For instructions on registering the administrator, see "Registering the Administrator".



• p.33 "Registering the Administrator"

Authentication Setting Procedure

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

Administrator Authentication	Specifying Administrator Privileges
See "Administrator Authentication".	See "Specifying Administrator Privileges".
	Registering the Administrator
	See "Registering the Administrator".
User Authentication	Specifying User Authentication
See "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".



 To specify Basic Authentication, Windows Authentication, LDAP Authentication, or Integration Server Authentication, you must first enable user administrator privileges in Administrator Authentication Management. • You can specify User Code Authentication without specifying administrator authentication.

■ Reference

- p.31 "Administrator Authentication"
- p.31 "Specifying Administrator Privileges"
- p.33 "Registering the Administrator"
- p.39 "User Authentication"
- p.40 "User Code Authentication"
- p.42 "Basic Authentication"
- p.48 "Windows Authentication"
- p.55 "LDAP Authentication"
- p.60 "Integration Server Authentication"

Administrator Authentication

Administrators are handled differently from the users registered in the address book. When registering an administrator, you cannot use a login user name already registered in the address book. Windows Authentication, LDAP Authentication and Integration Server Authentication are not performed for an administrator, so an administrator can log in even if the server is unreachable due to a network problem.

Each administrator is identified by a login user name. One person can act as more than one type of administrator if multiple administrator authorities are granted to a single login user name. You can specify the login user name, login password, and encryption password for each administrator. The encryption password is the password for performing encryption when specifying settings with an application using SNMPv3. The password registered in the machine must also be entered in the application.

Administrators are limited to managing the machine's settings and controlling user access, so they cannot use functions such as copying and scanning. To use these functions, the administrator must register as a user in the Address Book and then be authenticated as the user.



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

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 in as an administrator, use the default login user name and login password.

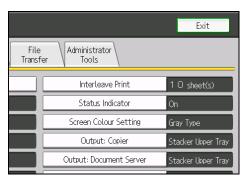
The defaults are "admin" for the login name and blank for the password.

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

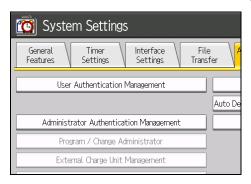


- If you have enabled [Administrator Authentication Management], make sure not to forget the
 administrator login user name and login password. If an administrator login user name or login
 password is forgotten, a new password must be specified using the supervisor's authority. For details
 about changing the administrator password using the supervisor's authority, see "Supervisor
 Operations".
- 1. Press the [User Tools] key.
- 2. Press [System Settings].

3. Press [Administrator Tools].

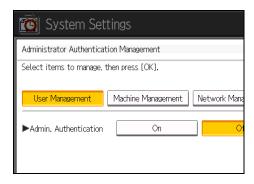


4. Press [Administrator Authentication Management].



If the setting to be specified does not appear, press [♥Next] to scroll down to other settings.

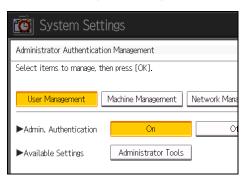
Press [User Management], [Machine Management], [Network Management], or [File Management] key to select which settings to manage.



6. Set "Admin. Authentication" to [On].

[&]quot;Available Settings" appears.

7. Select the settings to manage from "Available Settings".



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

- 8. Press [OK].
- 9. Press the [User Tools] key.



- "Available Settings" varies depending on the administrator.
- The settings selected in "Available Settings" for any of the administrators will be unavailable to users.
 For details about "Available Settings", see "Limiting Available Functions".

Reference

- p.36 "Logging in Using Administrator Authentication"
- p.37 "Logging out Using Administrator Authentication"
- p.112 "Limiting Available Functions"
- p.193 "Supervisor Operations"

Registering the Administrator

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

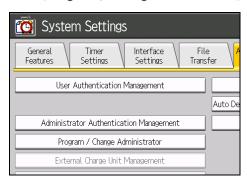
The sharing of administrator tasks eases the burden on individual administrators while also limiting unauthorized operation by a single administrator. You can register up to four login user names (Administrators 1-4) to which you can grant administrator privileges.

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 in using a registered administrator name and password.

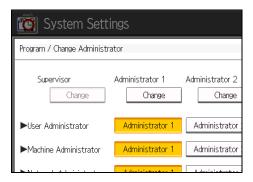
For details about logging in and logging out with administrator authentication, see "Logging in Using Administrator Authentication" and "Logging out Using Administrator Authentication".

- 1. Press the [User Tools] key.
- 2. Press [System Settings].
- 3. Press [Administrator Tools].
- 4. Press [Program / Change Administrator].

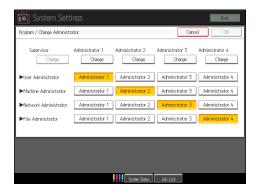


If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

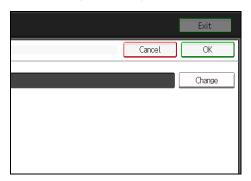
5. In the line for the administrator whose authority you want to specify, press [Administrator 1], [Administrator 2], [Administrator 3] or [Administrator 4], and then press [Change].



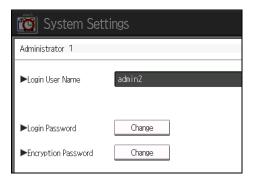
If you allocate each administrator's authority to a different person, the screen appears as follows:







- 7. Enter the login user name, and then press [OK].
- 8. Press [Change] for "Login Password".



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

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

For details about the password policy and how to specify it, see "Specifying the Extended Security Functions".

- 10. If a password reentry screen appears, enter the login password, and then press [OK].
- 11. Press [Change] for "Encryption Password".
- 12. Enter the encryption password, and then press [OK].
- 13. If a password reentry screen appears, enter the encryption password, and then press [OK].
- 14. Press [OK] twice.

You will be automatically logged out.

15. Press the [User Tools] key.



• 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. User names cannot contain numbers only, a space, colon (:), or quotation mark ("), nor can they be left blank.

For details about what characters the password can contain, see "Specifying the Extended Security Functions".

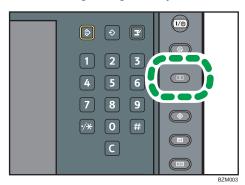
Reference

- p.36 "Logging in Using Administrator Authentication"
- p.37 "Logging out Using Administrator Authentication"
- p.161 "Specifying the Extended Security Functions"

Logging in Using Administrator Authentication

If administrator authentication has been specified, log in using an administrator's user name and password. This section describes how to log in.

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



The message, "Press [Login], then enter the login user name and login password." appears.

3. Press [Login].

If you do not want to log in, press [Cancel].

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

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

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

When the administrator is making settings for the first time, a password is not required; the administrator can simply press [OK] to proceed.

"Authenticating... Please wait." appears, followed by the screen for specifying the default.



- If user authentication has already been specified, a screen for authentication appears.
- To log in as an administrator, enter the administrator's login user name and login password.
- If you log in using administrator authority, the name of the administrator logging in appears.

- If the user name entered at login has multiple administrator privileges, any administrator name with administrator privileges will be displayed.
- If you try to log in from an operating screen, "You do not have the privileges to use this function. You
 can only change setting(s) as an administrator." appears. Press the [User Tools] key to change the
 default.

Logging out Using Administrator Authentication

If administrator authentication has been specified, be sure to log out after completing settings. This section describes how to log out after completing settings.

- 1. Press the [Login/Logout] key.
- 2. Press [Yes].

The message, "Logging out...Please wait." appears.

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 in and logging out with administrator authentication, see "Logging in Using Administrator Authentication" and "Logging out Using Administrator Authentication".

- 1. Press the [User Tools] key.
- 2. Press [System Settings].
- 3. Press [Administrator Tools].
- 4. Press [Program / Change Administrator].

If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

- 5. In the line for the administrator you want to change, press [Administrator 1], [Administrator 2], [Administrator 3] or [Administrator 4], and then press [Change].
- 6. Press [Change] for the setting you want to change, and re-enter the setting.
- 7. Press [OK].
- 8. Press [OK] twice.

You will be automatically logged out.

9. Press the [User Tools] key.



- An administrator's privileges can be changed only by an administrator who has the privileges of the administrator concerned.
- Administrator privileges cannot be revoked by any single administrator.

Reference

- p.36 "Logging in Using Administrator Authentication"
- p.37 "Logging out Using Administrator Authentication"

Using Web Image Monitor to Configure Administrator Authentication

Using Web Image Monitor, you can log in 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].

The Web browser might be configured to auto complete login dialog boxes by retaining user names and passwords. This function reduces security. To prevent the browser retaining user names and passwords, disable the browser's auto complete function.

- 5. Make settings as desired.
- 6. Click [Logout].



 When logging in 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.

User Authentication

There are five types of user authentication methods: User Code authentication, Basic authentication, Windows authentication, LDAP authentication, and Integration Server authentication. To use user authentication, select an authentication method on the control panel, and then make the required settings for the authentication. The settings vary depending on the authentication method.



- User Code authentication is used for authenticating on the basis of a user code, and Basic
 authentication, Windows authentication, LDAP authentication, and Integration Server authentication
 are used for authenticating individual users.
- A user code account, that has no more than eight digits and is used for User Code authentication,
 can be carried over and used as a login user name even after the authentication method has switched
 from User Code authentication to Basic authentication, Windows authentication, LDAP authentication,
 or Integration Server authentication. In this case, since the User Code authentication does not have
 a password, the login password is set as blank.
- When authentication switches to an external authentication method (Windows authentication, LDAP authentication, or Integration Server authentication), authentication will not occur, unless the external authentication device has the carried over user code account previously registered. However, the user code account will remain in the address book of the machine despite an authentication failure. From a security perspective, when switching from User Code authentication to another authentication method, we recommend that you delete accounts you are not going to use, or set up a login password. For details about deleting accounts, see "Deleting a Registered Name", 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.
- For printer job authentication, user code authentication is required.



p.43 "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. Specifying user code authentication allows you to enforce job authentication by user code.

For details about specifying user codes, see "Authentication Information", General Settings Guide.

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



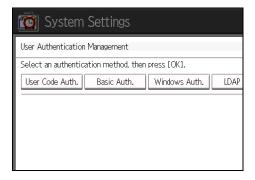
 To control the use of DeskTopBinder Professional for the delivery of files stored in the machine, select Basic Authentication, Windows Authentication, LDAP Authentication, or Integration Server Authentication.

Specifying User Code Authentication

This can be specified by the machine administrator.

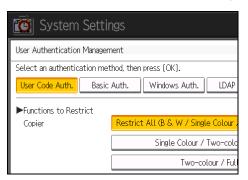
For details about logging in and logging out with administrator authentication, see "Logging in Using Administrator Authentication" and "Logging out Using Administrator Authentication".

- 1. Press the [User Tools] key.
- 2. Press [System Settings].
- 3. Press [Administrator Tools].
- Press [User Authentication Management].
 If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.
- 5. Select [User Code Auth.].



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

6. Select which of the machine's functions you want to limit.



The selected settings will be unavailable to users.

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

- 7. Press [OK].
- 8. Press the [User Tools] key.

A confirmation message appears.

If you press [Yes], you will be automatically logged out.

■ Reference

- p.36 "Logging in Using Administrator Authentication"
- p.37 "Logging out Using Administrator Authentication"
- p.112 "Limiting Available Functions"

Basic Authentication

Specify this authentication method when using the machine's address book to authenticate each user. Using Basic authentication, you can not only manage the machine's available functions but also limit access to stored files and to the personal data in the address book. Under Basic authentication, the administrator must specify the functions available to each user registered in the address book. For details about specifying which functions are available to which users, see "Authentication Information Stored in the Address Book".

Reference

• p.43 "Authentication Information Stored in the Address Book"

Specifying Basic Authentication

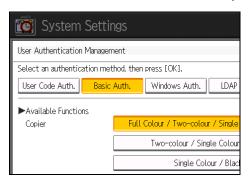
This can be specified by the machine administrator.

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

- 1. Press the [User Tools] key.
- 2. Press [System Settings].
- 3. Press [Administrator Tools].
- Press [User Authentication Management].
 If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.
- 5. Select [Basic Auth.].

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

6. Select which of the machine's functions you want to permit.



If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

The selected functions are registered as the initial settings for "Available Functions", in the address book. By specifying "Available Functions", you can limit the functions available to each user under Basic Authentication.

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

For details about printer job authentication, see "User Code Authentication".

- 7. Press [OK].
- 8. Press the [User Tools] key.

A confirmation message appears.

If you press [Yes], you will be automatically logged out.

Reference

- p.36 "Logging in Using Administrator Authentication"
- p.37 "Logging out Using Administrator Authentication"
- p.40 "User Code Authentication"
- p.112 "Limiting Available Functions"

Authentication Information Stored in the Address Book

This can be specified by the user administrator.

For details about logging in and logging out with administrator authentication, see "Logging in Using Administrator Authentication" and "Logging out 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 Web Image Monitor.

Reference

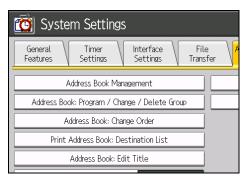
- p.36 "Logging in Using Administrator Authentication"
- p.37 "Logging out Using Administrator Authentication"

Specifying Login User Name and Login Password

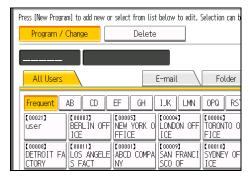
In [Address Book Management], specify the login user name and login password to be used for User Authentication Management.

- 1. Press the [User Tools] key.
- 2. Press [System Settings].
- 3. Press [Administrator Tools].

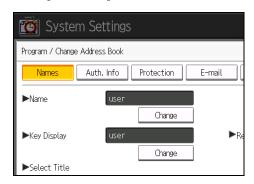
4. Press [Address Book Management].



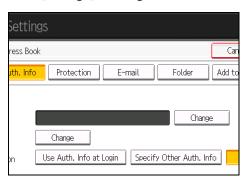
5. Select the user.



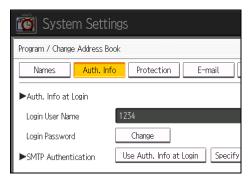
6. Press [Auth. Info].



7. Press [Change] for "Login User Name".



- 8. Enter a login user name, and then press [OK].
- 9. Press [Change] for "Login Password".



- 10. Enter a login password, and then press [OK].
- 11. If a password reentry screen appears, enter the login password, and then press [OK].
- 12. Press [OK].
- 13. Press [Exit].
- 14. Press the [User Tools] key.



- The administrator must inform general users concerning the number of characters that passwords can contain.
- Login user names and passwords can contain both alphanumeric characters and symbols.
- Login user names can contain up to 32 characters; passwords can contain up to 128 characters.
- Login user names cannot contain spaces, colons or quotation marks, and cannot be left blank.
- Do not use Japanese, Traditional Chinese, Simplified Chinese, or Hangul double-byte characters.
- If you use multi-byte characters when entering the login user name or password, you cannot
 authenticate using Web Image Monitor. For details about characters that the password can contain,
 see "Specifying the Extended Security Functions".

• p.161 "Specifying the Extended Security Functions"

Specifying Authentication Information to Log in

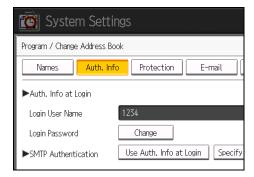
The login user name and password specified in [Address Book Management] can be used as the login information for "SMTP Authentication", "Folder Authentication", and "LDAP Authentication".

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

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



- When using [Use Auth. Info at Login] for "SMTP Authentication", "Folder Authentication", or "LDAP Authentication", a user name other than "other", "admin", "supervisor" or "HIDE***" must be specified. The symbol "***" represents any character.
- To use [Use Auth. Info at Login] for "SMTP Authentication", a login password up to 128 characters in length must be specified.
- 1. Press the [User Tools] key.
- 2. Press [System Settings].
- 3. Press [Administrator Tools].
- Press [Address Book Management].
 If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.
- 5. Select the user.
- 6. Press [Auth. Info].
- 7. Select [Use Auth. Info at Login] in "SMTP Authentication".



If the setting to be specified does not appear, press [\P Next] to scroll down to other settings.

9

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

- 8. Press [OK].
- 9. Press [Exit].
- 10. Press the [User Tools] key.
- **■** Reference
 - p.43 "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. If you can obtain user information, the sender's address (From:) is fixed to prevent unauthorized access when sending e-mails under the scanner function.

Operational Requirements for Windows Authentication

To specify Windows authentication, the following requirements must be met:

- This machine supports NTLMv1 authentication and NTLMv2 authentication.
- A domain controller has been set up in a designated domain.
- This function is supported by the operating systems listed below. To obtain user information when running Active Directory, use LDAP. If SSL is being used, a version of Windows that supports TLSv1, SSLv2, or SSLv3 is required.
 - Windows 2000 Server
 - Windows Server 2003/Windows Server 2003 R2
 - Windows Server 2008/Windows Server 2008 R2

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.
- If you have created a new user in the domain controller and selected "User must change password
 at next logon", log in to the machine from the computer to change the password before logging in
 from the machine's control panel.



- Remember that the login user names and passwords are 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.

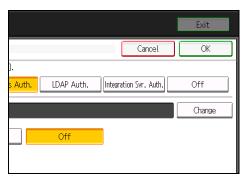
- If the "Guest" account on the Windows server is enabled, even users not registered in the domain controller can be authenticated. When this account is enabled, users are registered in the address book and can use the functions available under [*Default Group].
- Under Windows Authentication, you can select whether or not to use secure sockets layer (SSL)
 authentication.
- To automatically register user information under Windows authentication, we recommend that communication between the machine and domain controller is encrypted by SSL.
- Under Windows Authentication, you do not have to create a server certificate unless you want to automatically register user information.

Specifying Windows Authentication

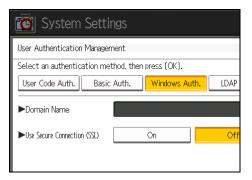
This can be specified by the machine administrator.

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

- 1. Press the [User Tools] key.
- 2. Press [System Settings].
- 3. Press [Administrator Tools].
- Press [User Authentication Management].
 If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.
- Select [Windows Auth.].If you do not want to use user authentication management, select [Off].
- Press [Change] for "Domain Name", enter the name of the domain controller to be authenticated, and then press [OK].



7. Press [On] for "Use Secure Connection (SSL)".



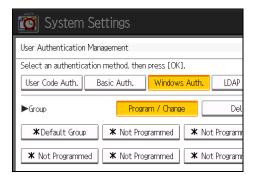
If you are not using secure sockets layer (SSL) for authentication, press [Off].

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

You need to create global groups in the Windows server in advance and register in each group the users to be authenticated. You also need to register in the machine the functions available to the global group members. Create global groups in the machine by entering the names of the global groups registered in the Windows Server. (Keep in mind that group names are case sensitive.) Then specify the machine functions available to each group.

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

8. Under "Group", press [Program / Change], and then press [* Not Programmed].

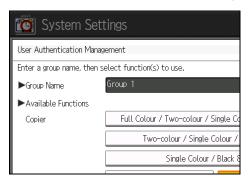


If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

9. Under "Group Name", press [Change], and then enter the group name.



- 10. Press [OK].
- 11. Select which of the machine's functions you want to permit.



If the setting to be specified does not appear, press [Next] to scroll down to other settings.

Windows Authentication will be applied to the selected functions.

Users can use the selected functions only.

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

For details about printer job authentication, see "User Code Authentication".

- 12. Press [OK] twice.
- 13. Press the [User Tools] key.

A confirmation message appears.

If you press [Yes], you will be automatically logged out.

Reference

- p.36 "Logging in Using Administrator Authentication"
- p.37 "Logging out Using Administrator Authentication"
- p.40 "User Code Authentication"
- p.112 "Limiting Available Functions"

Installing Internet Information Services (IIS) and Certificate services

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

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

Install the components, and then create the server certificate.

If they are not installed, install them as follows:

The following describes the procedure using Windows 2000 Server as an example.

- 1. Select [Add/Remove Programs] on the Control Panel.
- 2. Select [Add/Remove Windows Components].
- 3. Select the "Internet Information Services (IIS)" check box.
- 4. Select the "Certificate Services" check box, and then click [Next].
- 5. Installation of the selected Windows components starts, and a warning message appears.
- 6. Click [Yes].
- 7. Click [Next].
- 8. Select the "Certificate Authority", and then click [Next].

On the displayed screen, "Enterprise root CA" is selected.

- 9. Enter the Certificate Authority name (optional) in "CA Identifying Information", and then click [Next].
- 10. Leave "Data Storage Location" at its default, and then click [Next].

Internet Information Services and Certificate services are installed.

Creating the Server Certificate

After installing Internet Information Services (IIS) and Certificate services Windows components, create the Server Certificate as follows:

The following describes the procedure using Windows 2000 Server as an example.

- 1. Start Internet Services Manager.
- 2. Right-click [Default Web Site], and then click [Properties].
- On the "Directory Security" tab, click [Server Certificate].

Web Server Certificate Wizard starts.

- 4. Click [Next].
- 5. Select [Create a new certificate], and then click [Next].

- 6. Select [Prepare the request now, but send it later], and then click [Next].
- Enter the required information according to the instructions given by Web Server Certificate Wizard.
- Check the specified data, which appears as "Request File Summary", and then click [Next].
 The server certificate is created.

Installing the Device Certificate (Certificate Issued by a Certificate Authority)

Install the device certificate using Web Image Monitor.

This section describes 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 in.

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.

In the "Certificate Request" box, enter the contents of the device certificate received from the certificate authority.

8. Click [OK].

The setting is changed.

9. Click [OK].

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

10. Click [Logout].



- If a certificate authority issues a certificate that must be authenticated by an intermediate certificate authority, and the certificate is installed on this machine, an intermediate certificate must be installed on the client computer. If it is not, validation by the certificate authority will not be performed correctly, and a warning message might appear when the destination user receives an e-mail with an S/MIME signature. A warning message might also appear if you attempt to access this machine through Web Image Monitor with SSL enabled. To enable authentication from the client computer, install the intermediate certificate on the client computer, and then reestablish connection.
- Intermediate certificates cannot be installed on this machine.

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.

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
 - Use Secure Connection (SSL)
 - Authentication

Select either "High Security", or "On".

• 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".

Mportant (

- During LDAP authentication, the data registered in the LDAP server such as the user's e-mail address, is automatically registered in the machine. If user information on the server is changed, information registered in the machine may be overwritten when authentication is performed.
- Under LDAP authentication, you cannot specify access limits for groups registered in the LDAP server.

• Enter the user's login user name using up to 128 characters and login password using up to 128 characters. Make sure the first 32 characters of the login user name are unique.



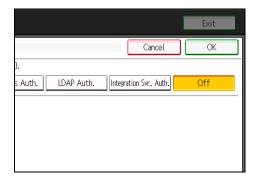
- Under LDAP Authentication, if "Anonymous Authentication" in the LDAP server's settings is not set to Prohibit, users who do not have an LDAP server account might still be able to gain access.
- If the LDAP server is configured using Windows Active Directory, "Anonymous Authentication" might be available. 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.

Specifying LDAP Authentication

This can be specified by the machine administrator.

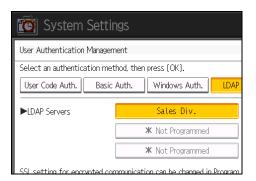
For details about logging in and logging out with administrator authentication, see "Logging in Using Administrator Authentication" and "Logging out Using Administrator Authentication".

- 1. Press the [User Tools] key.
- 2. Press [System Settings].
- 3. Press [Administrator Tools].
- Press [User Authentication Management].
 If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.
- 5. Select [LDAP Auth.].

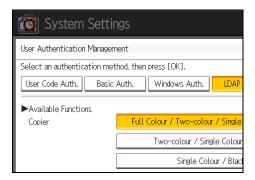


If you do not want to use user authentication management, select [Off].

6. Select the LDAP server to be used for LDAP authentication.



7. Select which of the machine's functions you want to permit.



If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

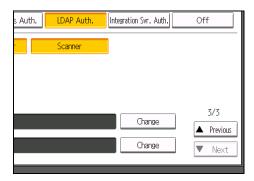
LDAP Authentication will be applied to the selected functions.

Users can use the selected functions only.

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

For details about printer job authentication, see "User Code Authentication".

8. Press [Change] for "Login Name Attribute".



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

Use the Login Name Attribute as a search criterion to obtain information about an authenticated user. You can create a search filter based on the Login Name Attribute, select a user, and then retrieve the user information from the LDAP server so it is transferred to the machine's address book.

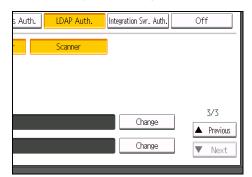
To specify multiple login attributes, place a comma (,) between them. The search will return hits for either or both attributes.

Also, if you place an equals sign (=) between two login attributes (for example: cn=abcde, uid=xyz), the search will return only hits that match the attributes. This search function can also be applied when Cleartext authentication is specified.

When authenticating using the DN format, login attributes do not need to be registered.

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

10. Press [Change] for "Unique Attribute".



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

Specify Unique Attribute on the machine to match the user information in the LDAP server with that in the machine. By doing this, if the Unique Attribute of a user registered in the LDAP server matches that of a user registered in the machine, the two instances are treated as referring to the same user. You can enter an attribute such as "serialNumber" or "uid". Additionally, you can enter "cn" or "employeeNumber", provided it is unique. If you do not specify the Unique Attribute, an account with the same user information but with a different login user name will be created in the machine.

12. Press [OK].

13. Press the [User Tools] key.

A confirmation message appears.

If you press [Yes], you will be automatically logged out.

Reference

- p.36 "Logging in Using Administrator Authentication"
- p.37 "Logging out Using Administrator Authentication"
- p.40 "User Code Authentication"

72

• p.112 "Limiting Available Functions"

Integration Server Authentication

To use Integration Server authentication with this machine, you need a server on which Authentication Manager or another application 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 Professional.

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.



- During Integration Server Authentication, the data registered in the server such as the user's e-mail address, is automatically registered in the machine.
- If user information on the server is changed, information registered in the machine may be overwritten when authentication is performed.

Specifying Integration Server Authentication

This can be specified by the machine administrator.

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

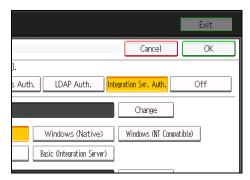
- 1. Press the [User Tools] key.
- 2. Press [System Settings].
- 3. Press [Administrator Tools].
- 4. Press [User Authentication Management].

If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

5. Select [Integration Svr. Auth.].

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

6. Press [Change] for "Server Name".



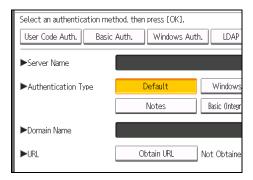
Specify the name of the server for external authentication.

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

Enter the IPv4 address or host name.

8. In "Authentication Type", select the authentication system for external authentication.

Select an available authentication system. For general usage, select [Default].



- 9. Press [Change] for "Domain Name".
- 10. Enter the domain name, and then press [OK].

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

11. Press [Obtain URL].

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

If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

If "Server Name" or the setting for enabling SSL is changed after obtaining the URL, the URL is "Not Obtained".

12. Press [Exit].

In the "Authentication Type", if you have not registered a group, proceed to step 17.

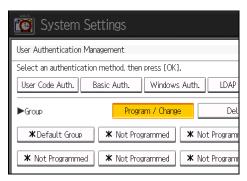
If you have registered a group, proceed to step 13.

2

If you set "Authentication Type" to [Windows (Native)] or [Windows (NT Compatible)], you can use the global group.

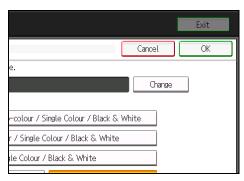
If you set "Authentication Type" to [Notes], you can use the Notes group. If you set "Authentication Type" to [Basic (Integration Server)], you can use the groups created using the Authentication Manager.

13. Under "Group", press [Program / Change], and then press [* Not Programmed].

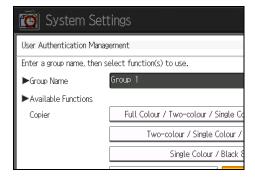


If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

14. Under "Group Name", press [Change], and then enter the group name.



- 15. Press [OK].
- 16. Select which of the machine's functions you want to permit.



If the setting to be specified does not appear, press [*Next] to scroll down to other settings.

Authentication will be applied to the selected functions.

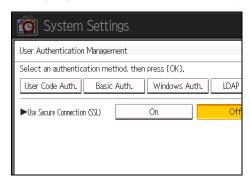
Users can use the selected functions only.

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

For details about printer job authentication, see "User Code Authentication".

17. Press [OK].

18. Press [On] for "Use Secure Connection (SSL)", and then press [OK].



If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

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

19. Press the [User Tools] key.

A confirmation message appears.

If you press [Yes], you will be automatically logged out.

Reference

- p.36 "Logging in Using Administrator Authentication"
- p.37 "Logging out Using Administrator Authentication"
- p.40 "User Code Authentication"
- p.112 "Limiting Available 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. To use the machine's security functions, each user must enter a valid user name and password. Log in to operate the machine, and log out when you are finished operations. Be sure to log out to prevent unauthorized users from using the machine. When auto logout timer is specified, the machine automatically logs you out 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, contact your service representative.



- Consult the User Administrator about your login user name, password, and user code.
- For user code authentication, enter a number registered in the Address Book as "User Code".
- The Auto Logout Timer can only be used under Basic Authentication, Windows Authentication, LDAP Authentication, or Integration Server Authentication.

Reference

p.66 "Auto Logout"

If User Code Authentication is Specified

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



Enter your user code.

Logging in Using the Control Panel

Use the following procedure to log in when User Code Authentication is enabled.

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

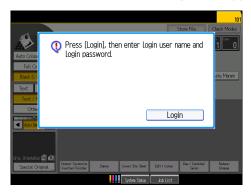
When the authentication is successful, a screen showing the corresponding function is displayed.



- To log out, do one of the following:
 - Press the operation switch.
 - Press the [Energy Saver] key after jobs are completed.
 - Press the [Clear] key and the [Clear Modes] key at the same time.

If Basic, Windows, LDAP or Integration Server Authentication is Specified

When Basic Authentication, Windows Authentication, LDAP Authentication or Integration Server Authentication is set, the following screen appears.



Enter your login user name and password.

Logging in 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. Press [Login].
- 2. Enter the login user name, and then press [OK].
- 3. Enter the login password, and then press [OK].

The message, "Authenticating... Please wait." appears.

When the authentication is successful, a screen showing the corresponding function is displayed.

Logging out Using the Control Panel

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

- 1. Press the [Login/Logout] key.
- 2. Press [Yes].

The message, "Logging out... Please wait." appears.



- You can log out using the following procedures also.
 - Press the operation switch.
 - Press the [Energy Saver] key.

Logging in Using Web Image Monitor

Use the following procedure to log in via Web Image Monitor.

- 1. Click [Login] on the top page of Web Image Monitor.
- 2. Enter a login user name and password, and then click [Login].



- For user code authentication, enter a user code in "Login User Name", and then click [Login].
- The Web browser might be configured to auto complete login dialog boxes by retaining user names and passwords. This function reduces security. To prevent the browser retaining user names and passwords, disable the browser's auto complete function.

Logging out Using Web Image Monitor

Use the following procedure to log out via Web Image Monitor.

1. Click [Logout] to log out.



• Delete the cache memory in Web Image Monitor after logging out.

Auto Logout

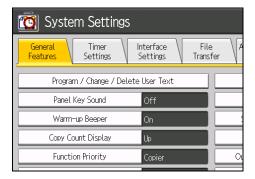
This can be specified by the machine administrator.

When using Basic Authentication, Windows Authentication, LDAP Authentication or Integration Server Authentication, the machine automatically logs you out if you do not use the control panel within a given

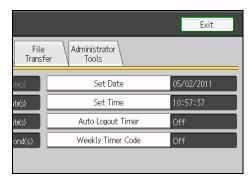
time. This feature is called "Auto Logout". Specify how long the machine is to wait before performing Auto Logout.

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

- 1. Press the [User Tools] key.
- 2. Press [System Settings].
- 3. Press [Timer Settings].

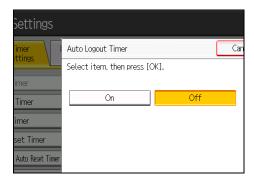


4. Press [Auto Logout Timer].



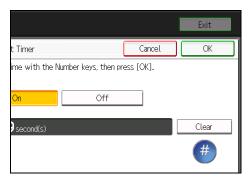
If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

5. Select [On].



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

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



7. Press the [User Tools] key.

A confirmation message appears.

If you press [Yes], you will be automatically logged out.



• If the paper jams or the toner runs out, the machine might be unable to perform the Auto Logout function.

■ Reference

- p.36 "Logging in Using Administrator Authentication"
- p.37 "Logging out Using Administrator Authentication"

7

Authentication Using an External Device

To authenticate using an external device, see the device manual.

For details, contact your sales representative.

3. Ensuring Information Security

This chapter describes how to protect data that is stored on the machine and transmitted information from unauthorized viewing and modification.

Specifying Access Permission for Stored Files

This section describes Specifying Access Permission for Stored Files.

You can specify who is allowed to access stored scan files and files stored in the Document Server.

This can prevent activities such as printing or sending of stored files by unauthorized users.

You can also specify which users can change or delete stored files.

Access Permission

To limit the use of stored files, you can specify four types of access permissions.

Read-only	In addition to checking the content of and information about stored files, you can also print and send the files.
Edit	You can change the print settings for stored files. This includes permission to view files.
Edit / Delete	You can delete stored files. This includes permission to view and edit files.
Full Control	You can specify the user and access permission. This includes permission to view, edit, and edit / delete files.

Password for Stored Files

- Passwords for stored files can be specified by the file creator (owner) or file administrator.
- You can obtain greater protection against the unauthorized use of files.
- Even if User Authentication is not set, passwords for stored files can be set.



- The file administrator can also delete stored files. For details, see "Deleting a Stored Document",
 Copy/Document Server Reference.
- Files can be stored by any user who is allowed to use the Document Server, copy function, or scanner function.
- Using Web Image Monitor, you can check the content of stored files. For details, see Web Image Monitor Help.

• The default access permission for the file creator (owner) is "Read-only". You can also specify the access permission.

Assigning Users and Access Permission for Stored Files

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

Specify the users and their access permissions for each stored file.

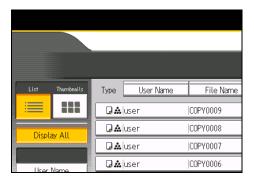
By making this setting, only users granted access permission can access stored files.

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

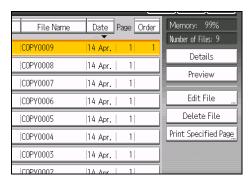
For details about logging in and logging out with administrator authentication, see "Logging in Using Administrator Authentication" and "Logging out Using Administrator Authentication".



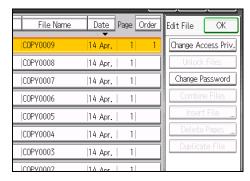
- If files become inaccessible, reset their access permission as the file creator (owner). This can also be done by the file administrator. If you want to access a file but do not have access permission, ask the file creator (owner).
- The file administrator can change the owner of a document using the document's [Change Access Priv.] setting. This setting also allows the file administrator to change the access privileges of the owner and other users.
- To change the access privileges of a document's owner or another user with Full Control privileges
 for a document, use the [Change Access Priv.] setting of the document.
- 1. Press the [Document Server] key.
- 2. Select the file.



3. Press [Edit File].



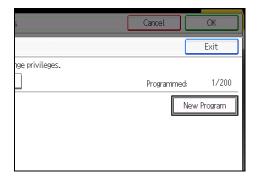
4. Press [Change Access Priv.].



5. Press [Program/Change/Delete].



6. Press [New Program].

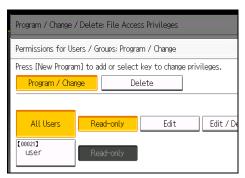


7. Select the users or groups you want to assign permission to.

You can select more than one user.

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

- 8. Press [Exit].
- 9. Select the user who you want to assign access permission to, and then select the permission.



Select the access permission from [Read-only], [Edit], [Edit / Delete], or [Full Control].

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



- p.36 "Logging in Using Administrator Authentication"
- p.37 "Logging out Using Administrator Authentication"

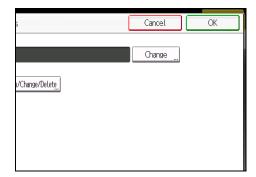
Changing the Owner of a Document

This section describes how to change the owner of a document.

This can be specified by the file administrator.

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

- 1. Press the [Document Server] key.
- 2. Select the file.
- 3. Press [Edit File].
- 4. Press [Change Access Priv.].
- 5. Under "Owner", press [Change].



- 6. Select the user you want to register.
- 7. Press [Exit].
- 8. Press [OK] twice.

Reference

- p.36 "Logging in Using Administrator Authentication"
- p.37 "Logging out Using Administrator Authentication"

Specifying Access Privileges for Files Stored using the Scanner Function

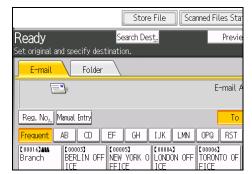
If user authentication is set for the scanner function, you can specify access privileges for stored files when storing them in the machine. You can also change the access privileges for the file.

Specifying Access Privileges When Storing Files

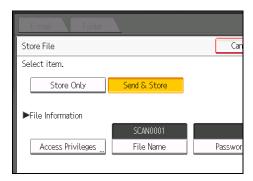
This section describes how to specify the access privileges and then store a file in the machine under the scanner.

1. Press the [Scanner] key.

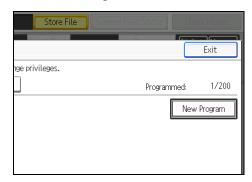
2. Press [Store File].



3. Press [Access Privileges].



4. Press [New Program].



5. Select the users or groups you want to assign permission to.

You can select more than one user.

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

- 6. Press [Exit].
- 7. Select the user who you want to assign access permission to, and then select the permission.

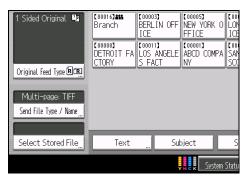
 Select the access permission from [Read-only], [Edit], [Edit / Delete], or [Full Control].
- 8. Press [Exit].
- 9. Press [OK].

10. Store files in the machine.

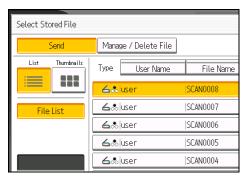
Changing Access Privileges for Previously Stored Files

This section describes how to change access privileges for a file stored in the machine under the scanner.

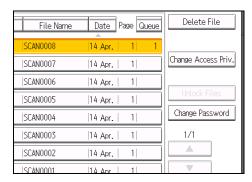
- 1. Press the [Scanner] key.
- 2. Press [Select Stored File].



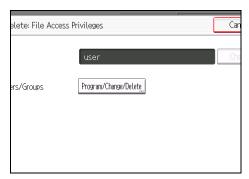
- 3. Select the file.
- 4. Press [Manage / Delete File].



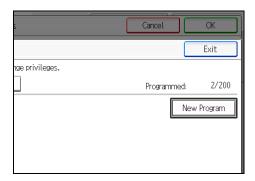
5. Press [Change Access Priv.].



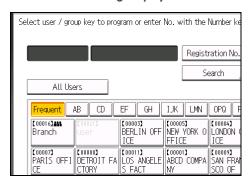
6. Press [Program/Change/Delete].



7. Press [New Program].



8. Select the users or groups you want to assign permission to.



You can select more than one user.

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

- 9. Press [Exit].
- 10. Select the user who you want to assign access permission to, and then select the permission.
 Select the access permission from [Read-only], [Edit], [Edit / Delete], or [Full Control].
- 11. Press [Exit].
- 12. Press [OK].

13. Press [Exit].

Assigning the User and the Access Permission for the User's Stored Files

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

Specify the users and their access permission to files stored by a particular user.

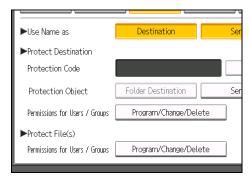
Only those users granted access permission can access stored files.

This makes managing access permission easier than specifying and managing access permissions for each stored file.

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

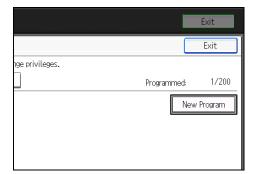
☆ Important

- If files become inaccessible, be sure to enable the user administrator, so that the user administrator can reset the access permission for the files in question.
- 1. Press the [User Tools] key.
- 2. Press [System Settings].
- 3. Press [Administrator Tools].
- 4. Press [Address Book Management].
- 5. Select the user.
- 6. Press [Protection].
- Under "Protect File(s)", press [Program/Change/Delete] for "Permissions for Users/ Groups".



If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

8. Press [New Program].



9. Select the users or groups to register.

You can select more than one user.

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

- 10. Press [Exit].
- 11. Select the user who you want to assign access permission to, and then select the permission.

 Select the access permission from [Read-only], [Edit], [Edit / Delete], or [Full Control].
- 12. Press [Exit].
- 13. Press [OK].
- 14. Press [Exit].
- 15. Press the [User Tools] key.

■ Reference

- p.36 "Logging in Using Administrator Authentication"
- p.37 "Logging out Using Administrator Authentication"

Specifying Passwords for Stored Files

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

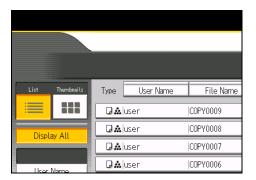
Specify passwords for stored files.

This provides increased protection against unauthorized use of files.

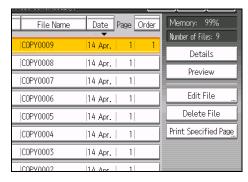
For details about logging in and logging out with administrator authentication, see "Logging in Using Administrator Authentication" and "Logging out Using Administrator Authentication".

1. Press the [Document Server] key.

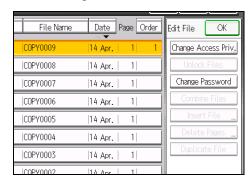
2. Select the file.



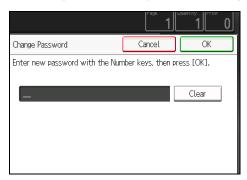
3. Press [Edit File].



4. Press [Change Password].



5. Enter the password using the number keys.



You can use 4 to 8 numbers as the password for the stored file.

- 6. Press [OK].
- 7. Confirm the password by re-entering it using the number keys.
- 8. Press [OK].

The $\frac{1}{2}$ icon appears next to a stored file protected by password.

Reference

- p.36 "Logging in Using Administrator Authentication"
- p.37 "Logging out Using Administrator Authentication"

Unlocking Files

If you specify "Enhance File Protection", the file will be locked and become inaccessible if an invalid password is entered ten times. This section describes how to unlock files.

"Enhance File Protection" is one of the extended security functions. For details about this and other extended security functions, see "Specifying the Extended Security Functions".

Only the file administrator can unlock files.

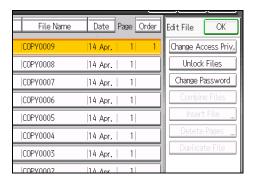
For details about logging in and logging out with administrator authentication, see "Logging in Using Administrator Authentication" and "Logging out Using Administrator Authentication".

- 1. Press the [Document Server] key.
- 2. Select the file.

The 🕙 icon appears next to a file locked by the Enhance File Protection function.

3. Press [Edit File].

4. Press [Unlock Files].



5. Press [Yes].

The 🔕 icon changes to the 🕹 icon.

6. Press [OK].

■ Reference

- p.36 "Logging in Using Administrator Authentication"
- p.37 "Logging out Using Administrator Authentication"
- p.161 "Specifying the Extended Security Functions"

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 in 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 e-mail addresses under the scanner function.

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

If you set "Restrict Use of Destinations" to [On], you can prohibit users from directly entering e-mail addresses, or Folder Path in order to send files. If you set "Restrict Use of Destinations" to [Off], "Restrict Adding of User Destinations" appears. In "Restrict Adding of User Destinations", you can restrict users from registering data in the Address Book.

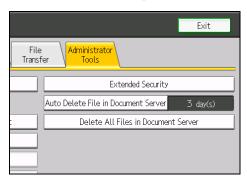
If you set "Restrict Adding of User Destinations" to [Off], users can directly enter e-mail addresses, and Folder Path in "Prg. Dest." on the scanner screens. If you set "Restrict Adding of User Destinations" to [On], users can specify destinations directly, but cannot use "Prg. Dest." to register data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

"Restrictions on Destinations" can also be specified using Web Image Monitor. For details, see Web Image Monitor Help.

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

- 1. Press the [User Tools] key.
- 2. Press [System Settings].
- 3. Press [Administrator Tools].

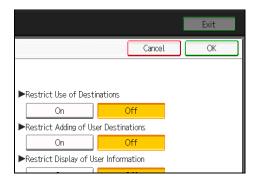
4. Press [Extended Security].



If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

5. Press [On] for "Restrict Use of Destinations".

If "Restrict Use of Destinations" is set to [On], "Restrict Adding of User Destinations" does not appear.



- 6. Press [OK].
- 7. Press the [User Tools] key.
- Reference
 - p.36 "Logging in Using Administrator Authentication"
 - p.37 "Logging out Using Administrator Authentication"
 - p.161 "Specifying the Extended Security Functions"

By registering a user certificate in the Address Book, you can send e-mail that is encrypted with a public key which prevents its content from being altered during transmission. You can also prevent sender impersonation (spoofing) by installing a device certificate on the machine, and attaching an electronic signature created with a private key. You can apply these functions separately or, for stronger security, together.

To send encrypted e-mail, both the sender (this machine) and the receiver must support S/MIME.

Compatible Mailer Applications

The S/MIME function can be used with the following applications:

- Microsoft Outlook 98 and later
- Microsoft Outlook Express 5.5 and later
- Netscape Messenger 7.1 and later
- Lotus Notes R5 and later



• To use S/MIME, you must first specify "Administrator's E-mail Address" in [System Settings].



- If an electronic signature is specified for an e-mail, the administrator's address appears in the "From" field and the address of the user specified as "sender" appears in the "Reply To" field.
- When sending e-mail to users that support S/MIME and users that do not support S/MIME at the same time, the e-mail is separated into encrypted and unencrypted groups and then sent.
- When using S/MIME, the e-mail size is larger than normal.
- For details about using S/MIME with the scanner function, see "Security Settings to E-mails", Scanner Reference.

E-mail Encryption

To send encrypted e-mail using S/MIME, the user certificate must first be prepared using Web Image Monitor and registered in the Address Book by the user administrator. Registering the certificate in the Address Book specifies each user's public key. After installing the certificate, specify the encryption algorithm using Web Image Monitor. The network administrator can specify the algorithm.

E-mail Encryption

- 1. Prepare the user certificate.
- 2. Install the user certificate in the Address Book using Web Image Monitor. (The public key on the certificate is specified in the Address Book.)
- 3. Specify the encryption algorithm using Web Image Monitor.

3

- 4. Using the shared key, encrypt the e-mail message.
- 5. The shared key is encrypted using the user's public key.
- 6. The encrypted e-mail is sent.
- 7. The receiver decrypts the shared key using a secret key that corresponds to the public key.
- 8. The e-mail is decrypted using the shared key.



- There are three types of user certificates that can be installed on this machine, "DER encoded binary X.509", "Base 64 encoded X.509", and "PKCS #7 certificate".
- When installing a user certificate to the Address Book using Web Image Monitor, an error message appears if the certificate file contains more than one certificates. In such cases, install one certificate at a time.

Specifying the User Certificate

This can be specified by the user administrator. Each user certificate must be prepared in advance.

- 1. Open a Web browser.
- 2. Enter "http://(the machine's IP address or host name)/" in the address bar.

When entering an IPv4 address, do not begin segments with zeros. For example: If the address is "192.168.001.010", you must enter it as "192.168.1.10" to connect to the machine.

The top page of Web Image Monitor appears.

3. Click [Login].

The user administrator can log in.

Enter the login user name and login password.

4. Click [Address Book].

The Address Book page appears.

5. Select the user for whom the certificate will be installed, and then click [Change].

The Change User Information screen appears.

- 6. Enter the user address in the "E-mail Address" field under "E-mail".
- 7. Click [Change] in "User Certificate".
- 8. Click [Browse], select the user certificate file, and then click [Open].
- 9. Click [OK].

The user certificate is installed.

- 10. Click [OK].
- 11. Click [Logout].

Specifying the Encryption Algorithm

This can be specified by the network administrator.

- 1. Open a Web browser.
- 2. Enter "http://(the machine's IP address or host name)/" in the address bar.

When entering an IPv4 address, do not begin segments with zeros. For example: If the address is "192.168.001.010", you must enter it as "192.168.1.10" to connect to the machine.

The top page of Web Image Monitor appears.

3. Click [Login].

The network administrator can log in.

Enter the login user name and login password.

4. Click [Configuration], and then click [S/MIME] under "Security".

The S/MIME settings page appears.

- Select the encryption algorithm from the drop down menu next to "Encryption Algorithm" under "Encryption".
- 6. Click [OK].

The algorithm for S/MIME is set.

7. Click [Logout].

Attaching an Electronic Signature

To attach an electronic signature to sent e-mail, a device certificate must be installed in advance.

It is possible to use either a self-signed certificate created by the machine, or a certificate issued by a certificate authority.



 To install an S/MIME device certificate, you must first register "Administrator's E-mail Address" in [System Settings] as the e-mail address for the device certificate. Note that even if you will not be using S/MIME, you must still specify an e-mail address for the S/MIME device certificate.

Electronic Signature

- 1. Install a device certificate on the machine. (The secret key on the certificate is configured on the machine.)
- 2. Attach the electronic signature to an e-mail using the secret key provided by the device certificate.
- 3. Send the e-mail with the electronic signature attached to the user.
- 4. The receiver requests the public key and device certificate from the machine.
- 5. Using the public key, you can determine the authenticity of the attached electronic signature to see if the message has been altered.

Configuration flow (self-signed certificate)

1. Creating and installing the device certificate.

Create and install the device certificate using Web Image Monitor.

2. Make certificate settings.

Make settings for the certificate to be used for S/MIME using Web Image Monitor.

3. Make electronic signature settings.

Make settings for the electronic signature using Web Image Monitor.

Configuration flow (certificate issued by a certificate authority)

1. Create the device certificate.

Create the device certificate using Web Image Monitor.

The application procedure for a created certificate depends on the certificate authority. Follow the procedure specified by the certificate authority.

2. Install the device certificate.

Install the device certificate using Web Image Monitor.

3. Make certificate settings.

Make settings for the certificate to be used for S/MIME using Web Image Monitor.

4. Make electronic signature settings.

Make settings for the electronic signature using Web Image Monitor.

Creating and Installing the Self-Signed Certificate

This can be specified by the network administrator.

Create and install the device certificate using Web Image Monitor.

This section describes 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 in.

Enter the login user name and login password.

4. Click [Configuration], and then click [Device Certificate] under "Security".

The Device Certificate page appears.

- Check the radio button next to the number of the certificate you want to create.
- 6. Click [Create].
- Make the necessary settings.

For details about the displayed items and selectable items, see Web Image Monitor Help.

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].



• Click [Delete] to delete the device certificate from the machine.

Creating the Device Certificate (Certificate Issued by a Certificate Authority)

This can be specified by the network administrator.

Create the device certificate using Web Image Monitor.

Use this procedure to create a device certificate issued by a certificate authority.

- 1. Open a Web browser.
- 2. Enter "http://(the machine's IP address or host name)/" in the address bar.

When entering an IPv4 address, do not begin segments with zeros. For example: If the address is "192.168.001.010", you must enter it as "192.168.1.10" to connect to the machine.

The top page of Web Image Monitor appears.

3. Click [Login].

The network administrator can log in.

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.

For details about the displayed items and selectable items, see Web Image Monitor Help.

8. Click [OK].

The setting is changed.

9. Click [OK].

"Requesting" appears under "Certificate Status".

- 10. Click [Logout].
- 11. Apply to the certificate authority for the device certificate.

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

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



- 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)

This can be specified by the network administrator.

Install the device certificate using Web Image Monitor.

Use this procedure to install a server certificate issued by a certificate authority.

Enter the details of the device certificate issued by the certificate authority.

- 1. Open a Web browser.
- 2. Enter "http://(the machine's IP address or host name)/" in the address bar.

When entering an IPv4 address, do not begin segments with zeros. For example: If the address is "192.168.001.010", you must enter it as "192.168.1.10" to connect to the machine.

The top page of Web Image Monitor appears.

3. Click [Login].

The network administrator can log in.

Enter the login user name and login password.

4. Click [Configuration], and then click [Device Certificate] under "Security".

The Device Certificate page appears.

- 5. Check the radio button next to the number of the certificate you want to install.
- 6. Click [Install].

7. Enter the details of the device certificate.

In the "Certificate Request" box, enter the details of the device certificate received from the certificate authority.

For details about the displayed items and selectable items, see Web Image Monitor Help.

8. Click [OK].

The setting is changed.

9. Click [OK].

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

10. Click [Logout].



- If a certificate authority issues a certificate that must be authenticated by an intermediate certificate authority, and the certificate is installed on this machine, an intermediate certificate must be installed on the client computer. If it is not, validation by the certificate authority will not be performed correctly, and a warning message might appear when the destination user receives an e-mail with an S/MIME signature. A warning message might also appear if you attempt to access this machine through Web Image Monitor with SSL enabled. To enable authentication from the client computer, install the intermediate certificate on the client computer, and then reestablish connection.
- Intermediate certificates cannot be installed on this machine.

Selecting the Device Certificate

This can be specified by the network administrator.

Select the device certificate to be used for S/MIME using Web Image Monitor.

- 1. Open a Web browser.
- 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 in.

Enter the login user name and login password.

4. Click [Configuration], and then click [Device Certificate] under "Security".

The Device Certificate page appears.

Select the certificate to be used for the electronic signature from the drop down box in "S/ MIME" under "Certification". 6. Click [OK].

The certificate to be used for the S/MIME electronic signature is set.

- 7. Click [OK].
- 8. Click [Logout].

Specifying the Electronic Signature

This can be specified by the network administrator.

After installing the device certificate on the machine, configure the electronic signature using Web Image Monitor. The configuration procedure is the same regardless of whether you are using a self-signed certificate or a certificate issued by a certificate authority.

- 1. Open a Web browser.
- 2. Enter "http://(the machine's IP address or host name)/" in the address bar.

When entering an IPv4 address, do not begin segments with zeros. For example: If the address is "192.168.001.010", you must enter it as "192.168.1.10" to connect to the machine.

The top page of Web Image Monitor appears.

3. Click [Login].

The network administrator can log in.

Enter the login user name and login password.

4. Click [Configuration], and then click [S/MIME] under "Security".

The S/MIME settings page appears.

- Select the digest algorithm to be used in the electronic signature next to "Digest Algorithm" under "Signature".
- Select the method for attaching the electronic signature when sending e-mail from the scanner next to "When Sending E-mail by Scanner" under "Signature".
- 7. Select the method for attaching the electronic signature when forwarding stored documents next to "When Transferring Files Stored in Document Server (Utility)" under "Signature".
- 8. Click [OK].

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

9. Click [Logout].



If the machine does not support the scanner, S/MIME will not appear on Web Image Monitor.

Protecting the Address Book

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.

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.

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

- 1. Press the [User Tools] key.
- 2. Press [System Settings].
- 3. Press [Administrator Tools].
- 4. Press [Address Book Management].
- 5. Select the user.
- 6. Press [Protection].
- Press [Program/Change/Delete] for "Permissions for Users/Groups", under "Protect Destination".
- 8. Press [New Program].



9. Select the users or groups to register.

You can select more than one user.

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

- 10. Press [Exit].
- 11. Select the user who you want to assign access permission to, and then select the permission.

 Select the permission, from [Read-only], [Edit], [Edit / Delete], or [Full Control].

3

- 12. Press [Exit].
- 13. Press [OK].
- 14. Press [Exit].
- 15. Press the [User Tools] key.



An authenticated user's access to Address Book information is determined by the access permissions
granted to that user: "Read-only", "Edit", "Edit / Delete", or "Full Control". Note that granting a user
"Edit", "Edit / Delete", or "Full Control" permission allows that user to perform high level operations,
which could result in loss of or changes to sensitive information. For this reason, we recommend you
grant only the "Read-only" access permission to general users.

■ Reference

- p.36 "Logging in Using Administrator Authentication"
- p.37 "Logging out Using Administrator Authentication"

Encrypting Data in the Address Book

This can be specified by the user administrator.

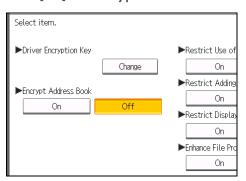
You can encrypt the data in the address book using the extended security function, "Encrypt Address Book".

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

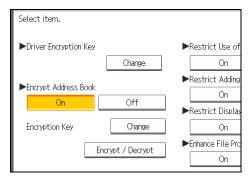
- 1. Press the [User Tools] key.
- 2. Press [System Settings].
- 3. Press [Administrator Tools].
- 4. Press [Extended Security].

If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

5. Press [On] for "Encrypt Address Book".



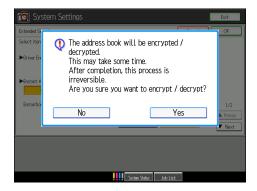
6. Press [Change] for "Encryption Key".



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

Enter the encryption key using up to 32 alphanumeric characters.

- 8. Press [Encrypt / Decrypt].
- 9. Press [Yes].



Do not switch off the machine's main power during encryption or decryption, as doing so risks corrupting the data.

Encrypting the data in the address book may take a long time.

The time it takes to encrypt the data in the address book depends on the number of registered users.

The machine cannot be used during encryption.

Normally, once encryption is complete, "Encryption / Decryption is successfully complete. Press [Exit]." appears.

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

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

- 10. Press [Exit].
- 11. Press [OK].
- 12. Press the [User Tools] key.

U Note

- If you register additional users after encrypting the data in the address book, those users are also encrypted.
- The backup copy of the address book data stored in the SD card is encrypted. For details about backing up and then restoring the address book using an SD card, see "Administrator Tools", General Settings Guide.

■ Reference

- p.36 "Logging in Using Administrator Authentication"
- p.37 "Logging out Using Administrator Authentication"
- p.161 "Specifying the Extended Security Functions"

Deleting Data on the Hard Disk

This can be specified by the machine administrator.

To use this function, the DataOverwriteSecurity unit must be installed.

The machine's hard disk stores all document data from the copier, printer, and scanner functions. It also stores the data of users' Document Server and code counters, and the Address Book.

To prevent data on the hard disk being leaked before disposing of the machine, you can overwrite all data stored on the hard disk. You can also automatically overwrite temporarily-stored data.

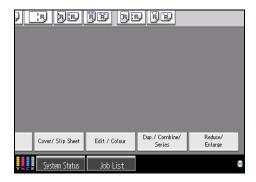
Auto Erase Memory

A document scanned in copier or scanner mode, or print data sent from a printer driver is temporarily stored on the machine's hard disk. Even after the job is completed, it remains in the hard disk as temporary data. Auto Erase Memory erases the temporary data on the hard disk by writing over it.

Overwriting starts automatically once the job is completed. The Copier and Printer functions take priority over the Auto Erase Memory function. If a copy or print job is in progress, overwriting will only be done after the job is completed.

Overwrite Icon

If the DataOverwriteSecurity unit has been correctly installed and is functioning properly, the Data Overwrite icon will be indicated in the bottom right hand corner of the panel display of your machine when "Auto Erase Memory Setting" is set to [On].



8	Dirty	This icon is lit when there is temporary data to be overwritten, and blinks during overwriting.
8	Clear	This icon is lit when there is no temporary data to be overwritten.





If the Data Overwrite icon is not displayed, first check if "Auto Erase Memory Setting" has been set
to [Off]. If the icon is not displayed even though "Auto Erase Memory Setting" is [On], contact your
service representative.

Methods of Overwriting

You can select a method of overwriting from the following:

[NSA] *1

Temporary data is overwritten twice with random numbers and once with zeros.

[DoD] *2

Temporary data is overwritten with a fixed value, the fixed value's complement, and random numbers. It is then verified.

[Random Numbers]

Temporary data is overwritten multiple times with random numbers. The number of overwrites can be selected from 1 to 9.

- * 1 National Security Agency, U.S.A.
- *2 Department of Defense, U.S.A.



Default: [Random Numbers], [3 time(s)]

Using Auto Erase Memory

This can be specified by the machine administrator.

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

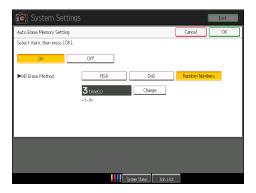


- When "Auto Erase Memory Setting" is set to [On], temporary data that remained on the hard disk when "Auto Erase Memory Setting" was [Off] might not be overwritten.
- 1. Press the [User Tools] key.
- 2. Press [System Settings].
- 3. Press [Administrator Tools].



If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

- 5. Press [On].
- 6. Select the method of overwriting.

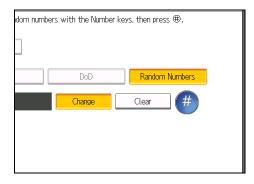


If you select [NSA] or [DoD], proceed to step 9.

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

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

- 7. Press [Change].
- 8. Enter the number of times that you want to overwrite using the number keys, and then press [#].



3

9. Press [OK].

Auto Erase Memory is set.

10. Press the [User Tools] key.



- If the main power switch is turned off before Auto Erase Memory is completed, overwriting will stop
 and data will be left on the hard disk. Do not stop the overwrite mid-process. Doing so will damage
 the hard disk.
- Should the main power switch be turned off before Auto Erase Memory is completed, overwriting will
 continue once the main power switch is turned back on.
- If an error occurs before overwriting is completed, turn off the main power, turn it back on, and then repeat the procedure from step 1.

Reference

- p.36 "Logging in Using Administrator Authentication"
- p.37 "Logging out Using Administrator Authentication"
- p.99 "Methods of Overwriting"

Canceling Auto Erase Memory

This can be specified by the machine administrator.

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

- 1. Follow steps 1 to 4 in "Using Auto Erase Memory".
- 2. Press [Off].
- 3. Press [OK].

Auto Erase Memory is disabled.

4. Press the [User Tools] key.



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

Reference

- p.36 "Logging in Using Administrator Authentication"
- p.37 "Logging out Using Administrator Authentication"

Types of Data that Can or Cannot Be Overwritten

The following table shows the types of data that can or cannot be overwritten by "Auto Erase Memory".

Data Overwritten by Auto Erase Memory

Copier

Copy jobs

Printer

Print jobs

Scanner*1

- Scanned files sent by e-mail
- Files sent by Scan to Folder
- Documents sent using DeskTopBinder Professional, the ScanRouter delivery software or Web Image Monitor

Data Not Overwritten by Auto Erase Memory

- Documents stored by the user in the Document Server using the Copier, Printer or Scanner function*2
- Information registered in the Address Book*3
- · Counters stored under each user code
- * 1 Data scanned with network TWAIN scanner will not be overwritten by Auto Erase Memory.
- *2 A stored document can only be overwritten after it has been printed or deleted from the Document Server.
- *3 Data stored in the Address Book can be encrypted for security. For details, see "Protecting the Address Book".

Reference

• p.94 "Protecting the Address Book"

Erase All Memory

You can erase all the data on the hard disk by writing over it. This is useful if you relocate or dispose of your machine.

- If you select "Erase All Memory", the following are also deleted: user codes, counters under each
 user code, user stamps, data stored in the Address Book, printer fonts downloaded by users,
 applications using Embedded Software Architecture, SSL server certificates, and the machine's
 network settings.
- If the main power switch is turned off before Erase All Memory is completed, overwriting will be stopped and data will be left on the hard disk. Do not stop the overwrite mid-process. Doing so will damage the hard disk.

3

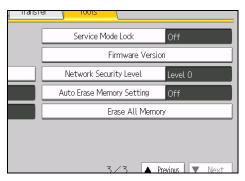
- Other than pausing, no operations are possible during the "Erase All Memory" process. If [Random Numbers] is specified and the number of overwrites set to "3", the erase process will take about four hours.
- The "Erase All Memory" function also clears the machine's security settings, with the result that
 afterward, neither machine nor user administration will be effective. Ensure that users do not save any
 data on the machine after "Erase All Memory" has completed.

Using Erase All Memory

This can be specified by the machine administrator.

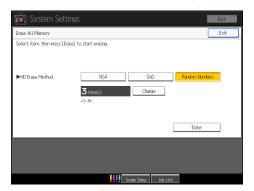
For details about logging in and logging out with administrator authentication, see "Logging in Using Administrator Authentication" and "Logging out Using Administrator Authentication".

- 1. Disconnect communication cables connected to the machine.
- 2. Press the [User Tools] key.
- 3. Press [System Settings].
- 4. Press [Administrator Tools].
- 5. Press [Erase All Memory].



If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

6. Select the method of overwriting.

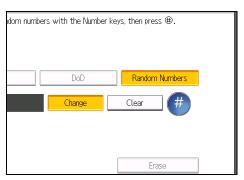


If you select [NSA] or [DoD], proceed to step 9.

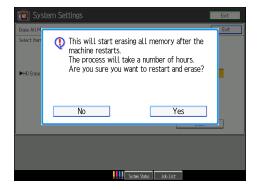
If you select [Random Numbers], proceed to step 7.

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

- 7. Press [Change].
- 8. Enter the number of times that you want to overwrite using the number keys, and then press [#].



- 9. Press [Erase].
- 10. Press [Yes].



The machine restarts automatically, and overwriting begins.

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

Before turning the power off, see "Turning On/Off the Power", About This Machine.



- Should the main power switch be turned off before Erase All Memory is completed, overwriting will
 continue once the main power switch is turned back on.
- If an error occurs before overwriting is completed, turn off the main power, turn it back on, and then repeat the procedure from step 2.

Reference

• p.36 "Logging in Using Administrator Authentication"

- p.37 "Logging out Using Administrator Authentication"
- p.99 "Methods of Overwriting"

Suspending Erase All Memory

The overwriting process can be suspended temporarily.



- Erase All Memory cannot be canceled.
- 1. Press [Suspend] while Erase All Memory is in progress.
- 2. Press [Yes].

Overwriting is suspended.

3. Turn off the main power.

Before turning the power off, see "Turning On/Off the Power", About This Machine.



• To resume overwriting, turn on the main power.

4. 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. Authentication", [Available Settings], the administrator can select which settings users cannot specify. For details about the administrator roles, see "Administrators and Users".

Register the administrators before using the machine. For instructions on registering the administrator, see "Administrator Authentication".

Type of Administrator

Register the administrator on the machine, and then authenticate the administrator using the administrator's login user name and password. The administrator can also specify [Available Settings] in "Admin. Authentication" to prevent users from specifying certain settings. Administrator type determines which machine settings can be modified. The following administrator types are possible:

- User Administrator
- Machine Administrator
- Network Administrator
- File Administrator

For details about which settings are available to which type of administrator, see the sections listing the settings available to each type of administrator.

Menu Protect

Use this function to specify the permission level for users to change those settings accessible by non administrators

You can specify Menu Protect for the following settings:

- Copier / Document Server Features
- Scanner Features

For a list of settings that users can specify according to the Menu Protect level, see "User Settings - Control Panel Settings" and "User Settings - Web Image Monitor Settings".

■ Reference

- p.23 "Administrators and Users"
- p.31 "Administrator Authentication"
- p.197 "Machine Administrator Settings"
- p.204 "Network Administrator Settings"

- p.208 "File Administrator Settings"
- p.210 "User Administrator Settings"
- p.216 "User Settings Control Panel Settings"
- p.234 "User Settings Web Image Monitor Settings"

Menu Protect

The administrator can also limit users' access permission to the machine's settings. This is done by locking the machine's system settings menu. 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.216 "User Settings Control Panel Settings"
- p.234 "User Settings Web Image Monitor Settings"

Enabling Menu Protect

If you want to enable Menu Protect, specify it to [Level 1] or [Level 2]. Select [Level 2] to impose stricter restrictions on users' access permission to the machine settings.

Disabling Menu Protect

If you want to disable Menu Protect, specify it to [Off]. If you select [Off], there are no restrictions of Menu Protect on users' access permission to the machine settings.

Specifying Menu Protect

This can be specified by the machine administrator.

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

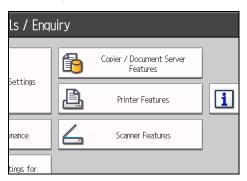
■ Reference

- p.36 "Logging in Using Administrator Authentication"
- p.37 "Logging out Using Administrator Authentication"

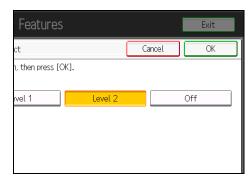
Copy Function

To specify [Menu Protect] in [Copier / Document Server Features], set [Machine Management] to [On] in [Administrator Authentication Management] in [Administrator Tools] in [System Settings].

1. Press the [User Tools] key.



- 3. Press [Administrator Tools].
- 4. Press [Menu Protect].
- 5. Select the menu protect level, and then press [OK].



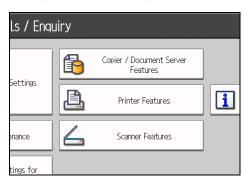
6. Press the [User Tools] key.

Scanner Function

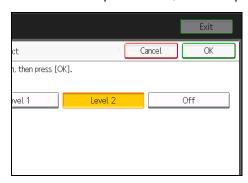
To specify [Menu Protect] in [Scanner Features], set [Machine Management] to [On] in [Administrator Authentication Management] in [Administrator Tools] in [System Settings].

1. Press the [User Tools] key.

2. Press [Scanner Features].



- 3. Press [Initial Settings].
- 4. Press [Menu Protect].
- 5. Select the menu protect level, and then press [OK].



6. Press the [User Tools] key.

Limiting Available Functions

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

Specify the available functions from the Copier, Printer, Document Server, and Scanner functions.

Available Functions

Copier

- [Full Colour / Two-colour / Single Colour / Black & White]
- [Two-colour / Single Colour / Black & White]
- [Single Colour / Black & White]
- [Black & White Only]

Printer

- [Colour / Black & White]
- [Black & White]
- [None]

Other Functions

- [Document Server]
- [Scanner]



- For details about the color mode, see "Selecting a Color Mode", Copy/Document Server Reference.
- Printer job authentication is possible only if user code authentication is enabled. For details, see "User Code Authentication".

Reference

• p.40 "User Code Authentication"

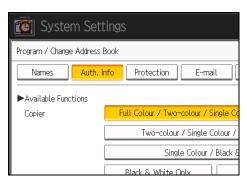
Specifying Which Functions are Available

This can be specified by the user administrator. Specify which functions will be available to users registered in the address book when they log in to the machine.

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

- 1. Press the [User Tools] key.
- 2. Press [System Settings].
- 3. Press [Administrator Tools].

- 4. Press [Address Book Management].
- 5. Select the user.
- 6. Press [Auth. Info].
- 7. In "Available Functions", select the functions you want to specify.



If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

- 8. Press [OK].
- 9. Press [Exit].
- 10. Press the [User Tools] key.

Reference

- p.36 "Logging in Using Administrator Authentication"
- p.37 "Logging out Using Administrator Authentication"

5. 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.

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].

- Using access control, you can limit access involving RCP/RSH, FTP, Web Image Monitor or DeskTopBinder Professional. You cannot limit access involving telnet.
- 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 in.

Enter the login user name and login password.

4. Click [Configuration], and then click [Access Control] under "Security".

The Access Control page appears.

To specify the IPv4 Address, enter an IP address that has access to the machine in "Access Control Range".

To specify the IPv6 Address, enter an IP address that has access to the machine in "Range" under "Access Control Range", or enter an IP address in "Mask" and specify the "Mask Length".

6. Click [OK].

Access control is set.

- 7. Click [OK].
- 8. Click [Logout].

Enabling/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 or telnet. For details about making settings using telnet, see "Remote Maintenance by telnet", Network Guide. To disable SMTP on Web Image Monitor, in E-mail settings, set the protocol to anything other than SMTP. For details, see Web Image Monitor Help.

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

Protocol	Port	Setting Method	Disabled Condition
IPv4	-	Control PanelWeb Image Monitortelnet	All applications that operate over IPv4 cannot be used. IPv4 cannot be disabled from Web Image Monitor when using IPv4 transmission.
IPv6	-	Control PanelWeb Image Monitortelnet	All applications that operate over IPv6 cannot be used.
IPsec	-	Control PanelWeb Image Monitortelnet	Encrypted transmission using IPsec is disabled.

Protocol	Port	Setting Method	Disabled Condition
FTP	TCP:21	Web Image Monitortelnet	Functions that require FTP cannot be used. You can restrict personal information from being displayed by making settings on the control panel using "Restrict Display of User Information".* 1
ssh/sftp	TCP:22	Web Image Monitortelnet	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.
SMTP	TCP:25 (variable)	Control Panel Web Image Monitor	E-mail notification that requires SMTP reception cannot be used.
НТТР	TCP:80	Web Image Monitor telnet	Functions that require HTTP cannot be used.

Protocol	Port	Setting Method	Disabled Condition
			Functions that require HTTPS cannot be used. @Remote functions are unavailable.
HTTPS	TCP:443	Web Image Monitor telnet	You can also make settings to require SSL transmission and restrict the use of other transmission methods using the control panel or Web Image Monitor.
SMB	TCP:139	Control PanelWeb Image Monitortelnet	SMB printing functions cannot be used.
NBT	UDP:137 UDP:138	• telnet	SMB printing functions via TCP/IP, as well as NetBIOS designated functions on the WINS server cannot be used.
			Functions that require SNMPv1, v2 cannot be used.
SNMPv1,v2	UDP:161	Web Image Monitor telnet	Using the control panel, Web Image Monitor or telnet, you can specify that SNMPv1, v2 settings are read-only, and cannot be edited.

Protocol	Port	Setting Method	Disabled Condition
SNMPv3	UDP:161	Web Image Monitortelnet	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 Monitortelnet	Functions that require remote shell (RSH) 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
SSDP	UDP:1900	Web Image Monitor telnet	Device discovery using UPnP from Windows cannot be used.
@Remote	TCP:7443 TCP:7444	• telnet	@Remote cannot be used.
RFU	TCP:10021	• telnet	You can attempt to update firmware via FTP.
NetWare	(IPX/SPX)	Control PanelWeb Image Monitortelnet	SNMP over IPX cannot be used.

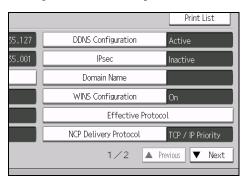
^{*1 &}quot;Restrict Display of User Information" is one of the Extended Security features. For details about making this setting, see "Specifying the Extended Security Functions".

■ Reference

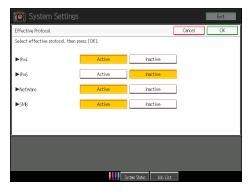
- p.36 "Logging in Using Administrator Authentication"
- p.37 "Logging out Using Administrator Authentication"
- p.161 "Specifying the Extended Security Functions"

Making Settings Using the Control Panel

- 1. Press the [User Tools] key.
- 2. Press [System Settings].
- 3. Press [Interface Settings].
- 4. Press [Effective Protocol].



5. Press [Inactive] for the protocol you want to disable.



- 6. Press [OK].
- 7. Press the [User Tools] key.

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 in.

Enter the login user name and login password.

4. Click [Configuration], and then click [Network Security] under "Security".

The Network Security page appears.

- 5. Set the desired protocols to active/inactive (or open/close).
- 6. Click [OK].

The setting is changed.

- 7. Click [OK].
- 8. Click [Logout].

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.

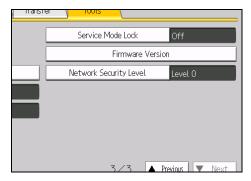
For details about logging in and logging out with administrator authentication, see "Logging in Using Administrator Authentication" and "Logging out Using Administrator Authentication".

Reference

- p.36 "Logging in Using Administrator Authentication"
- p.37 "Logging out Using Administrator Authentication"

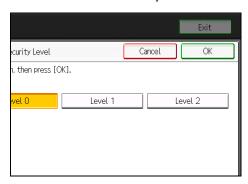
Making Settings Using the Control Panel

- 1. Press the [User Tools] key.
- 2. Press [System Settings].
- 3. Press [Administrator Tools].
- 4. Press [Network Security Level].



If the setting you want to specify does not appear, press [▼Next] to scroll down to other settings.

5. Select the network security level.



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

- 6. Press [OK].
- 7. Press the [User Tools] 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 in.

Enter the login user name and login password.

4. Click [Configuration], and then click [Network Security] under "Security".

The Network Security page appears.

- 5. Select the network security level in "Security Level".
- 6. Click [OK].

The setting is changed.

- 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
SSL/TLS> Port 443	Open	Open	Open
SSL/TLS> Permit SSL/TLS Communication	Ciphertext Priority	Ciphertext Priority	Ciphertext Only
FTP	Active	Active	Active
sftp	Active	Active	Active
ssh	Active	Active	Active
RSH/RCP	Active	Active	Inactive
TELNET	Active	Inactive	Inactive
SSDP	Active	Active	Inactive
SMB	Active	Active	Inactive
NetBIOS over TCP/IPv4	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/ Cleartext	Encryption Only

Encrypting Transmitted Passwords

We recommend you use one or more of the following security protocols: IPsec, SNMPv3, and SSL. Using these protocols can enhance your machine's security to make login and IPP authentication passwords harder to break.

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 TWAIN driver installed in the user's computer.

Driver Encryption Key

This can be specified by the network administrator.

Specify the driver encryption key on the machine.

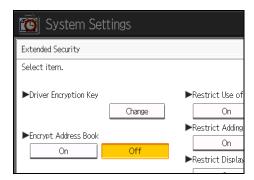
You can enhance security to make login passwords harder to break.

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

- 1. Press the [User Tools] key.
- 2. Press [System Settings].
- 3. Press [Administrator Tools].
- 4. Press [Extended Security].

If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

5. For "Driver Encryption Key", press [Change].



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

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

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

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

- 7. Press [OK].
- 8. Press the [User Tools] key.



• For details about specifying the encryption key on the TWAIN driver, see the TWAIN driver Help.

Reference

- p.36 "Logging in Using Administrator Authentication"
- p.37 "Logging out Using Administrator Authentication"
- p.161 "Specifying the Extended Security Functions"

Protection Using Encryption

This machine uses the SSL, SNMPv3, and IPsec protocols to protect the data that it transmits. These protocols encrypt the data, preventing it from being intercepted, analyzed, or tampered with.

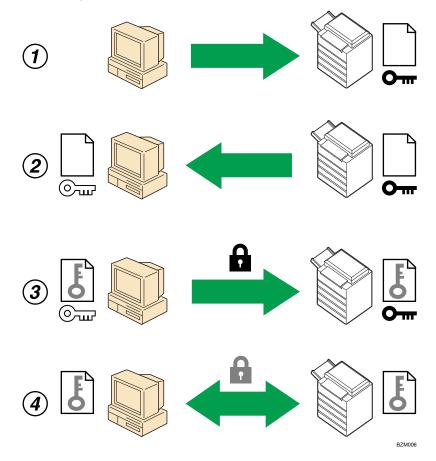
SSL (Secure Sockets Layer) Encryption

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. The shared key created with the computer is encrypted using the public key, sent to the machine, and then decrypted using the private key in the machine.
- 4. The shared key is used for data encryption and decryption, thus achieving secure transmission.

Configuration flow (self-signed certificate)

- 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.

- Installing the device certificate
 Install the device certificate using Web Image Monitor.
- 3. Enabling SSL

Enable the "SSL/TLS" setting using Web Image Monitor.



 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.

Creating and Installing the Self-Signed Certificate

Create and install the device certificate using Web Image Monitor.

This section describes 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 in.

Enter the login user name and login password.

4. Click [Configuration], and then click [Device Certificate] under "Security".

The Device Certificate page appears.

- 5. Click [Certificate1].
- 6. Click [Create].
- 7. Make the necessary settings.

For details about the displayed items and selectable items, see Web Image Monitor Help.

8. Click [OK].

The setting is changed.

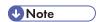
9. Click [OK].

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].



• 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.

This section describes 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 in.

Enter the login user name and login password.

4. Click [Configuration], and then click [Device Certificate] under "Security".

The Device Certificate page appears.

- 5. Click [Certificate1].
- 6. Click [Request].

Make the necessary settings.

For details about the displayed items and selectable items, see Web Image Monitor Help.

8. Click [OK].

The setting is changed.

9. Click [OK].

"Requesting" appears under "Certificate Status".

- 10. Click [Logout].
- 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 the Web Image Monitor Details icon and use the information that appears in "Certificate Details".



- 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.

This section describes 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.
- 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 in.

Enter the login user name and login password.

4. Click [Configuration], and then click [Device Certificate] under "Security".

The Device Certificate page appears.

5. Click [Certificate 1].

- 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.

For details about the displayed items and selectable items, see Web Image Monitor Help.

8. Click [OK].

The setting is changed.

9. Click [OK].

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

10. Click [Logout].



- If a certificate authority issues a certificate that must be authenticated by an intermediate certificate authority, and the certificate is installed on this machine, an intermediate certificate must be installed on the client computer. If it is not, validation by the certificate authority will not be performed correctly, and a warning message might appear when the destination user receives an e-mail with an S/MIME signature. A warning message might also appear if you attempt to access this machine through Web Image Monitor with SSL enabled. To enable authentication from the client computer, install the intermediate certificate on the client computer, and then reestablish connection.
- Intermediate certificates cannot be installed on this machine.

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 in.

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".
- Click [OK].The SSL setting is enabled.
- 8. Click [OK].
- 9. Click [Logout].



If you set "Permit SSL/TLS Communication" to [Ciphertext Only], enter "https://(the machine's IP address or host name)/" to access the machine.

User Settings for SSL (Secure Sockets Layer)

We recommend that after installing the self-signed certificate or device certificate from a private certificate authority on the main unit and enabling SSL (communication encryption), you instruct users to install the certificate on their computers. The network administrator must instruct each user to install the certificate.



- Take the appropriate steps when you receive a user's inquiry concerning problems such as an expired
 certificate.
- For details about how to install the certificate and about where to store the certificate, 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.
----------------------	--

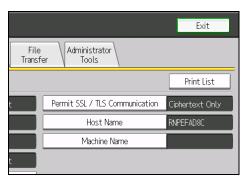
Setting the SSL / TLS Encryption Mode

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.

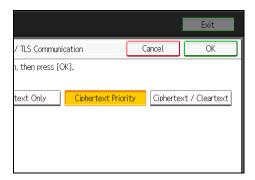
For details about logging in and logging out with administrator authentication, see "Logging in Using Administrator Authentication" and "Logging out Using Administrator Authentication".

- 1. Press the [User Tools] key.
- 2. Press [System Settings].
- 3. Press [Interface Settings].
- 4. Press [Permit SSL / TLS Communication].



If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

5. Select the encrypted communication mode.



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

6. Press [OK].



 The SSL/TLS encrypted communication mode can also be specified using Web Image Monitor. For details, see Web Image Monitor Help.

Reference

- p.36 "Logging in Using Administrator Authentication"
- p.37 "Logging out Using Administrator Authentication"

SNMPv3 Encryption

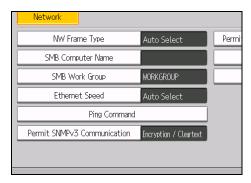
This can be specified by the network administrator.

You can encrypt the data sent for specifying various settings with an application using SNMPv3.

By making this setting, you can protect data from being tampered with.

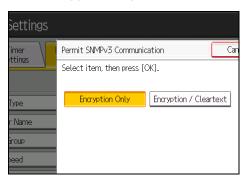
For details about logging in and logging out with administrator authentication, see "Logging in Using Administrator Authentication" and "Logging out Using Administrator Authentication".

- 1. Press the [User Tools] key.
- 2. Press [System Settings].
- 3. Press [Interface Settings].
- 4. Press [Permit SNMPv3 Communication].



If the setting to be specified does not appear, press [*Next] to scroll down to other settings.

5. Press [Encryption Only].



- 6. Press [OK].
- 7. Press the [User Tools] key.



- To encrypt the data transmitted for specifying various settings with an application using SNMPv3, specify [Permit SNMPv3 Communication] on the machine, configure the network administrator's [Encryption Password] setting, and then specify the encryption key in the application.
- If network administrator's [Encryption Password] setting is not specified, the data for transmission may
 not be encrypted or sent. For details about specifying the network administrator's [Encryption
 Password] setting, see "Registering the Administrator".

Reference

- p.33 "Registering the Administrator"
- p.36 "Logging in Using Administrator Authentication"
- p.37 "Logging out Using Administrator Authentication"

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.

- When "Inactive" is specified for "Exclude HTTPS Communication", access to Web Image Monitor can be lost if the key settings are improperly configured. In order to prevent this, you can specify IPsec to exclude HTTPS transmission by selecting "Active". When you want to include HTTPS transmission, we recommend that you select "Inactive" for "Exclude HTTPS Communication" after confirming that IPsec is properly configured. When "Active" is selected for "Exclude HTTPS Communication", even though HTTPS transmission is not targeted by IPsec, Web Image Monitor might become unusable when TCP is targeted by IPsec from the computer side. If you cannot access Web Image Monitor due to IPsec configuration problems, disable IPsec in System Settings on the control panel, and then access Web Image Monitor. For details about enabling and disabling IPsec using the control panel, see "System Settings", 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/7, Windows Server 2003/2003 R2/2008/2008 R2, Mac OS X 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.



• 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 ISAKMPSA (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.

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 ^{* 1}	Specify whether to enable or disable IPsec.	ActiveInactive
Exclude HTTPS Communication	Specify whether to enable IPsec for HTTPS transmission.	 Active Inactive Specify "Active" if you do not want to use IPsec for HTTPS transmission.
Encryption Key Manual Settings	Specify whether to enable Encryption Key Manual Settings, or use Encryption Key Auto Exchange Settings only.	Active Inactive Specify "Active" if you want to use Encryption Key Manual Settings.

^{* 1} The [IPsec] setting can also be made from the control panel.

Encryption Key Auto Exchange Security Level

When you select a security level, certain security settings are automatically configured. The following table explains security level features.

Security Level	Security Level Features
Authentication Only	Select this level if you want to authenticate the transmission partner and prevent unauthorized data tampering, but not perform data packet encryption. Since the data is sent in cleartext, data packets are vulnerable to eavesdropping attacks. Do not select this if you are exchanging sensitive information.
Authentication and Low Level Encryption	Select this level if you want to encrypt the data packets as well as authenticate the transmission partner and prevent unauthorized packet tampering. Packet encryption helps prevent eavesdropping attacks. This level provides less security than "Authentication and High Level Encryption".
Authentication and High Level Encryption	Select this level if you want to encrypt the data packets as well as authenticate the transmission partner and prevent unauthorized packet tampering. Packet encryption helps prevent eavesdropping attacks. This level provides higher security than "Authentication and Low Level Encryption".

The following table lists the settings that are automatically configured according to the security level.

Setting	Authentication Only	Authentication and Low Level Encryption	Authentication and High Level Encryption
Security Policy	Apply	Apply	Apply
Encapsul ation Mode	Transport	Transport	Transport
IPsec Requirem ent Level	Use When Possible	Use When Possible	Always Require
Authentic ation Method	PSK	PSK	PSK
Phase 1 Hash Algorithm	MD5	SHA1	SHA1

Setting	Authentication Only	Authentication and Low Level Encryption	Authentication and High Level Encryption
Phase 1 Encryptio n Algorithm	DES	3DES	3DES
Phase 1 Diffie- Hellman Group	2	2	2
Phase 2 Security Protocol	АН	ESP	ESP
Phase 2 Authentic ation Algorithm	HMAC-MD5-96/ HMAC-SHA1-96	HMAC-MD5-96/HMAC- SHA1-96	HMAC-SHA1-96
Phase 2 Encryptio n 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 Settings".

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.
Security Policy	Specify how IPsec is handled.	ApplyBypassDiscard
Encapsulation Mode	Specify the encapsulation mode. (auto setting)	Transport Tunnel (Tunnel beginning address - Tunnel ending address) Select the transport mode (this has no bearing on the security level). If you specify "Tunnel", you must then specify the "Tunnel End Point", which are the beginning and ending IP addresses. Set the same address for the beginning point as you set in "Local Address".

Setting	Description	Setting Value
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 are using "PSK", specify a PSK password using up to 32 ASCII characters. If you specify "Certificate", the certificate for IPsec must be installed and specified before it can be used.
PSK Text	Specify the pre-shared key for PSK authentication.	Enter the pre-shared key required for PSK authentication.
Phase 1 HASH Algorithm	Specify the HASH algorithm to be used in phase 1. (auto setting)	• MD5 • SHA1
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.).

Setting	Description	Setting Value
Phase 2 Security Protocol	Specify the security protocol to be used in Phase 2. To apply both encryption and authentication to sent data, specify ESP or AH + ESP. To apply authentication data only, specify AH. (auto setting)	• ESP • AH • ESP+AH
Phase 2 Authentication Algorithm	Specify the authentication algorithm to be used in phase 2. (auto setting)	HMAC-MD5-96HMAC-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. (auto setting)	Inactive1214
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 Setting Items

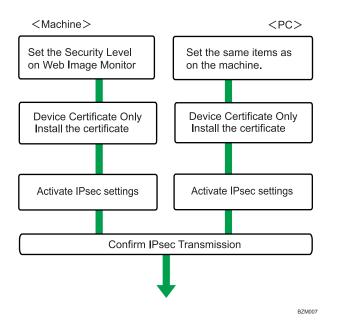
Setting	Description	Setting Value
Address Type	Specify the address type for which IPsec transmission is used.	 Inactive IPv4 IPv6 IPv4/IPv6 (Default Settings only)
Local Address	Specify the machine's address. If you are using multiple IPv6 addresses, you can also specify an address range.	The machine's IPv4 or IPv6 address. If you are not setting an address range, enter 32 after an IPv4 address, or enter 128 after an IPv6 address.
Remote Address	Specify the address of the IPsec transmission partner. You can also specify an address range.	The IPsec transmission partner's IPv4 or IPv6 address. If you are not setting an address range, enter 32 after an IPv4 address, or enter 128 after an IPv6 address.
Encapsulation Mode	Select the encapsulation mode.	• Transport • Tunnel (Tunnel beginning address - Tunnel ending address) If you select "Tunnel", set the "Tunnel End Point", the beginning and ending IP addresses. In "Tunnel End Point", set the same address for the beginning point as you set in "Local Address".
SPI (Output)	Specify the same value as your transmission partner's SPI input value.	Any number between 256 and 4095

Setting	Description	Setting Value
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 • ESP+AH
Authentication Algorithm	Specify the authentication algorithm.	HMAC-MD5-96HMAC-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 AES-128 AES-192 AES-256

Setting	Description	Setting Value
Encryption Key	Specify the key for the encryption algorithm.	Specify a value within the ranges shown below, according to the encryption algorithm. hexadecimal value 0-9, a-f, A-F • DES, set 16 digits • 3DES, set 48 digits • AES-128, set 32 digits • AES-192, set 48 digits • AES-256, set 64 digits AES-256, set 64 digits • DES, set 8 characters • 3DES, set 24 characters • AES-128, set 16 characters • AES-192, set 24 characters • AES-192, set 24 characters • AES-196, set 32 characters

Encryption Key Auto Exchange Settings Configuration Flow

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





- 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 in.

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".
- Set "Exclude HTTPS Communication" to [Active] if you do not want to use IPsec for HTTPS transmission.
- 10. Click [OK].

The setting is changed.

- 11. Click [OK].
- 12. Click [Logout].



To change the transmission partner authentication method for encryption key auto exchange settings
to "Certificate", you must first install and assign a certificate. For details about creating and installing
a device certificate, see "Using S/MIME to Protect E-mail Transmission".

Reference

• p.86 "Using S/MIME to Protect E-mail Transmission"

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 in.

Enter the login user name and login password.

4. Click [Configuration], and then click [Device Certificate] under "Security".

The Device Certificate page appears.

Select the certificate to be used for IPsec from the drop down box in "IPsec" under "Certification". 6. Click [OK].

The certificate for IPsec is specified.

- 7. Click [OK].
- 8. Click [Logout].

Specifying IPsec Settings on the Computer

Specify exactly the same settings for IPsec SA settings on your computer as are specified by the machine's security level on the machine. Setting methods differ according to the computer's operating system. The example procedure shown here uses Windows XP when the Authentication and Low Level Encryption Security level is selected.

- 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].
- 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.

If the settings are not displayed, click [Add].

- 12. Click [OK] twice.
- 13. Click [Add] in the "Rules" tab.

The Security Rule Wizard appears.

- 14. Click [Next].
- 15. Select "This rule does not specify a tunnel", and then click [Next].
- 16. Select the type of network for IPsec, and then click [Next].

17. Select the authentication method, and then click [Next].

If you select "Certificate" for authentication method in Encryption Key Auto Exchange Settings on the machine, specify the device certificate. If you select "PSK", enter the same PSK text specified on the machine with the pre-shared key.

- 18. Click [Add] in the IP Filter List.
- 19. In [Name], enter an IP Filter name, and then click [Add].

The IP Filter Wizard appears.

- 20. Click [Next].
- 21. Select "My IP Address" in "Source address", and then click [Next].
- 22. Select "A specific IP Address" in "Destination address", enter the machine's IP address, and then click [Next].
- 23. Select the protocol type for IPsec, and then click [Next].
- 24. Click [Finish].
- 25. Click [OK].
- 26. Select the IP filter that was just created, and then click [Next].
- 27. Select the IPsec security filter, and then click [Edit].
- 28. Click [Add] in the "Security Methods" tab, select the "Custom" check box, and then click [Settings].
- 29. In "Integrity algorithm", select the authentication algorithm that was specified on the machine in Encryption Key Auto Exchange Settings Phase 2.
- 30. In "Encryption algorithm", select the encryption algorithm that specified on the machine in Encryption Key Auto Exchange Settings Phase 2.
- 31. 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.
- 32. Click [OK] three times.
- 33. Click [Next].
- 34. Click [Finish].

If you are using IPv6 under Windows Vista or a newer version of Windows, you must repeat this procedure from step 13 and specify ICMPv6 as an exception. When you reach step 23, select [58] as the protocol number for the "Other" target protocol type, and then set [Negotiate security] to [Permit].

- 35. Click [OK].
- 36. Click [Close].

The new IP security policy (IPsec settings) is specified.

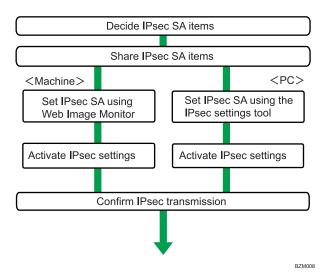
37. Select the security policy that was just created, right click, and then click [Assign].
IPsec settings on the computer are enabled.



- 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 27). 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 Settings" 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 describes the procedure for specifying encryption key manual settings. This can be specified by the network administrator.





- 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 in.

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".
- Set "Exclude HTTPS Communication" to [Active] if you do not want to use IPsec for HTTPS
 communication.
- 11. Click [OK].
- 12. Click [OK].

The setting is changed.

13. Click [Logout].

telnet Setting Commands

You can use telnet to confirm IPsec settings and make setting changes. This section describes 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.



 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 $\{1|2|3|4| default\}$ tunneladdr "beginning IP address" "ending IP address"

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

Authentication algorithm and authentication key settings

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

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

Encryption algorithm and encryption key setting

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

- Enter the separate setting number [1-4] or [default], specify the encryption algorithm, and then set the encryption key.
- If you are setting a hexadecimal number, attach 0x at the beginning. If you have set the encryption
 algorithm to [null], enter an encryption key of arbitrary numbers 2-64 digits long.
- If you are setting an ASCII character string, enter it as is. If you have set the encryption algorithm to [null], enter an encryption key of arbitrary numbers 1-32 digits long.

 Not specifying an encryption algorithm or key displays the current setting. (The encryption key is not displayed.)

Reset setting values

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

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

ipsec ike

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

Display current settings

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

- To display the settings 1-4, specify the number [1-4].
- To display the default setting, specify [default].
- Not specifying any value displays all of the settings.

Disable settings

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

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

Specify the local/remote address for settings 1-4

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

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

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 $\{1|2|3|4|\text{default}\}$ tunneladdr "beginning IP address" "ending IP address"

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

IKE partner authentication method setting

msh> ipsec ike {1|2|3|4|default} auth {psk|rsasig}

- Enter the separate setting number [1-4] or [default] and specify the authentication method.
- Specify [psk] to use a shared key as the authentication method. Specify [rsasig] to use a certificate
 at the authentication method.
- You must also specify the PSK character string when you select [psk].

Note that if you select "Certificate", the certificate for IPsec must be installed and specified before
it can be used. To install and specify the certificate use Web Image Monitor.

PSK character string setting

msh> ipsec ike {1|2|3|4|default} psk "PSK character string"

- If you select PSK as the authentication method, enter the separate setting number [1-4] or [default] and specify the PSK character string.
- Specify the PSK character string using up to 32 ASCII characters.

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 ISAKMPSA (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|\text{default}\}\$ ph2 encrypt $\{\text{null}|\text{des}|3\text{des}|\text{aes}128|\text{aes}192|\$ aes $256\}$

- 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.

6. 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.

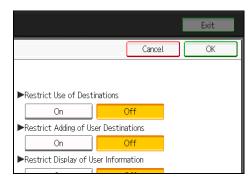
Administrators can change the extended security functions according to their role.

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

- 1. Press the [User Tools] key.
- 2. Press [System Settings].
- 3. Press [Administrator Tools].
- 4. Press [Extended Security].

If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

5. Press the setting you want to change, and change the setting.



6. Press [OK].

7. Press the [User Tools] key.

Reference

- p.36 "Logging in Using Administrator Authentication"
- p.37 "Logging out Using Administrator Authentication"

Extended Security Settings

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 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".

Default: [Off]

Restrict Use of Destinations

This can be specified by the user administrator.

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

A user cannot directly enter the destinations for transmission.

If you specify the setting to receive e-mails via SMTP, you cannot use [Restrict Use of Destinations].

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

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

Default: [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 scanner destination directly, you can register it in the Address Book by pressing [Prg. Dest.]. If [On] is selected for this setting, [Prg. Dest.] does not appear. If you set "Restrict Adding of User Destinations" to [On], users can specify destinations directly, but cannot use [Prg. Dest.] to register data in the Address Book.

When this setting is made, only the user administrator can change the Address Book.

Default: [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

"*****". Because information identifying registered users cannot be viewed, unauthorized users are prevented from obtaining information about the registered files.

Default: [Off]

Enhance File Protection

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

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

The locked files can only be unlocked by the file administrator. When "Enhance File Protection" is specified, (1) appears in the lower right corner of the screen.

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

Default: [Off]

Settings by SNMPv1 and v2

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

Default: [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, if SSL/TLS cannot be enabled when using an application such as DeskTopBinder Professional, change this setting to [Off].

When SSL/TLS can be enabled, make this setting to [On].

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

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

Default: [Off]

Authenticate Current Job

This can be specified by the machine administrator. Using this setting, the machine administrator can enable or disable authentication to protect operations such as canceling copy jobs.

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

If you select [Access Privilege], both the machine administrator and users who have canceled copy jobs in progress can operate this machine.

Even if you select [Login Privilege] and log in to the machine, you cannot cancel copy jobs that are in progress if you are not authorized to use the copier functions.

You can specify [Authenticate Current Job] only if [User Authentication Management] was specified.

Default: [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 #.

Default: [Off]

Passwords can contain the following characters:

- Upper-case letters: A to Z (26 characters)
- Lower-case letters: a to z (26 characters)
- Numbers: 0 to 9 (10 characters)
- Symbols: (space) ! " # \$ % & '() * + , . / : ; < = > ? @ [\]^_` { | } (33 characters)

Some characters are not available, regardless of whether their codes are entered using the keyboard or the control panel.

@Remote Service

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

Default: [Do not Prohibit]

Reference

- p.84 "Preventing Data Leaks Due to Unauthorized Transmission"
- p.94 "Protecting the Address Book"
- p.132 "Setting the SSL / TLS Encryption Mode"

6

Other Security Functions

This section describes settings for preventing information leaks, and functions that you can restrict to further increase security.

Scanner Function

Print & Delete Scanner Journal

To prevent personal information in the transmission/delivery history being printed automatically, set user authentication and the journal will specify [Do not Print: Disable Send] automatically. If you do this, the scanner is automatically disabled when the journal history exceeds 250 transmissions/deliveries. When this happens, click [Print Scanner Journal] or [Delete Scanner Journal]. To print the scanner journal automatically, set [On] for "Print & Delete Scanner Journal".

System Status

Pressing [System Status] on the control panel allows you to check the machine's current status and settings. If administrator authentication has been specified, the [Machine Address Info] tab is displayed only if you have logged in to the machine as an administrator.

Weekly Timer Code

If the weekly timer is enabled and [Weekly Timer Code] is set to [On], you must enter the weekly timer code to turn the power back on after the timer has turned it off.

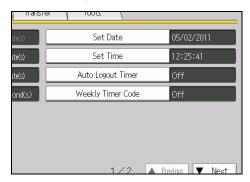
Specifying Weekly Timer Code

This can be specified by the machine administrator.

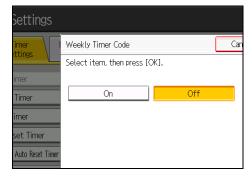
For details about logging in and logging out with administrator authentication, see "Logging in Using Administrator Authentication" and "Logging out Using Administrator Authentication".

- 1. Press the [User Tools] key.
- 2. Press [System Settings].
- 3. Press [Timer Settings].

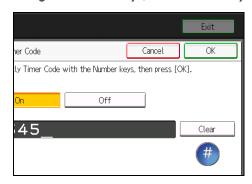
4. Press [Weekly Timer Code].



5. Press [On].



6. Using the number keys, enter the weekly timer code.



The weekly timer code must be one to eight digits long.

- 7. Press [OK].
- 8. Press the [User Tools] key.

Reference

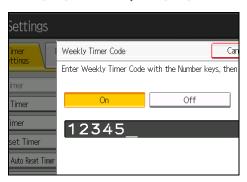
- p.36 "Logging in Using Administrator Authentication"
- p.37 "Logging out Using Administrator Authentication"

Canceling Weekly Timer Code

This can be specified by the machine administrator.

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

- 1. Press the [User Tools] key.
- 2. Press [System Settings].
- 3. Press [Timer Settings].
- 4. Press [Weekly Timer Code].
- 5. Press [Off], and then press [OK].



6. Press the [User Tools] key.



- p.36 "Logging in Using Administrator Authentication"
- p.37 "Logging out Using Administrator Authentication"

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

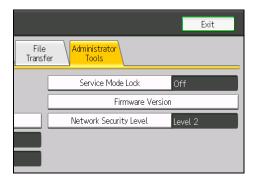
Service Mode Lock

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 in to the machine and cancels the service mode lock to allow the service representative to operate the machine for inspection and repair. This ensures that the inspection and repair are done under the supervision of the machine administrator.

Specifying Service Mode Lock

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

- 1. Press the [User Tools] key.
- 2. Press [System Settings].
- 3. Press [Administrator Tools].
- 4. Press [Service Mode Lock].

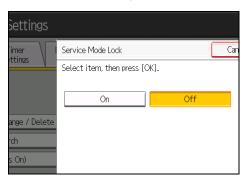


If the setting to be specified does not appear, press [\P Next] to scroll down to other settings.

6

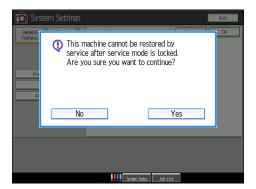
6

5. Press [On], and then press [OK].



A confirmation message appears.

6. Press [Yes].



7. Press the [User Tools] key.

Reference

- p.36 "Logging in Using Administrator Authentication"
- p.37 "Logging out Using Administrator Authentication"

Canceling Service Mode Lock

Before the service representative can carry out an inspection or repair in service mode, the machine administrator must first log in to the machine, release the service mode lock, and then call the service representative. After the inspection or repair is completed, the service mode lock must be reapplied.

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

- 1. Press the [User Tools] key.
- 2. Press [System Settings].
- 3. Press [Administrator Tools].

4. Press [Service Mode Lock].

If the setting to be specified does not appear, press [\P Next] to scroll down to other settings.

- 5. Press [Off], and then press [OK].
- 6. Press the [User Tools] key.

The service representative can switch to service mode.

Reference

- p.36 "Logging in Using Administrator Authentication"
- p.37 "Logging out Using Administrator Authentication"

7. Troubleshooting

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

Authentication Does Not Work Properly

This section describes 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 describes 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 has failed."	The entered login user name or login password is incorrect.	Ask the user administrator for the correct login user name and login password. See the error codes below for possible solutions: B,W,L,I 0206-003 W,L,I 0406-003
"Authentication has failed."	Authentication failed because no more users can be registered. (The number of users registered in the address book has reached capacity.)	Delete unnecessary user addresses. See the error codes below for possible solutions: W,L,I 0612-005
"Authentication has failed."	Cannot access the authentication server when using Windows Authentication, LDAP Authentication, or Integration Server Authentication.	A network or server error may have occurred. Confirm the network in use with the LAN administrator. If an error code appears, follow the instructions next to the error code in the table below.

Messages	Cause	Solutions
"Administrator Authentication for User Management must be set to on before this selection can be made."	User administrator privileges have not been enabled in Administrator Authentication Management.	To specify Basic Authentication, Windows Authentication, LDAP Authentication, or Integration Server Authentication, you must first enable user administrator privileges in Administrator Authentication Management. For details about authentication settings, see "Authentication Setting Procedure".
"The selected file(s) contained file (s) without access privileges. Only file(s) with access privileges will be deleted."	You have tried to delete files without the authority to do so.	Files can be deleted by the file creator (owner) or file administrator. To delete a file which you are not authorized to delete, contact the file creator (owner).

UNote

• If a service call message appears, contact your service representative.

Reference

• p.29 "Authentication Setting Procedure"

An Error Code Appears

When authentication fails, the message "Authentication has failed." appears with an error code. The following tables list the error codes, likely causes of the problems they indicate, and what you can do to resolve those problems. If the error code that appears is not on this table, take a note and contact your service representative.

Error Code Display Position



1. error code

An error code appears.

Basic Authentication

Error Code	Cause	Solution
B0103-000	A TWAIN operation occurred during authentication.	Make sure no other user is logged in to the machine, and then try again.
B0104-000	Failed to decrypt password.	A password error occurred. Make sure the password is entered correctly.
		2. "Restrict Use of Simple Encryption" is enabled. The administrator has restricted use of simple encryption. You can use the encryption key if it has been specified in the driver.
		3. A driver encryption key error occurred. Make sure that the encryption key is correctly specified on the driver.
B0105-000	A login user name was not specified but a DeskTopBinder Professional operation was performed.	Specify the DeskTopBinder Professional login user name correctly.

Error Code	Cause	Solution
B0206-002	A login user name or password error occurred.	Make sure the login user name and password are entered correctly and then log in.
B0206-002	2. The user attempted authentication from an application on the "System Settings" screen, where only the administrator has authentication ability.	Only the administrator has login privileges on this screen. Log in as a general user from the application's login screen.
B0206-003	An authentication error occurred because the user name contains a space, colon (:), or quotation mark (").	Recreate the account if the account name contains any of these prohibited characters. If the account name was entered incorrectly, enter it correctly and log in again.
B0207-001	An authentication error occurred because the address book is being used at another location.	Wait a few minutes and then try again.

Windows Authentication

Error Code	Cause	Solution
W0103-000	A TWAIN operation occurred during authentication.	Make sure no other user is logged in to the machine, and then try again.

Error Code	Cause	Solution
		A password error occurred. Make sure the password is entered correctly.
W0104-000	Failed to decrypt password.	2. "Restrict Use of Simple Encryption" is enabled. The administrator has restricted use of simple encryption. You can use the encryption key if it has been specified in the driver.
		3. A driver encryption key error occurred. Make sure that the encryption key is correctly specified on the driver.
W0105-000	A login user name was not specified but a DeskTopBinder Professional operation was performed.	Specify the DeskTopBinder Professional login user name correctly.
W0206-002	The user attempted authentication from an application on the "System Settings" screen, where only the administrator has authentication ability.	Only the administrator has login privileges on this screen. Log in as a general user from the application's login screen.
W0206-003	An authentication error occurred because the user name contains a space, colon (:), or quotation mark (").	Recreate the account if the account name contains any of these prohibited characters. If the account name was entered incorrectly, enter it correctly and log in again.
W0207-001	An authentication error occurred because the address book is being used at another location.	Wait a few minutes and then try again.

Error Code	Cause	Solution
W0406-101	Authentication cannot be completed because of the high number of authentication attempts.	Wait a few minutes and then try again.
		If the situation does not return to normal, make sure that an authentication attack is not occurring.
		Notify the administrator of the screen message by e-mail, and check the system log for signs of an authentication attack.
W0406-104	Cannot connect to the authentication server.	Make sure that connection to the authentication server is possible.
		Use the Ping Command to check the connection.
W0406-104	2. A login name or password error occurred.	Make sure that the user is registered on the server. Use a registered login user name and password.
W0406-104	3. A domain name error occurred.	Make sure that the Windows authentication domain name is specified correctly.

Error Code	Cause	Solution
W0406-104	4. Cannot resolve the domain name.	Specify the IP address in the domain name and confirm that authentication is successful. If authentication is successful: 1. Make sure that DNS is specified in "Interface Settings", if the top-level domain name is specified in the domain name (such as domainname.xxx.com). 2. Make sure that WINS is specified in "Interface Settings", if a NetBIOS domain name is specified in domain name (such as DOMAINNAME).

Error Code	Cause	Solution
W0406-104	4. Cannot resolve the domain name.	Specify the IP address in the domain name and confirm that authentication is successful. If authentication is unsuccessful: 1. Make sure that Restrict LM/NTLM is not set in either "Domain Controller Security Policy" or "Domain Security Policy". 2. Make sure that the ports for the domain control firewall and the firewall on the machine to the domain control connection path are open. If you are using a Windows firewall, open "Network Connection Properties". Then click detail settings, Windows firewall settings, Click the "Exceptions" tab and specify numbers 137, 139 as the exceptions. In "Network Connection" properties, open TCP/IP properties. Then click detail settings, WINS, and then check the "Enable NetBIOS over
		TCP/IP" box and set number 137 to "Open".
W0400-105	1. The UserPrincipleName (user@domainname.xxx.com) form is being used for the login user name.	The user group cannot be obtained if the UserPrincipleName (user@domainname.xxx.com) form is used. Use "sAMAccountName (user)" to log in, because this account allows you to obtain the user group.

Error Code	Cause	Solution
	2. Current settings do not allow group retrieval.	Make sure the user group's group scope is set to "Global Group" and the group type is set to "Security" in group properties.
		Make sure the account has been added to user group.
W0400-105		Make sure the user group name registered on the machine and the group name on the DC (domain controller) are exactly the same. The DC is case sensitive.
		Make sure that Use Auth. Info at Logon has been specified in Auth. Info in the user account registered on the machine.
		If there is more than one DC, make sure that a confidential relationship has been configured between each DC.
W0400-106	The domain name cannot be resolved.	Make sure that DNS/WINS is specified in the domain name in "Interface Settings".
W0400-200	Due to the high number of authentication attempts, all resources are busy.	Wait a few minutes and then try again.
W0400-202	The SSL settings on the authentication server and the machine do not match.	Make sure the SSL settings on the authentication server and the machine match.
W0400-202	2. The user entered sAMAccountName in the user name to log in.	If a user enters sAMAccountName as the login user name, Idap_bind fails in a parent/subdomain environment. Use UserPrincipleName for the login name instead.

Error Code	Cause	Solution
W0406-003	An authentication error occurred because the user name contains a space, colon (:), or quotation mark (").	Recreate the account if the account name contains any of these prohibited characters. If the account name was entered incorrectly, enter it correctly and log in again.
W0409-000	Authentication timed out because the server did not respond.	Check the network configuration, or settings on the authenticating server.
W0511-000	The authentication server login name is the same as a user name already registered on the machine. (Names are distinguished by the unique attribute specified in LDAP authentication settings.)	Delete the old, duplicated name or change the login name. If the authentication server has just been changed, delete the old name on the server.
W0607-001	An authentication error occurred because the address book is being used at another location.	Wait a few minutes and then try again.
W0606-004	Authentication failed because the user name contains language that cannot be used by general users.	Do not use "other", "admin", "supervisor" or "HIDE*" in general user accounts.
W0612-005	Authentication failed because no more users can be registered. (The number of users registered in the address book has reached capacity.)	Ask the user administrator to delete unused user accounts in the address book.
W0707-001	An authentication error occurred because the address book is being used at another location.	Wait a few minutes and then try again.

LDAP Authentication

Error Code	Cause	Solution
L0103-000	A TWAIN operation occurred during authentication.	Make sure no other user is logged in to the machine, and then try again.
L0104-000	Failed to decrypt password.	1. A password error occurred. Make sure the password is entered correctly. 2. "Restrict Use of Simple Encryption" is enabled. The administrator has restricted use of simple encryption. You can use the encryption key if it has been specified in the driver. 3. A driver encryption key error occurred. Make sure that the encryption key is correctly specified on the driver.
L0105-000	A login user name was not specified but a DeskTopBinder Professional operation was performed.	Specify the DeskTopBinder Professional login user name correctly.
L0206-002	A user attempted authentication from an application on the "System Settings" screen, where only the administrator has authentication ability.	Only the administrator has login privileges on this screen. Log in as a general user from the application's login screen.
L0206-003	An authentication error occurred because the user name contains a space, colon (:), or quotation mark (").	Recreate the account if the account name contains any of these prohibited characters. If the account name was entered incorrectly, enter it correctly and log in again.

Error Code	Cause	Solution
L0207-001	An authentication error occurred because the address book is being used at another location.	Wait a few minutes and then try again.
L0306-018	The LDAP server is not correctly configured.	Make sure that a connection test is successful with the current LDAP server configuration.
L0307-001	An authentication error occurred because the address book is being used at another location.	Wait a few minutes and then try again.
L0400-210	Failed to obtain user information in LDAP search.	The login attribute's search criteria might not be specified or the specified search information is unobtainable. Make sure the login name attribute is specified correctly.
L0406-003	An authentication error occurred because the user name contains a space, colon (:), or quotation mark (").	Recreate the account if the account name contains any of these prohibited characters. If the account name was entered incorrectly, enter it correctly and log in again.
L0406-200	Authentication cannot be completed because of the high number of authentication attempts.	Wait a few minutes and then try again. If the situation does not return to normal, make sure that an authentication attack is not occurring. Notify the administrator of the screen message by e-mail, and check the system log for signs of an authentication attack.

Error Code	Cause	Solution
L0406-201	Authentication is disabled in the LDAP server settings.	Change the LDAP server settings in administrator tools, in "System Settings".
	1. There is an error in the LDAP authentication settings, LDAP server, or network configuration.	1. Make sure that a connection test is successful with the current LDAP server configuration.
		If connection is not successful, there might be an error in the network settings.
10404 202		Check the domain name or DNS settings in "Interface Settings".
L0406-202 L0406-203		2. Make sure the LDAP server is specified correctly in the LDAP authentication settings.
		3. Make sure the login name attribute is entered correctly in the LDAP authentication settings.
		4. Make sure the SSL settings are supported by the LDAP server.
L0406-202 L0406-203 2. A login user name or password error occurred.		Make sure the login user name and password are entered correctly. Make sure a useable login name is registered on the machine. Authentication will fail in the
	password error occurred.	following cases: If the login user name contains a space, colon (:), or quotation mark ("). If the login user name exceeds 128 bytes.

Error Code	Cause	Solution
L0400-210	Failed to obtain user information in LDAP search.	The login attribute's search criteria might not be specified or the specified search information is unobtainable. Make sure the login name attribute is specified correctly.
L0406-003	An authentication error occurred because the user name contains a space, colon (:), or quotation mark (").	Recreate the account if the account name contains any of these prohibited characters. If the account name was entered incorrectly, enter it correctly and log in again.
L0409-000	Authentication timed out because the server did not respond.	Contact the server or network administrator. If the situation does not return to normal, contact your service representative.
L0511-000	The authentication server login name is the same as a user name already registered on the machine. (Names are distinguished by the unique attribute specified in the LDAP authentication settings.)	Delete the old, duplicated name or change the login name. If the authentication server has just been changed, delete the old name on the server.
L0607-001	An authentication error occurred because the address book is being used at another location.	Wait a few minutes and then try again.
L606-004	Authentication failed because the user name contains language that cannot be used by general users.	Do not use "other", "admin", "supervisor" or "HIDE*" in general user accounts.
L0612-005	Authentication failed because no more users can be registered. (The number of users registered in the address book has reached capacity.)	Ask the user administrator to delete unused user accounts in the address book.

Error Code	Cause	Solution
L0707-001	An authentication error occurred because the address book is being used at another location.	Wait a few minutes and then try again.

Integration Server Authentication

Error Code	Cause	Solution
10103-000	A TWAIN operation occurred during authentication.	Make sure no other user is logged in to the machine, and then try again.
		A password error occurred. Make sure the password is entered correctly.
10104-000	Failed to decrypt password.	2. "Restrict Use of Simple Encryption" is enabled. The administrator has restricted use of simple encryption. You can use the encryption key if it has been specified in the driver.
		3. A driver encryption key error occurred. Make sure that the encryption key is correctly specified on the driver.
10105-000	A login user name was not specified but a DeskTopBinder Professional operation was performed.	Specify the DeskTopBinder Professional login user name correctly.
10206-002	A user attempted authentication from an application on the "System Settings" screen, where only the administrator has authentication ability.	Only the administrator has login privileges on this screen. Log in as a general user from the application's login screen.

Error Code	Cause	Solution
10206-003	An authentication error occurred because the user name contains a space, colon (:), or quotation mark (").	Recreate the account if the account name contains any of these prohibited characters. If the account name was entered incorrectly, enter it correctly and log in again.
10207-001	An authentication error occurred because the address book is being used at another location.	Wait a few minutes and then try again.
10406-003	An authentication error occurred because the user name contains a space, colon (:), or quotation mark (").	Recreate the account if the account name contains any of these prohibited characters. If account name was entered incorrectly, enter it correctly and log in again.
10406-301	The URL could not be obtained.	Obtain the URL using [Obtain URL] in Integration Server authentication.
10406-301	2. A login user name or password error occurred.	1. Make sure the login user name and password are entered correctly. 2. Make sure that a useable login name is registered on the machine. Authentication will fail in the following cases. If the login user name contains a space, colon (:), or quotation mark ("). If the login user name exceeds 128 bytes.

Error Code	Cause	Solution
10409-000	Authentication timed out because the server did not respond.	Contact the server or network administrator. If the situation does not return to normal, contact your service representative.
10511-000	The authentication server login name is the same as a user name already registered on the machine. (Names are distinguished by the unique attribute specified in the LDAP authentication settings.)	Delete the old, duplicated name or change the login name. If the authentication server has just been changed, delete the old name on the server.
10607-001	An authentication error occurred because the address book is being used at another location.	Wait a few minutes and then try again.
10606-004	Authentication failed because the user name contains language that cannot be used by general users.	Do not use "other", "admin", "supervisor" or "HIDE*" in general user accounts.
10612-005	Authentication failed because no more users can be registered. (The number of users registered in the address book has reached capacity.)	Ask the user administrator to delete unused user accounts in the address book.
10707-001	An authentication error occurred because the address book is being used at another location.	Wait a few minutes and then try again.

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: Connect with the TWAIN 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: • Connect with the TWAIN 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 authenticate using the TWAIN driver.	Another user is logging in to the machine.	Wait for the user to log out.
Cannot authenticate using the TWAIN driver.	Authentication is taking time because of operating conditions.	Make sure the LDAP server setting is correct. Make sure the network settings are correct.
Cannot authenticate using the TWAIN driver.	Authentication is not possible while the machine is editing the Address Book data.	Wait until editing of the Address Book data is complete.
After you execute "Encrypt Address Book", the "Exit" message does not appear.	The hard disk may be faulty. The file may be corrupt.	Contact your service representative.
Cannot log in to the machine using [Document Server (MFP):Authentication/ Encryption] in DeskTopBinder Professional.	"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 [Off]. 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".

Condition	Cause	Solution
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 [Off]. Alternatively, enable "SSL/TLS", install the server certificate in the machine, and then install the certificate in the computer. See "Setting the SSL/TLS Encryption Mode".
Cannot connect to the ScanRouter delivery software.	The ScanRouter delivery software may not be supported by the machine.	Update to the latest version of the ScanRouter delivery software.
Cannot access the machine using ScanRouter EX Professional V2.	ScanRouter EX Professional V2 does not support user authentication.	ScanRouter EX Professional V2 does not support user authentication.
Cannot log out when using the copying or scanner functions.	The original has not been scanned completely.	When the original has been scanned completely, press [#], remove the original, and then log out.
"Prg. Dest." does not appear on the scanner screen for specifying destinations.	"Restrict Adding of User Destinations" is set to [On] 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 disabled, but stored files do not appear.	User authentication might have been disabled without "All Users" being selected for user access to stored files.	Enable user authentication, and then select "All Users" in "Change Access Priv." for all stored files. For details, see "Specifying Access Permission for Stored Files".

Condition	Cause	Solution
User authentication is disabled, but destinations registered in the machine's address book do not appear.	User authentication might have been disabled without "All Users" being selected for "Protect Destination".	Enable user authentication, and then select "All Users" in "Protect Destination" for all registered destinations.
		For details, see "Protecting the Address Book".
If you try to interrupt a job while copying or scanning, an authentication screen appears.	With this machine, you can log out while copying or scanning. If you try to interrupt copying or scanning after logging out, an authentication screen appears.	Only the user who executed a copying or scanning job can interrupt it. Wait until the job has completed or consult an administrator or the user who executed the job.

■ Reference

- p.71 "Specifying Access Permission for Stored Files"
- p.94 "Protecting the Address Book"
- p.125 "Driver Encryption Key"
- p.132 "Setting the SSL / TLS Encryption Mode"

8. Appendix

Supervisor Operations

The supervisor can delete an administrator's password and specify a new one.

If any of the administrators forget their passwords or if any of the administrators change, the supervisor can assign a new password. If logged in using the supervisor's user name and password, you cannot use normal functions or specify defaults.

Log in as the supervisor only to change an administrator's password.

Mportant !

- 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.
- User names cannot contain numbers only, a space, colon (:), or quotation mark ("), nor can they be
 left blank. For details about what characters the password can contain, see "Specifying the Extended
 Security Functions".
- 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.



- You cannot specify the same login user name for the supervisor and the administrators.
- Using Web Image Monitor, you can log in as the supervisor and delete an administrator's password
 or specify a new one.

Reference

• p.161 "Specifying the Extended Security Functions"

Logging in as the Supervisor

If administrator authentication has been specified, log in using the supervisor login user name and login password. This section describes how to log in.

- 1. Press the [User Tools] key.
- 2. Press the [Login/Logout] key.
- 3. Press [Login].

4. Enter a login user name, and then press [OK].

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

5. Enter a login password, and then press [OK].

When the supervisor is making settings for the first time, a password is not required; the supervisor can simply press [OK] to proceed.

The message, "Authenticating... Please wait." appears.

Logging out as the Supervisor

If administrator authentication has been specified, be sure to log out after completing settings. This section describes how to log out after completing settings.

- 1. Press the [Login/Logout] key.
- 2. Press [Yes].

The message, "Logging out... Please Wait." appears.

Changing the Supervisor

This section describes how to change the supervisor's login name and password. To do this, you must to enable the user administrator's privileges through the settings under [Administrator Authentication Management]. For details, see "Specifying Administrator Privileges".

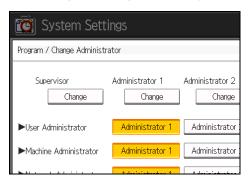
- 1. Press the [User Tools] key.
- 2. Press the [Login/Logout] key.
- 3. Log in as the supervisor.

For details about logging in as the supervisor, see "Logging in as the Supervisor".

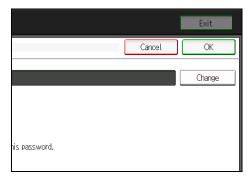
- 4. Press [System Settings].
- 5. Press [Administrator Tools].
- 6. Press [Program / Change Administrator].

If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

7. Under "Supervisor", press [Change].



8. Press [Change] for "Login User Name".



- 9. Enter the login user name, and then press [OK].
- 10. Press [Change] for "Login Password".
- 11. Enter the login password, and then press [OK].
- 12. If a password reentry screen appears, enter the login password, and then press [OK].
- 13. Press [OK] twice.

You will be automatically logged out.

14. Press the [User Tools] key.



- p.31 "Specifying Administrator Privileges"
- p.193 "Logging in as the Supervisor"

Resetting an Administrator's Password

This section describes how to reset the administrators' passwords. Administrator login names cannot be changed.

1. Press the [User Tools] key.

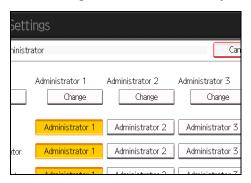
- 2. Press the [Login/Logout] key.
- 3. Log in as the supervisor.

For details about logging in as the supervisor, see "Logging in as the Supervisor".

- 4. Press [System Settings].
- 5. Press [Administrator Tools].
- 6. Press [Program / Change Administrator].

If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

7. Press [Change] for the administrator you wish to reset.



- 8. Press [Change] for "Login Password".
- 9. Enter the login password, and then press [OK].
- 10. If a password reentry screen appears, enter the login password, and then press [OK].
- 11. Press [OK] twice.

You will be automatically logged out.

12. Press the [User Tools] key.

Reference

• p.193 "Logging in as the Supervisor"

Q

ŏ

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.

Timer Settings

All the settings can be specified.

Interface Settings

DNS Configuration
 You can perform a connection test.

File Transfer

The following settings can be specified.

- Delivery Option
- SMTP Authentication

All the settings can be specified.

• POP before SMTP

All the settings can be specified.

- Reception Protocol
- POP3 / IMAP4 Settings

All the settings can be specified.

- Administrator's E-mail Address
- Default User Name / Password (Send)

All the settings can be specified.

Program / Change / Delete E-mail Message
 All the settings can be specified.

Administrator Tools

The following settings can be specified.

• Address Book Management

Search

Switch Title

• Address Book: Program / Change / Delete Group

Search

Switch Title

• Display / Print Counter

Print Counter List

• Display / Clear / Print Counter per User

Print the counter list for all users' jobs

Print the counter list for each user's jobs

• User Authentication Management

You can specify which authentication to use.

You can also edit the settings for each function.

- Enhanced Authentication Management
- Administrator Authentication Management

Machine Management

• Program / Change Administrator

Machine Administrator

- External Charge Unit Management
- Enhanced External Charge Unit Management
- Extended Security

Restrict Display of User Information

Authenticate Current Job

@Remote Service

Program / Change / Delete LDAP Server
 All the settings can be specified.

- LDAP Search
- AOF (Always On)
- Service Test Call
- Notify Machine Status
- Service Mode Lock
- Auto Erase Memory Setting
- Erase All Memory



 "Auto Erase Memory Setting" and the "Erase All Memory" setting are available only if the DataOverwriteSecurity unit is installed.

Maintenance

The following settings can be specified.

- Auto Colour Calibration
 - All the settings can be specified.
- Colour Registration
 - All the settings can be specified.
- Erase Print Image Traces
 - All the settings can be specified.

Copier / Document Server Features

The following settings can be specified.

General Features

All the settings can be specified.

Reproduction Ratio

All the settings can be specified.

Edit

All the settings can be specified.

Stamp

All the settings can be specified.

Input / Output

All the settings can be specified.

Adjust Colour Image

All the settings can be specified.

Administrator Tools

All the settings can be specified.

Scanner Features

The following settings can be specified.

General Settings

All the settings can be specified.

Scan Settings

All the settings can be specified.

Send Settings

The following settings can be specified.

- Compression (Black & White)
- Compression (Gray Scale / Full Colour)
- High Compression PDF Level
- Insert Additional E-mail Info
- No. of Digits for Single Page Files
- Stored File E-mail Method

Initial Settings

All the settings can be specified.

Tray Paper Settings

For details about the user privileges required for specifying the paper settings and advanced settings for various commercially-available paper types, contact your service representative.

Settings via Web Image Monitor

The following settings can be specified.

Home

Reset Device

Job

All the settings can be specified.

Device Settings

For details about the user privileges required for specifying the paper settings and advanced settings for various commercially-available paper types, contact your service representative.

System

Print Priority

Function Reset Timer

Permit Firmware Update

Display IP Address on Device Display Panel

Output Tray

Paper Tray Priority

Front Cover Sheet Tray

Back Cover Sheet Tray

Slip Sheet Tray

Designation Sheet 1 Tray

Designation Sheet 2 Tray

Designation Sheet 3 Tray

Designation Sheet 4 Tray

Designation Sheet 5 Tray

Designation Sheet 6 Tray

Designation Sheet 7 Tray

Designation Sheet 8 Tray

Designation Sheet 9 Tray

Separation Sheet Tray

• Date/Time

All the settings can be specified.

• Timer

All the settings can be specified.

• E-mail

Administrator E-mail Address

Reception Protocol

SMTP Authentication

SMTP Auth. E-mail Address

SMTP Auth. User Name

SMTP Auth. Password

SMTP Auth. Encryption

POP before SMTP

POP E-mail Address

POP User Name

POP Password

Timeout setting after POP Auth.

POP3/IMAP4 Server Name

POP3/IMAP4 Encryption

E-mail Notification E-mail Address

Receive E-mail Notification

E-mail Notification User Name

E-mail Notification Password

• Auto E-mail Notification

All the settings can be specified.

• On-demand E-mail Notification

All the settings can be specified.

• File Transfer

All the settings can be specified.

User Authentication Management

All the settings can be specified.

• Administrator Authentication Management

Machine Administrator Authentication

Available Settings for Machine Administrator

• Program/Change Administrator

You can specify the following administrator settings as 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.

Scanner

• General Settings

All the settings can be specified.

Scan Settings

All the settings can be specified.

• Send Settings

Compression (Black & White)

Compression (Gray Scale / Full Color)

High Compression PDF Level

Insert Additional E-mail Info

No. of Digits for Single Page Files

Stored File E-mail Method

• Initial Settings

All the settings can be specified.

• Default Settings for Normal Screens on Device

All the settings can be specified.

 Default Settings for Simplified Screens on Device All the settings can be specified.

Network

SNMPv3

Access Type (Machine Administrator)

RC Gate

All the settings can be specified.

Webpage

• Webpage

Download Help File

Extended Feature Settings

All the settings can be specified.

Network Administrator Settings

The network administrator settings that can be specified are as follows:

System Settings

The following settings can be specified.

Interface Settings

If DHCP is set to On, the settings that are automatically obtained via DHCP cannot be specified.

- Print list
- Network

All the settings can be specified.

File Transfer

- SMTP Server
 - All the settings can be specified.
- E-mail Communication Port
 - All the settings can be specified.
- E-mail Reception Interval
- Max. Reception E-mail Size
- E-mail Storage in Server
- Auto Specify Sender Name
- Scanner Resend Interval Time
- Number of Scanner Resends

Administrator Tools

- Address Book Management
 - Search
 - Switch Title
- Address Book: Program / Change / Delete Group
 - Search
 - Switch Title
- Administrator Authentication Management
 - Network Management
- Program / Change Administrator
 - Network Administrator

• Extended Security

Driver Encryption Key

Settings by SNMPv1 and v2

Restrict Use of Simple Encryption

• Network Security Level

Scanner Features

The following settings can be specified.

Send Settings

- Max. E-mail Size
- Divide & Send E-mail

Settings via Web Image Monitor

The following settings can be specified.

Device Settings

System

Device Name

Comment

Location

• E-mail

Max. Reception E-mail Size

E-mail Reception Interval

E-mail Storage in Server

SMTP Server Name

SMTP Port No.

POP3 Reception Port No.

IMAP4 Reception Port No.

• Auto E-mail Notification

You can select groups to notify.

• Administrator Authentication Management

Network Administrator Authentication

Available Settings for Network Administrator

• Program/Change Administrator

You can specify the following administrator settings for the network administrator.

Login User Name

Login Password

Encryption Password

Scanner

• Send Settings

Max E-mail Size

Divide & Send E-mail

Network

IPv/

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.

Security

Network Security

All the settings can be specified.

Access Control

All the settings can be specified.

• SSL/TLS

All the settings can be specified.

ssh

All the settings can be specified.

• Site Certificate

All the settings can be specified.

Device Certificate

All the settings can be specified.

IPsec

All the settings can be specified.

• S/MIME

All the settings can be specified.

Webpage

• Webpage

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.

Interface Settings

DNS Configuration

You can perform a connection test.

Administrator Tools

• Address Book Management

Search

Switch Title

• Address Book: Program / Change / Delete Group

Search

Switch Title

• Administrator Authentication Management

File Management

• Program / Change Administrator

File Administrator

Extended Security

Enhance File Protection

- Auto Delete File in Document Server
- Delete All Files in Document Server

Settings via Web Image Monitor

The following settings can be specified.

Document Server

All the settings can be specified.

Device Settings

• Auto E-mail Notification

You can select groups to notify.

• Administrator Authentication Management

File Administrator Authentication

Available Settings for File Administrator

• Program/Change Administrator

You can specify the following administrator settings for the file administrator.

Login User Name

Login Password

Encryption Password

Webpage

• Webpage

Download Help File

User Administrator Settings

The user administrator settings that can be specified are as follows:

System Settings

The following settings can be specified.

Interface Settings

DNS Configuration

You can perform a connection test.

Administrator Tools

- Address Book Management
 All the settings can be specified.
- Address Book: Program / Change / Delete Group
 All the settings can be specified.
- Address Book: Change Order
- Print Address Book: Destination List
- Address Book: Edit Title
- Address Book: Switch Title
- Back Up / Restore Address Book
- Display / Clear / Print Counter per User

Clear the counter for all user's jobs

Clear the counter for each user's jobs

- Administrator Authentication Management
 - User Management
- Program / Change Administrator

User Administrator

• Extended Security

Encrypt Address Book

Restrict Use of Destinations

Restrict Adding of User Destinations

Password Policy

Q

R

Settings via Web Image Monitor

The following settings can be specified.

Address Book

All the settings can be specified.

Device Settings

• Auto E-mail Notification

You can select groups to notify.

• Administrator Authentication Management

User Administrator Authentication

Available Settings for User Administrator

• Program/Change Administrator

You can specify the following administrator settings for the user administrator.

Login User Name

Login Password

Encryption Password

Webpage

Webpage

Download Help File

Document Server File Permissions

The authorities for using the files stored in Document Server are as follows.

The authority designations in the list indicate users with the following authorities.

- Read-only (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.
- Full Control (User) = This is a user assigned "Full Control" authority.
- Owner (User) = This is a user who can store files in the machine and authorize other users to view, edit, or delete those files.
- File Admin. = This is the file administrator.

A =Granted authority to operate.

- =Not granted authority to operate.

Settings	Read-only (User)	Edit (User)	Edit / Delete (User)	Full Control (User)	Owner (User)	File Admin.
Viewing Details About Stored Files	А	А	А	А	А	A
Viewing Thumbnails	А	А	А	Α	Α	A
Print/Transmission	А	Α	А	Α	А	-
Changing Information About Stored Files	-	А	А	А	A*1	-
Deleting Files	-	-	А	Α	A*1	A
Specifying File Password	-	-	-	-	А	А
Specifying Permissions for Users/Groups	-	-	-	А	A*1	А
Unlocking Files	-	-	-	-	-	А

^{*1} The owner can change the authorities for these settings as necessary.

The Privilege for User Account Settings in the Address Book

The authorities for using the Address Book are as follows:

The authority designations in the list indicate users with the following authorities.

- Abbreviations in the table heads
 - Read-only (User) = This is a user assigned "Read-only" authority.
 - Edit (User) = This is a user assigned "Edit" authority.
 - Edit / Delete (User) = This is a user assigned "Edit / Delete" authority.
 - Full Control (User) = This is a user assigned "Full Control" authority.
 - Registered User = This is a user that has personal information registered in the Address Book and has a login password and user name.
 - User Admin. = This is the user administrator.
- Abbreviations in the table columns
 - R/W (Read and Write) = You can view and change the setting.
 - R (Read) = You can view the setting.
 - N/A (Not Applicable) = You cannot view or specify the setting.

Tab Name: Names

Settings	Read- only (User)	Edit (User)	Edit / Delete (User)	Full Control (User)	Registere d User	User Admin.
Name	R	R/W	R/W	R/W	R/W	R/W
Key Display	R	R/W	R/W	R/W	R/W	R/W
Registration No.	R	R/W	R/W	R/W	R/W	R/W
Select Title	R	R/W	R/W	R/W	R/W	R/W

Tab Name: Auth. Info

Settings	Read- only (User)	Edit (User)	Edit / Delete (User)	Full Control (User)	Registere d User	User Admin.
User Code	N/A	N/A	N/A	N/A	N/A	R/W

g

Settings	Read- only (User)	Edit (User)	Edit / Delete (User)	Full Control (User)	Registere d User	User Admin.
Login User Name	N/A	N/A	N/A	N/A	R	R/W
Login Password	N/A	N/A	N/A	N/A	R/W*1	R/W*1
SMTP Authentication	N/A	N/A	N/A	N/A	R/W*1	R/W*1
Folder Authentication	R	R/W*1	R/W*1	R/W*1	R/W*1	R/W*1
LDAP Authentication	N/A	N/A	N/A	N/A	R/W*1	R/W*1
Available Functions	N/A	N/A	N/A	N/A	R	R/W

^{* 1} The password for "Login Password", "SMTP Authentication", "Folder Authentication" or "LDAP Authentication" can be entered or changed but not displayed.

Tab Name: Protection

Settings	Read- only (User)	Edit (User)	Edit / Delete (User)	Full Control (User)	Registere d User	User Admin.
Use Name as	R	R/W	R/W	R/W	R/W	R/W
Protection Code	N/A	N/A	N/A	R/W*2	R/W*2	R/W*2
Protection Object	R	R/W	R/W	R/W	R/W	R/W
Protect Destination: Permissions for Users/Groups	N/A	N/A	N/A	R/W	R/W	R/W
Protect File(s): Permissions for Users/Groups	N/A	N/A	N/A	R/W	R/W	R/W

^{*2} The code for "Protection Code" can be entered or changed but not displayed.

8

Tab Name: E-mail

Settings	Read- only (User)	Edit (User)	Edit / Delete (User)	Full Control (User)	Registere d User	User Admin.
E-mail Address	R	R/W	R/W	R/W	R/W	R/W

Tab Name: Folder

Settings	Read- only (User)	Edit (User)	Edit / Delete (User)	Full Control (User)	Register ed User	User Admin.
SMB/FTP/NCP	R	R/W	R/W	R/W	R/W	R/W
SMB: Path	R	R/W	R/W	R/W	R/W	R/W
FTP: Server Name	R	R/W	R/W	R/W	R/W	R/W
FTP: Path	R	R/W	R/W	R/W	R/W	R/W
FTP: Port Number	R	R/W	R/W	R/W	R/W	R/W
NCP: Path	R	R/W	R/W	R/W	R/W	R/W
NCP: Connection Type	R	R/W	R/W	R/W	R/W	R/W

Tab Name: Add to Group

Settings	Read- only (User)	Edit (User)	Edit / Delete (User)	Full Control (User)	Registere d User	User Admin.
Registration No.	R	R/W	R/W	R/W	R/W	R/W
Search	N/A	R/W	R/W	R/W	R/W	R/W
Switch Title	R/W	R/W	R/W	R/W	R/W	R/W

User Settings - Control Panel Settings

This section describes 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.

8

ŏ

Copier / Document Server Features

When administrator authentication is enabled, the administrator's configuration of Menu Protect determines which functions and settings are available to users.

User privileges are as follows:

• Abbreviations in the table columns

R/W (Read and Write) = Both reading and modifying the setting are available.

R(Read) = Reading only.

N/A (Not Applicable) = Neither reading nor modifying the setting is available.

When [Menu Protect] is set to [Off], all the following settings can be viewed and modified.

General Features

Settings	Level 1	Level 2
Auto Image Density Priority	R	R
Original Type Priority	R	R
Original Photo Type Priority	R	R
Original Orientation in Duplex Mode	R	R
Copy Orientation in Duplex Mode	R	R
Reserve Job Mode	R	R
Reservation Screen Auto-off Timer	R	R
Max. Copy Quantity	R	R
Manual Original Counter Reset	R	R
Auto Tray Switching	R	R
Dark Background	R/W	R
Panel Features Default	R	R
Image Adjustment Priority	R	R
Paper Display	R	R
Original Type Display	R	R
Alert Sound: Original left on Exposure Glass	R	R

Reproduction Ratio

Settings	Level 1	Level 2
Shortcut Reduce/Enlarge	R	R
Reproduction Ratio	R	R
Reduce/Enlarge Ratio Priority	R	R
Ratio for Create Margin	R	R

Edit

Settings	Level 1	Level 2
Front Margin: Left / Right	R	R
Back Margin: Left / Right	R	R
Front Margin: Top / Bottom	R	R
Back Margin: Top / Bottom	R	R
1 Sided→2 Sided Auto Margin: TtoT	R	R
1 Sided→2 Sided Auto Margin: TtoB	R	R
Creep Setting for Magazine	R	R
Erase Border Width	R	R
Erase Original Shadow in Combine	R/W	R
Erase Centre Width	R	R
Front Cover Copy in Combine	R/W	R
Copy Order in Combine	R	R

Settings	Level 1	Level 2
Orientation: Booklet, Magazine	R/W	R
Image Repeat Separation Line	R/W	R
Double Copies Separation Line	R/W	R
Separation Line in Combine	R/W	R
Copy on Designating Page in Combine	R/W	R
Copy Back Cover	R/W	R
Double Copies Position	R/W	R

Stamp

Preset Stamp

Settings	Level 1	Level 2
Stamp Language	R/W	R
Stamp Priority	R	R
Stamp Format: COPY	R/W	R
Stamp Format: URGENT	R/W	R
Stamp Format: PRIORITY	R/W	R
Stamp Format: For Your Info.	R/W	R
Stamp Format: PRELIMINARY	R/W	R
Stamp Format: For Internal Use Only	R/W	R
Stamp Format: CONFIDENTIAL	R/W	R
Stamp Format: DRAFT	R/W	R
Stamp Colour: COPY	R	R
Stamp Colour: URGENT	R	R
Stamp Colour: PRIORITY	R	R
Stamp Colour: For Your Info.	R	R

Settings	Level 1	Level 2
Stamp Colour: PRELIMINARY	R	R
Stamp Colour: For Internal Use Only	R	R
Stamp Colour: CONFIDENTIAL	R	R
Stamp Colour: DRAFT	R	R

If you select [Level 1], you can only specify "Adjust Stamp Position" and "Stamp Position" in "Stamp Format".

User Stamp

Settings	Level 1	Level 2
Program / Delete Stamp	R/W	R
Stamp Format: 1-5	R/W	R
Stamp Colour: 1-5	R/W	R

Date Stamp

Settings	Level 1	Level 2
Format	R	R
Font	R/W	R
Size	R/W	R
Superimpose	R/W	R
Stamp Colour	R	R
Stamp Setting	R/W	R

If you select [Level 1], you can only specify "Adjust Stamp Position" and "Stamp Position" in "Stamp Setting".

Page Numbering

Settings	Level 1	Level 2
Stamp Format	R	R

8

Settings	Level 1	Level 2
Font	R/W	R
Size	R/W	R
Duplex Back Page Stamping Position	R/W	R
Page Numbering in Combine	R/W	R
Stamp on Designating Slip Sheet	R/W	R
Stamp Position: P1, P2	R/W	R
Stamp Position: 1/5, 2/5	R/W	R
Stamp Position: -1-, -2	R/W	R
Stamp Position: P.1, P.2	R/W	R
Stamp Position: 1, 2	R/W	R
Stamp Position: 1-1, 1-2	R/W	R
Superimpose	R/W	R
Stamp Colour	R	R
Page Numbering Initial Letter	R/W	R/W

Stamp Text

Settings	Level 1	Level 2
Font	R/W	R
Size	R/W	R
Superimpose	R/W	R
Stamp Colour	R	R
Stamp Setting	R/W	R

If you select [Level 1], you can only specify "Adjust Stamp Position" and "Stamp Position" in "Stamp Setting".

Settings	Level 1	Level 2
SADF Auto Reset	R	R
Copy Eject Face Method in Glass Mode	R	R
Memory Full Auto Scan Restart	R	R
Sort / Stack Shift Tray Setting	R	R
Insert Separation Sheet	R	R
Letterhead Setting	R	R
Fore Edge Cut Setting	R	R
Staple Position	R/W	R
Punch Type	R/W	R
Ring Binding/Fold Type/Stacker Output Tray	R/W	R
Finisher: Staple Position	R/W	R
Finisher: Punch Type	R/W	R
Finisher: Ring Binding Type	R/W	R
Simplified Screen: Finishing Types	R/W	R

The "Fore Edge Cut Setting" is available only if the trimmer is installed.

Depending on which options are installed, "Ring Binding/Fold Type/Stacker Output Tray" will appear under different names.

The "Finisher: Ring Binding Type" setting is available only if the ring binder is installed.

Adjust Colour Image

Settings	Level 1	Level 2
Background Density of ADS (Full Colour / Two-colour)	R/W	R
Colour Sensitivity	R/W	R
A.C.S. Sensitivity	R/W	R
A.C.S. Priority	R/W	R

Settings	Level 1	Level 2
Inkjet Output Type	R/W	R



- The default for Menu Protect is [Level 2].
- Settings that are not in the list can only be viewed, regardless of the menu protect level setting.

Scanner Features

When administrator authentication is enabled, the administrator's configuration of Menu Protect determines which functions and settings are available to users.

User privileges are as follows:

• Abbreviations in the table columns

R/W (Read and Write) = Both reading and modifying the setting are available.

R (Read) = Reading only.

N/A (Not Applicable) = Neither reading nor modifying the setting is available.

When [Menu Protect] is set to [Off], all the following settings can be viewed and modified.

General Settings

Settings	Level 1	Level 2
Switch Title	R	R
Update Delivery Server Destination List	R/W	R
Search Destination	R	R
TWAIN Standby Time	R	R
Destination List Display Priority 1	R	R
Destination List Display Priority 2	R	R
Print & Delete Scanner Journal	R	R
Print Scanner Journal	N/A	N/A
Delete Scanner Journal	N/A	N/A

Scan Settings

Settings	Level 1	Level 2
A.C.S. Sensitivity Level	R	R
Wait Time for Next Orig. : Exposure Glass	R	R
Wait Time for Next Original(s): SADF	R	R
Background Density of ADS (Full Colour)	R	R

8

8

Send Settings

Settings	Level 1	Level 2
Compression (Black & White)	R/W	R
Compression (Gray Scale / Full Colour)	R/W	R
High Compression PDF Level	R/W	R
Insert Additional E-mail Info	R/W	R
No. of Digits for Single Page Files	R/W	R
Stored File E-mail Method	R/W	R



- The default for Menu Protect is [Level 2].
- Settings that are not in the list can only be viewed, regardless of the menu protect level setting.

System Settings

When administrator authentication is enabled, the administrator's configuration of Available Settings determines which system settings are available to users. If user authentication is specified, no settings are accessible to unauthorized users or authorized users before logging in.

User privileges are as follows:

- Abbreviations in the table heads
 - Not Specified = Authorized user when "Available Settings" have not been specified.
 - Specified = Authorized user when "Available Settings" have been specified.
- Abbreviations in the table columns
 - R/W (Read and Write) = Both reading and modifying the setting are available.
 - R (Read) = Reading only.
 - N/A (Not Applicable) = Neither reading nor modifying the setting is available.

General Features

Settings	Not Specified	Specified
Program / Change / Delete User Text	R/W	R
Panel Key Sound	R/W	R
Warm-up Beeper	R/W	R
Copy Count Display	R/W	R
Function Priority	R/W	R
Print Priority	R/W	R
Function Reset Timer	R/W	R
Interleave Print	R/W	R
Status Indicator	R/W	R
Screen Colour Setting	R/W	R
Output: Copier	R/W	R
Output: Document Server	R/W	R
Output: Printer	R/W	R
Paper Tray Priority: Copier	R/W	R

8

Settings	Not Specified	Specified
Paper Tray Priority: Printer	R/W	R
System Status/ Job List Display Time	R/W	R
Time Interval between Printing Jobs	R/W	R
ADF Original Table Elevation	R/W	R
ADF Feed Speed	R/W	R
Key Repeat	R/W	R
Z-fold Position	R/W	R
Output Tray Setting	R/W	R
Perfect Binding Cut Fine Adjustment	R/W	R

The "Z-fold Position" setting is available only if the Z-folding unit is installed.

The "Perfect Binding Cut Fine Adjustment" setting is available only if the perfect binder is installed.

To specify "Output Tray Setting" is available only if the stacker is installed.

Timer Settings

Settings	Not Specified	Specified
Auto Off Timer	R/W	R
Energy Saver Timer	R/W	R
Panel Off Timer	R/W	R
System Auto Reset Timer	R/W	R
Copier / Document Server Auto Reset Timer	R/W	R
Scanner Auto Reset Timer	R/W	R
Set Date	R/W	R
Set Time	R/W	R
Auto Logout Timer	R/W	R
Weekly Timer Code	R/W	R
Binding Glue Heater Auto Off Timer	R/W	R

Settings	Not Specified	Specified
Weekly Timer	R/W	R

The "Binding Glue Heater Auto Off Timer" setting is available only if the perfect binder is installed.

Interface Settings

Settings	Not Specified	Specified
Print List	R/W	N/A

Network

Settings	Not Specified	Specified
Machine IPv4 Address	R/W	R
IPv4 Gateway Address	R/W	R
IPv6 Stateless Address Autoconfiguration	R/W	R
DNS Configuration	R/W	R
DDNS Configuration	R/W	R
IPsec	R/W	R
Domain Name	R/W	R
WINS Configuration	R/W	R
Effective Protocol	R/W	R
NCP Delivery Protocol	R/W	R
NW Frame Type	R/W	R
SMB Computer Name	R/W	R
SMB Work Group	R/W	R
Ethernet Speed	R/W	R
Ping Command	R/W	R
Permit SNMPv3 Communication	R/W	R
Permit SSL / TLS Communication	R/W	R

Settings	Not Specified	Specified
Host Name	R/W	R
Machine Name	R/W	R

If you set "Machine IPv4 Address", "DNS Configuration", or "Domain Name" to "Auto-Obtain (DHCP)", you can only display the settings.

File Transfer

Settings	Not Specified	Specified
Delivery Option	R/W	R
SMTP Server	R/W	R
SMTP Authentication	R/W	R
POP before SMTP	R/W	R
Reception Protocol	R/W	R
POP3 / IMAP4 Settings	R/W	R
Administrator's E-mail Address	R/W	R
E-mail Communication Port	R/W	R
E-mail Reception Interval	R/W	R
Max. Reception E-mail Size	R/W	R
E-mail Storage in Server	R/W	R
Default User Name / Password (Send)	R/W	R
Program / Change / Delete E-mail Message	R/W	R/W
Auto Specify Sender Name	R/W	R
Scanner Resend Interval Time	R/W	R
Number of Scanner Resends	R/W	R

The settings made for "Main Delivery Server IPv4 Address" and "Sub Delivery Server IPv4 Address" in "Delivery Option" can only be displayed, not changed.

The passwords for "SMTP Authentication" and "Default User Name / Password (Send)" can be entered or changed but not displayed.

	-	
	۸	м
	۰	2
•	۸	٦
	v	ш

Settings	Not Specified	Specified
Address Book Management	R/W	R/W
Address Book: Program / Change / Delete Group	R/W	R/W
Address Book: Change Order	R/W	N/A
Print Address Book: Destination List	R/W	R/W
Address Book: Edit Title	R/W	N/A
Address Book: Switch Title	R/W	R
Back Up / Restore Address Book	R/W	N/A
Display / Print Counter	R/W	R/W
Display / Clear / Print Counter per User	R/W	N/A
User Authentication Management	R/W	R
Enhanced Authentication Management	R/W	R
Administrator Authentication Management	R/W	N/A
External Charge Unit Management	R/W	R
Enhanced External Charge Unit Management	R/W	R
Extended Security	R/W	R
Auto Delete File in Document Server	R/W	R
Delete All Files in Document Server	R/W	N/A
Program / Change / Delete LDAP Server	R/W	R
LDAP Search	R/W	R
AOF (Always On)	R/W	R
Service Test Call	R/W	N/A
Notify Machine Status	R/W	N/A
Service Mode Lock	R/W	R
Auto Erase Memory Setting	R/W	R

Settings	Not Specified	Specified
Erase All Memory	R/W	R

The password for "Program / Change / Delete LDAP Server" can be entered or changed but not displayed.

The "Auto Erase Memory Setting" and "Erase All Memory" settings are available only if the DataOverwriteSecurity unit is installed.

Maintenance

When administrator authentication is enabled, the administrator's configuration of Available Settings determines which system settings are available to users. If user authentication is specified, no settings are accessible to unauthorized users or authorized users before logging in.

User privileges are as follows:

- Abbreviations in the table heads
 - Not Specified = Authorized user when "Available Settings" have not been specified.
 - Specified = Authorized user when "Available Settings" have been specified.
- Abbreviations in the table columns
 - R/W (Read and Write) = Both reading and modifying the setting are available.
 - R (Read) = Reading only.
 - N/A (Not Applicable) = Neither reading nor modifying the setting is available.

Settings	Not Specified	Specified
Auto Colour Calibration	R/W	N/A
Colour Registration	R/W	N/A
Erase Print Image Traces	R/W	N/A

Tray Paper Settings

For details about the user privileges required for specifying the paper settings and advanced settings for various commercially-available paper types, contact your service representative.

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.

8

ŏ

Device Settings

The settings available to the user depend on whether or not administrator authentication is enabled.

If administrator authentication is enabled, the settings available to the user depend on whether or not "Available Settings" has been specified.

User privileges are as follows:

- Abbreviations in the table heads
 - Not Specified = Authorized user when "Available Settings" have not been specified.
 - Specified = Authorized user when "Available Settings" have been specified.
- Abbreviations in the table columns
 - R/W (Read and Write) = Both reading and modifying the setting are available.
 - R (Read) = Reading only.
 - N/A (Not Applicable) = Neither reading nor modifying the setting is available.

System

Settings	Not Specified	Specified
General Settings : Device Name	R/W	R
General Settings : Comment	R/W	R
General Settings : Location	R/W	R
Output Tray: Copier	R/W	R
Output Tray : Printer	R/W	R
Output Tray : Document Server	R/W	R
Paper Tray Priority : Copier	R/W	R
Paper Tray Priority : Printer	R/W	R
Front Cover Sheet Tray : Tray to set	R/W	R
Front Cover Sheet Tray : Apply Duplex	R/W	R
Front Cover Sheet Tray : Display Time	R/W	R
Back Cover Sheet Tray : Tray to set	R/W	R
Back Cover Sheet Tray : Apply Duplex	R/W	R

Settings	Not Specified	Specified
Back Cover Sheet Tray : Display Time	R/W	R
Slip Sheet Tray : Tray to set	R/W	R
Slip Sheet Tray : Display Time	R/W	R
Designation Sheet 1-9 Tray : Tray to set	R/W	R
Designation Sheet 1-9 Tray : Apply Duplex	R/W	R
Designation Sheet 1-9 Tray : Display Time	R/W	R
Separation Sheet Tray : Tray to set	R/W	R
Separation Sheet Tray : Display Time	R/W	R

Date/Time

Settings	Not Specified	Specified
Set Date	R/W	R
Set Time	R/W	R
SNTP Server Address	R/W	R
SNTP Polling Interval	R/W	R
Time Zone	R/W	R

Timer

Settings	Not Specified	Specified
Auto Off Timer	R/W	R
Energy Saver Timer	R/W	R
Panel Off Timer	R/W	R
System Auto Reset Timer	R/W	R
Copier/Document Server Auto Reset Timer	R/W	R

Settings	Not Specified	Specified
Scanner Auto Reset Timer	R/W	R
Auto Logout Timer	R/W	R
Weekly Timer Code	R/W	R
Weekly Timer	R/W	R

E-mail

Settings	Not Specified	Specified
Administrator E-mail Address	R/W	R
Reception Protocol	R/W	R
E-mail Reception Interval	R/W	R
Max. Reception E-mail Size	R/W	R
E-mail Storage in Server	R/W	R
SMTP Server Name	R/W	R
SMTP Port No.	R/W	R
SMTP Authentication	R/W	R
SMTP Auth. E-mail Address	R/W	R
SMTP Auth. User Name	R/W	N/A
SMTP Auth. Password	R/W	N/A
SMTP Auth. Encryption	R/W	R
POP before SMTP	R/W	R
POP E-mail Address	R/W	R
POP User Name	R/W	N/A
POP Password	R/W	N/A
Timeout setting after POP Auth.	R/W	R

Auto E-mail Notification

Settings	Not Specified	Specified
Groups to Notify : Address List	R/W	R/W

On-demand E-mail Notification

Settings	Not Specified	Specified
Notification Subject	R	R
Notification Message	R	R
Restriction to System Config. Info.	R	R
Restriction to Network Config. Info.	R	R
Restriction to Supply Info.	R	R
Restriction to Device Status Info.	R	R
Receivable E-mail Address/Domain Name Settings	R	R

File Transfer

Settings	Not Specified	Specified
SMB User Name	R/W	N/A
SMB Password	R/W	N/A
FTP User Name	R/W	N/A
FTP Password	R/W	N/A
NCP User Name	R/W	N/A
NCP Password	R/W	N/A

The passwords for "SMB Password", "FTP Password", and "NCP Password" can be entered or changed but not displayed.

User Authentication Management

Settings	Not Specified	Specified
User Authentication Management	R/W	R
User Code Authentication - Available Functions	R/W	R
Basic Authentication - Available Function	R/W	R
Windows Authentication - SSL	R/W	R
Windows Authentication - Domain Name	R/W	R
Windows Authentication - Group Settings for Windows Authentication	R/W	R
LDAP Authentication - LDAP Authentication	R/W	R
LDAP Authentication - Login Name Attribute	R/W	R
LDAP Authentication - Unique Attribute	R/W	R
LDAP Authentication - Available Functions	R/W	R
Integration Server Authentication - SSL	R/W	R
Integration Server Authentication - Integration Server Name	R/W	R

LDAP Server

Settings	Not Specified	Specified
LDAP Search	R/W	N/A
Program/Change/Delete	R/W	N/A



 For details about the user privileges required for specifying the paper settings and advanced settings for various commercially-available paper types, contact your service representative.

Scanner

If you have enabled administrator authentication, the menu protection setting determines which functions and settings are available.

User privileges are as follows:

• Abbreviations in the table columns

R/W (Read and Write) = Both reading and modifying the setting are available.

R (Read) = Reading only.

N/A (Not Applicable) = Neither reading nor modifying the setting is available.

When [Menu Protect] is set to [Off], all the following settings can be viewed and modified.

General Settings

Settings	Level 1	Level 2
Switch Title	R	R
Search Destination	R	R
TWAIN Standby Time	R	R
Destination List Display Priority 1	R	R
Destination List Display Priority 2	R	R
Print & Delete Scanner Journal	R	R

Scan Settings

Settings	Level 1	Level 2
A.C.S. Sensitivity Level	R	R
Wait Time for Next Original(s)	R	R
Background Density of ADS (Full Color)	R	R

Send Settings

Settings	Level 1	Level 2
Compression (Black & White)	R/W	R
Compression (Gray Scale/Full Color)	R/W	R

Default Settings for Normal Screens on Device

Settings	Level 1	Level 2
Store File	R	R
Preview	R	R
Scan Type	R	R
Resolution	R	R
Auto Density	R	R
Dropout Color	R	R
Send File Type	R	R

Default Settings for Simplified Screens on Device

Settings	Level 1	Level 2
Scan Type	R	R
Resolution	R	R
Send File Type	R	R



- The default for Menu Protect is [Level 2].
- Settings that are not in the list can only be viewed, regardless of the menu protect level setting.

Network

The settings available to the user depend on whether or not administrator authentication is enabled.

If administrator authentication is enabled, the settings available to the user depend on whether or not "Available Settings" has been specified.

User privileges are as follows:

- Abbreviations in the table heads
 - Not Specified = Authorized user when "Available Settings" have not been specified.
 - Specified = Authorized user when "Available Settings" have been specified.
- Abbreviations in the table columns
 - R/W (Read and Write) = Both reading and modifying the setting are available.
 - R (Read) = Reading only.
 - N/A (Not Applicable) = Neither reading nor modifying the setting is available.

IPv4

Settings	Not Specified	Specified
Host Name	R/W	R
DHCP	R/W	R
Domain Name	R/W	R
IPv4 Address	R/W	R
Subnet Mask	R/W	R
DDNS	R/W	R
WINS	R/W	R
Primary WINS Server	R/W	R
Secondary WINS Server	R/W	R
Scope ID	R/W	R
Default Gateway Address	R/W	R
DNS Server	R/W	R
RSH/RCP	R/W	R

Settings	Not Specified	Specified
FTP	R/W	R
sftp	R/W	R

IPv6

Settings	Not Specified	Specified
IPv6	R/W	R
Host Name	R/W	R
Domain Name	R/W	R
Stateless Address	R/W	R
Manual Configuration Address	R/W	R
DHCPv6-lite	R/W	R
DDNS	R/W	R
Default Gateway Address	R/W	R
DNS Server	R/W	R
RSH/RCP	R/W	R
FTP	R/W	R
sftp	R/W	R

NetWare

Settings	Not Specified	Specified
NetWare	R/W	R
Logon Mode	R/W	R
File Server Name	R/W	R
NDS Tree	R/W	N/A

Settings	Not Specified	Specified
Frame Type	R/W	R
NCP Delivery Protocol	R/W	R

SMB

Settings	Not Specified	Specified
SMB	R/W	R
Workgroup Name	R/W	R
Computer Name	R/W	R
Comment	R/W	R
Notify Print Completion	R/W	R

Webpage

The settings available to the user depend on whether or not administrator authentication is enabled.

If administrator authentication is enabled, the settings available to the user depend on whether or not "Available Settings" has been specified.

User privileges are as follows:

• Abbreviations in the table heads

Not Specified = Authorized user when "Available Settings" have not been specified.

Specified = Authorized user when "Available Settings" have been specified.

• Abbreviations in the table columns

R/W (Read and Write) = Both reading and modifying the setting are available.

R (Read) = Reading only.

N/A (Not Applicable) = Neither reading nor modifying the setting is available.

Webpage

Settings	Not Specified	Specified
Webpage Language	R/W	R
Set URL Target of Link Page	R/W	R
Set Help URL Target	R/W	R
UPnP Setting	R/W	R
Download Help File	R/W	R/W

8

5

Functions That Require Options

The following functions require certain options and additional functions.

Hard Disk overwrite erase function
 DataOverwriteSecurity unit

Trademarks

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

Mac OS X is a trademarks of Apple Inc., registered in the U.S. and other countries.

Lotus Notes[®] is a trademarks of International Business Machines Corporation in the United States, other countries, or both.

Linux[®] is the registered trademark of Linus Torvalds in the U.S. and other countries.

Microsoft[®], Windows[®], Windows Server[®], and Windows Vista[®], and Outlook[®] are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

RED HAT is a registered trademark of Red Hat, Inc.

Solaris is a trademark or registered trademark of Sun Microsystems, Inc. in the United States and other countries.

UPnPTM is a trademark of the UPnPTM Implementers Corporation.

NetWare and NDS are registered trademarks of Novell, Inc.

Other product names used herein are for identification purposes only and might be trademarks of their respective companies. We disclaim any and all rights to those marks.

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

• The product names of Windows 2000 are as follows:

Microsoft® Windows® 2000 Professional

Microsoft® Windows® 2000 Server

Microsoft® Windows® 2000 Advanced Server

• The product names of Windows XP are as follows:

Microsoft® Windows® XP Professional

Microsoft® Windows® XP Home Edition

Microsoft® Windows® XP Media Center Edition

Microsoft® Windows® XP Tablet PC Edition

• The product names of Windows Vista are as follows:

Microsoft® Windows Vista® Ultimate

Microsoft® Windows Vista® Enterprise

Microsoft® Windows Vista® Business

Microsoft® Windows Vista® Home Premium

Microsoft® Windows Vista® Home Basic

• The product names of Windows 7 are as follows:

Q

Microsoft® Windows® 7 Starter

Microsoft® Windows® 7 Home Premium

Microsoft® Windows® 7 Professional

Microsoft® Windows® 7 Ultimate

• The product names of Windows Server 2003 are as follows:

Microsoft® Windows Server® 2003 Standard Edition

Microsoft® Windows Server® 2003 Enterprise Edition

• The product names of Windows Server 2003 R2 are as follows:

Microsoft® Windows Server® 2003 R2 Standard Edition

Microsoft® Windows Server® 2003 R2 Enterprise Edition

• The product names of Windows Server 2008 are as follows:

Microsoft® Windows Server® 2008 Standard

Microsoft® Windows Server® 2008 Enterprise

• The product names of Windows Server 2008 R2 are as follows:

Microsoft® Windows Server® 2008 R2 Standard

Microsoft® Windows Server® 2008 R2 Enterprise

R

INDEX

Α	Encryption Key Auto Exchange Settings138
Access Control115	Encryption Key Manual Settings138, 144, 151
Access Permission71	Encryption Technology16
Address Book Access Permission94	Enhance File Protection82, 163
Address Book Privileges213	Erase All Memory102, 103
Administrator17	Error Code173
Administrator Authentication17, 26, 31	Error Message171
Administrator Privileges31	ESP Protocol136
AH Protocol137	Extended Security84, 95, 125, 161
Authenticate Current Job163	
Authentication and Access Limits16	F
Authentication Information46	File Administrator24, 212
Authentication Using an External Device69	File Administrator Settings208
Auto Erase Memory98, 99, 101	File Creator17, 74
Auto Logout66	Full Control212, 213
Available Functions112	Functions That Require Options247
В	1
Basic Authentication	Important
Before Using the Security Functions11	Installing the Device Certificate91, 130
C	Integration Server Authentication60
	IP Address9
Certificate Authority90, 91, 129, 130	IPsec136
Control Panel Settings216	IPsec Settings138
Copier / Document Server Features199, 217	IPsec telnet Setting Commands152
Creating the Device Certificate90, 129	L
D	LDAP Authentication55
Deleting Data on the Hard Disk98	LDAP Authentication - Operational Requirements
Device Settings235	for LDAP Authentication55
Document Server File Permissions212	Login17
Driver Encryption Key125, 162	Login (Administrator)36
E	Login (Supervisor)193
	Login (User)64, 65
E-mail Encryption86	Login (Web Image Monitor)66
Edit212, 213	Login Password43
Edit / Delete212, 213	Login User Name43
Electronic Signature88	Logout18
Enabling Authentication29	Logout (Administrator)37
Enabling/Disabling Protocols116	Logout (Supervisor)194
Encrypt Address Book95, 162	Logout (User)66
Encryption Key Auto Exchange Security Level	Logout (Web Image Monitor)66

IN
Machine Administrator24
Machine Administrator Settings197
Maintenance199, 232
Manuals for This Machine
Menu Protect107, 109
Methods of Overwriting99
N
Names of Major Items9
Network243
Network Administrator24
Network Administrator Settings204
Network Security Level121
Notes10
0
Operational Issues188
Operational Requirements for Windows Authentication48
Other Security Functions
Overwrite Icon
Owner17, 74, 212
P
Password for Stored Files71
Password Policy164
Print & Delete Scanner Journal165
R
Read-only212, 213
Registered User17, 213
Registering the Administrator33
Remote Service164
Restrict Adding of User Destinations84, 162
Restrict Display of User Information162
Restrict Use of Destinations84, 162
Restrict Use of Simple Encryption163
S
S/MIME86
Scanner241
Scanner Features200, 205, 224
Scanner Function165

Security Measures Provided by this Machine19
Self-Signed Certificate89, 128
Service Mode Lock168
Setting Up the Machine12
Settings by SNMPv1 and v2163
SNMPv3 Encryption134
SSL (Secure Sockets Layer)127, 13
SSL/TLS Encryption Mode132, 133
Supervisor17, 24, 193
Suspending Erase All Memory105
Symbols
System Settings197, 204, 208, 210, 226
System Status165
,
Г
Transmitted Passwords125
Tray Paper Settings200, 233
Type of Administrator107
Types of Data that Can or Cannot Be Overwritten
102
U
User17, 24
User Administrator23, 213
User Administrator Settings210
User Authentication17, 27, 39, 64
User Certificate87
User Code Authentication40
User Settings216, 234
W
000
Web Image Monitor Settings234
Webpage24d
Weekly Timer Code165, 167 Windows Authentication48



