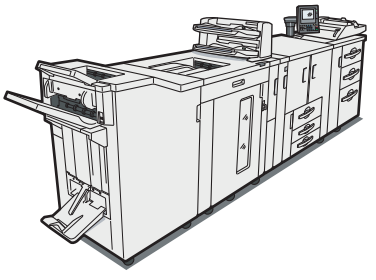
Pro 907
Pro 1107
Pro 1357

Operating Instructions

Security Reference



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

TABLE OF CONTENTS

3. Configuring User Authentication

4. Securing Information Stored on Hard Disk

5. Managing Access to the Machine

6. Enhanced Network Security

7. Specifying the Extended Security Functions

8. Troubleshooting

9. Appendix

Manuals for This Machine

Read this manual carefully before you use this printer.

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

Important

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

About This Machine

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

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

Troubleshooting

Provides a guide for resolving common usage-related problems.

Printer Reference

Explains Printer functions and operations.

Network and System Settings Guide

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

Security Reference

This manual is for administrators of the printer. It explains security functions that you can use to prevent unauthorized use of the printer, data tampering, or information leakage. Be sure to read this manual when setting the enhanced security functions, or user and administrator authentication.

Other manual

- Quick Reference Printer Guide

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 print quality, the supplier recommends that you use genuine toner from the supplier.

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

How to Read This Manual

Symbols

This manual uses the following symbols:

Important

Indicates points to pay attention to when using the printer, and explanations of likely causes of paper misfeeds, damage to originals, or loss of data. Be sure to read these explanations.

Note

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

Reference

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

[ ]

Indicates the names of keys that appear on the printer's display panel.

[ ]

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

About IP Address

- In this manual, "IP address" covers both IPv4 and IPv6 environments. Read the instructions that are relevant to the environment you are using.
- Two IP addresses must be specified on this printer. For the IP address referred to as "system's IP address" in this manual, enter the IP address that was specified in the System Settings menu. For "printer's IP address", enter the IP address specified in the Printer Features menu.

Note

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

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

Certain options might not be available in some countries. For details, please contact your local dealer.

Depending on which country you are in, certain units may be optional. For details, please contact your local dealer.

Laws and Regulations

Legal Prohibition

Do not copy or print any item for which reproduction is prohibited by law.

Copying or printing the following items is generally prohibited by local law:

bank notes, revenue stamps, bonds, stock certificates, bank drafts, checks, passports, driver's licenses.

The preceding list is meant as a guide only and is not inclusive. We assume no responsibility for its completeness or accuracy. If you have any questions concerning the legality of copying or printing certain items, consult with your legal advisor.

1. Getting Started

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

Before Using the Security Functions

This printer has two separate network interfaces, which can be configured under System Settings and Printer Features. To enhance the security for both networks and so ensure safer network communication, configure the settings of both interfaces.

System Network

The system network allows system-level communication (such as specification of device-related settings) to be made over the network through the system interface. Specify the system network security settings using System Settings on the control panel or via Web Image Monitor. For details about connecting this printer to a network through the system interface, see "Connecting to the System Interface", Network and System Settings Guide.

Printing Network

The printing network allows print-level communication (such as specification of printer function-related settings) to be made over the network through the printer interface. Specify the printing network security settings using Printer Features on the control panel or via Web Interface. For details about connecting this printer to a network through the printer interface, see "Connecting to the Printer Interface", Network and System Settings Guide.

Important

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

1. To prevent this printer being stolen or willfully damaged, etc., install it in a secure location.
2. Purchasers of this printer must make sure that people who use it do so appropriately, in accordance with operations determined by the printer 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 printer'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 printer's logs to check for irregular and unusual events.
6. If this printer 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 printer's communication security functions and connect it to devices that support security functions such as encrypted communication.
8. Security information is included on the printer's hard drive. If the hard drive fails and is replaced, be sure to reconfigure the following security settings:

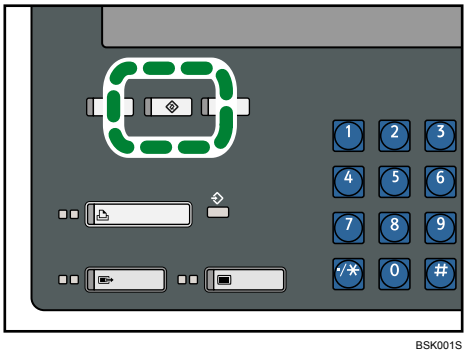
- Certificate Status of SSL/TLS in Printer Settings under Printer Features

- Imported Site Certificate in Site Certificate under Printer Features

Setting Up the Machine

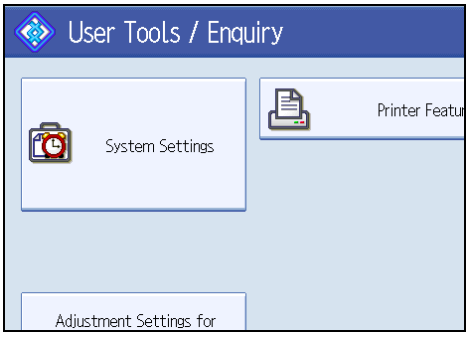
This section explains how to enable encryption of transmitted data, how to register the administrator, and how to specify the password for logging on to Printer Features. If you want higher security, make the following setting before using the printer.

1. **Turn the printer on.**
2. **Press the [User Tools] key.**

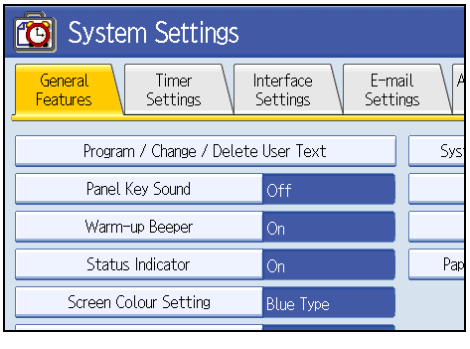


BSK001S

3. **Press [System Settings].**



4. **Press [Interface Settings].**

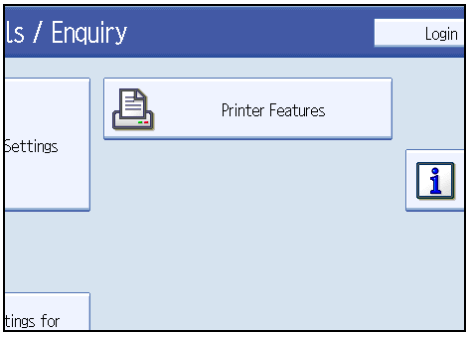


1

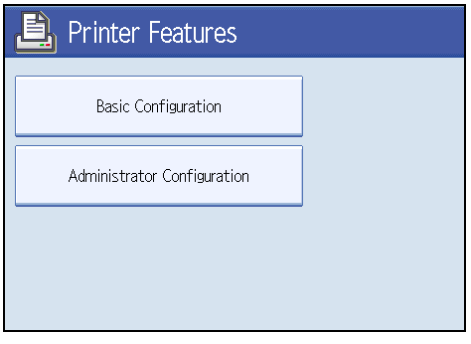
5. **Specify the required IPv4 address for the system network.**

   For details about how to specify the system's IPv4 address, see "System Settings", Network and System Settings Guide.

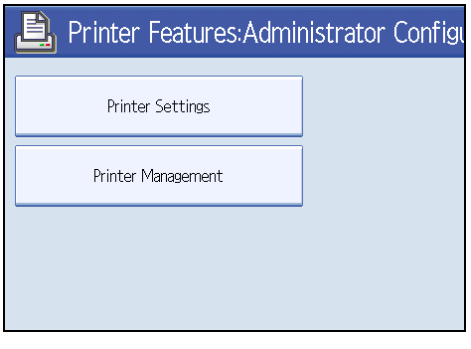
6. **Press [Printer Features].**



7. **Press [Administrator Configuration].**

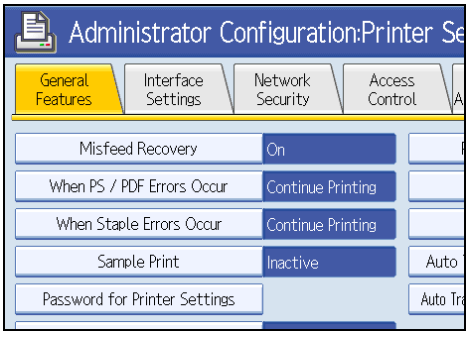


8. **Press [Printer Settings].**



   If you are logging on to Printer Features for the first time, enter the default password for printer settings. The default password is "1000".

9. **Press [Interface Settings].**



10. **Specify the required IPv4 address for the printing network.**

    For details on how to specify the printer's IPv4 address, see "Printer Settings", Network and System Settings Guide.

11. **Connect the printer to the network.**

    For details about connecting the printer to a network through the system interface and printer interface, see "Connecting to the Interfaces", Network and System Settings Guide.

12. **Start Web Image Monitor, and then log on to the printer as the administrator.**

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

13. **Install the device certificate for the system network.**

    For details about how to install the device certificate, see "Specifying SSL for the System Network".

14. **Enable secure sockets layer (SSL) for the system network.**

    For details about enabling SSL, see "Specifying SSL for the System Network".

15. **Using Web Image Monitor, change the administrator's user name and password.**

    For details about specifying the administrator user name and password, see "Registering the Administrator".

    The administrator's default account (user name: "admin"; password: blank) is unencrypted between steps 6 to 9. If acquired during this time, this account information could be used to gain unauthorized access to the printer over the network.

    If you consider this risky, we recommend that you specify a temporary administrator password for accessing Web Image Monitor for the first time, before connecting to the network in step 6.

    We recommend you change the supervisor's password also. For details about changing the supervisor's user name and password, see "Changing the Supervisor".

16. **Start Web Interface, and then log on.**

    For details about logging on to Web Interface, see "Using Web Interface to Access the Machine".

17. **Install the required device certificate for the printing network.**

    For details about how to install the device certificate, see "Protection Using Encryption".

18. Enable SSL for the printing network.

For details about enabling SSL, see "Specifying SSL for the Printing Network".

19. Using Web Interface, change the password for printer settings.

The default password for printer settings is sent in plaintext format in step 11 and between steps 16 and 18. If the password is intercepted at this point, it could be used to gain unauthorized network access to the printer. Take the following precautionary measure if this is an unacceptable risk:

- Before you connect the printer to the network (step 11), specify a temporary password for first-use access to Web Interface.

For details about specifying the password, see "Changing the Password for Printer Settings".

Reference

- p.35 "Using Web Image Monitor to Configure Administrator Authentication"
- p.129 "Specifying SSL for the System Network"
- p.30 "Registering the Administrator"
- p.206 "Changing the Supervisor"
- p.39 "Using Web Interface to Access the Machine"
- p.133 "Specifying SSL for the Printing Network"
- p.36 "Changing the Password for Printer Settings"

Enhanced Security

This printer's security functions can be enhanced by managing the printer and its users using the improved authentication functions.

By specifying access limits for the printer's functions and the documents and data stored in the printer, information leaks and unauthorized access can be prevented.

Data encryption also prevents unauthorized data access and tampering via the network.

The printer also automatically checks the configuration and supplier of the firmware each time the main power is switched on and whenever firmware is installed.

Authentication and Access Limits

Using authentication, administrators manage the printer 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 printer usage, such as settings and user registration.

Access limits for each user are specified by the administrator responsible for user access to printer's functions.

For details about the administrator, see "Administrators".

For details about the user, see "Users".

Encryption Technology

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

Note

- To manage Printer Features, a login password in addition to the administrator's account is required. For details about managing Printer Features, see "Managing Printer Features Settings".

Reference

- p.23 "Administrators"
- p.41 "Users"
- p.36 "Managing Printer Features Settings"

Glossary

Administrator

There are four types of administrators according to administrative function: machine administrator, network administrator, file administrator, and user administrator. We recommend a different person for each administrator role.

In this way, you can spread the workload and limit unauthorized operation by a single administrator.

Basically, administrators make printer settings and manage the printer; but they cannot perform normal operations.

User

A user performs normal operations on the printer.

Registered User

Users with personal information registered in the Address Book who have a login password and user name.

Administrator Authentication

Administrators are authenticated by their login user name and login password, supplied by the administrator, when specifying the printer's settings or accessing the printer over the network.

User Authentication

Users are authenticated by a login user name and login password, supplied by the user, when specifying the printer's settings or accessing the printer over the network.

The user's login user name and password are stored in the printer'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 printer 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 printer's control panel. A login user name and login password may also be required when accessing the printer over the network or using such utilities as Web Image Monitor.

Logout

This action is required with administrator and user authentication. This action is required when you have finished using the printer 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 printer, perform administrator authentication and user authentication using login user names and login passwords. To perform authentication, the authentication function must be enabled. For details about authentication settings, see "Configuring User Authentication".

Specifying 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.43 "Configuring User Authentication"
- p.93 "Limiting Available Functions"

Ensuring Information Security

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 from being used by unregistered users.

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

Managing Log Files

The logs record failed access attempts and the names of users who accessed the printer successfully. You can use this information to help prevent data leaks.

For details about managing log files, see "Managing Log Files".

Overwriting the Data on the Hard Disk

To prevent data leaks, we recommend that before disposing of the printer, you overwrite all the data on the hard disk.

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

1

Reference

- p.81 "Protecting the Address Book"
- p.94 "Managing Log Files"
- p.85 "Deleting Data on the Hard Disk"

Limiting and Controlling Access

Preventing Modification of Printer Settings

The printer 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 printer settings, see "Preventing Changes to Machine Settings".

Limiting Available Functions

To prevent unauthorized operation, you can specify who is allowed to access the printer functions. For details about limiting available functions for users and groups, see "Limiting Available Functions".

Reference

- p.89 "Preventing Changes to Machine Settings"
- p.93 "Limiting Available Functions"

Enhancing Network Security

Preventing Unauthorized Access

You can limit IP addresses or disable ports to prevent unauthorized access over the network and protect the Address Book, and default settings. For details about preventing unauthorized access, see "Preventing Unauthorized Access".

Encrypting Transmitted Passwords

Prevent login passwords, and IPP authentication passwords from being revealed by encrypting them for transmission.

Also, encrypt the login password for administrator authentication and user authentication. For details about encrypting transmitted passwords, see "Encrypting Transmitted Passwords".

Safer Communication Using SSL, SNMPv3 and IPsec

You can encrypt this printer'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.109 "Preventing Unauthorized Access"
- p.124 "Encrypting Transmitted Passwords"
- p.127 "Protection Using Encryption"
- p.141 "Transmission Using IPsec"

2. Configuring Administrator Authentication

This chapter describes what an administrator can do, how to register an administrator, how to specify administrator authentication, and how to log on to and off from the printer as an administrator.

Administrators

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

When an administrator controls limited access and settings, first select the printer's administrator and enable the authentication function before using the printer. When the authentication function is enabled, the login user name and login password are required in order to use the printer. There are four types of administrators: machine administrator, network administrator, file administrator and user administrator. Sharing administrator tasks eases the burden on individual administrators while also limiting unauthorized operation by administrators. One person can act as more than one type of administrator. You can also specify a supervisor who can change each administrator's password. Administrators cannot use functions such as printing. To use these functions, the administrator must be authenticated as the user.

For instructions on registering the administrator, see "Registering the Administrator", and for instructions on changing the administrator's password, see "Supervisor Operations". For details on Users, see "Users".

Important

- **If user authentication is not possible because of a problem with the hard disk or network, you can use the printer by accessing it using administrator authentication and disabling user authentication. Do this if, for instance, you need to use the printer urgently.**
- **To manage Printer Features, a login password in addition to the administrator's account is required. Select one of the users as the Printer Features administrator. The selected administrator must specify the login password. For details about managing Printer Features, see "Managing Printer Features Settings".**

Reference

- p.30 "Registering the Administrator"
- p.205 "Supervisor Operations"
- p.41 "Users"
- p.36 "Managing Printer Features Settings"

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 printer again.

Machine Administrator

This is the administrator who mainly manages the printer's default settings. You can configure the printer to allow only the machine administrator to specify system settings and paper settings. By making this setting, you can prevent unauthorized people from changing the settings and allow the printer to be used securely by its many users.

Network Administrator

This is the administrator who manages the network settings. You can set the printer so that network settings such as the system's 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 printer, and thus ensure correct network operation.

Note

- To specify the network settings for printing, the password for printer settings in addition to the administrator's account is required at login.

File Administrator

You can specify Auto E-mail Notification. If you do, alert messages are sent to the registered e-mail addresses when paper jams occur or the print cartridge runs out of toner. Both the user administrator and machine administrator can specify Auto E-mail Notification.

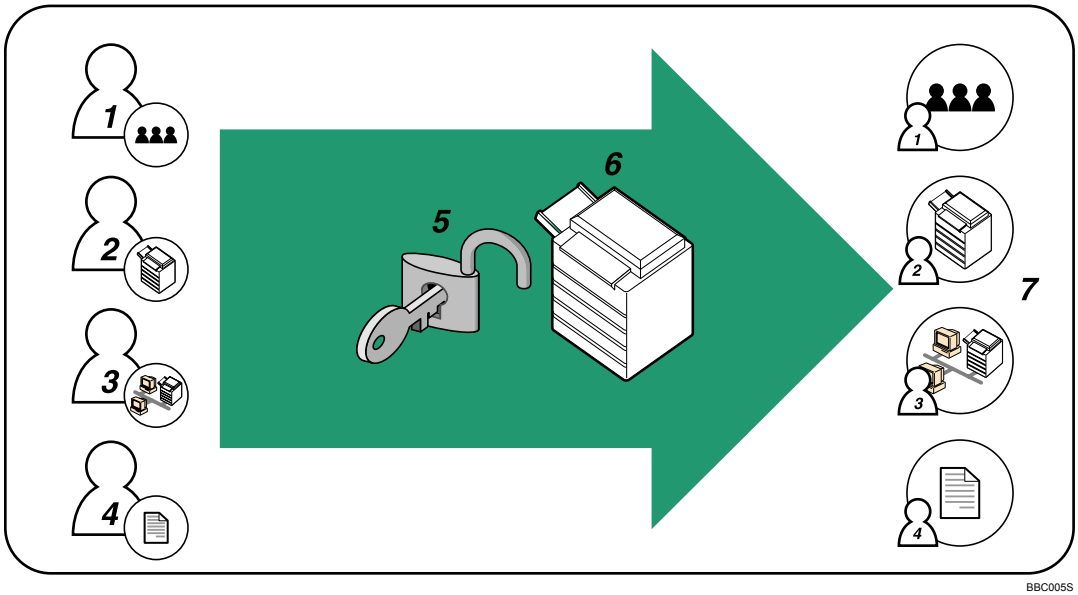
Supervisor

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 printer, the supervisor can provide support.

About Administrator Authentication

There are four types of administrators: user administrator, machine administrator, network administrator, and file administrator. For details about each administrator, see "Administrators".

To manage Printer Features, a login password in addition to the administrator's account is required. For details about managing Printer Features, see "Managing Printer Features Settings".



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 printer's default settings. You can configure the printer to allow only the machine administrator to specify system settings and paper settings.

3. **Network Administrator**

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

   To specify the network settings for printing, the password for printer settings in addition to the administrator's account is required.

4. **File Administrator**

   You can specify Auto E-mail Notification. If you do, alert messages are sent to the registered e-mail addresses when paper jams occur or the print cartridge runs out of toner. Both the user administrator and machine administrator can specify Auto E-mail Notification.

5. **Authentication**

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

6. **This printer**

7. **Administrators manage the printer's settings and access limits.**

Reference

- p.23 "Administrators"
- p.36 "Managing Printer Features Settings"

Enabling Administrator Authentication

To control administrators' access to the printer, perform administrator authentication using login user names and passwords. When registering an administrator, you cannot use a login user name already registered in the Address Book. Administrators are handled differently from the users registered in the Address Book. Windows Authentication, LDAP Authentication and Integration Server Authentication are not performed for an administrator, so an administrator can log on even if the server is unreachable due to a network problem. Each administrator is identified by a login user name. One person can act as more than one type of administrator if multiple administrator authorities are granted to a single login user name. For instructions on registering the administrator, see "Registering the Administrator".

You can specify the login user name, login password, and encryption password for each administrator. The encryption password is a password for performing encryption when specifying settings using Web Image Monitor. The password registered in the printer must be entered when using applications such as Web Image Monitor. Administrators are limited to managing the printer's settings and controlling user access, so they cannot use functions such as printing. To use these functions, the administrator must register as a user in the Address Book and then be authenticated as the user. Specify administrator authentication, and then specify user authentication. For details about specifying authentication, see "Configuring User Authentication".

Note

- Administrator authentication can also be specified via Web Image Monitor. For details see Web Image Monitor Help.
- You can specify User Code Authentication without specifying administrator authentication.

Reference

- p.30 "Registering the Administrator"
- p.43 "Configuring User Authentication"

Specifying Administrator Privileges

To specify administrator authentication, set Administrator Authentication Management to [On]. In addition, if enabled in the settings, you can choose how the initial settings are divided among the administrators as controlled items.

To log on as an administrator, use the default login user name and login password.

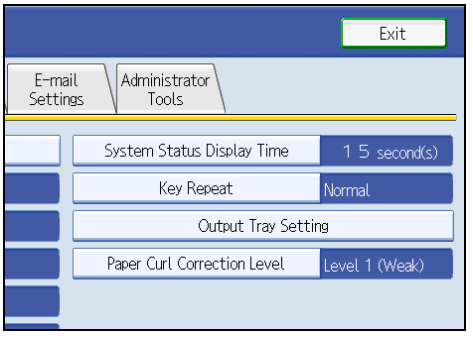
The default login user name is "admin", but there is no default password. For details about changing the administrator password using the supervisor's authority, see "Supervisor Operations".

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

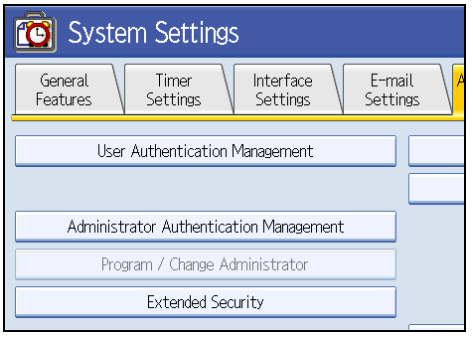
Important

- If you have enabled "Administrator Authentication Management", make sure not to forget the administrator login user name and login password. If an administrator login user name or login password is forgotten, a new password must be specified using the supervisor's authority. For instructions on registering the supervisor, see "Supervisor Operations".
- Be sure not to forget the supervisor login user name and login password. If you do forget them, a service representative will have to return the printer to its default state. This will result in all data in the printer being lost. Charges may also apply to the service call.

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

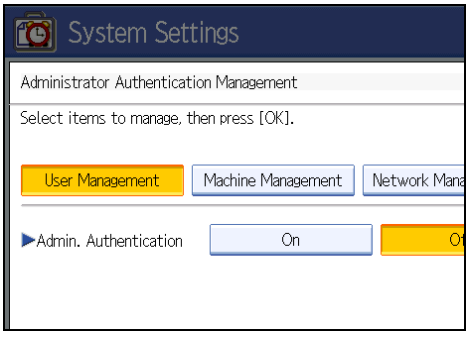


4. Press [Administrator Authentication Management].

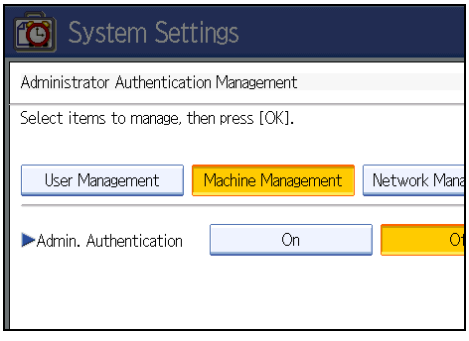


If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

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

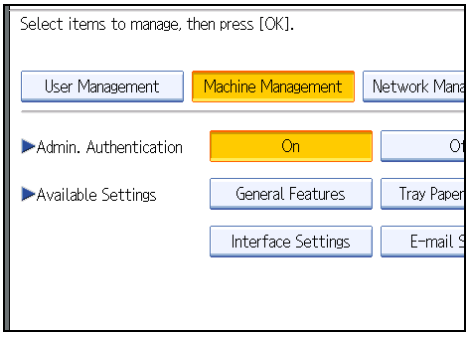


6. **Set "Admin. Authentication" to [On].**



"Available Settings" appears.

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



The selected settings will be unavailable to users.

"Available Settings" varies depending on the administrator.

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

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

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

Reference

- p.205 "Supervisor Operations"
- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"
- p.93 "Limiting Available Functions"

2

Registering the Administrator

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

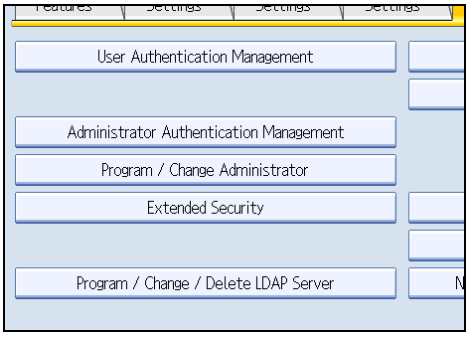
The sharing of administrator tasks eases the burden on individual administrators while also limiting unauthorized operation by a single administrator. You can register up to four login user names (Administrators 1-4) to which you can grant administrator privileges.

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

If administrator authentication has already been specified, log on using a registered administrator name and password.

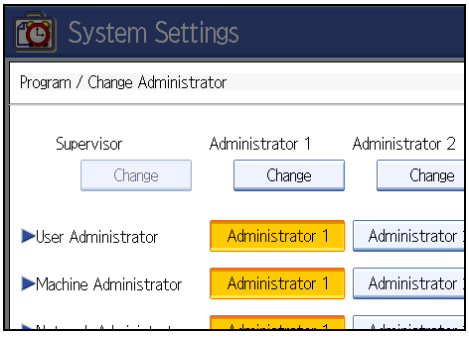
For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

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

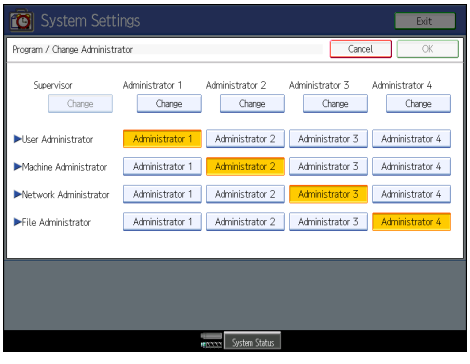


If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

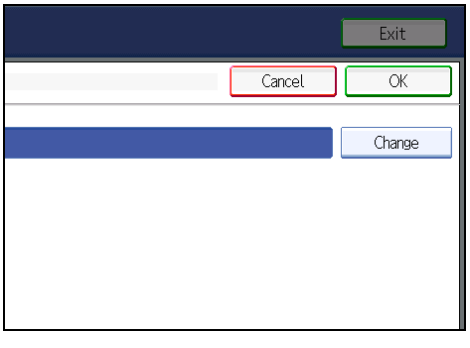
5. **In the line for the administrator whose authority you want to specify, press [Administrator 1], [Administrator 2], [Administrator 3] or [Administrator 4], and then press [Change].**



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

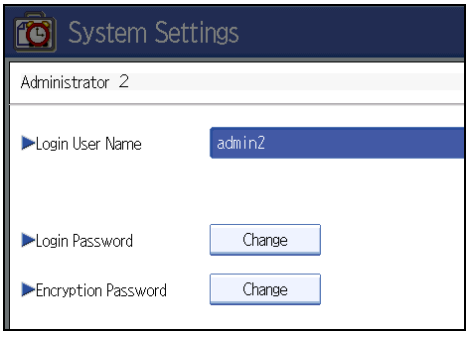


6. **Press [Change] for the login user name.**



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

8. **Press [Change] for the login password.**



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

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

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

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

    You will be automatically logged off.

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

Note

- You can use up to 32 alphanumeric characters and symbols when registering login user names and login passwords. Keep in mind that passwords are case-sensitive.
- User names cannot contain numbers only, a space, colon (:), or quotation mark ("), nor can they be left blank.
- Do not use Japanese, Traditional Chinese, Simplified Chinese, or Hangul double-byte characters when entering the login user name or password. If you use multi-byte characters when entering the login user name or password, you cannot authenticate using Web Image Monitor.

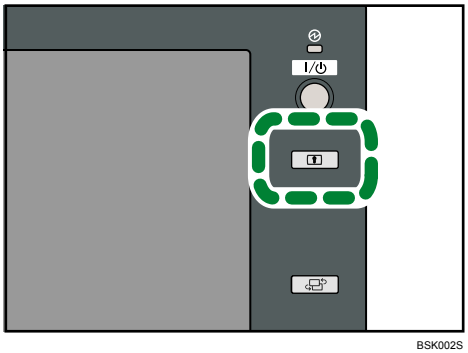
Reference

- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"
- p.173 "Specifying the Extended Security Functions"

Logging on Using Administrator Authentication

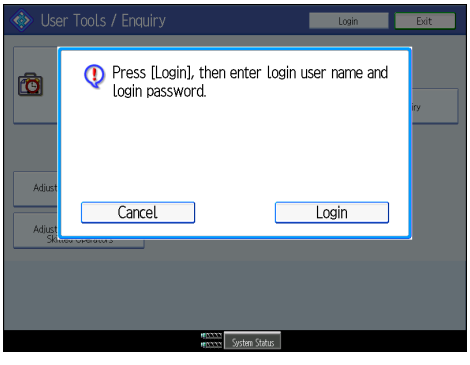
If administrator authentication has been specified, log on using an administrator's user name and password. This section describes how to log on. When you log on with a user name that has multiple administrator privileges, one of the administrator privileges associated with that name is displayed.

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



BSK002S

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



3. **Press [Login].**

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

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

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

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

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

Note

- If user authentication has already been specified, a screen for authentication appears.
- To log on as an administrator, enter the administrator's login user name and login password.

- If you log on using administrator authority, the name of the administrator logging on appears.
- If you log on using a login user name with the authority of more than one administrator, "Administrator" appears.

Logging off Using Administrator Authentication

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

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

Changing the Administrator

Change the administrator's login user name and login password. You can also assign administrator authority to the login user names [Administrator 1] to [Administrator 4]. To combine the authorities of multiple administrators, assign multiple administrators to a single administrator.

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

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

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

   If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.
5. **In the line for the administrator you want to change, press [Administrator 1], [Administrator 2], [Administrator 3] or [Administrator 4], and then press [Change].**
6. **Press [Change] for the setting you want to change, and re-enter the setting.**
7. **Press [OK].**
8. **Press [OK] twice.**

   You will be automatically logged off.
9. **Press the [User Tools] key.**

Reference

- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"

Using Web Image Monitor to Configure Administrator Authentication

Using Web Image Monitor, you can log on to the printer 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. For details about connecting this printer to a network through the system interface, see "Connecting to the Printer Interface", Network and System Settings Guide.

1. **Open a Web browser.**
2. **Enter "http://(system'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 printer.

   The top page of Web Image Monitor appears.
3. **Click [Login].**
4. **Enter the login name and password of an administrator, and then click [Login].**
5. **Make settings as desired.**

Note

- When logging on as an administrator use the login name and password of an administrator set in the printer. The default login user name is "admin", but there is no default password.

Managing Printer Features Settings

Using the password for printer settings, the Printer Features administrator can manage the Administrator Configuration menu in Printer Features.

Important

- You cannot log on to Printer Features using the login password registered in System Settings for the user administrator, machine administrator, network administrator, or file administrator. Only the Printer Features administrator may log on using the password for printer settings.
- If you set the password to "0", protection by login password is disabled, and even users who do not know the password will be able to configure any Printer Features setting.
- The default password for printer settings is "1000".
- The "Printer Management" menu in "Administrator Configuration" is for use by service engineers only, not general users.
- Every time [Printer Settings] is pressed, a message prompting you to enter a password will appear.

Password for Printer Settings

This password is for the Printer Features administrator's use only.

This password protects the settings under "Printer Settings" in "Administrator Configuration". To configure the printer function settings, such as the network and security settings required for printing, you must enter this password at login.

Changing the Password for Printer Settings

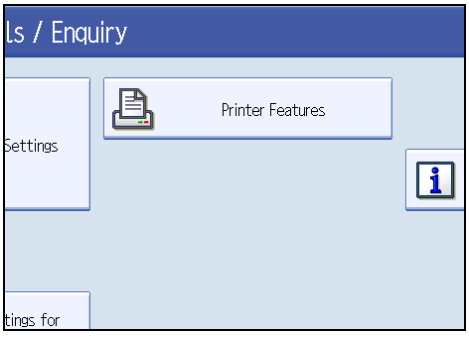
Use the following procedure to change the password for printer settings.

Important

- Be sure to remember the password for printer settings. If you forget it, contact your service representative.

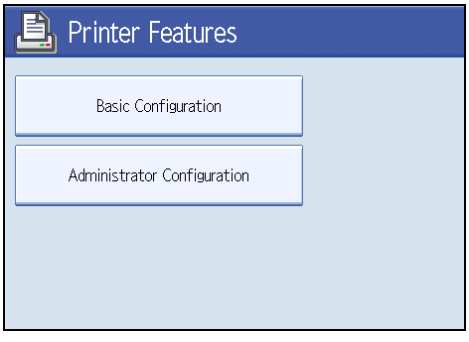
1. Press the [User Tools] key.

2. **Press [Printer Features].**

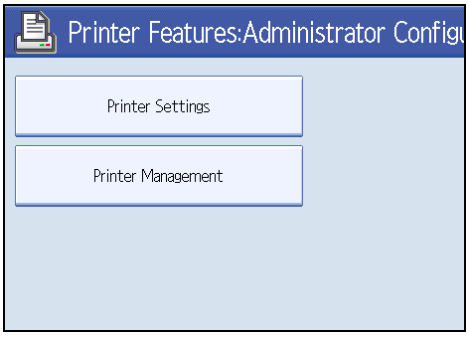


If user authentication is in operation, an authentication message will appear. To log on, enter the login user name and password.

3. **Press [Administrator Configuration].**

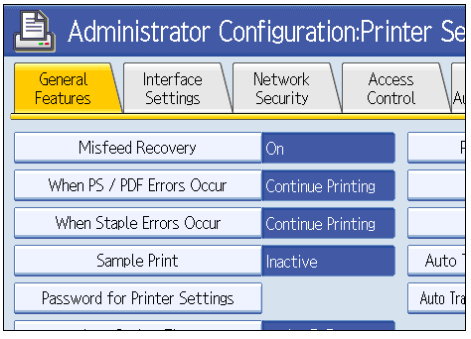


4. **Press [Printer Settings].**

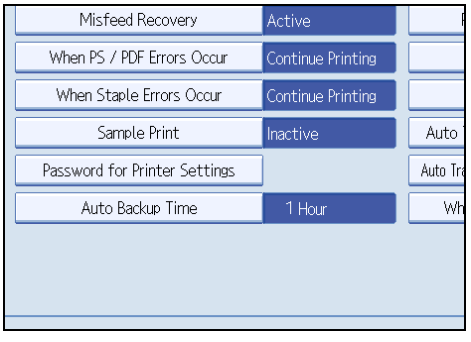


A message requesting you to enter the password appears. If you are logging on for the first time, enter the default password for printer settings. The default password is "1000".

5. **Press [General Features].**



6. **Press [Password for Printer Settings].**



7. **Enter the password using the number keys, and then press [OK].**
8. **If a message requesting you to re-enter the password appears, enter the password, and then press [OK].**
9. **Press the [User Tools] key.**

Using Web Interface to Specify the Password for Printer Settings

You can use Web Interface to specify the password for printer settings. For details about Web Interface, see the Web Interface help. For details about connecting this printer to a network through the printer interface, see "Connecting to the Printer Interface", Network and System Settings Guide.

Important

- **Be sure to remember the password for printer settings. If you forget it, contact your service representative.**

1. **Open a Web browser.**
2. **Enter "http://(printer'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 printer.

The top page of Web Interface appears.

3. **Click [Configurations/Jobs].**

   An authentication dialog box appears.

4. **Enter the login user name and password, and then click [OK].**

   Enter "system" as the login user name and enter the password for printer settings as the login password.

5. **Click [Printer Settings], and then click [Password for Printer Settings] under "Security".**

6. **Enter the current and the new password, and then click [OK].**

7. **Close the Web browser.**

   You will be logged off.

Using Web Interface to Access the Machine

You can access Web Interface by opening your Web browser and entering the IP address registered in Printer Features.

If you click a setting that requires the password for printer settings, a dialog box requesting you to enter the login user name and password will appear. Users who do not know the password cannot use Web Interface to change the printer's settings.

For details about the settings that can be specified with the password, see "Settings that can be Specified by Logging on with the Password for Printer Settings".

Note

- You cannot change the login user name "system" in the Web Interface login dialog box.
- The "Logs" menus is for use by service engineers only, not general users.

Reference

- p.222 "Settings that can be Specified by Logging on with the Password for Printer Settings"

3. Configuring User Authentication

This chapter describes what a user can do, how to specify user authentication, and how to log onto and off from the printer as a user.

Users

A user performs normal operations on the printer, such as printing. Users are managed using the personal information in the printer's Address Book, and can use only the functions they are permitted to access by administrators. By enabling user authentication, you can allow only people registered in the Address Book to use the printer. Users can be managed in the Address Book by the user administrator. For details about administrator, see "Administrators". For details about registering users in the Address Book, see "Administrator Tools", Network and System Settings Guide, or Web Image Monitor Help.

Important

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

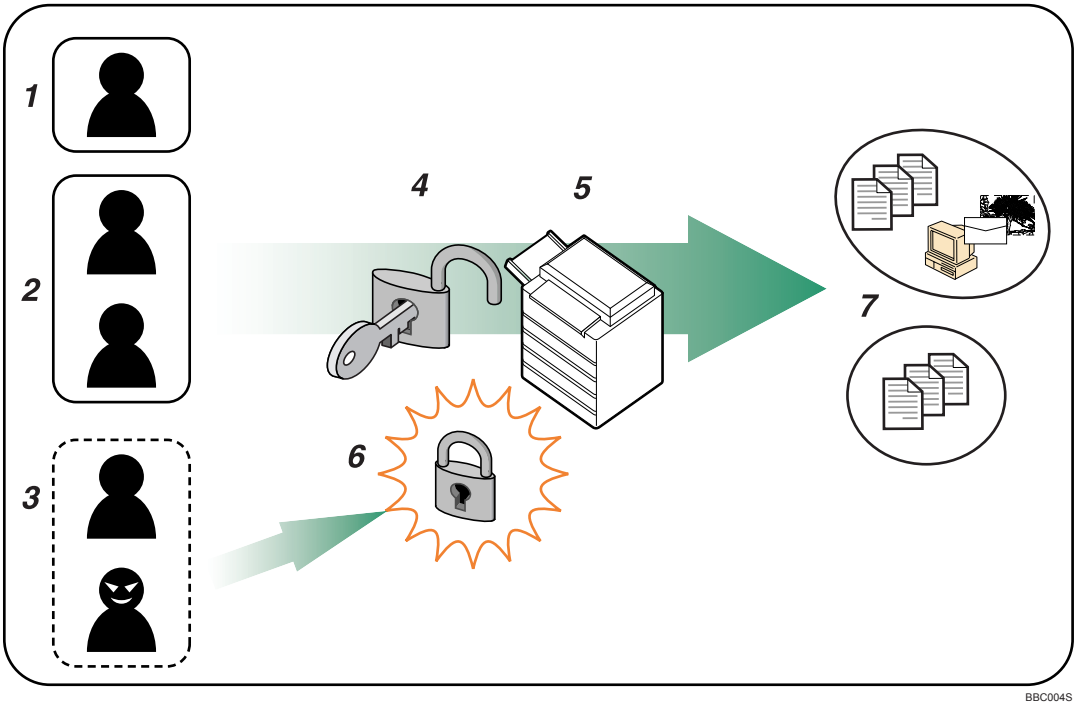
Reference

- p.23 "Administrators"

About User Authentication

This printer 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 printer, such as printing.

2. **Group**

   A group performs normal operations on the printer, such as printing.

3. **Unauthorized User**

4. **Authentication**

   Using a login user name and password, user authentication is performed.

5. **This Printer**

6. **Access Limit**

   Using authentication, unauthorized users are prevented from accessing the printer.

7. **Authorized users and groups can use only those functions permitted by the administrator.**

Configuring User Authentication

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

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

Note

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

Reference

- p.27 "Enabling Administrator Authentication"
- p.45 "Enabling User Authentication"
- p.27 "Specifying Administrator Privileges"
- p.30 "Registering the Administrator"
- p.46 "User Code Authentication"
- p.49 "Basic Authentication"

- p.54 "Windows Authentication"
- p.61 "LDAP Authentication"
- p.66 "Integration Server Authentication"

Enabling User Authentication

To control users' access to the printer, perform user authentication using login user names and passwords. There are five types of user authentication methods: User Code authentication, Basic authentication, Windows authentication, LDAP authentication, and Integration Server authentication. To use user authentication, select an authentication method on the control panel, and then make the required settings for the authentication. The settings depend on the authentication method. Specify administrator authentication, and then specify user authentication.

Note

- User Code authentication is used for authenticating on the basis of a user code, and Basic authentication, Windows authentication, LDAP authentication, and Integration Server authentication are used for authenticating individual users.
- You can specify User Code authentication without specifying administrator authentication.
- A user code account, that has no more than eight digits and is used for User Code authentication, can be carried over and used as a login user name even after the authentication method has switched from User Code authentication to Basic authentication, Windows authentication, LDAP authentication, or Integration Server authentication. In this case, since the User Code authentication does not have a password, the login password is set as blank.
- Numbers containing up to eight digits can be registered in the printer's address book. If the user code authentication setting is set to "Printer: PC Control", make sure any user code entered from the printer driver contains no more than eight digits. We recommend you register user codes from the printer's address book.
- 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 printer despite an authentication failure. From a security perspective, when switching from User Code authentication to another authentication method, we recommend that you delete accounts you are not going to use, or set up a login password. For details about deleting accounts, see "Deleting a Registered Name", Network and System Settings Guide. For details about changing passwords, see "Specifying Login User Names and Passwords".
- You cannot use more than one authentication method at the same time.
- User authentication can also be specified via Web Image Monitor. For details, see Web Image Monitor Help.

Reference

- p.51 "Specifying Login User Names and Passwords"

User Code Authentication

This is an authentication method for limiting access to functions according to a user code. The same user code can be used by more than one user. For details about specifying user codes, see "Authentication Information", Network and System Settings Guide.

Specifying User Code Authentication

This can be specified by the machine administrator.

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

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

   If you do not need to apply printer job authentication, skip to step 11.
2. **Press [Printer Features].**
3. **Press [Administrator Configuration].**
4. **Press [Printer Settings].**

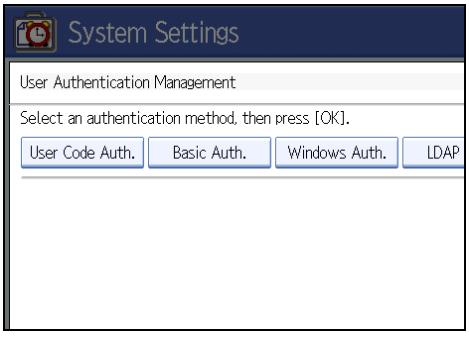
   If a message requesting you to enter a password appears, enter the password for printer settings.
5. **Press [Access Control].**
6. **Select the IP address protocol (IPv4 or IPv6), and then press an access control range between [Access Control Range 1] and [Access Control Range 5].**
7. **Enter the range of IP addresses that are allowed access to the printer.**

   For details about access control, see "Access Control".
8. **Set "Authentication" to [On].**

   If you select [Off], print jobs will not be authenticated.
9. **Press [OK].**
10. **Press [Exit] three times.**
11. **Press [System Settings].**
12. **Press [Administrator Tools].**
13. **Press [User Authentication Management].**

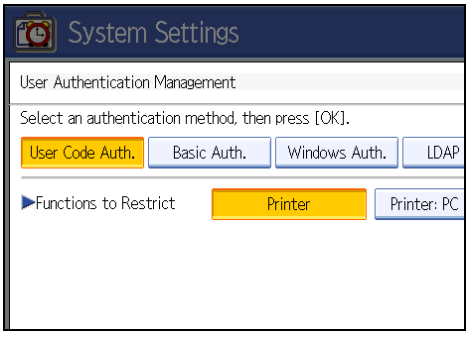
    If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

14. **Select [User Code Auth.].**



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

15. **Select which of the printer's functions you want to limit.**



The selected settings will be unavailable to users.

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

16. **Press [OK].**
17. **Press [Exit].**

A confirmation message appears.

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

18. **Press the [User Tools] key.**

Note

- Some combinations of user authentication setting and type of print job can conflict, resulting in misprinted jobs. For details, see "Notes on User Authentication/Type Combinations".

Reference

- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"
- p.109 "Access Control"

- p.93 "Limiting Available Functions"
- p.71 "Notes on User Authentication/Type Combinations"

Basic Authentication

Specify this authentication method when using the printer's Address Book to authenticate each user. Using Basic authentication, you can not only manage the printer's available functions but also limit access to the personal data in the Address Book. Under Basic authentication, the User administrator must specify the functions available to each user registered in the Address Book.

Specifying Basic Authentication

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

This can be specified by the machine administrator.

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

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

   If you do not need to apply printer job authentication, skip to step 11.
2. **Press [Printer Features].**
3. **Press [Administrator Configuration].**
4. **Press [Printer Settings].**

   If a message requesting you to enter a password appears, enter the password for printer settings.
5. **Press [Access Control].**
6. **Select the IP address protocol (IPv4 or IPv6), and then press an access control range between [Access Control Range 1] and [Access Control Range 5].**
7. **Enter the range of IP addresses that are allowed access to the printer.**

   For details about access control, see "Access Control".
8. **Set "Authentication" to [On].**

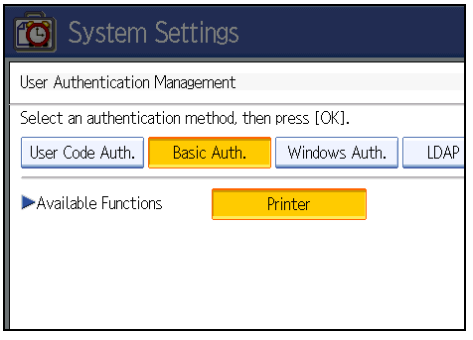
   If you select [Off], print jobs will not be authenticated.
9. **Press [OK].**
10. **Press [Exit] three times.**
11. **Press [System Settings].**
12. **Press [Administrator Tools].**
13. **Press [User Authentication Management].**

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

14. **Select [Basic Auth.].**

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

15. **Select which of the printer's functions you want to permit.**



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

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

16. **Press [OK].**

17. **Press [Exit].**

    A confirmation message appears.

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

18. **Press the [User Tools] key.**

Note

- Some combinations of user authentication setting and type of print job can conflict, resulting in misprinted jobs. For details, see "Notes on User Authentication/Type Combinations".

Reference

- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"
- p.109 "Access Control"
- p.93 "Limiting Available Functions"
- p.71 "Notes on User Authentication/Type Combinations"

Authentication Information Stored in the Address Book

This can be specified by the user administrator.

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

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

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

User authentication can also be specified via Web Image Monitor.

Reference

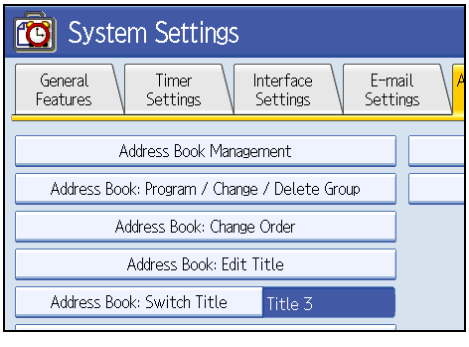
- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"

Specifying Login User Names and Passwords

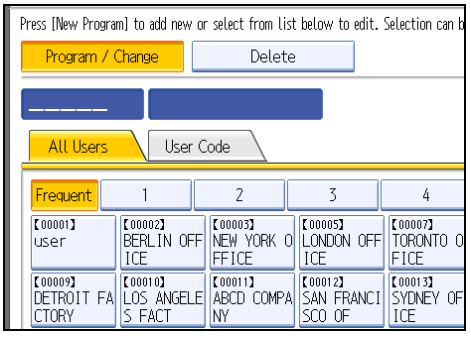
In "Address Book Management", specify the login user name and login password to be used for User Authentication Management.

Login user names can contain up to 32 characters; passwords can contain up to 128 characters. Both user names and passwords can contain alphanumeric characters and symbols. User names cannot contain spaces, colons, or quotation marks, and cannot be blank.

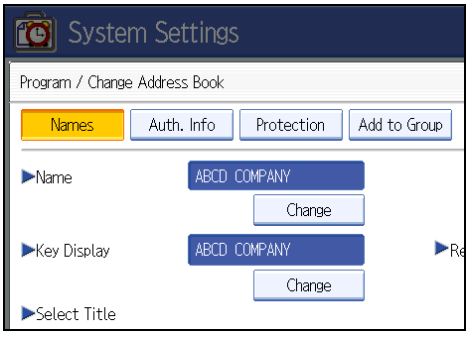
1. **Press the [User Tools] key.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [Address Book Management].**



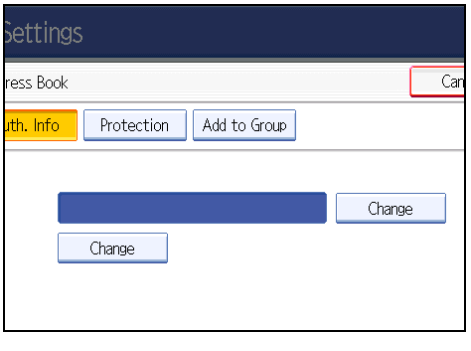
5. Select the user or group.



6. Press [Auth. Info].

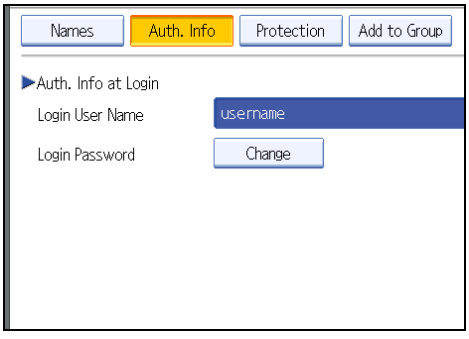


7. Press [Change] for "Login User Name".



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

9. Press [Change] for "Login Password".



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

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 printer, enabling user authentication without first using the printer to register individual settings in the Address Book.

Windows authentication can be performed using one of two authentication methods: NTLM or Kerberos authentication. The operational requirements for both methods are listed below.

Operational Requirements for NTLM authentication

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

- This printer only supports NTLMv1 authentication.
- A domain controller has been set up in a designated domain.
- This function is supported by the operating systems listed below. To obtain user information when running Active Directory, use LDAP. If SSL is being used, a version of Windows that supports TLS v1, SSL v2, or SSL v3 is required.
  - Windows 2000 Server
  - Windows Server 2003/2003 R2
  - Windows Server 2008

Operational Requirements for Kerberos authentication

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

- A domain controller must be set up in a designated domain.
- The operating system must be able to support KDC (Key Distribution Center). To obtain user information when running Active Directory, use LDAP. If SSL is being used, a version of Windows that supports TLSv1, SSLv2, or SSLv3 is required. Compatible operating systems are listed below.
  - Windows 2000 Server
  - Windows Server 2003/2003 R2
  - Windows Server 2008

Important

- **During Windows Authentication, data registered in the directory server is automatically registered in the printer. If user information on the server is changed, information registered in the printer may be overwritten when authentication is performed.**
- **Users not registered in the same domain are also authenticated with user authentication. However, the printer cannot acquire those users' user information.**

- **If you have created a new user in the domain controller and selected "User must change password at next logon", log on to the printer from the computer to change the password before logging on from the printer's control panel.**
- **If the authenticating server only supports NTLM when Kerberos authentication is selected on the printer, the authenticating method will automatically switch to NTLM.**

Note

- Enter the login password correctly; keeping in mind that it is case-sensitive.
- The first time you access the printer, 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 printer 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, it is recommended that communication between the printer and domain controller be encrypted using SSL.
- Under Windows Authentication, you do not have to create a server certificate unless you want to automatically register user information using SSL.
- To enable Kerberos for LDAP authentication, a realm must be registered beforehand. The realm must be programmed in capital letters. For details about registering a realm, see the "Programming the LDAP Server", or "Programming the Realm", Network and System Settings Guide.

Specifying Windows Authentication

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

This can be specified by the machine administrator.

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

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

   If you do not need the printer job authentication, skip to step 11.

2. **Press [Printer Features].**
3. **Press [Administrator Configuration].**
4. **Press [Printer Settings].**

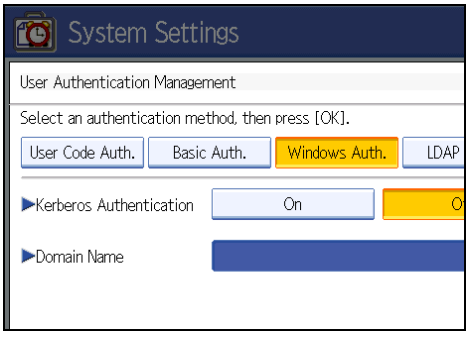
   If a message requesting you to enter a password appears, enter the password for printer settings.
5. **Press [Access Control].**
6. **Select the IP address protocol (IPv4 or IPv6), and then press an access control range between [Access Control Range 1] and [Access Control Range 5].**
7. **Enter the range of IP addresses that are allowed access to the printer.**

   For details about access control, see "Access Control".
8. **Set "Authentication" to [On].**

   If you select [Off], print jobs will not be authenticated.
9. **Press [OK].**
10. **Press [Exit] three times.**
11. **Press [System Settings].**
12. **Press [Administrator Tools].**
13. **Press [User Authentication Management].**

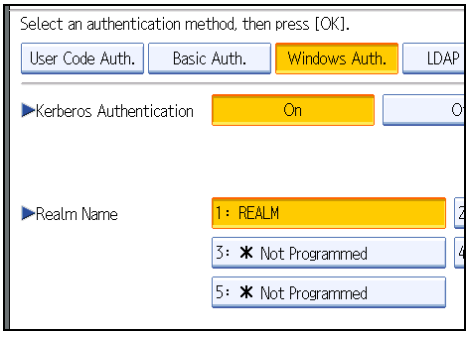
    If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.
14. **Select [Windows Auth.].**

    If you do not want to use user authentication management, select [Off].
15. **If you want to use Kerberos authentication, press [On].**



If you want to use NTLM authentication, press [Off] and proceed to step 17.

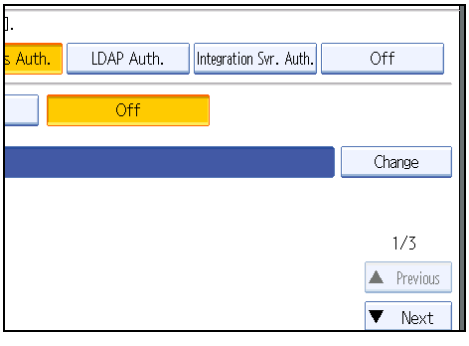
16. **Select Kerberos authentication realm and proceed to step 18.**



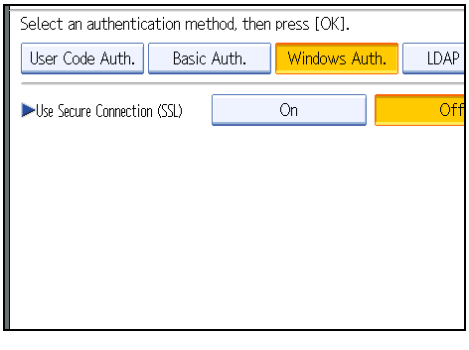
To enable Kerberos authentication, a realm must be registered beforehand. The realm name must be registered in capital letters. For details about registering a realm, see "Programming the Realm", Network and System Settings Guide.

Up to 5 realms can be registered.

17. **Press [Change] for "Domain Name", enter the name of the domain controller to be authenticated, and then press [OK].**



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



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

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

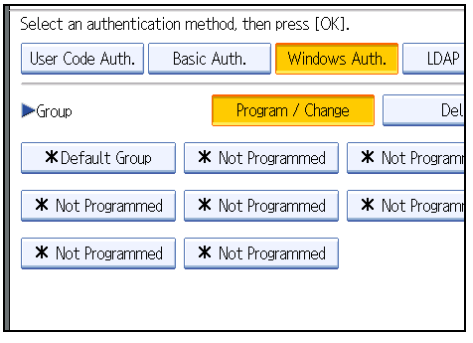
If global groups have been registered under Windows server, you can limit the use of functions for each global group.

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 printer the functions available to the global group members. Create global groups in the printer 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 printer functions available to each group.

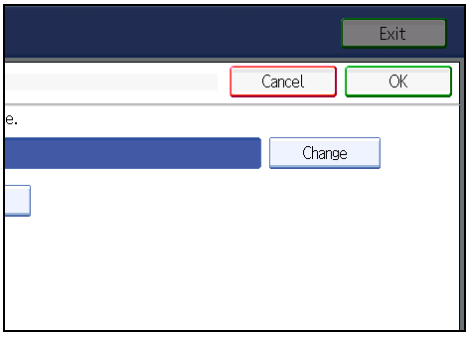
If global groups are not specified, users can use the available functions specified in [*Default Group]. If global groups are specified, users not registered in global groups can use the available functions specified in [*Default Group]. By default, all functions are available to *Default Group members.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

19. **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.

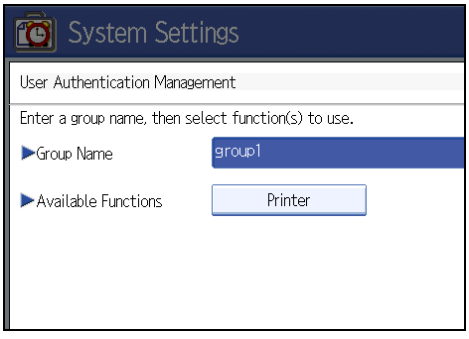


20. **Under "Group Name", press [Change], and then enter the group name.**



21. **Press [OK].**

22. **Select which of the printer's functions you want to permit.**



Windows Authentication will be applied to the selected functions.

Users can use the selected functions only.

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

23. **Press [OK] twice.**
24. **Press the [User Tools] key.**

A confirmation message appears.

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

Note

- Some combinations of user authentication setting and type of print job can conflict, resulting in misprinted jobs. For details, see "Notes on User Authentication/Type Combinations".

Reference

- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"
- p.109 "Access Control"
- p.93 "Limiting Available Functions"
- p.71 "Notes on User Authentication/Type Combinations"

Creating the Server Certificate

To create the server certificate for the domain controller, use the following procedure:

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

Web Server Certificate Wizard starts.

4. **Click [Next].**
5. **Select [Create a new certificate], and then click [Next].**
6. **Select [Prepare the request now, but send it later], and then click [Next].**
7. **Enter the required information according to the instructions given by Web Server Certificate Wizard.**
8. **Check the specified data, which appears as "Request File Summary", and then click [Next].**

   The server certificate is created.

Installing the Device Certificate (issued by a Certificate Authority)

Install the device certificate using Web Image Monitor.

Use the following procedure to apply a certificate issued by a certificate authority as the device certificate.

1. **Open a Web browser.**
2. **Enter "http://(system'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 printer.

   The top page of Web Image Monitor appears.
3. **Click [Login].**

   The network administrator can log on.

   Enter the login user name and password.
4. **Click [Configuration], and then click [Device Certificate] under "Security".**

   The Device Certificate page appears.
5. **Check the option button next to the number of the certificate you want to install.**
6. **Click [Install].**
7. **Open the certificate sent from the certificate authority in a text editor, and then copy all the text.**
8. **Paste all the copied text into the "Certificate Request" box.**
9. **Click [OK].**

   "Installed" appears under "Certificate Status" to show that a device certificate for the printer has been installed.
10. **Click [Logout].**

LDAP Authentication

Specify this authentication method when using the LDAP server to authenticate users who have their accounts on the LDAP server. Users cannot be authenticated if they do not have their accounts on the LDAP server. The Address Book stored in the LDAP server can be registered to the printer, enabling user authentication without first using the printer 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 printer and LDAP server be encrypted using SSL. You can specify on the LDAP server whether or not to enable SSL. To do this, you must create a server certificate for the LDAP server.

Using Web Image Monitor, you can specify whether or not to check the reliability of the connecting SSL server. For details about specifying LDAP authentication using Web Image Monitor, see Web Image Monitor Help.

Important

- **During LDAP authentication, the data registered in the LDAP server is automatically registered in the printer. If user information on the server is changed, information registered in the printer may be overwritten when authentication is performed.**
- **Under LDAP authentication, you cannot specify access limits for groups registered in the LDAP server.**
- **Enter the user's login user name using up to 32 characters and login password using up to 128 characters.**
- **Do not use double-byte Japanese, Traditional Chinese, Simplified Chinese, or Hangul characters when entering the login user name or password. If you use double-byte characters, you cannot authenticate using Web Image Monitor.**

Operational Requirements for LDAP Authentication

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

- The network configuration must allow the printer 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 printer.
- When registering the LDAP server, the following setting must be specified.
  - Server Name
  - Search Base
  - Port Number
  - SSL Communication
  - Authentication

    Select either Kerberos, DIGEST, or Cleartext authentication.
  - User Name

You do not have to enter the user name if the LDAP server supports "Anonymous Authentication".

- Password

  You do not have to enter the password if the LDAP server supports "Anonymous Authentication".

Note

- When you select Cleartext authentication, LDAP Simplified authentication is enabled. Simplified authentication can be performed with a user attribute (such as cn, or uid), instead of the DN.
- You can also prohibit blank passwords at login for simplified authentication. For details about LDAP Simplified authentication, contact your sales representative.
- Under LDAP Authentication, if "Anonymous Authentication" in the LDAP server's settings is not set to Prohibit, users who do not have an LDAP server account might still be able to gain access.
- If the LDAP server is configured using Windows Active Directory, "Anonymous Authentication" might be available. If Windows authentication is available, we recommend you use it.
- The first time an unregistered user accesses the printer after LDAP authentication has been specified, the user is registered in the printer 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 printer subsequently.
- To enable Kerberos for LDAP authentication, a realm must be registered beforehand. The realm must be programmed in capital letters. For details about registering a realm, see "Programming the Realm", Network and System Settings Guide.

Specifying LDAP Authentication

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

This can be specified by the machine administrator.

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

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

   If you do not need to apply printer job authentication, skip to step 11.

2. **Press [Printer Features].**
3. **Press [Administrator Configuration].**
4. **Press [Printer Settings].**

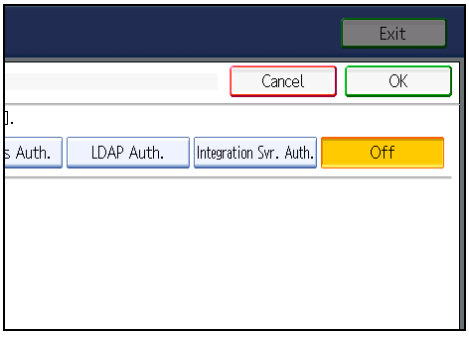
   If a message requesting you to enter a password appears, enter the password for printer settings.

5. **Press [Access Control].**
6. **Select the IP address protocol (IPv4 or IPv6), and then press an access control range between [Access Control Range 1] and [Access Control Range 5].**
7. **Enter the range of IP addresses that are allowed access to the printer.**

   For details about access control, see "Access Control".
8. **Set "Authentication" to [On].**

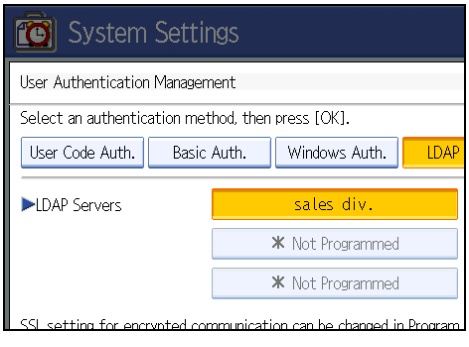
   If you select [Off], print jobs will not be authenticated.
9. **Press [OK].**
10. **Press [Exit] three times.**
11. **Press [System Settings].**
12. **Press [Administrator Tools].**
13. **Press [User Authentication Management].**

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

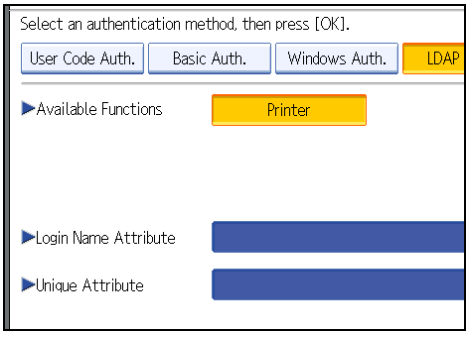


If you do not want to use user authentication management, select [Off].

15. **Select the LDAP server to be used for LDAP authentication.**



16. **Select which of the printer's functions you want to permit.**

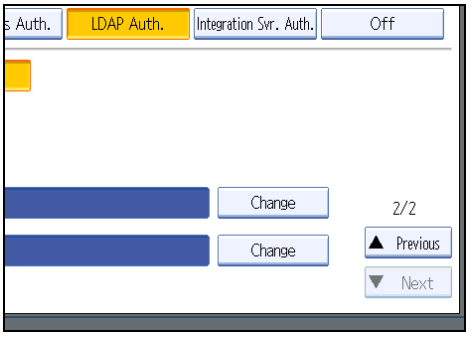


LDAP Authentication will be applied to the selected functions.

Users can use the selected functions only.

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

17. **Press [Change] for "Login Name Attribute".**



18. **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 printer's Address Book.

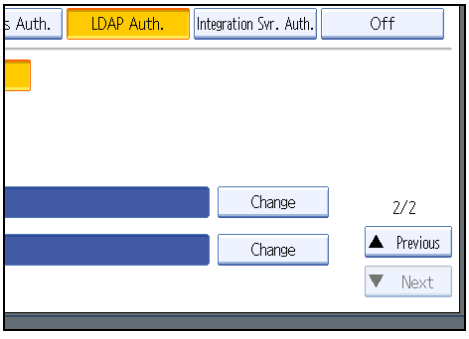
To specify multiple login attributes, place a comma (,) between them. The search will return hits for either or both attributes.

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

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

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

19. **Press [Change] for "Unique Attribute".**



20. **Enter the unique attribute and then press [OK].**

    Specify Unique Attribute on the printer to match the user information in the LDAP server with that in the printer. By doing this, if the Unique Attribute of a user registered in the LDAP server matches that of a user registered in the printer, 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 printer.

21. **Press [OK].**

22. **Press the [User Tools] key.**

    A confirmation message appears.

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

Note

- Some combinations of user authentication setting and type of print job can conflict, resulting in misprinted jobs. For details, see "Notes on User Authentication/Type Combinations".

Reference

- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"
- p.109 "Access Control"
- p.93 "Limiting Available Functions"
- p.71 "Notes on User Authentication/Type Combinations"

Integration Server Authentication

To use Integration Server authentication with this printer, you need a server on which "Authentication Manager" or another application that supports authentication is installed. For details about the software, contact your sales representative.

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.

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

Important

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

Specifying Integration Server Authentication

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

This can be specified by the machine administrator.

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

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

   If you do not need to apply printer job authentication, skip to step 11.

2. **Press [Printer Features].**
3. **Press [Administrator Configuration].**
4. **Press [Printer Settings].**

   If a message requesting you to enter a password appears, enter the password for printer settings.

5. **Press [Access Control].**
6. **Select the IP address protocol (IPv4 or IPv6), and then press an access control range between [Access Control Range 1] and [Access Control Range 5].**
7. **Enter the range of IP addresses that are allowed access to the printer.**

   For details about access control, see "Access Control".

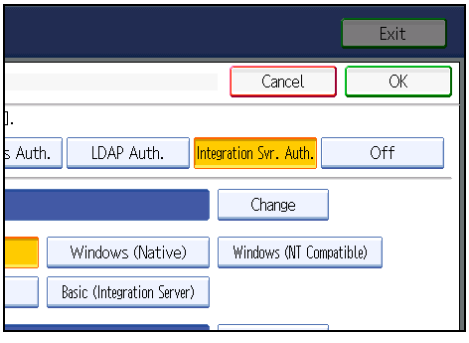
8. **Set "Authentication" to [On].**

   If you select [Off], print jobs will not be authenticated.

9. **Press [OK].**
10. **Press [Exit] three times.**
11. **Press [System Settings].**
12. **Press [Administrator Tools].**
13. **Press [User Authentication Management].**

    If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.
14. **Select [Integration Svr. Auth.].**

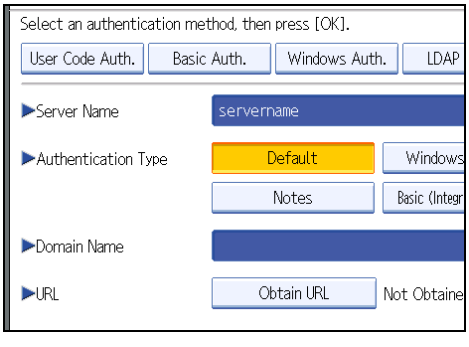
    If you do not want to use User Authentication Management, select [Off].
15. **Press [Change] for "Server Name".**



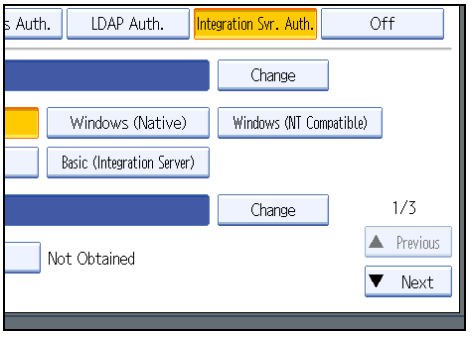
    Specify the name of the server for external authentication.
16. **Enter the server name, and then press [OK].**

    Enter the IPv4 address or host name.
17. **In "Authentication Type", select the authentication system for external authentication.**

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



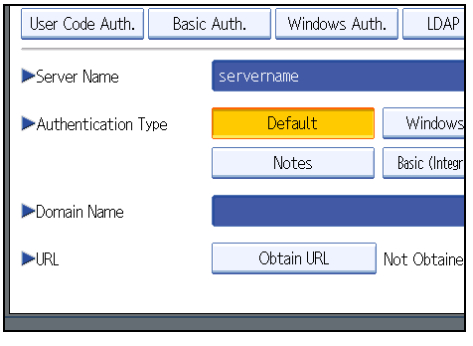
18. **Press [Change] for "Domain Name".**



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

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

20. **Press [Obtain URL].**



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

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

21. **Press [Exit].**

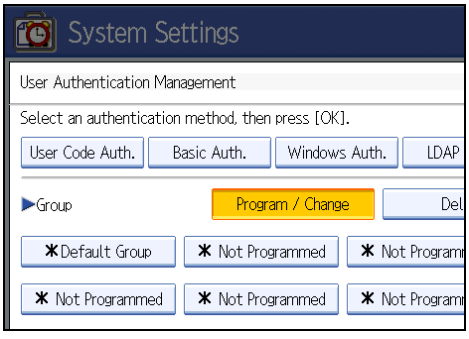
In the "Authentication Type", if you have not registered a group, proceed to step 26.

If you have registered a group, proceed to step 22.

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

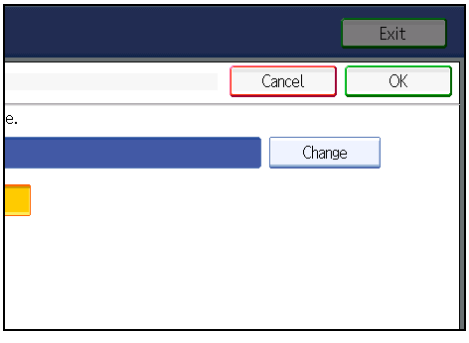
If you set "Authentication Type" to [Notes], you can use the Notes group. If you set "Authentication Type" to [Basic (Integration Server)], you can use the groups created using the Authentication Manager.

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



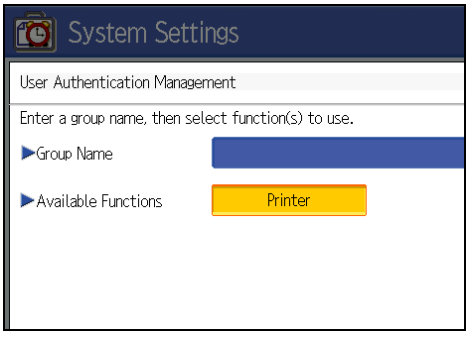
If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

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



24. **Press [OK].**

25. **Select which of the printer's functions you want to permit.**



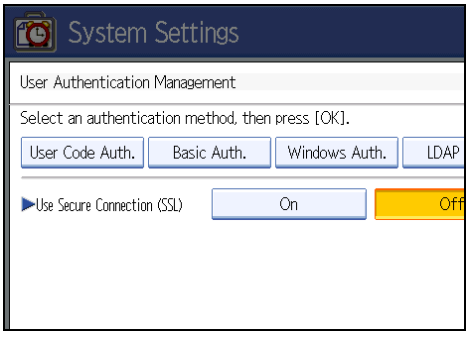
Authentication will be applied to the selected functions.

Users can use the selected functions only.

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

26. **Press [OK].**

27. 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].

28. Press the [User Tools] key.

A confirmation message appears.

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

Note

- Some combinations of user authentication setting and type of print job can conflict, resulting in misprinted jobs. For details, see "Notes on User Authentication/Type Combinations".

Reference

- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"
- p.109 "Access Control"
- p.93 "Limiting Available Functions"
- p.71 "Notes on User Authentication/Type Combinations"

Notes on User Authentication/Type Combinations

When user authentication is applied, a job can be printed only if the user associated with the job is registered in the printer's address book. If there is no match, the job will be cancelled.

Some combinations of user authentication setting and type of printer job can conflict, resulting in misprinted jobs. To avoid this, refer to the following table when specifying the user authentication setting.

User authentication is supported by the M driver.

Combination List

For users allowed by access control to access the printer.

Access Control "Authentication"	On	On	Off	Off
User Authentication Management	On*1	Off	On*1	Off
Printer Job Type 1	●	☆	☆	☆
Printer Job Type 2	○	☆	☆	☆
Printer Job Type 3	×	☆	☆	☆

*1 When User Code, Basic, Windows, LDAP, or Integration Server authentication is enabled.

☆: Printing is possible regardless of user authentication.

○: Printing is possible if user authentication is successful. If user authentication fails, the print job is reset.

●: Printing is possible if user authentication is successful and "Driver Encryption Key" for the printer driver and printer match.

×: Printing is not possible regardless of user authentication, and the print job is reset.

Printer Job Types

- "Printer Job Type 1" is defined by the following conditions: In the M driver's "Advanced Options", the "Confirm authentication information when printing" and the "Encrypt" check boxes are both selected, the driver encryption key has been entered, and the login user name and password have been entered in "Job Options".
- "Printer Job Type 2" is defined by the following conditions: In the M driver's "Advanced Options", the "Confirm authentication information when printing" check box is selected and the login user name and password have been entered in "Job Options".
- "Printer Job Type 3" is defined by the following conditions: In the M driver's "Advanced Options", the "Confirm authentication information when printing" check box is not selected and the login user name and password have not been entered in "Job Options".

Note

- Print jobs sent by users excluded by access control will be cancelled, irrespective of the User Authentication setting or type of print job.
- If access control has not been specified, print jobs can be printed irrespective of the User Authentication setting or type of print job.
- With a parallel or AppleTalk connection, print jobs can be printed irrespective of the User Authentication setting or type of print job.
- For details about the driver encryption key, see "Specifying the Extended Security Function".

Reference

- p.173 "Specifying the Extended Security Functions"

Specifying Exemption from User Authentication

You can specify an exemption sub-range within the access control range.

Any jobs originating from addresses within the exemption sub-range will be printed, irrespective of the user authentication setting or type of print job. Similarly, any jobs originating from addresses outside the exemption sub-range will be printed subject to the user authentication setting and type of print job.

Perform the following procedure if the printer driver you are using does not support User Authentication, or if you want to print by bypassing the printer driver.

1. **Specify the access control range according to the User Authentication setting procedure, and then set "Authentication" for that range to "On".**
2. **Specify a sub-range within the range specified in Step 1, and then set "Authentication" for that range to "Off".**

   For example: in "Access Control Range 1", specify the start and end addresses as [192.168.1.1]-[192.168.1.255], and then set "Authentication" for that range to "On". To exempt the sub-range 192.168.1.10 to 192.168.1.50 from authentication, in "Access Control Range 2", specify the start and end addresses as [192.168.1.10]-[192.168.1.50], and then set "Authentication" for this range to "Off".

   With this setting, authentication is performed on addresses within the range 192.168.1.1 to 192.168.1.255, but not within the sub-range 192.168.1.10 to 192.168.1.50.

Note

- For details about specifying User Authentication, see "Enabling User Authentication".

Reference

- p.45 "Enabling User Authentication"

If User Authentication is Specified

When Basic Authentication, Windows Authentication, LDAP Authentication, or Integration Server Authentication is set, the authentication screen is displayed. Unless a valid user name and password are entered, operations are not possible with the printer. Log on to operate the printer, and log off when you are finished operations. Be sure to log off to prevent unauthorized users from using the printer. When auto logout timer is specified, the printer automatically logs you off if you do not use the control panel within a given time.

Note

- Consult the User Administrator about your login user name, password, and user code.
- The Auto Logout Timer can only be used under Basic Authentication, Windows Authentication, LDAP Authentication, or Integration Server Authentication.

If User Code Authentication is Specified

If User Code Authentication is enabled, the authentication message will not appear.

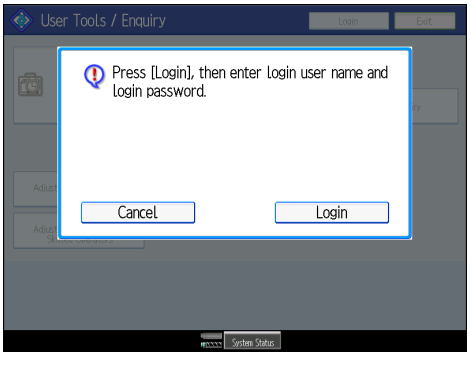
The printer's User Code Authentication supports authentication from the printer driver or utilities. For details about authentication using the printer driver, see "Logging on Using the Printer Driver".

Reference

- p.74 "Logging on Using the Printer Driver"

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

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



Enter your login user name and password.

Logging on Using the Control Panel

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

1. **Press [Login].**
2. **Enter the login user name, and then press [OK].**
3. **Enter the login password, and then press [OK].**

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

Logging off Using the Control Panel

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

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

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

Note

- You can log off using the following procedures also.
  - Press the [Power] key.
  - Press the [Energy Saver] key.

Logging on Using the Printer Driver

If User Code Authentication, Basic Authentication, Windows Authentication, LDAP Authentication, or Integration Server Authentication has been set, you must configure the encryption settings in the printer properties dialog box and then enter either the login user name and password or the user code.

Enter the following user information in the "User Authentication" area of the printer properties dialog box:

For Basic Authentication, Windows Authentication, LDAP Authentication, or Integration Server Authentication:

"Login user name": login user name

"Login password": login password

For User Code Authentication:

"Login user name": login user code (up to eight digits)

"Login password": blank (a login password is not necessary for user code authentication)

Note

- For details about applying user authentication via the printer driver, see "Using User Authentication", Printer Reference.
- When logged on using a printer driver, logging off is not required.

Logging on Using Web Image Monitor

This section explains how to log on to the printer via Web Image Monitor.

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

Note

- For user code authentication, enter the user code (up to eight digits) in "Login User Name", and then click [Login].

Logging off Using Web Image Monitor

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

Note

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

User Lockout Function

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

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

Note that User Lockout will not occur if you are logging on to Printer Features using the password for printer settings.

Lockout setting items

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

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

Lockout release privileges

Administrators with unlocking privileges are as follows.

Locked out User	Unlocking administrator
general user	user administrator
user administrator, network administrator, file administrator, machine administrator	supervisor
supervisor	machine administrator

Specifying the User Lockout Function

This can be specified by the machine administrator using Web Image Monitor.

1. **Open a Web browser.**
2. **Enter "http://(system'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 printer.

   The top page of Web Image Monitor appears.

3. **Click [Login].**

   The machine administrator can log on.

   Enter the login user name and login password.

4. **Click [Configuration], and then click [User Lockout Policy] under "Security".**

   The User Lockout Policy page appears.

5. **Set "Lockout" to [Active].**

6. **In the drop down menu, select the number of login attempts to permit before applying lockout.**

7. **Set the "Lockout Release Timer" to [Active].**

8. **In the "Lock Out User for" field, enter the number of minutes until lockout is disabled.**

9. **Click [OK].**

   User Lockout Policy is set.

10. **Click [Logout].**

Unlocking a Locked User Account

A locked user account can be unlocked by the administrator or supervisor with unlocking privileges using Web Image Monitor.

1. **Open a Web browser.**

2. **Enter "http://(system'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 printer.

   The top page of Web Image Monitor appears.

3. **Click [Login].**

   The administrator or supervisor with unlocking privileges can log on.

   Enter the login user name and login password.

4. **Click [Address Book].**

   The Address Book page appears.

5. **Select the locked out user's account.**

6. **Click [Change].**

7. **Set the "Lockout" to [Inactive] under "Authentication Information".**

8. **Click [OK].**

9. **Click [Logout].**

Auto Logout

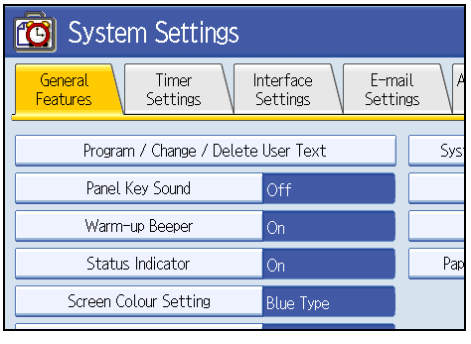
This can be specified by the machine administrator.

When using Basic Authentication, Windows Authentication, LDAP Authentication or Integration Server Authentication, the printer automatically logs you off if you do not use the control panel within a given time. This feature is called "Auto Logout". Specify how long the printer is to wait before performing Auto Logout.

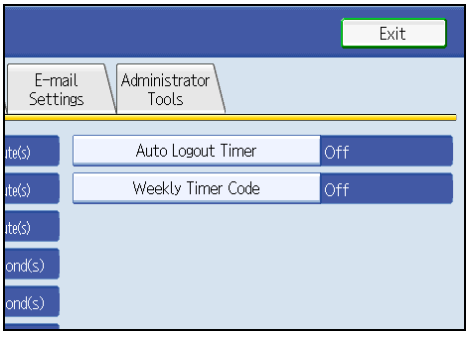
Note that Auto Logout is not applied if you have logged on to Printer Features using the password for printer settings.

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

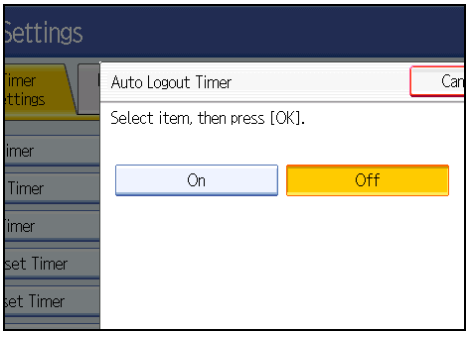
1. **Press the [User Tools] key.**
2. **Press [System Settings].**
3. **Press [Timer Settings].**



4. **Press [Auto Logout Timer].**

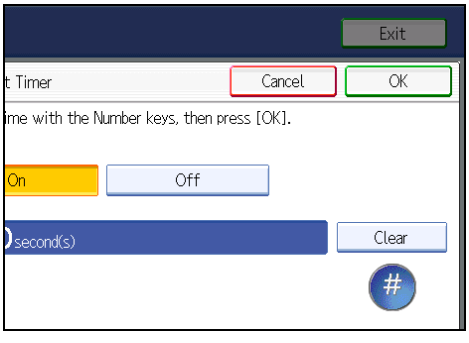


5. **Select [On].**



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

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



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

A confirmation message appears.

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

Note

- If a paper jam occurs or a print cartridge runs out of toner, the printer might not be able to perform the Auto Logout function.

Reference

- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"

Authentication Using an External Device

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

For details, contact your sales representative.

4. Securing Information Stored on Hard Disk

This chapter describes how to protect information stored on the hard disk from unauthorized viewing and modification.

Protecting the Address Book

If user authentication is specified, the user who has logged on will be designated as the sender to prevent data from being sent by an unauthorized person masquerading as the user.

To protect the data from unauthorized reading, you can also encrypt the data in the Address Book.

Configuring Address Book Access Permissions

This can be specified by the registered user.

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

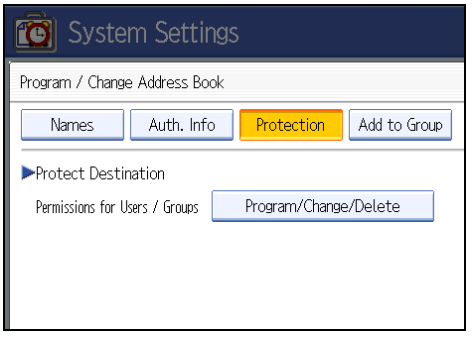
You can specify who is allowed to access the data in the Address Book.

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

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

1. **Press the [User Tools] key.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [Address Book Management].**
5. **Select the user or group.**
6. **Press [Protection].**

7. **Press [Program/Change/Delete] for "Permissions for Users/Groups", under "Protect Destination".**



8. **Press [New Program].**
9. **Select the users or groups to register.**

   You can select more than one user.

   By pressing [All Users], you can select all the users.
10. **Press [Exit].**
11. **Select the user who you want to assign access permission to, and then select the permission.**

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

Reference

- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"

Encrypting Data in the Address Book

This can be specified by the user administrator.

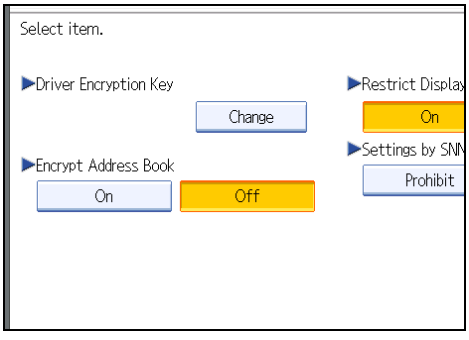
You can encrypt the data in the Address Book using the extended security function, "Encrypt Address Book". For details about this and other extended security functions, see "Specifying the Extended Security Functions".

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

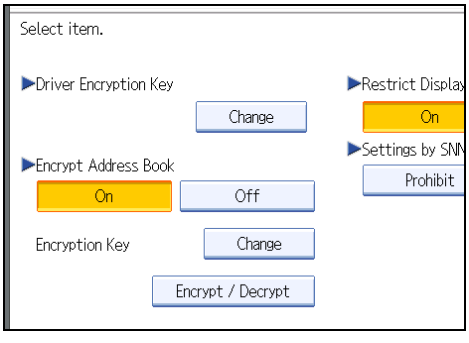
1. **Press the [User Tools] key.**
2. **Press [System Settings].**

3. **Press [Administrator Tools].**
4. **Press [Extended Security].**

   If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.
5. **Press [On] for "Encrypt Address Book".**

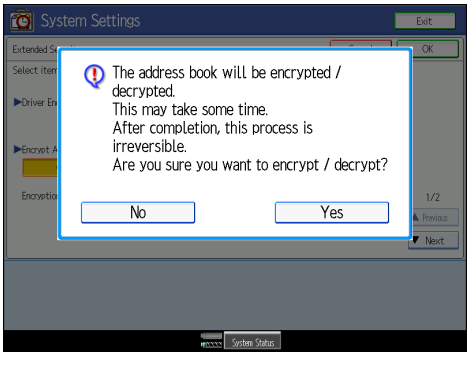


6. **Press [Change] for "Encryption Key".**



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

   Enter the encryption key using up to 32 alphanumeric characters.
8. **Press [Encrypt / Decrypt].**
9. **Press [Yes].**



Do not switch the main power off during encryption, as doing so may corrupt the data.

Encrypting the data in the Address Book may take a long time.

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

The printer cannot be used during encryption.

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

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

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

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

Note

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

Reference

- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"
- p.173 "Specifying the Extended Security Functions"

Deleting Data on the Hard Disk

This can be specified by the machine administrator.

To use this function, the optional security unit must be installed.

The following data is stored on the hard disk:

- Printer function jobs
- Address Book
- Counter figures (by user code)

We recommend that before disposing of the printer, you delete all the data on the hard disk by performing an overwrite. This will prevent leakage of sensitive data.

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 printer.

The Erase All Memory function erases all the data from the printer hard disk first and then the system hard disk.

Important

- **If you select "Erase All Memory", the following are also deleted: user codes, counters under each user code, data stored in the Address Book, printer fonts downloaded by users, applications using Embedded Software Architecture, device certificates, and the printer's network settings.**
- **If the main power switch is turned to [Stand by] while the Erase All Memory function is in progress, any data not yet deleted will remain on the hard disk.**
- **Do not stop the overwrite mid-process. Doing so will damage the hard disk.**
- **Other than pausing, no operations are possible during the "Erase All Memory" process.**
- **If the number of overwrites set to "3", the erase process will take about four and a half hours.**

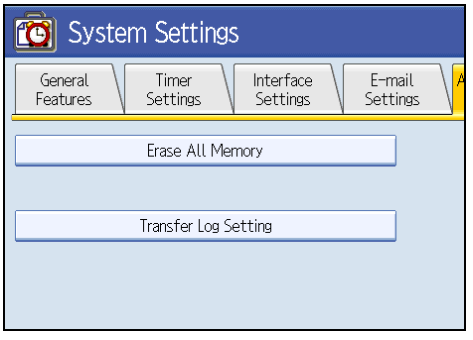
Using Erase All Memory

This can be specified by the machine administrator.

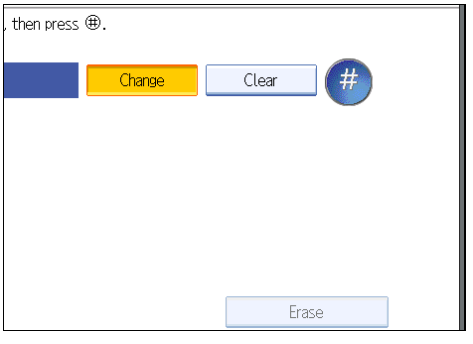
For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

1. **Disconnect communication cables connected to the printer.**
2. **Press the [User Tools] key.**
3. **Press [System Settings].**

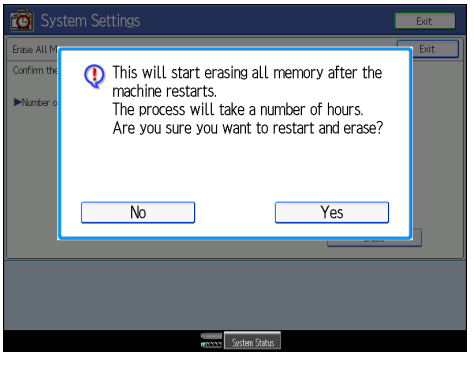
4. Press [Administrator Tools].
5. Press [▼Next] repeatedly until [Erase All Memory] appears.
6. Press [Erase All Memory].



7. 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 data on the printer hard disk is deleted, the printer automatically reboots, and then the data on the system hard disk is deleted.

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.

Note

- If power is lost or the main power switch is turned off while printer hard disk erasure (overwriting) is in progress, the erasure will be incomplete and a warning message will appear as soon as power to the printer is restored. To complete the erasure after power loss, you must repeat the Erase All Memory procedure again from Step 1.
- If power is lost or the main power switch is turned off while system hard disk erasure (overwriting) is in progress, the erasure will continue as soon as power to the printer is restored.
- If an error occurs before overwriting is completed, turn off the main power. Turn it on again, and then repeat from step 2.

Reference

- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"

Suspending Erase All Memory

Use the following procedure to temporarily suspend the overwriting of data on the system hard disk.

Important

- **Erase All Memory cannot be cancelled.**

1. **Press [Suspend] while Erase All Memory is in progress.**
2. **Press [Yes].**

   Erase All Memory is suspended.
3. **Turn off the main power.**

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

Note

- To resume overwriting, turn on the main power.
- You cannot suspend Erase All Memory while data is being deleted from the printer hard disk.

5. Managing Access to the Machine

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

Preventing Changes to Machine Settings

This section describes preventing modification of printer settings.

The administrator type determines which printer settings can be modified. Users cannot change the administrator settings. In "Available Settings" under "Administrator Authentication Management", the administrator can select which settings users cannot specify. For details about the administrator roles, see "Administrators".

Register the administrators before using the printer. For instructions on registering the administrator, see "Registering the Administrator".

Type of Administrator

Register the administrator on the printer, 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 printer settings can be modified. The following administrator types are possible:

- User Administrator

  For a list of settings that the user administrator can specify, see "User Administrator Settings".

- Machine Administrator

  For a list of settings that the machine administrator can specify, see "Machine Administrator Settings".

- Network Administrator

  For a list of settings that the network administrator can specify, see "Network Administrator Settings".

- File Administrator

  For a list of settings that the file administrator can specify, see "File Administrator Settings".

Menu Protect

There are settings on the Printer Features and general printer function menus that users without the password for printer settings can access. You can use this function to deny or permit access to those settings.

For a list of settings that users can specify depending on the configuration of the Menu Protect function, see "User Settings - Control Panel Settings".

Reference

- p.23 "Administrators"
- p.30 "Registering the Administrator"

- p.220 "User Administrator Settings"
- p.209 "Machine Administrator Settings"
- p.215 "Network Administrator Settings"
- p.218 "File Administrator Settings"
- p.225 "User Settings - Control Panel Settings"

Menu Protect

This section explains how to lock Printer Features and the printer's regular menus so they cannot be changed. This function is effective even if user authentication is not in operation. For a list of settings that users can specify according to Menu Protect, see "User Settings - Control Panel Settings".

Important

- **If you set the password for printer settings to "0", protection by login password is disabled, so the Menu Protect function will be not effective, whatever its setting.**
- **If a user tries to specify a setting that is locked by Menu Protect, a message requesting the user to enter a password appears. To specify the locked setting, the Printer Features administrator must enter the password for printer settings.**

Reference

- p.225 "User Settings - Control Panel Settings"

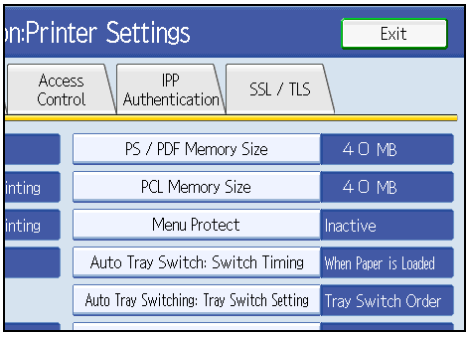
Specifying Menu Protect

This must be specified by the Printer Features administrator.

1. **Press the [User Tools] key.**
2. **Press [Printer Features].**

   If user authentication is in operation, an authentication message will appear. To log on, enter the login user name and password.
3. **Press [Administrator Configuration].**
4. **Press [Printer Settings].**

   If a message requesting you to enter a password appears, enter the password for printer settings.
5. **Press [General Features].**
6. **Press [Menu Protect].**



7. **Select [Active], and then press [OK].**

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

Note

- The default for Menu Protect is [Inactive].

Limiting Available Functions

To prevent unauthorized operation, you can specify who is allowed to access the printer functions.

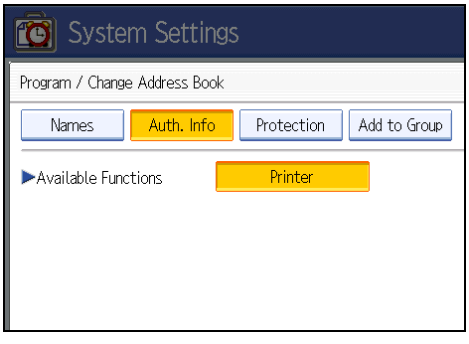
Specifying Which Functions are Available

This can be specified by the user administrator.

Specify the functions available to registered users. By making this setting, you can limit the functions available to users.

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

1. **Press the [User Tools] key.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [Address Book Management].**
5. **Select the user.**
6. **Press [Auth. Info].**
7. **In "Available Functions", select the functions you want to specify.**



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

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

Reference

- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"

Managing Log Files

The logs created by this printer allow you to track access to the printer, identities of users, and usage of the printer's various functions. For security, you can encrypt the logs. This prevents users who do not have the encryption key from accessing log information.

Note however that logs are data heavy and will consume hard disk space. To make hard disk space available, you might need to periodically delete the log files.

The logs can be viewed using Web Image Monitor. You can also convert log files into CSV files for downloading.

Log Types

This printer creates two types of log: the job log and the access log.

- Job Log

  Stores details of user file-related operations such as printing, and control panel operations such as printing reports (the configuration list, for example).

- Access Log

  Stores details of login/logout activity, service engineer operations such as hard disk formatting, system operations such as viewing the results of log transfers, and security operations such as specifying settings for encryption, unauthorized access detection, user lockout, and firmware authentication.

Note

- The access log does not record logins made using the password for printer settings.

Using the Control Panel to Specify Log File Settings

You can specify settings such as whether or not to delete the entire job log and access log.

Specifying Delete All Logs

This can be specified by the machine administrator.

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

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

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

1. **Press the [User Tools] key.**
2. **Press [System Settings].**

3. **Press [Administrator Tools].**
4. **Press [Delete All Logs].**

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

   The confirmation screen appears.
5. **Press [Yes].**
6. **Press [Exit].**
7. **Press the [User Tools] key.**

Reference

- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"

Using Web Image Monitor to Manage Log Files

You can specify the log collection level for the job and access logs. You can also encrypt, bulk delete, or download log files.

Specifying Log Collect Settings

This can be specified by the machine administrator.

Specify collection log settings. The Log collection levels are listed below.

Job Log Collect Level

Level 1

User Settings

Access Log Collect Level

Level 1

Level 2

User Settings

1. **Open a Web browser.**
2. **Enter "http://(system'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 printer.

   The top page of Web Image Monitor appears.
3. **Click [Login].**

   The machine administrator can log on using the appropriate login user name and login password.

4. **Click [Configuration], and then click [Logs] under "Device Settings".**
5. **Select Collect Job Logs to specify Job Log settings, or select Collect Access Logs to specify Access Log settings, and then select [Active].**
6. **Specify the recording levels for either Job Log Collect Level or Access Log Collect Level.**

   The settings shown for "Job Log Collect Settings Listed by Function Type" or "Access Log Collect Settings Listed by Function Type" vary depending on the collection level selected.

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

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

Note

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

Specifying Log Encryption

This can be specified by the machine administrator.

Use the following procedure to enable/disable log encryption.

1. **Open a Web browser.**
2. **Enter "http://(system'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 printer.

   The top page of Web Image Monitor appears.
3. **Click [Login].**

   The machine administrator can log on using the appropriate login user name and login password.
4. **Click [Configuration], and then click [Logs] under "Device Settings".**
5. **Select [Active] under "Encrypt Logs."**

   To disable log encryption, select [Inactive].

   If other changes have been made in related log settings, they will occur at the same time.
6. **Click [OK].**

   A confirmation message appears.
7. **Click [OK].**

   The log is encrypted.
8. **Click [Logout].**

Note

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

Deleting All Logs

This can be specified by the machine administrator.

Use the following procedure to delete all logs stored in the printer.

1. **Open a Web browser.**
2. **Enter "http://(system'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 printer.

   The top page of Web Image Monitor appears.
3. **Click [Login].**

   The machine administrator can log on using the appropriate login user name and login password.
4. **Click [Configuration], and then click [Logs] under "Device Settings".**
5. **Click [Delete] under "Delete All Logs".**
6. **Click [OK].**

   All job logs and device access log records are cleared.
7. **Click [Logout].**

Note

- On this page, "Delete All Logs" does not appear if either Collect Job Logs or Collect Access Logs are not set to [Active].

Downloading Logs

This can be specified by the machine administrator.

Use the following procedure to convert the logs stored in the printer into a CSV file for simultaneous batch download.

1. **Open a Web browser.**
2. **Enter "http://(system'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 printer.

   The top page of Web Image Monitor appears.

3. **Click [Login].**

   The machine administrator can log on using the appropriate login user name and login password.

4. **Click [Configuration], and then click [Download Logs].**
5. **Click [Download].**
6. **Specify the folder in which you want to save the file.**
7. **Click [OK].**
8. **Click [Logout].**

Note

- Downloaded logs contain data recorded up till the time you click the [Download] button. Any logs recorded after the [Download] button is clicked will not be downloaded.
- Downloading is slower if the number of logs is large.
- If an error occurs while the CSV file is downloading or being created, the download is cancelled and details of the error are included at the end of the file.
- For details about saving CSV log files, see your browser's Help.
- Depending on the configuration of your computer, some applications might not be able to display the downloaded CSV files.
- To collect logs, set "Collect Job Logs" and "Collect Access Logs" to [Active]. For details about setting, see Web Image Monitor Help.
- For details about the items contained in the logs, see "Attributes of Logs you can Download".

Reference

- p.100 "Attributes of Logs you can Download"

Logs that can be Managed Using Web Image Monitor

This section details the information items contained in the logs that are created for retrieval by Web Image Monitor.

Logs that can be Collected

The following tables explain the items in the job log and access log that the printer creates when you enable log collection using Web Image Monitor. If you require log collection, use Web Image Monitor to configure it. Web Image Monitor will then download the collected logs. For details, see the Help for Web Image Monitor.

Job Log Information Items

Job Log Item	Content
Printer: Printing	Details of normal print jobs.
Report Printing	Details of reports printed from the control panel.

Access Log Information Items

Access Log Item	Content
Login	Times of login and identity of logged in users.
Logout	Times of logout and identity of logged out users.
HDD Format	Details of hard disk formatting.
All Logs Deletion	Details of deletions of all logs.
Log Setting Change	Details of changes made to log settings.
Transfer Log Error	Details of changes made to log settings.
Log Collection Item Change	Details of changes made to log settings.
Collect Encrypted Communication Logs	Details of changes to job log collection levels, access log collection levels, and types of log collected.
Access Violation	Details of failed access attempts.
Lockout	Details of lockout activation.
Firmware: Update	Details of firmware updates.
Firmware: Structure Change	Details of structure changes that occurred when an SD card was inserted or removed, or when an unsupported SD card was inserted.
Firmware: Structure	Details of checks for changes to firmware module structure made at times such as when the printer was switched on.
Machine Data Encryption Key Change	Details of changes made to encryption keys.
Firmware: Invalid	Details of checks for firmware validity made at times such as when the printer was switched on.
Date/Time Change	Details of changes made to date and time settings.

Access Log Item	Content
Password Change	Details of changes made to the login password.
Administrator Change	Details of changes of administrator.
Address Book Change	Details of changes made to address book entries.

Note

- If "Job Log Collect Level" is set to "Level 1", all job logs are collected.
- If "Access Log Collect Level" is set to "Level 1", the following information items are recorded in the access log:
  - HDD Format
  - All Logs Deletion
  - Log Setting Change
  - Log Collection Item Change
- If "Access Log Collect Level" is set to "Level 2", all access logs are collected.
- If you format the hard disk, a log recording details of the format is created, but all actual logs up to that moment are deleted.

Attributes of Logs you can Download

If you use Web Image Monitor to download logs, a CSV file containing the information items shown in the following table is produced.

Job and Access Log Information Items

Item	Content
Start Date/Time	For a job log entry, indicates the start date and time of the operation. If the job has not been completed, this is blank. For an access log entry, indicates the same date and time as shown by "End Date/Time". This is in Item 1 of the CSV file.
End Date/Time	For a job log entry, indicates the end date and time of the operation. If the operation is still in progress, this will be blank. For an access log entry, indicates the same date and time as shown by "Result". This is Item 2 of the CSV file.

Item	Content
Log Type	Details of the log type. Access logs are classified under "Access Log Type". For details about the information items contained in each type of log, see "Logs that can be Collected". This is Item 3 of the CSV file.
Result	Indicates the result of an operation or event: • If "Succeeded" is displayed for a job log entry, the operation completed successfully; "Failed" indicates the operation was unsuccessful. If the operation is still in progress, this will be blank. • If "Succeeded" is displayed for an access log entry, the event completed successfully; "Failed" indicates the event was unsuccessful.
User Entry ID	ID assigned to the entry.
User Code/User Name	Identifies the user code or user name of the user who performed the operation. If an administrator performed the operation, this ID will contain the login name of that administrator.
Log ID	Identifies the ID that is assigned to the log. This is a hexadecimal ID that identifies the log.

Job Log Information Items

Input Information

Item	Content
Source	Type of the job log source. "Printer" indicates a printer driver job; "Report" indicates a printed report.
Start Date/Time	Dates and times "Printer" operation started. This is Item 52 of the CSV file.
End Date/Time	Dates and times "Printer" operation ended. This is Item 53 of the CSV file.
Print File Name	Name of "Printer" files.

Output Information

Item	Content
Target	Type of the job target. "Print" indicates a print file.
Start Date/Time	Dates and times "Print" operation started. This is Item 58 of the CSV file.
End Date/Time	Dates and times "Print" operation ended. This is Item 59 of the CSV file.

Access Log Information Items

Item	Content
Access Log Type	Indicates the type of access: "Authentication" indicates a user authentication access. "Network Attack Detection/Encrypted Communication" indicates a network attack or encrypted communication access. "Firmware" indicates a firmware verification access.
Logout Mode	Mode of logout. "Manual Logout" indicates a normal logout; "Auto logout" indicates an automatic logout.
Login Method	Identifies the method of login (authorization): "Control Panel" indicates the login was performed through the control panel; "via Network" indicates the login was performed remotely through a network computer; and "Others" indicates the login was performed through another method.

Item	Content
Login User Type	Indicates the type of login user: "User" indicates the logged in user was a registered general user. "Guest" indicates the logged in user was a guest user. "File Administrator" indicates the logged in user was a registered file administrator. "Machine Administrator" indicates the logged in user was a registered machine administrator. "Network Administrator" indicates the logged in user was a registered network administrator. "Supervisor" indicates the logged in user was a registered supervisor. "Custom Engineer (Service Mode)" indicates the logged in user was a customer engineer. "Others" indicates the logged in user did not belong to any of the above types of user.
Target User Entry ID	Indicates the entry ID of the target user. This is a hexadecimal ID that indicates users to whom the following settings are applied: • Lockout • Password Change
Target User Code/User Name	User code or user name of the user whose data was accessed. If the administrator's data was accessed, the administrator's user name is logged.
Lockout/Release	The mode of operation access. "Lockout" indicates activation of password lockout; "Release" indicates deactivation of password lockout.
Lockout/Release Method	"Manual" is recorded if the printer is unlocked manually. "Auto" is recorded if the printer is unlocked by the lockout release timer.
Collect Job Logs	Indicates the status of the job log collection setting: "Active" indicates job log collection is enabled. "Inactive" indicates job log collection is disabled. "Not Changed" indicates no changes have been made to the job log collection setting.

Item	Content
Collect Access Logs	Indicates the status of the access log collection setting: "Active" indicates access log collection is enabled. "Inactive" indicates access log collection is disabled. "Not Changed" indicates no changes have been made to the access log collection setting.
Transfer Logs	Indicates the status of the log transfer setting: "Active" indicates log transfer is enabled. "Inactive" indicates log transfer is disabled. "Not Changed" indicates no changes have been made to the log transfer setting.
Encrypt Logs	Indicates the status of the log encryption setting: "Active" indicates log encryption is enabled. "Inactive" indicates log encryption is disabled. "Not Changed" indicates no changes have been made to the log encryption setting.
Log Type	If a log's collection level setting has been changed, this function indicates details of the change: "Job Log" indicates the Job Log's collection level has been changed. "Access Log" indicates the Access Log's collection level has been changed. "Level 1" indicates a level 1 collection setting. "Level 2" indicates a level 2 collection setting. "User Settings" indicates a user-specified collection level setting. This is Item 24 of the CSV file.
Log Collect Level	Indicates the level of log collection: "Level 1", "Level 2", or "User Settings".
Encryption/Cleartext	Indicates whether communication encryption is enabled or disabled: "Encryption Communication" indicates encryption is enabled; "Cleartext Communication" indicates encryption is disabled.
Machine Port No.	Indicates the printer's port number.

Item	Content
Protocol	Destination protocol. "TCP" indicates the destination's protocol is TCP; "UDP" indicates the destination's protocol is UDP; "Unknown" indicates the destination's protocol could not be identified.
IP Address	Destination IP address.
Port No.	Destination port number. This is in decimal.
MAC Address	Destination MAC (physical) address.
Primary Communication Protocol	Indicates the primary communication protocol name.
Secondary Communication Protocol	Indicates the secondary communication protocol name.
Encryption Protocol	Indicates the protocol used to encrypt the communication.
Communication Direction	Indicates the direction of communication: "Communication Start Request Receiver (In)" indicates the machine received a request to start communication; "Communication Start Request Sender (Out)" indicates the machine sent a request to start communication.
Communication Start Log ID	Indicates the log ID for the communication start time. This is a hexadecimal ID that indicates the time at which the communication started.
Communication Start/End	Indicates the times at which the communication started and ended.

Item	Content
Network Attack Status	Indicates the attack status of the network: "Violation Detected" indicates an attack on the network was detected. "Recovered from Violation" indicates the network recovered from an attack. "Max. Host Capacity Reached" indicates the machine became inoperable due to the volume of incoming data reaching the maximum host capacity. "Recovered from Max. Host Capacity" indicates that the machine became operable again following reduction of the volume of incoming data.
Network Attack Type	Identifies the type of network attack as either "Password Entry Violation" or "Device Access Violation".
Network Attack Type Details	Indicates details about the type of network attack: "Authentication Error" or "Encryption Error".
Network Attack Route	Identifies the route of the network attack as either "Attack from Control Panel" or "Attack from Other than Control Panel".
Login User Name used for Network Attack	Identifies the login user name that the network attack was performed under.
Add/Update/Delete Firmware	Indicates the method used to add, update, or delete the machine's firmware: "Updated with SD Card" indicates an SD card was used to perform the firmware update. "Added with SD Card" indicates an SD card was used to add the firmware. "Deleted with SD Card" indicates an SD card was used to delete the firmware. "Moved to Another SD Card" indicates the firmware was moved to another SD card. "Updated via Remote" indicates the firmware was updated remotely from a computer. "Updated by Other Method" indicates the firmware update was performed using a method other than any of the above.
Module Name	Firmware module name.

Item	Content
Parts Number	Firmware module part number.
Version	Firmware version.
Validity Error File Name	Indicates the name of the file in which a validity error was detected.
Access Result	Indicates the results of logged operations: "Complete" indicates an operation completed successfully; "Failed" indicates an operation completed unsuccessfully.

Note

- Only the items listed here will be printed. Also, an item will be printed only if the log contains data about that item.

Reference

- p.98 "Logs that can be Collected"

6. Enhanced Network Security

This chapter describes how to increase security over the network using the printer's functions.

Preventing Unauthorized Access

You can limit IP addresses, disable ports and protocols, or use Web Image Monitor and Web Interface to specify the network security to prevent unauthorized access over the network and protect the Address Book, and default settings.

Access Control

The printer can control TCP/IP access.

Limit the IP addresses from which access is possible by specifying the access control range.

For example, if you specify the access control range as [192.168.15.16] - [192.168.15.20], the client PC addresses from which access is possible will be from [192.168.15.16] to [192.168.15.20].

Important

- **Using the access control functions of Web Image Monitor, you can limit access over the system network through RCP/RSH, FTP, SSH/SFTP, SMB, and Web Image Monitor. You cannot limit access involving telnet or SNMP.**
- **Using the access control functions of Printer Features and Web Interface, you can limit access over the printing network through HTTP, IPP, SSL, LPR/LPD, DIPRINT, RHPP, SNMP, and Web Interface.**

Reference

- p.109 "Specifying Access Control for the System Network"
- p.110 "Specifying Access Control for the Printing Network"

Specifying Access Control for the System Network

Only the network administrator can specify access control for the system network.

Using Web Image Monitor to Specify Access Control

This can be specified by the network administrator.

1. **Open a Web browser.**
2. **Enter "http://(system'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 printer.

The top page of Web Image Monitor appears.

3. **Click [Login].**

   The network administrator can log on using the appropriate login user name and login password.

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

   The Access Control page appears.

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

   To specify the IPv6 Address, enter an IP address that has access to the printer 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].**

6 Specifying Access Control for the Printing Network

Only the Printer Features administrator can specify access control for the printing network.

Specifying Access Control (Printer Features)

This must be specified by the Printer Features administrator.

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

2. **Press [Printer Features].**

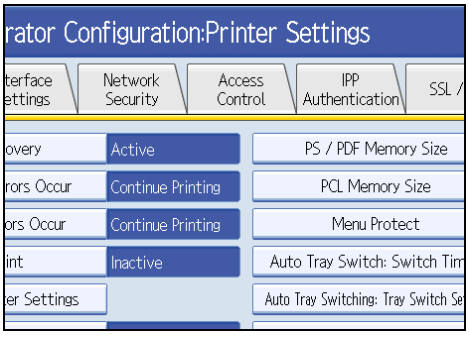
   If user authentication is in operation, an authentication message will appear. To log on, enter the login user name and password.

3. **Press [Administrator Configuration].**

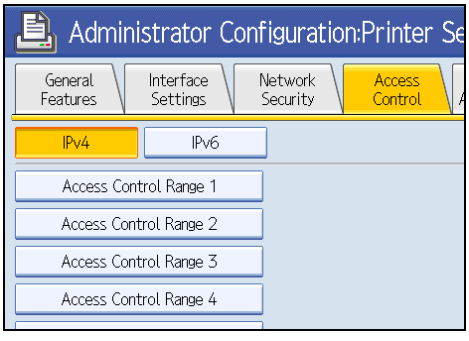
4. **Press [Printer Settings].**

   If a message requesting you to enter a password appears, enter the password for printer settings.

5. **Press [Access Control].**

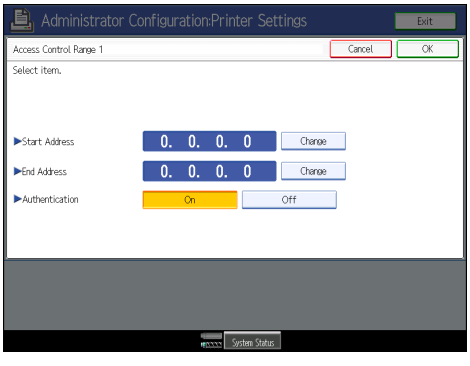


6. **Select [IPv4], and then press an access control range between [Access Control Range 1] and [Access Control Range 5].**



If you need to configure this setting for IPv6 addresses, select "IPv6", and then press one of the access control ranges between [Access Control Range 1] and [Access Control Range 5].

7. **Enter the range of IP addresses that are allowed access to the printer.**



If you need to configure this setting for IPv6 addresses, select "Range", and enter the range of allowed IP addresses. Alternatively, select "Mask", and enter the range of allowed IP addresses as the "Mask Length" and specify the "Mask Value".

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

Note

- The "Authentication" setting specified here will be used to specify user authentication. For details about user authentication, see "Enabling User Authentication".

Reference

- p.45 "Enabling User Authentication"

Using Web Interface to Specify Access Control

This must be specified by the Printer Features administrator.

1. **Open a Web browser.**
2. **Enter "http://(printer'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 printer.

   The top page of Web Interface appears.
3. **Click [Configurations/Jobs].**

   An authentication dialog box appears.
4. **Enter the login user name and password, and then click [OK].**

   Enter "system" as the login user name and the password for printer settings as the login password.
5. **Click [Printer Settings], and then click [IPv4 Access Control] under "Security".**

   To configure this setting for an IPv6 address, click [IPv6 Access Control].
6. **In "Access Control Range", enter the range of IP addresses that are allowed access to the printer.**

   If you need to configure this setting for IPv6 addresses, select "Range", and enter the range of allowed IP addresses. Alternatively, select "Mask", and enter the range of allowed IP addresses and specify the "Mask Length".
7. **Click [OK].**

   Access control is set.
8. **Close the Web browser.**

   You will be logged off.

Note

- The "Authentication" setting specified here will be used to specify user authentication. For details about user authentication, see "Enabling User Authentication".

Reference

- p.45 "Enabling User Authentication"

Enabling and Disabling Protocols

Specify whether to enable or disable the function for each protocol. By making this setting, you can specify which protocols are available and so prevent unauthorized access over the network. Network settings can be specified on the control panel, or using Web Image Monitor, Web Interface or telnet. For details about making settings using telnet, see "Remote Maintenance by telnet ", Network and System Settings Guide. To disable SMTP on Web Image Monitor, in E-mail settings, set the protocol to anything other than SMTP. For details, see Web Image Monitor Help.

Protocol	Port	Setting Method	When Disabled
IPv4	-	• Control Panel • Web Image Monitor • Web Interface • telnet	All applications that operate over IPv4 cannot be used. IPv4 cannot be disabled from Web Image Monitor when using IPv4 transmission.
IPv6	-	• Control Panel • Web Image Monitor • Web Interface • telnet	All applications that operate over IPv6 cannot be used.
IPsec	-	• Control Panel • Web Image Monitor • telnet	Encrypted transmission using IPsec is disabled.
FTP	TCP: 21	• Web Image Monitor • telnet	Functions that require FTP cannot be used. You can restrict personal information from being displayed by making settings on the control panel using "Restrict Display of User Information".

Protocol	Port	Setting Method	When Disabled
ssh/sftp	TCP: 22	• Web Image Monitor • telnet	Functions that require sftp cannot be used. You can restrict personal information from being displayed by making settings on the control panel using "Restrict Display of User Information".
telnet	TCP: 23	• Web Image Monitor	Commands using telnet are disabled.
SMTP	TCP: 25 (variable)	• Control Panel • Web Image Monitor	E-mail notification that requires SMTP reception cannot be used.
HTTP	TCP: 80	• Control Panel • Web Image Monitor • Web Interface • telnet	Functions that require HTTP cannot be used. Cannot print using IPP on port 80.
HTTPS	TCP: 443	• Web Image Monitor • Web Interface • telnet	Functions that require HTTPS cannot be used. @Remote cannot be used. You can also make settings to require SSL transmission using the control panel, Web Image Monitor or Web Interface.
SMB	TCP: 139	• Control Panel • Web Image Monitor • telnet	SMB printing functions cannot be used.

Protocol	Port	Setting Method	When Disabled
NBT	UDP: 137 UDP: 138	• telnet	SMB printing functions via TCP/IP, as well as NetBIOS designated functions on the WINS server cannot be used.
SNMPv1,v2 (SNMP)	UDP: 161	• Control panel • Web Image Monitor • Web Interface • telnet	Functions that require SNMPv1, v2 cannot be used. Using the control panel, Web Image Monitor or telnet, you can specify that SNMPv1, v2 settings are read-only, and cannot be edited.
SNMPv3	UDP: 161	• Web Image Monitor • telnet	Functions that require SNMPv3 cannot be used. You can also make settings to require SNMPv3 encrypted transmission and restrict the use of other transmission methods using the control panel, Web Image Monitor, or telnet.
RSH/RCP	TCP: 514	• Web Image Monitor • telnet	Functions that require 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".

Protocol	Port	Setting Method	When Disabled
LPR/LPD	TCP: 515	• Control Panel • Web Interface	LPR/LPD functions cannot be used. You can restrict personal information from being displayed by making settings on the control panel using "Restrict Display of User Information".
IPP	TCP: 631	• Control Panel • Web Interface	IPP functions cannot be used.
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.
DIPRINT	TCP: 9100	• Control Panel • Web Interface	DIPRINT functions cannot be used.
RFU	TCP: 10021	• telnet	You can attempt to update firmware via FTP.
AppleTalk	(PAP)	• Control Panel • Web Interface	Cannot print with AppleTalk.
RHPP	TCP: 59100	• Web Interface	Cannot print with RHPP.

Note

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

Reference

- p.173 "Specifying the Extended Security Functions"
- p.117 "Configuring Protocols for the System Network"
- p.121 "Configuring Protocols for the Printing Network"

Configuring Protocols for the System Network

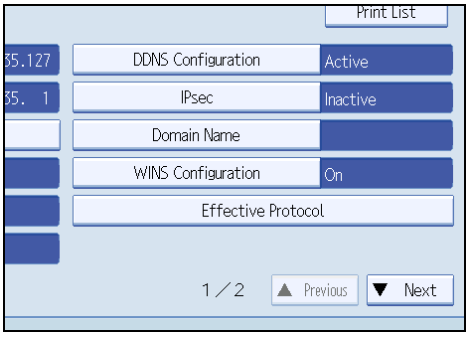
The network administrator can enable or disable each available system network protocol.

Enabling/Disabling Protocols (System Settings)

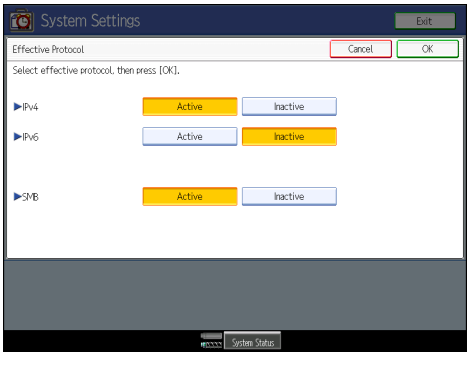
This can be specified by the network administrator.

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

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

Reference

- p.33 "Logging on Using Administrator Authentication"

- p.34 "Logging off Using Administrator Authentication"

Using Web Image Monitor to Enable/Disable Protocols

This can be specified by the network administrator.

1. **Open a Web browser.**
2. **Enter "http://(system'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 printer.

   The top page of Web Image Monitor appears.
3. **Click [Login].**

   The network administrator can log on.

   Enter the login user name and login password.
4. **Click [Configuration], and then click [Network Security] under "Security".**
5. **Set the desired protocols to active/inactive (or open/close).**
6. **Click [OK].**
7. **Click [OK].**
8. **Click [Logout].**

Note

- To disable SMTP from Web Image Monitor, specify a protocol other than SMTP as the mail receiving protocol. See Web Image Monitor help for instructions to configure this setting.
- For details about how to configure telnet, see "Using telnet", Network and System Settings Guide.

Specifying Network Security Level

You can select one of three security levels. Based on the security level you select, the printer will automatically determine which protocols to enable. Use this setting to change the security level of the system network. 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 printer 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.

Note

- The security settings for the printing network cannot be specified in a single operation. Each protocol must be enabled/disabled individually. For details about configuring the protocols, see "Configuring Protocols for the Printing Network".

Reference

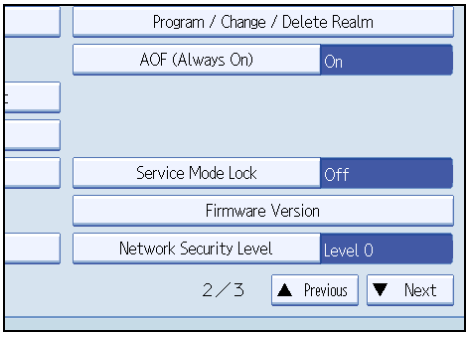
- p.121 "Configuring Protocols for the Printing Network"

Specifying Network Security Level (System Settings)

This can be specified by the network administrator.

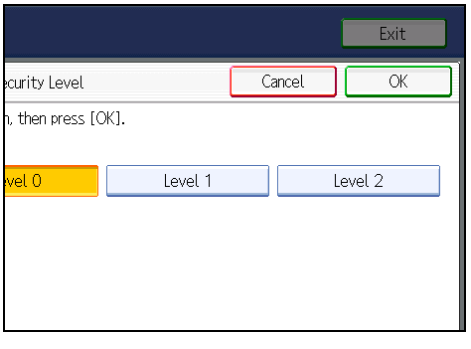
For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

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



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

5. **Select the network security level.**



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

6. **Press [OK].**
7. **Press [Exit].**
8. **Press the [User Tools] key.**

Reference

- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"

Specifying Network Security Level Using Web Image Monitor

This can be specified by the network administrator.

1. **Open a Web browser.**
2. **Enter "http://(system'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 printer.

   The top page of Web Image Monitor appears.
3. **Click [Login].**

   The network administrator can log on.

   Enter the login user name and login password.
4. **Click [Configuration], and then click [Network Security] under "Security".**
5. **Select the network security level in "Security Level".**
6. **Click [OK].**
7. **Click [OK].**
8. **Click [Logout].**

Status of Functions under Each Network Security Level

Tab Name: TCP/IP

Function	Level 0	Level 1	Level 2
TCP/IP	Active	Active	Active
HTTP> Port 80	Open	Open	Open
SSL/TLS> Port 443	Open	Open	Open
SSL/TLS> Permit SSL/TLS Communication	Ciphertext Priority	Ciphertext Priority	Ciphertext Only

Function	Level 0	Level 1	Level 2
SSL/TLS> Certificate Status	None	None	None
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: 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

Configuring Protocols for the Printing Network

The Printer Features administrator can enable or disable each available printing network protocol.

Enabling/Disabling Protocols (Printer Features)

This must be specified by the Printer Features administrator.

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

2. **Press [Printer Features].**

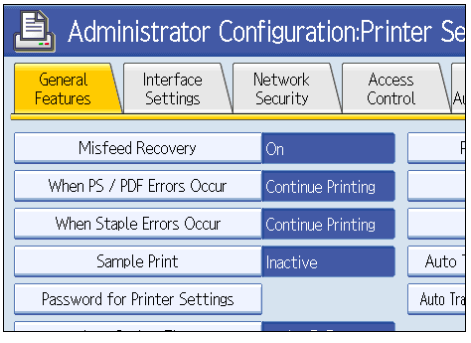
   If user authentication is in operation, an authentication message will appear. To log on, enter the login user name and password.

3. **Press [Administrator Configuration].**

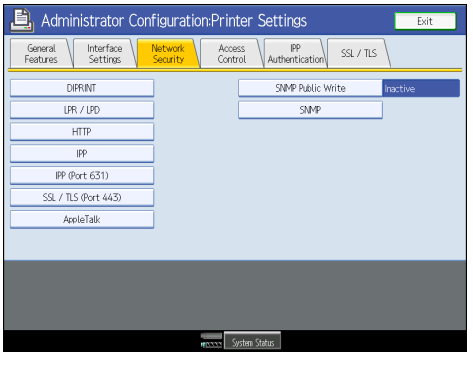
4. **Press [Printer Settings].**

   If a message requesting you to enter a password appears, enter the password for printer settings.

5. **Press [Network Security].**



6. **Press the protocol you require.**



7. **Select whether or not to enable the protocol, and then press [OK].**

8. **According to the displayed message, turn the main power switch off and then back on.**

   After changing the protocol from "Active" to "Inactive", you do not need to switch the main power off and then back on.

Note

- With AppleTalk, you must switch the main power off and then back on whenever you change the protocol setting from "Active" to "Inactive" or vice versa.

Using Web Interface to Enable/Disable Protocols

This must be specified by the Printer Features administrator.

1. **Open a Web browser.**
2. **Enter "http://(printer'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 printer.

   The top page of Web Interface appears.
3. **Click [Configurations/Jobs].**

   An authentication dialog box appears.
4. **Enter the login user name and password, and then click [OK].**

   Enter "system" as the login user name and enter the password for printer settings as the login password.
5. **Click [Printer Settings], and then click [Network Security] under "Security".**
6. **Set the desired protocols to active/inactive (or open/close).**
7. **Click [OK].**
8. **Close the Web browser.**

   You will be logged off.
9. **Turn the main power switch off and then back on.**

   For details about how to turn the main power on and off, see "Turning On/Off the Power", About This Machine.

   The specified setting is applied after the printer is switched off and then back on.

   After changing the protocol from "Active" (or "Open") to "Inactive" (or "Close"), you do not need to switch the main power off and then back on.

Note

- With AppleTalk, you must switch the main power off and then back on whenever you change the protocol setting from "Active" to "Inactive" or vice versa.

Encrypting Transmitted Passwords

Prevent login passwords and IPP authentication passwords from being revealed by encrypting them for transmission.

Also, encrypt the login password for administrator authentication and user authentication.

Driver Encryption Key

Encrypt the password transmitted when specifying user authentication.

To encrypt the login password, specify the driver encryption key on the printer and on the printer driver installed in the user's computer.

Password for IPP Authentication

To encrypt the IPP Authentication password on Web Interface, set "Authentication" to [DIGEST], and then specify the IPP Authentication password set on the printer.

Specifying a Driver Encryption Key

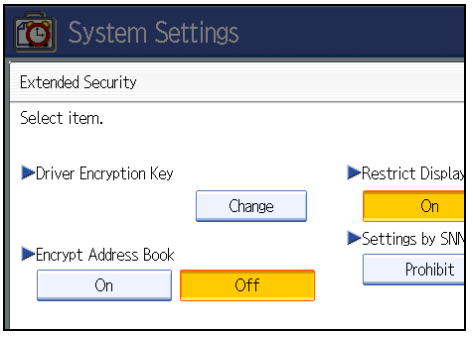
This can be specified by the network administrator.

Specify the driver encryption key on the printer. By making this setting, you can encrypt login passwords for transmission to prevent them from being analyzed.

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

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

   If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.
5. **For "Driver Encryption Key", press [Change].**



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

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

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

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

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

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

Reference

- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"
- p.173 "Specifying the Extended Security Functions"

Specifying an IPP Authentication Password

This must be specified by the Printer Features administrator.

Specify the IPP authentication passwords for the printer using Web Interface.

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

1. **Open a Web browser.**
2. **Enter "http://(printer'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 printer.

   The top page of Web Interface appears.

3. **Click [Configurations/Jobs].**

   An authentication dialog box appears.

4. **Enter the login user name and password, and then click [OK].**

   Enter "system" as the login user name and enter the password for printer settings as the login password.

5. **Click [Printer Settings], and then click [IPP Authentication] under "Security".**
6. **Select [DIGEST] from the "Authentication" list.**
7. **Enter the user name in the "User Name" box.**
8. **Click [Change] next to "Password".**

9. **Enter the password, and then click [OK].**
10. **Click [OK].**
11. **Close the Web browser.**

    You will be logged off.

Note

- To use the IPP port under Windows 2000/XP or Windows Server 2003/2003 R2, select the operating system's standard IPP port. Note that the IPP port cannot be used on an IPv6 network.
- This printer does not support the IPP port under Windows Vista/7 and Windows Server 2008/2008 R2.
- You can also apply IPP authentication using the control panel.

Protection Using Encryption

Establish encrypted transmission on this printer 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.

Important

- **IPsec is not effective for the printing network.**

This printer requires certificates for network communication using SSL, IPsec, or IEEE802.1X. Install the certificates in both the system and printer interface. You can share certificates under SSL, IPsec, and IEEE802.1X. The following certificates are necessary if you want to use one of these protocols:

- SSL: two device certificates are required, one for the system interface and one for the printer interface.
- IPsec: a device certificate for the system interface is required if "Encryption Key Auto Exchange Setting" is set to authentication by certificate.
- IEEE802.1X: two device certificates are required, one for the system interface and one for the printer interface. (Depending on the EAP type, a site certificate for both the system interface and the printer interface may also required for IEEE8021.X.)

Note

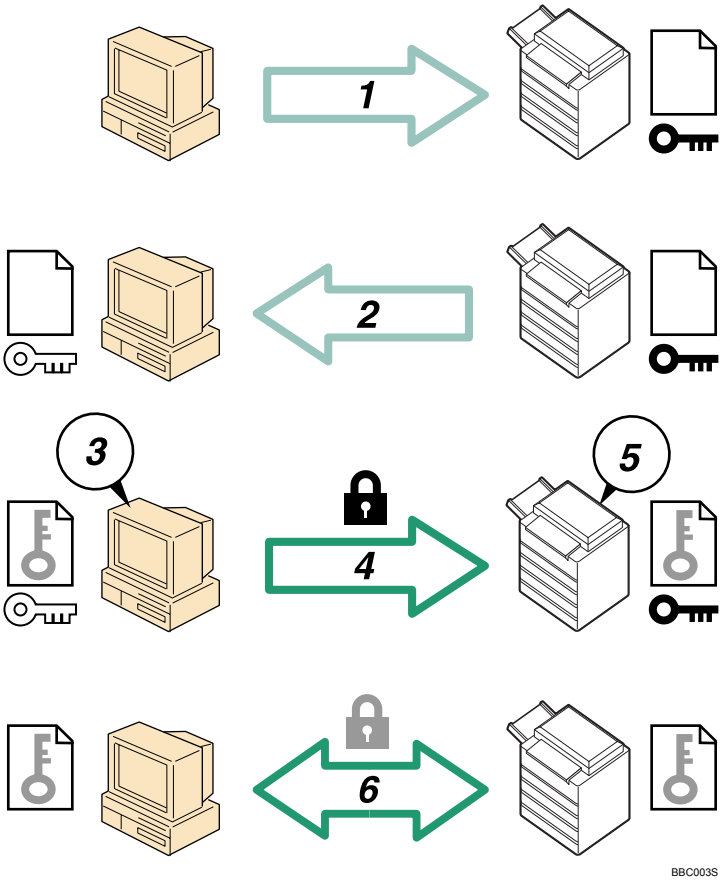
- Install the certificate for the system interface via Web Image Monitor, and install the certificate for the printer interface via Web Interface.
- Depending on the configuration of the machine's security settings, certificates may not be required.

SSL (Encrypted Communication)

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 printer, or request a certificate from a certificate authority and install it.

SSL (Secure Sockets Layer)



1. **To access the printer from a user's computer, request the SSL device certificate and public key.**
2. **The device certificate and public key are sent from the printer to the user's computer.**
3. **Create a shared key from the user's computer, and then encrypt it using the public key.**
4. **The encrypted shared key is sent to the printer.**
5. **The encrypted shared key is decrypted in the printer using the private key.**
6. **Transmit the encrypted data using the shared key, and the data is then decrypted at the printer to attain secure transmission.**

Configuration flow (self-signed certificate)

1. Creating and installing the device certificate

   Install the device certificate using Web Image Monitor/Web Interface.
2. Enabling SSL

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

Configuration flow (certificate issued by a certificate authority)

1. Creating the device certificate

   Create the device certificate using Web Image Monitor/Web Interface.

   The application procedure after creating the certificate depends on the certificate authority. Follow the procedure specified by the certificate authority.

2. Installing the device certificate

   Install the device certificate using Web Image Monitor/Web Interface.

3. Enabling SSL

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

Note

- To confirm whether SSL configuration is enabled, enter "https://(IP address or host name)/" in your Web browser's address bar to access this printer. If the "The page cannot be displayed" message appears, check the configuration because the current SSL configuration is invalid.
- If you enable SSL for IPP (printer functions), sent data is encrypted, preventing it from being intercepted, analyzed, or tampered with.

Reference

- p.129 "Specifying SSL for the System Network"
- p.133 "Specifying SSL for the Printing Network"

Specifying SSL for the System Network

Only the network administrator can specify SSL for the system network.

Using Web Image Monitor to Create and Install the Device Certificate (Self-Signed)

This can be specified by the network administrator.

You can create and install the device certificate using Web Image Monitor. For details about the displayed items and selectable items, see Web Image Monitor Help.

Use the following procedure to apply a self-signed certificate as the device certificate.

1. **Open a Web browser.**
2. **Enter "http://(system'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 printer.

   The top page of Web Image Monitor appears.

3. **Click [Login].**

   The network administrator can log on.

   Enter the login user name and login password.

4. **Click [Configuration], and then click [Device Certificate] under "Security".**
5. **Click [Certificate1].**
6. **Click [Create].**
7. **Make the necessary settings.**
8. **Click [OK].**

   The setting is changed.

9. **Click [OK].**

   A security warning dialog box appears.

10. **Check the details, and then click [OK].**

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

11. **Click [Logout].**

Note

- Click [Delete] to delete the device certificate from the printer.

Using Web Image Monitor to Create the Device Certificate (issued by a Certificate Authority)

This can be specified by the network administrator.

You can create the device certificate using Web Image Monitor. For details about the displayed items and selectable items, see Web Image Monitor Help.

Use the following procedure to apply a certificate issued by a certificate authority as the device certificate.

1. **Open a Web browser.**
2. **Enter "http://(system'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 printer.

   The top page of Web Image Monitor appears.

3. **Click [Login].**

   The network administrator can log on.

   Enter the login user name and login password.

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

   The Device Certificate page appears.

5. **Click [Certificate1].**
6. **Click [Request].**
7. **Make the necessary settings.**
8. **Click [OK].**

   The setting is changed.
9. **Click [OK].**

   "Requesting" appears for "Certificate Status".
10. **Click [Logout].**
11. **Apply to the certificate authority for the device certificate.**

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

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

Note

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

Using Web Image Monitor to Install the Device Certificate (issued by a Certificate Authority)

This can be specified by the network administrator.

You can install the device certificate using Web Image Monitor. For details about the displayed items and selectable items, see Web Image Monitor Help.

Use the following procedure to apply a certificate issued by a certificate authority as the device certificate.

1. **Open a Web browser.**
2. **Enter "http://(system'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 printer.

   The top page of Web Image Monitor appears.
3. **Click [Login].**

   The network administrator can log on.

   Enter the login user name and login password.

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

   The Device Certificate page appears.

5. **Click [Certificate1].**
6. **Click [Install].**
7. **Open the certificate sent from the certificate authority in a text editor, and then copy all the text.**
8. **Paste all the copied text into the "Certificate Request" box.**
9. **Click [OK].**

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

10. **Click [Logout].**

Enabling SSL (System Settings)

This can be specified by the network administrator.

After installing the device certificate in the printer, enable the SSL setting.

Use the following procedure to apply a self-signed certificate or a certificate issued by a certificate authority.

1. **Open a Web browser.**
2. **Enter "http://(system'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 printer.

   The top page of Web Image Monitor appears.

3. **Click [Login].**

   The network administrator can log on.

   Enter the login user name and login password.

4. **Click [Configuration], and then click [SSL/TLS] under "Security".**

   The SSL/TLS page appears.

5. **Click [Active] for the protocol version used in "SSL/TLS".**
6. **Select the encryption communication mode for "Permit SSL/TLS Communication".**
7. **Click [OK].**

   The SSL setting is enabled.

8. **Click [OK].**
9. **Click [Logout].**

Note

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

Specifying SSL for the Printing Network

The Printer Features administrator can configure the printing network for use with SSL.

Using Web Interface to Create and Install the Device Certificate (Self-Signed)

This must be specified by the Printer Features administrator.

You can create and install the device certificate using Web Interface. Use the following procedure to apply a self-signed certificate as the device certificate.

1. **Open a Web browser.**
2. **Enter "http://(printer'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 printer.

   The top page of Web Interface appears.
3. **Click [Configurations/Jobs].**

   An authentication dialog box appears.
4. **Enter the login user name and password, and then click [OK].**

   Enter "system" as the login user name and enter the password for printer settings as the login password.
5. **Click [Printer Settings], and then click [Device Certificate] under "Security".**
6. **Click [Certificate1].**
7. **Click [Create].**
8. **Make the necessary settings.**
9. **Click [OK].**

   A security warning dialog box appears.
10. **Check the details, and then click [OK].**

    "Imported" appears under "Certificate Status" to show that a device certificate for the printer has been installed.
11. **Click [OK].**
12. **Close the Web browser.**

    You will be logged off.

Using Web Interface to Create the Device Certificate (issued by a Certificate Authority)

This must be specified by the Printer Features administrator.

You can create the device certificate using Web Interface. Use the following procedure to apply a certificate issued by a certificate authority as the device certificate.

1. **Open a Web browser.**
2. **Enter "http://(printer'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 printer.

   The top page of Web Interface appears.
3. **Click [Configurations/Jobs].**

   An authentication dialog box appears.
4. **Enter the login user name and password, and then click [OK].**

   Enter "system" as the login user name and enter the password for printer settings as the login password.
5. **Click [Printer Settings], and then click [Device Certificate] under "Security".**
6. **Click [Certificate1].**
7. **Click [Request].**
8. **Make the necessary settings.**
9. **Click [OK].**

   "Requesting" appears for "Certificate Status".
10. **Click [OK].**
11. **Close the Web browser.**

    You will be logged off.
12. **Apply to the certificate authority for the device certificate.**

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

    For the application, click Web Interface Details icon and use the information that appears in "Text for Requested Certificate".

Note

- The issuing location may not be displayed if you request two certificates at the same time. When you install a certificate, be sure to check the certificate destination and installation procedure.
- Using Web Interface, 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.

Using Web Interface to Install the Device Certificate (issued by a Certificate Authority)

This must be specified by the Printer Features administrator.

You can install the device certificate using Web Interface. Use the following procedure to apply a certificate issued by a certificate authority as the device certificate.

1. **Open a Web browser.**
2. **Enter "http://(printer'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 printer.

   The top page of Web Interface appears.
3. **Click [Configurations/Jobs].**

   An authentication dialog box appears.
4. **Enter the login user name and password, and then click [OK].**

   Enter "system" as the login user name and enter the password for printer settings as the login password.
5. **Click [Printer Settings], and then click [Device Certificate] under "Security".**
6. **Click [Certificate1].**
7. **Click [Import].**
8. **Open the certificate sent from the certificate authority in a text editor, and then copy all the text.**
9. **In "Import Format", select "Text", and then paste all the copied text into the "Text" box.**

   If you selected "File" in "Import Format", specify the file location.
10. **Click [OK].**

    "Import" appears under "Certificate Status" to show that a device certificate for the printer has been installed.
11. **Click [OK].**
12. **Close the Web browser.**

    You will be logged off.

Enabling SSL (Printer Features)

This must be specified by the Printer Features administrator.

After installing the device certificate in the printer, enable the SSL setting.

Use the following procedure to apply a self-signed certificate or a certificate issued by a certificate authority.

1. **Open a Web browser.**

2. **Enter "http://(printer'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 printer.

   The top page of Web Interface appears.

3. **Click [Configurations/Jobs].**

   An authentication dialog box appears.

4. **Enter the login user name and password, and then click [OK].**

   Enter "system" as the login user name and enter the password for printer settings as the login password.

5. **Click [Printer Settings], and then click [SSL/TLS] under "Security".**
6. **Click [Active] for the protocol version used in "SSL/TLS".**
7. **Select the encryption communication mode for "Permit SSL/TLS Communication".**
8. **Click [OK].**

   The SSL setting is enabled.

9. **Close the Web browser.**

   You will be logged off.

Note

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

User Settings for SSL (Secure Sockets Layer)

If you have installed a device certificate using a self-signed certificate and enabled Secure Sockets Layer (SSL), a warning message may appear whenever you access the printer using Web Image Monitor, Web Interface, or IPP. To stop this message from appearing, install the certificate using the procedure for your particular browser. The network administrator or Printer Features administrator must explain to users that to prevent the warning dialog box from appearing, the user must install the certificate him/herself.

Note

- Take the appropriate steps when you receive a user's inquiry concerning problems such as an expired certificate.
- For details about how to install the certificate and about where to store the certificate when accessing the printer using IPP, see Web Interface Help.
- If a certificate issued by a certificate authority is installed in the printer, 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 printer does not communicate.
Ciphertext Priority	Performs encrypted communication if encryption is possible. If encryption is not possible, the printer communicates without it.
Ciphertext / Cleartext	Communicates with or without encryption, according to the setting.

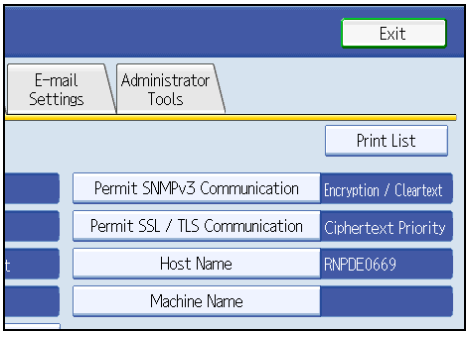
Specifying SSL/TLS Encryption Mode for the System Network

This can be specified by the network administrator.

After installing the device certificate, specify the SSL/TLS encrypted communication mode. By making this setting, you can change the security level.

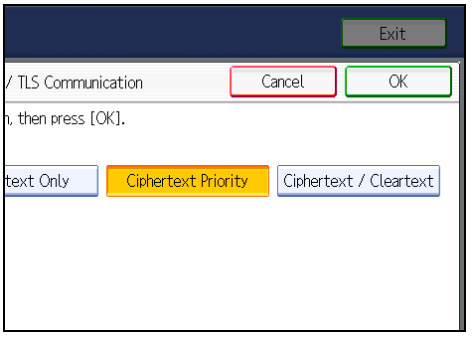
For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

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



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

5. **Select the encrypted communication mode.**



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

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

6

Note

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

Reference

- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"

Specifying SSL/TLS Encryption Mode for the Printing Network

This must be specified by the Printer Features administrator.

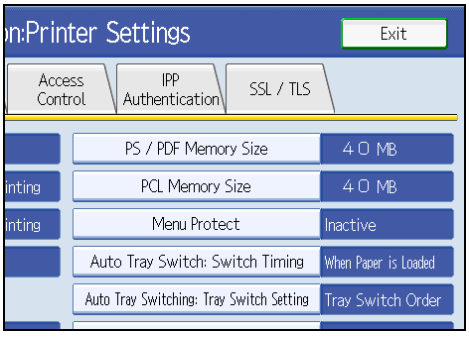
After installing the device certificate, specify the SSL/TLS encrypted communication mode. By making this setting, you can change the security level.

1. **Press the [User Tools] key.**
2. **Press [Printer Features].**

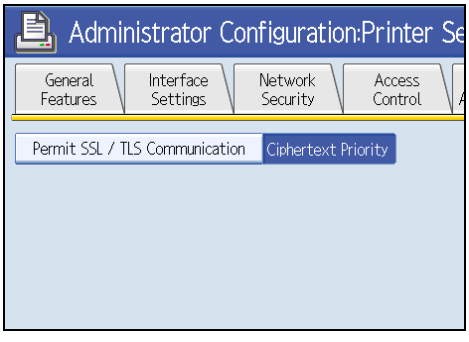
   If user authentication is in operation, an authentication message will appear. To log on, enter the login user name and password.
3. **Press [Administrator Configuration].**
4. **Press [Printer Settings].**

   If a message requesting you to enter a password appears, enter the password for printer settings.

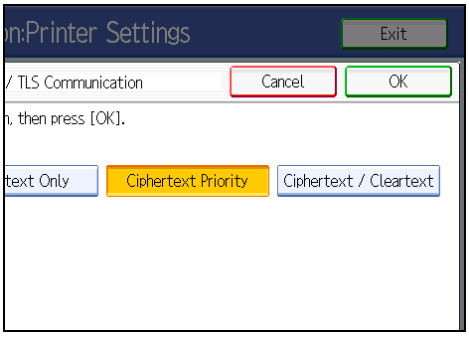
5. **Press [SSL / TLS].**



6. **Press [Permit SSL / TLS Communication].**



7. **Select the encrypted communication mode.**



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

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

Note

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

SNMPv3 Encryption

This can be specified by the network administrator.

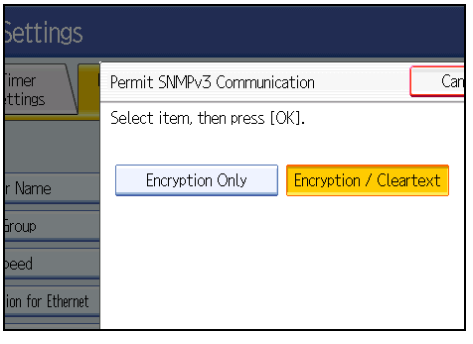
When using Web Image Monitor or another application to make various settings, you can encrypt the data transmitted.

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

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

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

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



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

Note

- If network administrator's [Encryption Password] setting is not specified, the data for transmission may not be encrypted or sent. For details about specifying the network administrator's [Encryption Password] setting, see "Registering the Administrator".

Reference

- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"
- p.30 "Registering the Administrator"

Transmission Using IPsec

This can be specified by the network administrator.

For communication security, this printer 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 printer has two methods that you can use to specify the shared encryption key for both parties: encryption key auto exchange and encryption key manual settings. Using the auto exchange setting, you can renew the shared key exchange settings within a specified validity period, and achieve higher transmission security.

Important

- **This setting is not effective for the printing network.**
- **When "Inactive" is specified for "Exclude HTTPS Communication", access to Web Image Monitor can be lost if the key settings are improperly configured. In order to prevent this, you can specify IPsec to exclude HTTPS transmission by selecting "Active". When you want to include HTTPS transmission, we recommend that you select "Inactive" for "Exclude HTTPS Communication" after confirming that IPsec is properly configured. When "Active" is selected for "Exclude HTTPS Communication", even though HTTPS transmission is not targeted by IPsec, Web Image Monitor might become unusable when TCP is targeted by IPsec from the computer side. If you cannot access Web Image Monitor due to IPsec configuration problems, disable IPsec in System Settings on the control panel, and then access Web Image Monitor. For details about enabling and disabling IPsec using the control panel, see "System Settings", Network and System Settings Guide.**
- **IPsec is not applied to data obtained through DHCP, DNS, or WINS.**
- **IPsec compatible operating systems are Windows XP SP2, Windows Vista, Windows Server 2003/2003 R2, Mac OS X 10.5 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 printer's IPsec function supports two security protocols: the ESP protocol, which enables both of the IPsec functions at the same time, and the AH protocol, which enables only the authentication function.

ESP Protocol

The ESP protocol provides secure transmission through both encryption and authentication. This protocol does not provide header authentication.

- For successful encryption, both the sender and receiver must specify the same encryption algorithm and encryption key. If you use the encryption key auto exchange method, the encryption algorithm and encryption key are specified automatically.

- For successful authentication, the sender and receiver must specify the same authentication algorithm and authentication key. If you use the encryption key auto exchange method, the authentication algorithm and authentication key are specified automatically.

AH Protocol

The AH protocol provides secure transmission through authentication of packets only, including headers.

- For successful authentication, the sender and receiver must specify the same authentication algorithm and authentication key. If you use the encryption key auto exchange method, the authentication algorithm and authentication key are specified automatically.

AH Protocol + ESP Protocol

When combined, the ESP and AH protocols provide secure transmission through both encryption and authentication. These protocols provide header authentication.

- For successful encryption, both the sender and receiver must specify the same encryption algorithm and encryption key. If you use the encryption key auto exchange method, the encryption algorithm and encryption key are specified automatically.
- For successful authentication, the sender and receiver must specify the same authentication algorithm and authentication key. If you use the encryption key auto exchange method, the authentication algorithm and authentication key are specified automatically.

Note

- Some operating systems use the term "Compliance" in place of "Authentication".

Encryption Key Auto Exchange Settings and Encryption Key Manual Settings

This printer 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' printers. However, before setting the IPsec SA, the ISAKMP SA (Phase 1) settings are auto configured. After this, the IPsec SA (Phase 2) settings, which allow actual IPsec transmission, are auto configured.

Also, for further security, the SA can be periodically auto updated by applying a validity period (time limit) for its settings. This printer only supports IKEv1 for encryption key auto exchange.

If you specify the encryption key manually, the SA settings must be shared and specified identically by both parties. To preserve the security of your SA settings, we recommend that they are not exchanged over a network.

Note that for both the manual and auto method of encryption key specification, multiple settings can be configured in the SA.

Settings 1-4 and Default Setting

Using either the manual or auto exchange method, you can configure four separate sets of SA details (such as different shared keys and IPsec algorithms). In the default settings of these sets, you can include settings that the fields of sets 1 to 4 cannot contain.

When IPsec is enabled, set 1 has the highest priority and 4 has the lowest. You can use this priority system to target IP addresses more securely. For example, set the broadest IP range at the lowest priority (4), and then set specific IP addresses at a higher priority level (3 and higher). This way, when IPsec transmission is enabled for a specific IP address, the higher level security settings will be applied.

IPsec Settings

IPsec settings for this printer can be made on Web Image Monitor. The following table explains individual setting items.

Encryption Key Auto Exchange / Manual Settings - Shared Settings

Setting	Description	Setting Value
IPsec	Specify whether to enable or disable IPsec.	• Active • Inactive
Exclude HTTPS Communication	Specify whether to enable IPsec for HTTPS transmission.	• Active • Inactive Specify "Active" if you do not want to use IPsec for HTTPS transmission.
Encryption Key Manual Settings	Specify whether to enable Encryption Key Manual Settings, or use Encryption Key Auto Exchange Settings only.	• Active • Inactive Specify "Active" if you want to use "Encryption Key Manual Exchange Settings".

Encryption Key Auto Exchange Security Level

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

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

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

Setting	Authentication Only	Authentication and Low Level Encryption	Authentication and High Level Encryption
Security Policy	Apply	Apply	Apply
Encapsulation Mode	Transport	Transport	Transport
IPsec Requirement Level	Use When Possible	Use When Possible	Always Require
Authentication Method	PSK	PSK	PSK
Phase 1 Hash Algorithm	MD5	SHA1	SHA1
Phase 1 Encryption Algorithm	DES	3DES	3DES
Phase 1 Diffie-Hellman Group	2	2	2

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

Encryption Key Auto Exchange Setting Items

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

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

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 system's IP address. If you are using multiple addresses in IPv6, you can also specify an address range.	The system's IPv4 or IPv6 address. If you are not setting an address range, enter 32 after an IPv4 address, or enter 128 after an IPv6 address.

Setting	Description	Setting Value
Remote Address	Specify the address of the IPsec transmission partner. You can also specify an address range.	The IPsec transmission partner's IPv4 or IPv6 address. If you are not setting an address range, enter 32 after an IPv4 address, or enter 128 after an IPv6 address.
Security Policy	Specify how IPsec is handled.	• apply • bypass • discarded
Encapsulation Mode	Specify the encapsulation mode. (auto setting)	• Transport • Tunnel (Tunnel beginning address - Tunnel ending address) If you specify "Tunnel", you must then specify the "Tunnel End Points", which are the beginning and ending IP addresses. Set the same address for the beginning point as you set in "Local Address".
IPsec Requirement Level	Specify whether to only transmit using IPsec, or to allow cleartext transmission when IPsec cannot be established. (auto setting)	• Use When Possible • Always Require
Authentication Method	Specify the method for authenticating transmission partners. (auto setting)	• PSK • Certificate If you specify PSK, you must then set the PSK text (using ASCII characters). If you specify Certificate, the certificate for IPsec must be installed and specified before it can be used.

Setting	Description	Setting Value
PSK Text	Specify the pre-shared key for PSK authentication.	Enter the pre-shared key required for PSK authentication.
Phase 1 Hash Algorithm	Specify the hash algorithm to be used in phase 1. (auto setting)	• 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.).
Phase 2 Security Protocol	Specify the security protocol to be used in Phase 2. To apply both encryption and authentication to sent data, specify ESP or ESP+AH. To apply authentication data only, specify AH. (auto setting)	• ESP • AH • ESP+AH
Phase 2 Authentication Algorithm	Specify the authentication algorithm to be used in phase 2. (auto setting)	• HMAC-MD5-96 • HMAC-SHA1-96

Setting	Description	Setting Value
Phase 2 Encryption Algorithm Permissions	Specify the encryption algorithm to be used in phase 2. (auto setting)	• Cleartext (NULL encryption) • DES • 3DES • AES-128 • AES-192 • AES-256
Phase 2 PFS	Specify whether to activate PFS. Then, if PFS is activated, select the Diffie-Hellman group. (auto setting)	• Inactive • 1 • 2 • 14
Phase 2 Validity Period	Specify the time period for which the SA settings in phase 2 are valid.	Specify a period (in seconds) from 300 (5min.) to 172800 (48 hrs.).

Encryption Key Manual Settings Items

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

Setting	Description	Setting Value
Remote Address	Specify the address of the IPsec transmission partner. You can also specify an address range.	The IPsec transmission partner's IPv4 or IPv6 address. If you are not setting an address range, enter 32 after an IPv4 address, or enter 128 after an IPv6 address.
Encapsulation Mode	Select the encapsulation mode.	• Transport • Tunnel (Tunnel beginning address - Tunnel ending address) If you select "Tunnel", set the "Tunnel End Point", the beginning and ending IP addresses. In "Tunnel End Point", set the same address for the beginning point as you set in "Local Address".
SPI (Output)	Specify the same value as your transmission partner's SPI input value.	Any number between 256 and 4095
SPI (Input)	Specify the same value as your transmission partner's SPI output value.	Any number between 256 and 4095
Security Protocol	To apply both encryption and authentication to sent data, specify ESP or ESP+AH. To apply authentication data only, specify AH.	• ESP • AH • ESP+AH
Authentication Algorithm	Specify the authentication algorithm.	• HMAC-MD5-96 • HMAC-SHA1-96

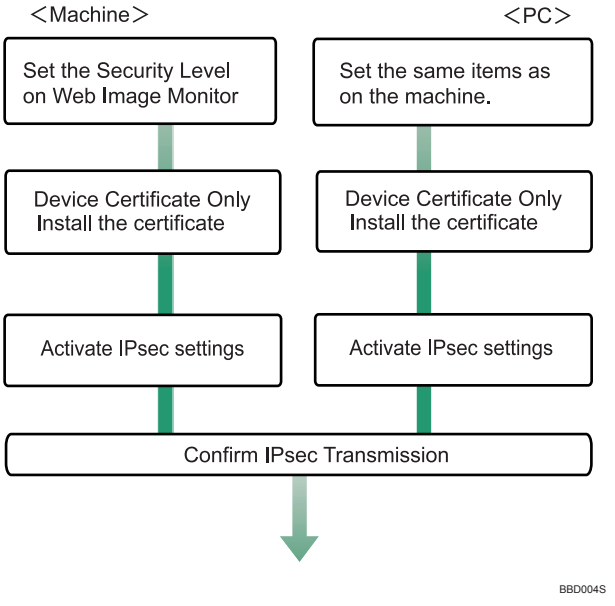
Setting	Description	Setting Value
Authentication Key	Specify the key for the authentication algorithm.	Specify a value within the ranges shown below, according to the encryption algorithm. Hexadecimal value 0-9, a-f, A-F • If HMAC-MD5-96, set 32 digits • If HMAC-SHA1-96, set 40 digits ASCII • IF HMAC-MD5-96, 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 ASCII • DES, set 8 characters • 3DES, set 24 characters • AES-128, set 16 characters • AES-192, set 24 characters • AES-256, set 32 characters

Encryption Key Auto Exchange Settings Configuration Flow

This section explains the procedure for specifying Encryption Key Auto Exchange Settings.

This can be specified by the network administrator.



Note

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

Specifying Encryption Key Auto Exchange Settings

This can be specified using Web Image Monitor.

1. **Open a Web browser.**
2. **Enter "http://(system'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 printer.

   The top page of Web Image Monitor appears.
3. **Click [Login].**

   The network administrator can log on.

   Enter the login user name and login password.
4. **Click [Configuration], and then click [IPsec] under "Security".**

   The IPsec settings page appears.

5. **Click [Edit] under "Encryption Key Auto Exchange Settings".**
6. **Make encryption key auto exchange settings in [Settings 1].**

   If you want to make multiple settings, select the settings number and add settings.
7. **Click [OK].**
8. **Select [Active] for "IPsec".**
9. **Set "Exclude HTTPS Communication" to [Active] if you do not want to use IPsec for HTTPS transmission.**
10. **Click [OK].**
11. **Click [OK].**
12. **Click [Logout].**

Note

- To change the transmission partner authentication method for encryption key auto exchange settings to "Certificate", you must first install and assign a certificate. For details about creating and installing a device certificate, see "Specifying SSL for the System Network".

Reference

- p.129 "Specifying SSL for the System Network"

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://(system'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 printer.

   The top page of Web Image Monitor appears.
3. **Click [Login].**

   The network administrator can log on.

   Enter the login user name and login password.
4. **Click [Configuration], and then click [Device Certificate] under "Security".**

   The Device Certificate page appears.
5. **Select the certificate to be used for IPsec from the drop down box in "IPsec" under "Certificate".**

6. **Click [OK].**

   The certificate for IPsec is specified.

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

Specifying IPsec Settings on the Computer

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

1. **On the [Start] menu, click [Control Panel], click [Performance and Maintenance], and then click [Administrative Tools].**
2. **Click [Local Security Policy].**
3. **Click [IP Security Policies on Local Computer].**
4. **In the "Action" menu, click [Create IP Security Policy].**

   The IP Security Policy Wizard appears.

5. **Click [Next].**
6. **Enter a security policy name in "Name", and then click [Next].**
7. **Clear the "Activate the default response rule" check box, and then click [Next].**
8. **Select "Edit properties", and then click [Finish].**
9. **In the "General" tab, click [Advanced].**
10. **In "Authenticate and generate a new key after every", enter the same validity period (in minutes) that is specified on the printer 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 printer in Encryption Key Auto Exchange Settings Phase 1.**
12. **If the settings are not displayed, click [Add].**
13. **Click [OK] twice.**
14. **Click [Add] in the "Rules" Tab.**

    The Security Rule Wizard appears.

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

18. **Select the "initial authentication method", and then click [Next].**
19. **If you select "Certificate" for authentication method in Encryption Key Auto Exchange Settings on the printer, specify the device certificate. If you select PSK, enter the same PSK text specified on the printer with the pre-shared key.**
20. **Click [Add] in the IP Filter List.**
21. **In [Name], enter an IP Filter name, and then click [Add].**

    The IP Filter Wizard appears.
22. **Click [Next].**
23. **Select "My Address" in "Source Address", and then click [Next].**
24. **Select "A specific IP address" in "Destination Address", enter the system's IP address, and then click [Next].**
25. **Select the protocol type for IPsec, and then click [Next].**
26. **Click [Finish].**
27. **Click [OK].**
28. **Select the IP filter that was just created, and then click [Next].**
29. **Select the IPsec security filter, and then click [Edit].**
30. **Click [Add], select the "Custom" check box, and then click [Settings].**
31. **In "Integrity algorithm", select the authentication algorithm that was specified on the printer in Encryption Key Auto Exchange Settings Phase 2.**
32. **In "Encryption algorithm", select the encryption algorithm that was specified on the printer in Encryption Key Auto Exchange Settings Phase 2.**
33. **In Session Key settings, select "Generate a new key every", and enter the validity period (in seconds) that was specified on the printer in Encryption Key Auto Exchange Settings Phase 2.**
34. **Click [OK] three times.**
35. **Click [Next].**
36. **Click [Finish].**
37. **Click [OK].**
38. **Click [Close].**

    The new IP security policy (IPsec settings) is specified.
39. **Select the security policy that was just created, right click, and then click [Assign].**

    IPsec settings on the computer are enabled.

Note

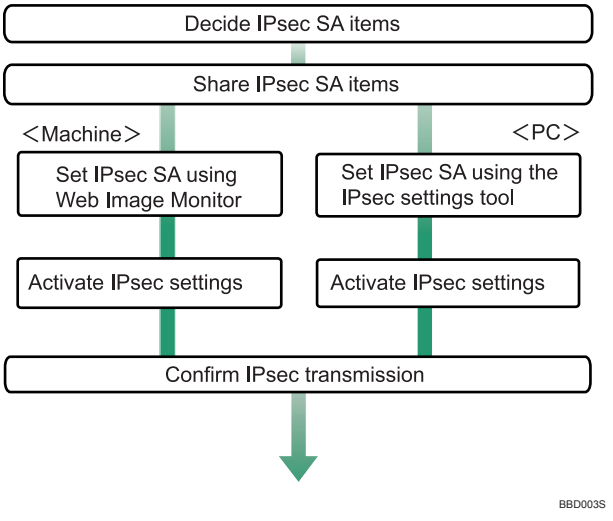
- To disable the computer's IPsec settings, select the security policy, right click, and then click [Unassign].

- If you specify the "Authentication and High Level Encryption" security level in encryption key auto exchange settings, also select the "Master key perfect forward secrecy (PFS)" check box in the Security Filter Properties screen (which appears in step 29). If using PFS in Windows XP, the PFS group number used in phase 2 is automatically negotiated in phase 1 from the Diffie-Hellman group number (set in step 11). Consequently, if you change the security level specified automatic settings on the printer and "User Setting" appears, you must set the same group number for "Phase 1 Diffie-Hellman Group" and "Phase 2 PFS" on the printer to establish IPsec transmission.

Encryption Key Manual Settings Configuration Flow

This section explains the procedure for specifying encryption key manual settings.

This can be specified by the network administrator.



Note

- Before transmission, SA information is shared and specified by the sender and receiver. To prevent SA information leakage, we recommend that this exchange is not performed over the network.
- After configuring IPsec, you can use "Ping" command to check if the connection is established correctly. However, you cannot use "Ping" command when ICMP is excluded from IPsec transmission. Also, because the response is slow during initial key exchange, it may take some time to confirm that transmission has been established.

Specifying Encryption Key Manual Settings

This can be specified using Web Image Monitor.

1. **Open a Web browser.**
2. **Enter "http://(system'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 printer.

   The top page of Web Image Monitor appears.
3. **Click [Login].**

   The network administrator can log on.

   Enter the login user name and login password.
4. **Click [Configuration], and then click [IPsec] under "Security".**

   The IPsec settings page appears.
5. **Select [Active] for "Encryption Key Manual Settings".**
6. **Click [Edit] under "Encryption Key Manual Settings".**
7. **Set items for encryption key manual settings in [Settings 1].**

   If you want to make multiple settings, select the settings number and add settings.
8. **Click [OK].**
9. **Select [Active] for "IPsec:" in "IPsec".**
10. **Set "Exclude HTTPS Communication" to [Active] if you do not want to use IPsec for HTTPS communication.**
11. **Click [OK].**
12. **Click [OK].**
13. **Click [Logout].**

telnet Setting Commands

You can use telnet to confirm IPsec settings and make setting changes. This section explains telnet commands for IPsec. If you are logging on as an administrator through telnet, the default login user name is "admin", but there is no default password. For details about logging on to telnet and telnet operations, see "Using telnet", Network and System Settings Guide.

Important

- **If you are using a certificate as the authentication method in encryption key auto exchange settings (IKE), install the certificate using Web Image Monitor. A certificate cannot be installed using telnet.**

ipsec

To display IPsec related settings information, use the "ipsec" command.

Display current settings

```
msh> ipsec
```

Displays the following IPsec settings information:

- IPsec shared settings values
- Encryption key manual settings, SA setting 1-4 values
- Encryption key manual settings, default setting values
- Encryption key auto exchange settings, IKE setting 1-4 values
- Encryption key auto exchange settings, IKE default setting values

Display current settings portions

```
msh> ipsec -p
```

- Displays IPsec settings information in portions.

ipsec manual mode

To display or specify encryption key manual settings, use the "ipsec manual_mode" command.

Display current settings

```
msh> ipsec manual_mode
```

- Displays the current encryption key manual settings.

Specify encryption key manual settings

```
msh> ipsec manual_mode {on|off}
```

- To enable encryption key manual settings, set to [on]. To disable settings, set to [off].

ipsec exclude

To display or specify protocols excluded by IPsec, use the "ipsec exclude" command.

Display current settings

```
msh> ipsec exclude
```

- Displays the protocols currently excluded from IPsec transmission.

Specify protocols to exclude

```
msh> ipsec exclude {https|dns|dhcp|wins|all} {on|off}
```

- Specify the protocol, and then enter [on] to exclude it, or [off] to include it for IPsec transmission. Entering [all] specifies all protocols collectively.

ipsec manual

To display or specify the encryption key manual settings, use the "ipsec manual" command.

Display current settings

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

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

Disable settings

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

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

Specify the local/remote address for settings 1-4

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

- Enter the separate setting number [1-4] and specify the local address and remote address.
- To specify the local or remote address value, specify masklen by entering [/] and an integer 0-32 if you are specifying an IPv4 address. If you are specifying an IPv6 address, specify masklen by entering [/] and an integer 0-128.
- Not specifying an address value displays the current setting.

Specify the address type in default setting

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

- Specify the address type for the default setting.
- To specify both IPv4 and IPv6, enter [any].

Security protocol setting

```
msh> ipsec manual {1|2|3|4|default} proto {ah|esp|dual}
```

- Enter the separate setting number [1-4] or [default] and specify the security protocol.
- To specify AH, enter [ah]. To specify ESP, enter [esp]. To specify AH and ESP, enter [dual].
- Not specifying a protocol displays the current setting.

SPI value setting

```
msh> ipsec manual {1|2|3|4|default} spi SPI input value SPI output value
```

- Enter the separate setting number [1-4] or [default] and specify the SPI input and output values.
- Specify a decimal number between 256-4095, for both the SPI input and output values.

Encapsulation mode setting

```
msh> ipsec manual {1|2|3|4|default} mode {transport|tunnel}
```

- Enter the separate setting number [1-4] or [default] and specify the encapsulation mode.
- To specify transport mode, enter [transport]. To specify tunnel mode, enter [tunnel].

- If you have set the address type in the default setting to [any], you cannot use [tunnel] in encapsulation mode.
- Not specifying an encapsulation mode displays the current setting.

Tunnel end point setting

```
msh> ipsec manual {1|2|3|4|default} tunneladdar beginning IP address ending IP address
```

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

Authentication algorithm and authentication key settings

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

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

Encryption algorithm and encryption key setting

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

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

Reset setting values

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

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

ipsec ike

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

Display current settings

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

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

Disable settings

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

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

Specify the local/remote address for settings 1-4

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

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

Specify the address type in default setting

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

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

Security policy setting

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

- Enter the separate setting number [1-4] or [default] and specify the security policy for the address specified in the selected setting.
- To apply IPsec to the relevant packets, specify [apply]. To not apply IPsec, specify [bypass].
- If you specify [discard], any packets that IPsec can be applied to are discarded.
- Not specifying a security policy displays the current setting.

Security protocol setting

```
msh> ipsec ike {1|2|3|4|default} proto {ah|esp|dual}
```

- Enter the separate setting number [1-4] or [default] and specify the security protocol.
- To specify AH, enter [ah]. To specify ESP, enter [esp]. To specify AH and ESP, enter [dual].
- Not specifying a protocol displays the current setting.

IPsec requirement level setting

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

- Enter the separate setting number [1-4] or [default] and specify the IPsec requirement level.
- If you specify [require], data will not be transmitted when IPsec cannot be used. If you specify [use], data will be sent normally when IPsec cannot be used. When IPsec can be used, IPsec transmission is performed.
- Not specifying a requirement level displays the current setting.

Encapsulation mode setting

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

- Enter the separate setting number [1-4] or [default] and specify the encapsulation mode.
- To specify transport mode, enter [transport]. To specify tunnel mode, enter [tunnel].
- If you have set the address type in the default setting to [any], you cannot use [tunnel] in encapsulation mode.
- Not specifying an encapsulation mode displays the current setting.

Tunnel end point setting

```
msh> ipsec ike {1|2|3|4|default} tunneladdar beginning IP address ending IP
address
```

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

IKE partner authentication method setting

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

- Enter the separate setting number [1-4] or [default] and specify the authentication method.
- Specify [psk] to use a shared key as the authentication method. Specify [rsasig] to use a certificate at the authentication method.
- You must also specify the PSK character string when you select [psk].
- Note that if you select "Certificate", the certificate for IPsec must be installed and specified before it can be used. To install and specify the certificate use Web Image Monitor.

PSK character string setting

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

- If you select PSK as the authentication method, enter the separate setting number [1-4] or [default] and specify the PSK character string.
- Specify the character string in ASCII characters. There can be no abbreviations.

ISAKMP SA (phase 1) hash algorithm setting

```
msh> ipsec ike {1|2|3|4|default} ph1 hash {md5|sha1}
```

- Enter the separate setting number [1-4] or [default] and specify the ISAKMP SA (phase 1) hash algorithm.
- To use MD5, enter [md5]. To use SHA1, enter [sha1].
- Not specifying the hash algorithm displays the current setting.

ISAKMP SA (phase 1) encryption algorithm setting

```
msh> ipsec ike {1|2|3|4|default} ph1 encrypt {des|3des}
```

- Enter the separate setting number [1-4] or [default] and specify the ISAKMP SA (phase 1) encryption algorithm.
- To use DES, enter [des]. To use 3DES, enter [3des].
- Not specifying an encryption algorithm displays the current setting.

ISAKMP SA (phase 1) Diffie-Hellman group setting

```
msh> ipsec ike {1|2|3|4|default} ph1 dhgroup {1|2|14}
```

- Enter the separate setting number [1-4] or [default] and specify the ISAKMP SA (phase 1) Diffie-Hellman group number.
- Specify the group number to be used.
- Not specifying a group number displays the current setting.

ISAKMP SA (phase 1) validity period setting

```
msh> ipsec ike {1|2|3|4|default} ph1 lifetime validity period
```

- Enter the separate setting number [1-4] or [default] and specify the ISAKMP SA (phase 1) validity period.
- Enter the validity period (in seconds) from 300 to 172800.
- Not specifying a validity period displays the current setting.

IPsec SA (phase 2) authentication algorithm setting

```
msh> ipsec ike {1|2|3|4|default} ph2 auth {hmac-md5|hmac-sha1}
```

- Enter the separate setting number [1-4] or [default] and specify the IPsec SA (phase 2) authentication algorithm.
- Separate multiple encryption algorithm entries with a comma (,). The current setting values are displayed in order of highest priority.
- Not specifying an authentication algorithm displays the current setting.

IPsec SA (phase 2) encryption algorithm setting

```
msh> ipsec ike {1|2|3|4|default} ph2 encrypt {null|des|3des|aes128|aes192|
aes256}
```

- Enter the separate setting number [1-4] or [default] and specify the IPsec SA (phase 2) encryption algorithm.

- Separate multiple encryption algorithm entries with a comma (,). The current setting values are displayed in order of highest priority.
- Not specifying an encryption algorithm displays the current setting.

IPsec SA (phase 2) PFS setting

```
msh> ipsec ike {1|2|3|4|default} ph2 pfs {none|1|2|14}
```

- Enter the separate setting number [1-4] or [default] and specify the IPsec SA (phase 2) Diffie-Hellman group number.
- Specify the group number to be used.
- Not specifying a group number displays the current setting.

IPsec SA (phase 2) validity period setting

```
msh> ipsec ike {1|2|3|4|default} ph2 lifetime validity period
```

- Enter the separate setting number [1-4] or [default] and specify the IPsec SA (phase 2) validity period.
- Enter the validity period (in seconds) from 300 to 172800.
- Not specifying a validity period displays the current setting.

Reset setting values

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

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

Configuring IEEE 802.1X Authentication for Ethernet

This section explains how to configure IEEE 802.1X for enhanced security. You can select four types of EAP authentication method: EAP-TLS, LEAP, EAP-TTLS and PEAP. Note that each EAP authentication method has different configuration settings and authentication procedures.

Types and requirements of certificates are as follows:

If a certificate is required, configure all settings after installing the certificate.

EAP Types Requiring a "Site Certificate"

EAP-TLS, EAP-TTLS, PEAP (Necessary except LEAP)

EAP Types Requiring a "Site Certificate" and a "Device Certificate"

EAP-TLS, PEAP (Phase 2 is for TLS only)

Specifying IEEE 802.1X Authentication for the System Network

The network administrator can configure the system network for use with IEEE802.1X.

Using Web Image Monitor to Install the Site Certificate

This can be specified by the network administrator.

Access the authentication server and obtain the CA certificate. Methods of obtaining certificates differ according to the operating system you are using.

1. **Open a Web browser.**
2. **Enter "http://(system'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 printer.

   The top page of Web Image Monitor appears.
3. **Click [Login].**

   The network administrator can log on.

   Enter the login user name and login password.
4. **Click [Configuration], and then click [Site Certificate] under "Security".**

   The Site Certificate page appears.
5. **Click [Browse] on the "Site Certificate to Import" window, and then select the CA certificate you obtained.**
6. **Click [Import].**

7. **Check that the imported certificate's [Status] shows "Trustworthy".**

   If [Site Certificate Check] shows [Active], and the [Status] of the certificate shows [Untrustworthy], communication might not be possible.

8. **Click [OK].**
9. **Click [Logout].**

Using Web Image Monitor to Install the Device Certificate (issued by a Certificate Authority)

This can be specified by the network administrator.

Use the following procedure to install the device certificate.

1. **Open a Web browser.**
2. **Enter "http://(system'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 printer.

   The top page of Web Image Monitor appears.

3. **Click [Login].**

   The network administrator can log on.

   Enter the login user name and login password.

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

   The Device Certificate page appears.

5. **Click [Certificate2] on the "Device Certificate" window, and then click [Request].**
6. **Enter appropriate "Common Name" and "Country Code" on "Certificate Information" page, and then click [OK].**
7. **"Updating..." appears. Wait for about 2 minutes, and then click [OK].**
8. **Click [ ], shown in the "Device Certificate" window as the memo pad icon for "Requesting".**
9. **Select all, and then copy the entire "Text for Requested Certificate" text that is displayed in the "Certificate Details" window.**
10. **Access the certificate authority server, and then obtain the CA signified certificate using the text copied into "Text for Requested Certificate" windows.**

    Obtaining the certificate differs depending on the environment you want to use.

11. **Click [Certificate2] on "Device Certificate" window, and then click [Install].**
12. **Open the CA signified certificate in a text editor, and then copy all the text.**
13. **In the "Install Certificate" window, paste all the text copied into the CA signified certificate.**
14. **Click [OK].**

15. **"Updating..." appears. Wait for about one or two minutes, and then click [OK].**
16. **Check that the "Device Certificate" shows "Installed".**
17. **In "Application", "Certification", set "IEEE 802.1X" to "Certificate2", and then click [OK].**
18. **Click [Logout].**

Note

- You request two certificates simultaneously, the certificate authority might not display either certificate. Click [Cancel Request] to cancel the request.
- You can select [Certificate 1-4] in the "Device Certificate" window. Note that if you select [Certificate 1] in the "Device Certificate" window, you must select "Certificate1" in the "IEEE 802.1X" drop down menu in the "Certification" window.
- Click [Cancel Request] to cancel the request for the server certificate.
- If "Not found" appears after clicking [OK] in steps 7 and 15, wait one or two minutes, and then click [Refresh].

Using Web Image Monitor to Specify IEEE 802.1X Authentication

This can be specified by the network administrator.

Use the following procedure to configure the printer for use with IEEE 802.1X over Ethernet.

1. **Open a Web browser.**
2. **Enter "http://(system'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 printer.

   The top page of Web Image Monitor appears.
3. **Click [Login].**

   The network administrator can log on.

   Enter the login user name and login password
4. **Click [Configuration], and then click [IEEE 802.1X] under "Security".**

   The IEEE 802.1X page appears.
5. **In "User Name", enter the user name set in the RADIUS server.**
6. **Enter the domain name in "Domain Name".**
7. **Select "EAP Type". Configurations differ according to the EAP Type.**

   EAP-TLS

   - Make the following settings according to the operating system you are using:
     - Select [On] or [Off] in "Authenticate Server Certificate".
     - Select [On] or [Off] in "Trust Intermediate Certificate Authority".

- Enter the host name of the RADIUS server on "Server ID".

LEAP

- Click [Change] in "Password", and then enter the password set in the RADIUS server.

EAP-TTLS

- Click [Change] in "Password", and then enter the password set in the RADIUS server.
- Click [Change] in "Phase 2 User Name", and then enter the user name set in the RADIUS server.
- Select [CHAP], [MSCHAP], [MSCHAPv2], [PAP], or [MD5] in "Phase 2 Method".
- Certain methods might not be available, depending on the RADIUS server you want to use.
- Make the following settings according to the operating system you are using:
  - Select [On] or [Off] in "Authenticate Server Certificate".
  - Select [On] or [Off] in "Trust Intermediate Certificate Authority".
  - Enter the host name of the RADIUS server in "Server ID".

PEAP

- Click [Change] in "Password", and then enter the password set in the RADIUS server.
- Click [Change] on "Phase 2 User Name", and then enter the user name set in the RADIUS server.
- Select [MSCHAPv2] or [TLS] in "Phase 2 Method".
- When you select [TLS], you must install "IEEE 802.1X Client Certificate".
- Make the following settings according to the operating system you are using:
  - Select [On] or [Off] in "Authenticate Server Certificate".
  - Select [On] or [Off] in "Trust Intermediate Certificate Authority".
  - Enter the host name of the RADIUS server on "Server ID".

8. **Click [OK].**
9. **Click [OK].**
10. **Click [Configuration], and then click [Interface Settings] in the "Interface" area.**
11. **Select Active in "Ethernet Security".**
12. **Click [OK].**
13. **Click [Logout].**

Note

- If there is a problem with settings, you might not be able to communicate with the printer. To identify the problem, print a network summary.
- If you cannot identify the problem, reset the printer's interface settings to normal, and then repeat the procedure from the beginning.

Specifying IEEE 802.1X Authentication for the Printing Network

The Printer Features administrator can configure the printing network for use with IEEE802.1X.

Using Web Interface to Install the Site Certificate

This must be specified by the Printer Features administrator.

Access the authentication server and obtain the CA certificate. Methods of obtaining certificates differ according to the operating system you are using.

1. **Open a Web browser.**
2. **Enter "http://(printer'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 printer.

   The top page of Web Interface appears.
3. **Click [Configurations/Jobs].**

   An authentication dialog box appears.
4. **Enter the login user name and login password.**

   Enter "system" as the login user name and enter the password for printer settings as the login password.
5. **Click [Printer Settings], and then click [Site Certificate] under "Security".**

   The Site Certificate page appears.
6. **Click [Browse] on the "Site Certificate to Import" window, and then select the CA certificate you obtained.**
7. **Click [Import].**
8. **Click [OK].**
9. **Close the Web browser.**

   You will be logged off.

Using Web Interface to Install the Device Certificate (issued by a Certificate Authority)

This must be specified by the Printer Features administrator.

Use the following procedure to install the device certificate.

1. **Open a Web browser.**
2. **Enter "http://(printer'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 printer.

The top page of Web Interface appears.

3. **Click [Configurations/Jobs].**

   An authentication dialog box appears.

4. **Enter the login user name and login password.**

   Enter "system" as the login user name and enter the password for printer settings as the login password.

5. **Click [Printer Settings], and then click [Device Certificate] under "Security".**

   The Device Certificate page appears.

6. **Click [Certificate2] on the "Device Certificate" window, and then click [Request].**

7. **Enter appropriate "Common Name" and "Country Code" on "Certificate Information" page, and then click [OK].**

8. **Click [], shown in the "Device Certificate" window as the memo pad icon for "Requesting".**

9. **Select all, and then copy the entire "Text for Requested Certificate" text that is displayed in the "Certificate Request" window.**

   Also, by clicking [Export], you can export the text as a file.

10. **Access the certificate authority server, and then obtain the CA signified certificate using the text copied into "Text for Requested Certificate" windows.**

    Obtaining the certificate differs depending on the environment you want to use.

11. **Click [Certificate2] on "Device Certificate" window, and then click [Import].**

12. **Open the CA signified certificate in a text editor, and then copy all the text.**

13. **In "Import Format", select "Text", and then paste all the copied text into the "Text" box.**

    If you selected "File" in "Import Format", specify the file location.

14. **Click [OK].**

15. **Check that the "Device Certificate" shows "Imported".**

16. **In "Application", "Certification", set "IEEE 802.1X" to "Certificate2", and then click [OK].**

Note

- You can select [Certificate 1-2] in the "Device Certificate" window. Note that if you select [Certificate 1] in the "Device Certificate" window, you must select "Certificate1" in the "IEEE 802.1X" drop down menu in the "Certification" window.

Using Web Interface to Specify IEEE 802.1X Authentication

This must be specified by the Printer Features administrator.

Use the following procedure to configure the printer for use with IEEE 802.1X over Ethernet.

1. **Open a Web browser.**

2. **Enter "http://(printer'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 printer.

   The top page of Web Interface appears.

3. **Click [Configurations/Jobs].**

   An authentication dialog box appears.

4. **Enter the login user name and login password.**

   Enter "system" as the login user name and enter the password for printer settings as the login password.

5. **Click [Printer Settings], and then click [IEEE 802.1X] under "Network".**

   The IEEE 802.1X page appears.

6. **Select [Active] in "IEEE 802.1X".**
7. **In "User Name", enter the user name set in the RADIUS server.**
8. **Click [Change] in "Password".**
9. **Enter the password set in the RADIUS server, and then click [OK].**
10. **Enable or disable the various EAP authentication methods.**
11. **Click [OK].**
12. **Close the Web browser.**

    You will be logged off.

7. Specifying the Extended Security Functions

This chapter describes the printer'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 printer, security can also be increased by encrypting transmitted data and data in the Address Book. If you need extended security, specify the printer's extended security functions before using the printer.

This section outlines the extended security functions and how to specify them.

For details about when to use each function, see the corresponding chapters.

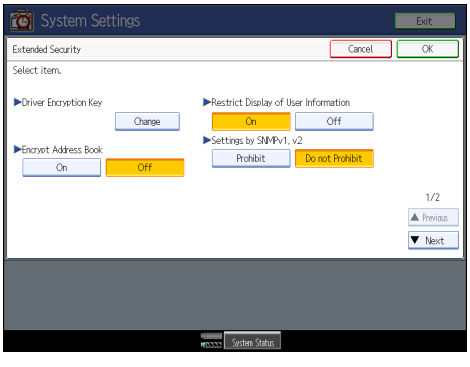
Changing the Extended Security Functions

This section describes how to change the Extended Security Functions.

Administrators can change the extended security functions according to their role. For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

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

   If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.
5. **Press the setting you want to change, and change the setting.**



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

Reference

- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"

Extended Security Settings

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

Driver Encryption Key

This can be specified by the network administrator. Encrypt the password transmitted when specifying user authentication. If you register the encryption key specified with the printer in the driver, passwords are encrypted. For details, see "Specifying a Driver Encryption Key".

Encrypt Address Book

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

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

- On
- **Off**

Restrict Display of User Information

This can be specified if user authentication is specified. When the job history is checked using a network connection for which authentication is not available, all personal information can be displayed as "********". Because information identifying registered users cannot be viewed, unauthorized users are prevented from obtaining information about the registered files.

- On
- **Off**

Settings by SNMPv1, v2

This can be specified by the network administrator. This setting allows machine administrator settings such as the paper setting to be changed. If you select [Prohibit], the setting can be viewed but not specified with SNMPv1, v2.

- Prohibit
- **Do not Prohibit**

Note that authentication is not possible if the printer is accessed over the system network using SNMP v1 or v2.

This setting does not apply to the printing network.

Authenticate Current Job

This setting is not available for this printer.

If Menu Protect is set to [Active], the password for printer settings will be required for the current job, and only the Printer Features administrator will be able to carry out operations such as canceling the current job.

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 #.

The password policy does not apply to the password for printer settings.

- Level 2
- Level 1
- **Off**
- Minimum Character No. (**0**)

@Remote Service

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

- Prohibit
- **Do not Prohibit**

Update Firmware

This can be specified by the machine administrator.

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

If you select [Prohibit], only the printer controller firmware can be updated. Any other firmware updates are blocked.

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

- Prohibit
- **Do not Prohibit**

Change Firmware Structure

This can be specified by the machine administrator.

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

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

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

When Change Firmware Structure is set to [Prohibit], administrator authentication must be enabled.

After [Prohibit] is specified, turn off administrator authentication once, and the next time administrator authentication is specified, the setting will return to the default, [Do not Prohibit].

If you select [Do not Prohibit], firmware structure change detection is disabled.

- Prohibit
- **Do not Prohibit**

Reference

- p.124 "Specifying a Driver Encryption Key"
- p.81 "Protecting the Address Book"
- p.137 "Setting the SSL/TLS Encryption Mode"

Other Security Functions

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

Weekly Timer Code

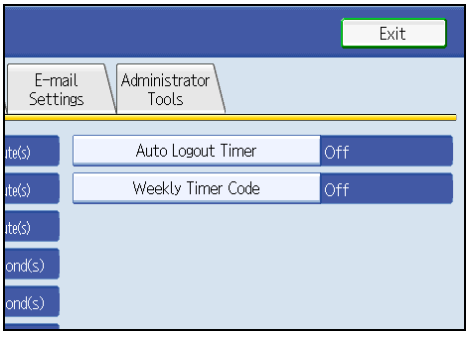
If the weekly timer is enabled and [Weekly Timer Code] is set to [On], you must enter the weekly timer code to turn the power back on after the timer has turned it off.

Specifying Weekly Timer Code

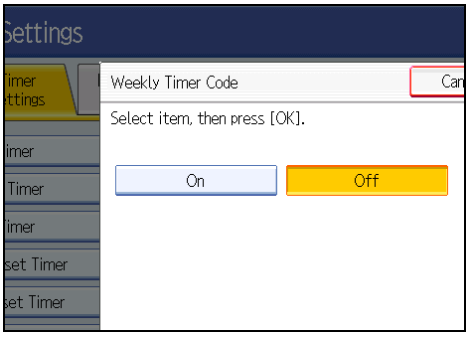
This can be specified by the machine administrator.

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

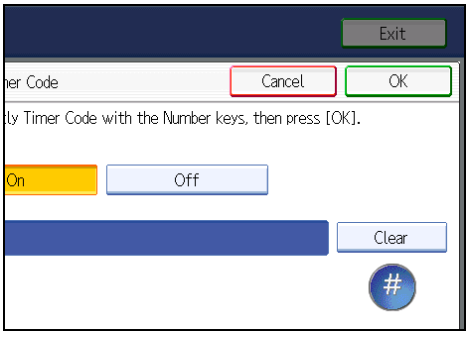
1. **Press the [User Tools] key.**
2. **Press [System Settings].**
3. **Press [Timer Settings].**
4. **Press [Weekly Timer Code].**



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.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"

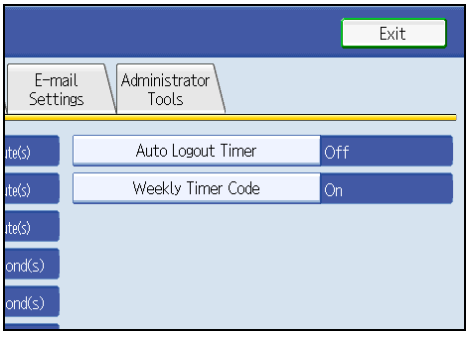
7

Canceling Weekly Timer Code

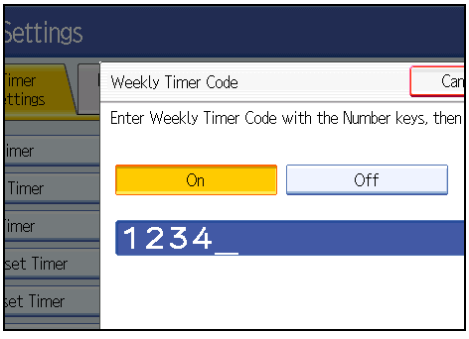
This can be specified by the machine administrator.

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

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.**

Reference

- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"

Limiting Machine Operations to Customers Only

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

The printer 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 printer without administrator permission.

Use the following settings.

- Service Mode Lock

Settings

Service Mode Lock

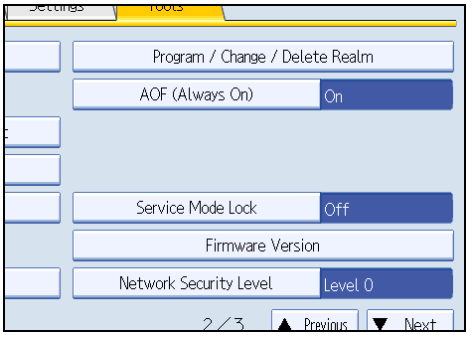
This can be specified by the machine administrator. Service mode is used by a service representative for inspection or repair. If you set the service mode lock to [On], service mode cannot be used unless the machine administrator logs on to the printer and cancels the service mode lock to allow the service representative to operate the printer for inspection and repair. This ensures that the inspection and repair are done under the supervision of the machine administrator.

Specifying Service Mode Lock

This can be specified by the machine administrator.

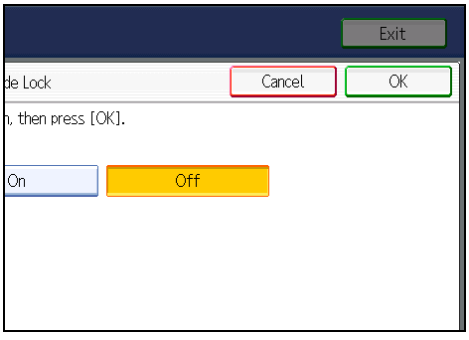
For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

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



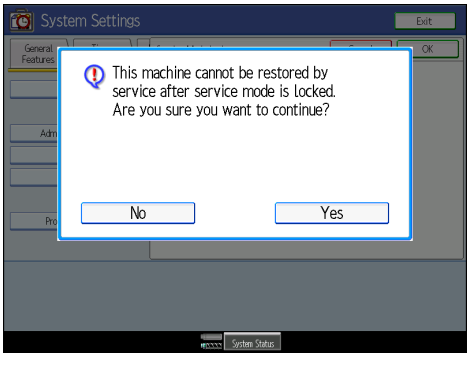
If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

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



A confirmation message appears.

6. **Press [Yes].**



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

Reference

- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"

Canceling Service Mode Lock

To enable a service representative to inspect or repair this printer, the machine administrator must log on and cancel the service mode lock beforehand.

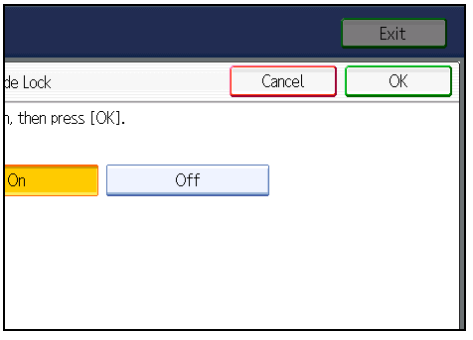
For details about logging on and logging off with administrator authentication, see "Logging on Using Administrator Authentication", "Logging off Using Administrator Authentication".

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

4. **Press [Service Mode Lock].**

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

5. **Press [Off], and then press [OK].**



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

   The service representative can switch to service mode.

Reference

- p.33 "Logging on Using Administrator Authentication"
- p.34 "Logging off Using Administrator Authentication"

Additional Information for Enhanced Security

This section explains the settings that you can configure to enhance the printer's security.

Settings you can Configure Using the Control Panel

Use the control panel to configure the security settings shown in the following table.

Menu

System Settings

Tab	Item	Setting
Timer Settings	Auto Logout Timer	[On]: 180 seconds or less. You cannot change the Web Image Monitor auto logout time. See "Auto Logout".
Administrator Tools	User Authentication Management	Select [Basic Auth.]. See "Basic Authentication".
Administrator Tools	Administrator Authentication Management/User Management	Select [On], and then select [Administrator Tools] for "Available Settings". See "Enabling Administrator Authentication".
Administrator Tools	Administrator Authentication Management/Machine Management	Select [On], and then select [Timer Settings], [Interface Settings], [E-mail Settings], and [Administrator Tools] for "Available Settings". See "Enabling Administrator Authentication".
Administrator Tools	Administrator Authentication Management/Network Management	Select [On], and then select [Interface Settings], [E-mail Settings], and [Administrator Tools] for "Available Settings". See "Enabling Administrator Authentication".
Administrator Tools	Administrator Authentication Management/File Management	Select [On], and then select [Administrator Tools] for "Available Settings". See "Enabling Administrator Authentication".

Tab	Item	Setting
Administrator Tools	Extended Security/Settings by SNMPv1 and v2	[Prohibit] See "Specifying the Extended Security Functions".
Administrator Tools	Extended Security/ Password Policy	"Complexity Setting": [Level 1] or higher, "Minimum Character No.": 6 or higher See "Specifying the Extended Security Functions".
Administrator Tools	Network Security Level	[Level 2] To acquire the printer status through printer driver or Web Image Monitor, set "SNMP" to Active on Web Image Monitor. See "Specifying Network Security Level".
Administrator Tools	Service Mode Lock	[On] See "Limiting Machine Operations to Customers Only".

Note

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

Reference

- p.78 "Auto Logout"
- p.49 "Basic Authentication"
- p.27 "Enabling Administrator Authentication"
- p.173 "Specifying the Extended Security Functions"
- p.118 "Specifying Network Security Level"
- p.180 "Limiting Machine Operations to Customers Only"

Settings you can Configure Using Web Image Monitor

Use Web Image Monitor to configure the security settings shown in the following table.

Category	Item	Setting
Device Settings/ Logs	Collect Job Logs	Active

Category	Item	Setting
Device Settings/ Logs	Collect Access Logs	Active
Security/User Lockout Policy	Lockout	Active
Security/User Lockout Policy	Number of Attempts before Lockout	5 times or less. See "User Lockout Function".
Security/User Lockout Policy	Lockout Release Timer	Set to Active or Inactive. When setting to Active, set the Lockout release timer to 60 minutes or more. See "User Lockout Function".
Security/User Lockout Policy	Lock Out User for	When setting "Lockout Release Timer" to Active, set the Lockout release timer to 60 minutes or more. See "User Lockout Function".
Network/ SNMPv3	SNMPv3 Function	Inactive To use SNMPv3 functions, set "SNMPv3 Function" to "Active", and set "Permit SNMPv3 Communication" to "Encryption Only". Because SNMPv3 enforces authentication for each packet, Login log will be disabled as long as SNMPv3 is active.
Security/Network Security	FTP	Inactive Before specifying this setting, set Security Level to Level 2 on the control panel.

Note

- For details about the collect log setting and SNMPv3 setting, see Web Image Monitor Help.

Reference

- p.75 "User Lockout Function"

Settings you can Configure when IPsec is Available/Unavailable

IPsec encrypts all the data traveling on your system network.

If your network supports IPsec, we recommend you enable it.

Settings you can Configure when IPsec is Available

If IPsec is available, configure the settings shown in the following table to enhance the security of the data traveling on your system network.

System Settings (Control panel)

Tab	Item	Setting
Interface Settings	IPsec	[Active]
Interface Settings	Permit SSL / TLS Communication	[Ciphertext Only]

Web Image Monitor settings

Category	Item	Setting
Security/SSL/TLS	Permit SSL/TLS Communication	If you set "Exclude HTTPS Communication" to Active, you must also set "Permit SSL/TLS Communication" to Ciphertext Priority.
Security/IPsec	Encryption Key Manual Settings	Inactive
Security/IPsec	Encryption Key Auto Exchange Settings/ Security Level	Authentication and High Level Encryption

Note

- You can set "Permit SSL/TLS Communication" using either Web Image Monitor or the printer's control panel.

Settings you can Configure when IPsec is Unavailable

If IPsec is not available, configure the settings shown in the following table to enhance the security of the data traveling on your system network.

System Settings (Control panel)

Tab	Item	Setting
Interface Settings	IPsec	[Inactive]
Interface Settings	Permit SSL / TLS Communication	[Ciphertext Only]

8. Troubleshooting

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

If Authentication Fails

This section explains what to do if a user cannot operate the printer because of a problem related to user authentication. Refer to this section if a user comes to you with such a problem.

If a Message is Displayed

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

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

Messages	Cause	Solutions
"You do not have the privileges to use this function."	The authority to use the function is not specified.	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.
"Failed to obtain URL."	The printer 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 printer. Make sure the host name of the UA Server is specified correctly.
"Failed to obtain URL."	The printer 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 printer.

Messages	Cause	Solutions
"Authentication has failed."	The entered login user name or login password is incorrect.	Ask the user administrator for the correct login user name and login password. See the error codes below for possible solutions: B,W,L,I 0104-000 B,W,L,I 0206-003 W,L,I 0406-003
"Authentication has failed."	Authentication failed because no more users can be registered. (The number of users registered in the Address Book has reached capacity.)	Delete unnecessary user addresses. See the error codes below for possible solutions: W,L,I 0612-005
"Authentication has failed."	Cannot access the authentication server when using Windows Authentication, LDAP Authentication, or Integration Server Authentication.	A network or server error may have occurred. Confirm the network in use with the LAN administrator. If an error code appears, follow the instructions next to the error code in the table below.
"Administrator Authentication for User Management must be set to on before this selection can be made."	User administrator privileges have not been enabled in Administrator Authentication Management.	To specify Basic Authentication, Windows Authentication, LDAP Authentication, or Integration Server Authentication, you must first enable user administrator privileges in Administrator Authentication Management. For details about authentication settings, see "Configuring User Authentication".

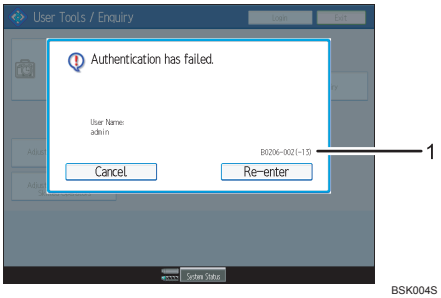
Reference

- p.43 "Configuring User Authentication"

If an Error Code is Displayed

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

Error Code Display Position



1. **error code**

   An error code appears.

Basic Authentication

Error Code	Cause	Solution
B0104-000	Failed to decrypt password.	1. A password error occurred. Make sure the password is entered correctly. 2. A driver encryption key error occurred. Make sure that the encryption key is correctly specified on the driver.
B0206-002	1. A login user name or password error occurred.	Make sure the login user name and password are entered correctly and then log on.
B0206-003	An authentication error occurred because the user name contains a space, colon (:), or quotation mark (").	Recreate the account if the account name contains any of these prohibited characters. If the account name was entered incorrectly, enter it correctly and log on again.

Error Code	Cause	Solution
B0207-001	An authentication error occurred because the Address Book is being used at another location.	Wait a few minutes and then try again.
B0208-000	The account is locked because you have reached the maximum number of failed authentication attempts allowed.	Ask the user administrator to unlock the account.

Windows Authentication

Error Code	Cause	Solution
W0104-000	Failed to encrypt password.	1. A password error occurred. Make sure the password is entered correctly. 2. A driver encryption key error occurred. Make sure that the encryption key is correctly specified on the driver.
W0206-003	An authentication error occurred because the user name contains a space, colon (:), or quotation mark (").	Recreate the account if the account name contains any of these prohibited characters. If the account name was entered incorrectly, enter it correctly and log on again.
W0207-001	An authentication error occurred because the Address Book is being used at another location.	Wait a few minutes and then try again.

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.
W0400-102	Kerberos authentication failed because the server or security module is not functioning correctly.	1. Make sure that the server is functioning properly. 2. Make sure that the security module is installed.
W0406-104	1. Cannot connect to the authentication server.	Make sure that connection to the authentication server is possible. Use the PING Command to check the connection.
W0406-104	2. A login name or password error occurred.	Make sure that the user is registered on the server. Use a registered login user name and password.
W0406-104	3. A domain name error occurred.	Make sure that the Windows authentication domain name is specified correctly.

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

Error Code	Cause	Solution
W0406-104	4. Cannot resolve the domain name.	Specify the IP address in the domain name and confirm that authentication is successful. If authentication was unsuccessful: 1. Make sure that Restrict LM/NTLM is not set in either "Domain Controller Security Policy" or "Domain Security Policy". Authentication is rejected because NTLMv2 is not supported. 2. Make sure that the ports for the domain control firewall and the firewall on the printer 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, permit exceptions 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".

Error Code	Cause	Solution
W0406-104	5. Kerberos authentication failed.	1. Kerberos authentication settings are not correctly configured. Make sure the realm name, KDC (Key Distribution Center) name and corresponding domain name are specified correctly. 2. The KDC and printer timing do not match. Authentication will fail if the difference between the KDC and printer timing is more than 5 minutes. Make sure the timing matches. 3. Kerberos authentication will fail if the realm name is specified in lower-case letters. Make sure the realm name is specified in capital letters. 4. Kerberos authentication will fail if automatic retrieval for KDC fails. Ask your service representative to make sure the KDC retrieval settings are set to "automatic retrieval". If automatic retrieval is not functioning properly, switch to manual retrieval.

Error Code	Cause	Solution
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 on, because this account allows you to obtain the user group.
W0400-105	2. Current settings do not allow group retrieval.	Make sure the user group's group scope is set to "Global Group" and the group type is set to "Security" in group properties. Make sure the account has been added to user group. Make sure the user group name registered on the printer and the group name on the DC (domain controller) are exactly the same. The DC is case sensitive. Make sure that "Use Auth. Info at Login" has been specified in Auth. Info in the user account registered on the printer. 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.

Error Code	Cause	Solution
W0400-202	1. The SSL settings on the authentication server and the printer do not match.	Make sure the SSL settings on the authentication server and the printer match.
W0400-202	2. The user entered sAMAccountName in the user name to log on.	If a user enters sAMAccountName as the login user name, ldap_bind fails in a parent/subdomain environment. Use UserPrincipleName for the login name instead.
W0406-003	An authentication error occurred because the user name contains a space, colon (:), or quotation mark (").	Recreate the account if the account name contains any of these prohibited characters. If the account name was entered incorrectly, enter it correctly and log on again.
W0409-000	Authentication timed out because the server did not respond.	Check the network configuration, or settings on the authenticating server.
W0511-000	The authentication server login name is the same as a user name already registered on the printer. (Names are distinguished by the unique attribute specified in LDAP authentication settings.)	1. Delete the old, duplicated name or change the login name. 2. If the authentication server has just been changed, delete the old name on the server.
W0607-001	An authentication error occurred because the Address Book is being used at another location.	Wait a few minutes and then try again.
W0606-004	Authentication failed because the user name contains language that cannot be used by general users.	Do not use "other", "admin", "supervisor" or "HIDE*" in general user accounts.

Error Code	Cause	Solution
W0612-005	Authentication failed because no more users can be registered. (The number of users registered in the Address Book has reached capacity.)	Ask the user administrator to delete unused user accounts in the Address Book.
W0707-001	An authentication error occurred because the Address Book is being used at another location.	Wait a few minutes and then try again.

LDAP Authentication

Error Code	Cause	Solution
L0104-000	Failed to encrypt password.	1. A password error occurred. Make sure the password is entered correctly. 2. A driver encryption key error occurred. Make sure that the encryption key is correctly specified on the driver.
L0206-003	An authentication error occurred because the user name contains a space, colon (:), or quotation mark (").	Recreate the account if the account name contains any of these prohibited characters. If the account name was entered incorrectly, enter it correctly and log on again.
L0207-001	An authentication error occurred because the Address Book is being used at another location.	Wait a few minutes and then try again.
L0306-018	The LDAP server is not correctly configured.	Make sure that a connection test is successful with the current LDAP server configuration.

Error Code	Cause	Solution
L0307-001	An authentication error occurred because the Address Book is being used at another location.	Wait a few minutes and then try again.
L0406-200	Authentication cannot be completed because of the high number of authentication attempts.	Wait a few minutes and then try again. If the situation does not return to normal, make sure that an authentication attack is not occurring. Notify the administrator of the screen message by e-mail, and check the system log for signs of an authentication attack.
L0406-201	Authentication is disabled in the LDAP server settings.	Change the LDAP server settings in administrator tools, in "System Settings".
L0406-202 L0406-203	1. There is an error in the LDAP authentication settings, LDAP server, or network configuration.	1. Make sure that a connection test is successful with the current LDAP server configuration. If connection is not successful, there might be an error in the network settings. Check the domain name or DNS settings in "Interface Settings". 2. Make sure the LDAP server is specified correctly in the LDAP authentication settings. 3. Make sure the login name attribute is entered correctly in the LDAP authentication settings. 4. Make sure the SSL settings are supported by the LDAP server.

Error Code	Cause	Solution
L0406-202 L0406-203	2. A login user name or password error occurred.	1. Make sure the login user name and password are entered correctly. 2. Make sure a usable login name is registered on the printer. Authentication will fail in the following cases: If the login user name contains a space, colon (:), or quotation mark ("). If the login user name exceeds 128 bytes.
L0406-202 L0406-203	3. There is an error in the simple encryption method.	1. Authentication will fail if the password is left blank in simple authentication mode. To allow blank passwords, contact your service representative. 2. In simple authentication mode, the DN of the login user name is obtained in the user account. Authentication fails if the DN cannot be obtained. Make sure there are no errors in the server name, login user name/password, or information entered for the search filter.

Error Code	Cause	Solution
L0406-204	Kerberos authentication failed.	1. Kerberos authentication settings are not correctly configured. Make sure the realm name, KDC (Key Distribution Center) name, and supporting domain name are specified correctly. 2. The KDC and printer timing do not match. Authentication will fail if the difference between the KDC and printer timing is more than 5 minutes. Make sure the timing matches. 3. Kerberos authentication will fail if the realm name is specified in lower-case letters. Make sure the realm name is specified in capital letters.
L0400-210	Failed to obtain user information in LDAP search.	The login attribute's search criteria might not be specified or the specified search information is unobtainable. Make sure the login name attribute is specified correctly.
L0406-003	An authentication error occurred because the user name contains a space, colon (:), or quotation mark (").	Recreate the account if the account name contains any of these prohibited characters. If the account name was entered incorrectly, enter it correctly and log on again.
L0409-000	Authentication timed out because the server did not respond.	Contact the server or network administrator. If the situation does not return to normal, contact your service representative.

Error Code	Cause	Solution
L0511-000	The authentication server login name is the same as a user name already registered on the printer. (Names are distinguished by the unique attribute specified in the LDAP authentication settings.)	1. Delete the old, duplicated name or change the login name. 2. If the authentication server has just been changed, delete the old name on the server.
L0607-001	An authentication error occurred because the Address Book is being used at another location.	Wait a few minutes and then try again.
L606-004	Authentication failed because the user name contains language that cannot be used by general users.	Do not use "other", "admin", "supervisor" or "HIDE*" in general user accounts.
L0612-005	Authentication failed because no more users can be registered. (The number of users registered in the Address Book has reached capacity.)	Ask the user administrator to delete unused user accounts in the Address Book.
L0707-001	An authentication error occurred because the Address Book is being used at another location.	Wait a few minutes and then try again.

Integration Server Authentication

Error Code	Cause	Solution
I0104-000	Failed to decrypt password.	1. A password error occurred. Make sure the password is entered correctly. 2. A driver encryption key error occurred. Make sure that the encryption key is correctly specified on the driver.

Error Code	Cause	Solution
I0206-003	An authentication error occurred because the user name contains a space, colon (:), or quotation mark (").	Recreate the account if the account name contains any of these prohibited characters. If the account name was entered incorrectly, enter it correctly and log on again.
I0207-001	An authentication error occurred because the Address Book is being used at another location.	Wait a few minutes and then try again.
I0406-003	An authentication error occurred because the user name contains a space, colon (:), or quotation mark (").	Recreate the account if the account name contains any of these prohibited characters. If account name was entered incorrectly, enter it correctly and log on again.
I0406-301	1. The URL could not be obtained.	Obtain the URL using Obtain URL in Integration Server authentication.
I0406-301	2. A login user name or password error occurred.	1. Make sure the login user name and password are entered correctly. 2. Make sure that a usable login name is registered on the printer. Authentication will fail in the following cases. If the login user name contains a space, colon (:), or quotation mark ("). If the login user name exceeds 128 bytes.
I0409-000	Authentication timed out because the server did not respond.	Contact the server or network administrator. If the situation does not return to normal, contact your service representative.

Error Code	Cause	Solution
I0511-000	The authentication server login name is the same as a user name already registered on the printer. (Names are distinguished by the unique attribute specified in the LDAP authentication settings.)	1. Delete the old, duplicated name or change the login name. 2. If the authentication server has just been changed, delete the old name on the server.
I0607-001	An authentication error occurred because the Address Book is being used at another location.	Wait a few minutes and then try again.
I0606-004	Authentication failed because the user name contains language that cannot be used by general users.	Do not use "other", "admin", "supervisor" or "HIDE*" in general user accounts.
I0612-005	Authentication failed because no more users can be registered. (The number of users registered in the Address Book has reached capacity.)	Ask the user administrator to delete unused user accounts in the Address Book.
I0707-001	An authentication error occurred because the Address Book is being used at another location.	Wait a few minutes and then try again.

If the Machine Cannot Be Operated

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

Condition	Cause	Solution
Cannot perform the following: • Print with the printer driver	User authentication has been rejected.	Confirm the user name and login name with the administrator of the network in use if using Windows Authentication, LDAP Authentication, or Integration Server Authentication. Confirm with the user administrator if using basic authentication.
Cannot perform the following: • Print with the printer driver	The encryption key specified in the driver does not match the printer's driver encryption key.	Specify the driver encryption key registered in the printer. See "Specifying a Driver Encryption Key".
Cannot print when user authentication has been specified.	User authentication may not be specified in the printer driver.	Specify user authentication in the printer driver. For details, see the printer driver Help.
After you execute "Encrypt Address Book", the "Exit" message does not appear.	The hard disk may be faulty. The file may be corrupt.	Contact your service representative.

Reference

- p.124 "Specifying a Driver Encryption Key"
- p.137 "Setting the SSL/TLS Encryption Mode"
- p.81 "Protecting the Address Book"

9. Appendix

Supervisor Operations

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

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

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

Important

- **The default login user name is "supervisor", but there is no default login password. We recommend changing the login user name and login password.**
- **When registering login user names and login passwords, you can specify up to 32 alphanumeric characters and symbols. Keep in mind that user names and passwords are case-sensitive.**
- **Be sure not to forget the supervisor login user name and login password. If you do forget them, a service representative will have to return the printer to its default state. This will result in all data in the printer being lost and the service call may not be free of charge.**

Note

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

Logging on as the Supervisor

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

1. **Press the [User Tools] key.**
2. **Press the [Login/Logout] key.**
3. **Press [Login].**
4. **Enter a login user name, and then press [OK].**

   When you assign the administrator for the first time, enter "supervisor".
5. **Enter a login password, and then press [OK].**

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

Logging off as the Supervisor

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

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

Changing the Supervisor

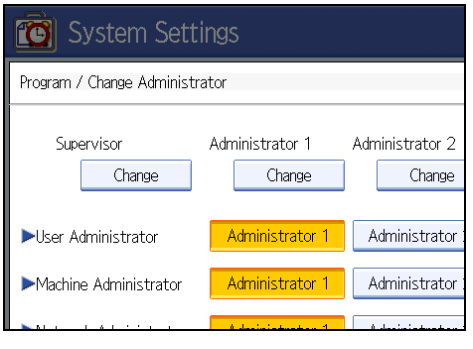
This section describes how to change the supervisor's login name and password.

To do this, you must enable the user administrator's privileges through the settings under "Administrator Authentication Management". For details, see "Specifying Administrator Privileges".

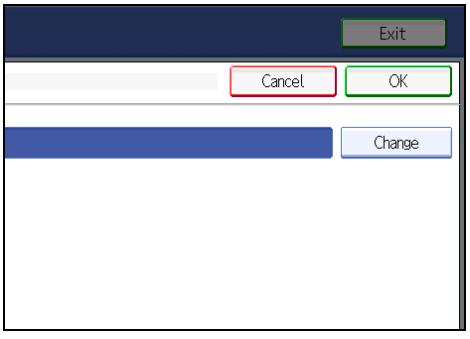
1. **Press the [User Tools] key.**
2. **Press the [Login/Logout] key.**
3. **Log on as the supervisor.**

   You can log on in the same way as an administrator.
4. **Press [System Settings].**
5. **Press [Administrator Tools].**
6. **Press [Program / Change Administrator].**

   If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.
7. **Under "Supervisor", press [Change].**



8. **Press [Change] for the login user name.**



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

    You will be automatically logged off.
14. **Press the [User Tools] key.**

Reference

- p.27 "Specifying Administrator Privileges"
- p.205 "Supervisor Operations"

Resetting the Administrator's Password

This section describes how to reset the administrators' passwords.

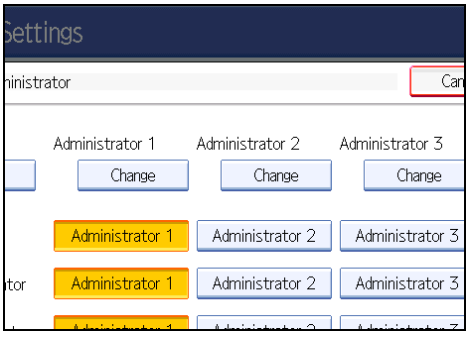
For details about logging on and logging off as the supervisor, see "Supervisor Operations".

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

   You can log on in the same way as an administrator.
4. **Press [System Settings].**
5. **Press [Administrator Tools].**
6. **Press [Program / Change Administrator].**

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

7. **Press [Change] for the administrator you wish to reset.**



8. **Press [Change] for the login password.**
9. **Enter the login password, and then press [OK].**
10. **If a password reentry screen appears, enter the login password, and then press [OK].**
11. **Press [OK] twice.**

    You will be automatically logged off.
12. **Press the [User Tools] key.**

Reference

- p.205 "Supervisor Operations"

Machine Administrator Settings

The machine administrator settings that can be specified are as follows:

System Settings

The following settings can be specified.

General Features

All the settings can be specified.

Timer Settings

All the settings can be specified.

E-mail Settings

The following settings can be specified.

- SMTP Authentication

  SMTP Authentication

  User Name

  E-mail Address

  Password

  Encryption
- POP before SMTP

  Wait Time after Authent.

  User Name

  E-mail Address

  Password
- Reception Protocol
- POP3 / IMAP4 Settings

  Server Name

  Encryption

  Connection Test
- Administrator's E-mail Address

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

  All Users

  Per User

- User Authentication Management

  You can specify which authentication to use.

  You can also edit the settings for each function.

- Administrator Authentication Management

  Machine Management

- Program / Change Administrator

  Machine Administrator

- Extended Security

  Restrict Display of User Information

  Authenticate Current Job

  @Remote Service

  Update Firmware

  Change Firmware Structure

- Program / Change / Delete LDAP Server

  Name

  Server Name

  Search Base

  Port Number

  Use Secure Connection (SSL)

  Authentication

  Realm Name

  Search Conditions

- Program / Change / Delete Realm

  Realm Name

KDC Server Name

Domain Name

- AOF (Always On)
- Service Mode Lock
- Delete All Logs
- Erase All Memory
- Transfer Log Setting

Note

- The "Erase All Memory" setting is available only if the optional security unit is installed.

Settings via Web Image Monitor

The following settings can be specified.

Top Page

- Reset Device

Device Settings

- System

  Permit Firmware Update

  Permit Firmware Structure Change

  Display IP Address on Device Display Panel

  Output Tray

  Paper Tray Priority
- Paper

  All the settings can be specified.
- Date/Time

  All the settings can be specified.
- Timer

  All the settings can be specified.
- Logs

  All the settings can be specified.
- Download Logs
- E-mail

  All the settings can be specified.

- Auto E-mail Notification

  All the settings can be specified.
- On-demand E-mail Notification

  All the settings can be specified.
- User Authentication Management

  All the settings can be specified.
- Administrator Authentication Management

  Machine Administrator Authentication

  Available Settings for Machine Administrator
- Program/Change Administrator

  You can specify the following administrator settings for the machine administrator.

  Login User Name

  Login Password

  Encryption Password
- LDAP Server

  All the settings can be specified.
- Firmware Update

  All the settings can be specified.
- Program/Change Realm

  All the settings can be specified.

Network

- SNMPv3

Security

- User Lockout Policy

  All the settings can be specified.

RC Gate

- Setup RC Gate

  Request No.
- Update RC Gate Firmware
- RC Gate Proxy Server

Webpage

- Webpage

  Download Help File

Extended Feature Settings

- Startup Setting
- Extended Feature Info
- Install
- Uninstall
- Change Allocation
- Administrator Tools
- Additional Program Startup Setting
- Install Additional Program
- Uninstall Additional Program
- Copy Extended Features
- Copy Card Save Data

Tray Paper Settings

The following settings can be specified.

Tray Paper Settings: Tray 1

- Paper Type
- Paper Thickness

Tray Paper Settings: Tray 2

- Paper Type
- Paper Size
- Paper Thickness

Tray Paper Settings: Tray 3

- Paper Type
- Paper Size
- Paper Thickness

Tray Paper Settings: Tray 4

- Paper Type
- Paper Size
- Paper Thickness

Tray Paper Settings: Tray 5

- Paper Type
- Paper Size

- Paper Thickness

Tray Paper Settings: Tray 6

- Paper Type
- Paper Size
- Paper Thickness

Tray Paper Settings: Tray 7

- Paper Type
- Paper Size
- Paper Thickness

Tray Paper Settings: Interposer Upper Tray

- Paper Size

Tray Paper Settings: Interposer Lower Tray

- Paper Size

Note

- "Tray Paper Settings: Tray 7" is available only if the optional multi bypass tray is installed.
- "Tray Paper Settings: Interposer Upper Tray" and "Tray Paper Settings: Interposer Lower Tray" are available only if the optional cover interposer is installed.

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.

E-mail Settings

- SMTP Server

  Server Name

  Port No.

  Connection Test
- E-mail Communication Port

  All the settings can be specified.
- E-mail Reception Interval
- E-mail Storage in Server

Administrator Tools

- Address Book Management

  Search

  Switch Title
- Address Book: Program / Change / Delete Group

  Search

  Switch Title
- Administrator Authentication Management

  Network Management
- Program / Change Administrator

  Network Administrator

  You can specify the user name and change the full-control user's authority.
- Extended Security

Driver Encryption Key

Settings by SNMPv1, v2

- Network Security Level

Settings via Web Image Monitor

The following settings can be specified.

Device Settings

- System

  Device Name

  Comment

  Location

- E-mail

  Reception

  SMTP

  E-mail Communication Port

- Auto E-mail Notification

  You can select groups to notify.

- Administrator Authentication Management

  Network Administrator Authentication

  Available Settings for Network Administrator

- Program/Change Administrator

  You can specify the following administrator settings for the network administrator.

  Login User Name

  Login Password

  Encryption Password

Interface

- Interface Settings

  Ethernet

Network

- IPv4

  All the settings can be specified.

- IPv6

  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.
- IEEE 802.1X

  All the settings can be specified.

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.

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

Settings via Web Image Monitor

The following 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.

Administrator Tools

- Address Book Management
- Address Book: Program / Change / Delete Group
- Address Book: Change Order
- Address Book: Edit Title
- Address Book: Switch Title
- Back Up / Restore Address Book
- Display / Clear / Print Counter per User

  All Users

  Per User
- Administrator Authentication Management

  User Management
- Program / Change Administrator

  User Administrator
- Extended Security

  Encrypt Address Book

  Encryption Key

  Password Policy

Settings via Web Image Monitor

The following settings can be specified.

Address Book

All the settings can be specified.

Device Settings

- Auto E-mail Notification

  You can select groups to notify.

- Administrator Authentication Management

  User Administrator Authentication

  Available Settings for User Administrator

- Program/Change Administrator

  You can specify the following administrator settings for the user administrator.

  Login User Name

  Login Password

  Encryption Password

Webpage

- Webpage

  Download Help File

Settings that can be Specified by Logging on with the Password for Printer Settings

Settings that can be specified by logging on with the password for printer settings are as follows:

Printer Features

The following settings can be specified.

General Features

All the settings can be specified.

Interface Settings

All the settings can be specified.

Network Security

All the settings can be specified.

Access Control

All the settings can be specified.

IPP Authentication

All the settings can be specified.

SSL / TLS

All the settings can be specified.

Setting via Web Interface

The following settings can be specified.

Configurations/Jobs

All the settings can be specified.

Privileges for User Account Settings in the Address Book

The authorities for using the Address Book are as follows:

The authority designations in the list indicate users with the following authorities.

- Abbreviations in the table heads

  Read-only (User) = This is a user assigned "Read-only" authority.

  Edit (User) = This is a user assigned "Edit" authority.

  Edit / Delete (User) = This is a user assigned "Edit / Delete" authority.

  User Admin. = This is the user administrator.

  Registered User = This is a user that has personal information registered in the Address Book and has a login password and user name.

  Full Control = This is a user granted full control.

- Abbreviations in the table columns

  R/W (Read and Write) = Both reading and modifying the setting are available.

  R (Read) = Reading only.

  N/A (Not Applicable) = Neither reading nor modifying the setting is available.

Tab Name: Names

Settings	Read-only (User)	Edit (User)	Edit / Delete (User)	Full Control	Registered User	User Admin.
Registration No.	R	R/W	R/W	R/W	R/W	R/W
Key Display	R	R/W	R/W	R/W	R/W	R/W
Name	R	R/W	R/W	R/W	R/W	R/W
Select Title	R	R/W	R/W	R/W	R/W	R/W

Tab Name: Auth. Info

Settings	Read-only (User)	Edit (User)	Edit / Delete (User)	Full Control	Registered User	User Admin.
User Code	N/A	N/A	N/A	N/A	N/A	R/W

Settings	Read-only (User)	Edit (User)	Edit / Delete (User)	Full Control	Registered User	User Admin.
Login User Name	N/A	N/A	N/A	N/A	R/W	R/W
Login Password	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" can be entered or changed but not displayed.

Tab Name: Protection

Settings	Read-only (User)	Edit (User)	Edit / Delete (User)	Full Control	Registered User	User Admin.
Protect Destination: Permissions for Users/Groups	N/A	N/A	N/A	R/W	R/W	R/W

User Settings - Control Panel Settings

This section explains which settings users can specify on the control panel. The available settings and functions depend on the configuration of "Available Settings" in "Administrator Authentication Management" and "Menu Protect" in Printer Features. If user authentication is specified, system settings and functions are available to authorized users only, who must log on to access them.

Reference

- p.226 "Printer Functions"
- p.227 "Printer Features"
- p.229 "System Settings"

Printer Functions

Depending on the Menu Protect setting, available functions will vary. If you attempt to specify a locked setting, a message requesting you to enter the password appears. To specify the locked setting, enter the password for printer settings.

When [Menu Protect] is set to [Inactive], all the following settings can be viewed and modified.

Normal Printer Screen

Functions	If Menu Protect is Set
Online/Offline Switching	Password not required
Program Tray Paper Settings	Password required
Recall / Change Tray Paper Settings	Password required
Paper Colour Settings	Password required
Printer Info	Password not required
Current / Waiting Job List	Password not required*1
Print Check Sample	Password required

*1 You can view any job that is currently queued or being printed. However, to cancel these jobs, the password for printer settings is required. Jobs must be canceled by the Printer Features administrator using the password.

Note

- The default for Menu Protect is [Inactive].
- Settings that are not in the list can only be viewed, regardless of the menu protect setting.

Printer Features

Depending on the "Menu Protect" setting, password may be required for operation and setting. If you attempt to specify a locked setting, a message requesting you to enter the password appears. To specify the locked setting, enter the password for printer settings.

When [Menu Protect] is set to [Inactive], all the following settings can be viewed and modified.

General Settings

Settings	If Menu Protect is Set
Resolution	Password required
Wait Timeout	Password required
LPD Job Reception Timing	Password required
Meth. for Switching between 1&2 Sided Feed	Password required
Auto Print Check Sample	Password required
Rotate by 180 Degrees	Password required
Face Up	Password required
Reverse Order Printing	Password required
Job Separation	Password required
Auto Tray Switching: Tray Setting	Password required

PS / PDF Menu

Settings	If Menu Protect is Set
Print Error Report	Password required
Alt. Paper Size with Reduced Print Image	Password required
Job Timeout	Password required
Wait Timeout (PS)	Password required
Halftone Density	Password required
Halftone Screen Frequency	Password required
PDF Password	Password required

Settings	If Menu Protect is Set
Switching between 1&2 Sided Print Functions	Password required

PCL Menu

Settings	If Menu Protect is Set
Extend A4 Width	Password required
Tray Switching	Password required
Auto Orientation (Portrait to Landscape)	Password required

Test Print

Settings	If Menu Protect is Set
System / Printer Information List	Password required
Configuration Page	Password required
Menu List	Password required
Printer HDD Usage Status List	Password required
Programmed Tray Paper Settings List	Password required
PS Configuration / Font Page	Password required
PCL Configuration / Font Page	Password required
Cross Pattern Print	Password required
Raster Pattern Print	Password required

Note

- The default for Menu Protect is [Inactive].

System Settings

When administrator authentication is enabled, the administrator's configuration of Available Settings determines which system settings are available to users.

User privileges are as follows:

- Abbreviations in the table heads

  Not Specified = Authorized user when "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
Status Indicator	R/W	R
Screen Colour Setting	R/W	R
Output: Printer	R/W	R
Paper Tray Priority: Printer	R/W	R
System Status Display Time	R/W	R
Key Repeat	R/W	R
Output Tray Setting	R/W	R
Paper Curl Correction Level	R/W	R
Z-fold Position	R/W	R
Half Fold Position	R/W	R
Letter Fold-out Position	R/W	R

Settings	Not Specified	Specified
Letter Fold-in Position	R/W	R
Double Parallel Fold Position	R/W	R
Gate Fold Position	R/W	R

The following settings are available only if the optional multi-folding unit is installed: "Z-fold Position", "Half Fold Position", "Letter Fold-out Position", "Letter Fold-in Position", "Double Parallel Fold Position", and "Gate Fold Position".

To specify "Output Tray Setting" is available only if the optional stacker is installed.

Tray Paper Settings

Settings	Not Specified	Specified
Paper Type: Tray 1-7	R/W	R
Paper Size: Tray 2-7	R/W	R
Paper Thickness: Tray 1-7	R/W	R
Tray Paper Settings: Interposer Upper Tray	R/W	R
Tray Paper Settings: Interposer Lower Tray	R/W	R

The "Tray Paper Settings: Interposer Upper Tray" and "Tray Paper Settings: Interposer Lower Tray" settings are available only if the optional cover interposer 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
Printer Auto Reset Timer	R/W	R
Set Date	R/W	R

Settings	Not Specified	Specified
Set Time	R/W	R
Auto Logout Timer	R/W	R
Weekly Timer Code	R/W	R
Weekly Timer (Monday-Sunday)	R/W	R

Interface Settings

Settings	Not Specified	Specified
Print List	R/W	N/A

Network

Settings	Not Specified	Specified
Machine IPv4 Address	R/W	R
IPv4 Gateway Address	R/W	R
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
SMB Computer Name	R/W	R
SMB Work Group	R/W	R
Ethernet Speed	R/W	R
IEEE 802.1X Authentication for Ethernet	R/W	R

Settings	Not Specified	Specified
Restore IEEE 802.1X Authentication to Defaults	R/W	N/A
Ping Command	R/W	R
Permit SNMPv3 Communication	R/W	R
Permit SSL / TLS Communication	R/W	R
Host Name	R/W	R
Machine Name	R/W	R

If you set "Machine IPv4 Address", "DNS Configuration", "Domain Name", or "WINS Configuration" to "Auto-Obtain (DHCP)", you can only display the settings.

E-mail Settings

Settings	Not Specified	Specified
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
E-mail Storage in Server	R/W	R

The passwords for "SMTP Authentication" can be entered or changed but not displayed.

Administrator Tools

Settings	Not Specified	Specified
Address Book Management	R/W	R/W

Settings	Not Specified	Specified
Address Book: Program / Change / Delete Group	R/W	R/W
Address Book: Change Order	R/W	N/A
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
Administrator Authentication Management	R/W	N/A
Extended Security	R/W	R
Program / Change / Delete LDAP Server	R/W	R
Program / Change / Delete Realm	R/W	R
AOF (Always On)	R/W	R
Service Mode Lock	R/W	R
Erase All Memory	R/W	N/A
Delete All Logs	R/W	N/A
Transfer Log Setting	R/W	N/A

The password for "Program / Change / Delete LDAP Server" can be entered or changed but not displayed.

The "Erase All Memory" setting is available only if the optional security unit is installed.

User Settings - Web Image Monitor Settings

This section displays the user settings that can be specified on Web Image Monitor when user authentication is specified.

Reference

- p.235 "Device Settings"
- p.241 "Interface"
- p.242 "Network"
- p.244 "Webpage"

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: Printer	R/W	R
Paper Tray Priority: Printer	R/W	R

Paper

Settings	Not Specified	Specified
Tray1: Paper Type	R/W	R
Tray1: Paper Thickness	R/W	R
Tray2: Paper Size	R/W	R
Tray2: Custom Paper Size	R/W	R
Tray2: Paper Type	R/W	R

Settings	Not Specified	Specified
Tray2: Paper Thickness	R/W	R
Tray3: Paper Size	R/W	R
Tray3: Custom Paper Size	R/W	R
Tray3: Paper Type	R/W	R
Tray3: Paper Thickness	R/W	R
Tray4: Paper Size	R/W	R
Tray4: Custom Paper Size	R/W	R
Tray4: Paper Type	R/W	R
Tray4: Paper Thickness	R/W	R
Tray5: Paper Size	R/W	R
Tray5: Custom Paper Size	R/W	R
Tray5: Paper Type	R/W	R
Tray5: Paper Thickness	R/W	R
Tray6: Paper Size	R/W	R
Tray6: Custom Paper Size	R/W	R
Tray6: Paper Type	R/W	R
Tray6: Paper Thickness	R/W	R
Tray7: Paper Size	R/W	R
Tray7: Custom Paper Size	R/W	R
Tray7: Paper Type	R/W	R
Tray7: Paper Thickness	R/W	R
Interposer Upper Tray: Paper Size	R/W	R
Interposer Upper Tray: Custom Paper Size	R/W	R
Interposer Lower Tray: Paper Size	R/W	R

Settings	Not Specified	Specified
Interposer Lower Tray: Custom Paper Size	R/W	R

Date/Time

Settings	Not Specified	Specified
Set Date	R/W	R
Set Time	R/W	R
SNTP Server Name	R/W	R
SNTP Polling Interval	R/W	R
Time Zone	R/W	R

Timer

Settings	Not Specified	Specified
Auto Off Timer	R/W	R
Energy Saver Timer	R/W	R
Panel Off Timer	R/W	R
System Auto Reset Timer	R/W	R
Printer Auto Reset Timer	R/W	R
Auto Logout Timer	R/W	R
Weekly Timer Code	R/W	R
Weekly Timer	R/W	R

Logs

Settings	Not Specified	Specified
Collect Job Logs	R/W	R

Settings	Not Specified	Specified
Job Log Collect Level	R/W	R
Collect Access Logs	R/W	R
Access Log Collect Level	R/W	R
Transfer Logs	R	R
Encrypt Logs	R/W	R
Classification Code	R/W	R
Delete All Logs	R/W	N/A

E-mail

Settings	Not Specified	Specified
Administrator E-mail Address	R/W	R
Reception Protocol	R/W	R
E-mail Reception Interval	R/W	R
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

Settings	Not Specified	Specified
POP Password	R/W	N/A
Timeout setting after POP Auth.	R/W	R
POP3/IMAP4 Server Name	R/W	R
POP3/IMAP4 Encryption	R/W	R
POP3 Reception Port No.	R/W	R
IMAP4 Reception Port No.	R/W	R
E-mail Notification E-mail Address	R/W	R
Receive E-mail Notification	R/W	N/A
E-mail Notification User Name	R/W	N/A
E-mail Notification Password	R/W	N/A

Auto E-mail Notification

Settings	Not Specified	Specified
Groups to Notify: Address List	R/W	R/W

User Authentication Management

Settings	Not Specified	Specified
User Authentication Management	R/W	R
User Code Authentication - User Code Authentication Settings	R/W	R
Basic Authentication - Basic Authentication Settings	R/W	R
Windows Authentication - Windows Authentication Settings	R/W	R
Windows Authentication - Group Settings for Windows Authentication	R/W	R
LDAP Authentication - LDAP Authentication Settings	R/W	R

Settings	Not Specified	Specified
Integration Server Authentication - Integration Server Authentication Settings	R/W	R
Integration Server Authentication - Group Settings for Integration Server Authentication	R/W	R

LDAP Server

Settings	Not Specified	Specified
Program/Change/Delete	R/W	N/A

Interface

The settings available to the user depend on whether or not administrator authentication is enabled.

If administrator authentication is enabled, the settings available to the user depend on whether or not "Available Settings" has been specified.

User privileges are as follows:

- Abbreviations in the table heads

  Not Specified = Authorized user when "Available Settings" have not been specified.

  Specified = Authorized user when "Available Settings" have been specified.

- Abbreviations in the table columns

  R/W (Read and Write) = Both reading and modifying the setting are available.

  R (Read) = Reading only.

  N/A (Not Applicable) = Neither reading nor modifying the setting is available.

Interface Settings

Settings	Not Specified	Specified
Ethernet: Ethernet Security	R/W	R
Ethernet: Ethernet Speed	R/W	R

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
FTP	R/W	R

Settings	Not Specified	Specified
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

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
Language1	R/W	R
Language2	R/W	R
URL1	R/W	R
URL2	R/W	R
Set Help URL Target	R/W	R
UPnP Setting	R/W	R
Download Help File	R/W	R/W

User Settings - Web Interface Settings

This section displays the user settings that can be specified on Web Interface.

Note

- The user authentication settings do not apply to Web Interface.

Reference

- p.246 "Home"
- p.247 "Test Print/Download"

Home

The following Home setting can only be viewed (not configured):

Status

- Selecting the Language

Test Print/Download

Test Print/Download

All the settings can be specified.

Download

All the settings can be specified.

Functions that Require Options

The following functions require certain options and additional functions.

- Hard Disk overwrite erase function

  Security unit

Trademarks

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

Adobe, Acrobat, Acrobat Reader, PostScript, and Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

UPnP™ is a trademark of the UPnP™ Implementers Corporation.

PCL® is a registered trademark of Hewlett-Packard Company.

Apple, AppleTalk, Macintosh, and Mac OS are trademarks of Apple Inc., registered in the U.S. and other countries.

Monotype is a registered trademark of Monotype Imaging, Inc.

Solaris is a trademark or registered trademark of Sun Microsystems, Inc. in the United States and other countries.

LINUX® is the registered trademark of Linus Torvalds in the U.S. and other countries.

RED HAT is a registered trademark of Red Hat, Inc.

PowerPC® is a trademark of International Business Machines Corporation in the United States, other countries, or both.

Other product names used herein are for identification purposes only and might be trademarks of their respective companies. We disclaim any and all rights to those marks.

The proper names of the Windows operating systems are as follows:

- The product names of Windows 2000 are as follows:

  Microsoft® Windows® 2000 Professional

  Microsoft® Windows® 2000 Server

  Microsoft® Windows® 2000 Advanced Server
- The product names of Windows XP are as follows:

  Microsoft® Windows® XP Professional

  Microsoft® Windows® XP Home Edition

  Microsoft® Windows® XP Media Center Edition

  Microsoft® Windows® XP Tablet PC Edition
- The product names of Windows Vista are as follows:

  Microsoft® Windows Vista® Ultimate

  Microsoft® Windows Vista® Enterprise

  Microsoft® Windows Vista® Business

  Microsoft® Windows Vista® Home Premium

Microsoft® Windows Vista® Home Basic

- The product names of Windows 7 are as follows:

  Microsoft® Windows® 7 Home Premium

  Microsoft® Windows® 7 Professional

  Microsoft® Windows® 7 Ultimate

  Microsoft® Windows® 7 Enterprise

- The product names of Windows Server 2003 are as follows:

  Microsoft® Windows Server® 2003 Standard Edition

  Microsoft® Windows Server® 2003 Enterprise Edition

- The product names of Windows Server 2003 R2 are as follows:

  Microsoft® Windows Server® 2003 R2 Standard Edition

  Microsoft® Windows Server® 2003 R2 Enterprise Edition

- The product names of Windows Server 2008 are as follows:

  Microsoft® Windows Server® 2008 Standard

  Microsoft® Windows Server® 2008 Enterprise

- The product names of Windows Server 2008 R2 are as follows:

  Microsoft® Windows Server® 2008 R2 Standard

  Microsoft® Windows Server® 2008 R2 Enterprise

INDEX

M

N

O

P

R

S

T

U

W

Operating Instructions Security Reference