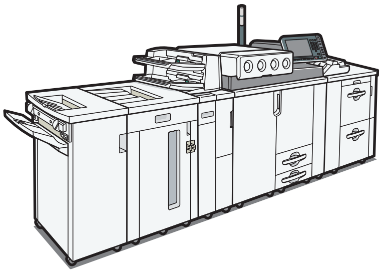
Pro C901

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. Ensuring Information Security

4. Managing Access to the Machine

5. Enhanced Network Security

6. Specifying the Extended Security Functions

7. Troubleshooting

8. Appendix

Manuals for This Machine

Read this manual carefully before you use this machine.

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

Important

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

About This Machine

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

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

Troubleshooting

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

Network Guide

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

General Settings Guide

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

Paper Settings Reference

Explains how to make paper settings.

Security Reference

This manual is for administrators of the machine. It explains security functions that you can use to prevent unauthorized use of the machine, data tampering, or information leakage.

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

Note

- In addition to the above, manuals are also provided for the Printer function.

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 manufacturer recommends that you use genuine toner from the manufacturer.

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

How to Read This Manual

Symbols

This manual uses the following symbols:

★ Important

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

↓ Note

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

Reference

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

[ ]

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

Names of Major Items

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

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

IP Address

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

Notes

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

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

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

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

1. Getting Started

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

Before Using the Security Functions

Important

- **If the security settings are not configured, the data in the machine is vulnerable to attack.**

1. To prevent this machine being stolen or willfully damaged, etc., install it in a secure location.
2. Purchasers of this machine must make sure that people who use it do so appropriately, in accordance with operations determined by the machine administrator and supervisor. If the administrator or supervisor does not make the required security settings, there is a risk of security breaches by users.
3. Before setting this machine's security features and to ensure appropriate operation by users, administrators must read the Security Reference completely and thoroughly, paying particular attention to the section entitled "Before Using the Security Functions".
4. Administrators must inform users regarding proper usage of the security functions.
5. Administrators should routinely examine the machine's logs to check for irregular and unusual events.
6. If this machine is connected to a network, its environment must be protected by a firewall or similar.
7. For protection of data during the communication stage, apply the machine's communication security functions and connect it to devices that support security functions such as encrypted communication.

This machine features a user authentication function that, when activated, prevents users without a login user name and password from using this machine or accessing it over a network. If user authentication is activated, users must enter a login user name and password to use this machine or access it over a network.

There are five types of user authentication methods: User Code authentication, Basic authentication, Windows authentication, LDAP authentication, and Integration Server authentication. If an application that enables use of extended features is installed on the machine, you can limit the extended features available under each user code by specifying Basic authentication, Windows authentication, LDAP authentication, or Integration Server authentication. If you specify Basic authentication, Windows authentication, LDAP authentication, or Integration Server authentication, you cannot apply authentication to control access to print jobs.

Note

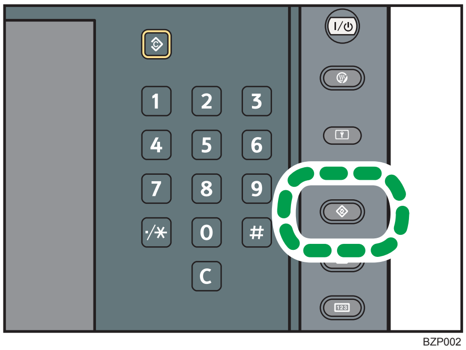
- For details about applications that enable use of extended features, contact your sales or service representative.

Setting Up the Machine

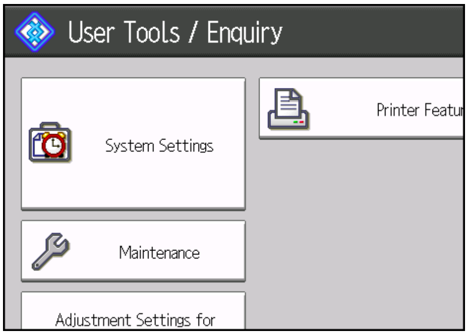
This section describes how to enable encryption of transmitted data and configure the administrator account. If you want a high level of security, make the following setting before using the machine.

Enabling security

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



3. Press [System Settings].



User Tools / Enquiry

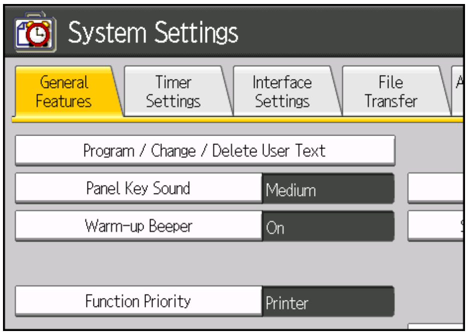
System Settings

Printer Featu

Maintenance

Adjustment Settings for

4. Press [Interface Settings].



System Settings

General Features | Timer Settings | Interface Settings | File Transfer | A

Program / Change / Delete User Text

Panel Key Sound: Medium

Warm-up Beeper: On

Function Priority: Printer

5. **Specify IPv4 Address.**

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

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

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

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

   The E-mail page appears.

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

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

11. **Enable secure sockets layer (SSL).**

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

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

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

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

Enabling enhanced security

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

   The Network Security page appears.

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

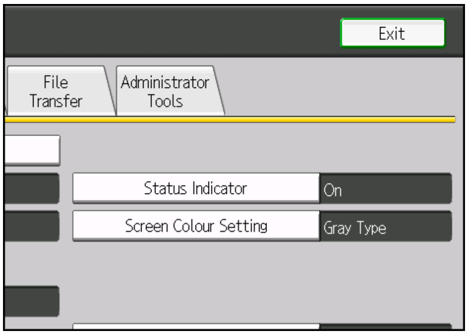
   Only ports that have high security can be used. Note that some functions will be unavailable after you select [Level 2] for this setting. For details, see "Status of Functions under each Network Security Level" and "Enabling/Disabling Protocols".

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

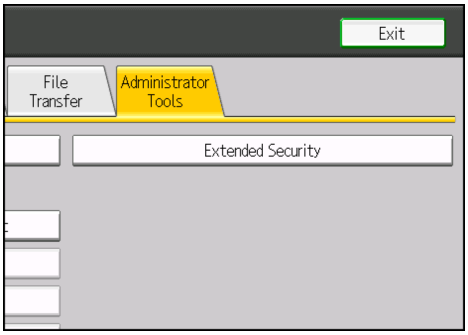
   For details about the functions that will be unavailable if "FTP" and "SNMPv3" are set to [Inactive], see "Enabling/Disabling Protocols".

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

8. **Press [Administrator Tools].**

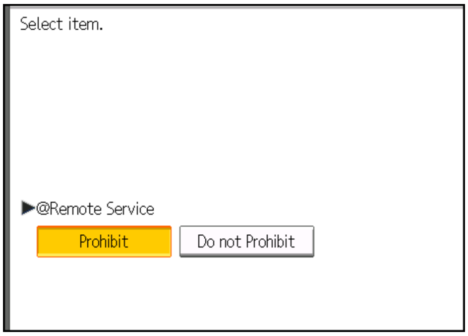


9. **Press [Extended Security].**



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

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



Select item.

▶@Remote Service

[✓ Prohibit] Do not Prohibit

11. **Press [OK].**

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

13. **Disconnect the machine from the administrators-only network, and then connect it to the general use network.**

Reference

- p.30 "Registering the Administrator"
- p.35 "Using Web Image Monitor to Configure Administrator Authentication"

- p.82 "Enabling/Disabling Protocols"
- p.88 "Status of Functions under each Network Security Level"
- p.90 "Protection Using Encryption"

Enhanced Security

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

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

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

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

Authentication and Access Limits

Using authentication, administrators manage the machine and its users. To enable authentication, information about both administrators and users must be registered in order to authenticate users via their login user names and passwords.

Four types of administrators manage specific areas of machine usage, such as settings and user registration.

Access limits for each user are specified by the administrator responsible for user access to machine functions and data stored in the machine.

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

Encryption Technology

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

Reference

- p.21 "Administrators and Users"

Glossary

Administrator

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

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

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

Supervisor

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

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

User

A user performs normal operations on the machine.

Registered User

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

Administrator Authentication

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

User Authentication

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

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

Login

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

Logout

This action is required with administrator and user authentication. This action is required when you have finished using the machine or changing the settings.

Security Measures Provided by this Machine

Using Authentication and Managing Users

Enabling Authentication

To control administrators' and users' access to the machine, perform administrator authentication and user authentication using login user names and login passwords. To perform authentication, the authentication function must be enabled. For details about authentication settings, see "Enabling Authentication".

Specifying 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.26 "Enabling Authentication"
- p.78 "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 being used by unregistered users.

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

Overwriting the Data on the Hard Disk

Before disposing of the machine, make sure all data on the hard disk is deleted. Prevent data leakage by automatically deleting transmitted printer jobs from the memory.

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

Reference

- p.65 "Protecting the Address Book"
- p.69 "Deleting Data on the Hard Disk"

Limiting and Controlling Access

Preventing Modification of Machine Settings

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

Register the administrators so that users cannot change the administrator settings. For details about preventing modification of machine settings, see "Preventing Modification of Machine Settings".

Limiting Available Functions

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

Reference

- p.77 "Preventing Modification of Machine Settings"
- p.78 "Limiting Available Functions"

Enhanced Network Security

Preventing Unauthorized Access

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

Safer Communication Using SSL and SNMPv3

You can encrypt this machine's transmissions using SSL and SNMPv3. 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 and SNMPv3, see "Protection Using Encryption".

Reference

- p.81 "Preventing Unauthorized Access"
- p.90 "Protection Using Encryption"

2. Authentication and its Application

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

Administrators and Users

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

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

Specify administrator authentication, and then specify user authentication.

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

Important

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

Reference

- p.40 "Specifying Login User Name and Login Password"

Administrators

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

Sharing administrator tasks eases the burden on individual administrators while also limiting unauthorized operation by administrators. You can also specify a supervisor who can change each administrator's password.

User Administrator

This is the administrator who manages personal information in the address book.

A user administrator can register/delete users in the address book or change users' personal information.

Users registered in the address book can also change and delete their own information.

If any of the users forget their password, the user administrator can delete it and create a new one, allowing the user to access the machine again.

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

Machine Administrator

This is the administrator who mainly manages the machine's default settings. You can set the machine so that the default for each function can only be specified by the machine administrator. By making this setting, you can prevent unauthorized people from changing the settings and allow the machine to be used securely by its many users.

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

Network Administrator

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

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

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

File Administrator

This is the administrator who manages permission to access stored files. You can specify 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.

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

Supervisor

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

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

Reference

- p.30 "Registering the Administrator"
- p.125 "Supervisor Operations"

User

Users are managed using the personal information in the machine's address book.

By enabling user authentication, you can allow only people registered in the address book to use the machine. Users can be managed in the address book by the user administrator.

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

The Management Function

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

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.**
- **Be sure not to forget the supervisor login user name and login password. If you do forget them, a service representative will have to return the machine to its default state. This will result in all data in the machine being lost and the service call may not be free of charge.**

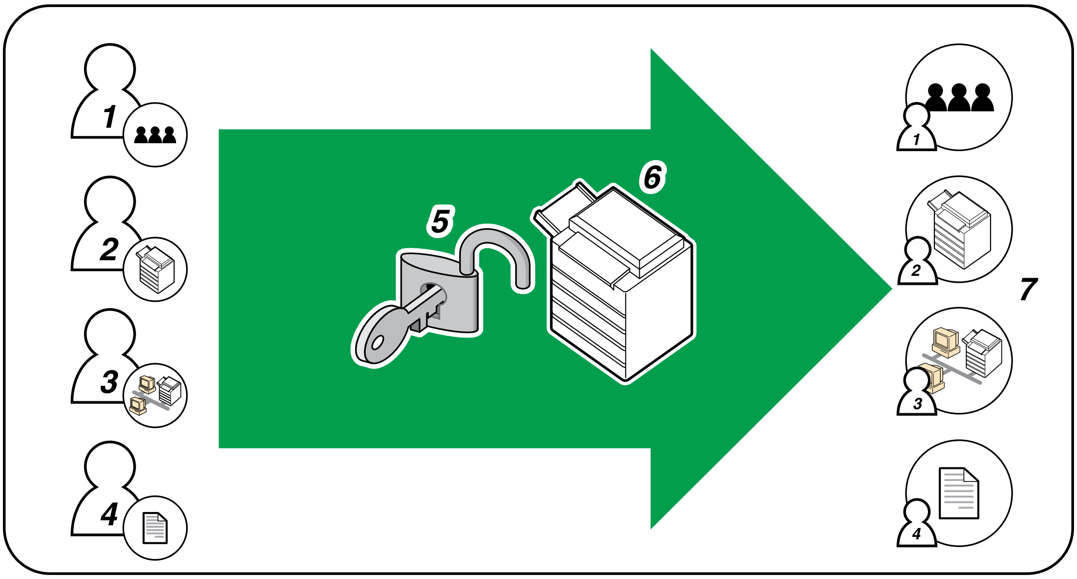
Reference

- p.125 "Supervisor Operations"

About Administrator Authentication

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

For details about each administrator, see "Administrators and Users".



BZM004

1. **User Administrator**

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

2. **Machine Administrator**

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

3. **Network Administrator**

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

4. **File Administrator**

   This administrator manages permission to access stored files. 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 machine**

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

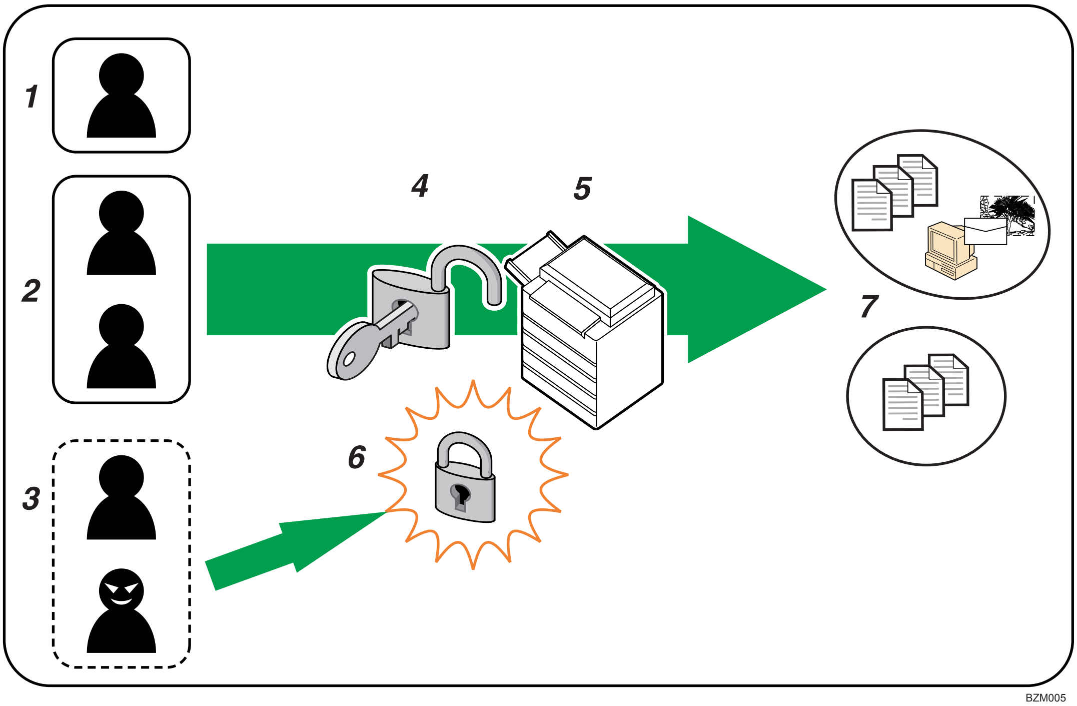
Reference

- p.21 "Administrators and Users"

About User Authentication

This machine has an authentication function to prevent unauthorized access.

By using login user name and login password, you can specify access limits for individual users and groups of users.



1. **User**

   A user performs normal operations on the machine.

2. **Group**

   A group performs normal operations on the machine.

3. **Unauthorized User**

4. **Authentication**

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

5. **This Machine**

6. **Access Limit**

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

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

Enabling Authentication

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

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

Reference

- p.30 "Registering the Administrator"

Authentication Setting Procedure

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

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

Note

- To specify Basic Authentication, Windows Authentication, LDAP Authentication, or Integration Server Authentication, you must first specify administrator authentication.

- You can specify User Code Authentication without specifying administrator authentication.

Reference

- p.28 "Administrator Authentication"
- p.28 "Specifying Administrator Privileges"
- p.30 "Registering the Administrator"
- p.36 "User Authentication"
- p.37 "User Code Authentication"
- p.39 "Basic Authentication"
- p.44 "Windows Authentication"
- p.50 "LDAP Authentication"
- p.55 "Integration Server Authentication"

Administrator Authentication

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

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

Note

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

Specifying Administrator Privileges

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

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

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

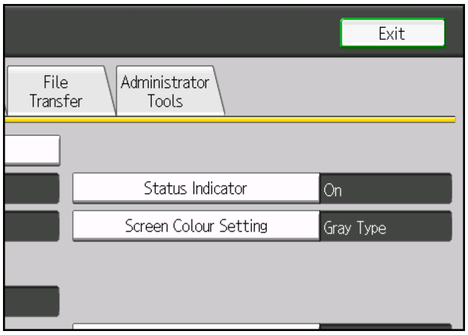
For details about logging in and logging out with administrator authentication, see "Logging in Using Administrator Authentication" and "Logging out Using Administrator Authentication".

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 details about changing the administrator password using the supervisor's authority, see "Supervisor Operations".**

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

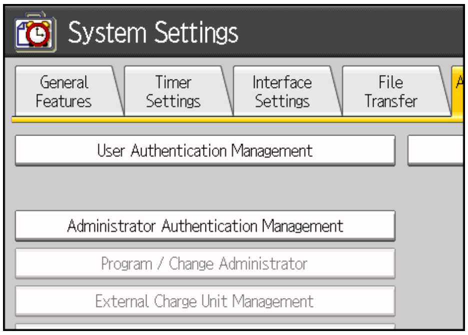
3. **Press [Administrator Tools].**



Status Indicator: On

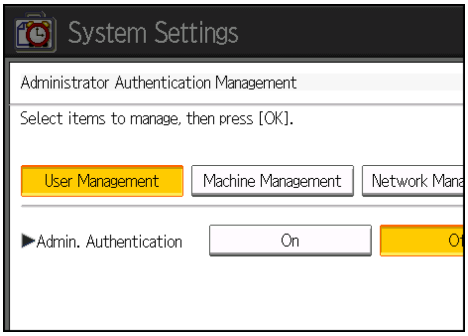
Screen Colour Setting: Gray Type

4. **Press [Administrator Authentication Management].**


System Settings
General Features
Timer Settings
Interface Settings
File Transfer
A
User Authentication Management
Administrator Authentication Management
Program / Change Administrator
External Charge Unit 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] key to select which settings to manage.**



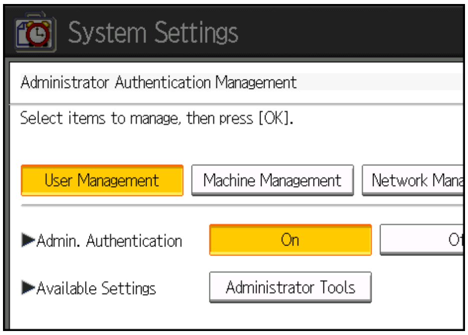
Select items to manage, then press [OK].

▶Admin. Authentication

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

"Available Settings" appears.

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



System Settings

Administrator Authentication Management

Select items to manage, then press [OK].

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

8. **Press [OK].**

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

Note

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

Reference

- p.33 "Logging in Using Administrator Authentication"
- p.34 "Logging out Using Administrator Authentication"
- p.78 "Limiting Available Functions"
- p.125 "Supervisor Operations"

Registering the Administrator

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

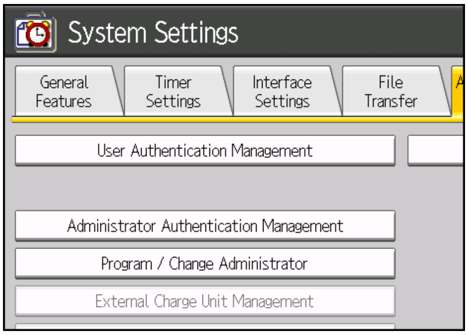
The sharing of administrator tasks eases the burden on individual administrators while also limiting unauthorized operation by a single administrator. You can register up to four login user names (Administrators 1-4) to which you can grant administrator privileges.

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

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

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

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



System Settings

General Features | Timer Settings | Interface Settings | File Transfer | A

User Authentication Management

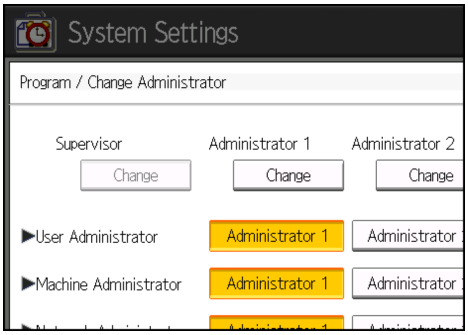
Administrator Authentication Management

Program / Change Administrator

External Charge Unit Management

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].**

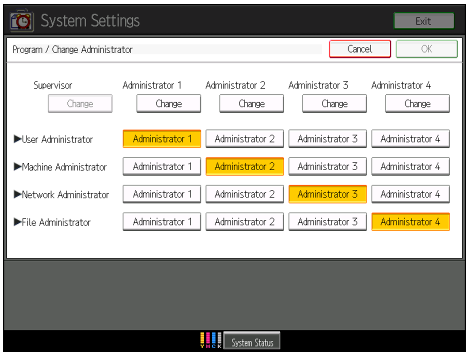


System Settings

Program / Change Administrator

	Supervisor	Administrator 1	Administrator 2
	Change	Change	Change
▶User Administrator		Administrator 1	Administrator
▶Machine Administrator		Administrator 1	Administrator

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



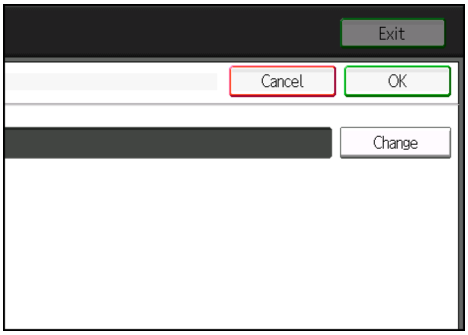
System Settings Exit

Program / Change Administrator Cancel OK

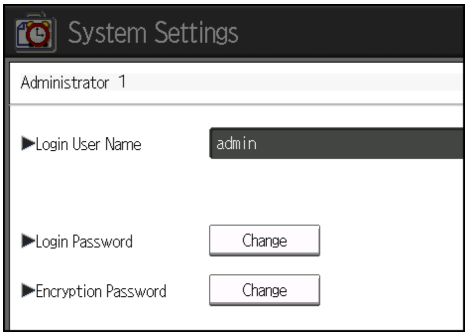
	Supervisor	Administrator 1	Administrator 2	Administrator 3	Administrator 4
	Change	Change	Change	Change	Change
▶User Administrator		Administrator 1	Administrator 2	Administrator 3	Administrator 4
▶Machine Administrator		Administrator 1	Administrator 2	Administrator 3	Administrator 4
▶Network Administrator		Administrator 1	Administrator 2	Administrator 3	Administrator 4
▶File Administrator		Administrator 1	Administrator 2	Administrator 3	Administrator 4

System Status

6. **Press [Change] for "Login User Name".**



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



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

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

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

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

    You will be automatically logged out.

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

Note

- When registering login user names and login passwords, you can specify up to 32 alphanumeric characters and symbols. Keep in mind that user names and passwords are case-sensitive. User names cannot contain numbers only, a space, colon (:), or quotation mark ("), nor can they be left blank.

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

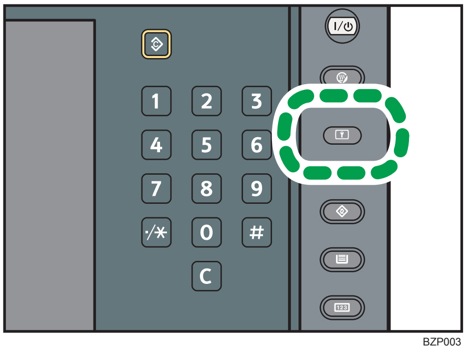
Reference

- p.33 "Logging in Using Administrator Authentication"
- p.34 "Logging out Using Administrator Authentication"
- p.99 "Specifying the Extended Security Functions"

Logging in Using Administrator Authentication

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

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



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

3. **Press [Login].**

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

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

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

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

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

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

Note

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

- If the user name entered at login has multiple administrator privileges, any administrator name with administrator privileges will be displayed.

Logging out Using Administrator Authentication

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

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

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

Changing the Administrator

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

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

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

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

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

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

Note

- An administrator's privileges can be changed only by an administrator who has the privileges of the administrator concerned.

- Administrator privileges cannot be revoked by any single administrator.

Reference

- p.33 "Logging in Using Administrator Authentication"
- p.34 "Logging out Using Administrator Authentication"

Using Web Image Monitor to Configure Administrator Authentication

Using Web Image Monitor, you can log in to the machine and change the administrator settings. This section describes how to access Web Image Monitor.

For details about Web Image Monitor, see Web Image Monitor Help.

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

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

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

   The Web browser might be configured to auto complete login dialog boxes by retaining user names and passwords. This function reduces security. To prevent the browser retaining user names and passwords, disable the browser's auto complete function.
5. **Make settings as desired.**
6. **Click [Logout].**

Note

- When logging in as an administrator use the login name and password of an administrator set in the machine. The default login name is "admin" and the password is blank.

User Authentication

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

For general usage, User Code authentication is adequate. Select Basic authentication, Windows authentication, LDAP authentication, or Integration Server authentication if an application that features extended features is installed on the machine and you require use of its extended features.

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.
- A user code account, that has no more than eight digits and is used for User Code authentication, can be carried over and used as a login user name even after the authentication method has switched from User Code authentication to Basic authentication, Windows authentication, LDAP authentication, or Integration Server authentication. In this case, since the User Code authentication does not have a password, the login password is set as blank.
- When authentication switches to an external authentication method (Windows authentication, LDAP authentication, or Integration Server authentication), authentication will not occur, unless the external authentication device has the carried over user code account previously registered. However, the user code account will remain in the address book of the machine despite an authentication failure. From a security perspective, when switching from User Code authentication to another authentication method, we recommend that you delete accounts you are not going to use, or set up a login password. For details about deleting accounts, see "Deleting a Registered Name", General Settings Guide. For details about changing passwords, see "Specifying Login User Name and Login Password".
- You cannot use more than one authentication method at the same time.
- User authentication can also be specified via Web Image Monitor. For details, see Web Image Monitor Help.
- For printer job authentication, user code authentication is required.

Reference

- p.40 "Specifying Login User Name and Login Password"

User Code Authentication

This is an authentication method for limiting access to functions according to a user code. The same user code can be used by more than one user. Specifying user code authentication allows you to enforce job authentication by user code.

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

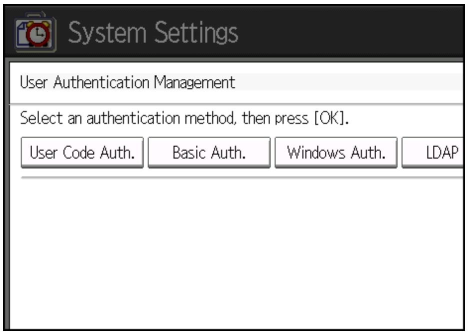
Specifying User Code Authentication

This can be specified by the machine administrator.

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

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

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

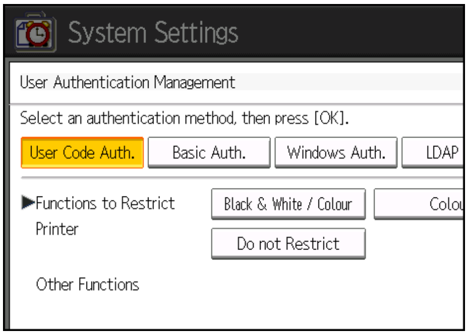
   System Settings

   User Authentication Management

   Select an authentication method, then press [OK].

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

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



System Settings

User Authentication Management

Select an authentication method, then press [OK].

The selected settings will be unavailable to users.

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

7. **Press [OK].**

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

A confirmation message appears.

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

Reference

- p.33 "Logging in Using Administrator Authentication"
- p.34 "Logging out Using Administrator Authentication"
- p.78 "Limiting Available Functions"

Basic Authentication

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

Reference

- p.40 "Authentication Information Stored in the Address Book"

Specifying Basic Authentication

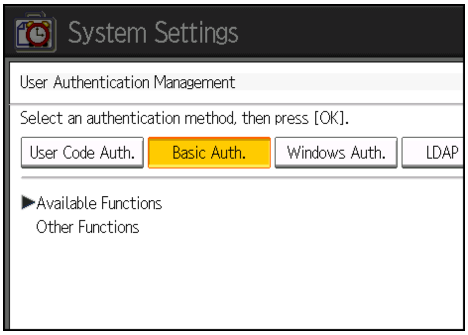
This can be specified by the machine administrator.

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

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

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

   If you do not want to use user authentication management, select [Off].
6. **Select which of the machine's functions you want to permit.**



System Settings

User Authentication Management

Select an authentication method, then press [OK].

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

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

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

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

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

   A confirmation message appears.

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

Reference

- p.33 "Logging in Using Administrator Authentication"
- p.34 "Logging out Using Administrator Authentication"
- p.37 "User Code Authentication"
- p.78 "Limiting Available Functions"

Authentication Information Stored in the Address Book

This can be specified by the user administrator.

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

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

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

User authentication can also be specified via Web Image Monitor.

Reference

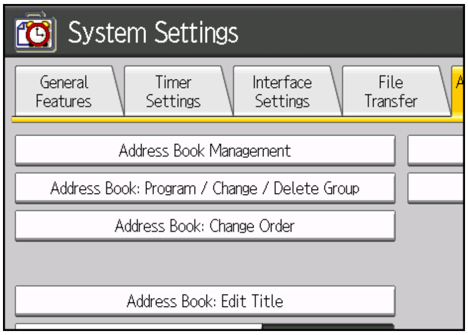
- p.33 "Logging in Using Administrator Authentication"
- p.34 "Logging out Using Administrator Authentication"

Specifying Login User Name and Login Password

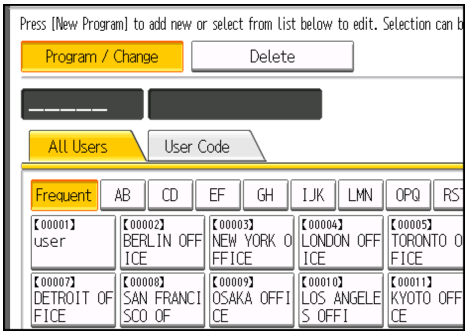
In [Address Book Management], specify the login user name and login password to be used for User Authentication Management.

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

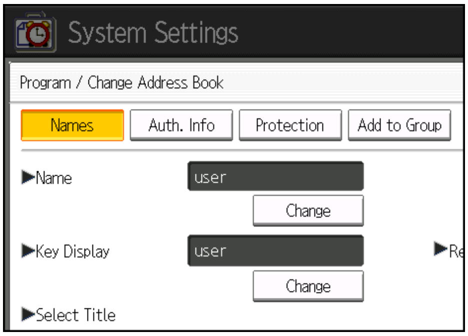
4. **Press [Address Book Management].**



5. **Select the user.**


Press [New Program] to add new or select from list below to edit. Selection can b

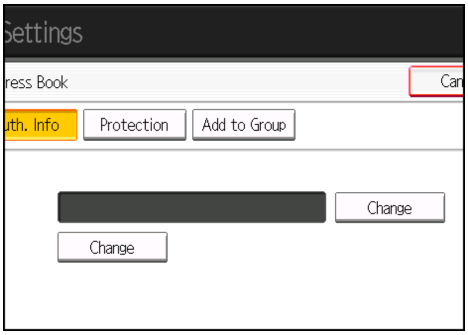
6. **Press [Auth. Info].**



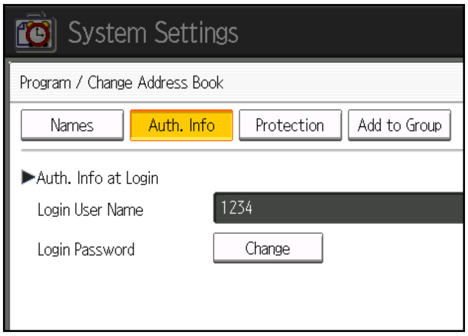
▶Name user

▶Key Display user

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



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



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

Note

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

Reference

- p.99 "Specifying the Extended Security Functions"

Windows Authentication

Specify this authentication when using the Windows domain controller to authenticate users who have their accounts on the directory server. Users cannot be authenticated if they do not have their accounts in the directory server. Under Windows authentication, you can specify the access limit for each group registered in the directory server. The address book stored in the directory server can be registered to the machine, enabling user authentication without first using the machine to register individual settings in the address book.

Operational Requirements for Windows Authentication

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

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

★ Important

- **During Windows Authentication, data registered in the directory server is automatically registered in the machine. If user information on the server is changed, information registered in the machine may be overwritten when authentication is performed.**
- **If you have created a new user in the domain controller and selected "User must change password at next logon", log in to the machine from the computer to change the password before logging in from the machine's control panel.**

Note

- Enter the login password correctly; keeping in mind that it is case-sensitive.
- The first time you access the machine, you can use the functions available to your group. If you are not registered in a group, you can use the functions available under [*Default Group]. To limit which functions are available to which users, first make settings in advance in the address book. When accessing the machine subsequently, you can use all the functions available to your group and to you as an individual user.
- Users who are registered in multiple groups can use all the functions available to those groups.
- A user registered in two or more global groups can use all the functions available to members of those groups.

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

Specifying Windows Authentication

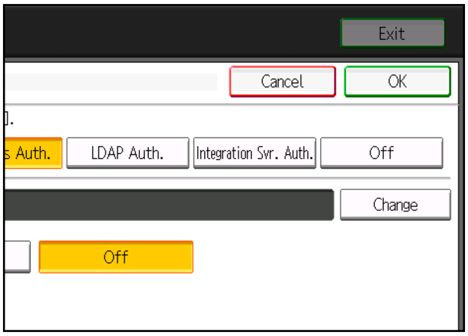
This can be specified by the machine administrator.

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

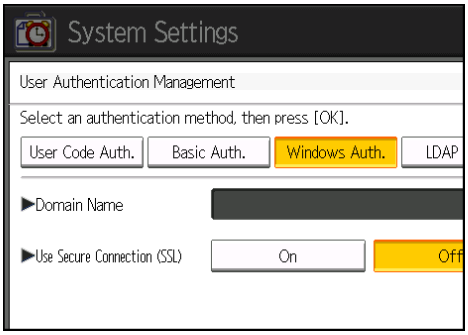
1. **Press the [User Tools] key.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [User Authentication Management].**

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

   If you do not want to use user authentication management, select [Off].
6. **Press [Change] for "Domain Name", enter the name of the domain controller to be authenticated, and then press [OK].**



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



System Settings

User Authentication Management

Select an authentication method, then press [OK].

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

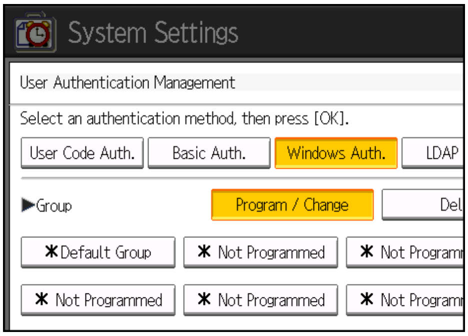
If global groups have been registered under Windows server, you can limit the use of functions for each global group.

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

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

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

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

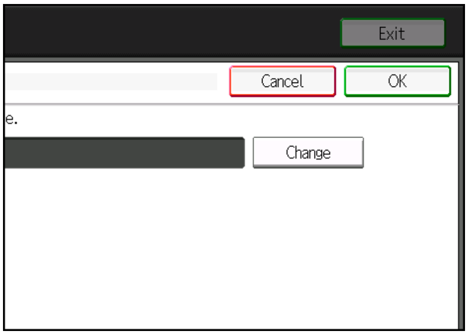


System Settings

User Authentication Management

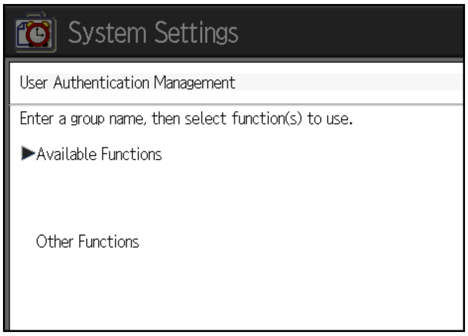
Select an authentication method, then press [OK].

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



10. **Press [OK].**

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



Enter a group name, then select function(s) to use.

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

Windows Authentication will be applied to the selected functions.

Users can use the selected functions only.

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

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

12. **Press [OK] twice.**

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

A confirmation message appears.

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

Reference

- p.33 "Logging in Using Administrator Authentication"
- p.34 "Logging out Using Administrator Authentication"
- p.37 "User Code Authentication"
- p.78 "Limiting Available Functions"

Creating the Server Certificate

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

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

1. **Start Internet Services Manager.**
2. **Right-click [Default Web Site], and then click [Properties].**
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 (Certificate Issued by a Certificate Authority)

Install the device certificate using Web Image Monitor.

This section describes the use of a certificate issued by a certificate authority as the device certificate.

Enter the device certificate contents issued by the certificate authority.

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

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

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

   The network administrator can log in.

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

   The Device Certificate page appears.
5. **Check the radio button next to the number of the certificate you want to install.**
6. **Click [Install].**

7. **Enter the contents of the device certificate.**

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

8. **Click [OK].**

   The setting is changed.

9. **Click [OK].**

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

10. **Click [Logout].**

Note

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

LDAP Authentication

Specify this authentication method when using the LDAP server to authenticate users who have their accounts on the LDAP server. Users cannot be authenticated if they do not have their accounts on the LDAP server. The address book stored in the LDAP server can be registered to the machine, enabling user authentication without first using the machine to register individual settings in the address book. When using LDAP authentication, to prevent the password information being sent over the network unencrypted, it is recommended that communication between the machine and LDAP server be encrypted using SSL. You can specify on the LDAP server whether or not to enable SSL. To do this, you must create a server certificate for the LDAP server.

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

Operational Requirements for LDAP Authentication

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

- The network configuration must allow the machine to detect the presence of the LDAP server.
- When SSL is being used, TLSv1, SSLv2, or SSLv3 can function on the LDAP server.
- The LDAP server must be registered in the machine.
- When registering the LDAP server, the following setting must be specified.
    - Server Name
    - Search Base
    - Port Number
    - Use Secure Connection (SSL)
    - Authentication

      Select either "High Security", or "On".
    - User Name

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

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

Important

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

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

Note

- Under LDAP Authentication, if "Anonymous Authentication" in the LDAP server's settings is not set to Prohibit, users who do not have an LDAP server account might still be able to gain access.
- If the LDAP server is configured using Windows Active Directory, "Anonymous Authentication" might be available. If Windows authentication is available, we recommend you use it.
- The first time an unregistered user accesses the machine after LDAP authentication has been specified, the user is registered in the machine and can use the functions available under "Available Functions" during LDAP Authentication. To limit the available functions for each user, register each user and corresponding "Available Functions" setting in the address book, or specify "Available Functions" for each registered user. The "Available Functions" setting becomes effective when the user accesses the machine subsequently.

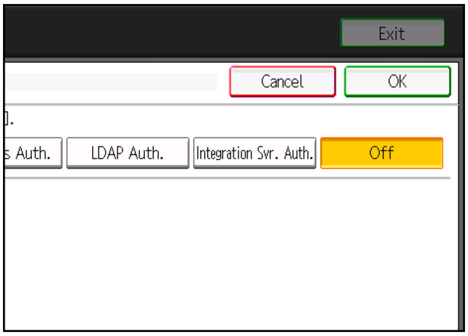
Specifying LDAP Authentication

This can be specified by the machine administrator.

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

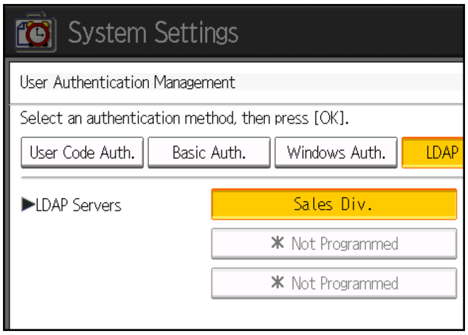
1. **Press the [User Tools] key.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [User Authentication Management].**

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

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

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

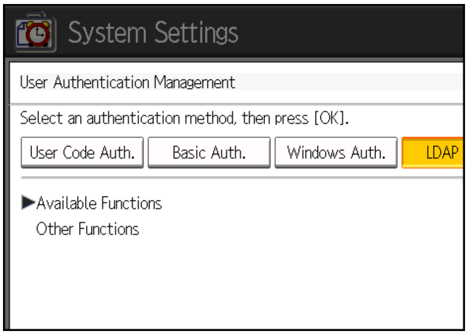


System Settings

User Authentication Management

Select an authentication method, then press [OK].

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



System Settings

User Authentication Management

Select an authentication method, then press [OK].

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

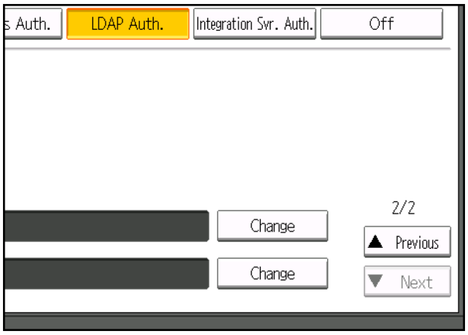
LDAP Authentication will be applied to the selected functions.

Users can use the selected functions only.

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

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

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



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

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

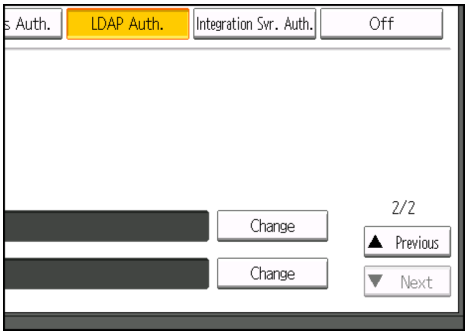
   To specify multiple login attributes, place a comma (,) between them. The search will return hits for either or both attributes.

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

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

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

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



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

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

12. **Press [OK].**

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

    A confirmation message appears.

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

Reference

- p.33 "Logging in Using Administrator Authentication"
- p.34 "Logging out Using Administrator Authentication"
- p.37 "User Code Authentication"

- p.78 "Limiting Available Functions"

Integration Server Authentication

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

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

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

Important

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

Specifying Integration Server Authentication

This can be specified by the machine administrator.

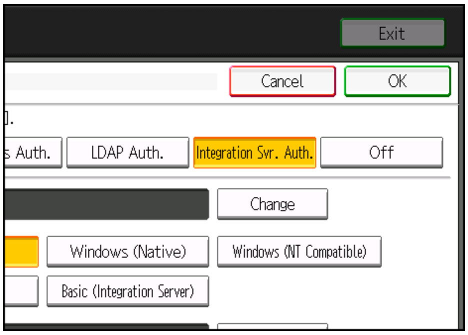
For details about logging in and logging out with administrator authentication, see "Logging in Using Administrator Authentication" and "Logging out Using Administrator Authentication".

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

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

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

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



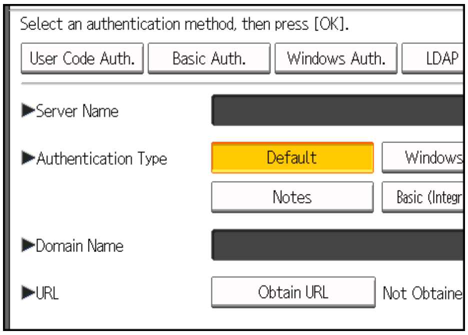
Specify the name of the server for external authentication.

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

Enter the IPv4 address or host name.

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

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


Select an authentication method, then press [OK].

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

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

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

11. **Press [Obtain URL].**

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

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

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

12. **Press [Exit].**

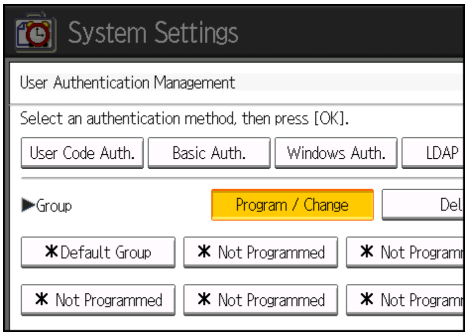
In the "Authentication Type", if you have not registered a group, proceed to step 17.

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

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

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

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



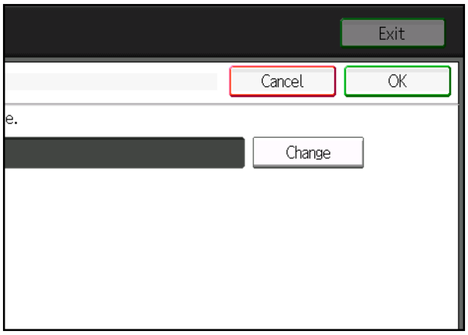
System Settings

User Authentication Management

Select an authentication method, then press [OK].

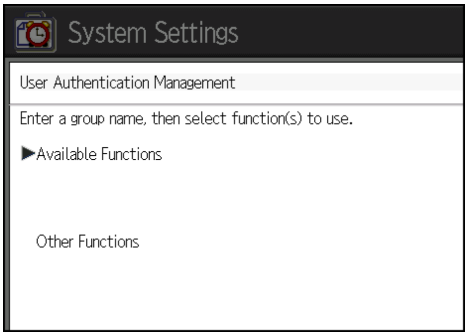
If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.

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



15. **Press [OK].**

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



System Settings

User Authentication Management

Enter a group name, then select function(s) to use.

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

Authentication will be applied to the selected functions.

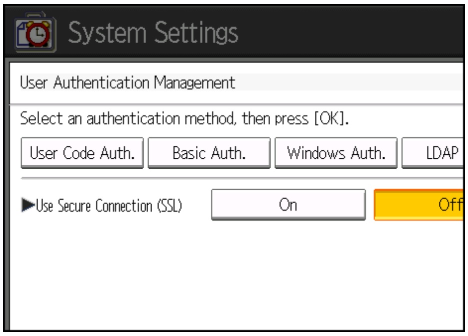
Users can use the selected functions only.

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

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

17. **Press [OK].**

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



System Settings

User Authentication Management

Select an authentication method, then press [OK].

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

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

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

A confirmation message appears.

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

Reference

- p.33 "Logging in Using Administrator Authentication"
- p.34 "Logging out Using Administrator Authentication"
- p.37 "User Code Authentication"
- p.78 "Limiting Available Functions"

If User Authentication is Specified

When user authentication (User Code Authentication, Basic Authentication, Windows Authentication, LDAP Authentication, or Integration Server Authentication) is set, the authentication screen is displayed. To use the machine's security functions, each user must enter a valid user name and password. Log in to operate the machine, and log out when you are finished operations. Be sure to log out to prevent unauthorized users from using the machine. When auto logout timer is specified, the machine automatically logs you out if you do not use the control panel within a given time.

Note

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

Reference

- p.61 "Auto Logout"

If User Code Authentication is Specified

If an application that enables use of extended features is installed on the machine and user code authentication is enabled, a message requesting authentication appears whenever you try to switch to an application. To log in to the machine, enter the user code. User code authentication can also be used for printer job authentication.

Logging in Using the Control Panel

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

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

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

Note

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

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

If an application that enables use of extended features is installed on the machine and Basic Authentication, Windows Authentication, LDAP Authentication, or Integration Server Authentication is enabled, a message requesting authentication appears whenever you try to switch to an application. To log in to the machine, enter the login user name and password.

Logging in Using the Control Panel

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

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

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

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

Logging out Using the Control Panel

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

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

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

Note

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

Logging in Using Web Image Monitor

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

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

Note

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

Logging out Using Web Image Monitor

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

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

Note

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

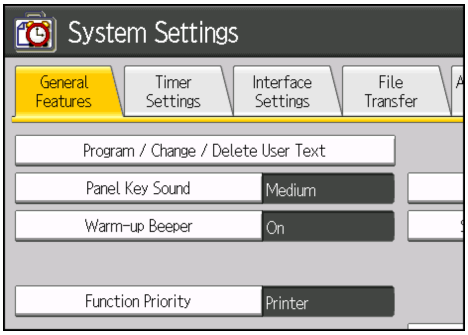
Auto Logout

This can be specified by the machine administrator.

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

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

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

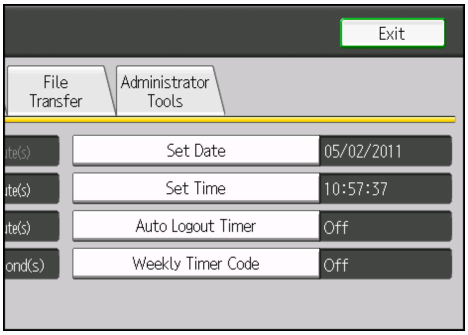


Panel Key Sound Medium

Warm-up Beeper On

Function Priority Printer

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



Set Date 05/02/2011

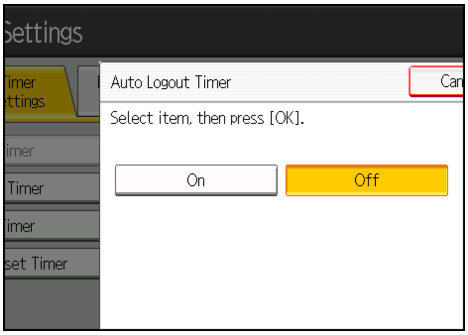
Set Time 10:57:37

Auto Logout Timer Off

Weekly Timer Code Off

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

5. **Select [On].**

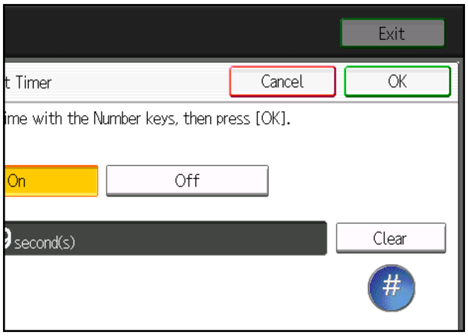


Auto Logout Timer

Select item, then press [OK].

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 [#].**



t Timer

ime with the Number keys, then press [OK].

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

A confirmation message appears.

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

Note

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

Reference

- p.33 "Logging in Using Administrator Authentication"
- p.34 "Logging out Using Administrator Authentication"

Authentication Using an External Device

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

For details, contact your sales representative.

3. Ensuring Information Security

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

Protecting the Address Book

You can specify who is allowed to access the data in the address book. By making this setting, you can prevent the data in the address book being used by unregistered users.

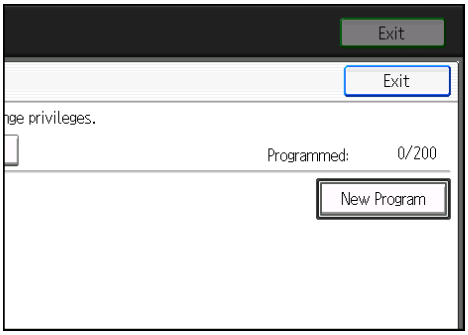
To protect the data from unauthorized reading, you can also encrypt the data in the address book.

Address Book Access Permission

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

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

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

Note

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

Reference

- p.33 "Logging in Using Administrator Authentication"
- p.34 "Logging out Using Administrator Authentication"

Encrypting Data in the Address Book

This can be specified by the user administrator.

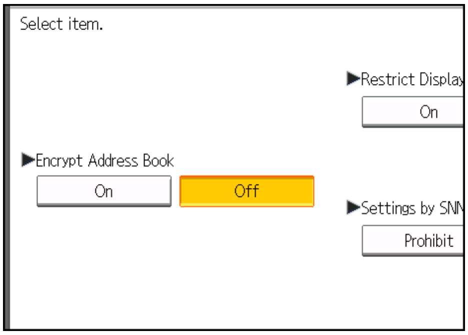
You can encrypt the data in the address book using the extended security function, "Encrypt Address Book".

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

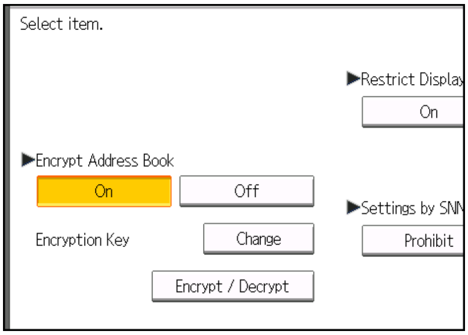
1. **Press the [User Tools] key.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [Extended Security].**

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

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


Select item.

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

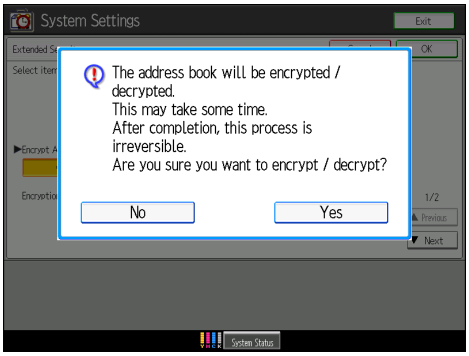

Select item.

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].**


The address book will be encrypted / decrypted.
This may take some time.
After completion, this process is irreversible.
Are you sure you want to encrypt / decrypt?

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

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

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

The machine cannot be used during encryption.

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

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

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

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

Note

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

Reference

- p.33 "Logging in Using Administrator Authentication"
- p.34 "Logging out Using Administrator Authentication"
- p.99 "Specifying the Extended Security Functions"

Deleting Data on the Hard Disk

This can be specified by the machine administrator.

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

The machine's hard disk lets you store data under the printer, as well as the address book and counters stored under each user code.

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

Auto Erase Memory

A print data sent from a printer driver is temporarily stored on the machine's hard disk.

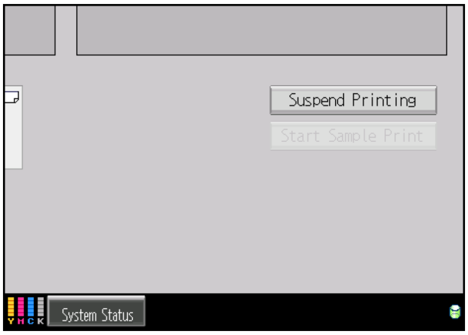
Even after the job is completed, it remains in the hard disk as temporary data. Auto Erase Memory erases the temporary data on the hard disk by writing over it.

Overwriting starts automatically once the job is completed.

The Printer functions take priority over the Auto Erase Memory function. If a print job is in progress, overwriting will only be done after the job is completed.

Overwrite Icon

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



🟧	Dirty	This icon is lit when there is temporary data to be overwritten, and blinks during overwriting.

	Clear	This icon is lit when there is no temporary data to be overwritten.

Note

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

Methods of Overwriting

You can select a method of overwriting from the following:

[NSA] *1

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

[DoD] *2

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

[Random Numbers]

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

*1 National Security Agency, U.S.A.

*2 Department of Defense, U.S.A.

Note

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

Using Auto Erase Memory

This can be specified by the machine administrator.

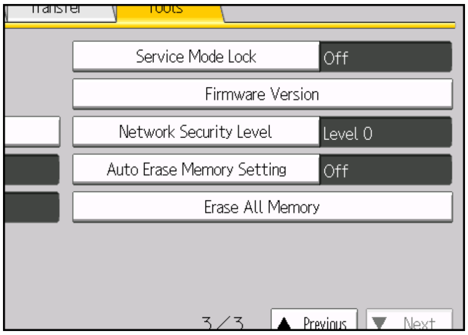
For details about logging in and logging out with administrator authentication, see "Logging in Using Administrator Authentication" and "Logging out Using Administrator Authentication".

Important

- **When "Auto Erase Memory Setting" is set to [On], temporary data that remained on the hard disk when "Auto Erase Memory Setting" was [Off] might not be overwritten.**

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

4. **Press [Auto Erase Memory Setting].**



Service Mode Lock Off

Firmware Version

Network Security Level Level 0

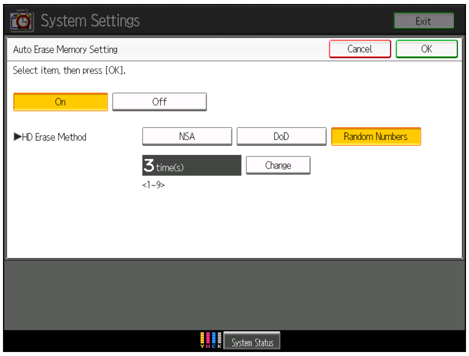
Auto Erase Memory Setting Off

Erase All Memory

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

5. **Press [On].**

6. **Select the method of overwriting.**



Auto Erase Memory Setting

Select item, then press [OK].

HD Erase Method: Random Numbers

3 time(s) <1~9>

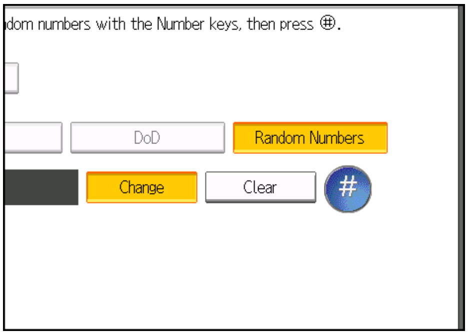
If you select [NSA] or [DoD], proceed to step 9.

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

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

7. **Press [Change].**

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



dom numbers with the Number keys, then press ⊕.

9. **Press [OK].**

   Auto Erase Memory is set.

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

Note

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

Reference

- p.33 "Logging in Using Administrator Authentication"
- p.34 "Logging out Using Administrator Authentication"
- p.70 "Methods of Overwriting"

Canceling Auto Erase Memory

This can be specified by the machine administrator.

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

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

   Auto Erase Memory is disabled.

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

Note

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

Reference

- p.33 "Logging in Using Administrator Authentication"
- p.34 "Logging out Using Administrator Authentication"

Types of Data that Can or Cannot Be Overwritten

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

Data Overwritten by Auto Erase Memory

Printer

- Print jobs

Data Not Overwritten by Auto Erase Memory

- Information registered in the address book *1
- Counters stored under each user code

*1 Data stored in the Address Book can be encrypted for security. For details, see "Protecting the Address Book".

Reference

- p.65 "Protecting the Address Book"

Erase All Memory

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

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, SSL server certificates, and the machine's network settings.**
- **If the main power switch is turned off before Erase All Memory is completed, overwriting will be stopped and data will be left on the hard disk. Do not stop the overwrite mid-process. Doing so will damage the hard disk.**
- **Other than pausing, no operations are possible during the "Erase All Memory" process. If [Random Numbers] is specified and the number of overwrites set to "3", the erase process will take about four hours.**
- **The "Erase All Memory" function also clears the machine's security settings, with the result that afterward, neither machine nor user administration will be effective. Ensure that users do not save any data on the machine after "Erase All Memory" has completed.**

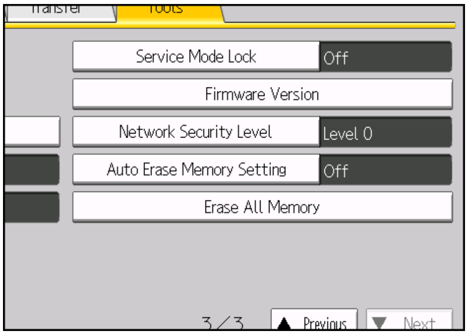
Using Erase All Memory

This can be specified by the machine administrator.

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

1. **Disconnect communication cables connected to the machine.**

2. **Press the [User Tools] key.**
3. **Press [System Settings].**
4. **Press [Administrator Tools].**
5. **Press [Erase All Memory].**



Service Mode Lock Off

Firmware Version

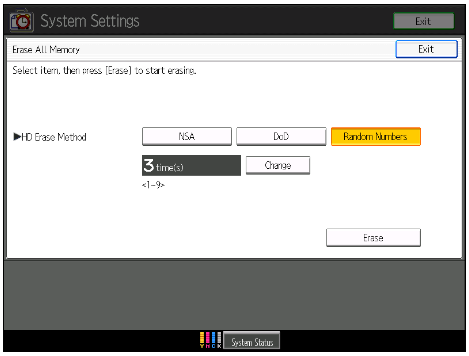
Network Security Level Level 0

Auto Erase Memory Setting Off

Erase All Memory

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

6. **Select the method of overwriting.**



Erase All Memory

Select item, then press [Erase] to start erasing.

▶HD Erase Method NSA DoD Random Numbers

3 time(s)

<1~9>

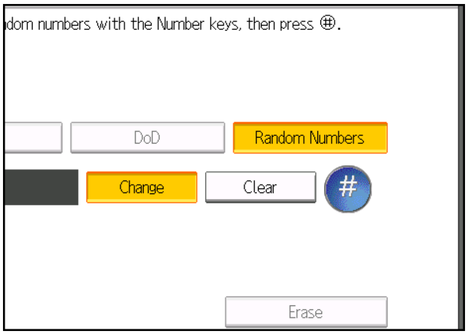
If you select [NSA] or [DoD], proceed to step 9.

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

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

7. **Press [Change].**

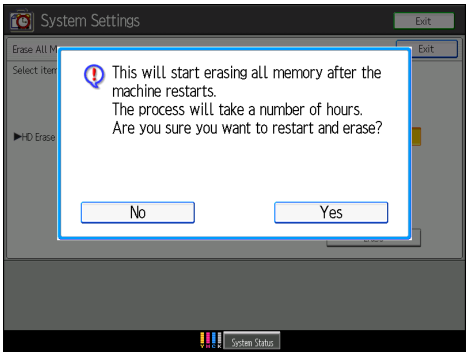
8. Enter the number of times that you want to overwrite using the number keys, and then press [#].



dom numbers with the Number keys, then press ⊕.

9. Press [Erase].

10. Press [Yes].



This will start erasing all memory after the machine restarts.
The process will take a number of hours.
Are you sure you want to restart and erase?

The machine restarts automatically, and overwriting begins.

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

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

Note

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

Reference

- p.33 "Logging in Using Administrator Authentication"
- p.34 "Logging out Using Administrator Authentication"
- p.70 "Methods of Overwriting"

Suspending Erase All Memory

The overwriting process can be suspended temporarily.

Important

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

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

   Overwriting is suspended.
3. **Turn off the main power.**

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

Note

- To resume overwriting, turn on the main power.

4. Managing Access to the Machine

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

Preventing Modification of Machine Settings

This section describes Preventing Modification of Machine Settings.

The administrator type determines which machine settings can be modified. Users cannot change the administrator settings. In "Admin. Authentication", [Available Settings], the administrator can select which settings users cannot specify. For details about the administrator roles, see "Administrators and Users".

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

Type of Administrator

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

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

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

Reference

- p.21 "Administrators and Users"
- p.28 "Administrator Authentication"
- p.129 "Machine Administrator Settings"
- p.134 "Network Administrator Settings"
- p.137 "File Administrator Settings"
- p.139 "User Administrator Settings"
- p.143 "User Settings - Control Panel Settings"
- p.150 "User Settings - Web Image Monitor Settings"

Limiting Available Functions

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

Specify the available functions from the Printer function and extended features.

Available Functions

Printer

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

Other Functions

Note

- Printer job authentication is possible only if user code authentication is enabled. For details, see "User Code Authentication".
- You can limit the availability of extended features only if an application that enables use of extended features is already installed on the machine. If such an application is installed, its name will be displayed under "Other Functions".
- For details about applications that enable use of extended features, contact your sales or service representative.

Reference

- p.37 "User Code Authentication"

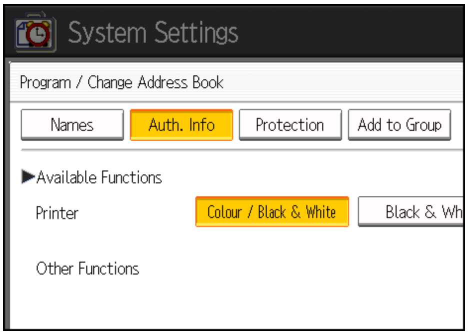
Specifying Which Functions are Available

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

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

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

7. **In "Available Functions", select the functions you want to specify.**



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

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

Reference

- p.33 "Logging in Using Administrator Authentication"
- p.34 "Logging out Using Administrator Authentication"

5. Enhanced Network Security

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

Preventing Unauthorized Access

You can limit IP addresses, disable ports and protocols, or use Web Image Monitor to specify the network security level to prevent unauthorized access over the network and protect the address book, stored files, and default settings.

Access Control

This can be specified by the network administrator.

The machine can control TCP/IP access.

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

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

Important

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

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

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

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

   The network administrator can log in.

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

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

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

   Access control is set.

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

Enabling/Disabling Protocols

This can be specified by the network administrator.

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

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

Protocol	Port	Setting Method	Disabled Condition
IPv4	-	• Control Panel • Web Image Monitor • 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 • telnet	All applications that operate over IPv6 cannot be used.
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".*1

Protocol	Port	Setting Method	Disabled Condition
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".*1
telnet	TCP:23	• Web Image Monitor	Commands using telnet are disabled.
SMTP	TCP:25 (variable)	• Control Panel • Web Image Monitor	E-mail notification that requires SMTP reception cannot be used.
HTTP	TCP:80	• Web Image Monitor • telnet	Functions that require HTTP cannot be used.
HTTPS	TCP:443	• Web Image Monitor • telnet	Functions that require HTTPS cannot be used. @Remote functions are unavailable. You can also make settings to require SSL transmission and restrict the use of other transmission methods using the control panel or Web Image Monitor.
SMB	TCP:139	• Control Panel • Web Image Monitor • telnet	SMB printing functions cannot be used.

Protocol	Port	Setting Method	Disabled Condition
NBT	UDP:137 UDP:138	• telnet	SMB printing functions via TCP/IP, as well as NetBIOS designated functions on the WINS server cannot be used.
SNMPv1,v2	UDP:161	• Web Image Monitor • telnet	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 remote shell (RSH) cannot be used. You can restrict personal information from being displayed by making settings on the control panel using "Restrict Display of User Information".* 1

Protocol	Port	Setting Method	Disabled Condition
SSDP	UDP:1900	• Web Image Monitor • telnet	Device discovery using UPnP from Windows cannot be used.
@Remote	TCP:7443 TCP:7444	• telnet	@Remote cannot be used.
RFU	TCP:10021	• telnet	You can attempt to update firmware via FTP.

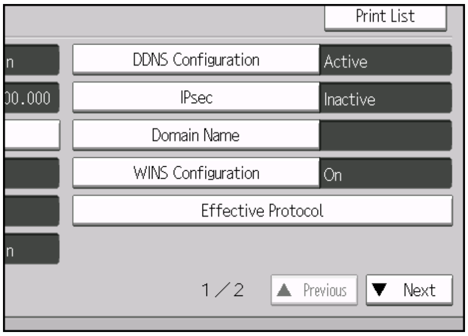
*1 "Restrict Display of User Information" is one of the Extended Security features. For details about making this setting, see "Specifying the Extended Security Functions".

Reference

- p.33 "Logging in Using Administrator Authentication"
- p.34 "Logging out Using Administrator Authentication"
- p.99 "Specifying the Extended Security Functions"

Making Settings Using the Control Panel

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



5. **Press [Inactive] for the protocol you want to disable.**
6. **Press [OK].**
7. **Press the [User Tools] key.**

Making Settings Using Web Image Monitor

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

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

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

   The network administrator can log in.

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

   The Network Security page appears.
5. **Set the desired protocols to active/inactive (or open/close).**
6. **Click [OK].**

   The setting is changed.
7. **Click [OK].**
8. **Click [Logout].**

Specifying Network Security Level

This can be specified by the network administrator. This setting lets you change the security level to limit unauthorized access. You can make network security level settings on the control panel, as well as Web Image Monitor. However, the protocols that can be specified differ.

Set the security level to [Level 0], [Level 1], or [Level 2].

Select [Level 2] for maximum security to protect confidential information. Make this setting when it is necessary to protect confidential information from outside threats.

Select [Level 1] for moderate security to protect important information. Use this setting if the machine is connected to the office local area network (LAN).

Select [Level 0] for easy use of all the features. Use this setting when you have no information that needs to be protected from outside threats.

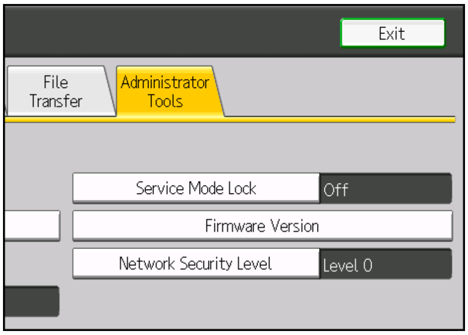
For details about logging in and logging out with administrator authentication, see "Logging in Using Administrator Authentication" and "Logging out Using Administrator Authentication".

Reference

- p.33 "Logging in Using Administrator Authentication"
- p.34 "Logging out Using Administrator Authentication"

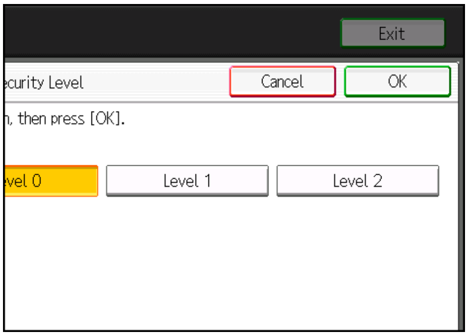
Making Settings Using the Control Panel

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



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

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



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

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

Making Settings Using Web Image Monitor

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

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

The top page of Web Image Monitor appears.

3. **Click [Login].**

   The network administrator can log in.

   Enter the login user name and login password.

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

   The Network Security page appears.

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

   The setting is changed.

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

Status of Functions under each Network Security Level

Tab Name: TCP/IP

Function	Level 0	Level 1	Level 2
TCP/IP	Active	Active	Active
HTTP> Port 80	Open	Open	Open
SSL/TLS> Port 443	Open	Open	Open
SSL/TLS> Permit SSL/TLS Communication	Ciphertext Priority	Ciphertext Priority	Ciphertext Only
FTP	Active	Active	Active
sftp	Active	Active	Active
ssh	Active	Active	Active
RSH/RCP	Active	Active	Inactive
TELNET	Active	Inactive	Inactive
SSDP	Active	Active	Inactive
SMB	Active	Active	Inactive
NetBIOS over TCP/IPv4	Active	Active	Inactive

Tab Name: 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

Protection Using Encryption

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

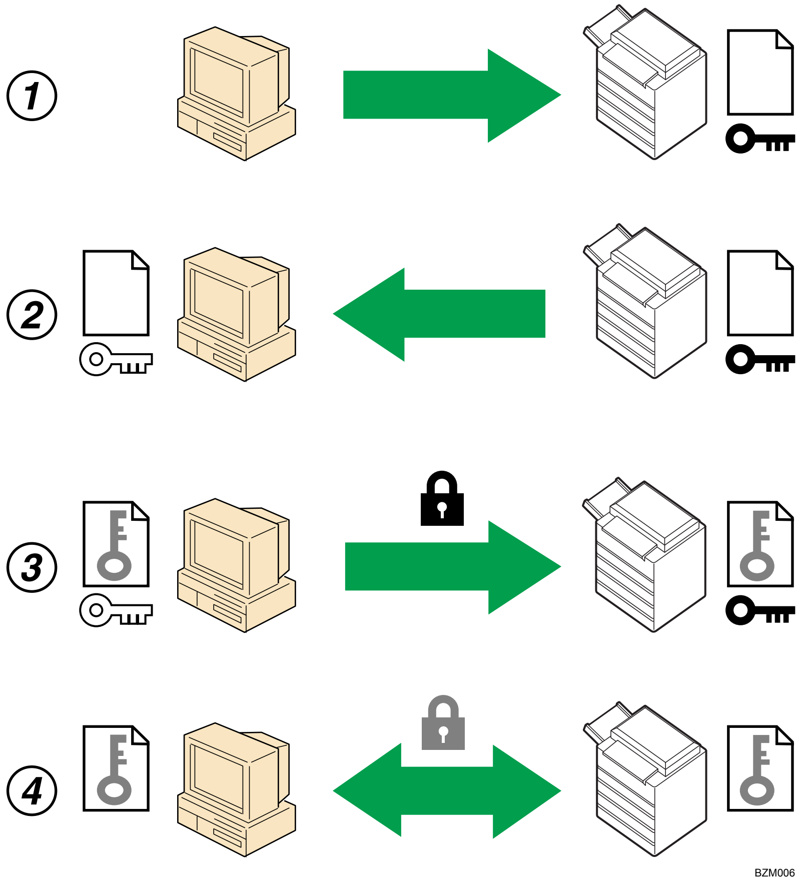
SSL (Secure Sockets Layer) Encryption

This can be specified by the network administrator.

To protect the communication path and establish encrypted communication, create and install the device certificate.

There are two ways of installing a device certificate: create and install a self-signed certificate using the machine, or request a certificate from a certificate authority and install it.

SSL (Secure Sockets Layer)



1. To access the machine from a user's computer, request the SSL device certificate and public key.
2. The device certificate and public key are sent from the machine to the user's computer.

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

Configuration flow (self-signed certificate)

1. Creating and installing the device certificate

   Install the device certificate using Web Image Monitor.

2. Enabling SSL

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

Configuration flow (certificate issued by a certificate authority)

1. Creating the device certificate

   Create the device certificate using Web Image Monitor.

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

2. Installing the device certificate

   Install the device certificate using Web Image Monitor.

3. Enabling SSL

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

Note

- To confirm whether SSL configuration is enabled, enter "https://(the machine's IP address or host name)/" in your Web browser's address bar to access this machine. If the "The page cannot be displayed" message appears, check the configuration because the current SSL configuration is invalid.

Creating and Installing the Self-Signed Certificate

Create and install the device certificate using Web Image Monitor.

This section describes the use of a self-signed certificate as the device certificate.

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

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

   The top page of Web Image Monitor appears.

3. **Click [Login].**

   The network administrator can log in.

   Enter the login user name and login password.

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

   The Device Certificate page appears.

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

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

8. **Click [OK].**

   The setting is changed.

9. **Click [OK].**

   A security warning dialog box appears.

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

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

11. **Click [Logout].**

Note

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

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

Create the device certificate using Web Image Monitor.

This section describes the use of a certificate issued by a certificate authority as the device certificate.

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

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

   The top page of Web Image Monitor appears.

3. **Click [Login].**

   The network administrator can log in.

   Enter the login user name and login password.

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

   The Device Certificate page appears.

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

7. **Make the necessary settings.**

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

8. **Click [OK].**

   The setting is changed.

9. **Click [OK].**

   "Requesting" appears under "Certificate Status".

10. **Click [Logout].**

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

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

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

Note

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

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

Install the device certificate using Web Image Monitor.

This section describes the use of a certificate issued by a certificate authority as the device certificate.

Enter the device certificate contents issued by the certificate authority.

1. **Open a Web browser.**

2. **Enter "http://(the machine's IP address or host name)/" in the address bar.**

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

   The top page of Web Image Monitor appears.

3. **Click [Login].**

   The network administrator can log in.

   Enter the login user name and login password.

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

   The Device Certificate page appears.

5. **Click [Certificate1].**

6. **Click [Install].**
7. **Enter the contents of the device certificate.**

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

   For details about the displayed items and selectable items, see Web Image Monitor Help.
8. **Click [OK].**

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

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

Note

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

Enabling SSL

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

This procedure is used for a self-signed certificate or a certificate issued by a certificate authority.

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

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

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

   The network administrator can log in.

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

   The SSL/TLS page appears.
5. **Click [Active] for the protocol version used in "SSL/TLS".**

6. **Select the encryption communication mode for "Permit SSL/TLS Communication".**
7. **Click [OK].**

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

Note

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

User Settings for SSL (Secure Sockets Layer)

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

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, see Web Image Monitor Help.
- If a certificate issued by a certificate authority is installed in the machine, confirm the certificate store location with the certificate authority.

Setting the SSL / TLS Encryption Mode

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

Encrypted Communication Mode

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

Ciphertext Only	Allows encrypted communication only. If encryption is not possible, the machine does not communicate.
Ciphertext Priority	Performs encrypted communication if encryption is possible. If encryption is not possible, the machine communicates without it.

Ciphertext/Cleartext	Communicates with or without encryption, according to the setting.

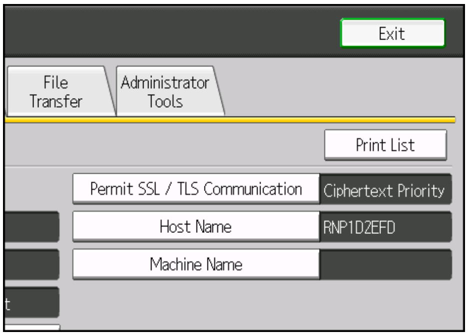
Setting the SSL / TLS Encryption Mode

This can be specified by the network administrator.

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

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

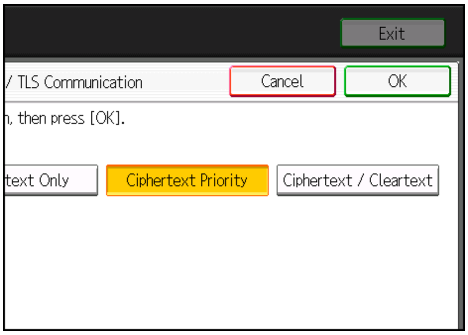
1. **Press the [User Tools] key.**
2. **Press [System Settings].**
3. **Press [Interface Settings].**
4. **Press [Permit SSL / TLS Communication].**



Permit SSL / TLS Communication: Ciphertext Priority
Host Name: RNP1D2EFD
Machine Name

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

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



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

6. **Press [OK].**

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

Note

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

Reference

- p.33 "Logging in Using Administrator Authentication"
- p.34 "Logging out Using Administrator Authentication"

SNMPv3 Encryption

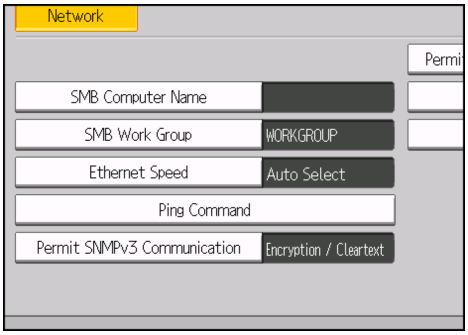
This can be specified by the network administrator.

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

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

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

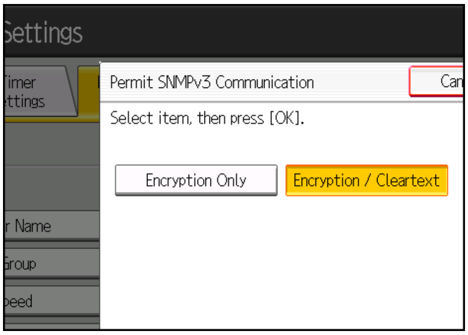
1. **Press the [User Tools] key.**
2. **Press [System Settings].**
3. **Press [Interface Settings].**
4. **Press [Permit SNMPv3 Communication].**



SMB Computer Name
SMB Work Group: WORKGROUP
Ethernet Speed: Auto Select
Ping Command
Permit SNMPv3 Communication: Encryption / Cleartext

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

5. **Press [Encryption Only].**



Permit SNMPv3 Communication

Select item, then press [OK].

6. **Press [OK].**

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

5

Note

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

Reference

- p.30 "Registering the Administrator"
- p.33 "Logging in Using Administrator Authentication"
- p.34 "Logging out Using Administrator Authentication"

6. Specifying the Extended Security Functions

This chapter describes the machine's extended security features and how to specify them.

Specifying the Extended Security Functions

In addition to providing basic security through user authentication and administrator specified access limits on the machine, security can also be increased by encrypting transmitted data and data in the address book. If you need extended security, specify the machine's extended security functions before using the machine.

This section outlines the extended security functions and how to specify them.

For details about when to use each function, see the corresponding chapters.

Changing the Extended Security Functions

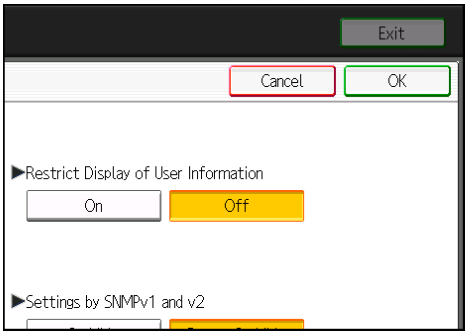
To change the extended security functions, display the extended security screen as follows.

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

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

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

   If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.
5. **Press the setting you want to change, and change the setting.**



▶Restrict Display of User Information

On [✓ Off]

▶Settings by SNMPv1 and v2

6. **Press [OK].**

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

Reference

- p.33 "Logging in Using Administrator Authentication"
- p.34 "Logging out Using Administrator Authentication"

Extended Security Settings

Encrypt Address Book

This can be specified by the user administrator. Encrypt the data in the machine's address book.

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

Default: [**Off**]

Restrict Display of User Information

This can be specified if user authentication is specified. When the job history is checked using a network connection for which authentication is not available, all personal information can be displayed as "********". Because information identifying registered users cannot be viewed, unauthorized users are prevented from obtaining information about the registered files.

Default: [**Off**]

Settings by SNMPv1 and v2

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

Default: [**Do not Prohibit**]

Authenticate Current Job

This function is not available on this model.

Password Policy

This can be specified by the user administrator.

The password policy setting is effective only if [Basic Auth.] is specified.

This setting lets you specify [Complexity Setting] and [Minimum Character No.] for the password. By making this setting, you can limit the available passwords to only those that meet the conditions specified in [Complexity Setting] and [Minimum Character No.].

If you select [Level 1], specify the password using a combination of two types of characters selected from upper-case letters, lower-case letters, decimal numbers, and symbols such as #.

If you select [Level 2], specify the password using a combination of three types of characters selected from upper-case letters, lower-case letters, decimal numbers, and symbols such as #.

Default: [**Off**]

Passwords can contain the following characters:

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

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

@Remote Service

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

Default: [**Do not Prohibit**]

Reference

- p.65 "Protecting the Address Book"

Other Security Functions

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

System Status

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

Weekly Timer Code

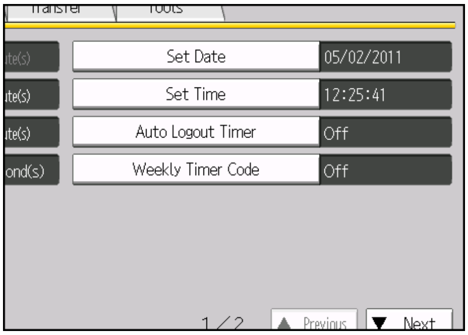
If the weekly timer is enabled and [Weekly Timer Code] is set to [On], you must enter the weekly timer code to turn the power back on after the timer has turned it off.

Specifying Weekly Timer Code

This can be specified by the machine administrator.

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

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



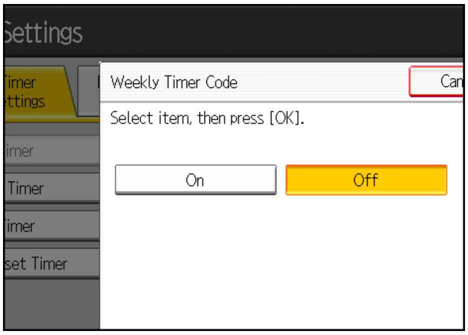
Set Date 05/02/2011

Set Time 12:25:41

Auto Logout Timer Off

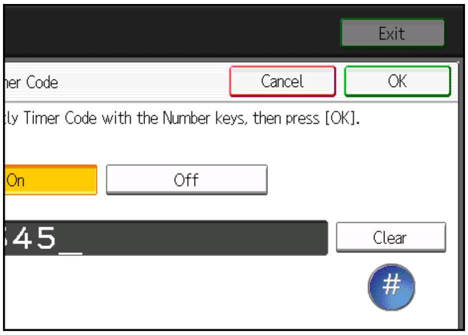
Weekly Timer Code Off

5. **Press [On].**



Select item, then press [OK].

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



ly Timer Code with the Number keys, then press [OK].

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

7. **Press [OK].**

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

Reference

- p.33 "Logging in Using Administrator Authentication"
- p.34 "Logging out Using Administrator Authentication"

Canceling Weekly Timer Code

This can be specified by the machine administrator.

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

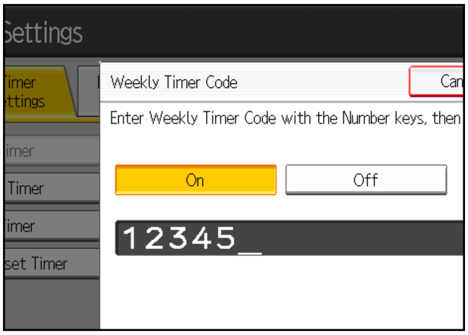
1. **Press the [User Tools] key.**

2. **Press [System Settings].**

3. **Press [Timer Settings].**

4. **Press [Weekly Timer Code].**

5. **Press [Off], and then press [OK].**



Settings

Weekly Timer Code

Enter Weekly Timer Code with the Number keys, then

12345_

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

Reference

- p.33 "Logging in Using Administrator Authentication"
- p.34 "Logging out Using Administrator Authentication"

Limiting Machine Operation to Customers Only

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

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

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

Use the following settings.

- Service Mode Lock

Settings

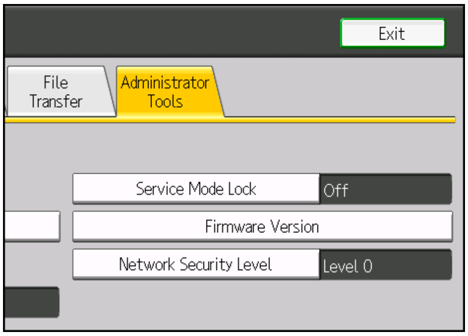
Service Mode Lock

This can be specified by the machine administrator. Service mode is used by a service representative for inspection or repair. If you set the service mode lock to [On], service mode cannot be used unless the machine administrator logs in to the machine and cancels the service mode lock to allow the service representative to operate the machine for inspection and repair. This ensures that the inspection and repair are done under the supervision of the machine administrator.

Specifying Service Mode Lock

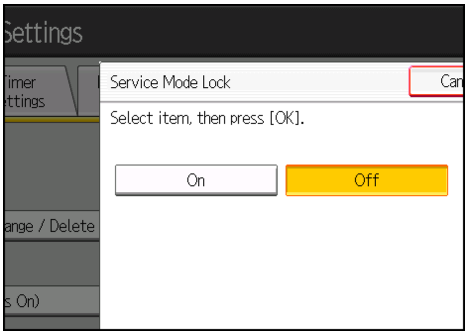
For details about logging in and logging out with administrator authentication, see "Logging in Using Administrator Authentication" and "Logging out Using Administrator Authentication".

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



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

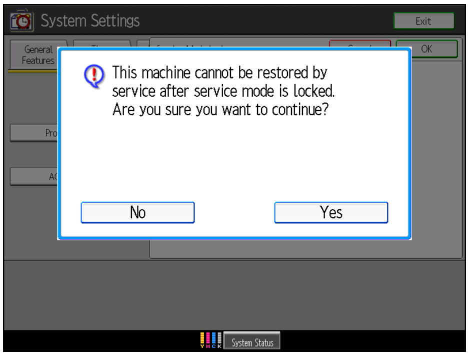
5. **Press [On], and then press [OK].**



Select item, then press [OK].

A confirmation message appears.

6. **Press [Yes].**



This machine cannot be restored by service after service mode is locked. Are you sure you want to continue?

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

Reference

- p.33 "Logging in Using Administrator Authentication"
- p.34 "Logging out Using Administrator Authentication"

Canceling Service Mode Lock

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

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

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

4. **Press [Service Mode Lock].**

   If the setting to be specified does not appear, press [▼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 in Using Administrator Authentication"
- p.34 "Logging out Using Administrator Authentication"

7. Troubleshooting

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

Authentication Does Not Work Properly

This section describes what to do if a user cannot operate the machine because of a problem related to user authentication. Refer to this section if a user comes to you with such a problem.

A Message Appears

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

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

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

Messages	Cause	Solutions
"Failed to obtain URL."	The machine cannot connect to the server or cannot establish communication.	Make sure the server's settings, such as the IP address and host name, are specified correctly on the machine. Make sure the host name of the UA Server is specified correctly.
"Failed to obtain URL."	The machine is connected to the server, but the UA service is not responding properly.	Make sure the UA service is specified correctly.
"Failed to obtain URL."	SSL is not specified correctly on the server.	Specify SSL using Authentication Manager.
"Failed to obtain URL."	Server authentication failed.	Make sure server authentication is specified correctly on the machine.
"Authentication has failed."	The entered login user name or login password is incorrect.	Ask the user administrator for the correct login user name and login password. See the error codes below for possible solutions: B,W,L,I 0206-003 W,L,I 0406-003
"Authentication has failed."	Authentication failed because no more users can be registered. (The number of users registered in the address book has reached capacity.)	Delete unnecessary user addresses. See the error codes below for possible solutions: W,L,I 0612-005
"Authentication has failed."	Cannot access the authentication server when using Windows Authentication, LDAP Authentication, or Integration Server Authentication.	A network or server error may have occurred. Confirm the network in use with the LAN administrator. If an error code appears, follow the instructions next to the error code in the table below.

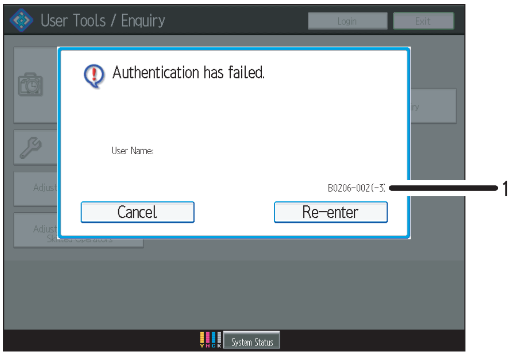
Note

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

An Error Code Appears

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

Error Code Display Position



User Tools / Enquiry

Authentication has failed.

User Name:

B0206-002(-3)

1. **error code**

   An error code appears.

Basic Authentication

Error Code	Cause	Solution
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 in.
B0206-002	2. The user attempted authentication from an application on the "System Settings" screen, where only the administrator has authentication ability.	Only the administrator has login privileges on this screen. Log in as a general user from the application's login screen.

Error Code	Cause	Solution
B0206-003	An authentication error occurred because the user name contains a space, colon (:), or quotation mark (").	Recreate the account if the account name contains any of these prohibited characters. If the account name was entered incorrectly, enter it correctly and log in again.
B0207-001	An authentication error occurred because the address book is being used at another location.	Wait a few minutes and then try again.

Windows Authentication

Error Code	Cause	Solution
W0206-002	The user attempted authentication from an application on the "System Settings" screen, where only the administrator has authentication ability.	Only the administrator has login privileges on this screen. Log in as a general user from the application's login screen.
W0206-003	An authentication error occurred because the user name contains a space, colon (:), or quotation mark (").	Recreate the account if the account name contains any of these prohibited characters. If the account name was entered incorrectly, enter it correctly and log in again.
W0207-001	An authentication error occurred because the address book is being used at another location.	Wait a few minutes and then try again.

Error Code	Cause	Solution
W0406-101	Authentication cannot be completed because of the high number of authentication attempts.	Wait a few minutes and then try again. If the situation does not return to normal, make sure that an authentication attack is not occurring. Notify the administrator of the screen message by e-mail, and check the system log for signs of an authentication attack.
W0406-104	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 is successful: 1. Make sure that DNS is specified in "Interface Settings", if the top-level domain name is specified in the domain name (such as domainname.xxx.com). 2. Make sure that WINS is specified in "Interface Settings", if a NetBIOS domain name is specified in domain name (such as DOMAINNAME).

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

Error Code	Cause	Solution
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 machine and the group name on the DC (domain controller) are exactly the same. The DC is case sensitive. Make sure that Use Auth. Info at Logon has been specified in Auth. Info in the user account registered on the machine. If there is more than one DC, make sure that a confidential relationship has been configured between each DC.
W0400-106	The domain name cannot be resolved.	Make sure that DNS/WINS is specified in the domain name in "Interface Settings".
W0400-200	Due to the high number of authentication attempts, all resources are busy.	Wait a few minutes and then try again.
W0400-202	1. The SSL settings on the authentication server and the machine do not match.	Make sure the SSL settings on the authentication server and the machine match.
W0400-202	2. The user entered sAMAccountName in the user name to log in.	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.

Error Code	Cause	Solution
W0406-003	An authentication error occurred because the user name contains a space, colon (:), or quotation mark (").	Recreate the account if the account name contains any of these prohibited characters. If the account name was entered incorrectly, enter it correctly and log in again.
W0409-000	Authentication timed out because the server did not respond.	Check the network configuration, or settings on the authenticating server.
W0511-000	The authentication server login name is the same as a user name already registered on the machine. (Names are distinguished by the unique attribute specified in LDAP authentication settings.)	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.
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
L0206-002	A user attempted authentication from an application on the "System Settings" screen, where only the administrator has authentication ability.	Only the administrator has login privileges on this screen. Log in as a general user from the application's login screen.
L0206-003	An authentication error occurred because the user name contains a space, colon (:), or quotation mark (").	Recreate the account if the account name contains any of these prohibited characters. If the account name was entered incorrectly, enter it correctly and log in again.
L0207-001	An authentication error occurred because the address book is being used at another location.	Wait a few minutes and then try again.
L0306-018	The LDAP server is not correctly configured.	Make sure that a connection test is successful with the current LDAP server configuration.
L0307-001	An authentication error occurred because the address book is being used at another location.	Wait a few minutes and then try again.
L0400-210	Failed to obtain user information in LDAP search.	The login attribute's search criteria might not be specified or the specified search information is unobtainable. Make sure the login name attribute is specified correctly.
L0406-003	An authentication error occurred because the user name contains a space, colon (:), or quotation mark (").	Recreate the account if the account name contains any of these prohibited characters. If the account name was entered incorrectly, enter it correctly and log in again.

Error Code	Cause	Solution
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 useable login name is registered on the machine. Authentication will fail in the following cases: If the login user name contains a space, colon (:), or quotation mark ("). If the login user name exceeds 128 bytes.
L0409-000	Authentication timed out because the server did not respond.	Contact the server or network administrator. If the situation does not return to normal, contact your service representative.
L0511-000	The authentication server login name is the same as a user name already registered on the machine. (Names are distinguished by the unique attribute specified in the LDAP authentication settings.)	1. Delete the old, duplicated name or change the login name. 2. If the authentication server has just been changed, delete the old name on the server.
L0607-001	An authentication error occurred because the address book is being used at another location.	Wait a few minutes and then try again.
L606-004	Authentication failed because the user name contains language that cannot be used by general users.	Do not use "other", "admin", "supervisor" or "HIDE*" in general user accounts.
L0612-005	Authentication failed because no more users can be registered. (The number of users registered in the address book has reached capacity.)	Ask the user administrator to delete unused user accounts in the address book.

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

Integration Server Authentication

Error Code	Cause	Solution
I0206-002	A user attempted authentication from an application on the "System Settings" screen, where only the administrator has authentication ability.	Only the administrator has login privileges on this screen. Log in as a general user from the application's login screen.
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 in 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 in again.
I0406-301	1. The URL could not be obtained.	Obtain the URL using [Obtain URL] in Integration Server authentication.

Error Code	Cause	Solution
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 useable login name is registered on the machine. Authentication will fail in the following cases. If the login user name contains a space, colon (:), or quotation mark ("). If the login user name exceeds 128 bytes.
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.
I0511-000	The authentication server login name is the same as a user name already registered on the machine. (Names are distinguished by the unique attribute specified in the LDAP authentication settings.)	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.

Error Code	Cause	Solution
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.

Machine Cannot Be Operated

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

Condition	Cause	Solution
User authentication is disabled, but destinations registered in the machine's address book do not appear.	User authentication might have been disabled without "All Users" being selected for "Protect Destination".	Enable user authentication, and then select "All Users" in "Protect Destination" for all registered destinations. For details, see "Protecting the Address Book".
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.65 "Protecting the Address Book"
- p.95 "Setting the SSL / TLS Encryption Mode"

8. Appendix

Supervisor Operations

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

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

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

Important

- **The default login user name is "supervisor" and the login password is blank. We recommend changing the login user name and login password.**
- **When registering login user names and login passwords, you can specify up to 32 alphanumeric characters and symbols. Keep in mind that user names and passwords are case-sensitive.**
- **User names cannot contain numbers only, a space, colon (:), or quotation mark ("), nor can they be left blank. For details about what characters the password can contain, see "Specifying the Extended Security Functions".**
- **Be sure not to forget the supervisor login user name and login password. If you do forget them, a service representative will to have to return the machine to its default state. This will result in all data in the machine being lost and the service call may not be free of charge.**

Note

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

Reference

- p.99 "Specifying the Extended Security Functions"

Logging in as the Supervisor

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

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

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

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

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

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

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

Logging out as the Supervisor

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

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

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

Changing the Supervisor

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

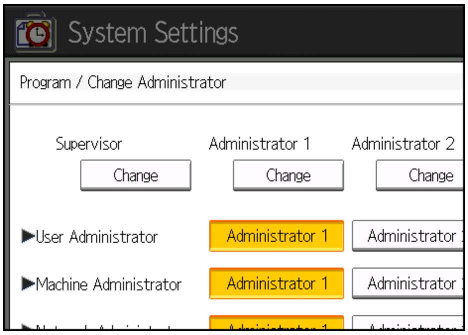
1. **Press the [User Tools] key.**
2. **Press the [Login/Logout] key.**
3. **Log in as the supervisor.**

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

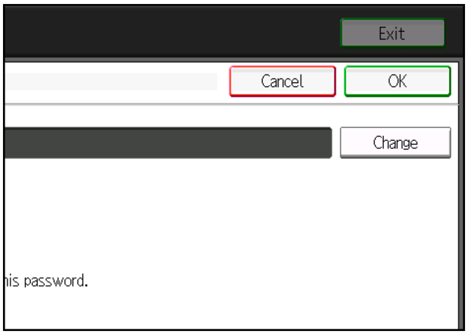
4. **Press [System Settings].**
5. **Press [Administrator Tools].**
6. **Press [Program / Change Administrator].**

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

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



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



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

    You will be automatically logged out.

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

Reference

- p.28 "Specifying Administrator Privileges"
- p.125 "Logging in as the Supervisor"

Resetting an Administrator's Password

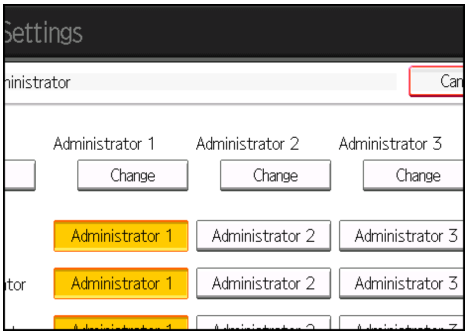
This section describes how to reset the administrators' passwords. Administrator login names cannot be changed.

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

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

   For details about logging in as the supervisor, see "Logging in as the Supervisor".
4. **Press [System Settings].**
5. **Press [Administrator Tools].**
6. **Press [Program / Change Administrator].**

   If the setting to be specified does not appear, press [▼Next] to scroll down to other settings.
7. **Press [Change] for the administrator you wish to reset.**



8. **Press [Change] for "Login Password".**
9. **Enter the login password, and then press [OK].**

10. **If a password reentry screen appears, enter the login password, and then press [OK].**
11. **Press [OK] twice.**

    You will be automatically logged out.
12. **Press the [User Tools] key.**

Reference

- p.125 "Logging in as the Supervisor"

Machine Administrator Settings

The machine administrator settings that can be specified are as follows:

System Settings

The following settings can be specified.

General Features

All the settings can be specified.

Timer Settings

All the settings can be specified.

Interface Settings

- DNS Configuration

  You can perform a connection test.

File Transfer

The following settings can be specified.

- SMTP Authentication

  All the settings can be specified.

- POP before SMTP

  All the settings can be specified.

- Reception Protocol
- POP3 / IMAP4 Settings

  All the settings can be specified.

- Administrator's E-mail Address

Administrator Tools

The following settings can be specified.

- Address Book Management

  Search

  Switch Title

- Address Book: Program / Change / Delete Group

  Search

  Switch Title

- Display / Print Counter

  Print Counter List

- Display / Clear / Print Counter per User

  Print the counter list for all users' jobs

  Print the counter list for each user's jobs
- User Authentication Management

  You can specify which authentication to use.

  You can also edit the settings for each function.
- Administrator Authentication Management

  Machine Management
- Program / Change Administrator

  Machine Administrator
- External Charge Unit Management
- Enhanced External Charge Unit Management
- Extended Security

  Restrict Display of User Information

  @Remote Service
- Program / Change / Delete LDAP Server

  All the settings can be specified.
- AOF (Always On)
- Service Test Call
- Notify Machine Status
- Service Mode Lock
- Auto Erase Memory Setting
- Erase All Memory

Note

- "Auto Erase Memory Setting" and the "Erase All Memory" setting are available only if the DataOverwriteSecurity unit is installed.

Maintenance

The following settings can be specified.

- Colour Registration

  All the settings can be specified.
- Erase Print Image Traces

  All the settings can be specified.

Tray Paper Settings

For details about the user privileges required for specifying the paper settings and advanced settings for various commercially-available paper types, contact your service representative.

Settings via Web Image Monitor

The following settings can be specified.

Home

- Reset Device

Device Settings

For details about the user privileges required for specifying the paper settings and advanced settings for various commercially-available paper types, contact your service representative.

- System

  Permit Firmware Update

  Display IP Address on Device Display Panel

  Output Tray

  Paper Tray Priority

- Date/Time

  All the settings can be specified.

- Timer

  All the settings can be specified.

- E-mail

  Administrator E-mail Address

  Reception Protocol

  SMTP Authentication

  SMTP Auth. E-mail Address

  SMTP Auth. User Name

  SMTP Auth. Password

  SMTP Auth. Encryption

  POP before SMTP

  POP E-mail Address

  POP User Name

  POP Password

Timeout setting after POP Auth.

POP3/IMAP4 Server Name

POP3/IMAP4 Encryption

E-mail Notification E-mail Address

Receive E-mail Notification

E-mail Notification User Name

E-mail Notification Password

- Auto E-mail Notification

  All the settings can be specified.

- On-demand E-mail Notification

  All the settings can be specified.

- User Authentication Management

  All the settings can be specified.

- Administrator Authentication Management

  Machine Administrator Authentication

  Available Settings for Machine Administrator

- Program/Change Administrator

  You can specify the following administrator settings as the machine administrator.

  Login User Name

  Login Password

  Encryption Password

- LDAP Server

  All the settings can be specified.

- Firmware Update

  All the settings can be specified.

Network

- SNMPv3

  Access Type (Machine Administrator)

RC Gate

All the settings can be specified.

Webpage

- Webpage

  Download Help File

Extended Feature Settings

All the settings can be specified.

Network Administrator Settings

The network administrator settings that can be specified are as follows:

System Settings

The following settings can be specified.

Interface Settings

If DHCP is set to On, the settings that are automatically obtained via DHCP cannot be specified.

- Print List
- Network

  All the settings can be specified.

File Transfer

- SMTP Server

  All the settings can be specified.

- E-mail Communication Port

  All the settings can be specified.

- E-mail Reception Interval
- 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

- Extended Security

  Settings by SNMPv1 and v2

- Network Security Level

Settings via Web Image Monitor

The following settings can be specified.

Device Settings

- System

  Device Name

  Comment

  Location

- E-mail

  E-mail Reception Interval

  E-mail Storage in Server

  SMTP Server Name

  SMTP Port No.

  POP3 Reception Port No.

  IMAP4 Reception Port No.

- Auto E-mail Notification

  You can select groups to notify.

- Administrator Authentication Management

  Network Administrator Authentication

  Available Settings for Network Administrator

- Program/Change Administrator

  You can specify the following administrator settings for the network administrator.

  Login User Name

  Login Password

  Encryption Password

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.

Webpage

- Webpage

  All the settings can be specified.

File Administrator Settings

The file administrator settings that can be specified are as follows:

System Settings

The following settings can be specified.

Interface Settings

- DNS Configuration

  You can perform a connection test.

Administrator Tools

- Address Book Management

  Search

  Switch Title

- Address Book: Program / Change / Delete Group

  Search

  Switch Title

- Administrator Authentication Management

  File Management

- Program / Change Administrator

  File Administrator

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.

Interface Settings

- DNS Configuration

  You can perform a connection test.

Administrator Tools

- Address Book Management

  All the settings can be specified.

- Address Book: Program / Change / Delete Group

  All the settings can be specified.

- Address Book: Change Order
- Address Book: Edit Title
- Address Book: Switch Title
- Back Up / Restore Address Book
- Display / Clear / Print Counter per User

  Clear the counter for all users' jobs

  Clear the counter for each user's jobs

- Administrator Authentication Management

  User Management

- Program / Change Administrator

  User Administrator

- Extended Security

  Encrypt Address Book

  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

The Privilege for User Account Settings in the Address Book

The authorities for using the address book are as follows:

The authority designations in the list indicate users with the following authorities.

- Abbreviations in the table heads
  - Read-only (User) = This is a user assigned "Read-only" authority.
  - Edit (User) = This is a user assigned "Edit" authority.
  - Edit / Delete (User) = This is a user assigned "Edit / Delete" authority.
  - Full Control (User) = This is a user assigned "Full Control" authority.
  - Registered User = This is a user that has personal information registered in the address book and has a login password and user name.
  - User Admin. = This is the user administrator.
- Abbreviations in the table columns
  - R/W (Read and Write) = You can view and change the setting.
  - R (Read) = You can view the setting.
  - N/A (Not Applicable) = You cannot view or specify the setting.

Tab Name: Names

Settings	Read-only (User)	Edit (User)	Edit / Delete (User)	Full Control (User)	Registered User	User Admin.
Name	R	R/W	R/W	R/W	R/W	R/W
Key Display	R	R/W	R/W	R/W	R/W	R/W
Registration No.	R	R/W	R/W	R/W	R/W	R/W
Select Title	R	R/W	R/W	R/W	R/W	R/W

Tab Name: Auth. Info

Settings	Read-only (User)	Edit (User)	Edit / Delete (User)	Full Control (User)	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 (User)	Registered User	User Admin.
Login User Name	N/A	N/A	N/A	N/A	R	R/W
Login Password	N/A	N/A	N/A	N/A	R/W*1	R/W*1
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 (User)	Registered User	User Admin.
Permissions for Users/Groups	N/A	N/A	N/A	R/W	R/W	R/W

Tab Name: Add to Group

Settings	Read-only (User)	Edit (User)	Edit / Delete (User)	Full Control (User)	Registered User	User Admin.
Registration No.	R	R/W	R/W	R/W	R/W	R/W
Search	N/A	R/W	R/W	R/W	R/W	R/W
Switch Title	R/W	R/W	R/W	R/W	R/W	R/W

User Settings - Control Panel Settings

This section describes which functions and system settings are available to users when administrator authentication is specified. If user authentication is specified, system settings and functions are available to authorized users only, who must log in to access them.

System Settings

When administrator authentication is enabled, the administrator's configuration of Available Settings determines which system settings are available to users. If user authentication is specified, no settings are accessible to unauthorized users or authorized users before logging in.

User privileges are as follows:

- Abbreviations in the table heads

  Not Specified = Authorized user when "Available Settings" have not been specified.

  Specified = Authorized user when "Available Settings" have been specified.

- Abbreviations in the table columns

  R/W (Read and Write) = Both reading and modifying the setting are available.

  R (Read) = Reading only.

  N/A (Not Applicable) = Neither reading nor modifying the setting is available.

General Features

Settings	Not Specified	Specified
Program / Change / Delete User Text	R/W	R
Panel Key Sound	R/W	R
Warm-up Beeper	R/W	R
Function Priority	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/ Job List Display Time	R/W	R
Key Repeat	R/W	R
Z-fold Position	R/W	R
Output Tray Setting	R/W	R
Perfect Binding Cut Fine Adjustment	R/W	R

The "Z-fold Position" setting is available only if the Z-folding unit is installed.

The "Perfect Binding Cut Fine Adjustment" setting is available only if the perfect binder is installed.

To specify "Output Tray Setting" is available only if the stacker is installed.

Timer Settings

Settings	Not Specified	Specified
Auto Off Timer	R/W	R
Energy Saver Timer	R/W	R
Panel Off Timer	R/W	R
System Auto Reset Timer	R/W	R
Set Date	R/W	R
Set Time	R/W	R
Auto Logout Timer	R/W	R
Weekly Timer Code	R/W	R
Binding Glue Heater Auto Off Timer	R/W	R
Weekly Timer	R/W	R

The "Binding Glue Heater Auto Off Timer" setting is available only if the perfect binder is installed.

Interface Settings

Settings	Not Specified	Specified
Print List	R/W	N/A

Network

Settings	Not Specified	Specified
Machine IPv4 Address	R/W	R
IPv4 Gateway Address	R/W	R
IPv6 Stateless Address Autoconfiguration	R/W	R
DNS Configuration	R/W	R
DDNS Configuration	R/W	R

Settings	Not Specified	Specified
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
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", or "Domain Name" to "Auto-Obtain (DHCP)", you can only display the settings.

File Transfer

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
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
External Charge Unit Management	R/W	R
Enhanced External Charge Unit Management	R/W	R
Extended Security	R/W	R
Program / Change / Delete LDAP Server	R/W	R
AOF (Always On)	R/W	R
Service Test Call	R/W	N/A
Notify Machine Status	R/W	N/A
Service Mode Lock	R/W	R
Auto Erase Memory Setting	R/W	R
Erase All Memory	R/W	R

The password for "Program / Change / Delete LDAP Server" can be entered or changed but not displayed.

The "Auto Erase Memory Setting" and "Erase All Memory" settings are available only if the DataOverwriteSecurity unit is installed.

Maintenance

When administrator authentication is enabled, the administrator's configuration of Available Settings determines which system settings are available to users. If user authentication is specified, no settings are accessible to unauthorized users or authorized users before logging in.

User privileges are as follows:

- Abbreviations in the table heads

  Not Specified = Authorized user when "Available Settings" have not been specified.

  Specified = Authorized user when "Available Settings" have been specified.

- Abbreviations in the table columns

  R/W (Read and Write) = Both reading and modifying the setting are available.

  R (Read) = Reading only.

  N/A (Not Applicable) = Neither reading nor modifying the setting is available.

Settings	Not Specified	Specified
Colour Registration	R/W	N/A
Erase Print Image Traces	R/W	N/A

Tray Paper Settings

For details about the user privileges required for specifying the paper settings and advanced settings for various commercially-available paper types, contact your service representative.

User Settings - Web Image Monitor Settings

This section displays the user settings that can be specified on Web Image Monitor when user authentication is specified. Settings that can be specified by the user vary according to the available settings specifications.

Device Settings

The settings available to the user depend on whether or not administrator authentication is enabled.

If administrator authentication is enabled, the settings available to the user depend on whether or not "Available Settings" has been specified.

User privileges are as follows:

- Abbreviations in the table heads

  Not Specified = Authorized user when "Available Settings" have not been specified.

  Specified = Authorized user when "Available Settings" have been specified.

- Abbreviations in the table columns

  R/W (Read and Write) = Both reading and modifying the setting are available.

  R (Read) = Reading only.

  N/A (Not Applicable) = Neither reading nor modifying the setting is available.

System

Settings	Not Specified	Specified
General Settings : Device Name	R/W	R
General Settings : Comment	R/W	R
General Settings : Location	R/W	R
Output Tray : Printer	R/W	R
Paper Tray Priority : Printer	R/W	R

Date/Time

Settings	Not Specified	Specified
Set Date	R/W	R
Set Time	R/W	R
SNTP Server Address	R/W	R
SNTP Polling Interval	R/W	R
Time Zone	R/W	R

Timer

Settings	Not Specified	Specified
Auto Off Timer	R/W	R
Energy Saver Timer	R/W	R
Panel Off Timer	R/W	R
System Auto Reset Timer	R/W	R
Auto Logout Timer	R/W	R
Weekly Timer Code	R/W	R
Weekly Timer	R/W	R

E-mail

Settings	Not Specified	Specified
Administrator E-mail Address	R/W	R
Reception Protocol	R/W	R
E-mail Reception Interval	R/W	R
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

On-demand E-mail Notification

Settings	Not Specified	Specified
Notification Subject	R	R
Notification Message	R	R
Restriction to System Config. Info.	R	R
Restriction to Network Config. Info.	R	R
Restriction to Supply Info.	R	R
Restriction to Device Status Info.	R	R
Receivable E-mail Address/Domain Name Settings	R	R

User Authentication Management

Settings	Not Specified	Specified
User Authentication Management	R/W	R
User Code Authentication - Available Functions	R/W	R
Windows Authentication - SSL	R/W	R
Windows Authentication - Domain Name	R/W	R
Windows Authentication - Group Settings for Windows Authentication	R/W	R
LDAP Authentication - LDAP Authentication	R/W	R
LDAP Authentication - Login Name Attribute	R/W	R
LDAP Authentication - Unique Attribute	R/W	R
Integration Server Authentication - SSL	R/W	R
Integration Server Authentication - Integration Server Name	R/W	R
Integration Server Authentication - Authentication Type	R/W	R
Integration Server Authentication - Obtain URL	R	R
Integration Server Authentication - Domain Name	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

Note

- For details about the user privileges required for specifying the paper settings and advanced settings for various commercially-available paper types, contact your service representative.

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
Webpage Language	R/W	R
Set URL Target of Link Page	R/W	R
Set Help URL Target	R/W	R
UPnP Setting	R/W	R
Download Help File	R/W	R/W

Functions That Require Options

The following functions require certain options and additional functions.

- Hard Disk overwrite erase function

  DataOverwriteSecurity unit

Trademarks

Adobe, Acrobat, Acrobat Reader, and Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Microsoft®, Windows®, and Windows Server® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

UPnP™ is a trademark of the UPnP™ Implementers Corporation.

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 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

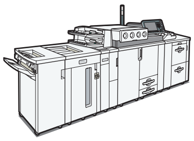
  Microsoft® Windows Server® 2008 R2 Enterprise

INDEX

MEMO

MEMO

Operating Instructions Security Reference



EN (US) M077-2182