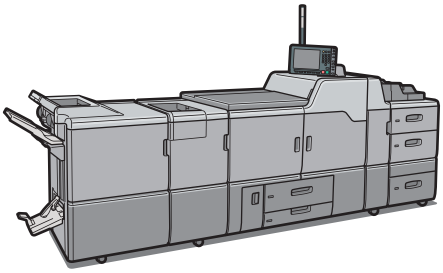
Pro C751

Operating Instructions
Security Reference



For safe and correct use, be sure to read the Safety Information in "About This Machine" before using the machine.

TABLE OF CONTENTS

1. Getting Started

2. Configuring Administrator Authentication

3. Configuring User Authentication

4. Securing Information Stored on Hard Disk

5. Managing Access to the Machine

6. Enhanced Network Security

7. Specifying the Extended Security Functions

8. Troubleshooting

9. Appendix

Manuals for This Machine

Read this manual carefully before you use this machine.

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

Important

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

About This Machine

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

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

Troubleshooting

Provides a guide for resolving common usage-related problems.

Network and System Settings Reference

Explains how to connect the machine to a network and how to configure and operate the machine in a network environment. It also explains how to change System Settings, how to specify Adjustment Settings for Operators, and how to register information in the Address Book.

Paper Settings Reference

Explains how to make paper settings for each tray using the paper library, which contains optimum printing conditions. It also explains how to manually specify a paper size and type for a paper tray.

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.

Guide to Paper

Explains paper characteristics and methods for handling paper.

Note

- Manuals provided are specific to machine types.
- 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.

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.**

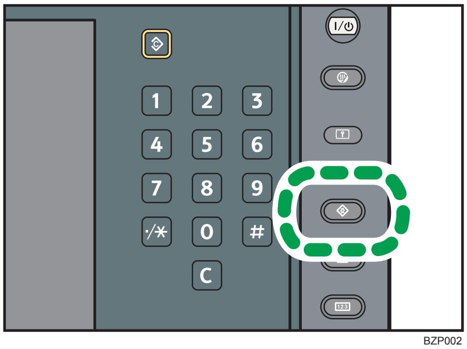
1. To prevent this machine being stolen or willfully damaged, etc., install it in a secure location.
2. Purchasers of this machine must make sure that people who use it do so appropriately, in accordance with operations determined by the machine administrator and supervisor. If the administrator or supervisor 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.

Setting up the Machine

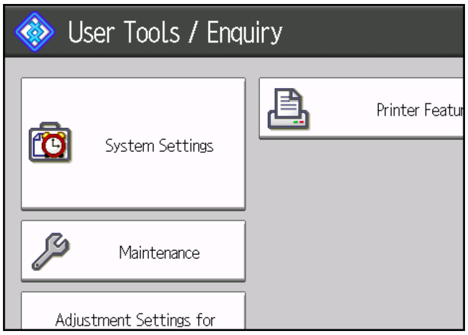
This section describes how to enable encryption of transmitted data and configure the administrator account. If you want a high level of security, make the following setting before using the machine.

Enabling security

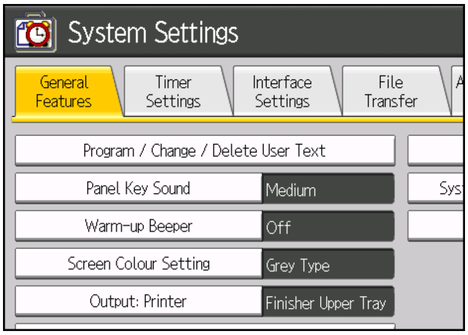
1. **Turn the machine on.**
2. **Press the [User Tools] key.**



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



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



Panel Key Sound	Medium
Warm-up Beeper	Off
Screen Colour Setting	Grey Type
Output: Printer	Finisher Upper Tray

5. **Specify IPv4 Address.**

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

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 p.60 "Logging in Using Web Image Monitor".

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

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 p.120 "Protection Using Encryption".

    The settings for device certificate creation can be configured only if an administrator e-mail address is specified.

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

    For details about enabling SSL, see p.124 "Enabling SSL/TLS".

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

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

    For details about specifying the administrator's user name and password, see p.31 "Changing the Administrator's User Name and Password".

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".**

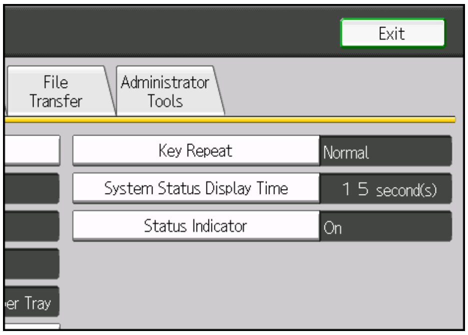
3. **Set "Network Security" to [Level 2].**

   Note that some functions will be unavailable after you select [Level 2] for this setting. For details, see p.118 "Status of Functions under Each Network Security Level" and p.112 "Enabling and Disabling Protocols".

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

   For details about the functions that will be unavailable if "FTP" and "SNMPv3" are set to [Inactive], see p.112 "Enabling and Disabling Protocols".

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

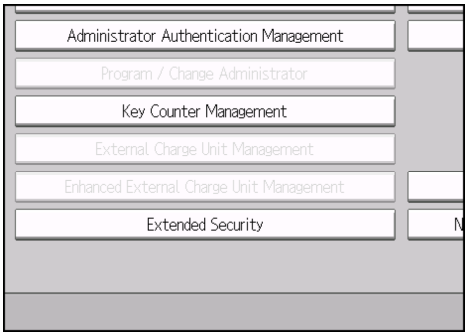


Key Repeat Normal

System Status Display Time 1 5 second(s)

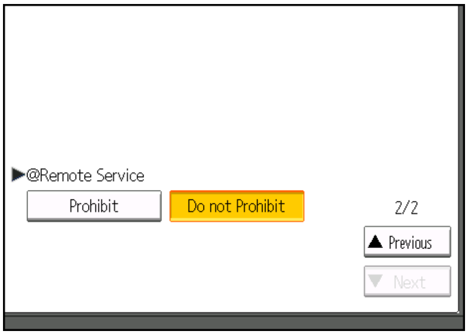
Status Indicator On

10. **Press [Extended Security].**


Administrator Authentication Management
Program / Change Administrator
Key Counter Management
External Charge Unit Management
Enhanced External Charge Unit Management
Extended Security
N

If this item is not visible, press [▼Next] to display more settings.

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



▶@Remote Service

Prohibit [✓ Do not Prohibit]

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

12. **Press [OK].**

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

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

Firmware Update Cautions

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

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

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 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.

Limits on each user’s access to machine functions and stored data are set by the administrator responsible for user access.

For details about the administrator, see p.21 "Administrators".

For details about the user, see p.33 "Users".

Encryption Technology

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

Glossary

Administrator

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

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

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

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. A login user name and login password may also be required when accessing the machine over the network or using such utilities as Web Image Monitor.

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 p.35 "Configuring User Authentication".

Specifying Authentication Information to Log in

Users are managed using the personal information managed in the machine's Address Book.

By enabling user authentication, you can allow only people registered in the Address Book to use the machine. Users can be managed in the Address Book by the user administrator. For information on specifying information to log in, see p.39 "Basic Authentication".

Specifying Which Functions are Available

This can be specified by the user administrator. Specify the functions available to registered users. By making this setting, you can limit the functions available to users. For information on how to specify which functions are available, see p.88 "Limiting Available Functions".

Ensuring Information Security

Protecting Registered Information in the Address Book

You can specify who is allowed to access the data in the Address Book. You can prevent the data in the Address Book from being used by unregistered users.

To protect the data from unauthorized reading, you can also encrypt the data in the Address Book. For details about protecting registered information in the Address Book, see p.67 "Protecting the Address Book".

Managing Log Files

The logs record failed access attempts and the names of users who accessed the machine successfully. You can use this information to help prevent data leaks. For details about managing log files, see p.90 "Managing Log Files".

Encrypting Data on the Hard Disk

Encrypt data stored on the hard disk to prevent information leakage. For details, see p.71 "Encrypting Data on the Hard Disk".

Overwriting the Data on the Hard Disk

To prevent data leaks, you can set the machine to automatically overwrite temporary data. We recommend that before disposing of the machine, you overwrite all the data on the hard disk. For details about overwriting the data on the hard disk, see p.78 "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 p.87 "Preventing Changes to Machine Settings".

Limiting Available Functions

To prevent unauthorized operation, you can specify who is allowed to access each of the machine's functions. For details about limiting available functions for users and groups, see p.88 "Limiting Available Functions".

Enhancing Network Security

Preventing Unauthorized Access

To prevent unauthorized access over the network and protect the Address Book and default settings, you can limit which IP addresses the machine can be accessed from or disable ports. For details about preventing unauthorized access, see p.111 "Preventing Unauthorized Access".

Safer Communication Using SSL, SNMPv3 and IPsec

You can encrypt this machine's transmissions using SSL, SNMPv3, and IPsec. By encrypting transmitted data and safeguarding the transmission route, you can prevent sent data from being intercepted, analyzed, and tampered with. For details about safer communication using SSL, SNMPv3 and IPsec, see p.120 "Protection Using Encryption" and p.129 "Transmission Using IPsec".

2. Configuring Administrator Authentication

This chapter describes what an administrator can do, how to register an administrator, how to specify administrator authentication, and how to log in to and out from the machine as an administrator.

Administrators

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

When an administrator controls limited access and settings, first select the machine's administrator and enable the authentication function before using the machine. When the authentication function is enabled, the login user name and login password are required in order to use the machine. The roles of user administrator, machine administrator, network administrator, and file administrator can be assigned to separate administrators. Sharing administrator tasks eases the burden on individual administrators while also reducing the possibility of unauthorized access and operations. Multiple administrator roles can be assigned to one administrator, and one role can also be shared by more than one administrator. You can also specify a supervisor who can change each administrator's password. The role of administrators is to manage system settings such as the machine's access restrictions. A person with administrator responsibilities cannot execute user functions when logged in as an administrator. To execute those functions, that person must be logged in as a normal user.

For instructions on registering the administrator, see p.26 "Registering the Administrator", and for instructions on changing the administrator's password, see p.185 "Supervisor Operations". For details on Users, see p.33 "Users".

Important

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

User Administrator

This is the administrator who manages personal information in the Address Book.

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

Users registered in the Address Book can also change and delete their own information.

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

Machine Administrator

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

Network Administrator

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

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

File Administrator

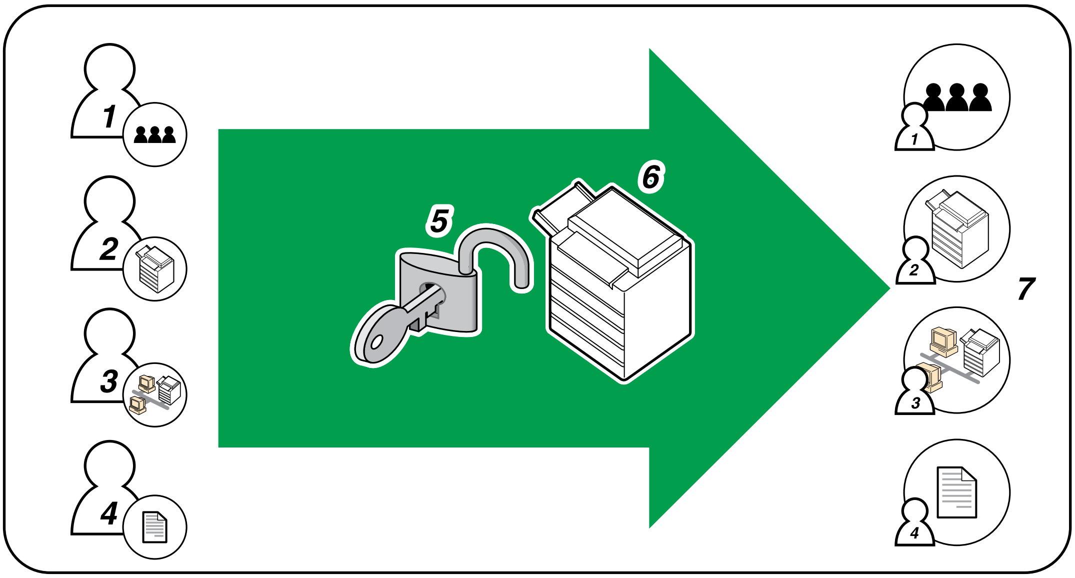
This is the administrator who manages files. Using Adjustment Settings for Operators, the file administrator can change settings related to print quality, such as image positioning. Adjustment Settings for Operators can also be specified by the user administrator, machine administrator, and network administrator.

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.

About Administrator Authentication

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



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. It is possible to set the machine so that only the machine administrator can specify paper settings and other defaults.

3. **Network Administrator**

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

4. **File Administrator**

   This is the administrator who manages files. Using Adjustment Settings for Operators, the file administrator can change settings related to print quality, such as image positioning. Adjustment Settings for Operators can also be specified by the user administrator, machine administrator, and network administrator.

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.**

   For details about each administrator, see p.21 "Administrators".

Enabling Administrator Authentication

To control administrators' access to the machine, perform administrator authentication using login user names and passwords. When registering an administrator, you cannot use a login user name already registered in the Address Book. Administrators are handled differently from the users registered in the Address Book. Windows authentication, LDAP authentication and Integration Server authentication are not performed for an administrator, so an administrator can log 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. For instructions on registering the administrator, see p.26 "Registering the Administrator".

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. The role of administrators is to manage system settings such as the machine's access restrictions. A person with administrator responsibilities cannot execute user functions when logged in as an administrator. To execute those functions, that person must be logged in as a normal user. Specify administrator authentication, and then specify user authentication. For details about specifying authentication, see p.35 "Configuring User Authentication".

Note

- Administrator authentication can also be specified via Web Image Monitor. For details, see Web Image Monitor Help.
- You can specify user code authentication without specifying administrator authentication.

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 changing the administrator password using the supervisor's authority, see p.185 "Supervisor Operations".

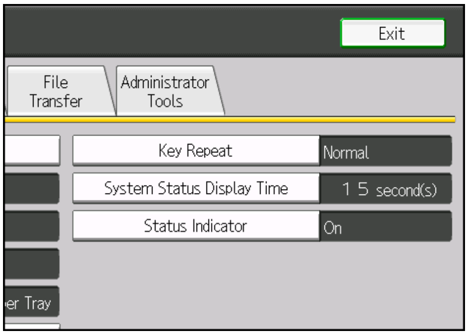
For details about logging in and logging out with administrator authentication, see p.28 "Logging in Using Administrator Authentication" and p.30 "Logging out Using Administrator Authentication".

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 instructions on registering the supervisor, see p.185 "Supervisor Operations".**

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

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

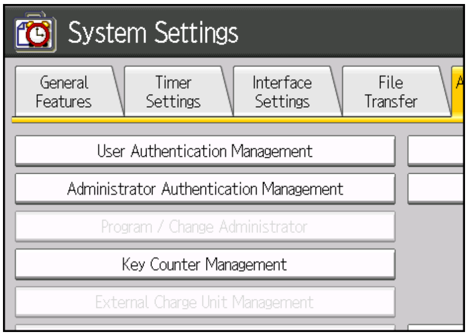


Key Repeat Normal

System Status Display Time 1 5 second(s)

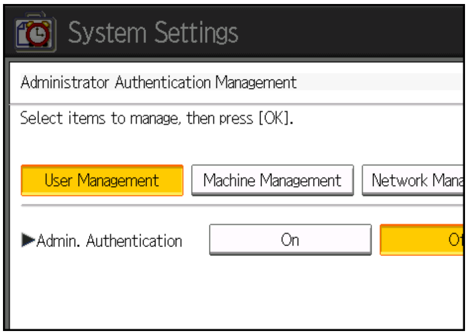
Status Indicator On

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
Key Counter Management
External Charge Unit Management

If this item is not visible, press [▼Next] to display more settings.

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

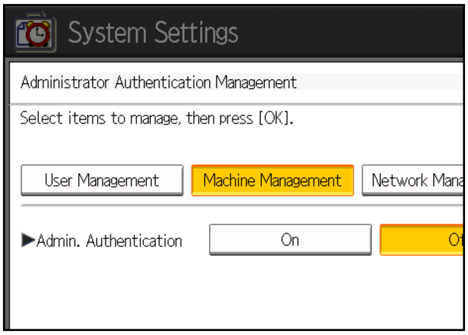


Administrator Authentication Management

Select items to manage, then press [OK].

▶Admin. Authentication

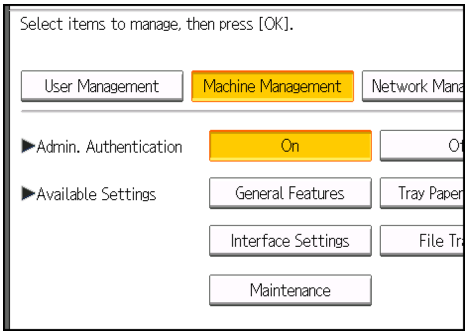
6. **Set "Admin. Authentication" to [On].**


System Settings

Administrator Authentication Management

Select items to manage, then press [OK].

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


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 p.88 "Limiting Available Functions".

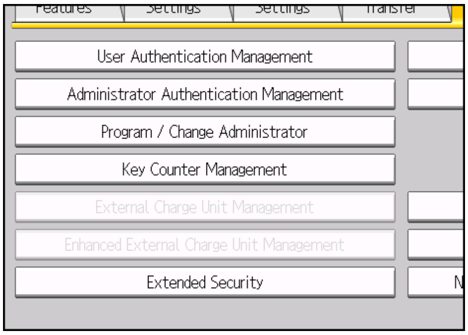
Registering the Administrator

If administrator authentication has been specified, we recommend only one person take each administrator role. The sharing of administrator tasks eases the burden on individual administrators while also limiting unauthorized operation by a single administrator. You can register up to four login user names (Administrators 1-4) to which you can grant administrator privileges.

If administrator authentication has already been specified, log in using a registered administrator name and password. The defaults are "admin" for the login name and blank for the password.

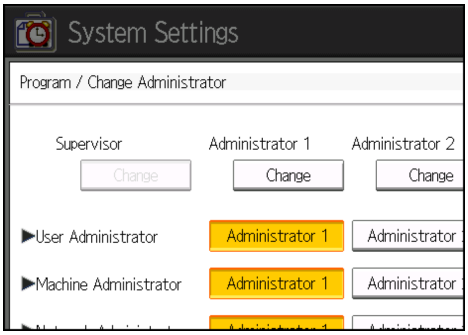
For details about logging in and logging out with administrator authentication, see p.28 "Logging in Using Administrator Authentication" and p.30 "Logging out Using Administrator Authentication".

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

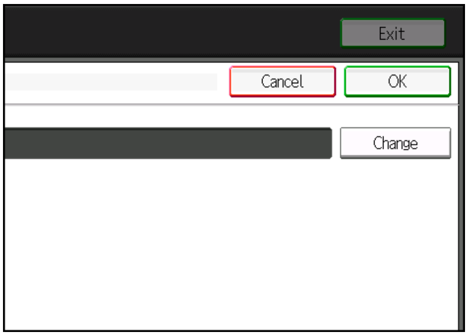

Features
Settings
Settings
Transfer
User Authentication Management
Administrator Authentication Management
Program / Change Administrator
Key Counter Management
External Charge Unit Management
Enhanced External Charge Unit Management
Extended Security
N

If this item is not visible, press [▼Next] to display more 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].**

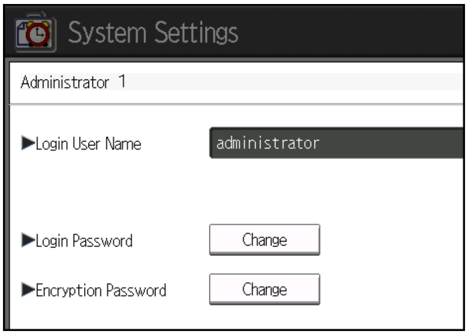


6. **Press [Change] for "Login User Name".**



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

8. **Press [Change] for "Login Password".**



System Settings

Administrator 1

▶Login User Name administrator

▶Login Password Change

▶Encryption Password Change

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 p.155 "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

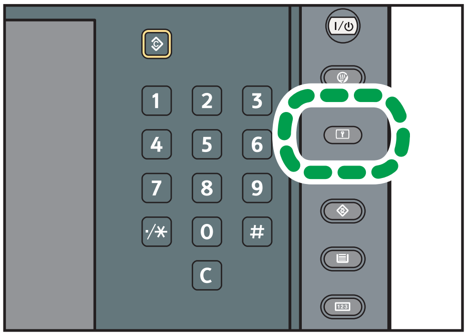
- When registering login user names and login passwords, you can specify up to 32 alphanumeric characters and symbols. Keep in mind that user names and passwords are case-sensitive. User names cannot contain numbers only, a space, colon (:), or quotation mark ("), nor can they be left blank. For details about characters that the password can contain, see p.155 "Specifying the Extended Security Functions".
- Administrator authentication can also be specified via Web Image Monitor. For details, see Web Image Monitor Help.

Logging in Using Administrator Authentication

If administrator authentication has been specified, log in using an administrator's user name and password.

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

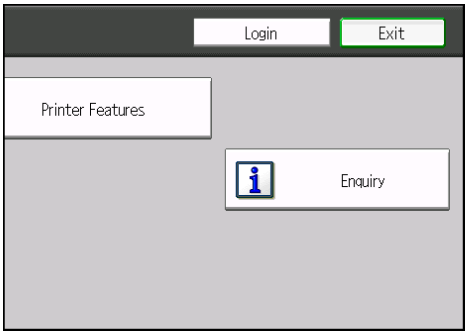
2. **Press the [Login/Logout] key.**



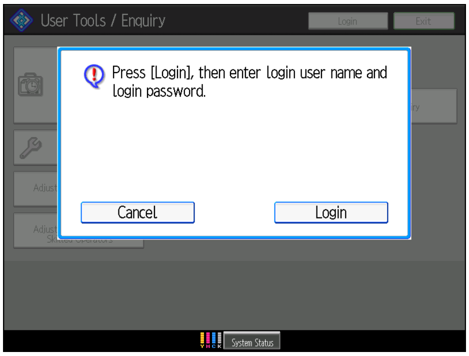
BZP003

The login screen appears.

The login screen can also be made to appear by pressing [Login] in the User Tools menu.



3. **Press [Login].**



Press [Login], then enter login user name and login password.

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.
- When you log in with a user name that has multiple administrator privileges, one of the administrator privileges associated with that name is displayed.
- If you log in using administrator authority, the name of the administrator logging on appears. If you try to log in from an operating screen, "You do not have the privileges to use this function. You can only change setting(s) as an administrator." appears. Press the [User Tools] key to change the default.

Logging out Using Administrator Authentication

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

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

Changing the Administrator

You can 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.

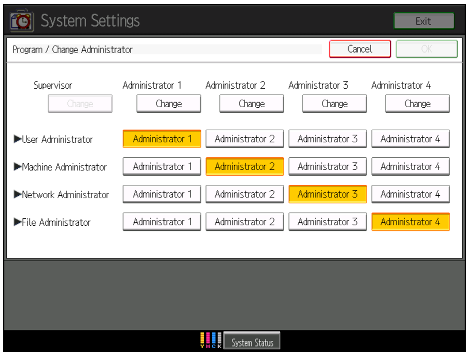
For example, to assign machine administrator authority and user administrator authority to [Administrator 1], press [Administrator 1] in the lines for the machine administrator and the user administrator.

For details about logging in and logging out with administrator authentication, see p.28 "Logging in Using Administrator Authentication" and p.30 "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 this item is not visible, press [▼Next] to display more settings.
5. **Press the [Administrator 1], [Administrator 2], [Administrator 3], or [Administrator 4] key next to each type of administrator to assign administrator privileges.**

   If you assign each administrator's authority to a different person, the following screen will appear:



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]

6. **Press [OK].**

   You will be automatically logged out.

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

Note

- An administrator's privileges can only be changed by an administrator with the relevant privileges.
- Administrator privileges cannot be revoked by any single administrator.

Changing the Administrator's User Name and Password

Using Web Image Monitor, you can log into the machine and change the administrator's user name and password.

1. **Open a Web browser.**
2. **Enter "http://(the machine's IP address or host name)/" in the address bar.**
3. **Click [Login].**
4. **Enter the login name and password of an administrator, and then click [Login].**

   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.

5. **Click [Configuration], and then click [Program/Change Administrator] under "Device Settings".**
6. **Enter the new login user name of the administrator whose name you wish to change.**
7. **Click [Change] next to "Login Password" under the administrator whose password you wish to change.**
8. **Enter the new password in the "New Password" and "Confirm Password" fields, and then click [OK].**
9. **Click [OK].**

   If the login information is changed successfully, an authentication message appears.

10. Click [OK].

The login screen appears.

Note

- 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.

3. Configuring User Authentication

This chapter describes what a user can do, how to specify user authentication, and how to log into and out from the machine as a user.

Users

A user performs normal operations on the machine. Users are managed using the personal information in the machine's Address Book, and can use only the functions they are permitted to access by administrators. By enabling user authentication, you can allow only people registered in the Address Book to use the machine. Users can be managed in the Address Book by the user administrator. For details about administrator, see p.21 "Administrators". For details about user registration, see "Registering Names", Network and System Settings Reference or Web Image Monitor Help.

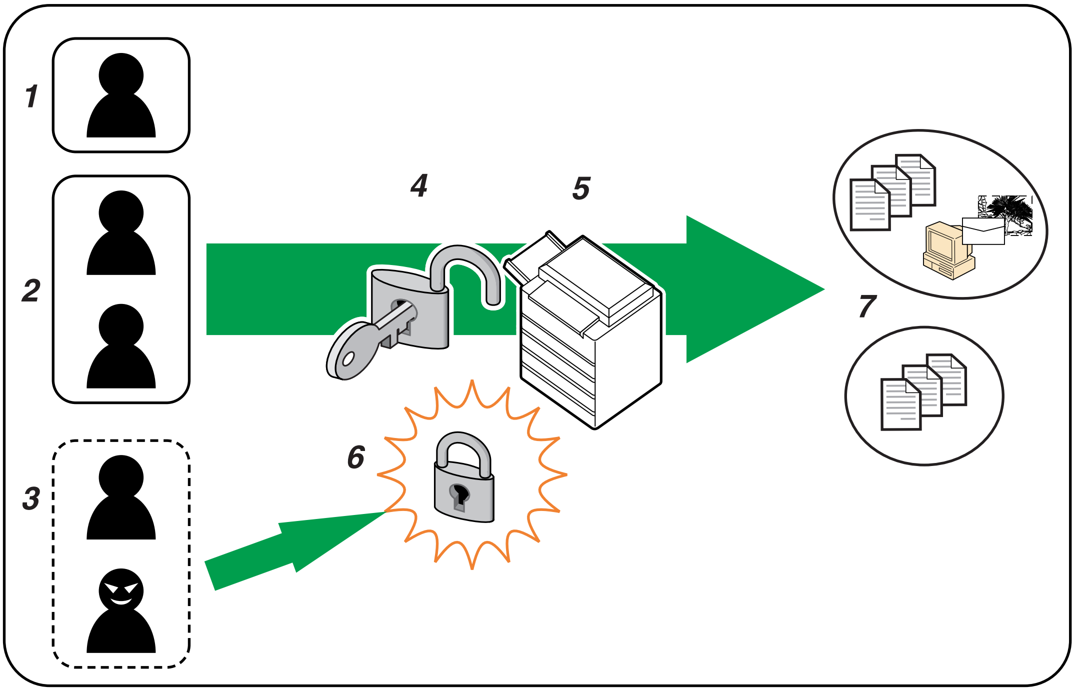
Important

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

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.



BZM005

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.**

Configuring User Authentication

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

Administrator authentication	p.24 "Specifying Administrator Privileges" p.26 "Registering the Administrator"
User authentication	Specify user authentication. Five types of user authentication are available: p.37 "User Code Authentication" p.39 "Basic Authentication" p.43 "Windows Authentication" p.49 "LDAP Authentication" p.53 "Integration Server Authentication"

Note

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

Enabling User Authentication

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

For printer job authentication, user code authentication is required.

Note

- User code authentication is used for authenticating on the basis of a user code, and basic authentication, Windows authentication, LDAP authentication, and Integration Server authentication are used for authenticating individual users.
- You can specify user code authentication without specifying administrator authentication.
- A user code account, that has no more than eight digits and is used for user code authentication, can be carried over and used as a login user name even after the authentication method has switched from user code authentication to basic authentication, Windows authentication, LDAP authentication, or Integration Server authentication. In this case, since the user code authentication does not have a password, the login password is set as blank.
- When authentication switches to an external authentication method (Windows authentication, LDAP authentication, or Integration Server authentication), authentication will not occur, unless the external authentication device has the carried over user code account previously registered. However, the user code account will remain in the Address Book of the machine despite an authentication failure.
- From a security perspective, when switching from user code authentication to another authentication method, we recommend that you delete accounts you are not going to use, or set up a login password. For details about deleting accounts, see "Deleting a Registered Name", Network and System Settings Reference. For details about changing passwords, see p.40 "Specifying Login User Names and Passwords".
- You cannot use more than one authentication method at the same time.
- User authentication can also be specified via Web Image Monitor. For details, see Web Image Monitor Help.

User Code Authentication

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

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

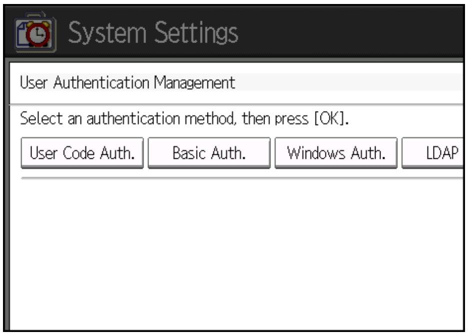
Specifying User Code Authentication

This can be specified by the machine administrator. For details about logging in and logging out with administrator authentication, see p.28 "Logging in Using Administrator Authentication" and p.30 "Logging out Using Administrator Authentication".

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

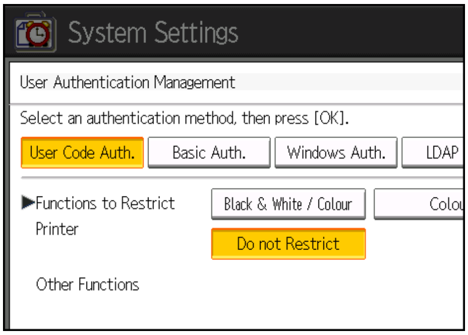
   If this item is not visible, press [▼Next] to display more settings.

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



Select an authentication method, then press [OK].

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



Select an authentication method, then press [OK].

User Code Auth.

Printer: Do not Restrict

The selected settings will be unavailable to users.

For details about limiting available functions for individuals or groups, see p.88 "Limiting Available Functions".

For details about printer job authentication, see p.57 "Printer Job Authentication".

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

   A confirmation message appears.

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

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 limitation of functions, see p.39 "Authentication Information Stored in the Address Book".

Specifying Basic Authentication

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

This can be specified by the machine administrator. For details about logging in and logging out with administrator authentication, see p.28 "Logging in Using Administrator Authentication" and p.30 "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 this item is not visible, press [▼Next] to display more settings.
5. **Select [Basic Auth.].**
6. **Press [OK].**
7. **Press the [User Tools] key.**

   A confirmation message appears.

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

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 p.28 "Logging in Using Administrator Authentication" and p.30 "Logging out Using Administrator Authentication".

If you have enabled user authentication, you can specify access limits and usage limits to the machine's functions for each user or group of users. Specify the necessary settings in the Address Book entry of each user. For details about limiting which functions of the machine are available, see p.88 "Limiting Available Functions".

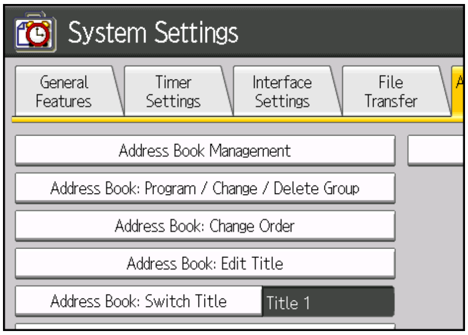
Users must have a registered account in the Address Book in order to use the machine when user authentication is specified. For details about user registration, see "Registering Names", Network and System Settings Reference.

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

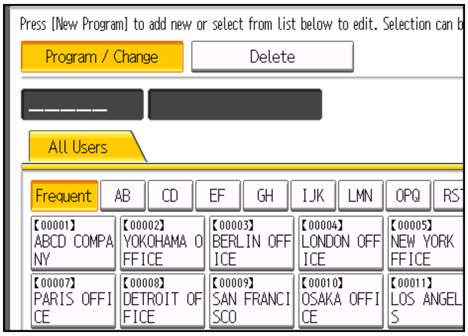
Specifying Login User Names and Passwords

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

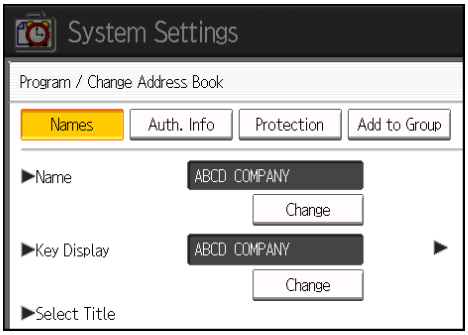
1. **Press the [User Tools] key.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [Address Book Management].**



5. **Select the user.**


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

6. Press [Auth. Info].

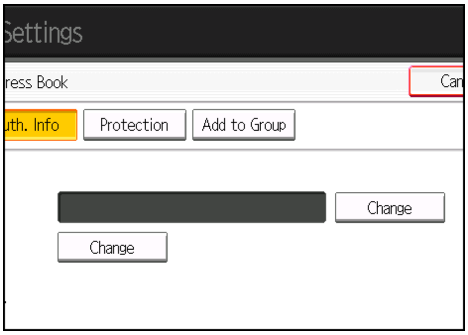


▶Name ABCD COMPANY

▶Key Display ABCD COMPANY

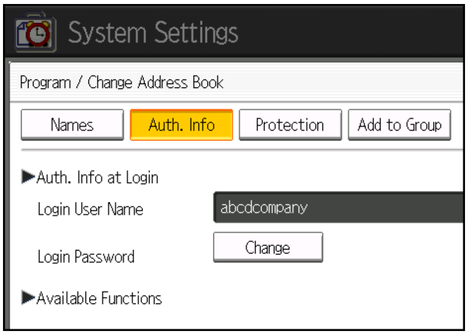
▶Select Title

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



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

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



▶Auth. Info at Login

Login User Name abcdcompany

Login Password

▶Available Functions

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

- Login user names and passwords are governed by the following rules, which the administrator must make sure general users are aware of.
    - Login user names and passwords can contain both alphanumeric characters and symbols.
    - Login user names can be up to 32 characters; passwords, 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 multibyte 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 p.155 "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.

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

Operational requirements for NTLM authentication

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

- This machine 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 you are using LDAP, we recommend you use SSL to encrypt communication between the machine and the LDAP server. Encryption by SSL is possible only if the LDAP server supports TLSv1, SSLv2, or SSLv3.
    - Windows 2000 Server
    - Windows Server 2003/2003 R2
    - Windows Server 2008/2008 R2

Operational requirements for Kerberos authentication

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

- A domain controller must be set up in a designated domain.
- The operating system must support KDC (Key Distribution Center). To obtain user information when running Active Directory, use LDAP. If you are using LDAP, we recommend you use SSL to encrypt communication between the machine and the LDAP server. Encryption by SSL is possible only if the LDAP server supports TLSv1, SSLv2, or SSLv3. Compatible operating systems are listed below.
    - Windows 2000 Server
    - Windows Server 2003/2003 R2
    - Windows Server 2008/2008 R2

    To use Kerberos authentication under Windows Server 2008, Service Pack 2 or later must be installed.

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.
- If the authenticating server only supports NTLM when Kerberos authentication is selected on the machine, the authenticating method will automatically switch to NTLM.

Note

- Enter the login name and 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.
- A user registered in two or more global groups can use all the functions available to members of those groups.
- When accessing the machine subsequently, you can use all the functions available to your group and to you as an individual user.
- If the "Guest" account on the Windows server is enabled, even users not registered in the domain controller can be authenticated. When this account is enabled, users are registered in the Address Book and can use the functions available under "*Default Group".
- Under Windows authentication, you can select whether or not to use secure sockets layer (SSL) authentication.
- To automatically register user information under Windows authentication, it is recommended that communication between the machine and domain controller be encrypted using SSL. To do this, you must create a server certificate for domain controller. For details about creating a server certificate, see p.47 "Creating the Server Certificate".
- Under Windows authentication, you do not have to create a server certificate unless you want to automatically register user information using SSL.
- To enable Kerberos for LDAP authentication, a realm must be registered beforehand. The realm must be programmed in capital letters. For details about registering a realm, see "Programming the Realm", Network and System Settings Reference.

Specifying Windows Authentication

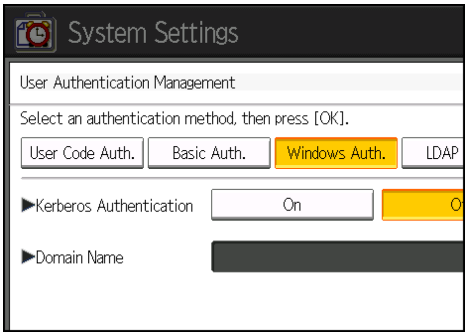
Before beginning to configure the machine, make sure that administrator authentication is properly configured under "Administrator Authentication Management".

This can be specified by the machine administrator. For details about logging in and logging out with administrator authentication, see p.28 "Logging in Using Administrator Authentication" and p.30 "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 this item is not visible, press [▼Next] to display more settings.

5. **Select [Windows Auth.].**
6. **If you want to use Kerberos authentication, press [On].**



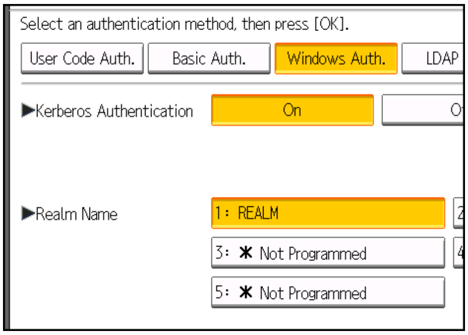
System Settings

User Authentication Management

Select an authentication method, then press [OK].

   If you want to use NTLM authentication, press [Off] and proceed to step 8.

7. **Select Kerberos authentication realm and proceed to step 9.**

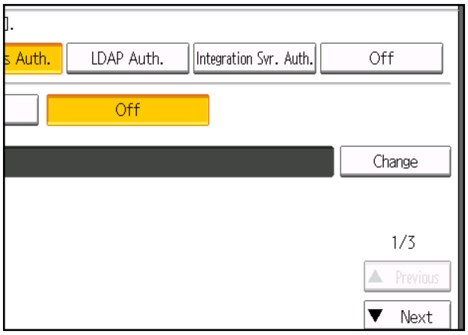


Select an authentication method, then press [OK].

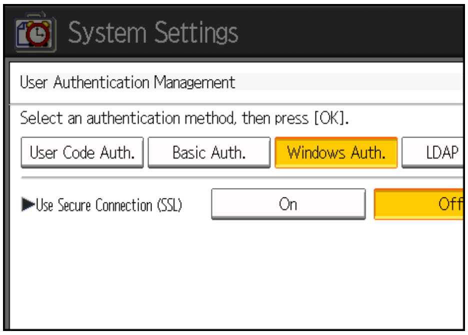
   To enable Kerberos authentication, a realm must be registered beforehand. The realm name must be registered in capital letters. For details about registering a realm, see "Programming the Realm", Network and System Settings Reference.

   Up to 5 realms can be registered.

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



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


System Settings
User Authentication Management
Select an authentication method, then press [OK].
User Code Auth.
Basic Auth.
Windows Auth.
LDAP
▶Use Secure Connection (SSL)
On
Off

If this item is not visible, press [▼Next] to display more settings.

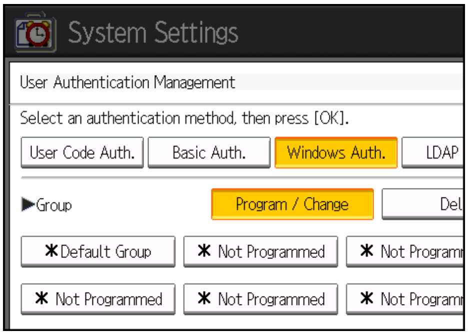
If you are not using secure sockets layer (SSL) for authentication, press [Off].

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

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

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



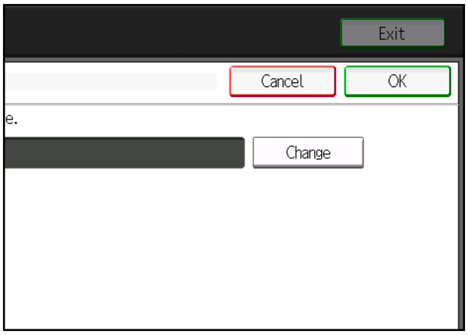
System Settings

User Authentication Management

Select an authentication method, then press [OK].

If this item is not visible, press [▼Next] to display more settings.

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



12. **Press [OK].**

13. **Press [OK].**

14. **Press [OK].**

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

A confirmation message appears.

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

Creating the Server Certificate

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

Windows Server 2008 R2 is used to illustrate the procedure.

1. **On the [Start] menu, point to [Administrator Tools], and then click [Internet Information Services (IIS) Manager].**

2. **In the left column, click the server name, and then double-click [Server Certificates].**

3. **In the right column, click [Create Certificate Request...].**

4. **Enter all the information, and then click [Next].**
5. **In "Cryptographic service provider:", select a provider, and then click [Next].**
6. **Click [...], and then specify a file name for the certificate request.**
7. **Specify a location in which to store the file, and then click [Open].**
8. **Close [Internet Information Services (IIS) Manager] by clicking [Finish].**

Installing the Device Certificate (Issued by a Certificate Authority)

Use this procedure to install the device certificate issued by a certificate authority.

1. **Open a Web browser.**
2. **Enter "http://(the machine's IP address or host name)/" in the address bar.**
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].**
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 box, enter the contents of the device certificate issued by the certificate authority.

   For details about the displayed items and selectable items, see Web Image Monitor Help.
8. **Click [OK].**
9. **Wait a moment for the device to restart, and then click [OK].**

   "Installed" appears under "Certificate Status" to show that a device certificate for the machine has been installed.
10. **Click [OK].**
11. **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. For details about creating a server certificate, see p.47 "Creating the Server Certificate". The setting for using SSL can be specified in the LDAP server setting.

Using Web Image Monitor, you can enable a function that checks whether the SSL server is trustworthy when you connect to the server. For details about specifying LDAP authentication using Web Image Monitor, see Web Image Monitor Help.

Important

- During LDAP authentication, the data registered in the LDAP server is automatically registered in the machine. If user information on the server is changed, information registered in the machine may be overwritten when authentication is performed.
- Under LDAP authentication, you cannot specify access limits for groups registered in the LDAP server.
- The reference function is not available for SSL servers when a search for LDAP is in progress.
- Enter the user's login user name using up to 128 characters, and then enter the user's login password using up to 128 characters. Make sure the first 32 characters of the login user name are unique.
- Do not use double-byte Japanese, Traditional Chinese, Simplified Chinese, or Hangul characters when entering the login user name or password. If you use double-byte characters, you cannot authenticate using Web Image Monitor.

Operational requirements for LDAP authentication

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

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

- SSL Communication
- Authentication

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

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

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

Note

- Enter the login name and password correctly; keeping in mind that it is case-sensitive.
- When you select Cleartext authentication, LDAP Simplified authentication is enabled. Simplified authentication can be performed with a user attribute (such as cn, or uid), instead of the DN.
- In LDAP simple authentication mode, authentication will fail if the password is left blank. To allow blank passwords, contact your service representative.
- Under LDAP authentication, if "Anonymous Authentication" in the LDAP server's settings is not set to Prohibit, users who do not have an LDAP server account might still be able to gain access.
- If the LDAP server is configured using Windows Active Directory, "Anonymous Authentication" might be available. If Windows authentication is available, we recommend you use it.
- The first time an unregistered user accesses the machine after LDAP authentication has been specified, the user is registered in the machine and can use the functions available under "Available Functions" during LDAP authentication. To limit the available functions for each user, register each user and corresponding "Available Functions" setting in the Address Book, or specify "Available Functions" for each registered user. The "Available Functions" setting becomes effective when the user accesses the machine subsequently.
- To enable Kerberos for LDAP authentication, a realm must be registered beforehand. The realm must be programmed in capital letters. For details about registering a realm, see "Programming the Realm", Network and System Settings Reference.

Specifying LDAP Authentication

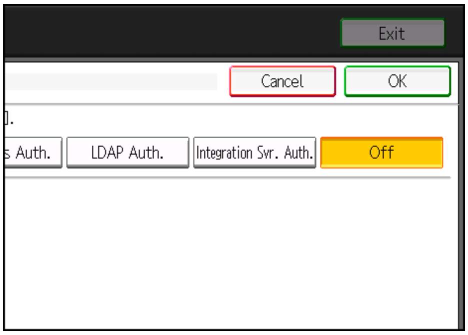
Before beginning to configure the machine, make sure that administrator authentication is properly configured under "Administrator Authentication Management".

This can be specified by the machine administrator. For details about logging in and logging out with administrator authentication, see p.28 "Logging in Using Administrator Authentication" and p.30 "Logging out Using Administrator Authentication".

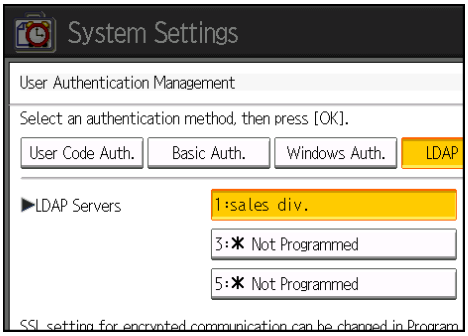
1. **Press the [User Tools] key.**

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

   If this item is not visible, press [▼Next] to display more settings.
5. **Select [LDAP Auth.].**



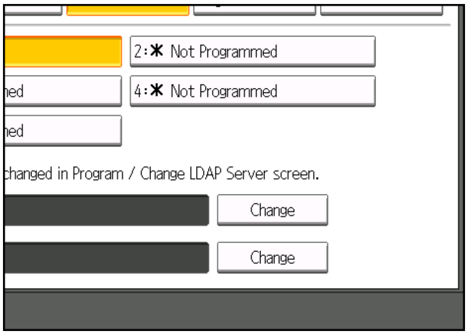
6. **Select the LDAP server to be used for LDAP authentication.**



Select an authentication method, then press [OK].

SSL setting for encrypted communication can be changed in Program

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



hanged in Program / Change LDAP Server screen.

If this item is not visible, press [▼Next] to display more settings.

8. **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.

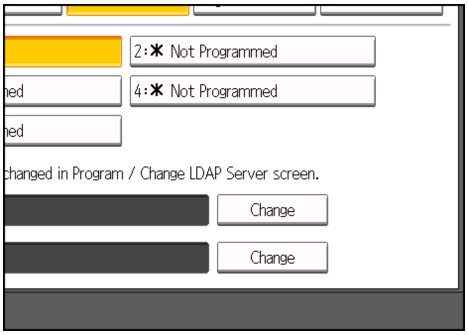
   To specify multiple login attributes, place a comma (,) between them. The search will return hits for either or both attributes.

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

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

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

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



10. **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.

11. **Press [OK].**

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

    A confirmation message appears.

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

Integration Server Authentication

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. By downloading the user information registered in the Integration Server into the machine's Address Book, you can authenticate a user without registering the user on the machine's control panel.

To use Integration Server authentication, you need a server on which Authentication Manager is installed in addition to the machine. For details about the software, contact your sales representative.

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

Important

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

Specifying Integration Server Authentication

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

This can be specified by the machine administrator. For details about logging in and logging out with administrator authentication, see p.28 "Logging in Using Administrator Authentication" and p.30 "Logging out Using Administrator Authentication".

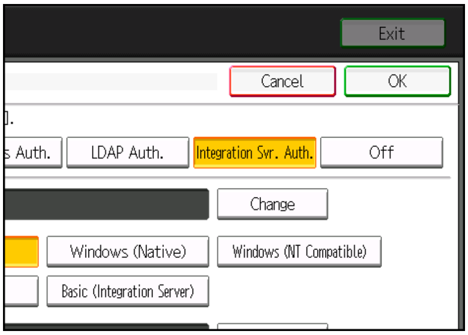
This section explains how to specify the machine settings.

For details about Integration Server authentication, see the Authentication Manager help.

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

   If this item is not visible, press [▼Next] to display more settings.
5. **Select [Integration Svr. Auth.].**

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

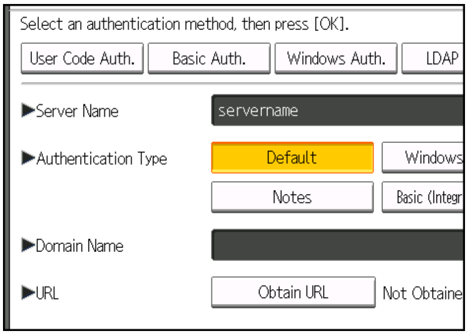


Specify the name of the server for external authentication.

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

Enter the IPv4 address or host name.

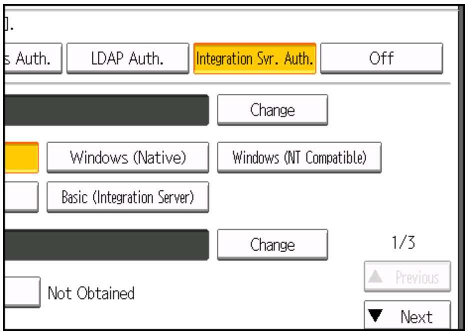
8. **In "Authentication Type", select the authentication system for external authentication.**


Select an authentication method, then press [OK].

▶Server Name servername

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

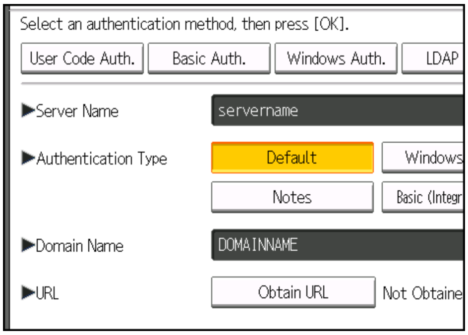
9. **Press [Change] for "Domain Name".**



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

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

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



Select an authentication method, then press [OK].

▶Server Name servername

▶Authentication Type Default

▶Domain Name DOMAINNAME

▶URL Not Obtaine

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

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

12. **Press [Exit].**

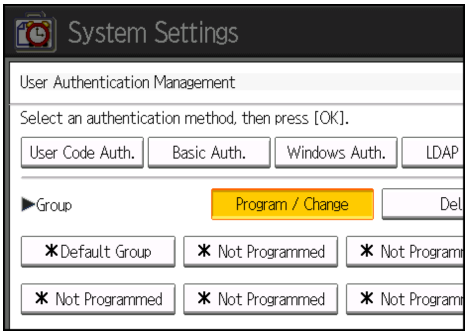
In the "Authentication Type", if you have not registered a group, proceed to step 17.

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

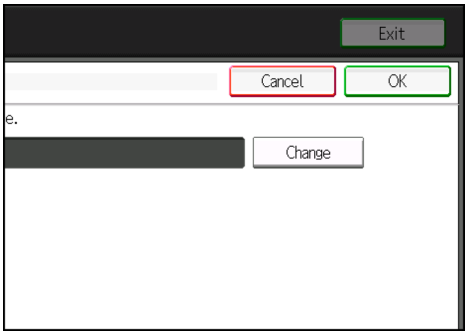
User Authentication Management

Select an authentication method, then press [OK].

▶Group

If this item is not visible, press [▼Next] to display more settings.

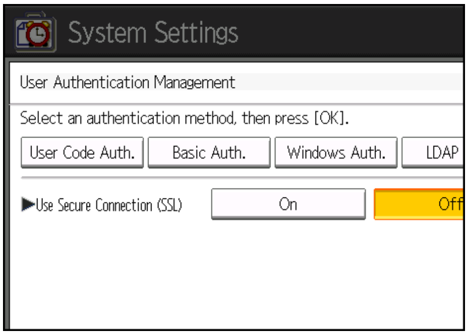
14. **Under "Group Name", press [Change], and then enter the group name.**



15. **Press [OK].**

16. **Press [OK].**

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



User Authentication Management

Select an authentication method, then press [OK].

▶Use Secure Connection (SSL)

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

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

A confirmation message appears.

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

Printer Job Authentication

Depending on the user authentication settings of the machine and printer driver, print jobs may not be printed. Specify these settings according to the operating environment.

A job can be printed if the user code entered in the printer properties dialog box matches a user code registered in the machine's Address Book and the job is authenticated. However, even if the user code matches, the job will be canceled if the user is not authorized to use printer functions.

Combination Table

Machine Setting		User Code	
[User Authentication Management]	Functions to Restrict	Matching	Non-matching
[User Code Auth.]	[Black & White / Colour]	●	×
	[Colour]	●	×
	[PC Control]	○	○
	[Do not Restrict]	○	○
[Basic Auth.] [Windows Auth.] [LDAP Auth.] [Integration Svr. Auth.]		○	○
[Off]		○	○

○: Printing is possible.

●: Printing is possible if the user is authorized to print in black and white or color.

×: Printing is not possible.

Note

- Of various types of user authentication, only user code authentication supports authentication of print jobs. Under basic authentication, Windows authentication, LDAP authentication, and Integration Server authentication, all jobs can be printed regardless of the user authentication settings.
- If you have enabled user code authentication on the machine, be sure to enter the user code in the printer properties dialog box.

- If you try to print without entering the user code, the print job will be unauthorized and it will be canceled.
- For details about entering the user code in the printer properties dialog box, see the Printer Reference or the printer driver Help.

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 off if you do not use the control panel within a given time. For details about auto logout timer, see p.63 "Auto Logout". Additionally, you can authenticate using an external device. For details about using an external device for user authentication, contact your service representative.

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 function can only be used under basic authentication, Windows authentication, LDAP authentication, or Integration Server authentication.

If User Code Authentication is Specified

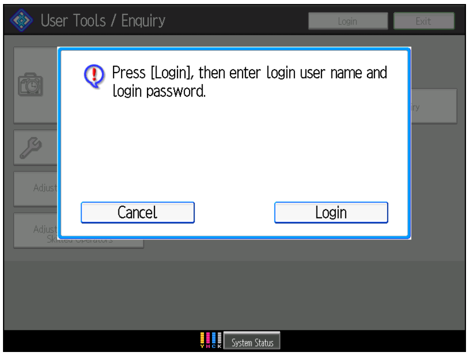
User code authentication can be used for printer job authentication.

Logging in Using the Printer Driver

When user code authentication is set, specify a user code in the printer driver's printing preferences dialog box. For details, see the printer driver Help.

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

When basic authentication, Windows authentication, LDAP authentication or Integration Server authentication is set, the following screen appears.



Press [Login], then enter login user name and login password.

Enter your login user name and password.

Logging in Using the Control Panel

Use the following procedure to log in if basic authentication, Windows authentication, LDAP authentication, or Integration Server authentication is enabled.

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

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].**

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

1. **Open a Web browser.**
2. **Enter "http://(the machine's IP address or host name)/" in the address bar.**
3. **Click [Login] on the top page of Web Image Monitor.**
4. **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

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

Note

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

User Lockout Function

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

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

Lockout setting items

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

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

Lockout release privileges

Administrators with unlocking privileges are as follows.

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

Specifying the User Lockout Function

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

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

   The machine administrator can log in.

   Enter the login user name and login password.
4. **Click [Configuration], and then click [User Lockout Policy] under "Security".**
5. **Set "Lockout" to [Active].**
6. **In the drop down menu, select the number of login attempts to permit before applying lockout.**
7. **After lockout, if you want to cancel lockout after a specified time elapses, set "Lockout Release Timer" to [Active].**
8. **In the "Lock Out User for" field, enter the number of minutes until lockout is disabled.**
9. **Click [OK].**
10. **Click [Logout].**

Canceling Password Lockout

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

   The administrator or supervisor with unlocking privileges can log in.

   Enter the login user name and login password.
4. **Click [Address Book].**
5. **Select the locked out user's account.**

6. **Click [Change].**
7. **Set "Lockout" to [Inactive] under "Authentication Information".**
8. **Click [OK].**
9. **Click [Logout].**

Note

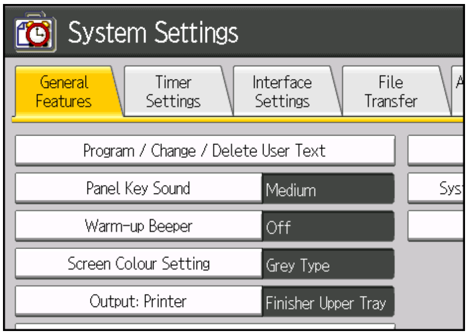
- You can cancel the administrator and supervisor password lockout by turning the power off and then turning it back on again, or by canceling the setting in [Program/Change Administrator] under [Configuration] in Web Image Monitor.

Auto Logout

This can be specified by the machine administrator. For details about logging in and logging out with administrator authentication, see p.28 "Logging in Using Administrator Authentication" and p.30 "Logging out Using Administrator Authentication".

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

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



System Settings

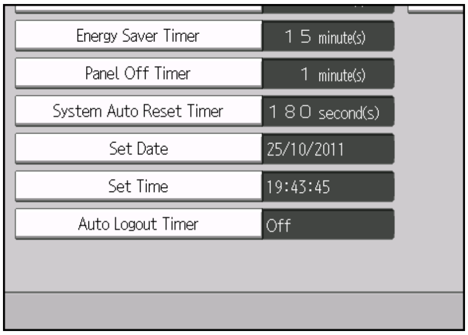
Panel Key Sound: Medium

Warm-up Beeper: Off

Screen Colour Setting: Grey Type

Output: Printer: Finisher Upper Tray

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



Energy Saver Timer 1 5 minute(s)

Panel Off Timer 1 minute(s)

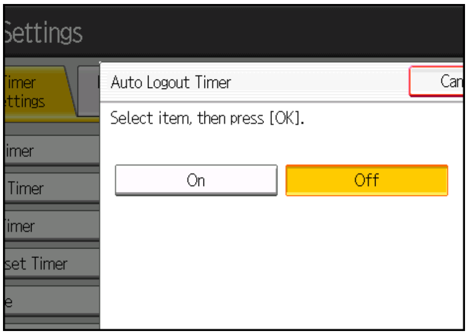
System Auto Reset Timer 1 8 0 second(s)

Set Date 25/10/2011

Set Time 19:43:45

Auto Logout Timer Off

5. **Select [On].**



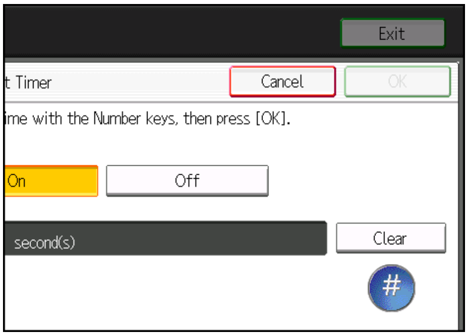
Settings

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].

second(s)

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

A confirmation message appears.

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

Note

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

Authentication Using an External Device

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

For details, contact your sales representative.

4. Securing Information Stored on Hard Disk

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

Protecting the Address Book

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

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

Configuring Address Book Access Permissions

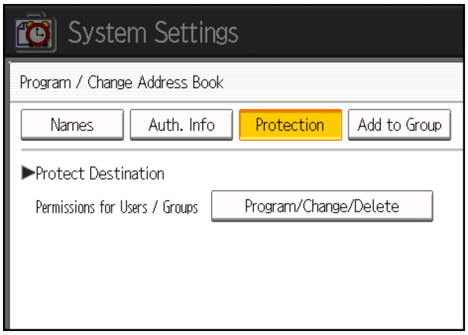
This can be specified by the registered user. Access permission can also be specified by a user granted full control or the user administrator. For details about logging in and logging out with administrator authentication, see p.28 "Logging in Using Administrator Authentication" and p.30 "Logging out Using Administrator Authentication".

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

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

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".**



System Settings

Program / Change Address Book

▶Protect Destination

Permissions for Users / Groups Program/Change/Delete

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 to whom you want to assign access permission, 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

- You can specify the access permissions for authenticated users regarding the personal data registered in the machine's Address Book by selecting [Read-only], [Edit], [Edit / Delete], or [Full Control].
- To ensure machine security, do not grant [Edit], [Edit/Delete], or [Full Control] permission to general users.

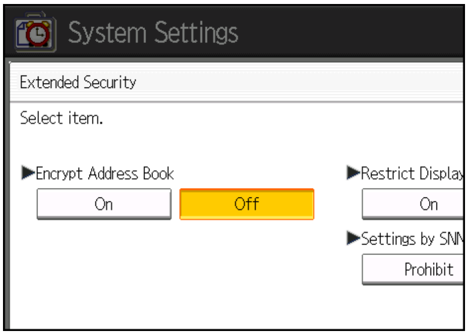
Encrypting Data in the Address Book

This can be specified by the user administrator. For details about logging in and logging out with administrator authentication, see p.28 "Logging in Using Administrator Authentication" and p.30 "Logging out Using Administrator Authentication".

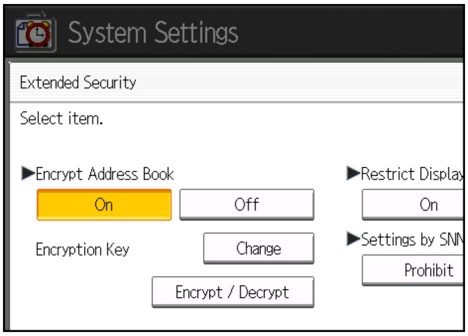
You can encrypt the data in the Address Book using the extended security function, "Encrypt Address Book". For details about this and other extended security functions, see p.155 "Specifying the Extended Security Functions".

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

   If this item is not visible, press [▼Next] to display more settings.
5. **Press [On] for "Encrypt Address Book".**



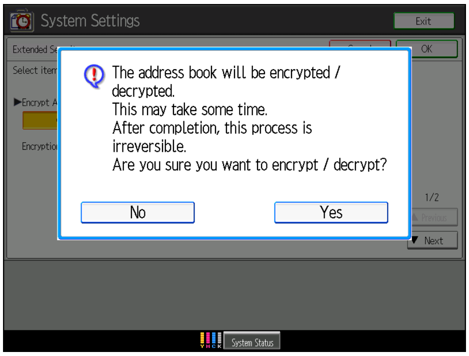
6. **Press [Change] for "Encryption Key".**



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

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

9. **Press [Yes].**



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 the main power off during encryption, as doing so may corrupt the data.

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

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

The machine cannot be used during encryption.

Normally, once encryption is complete, "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", Network and System Settings Reference.

Encrypting Data on the Hard Disk

This can be specified by the machine administrator. For details about logging in and logging out with administrator authentication, see p.28 "Logging in Using Administrator Authentication" and p.30 "Logging out Using Administrator Authentication".

Prevent information from leaking by using encryption when writing Address Book details and authentication data. In addition, if the machine malfunctions or needs to be replaced, your service representative can easily transfer existing data to a new machine.

When the data encryption settings are enabled, an encryption key is generated and this is used to restore the data. This key can be changed at any time.

Data that is encrypted

This function encrypts data that is stored in the machine's NVRAM (memory that remains even after the machine has been turned off) and on the hard disk.

The following data is encrypted:

- Address Book data
- User authentication information
- Temporarily stored document data
- Logs
- Network I/F setting information
- System settings information

Data that will not be encrypted

- Document data stored using printer function

Enabling the Encryption Settings

If you specify [Format All Data] to enable encryption when first setting up the machine, the encryption setting procedure will take only several minutes. Note that all data stored on the hard disk will be initialized when this setting is specified.

The table below describes which data will be kept and which data will be initialized when [Format All Data], [File System Data Only], or [All Data] is specified.

Setting	Data to be kept	Data not kept (Data to be initialized)	Required time
Format All Data	None	All data	Several minutes

Setting	Data to be kept	Data not kept (Data to be initialized)	Required time
File System Data Only	• Address Book • Job logs/access logs • Sent and received emails	None	Approximately 30 minutes
All Data	All data	None	Approximately 6 hours

Things to note when enabling encryption settings

- Note that the machine's settings will not be initialized to their system defaults even if [Format All Data], [File System Data Only], or [All Data] is specified.

Use the following procedure to enable the encryption settings when first setting up the machine, or after encryption settings have been canceled and settings must be made again.

Important

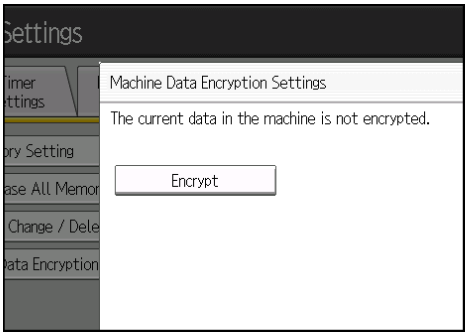
- The machine cannot be operated while data is being encrypted.
- Once the encryption process begins, it cannot be stopped. Make sure that the machine's main power is not turned off while the encryption process is in progress. If the machine's main power is turned off while the encryption process is in progress, the hard disk will be damaged and all data on it will be unusable.
- The encryption key is required for data recovery if the machine malfunctions. Be sure to store the encryption key safely for retrieving backup data.
- Encryption begins after you have completed the control panel procedure and rebooted the machine by turning off and on the main power switch. If there is unencrypted data on the hard disk that must be both transferred and encrypted, rebooting will take up to six and a half hours. If there is encrypted data on the hard disk that must be re-encrypted, rebooting will also take up to six and a half hours. If both the erase-by-overwrite function and the encryption function are specified, encryption begins after the data that is stored on the hard disk has been overwritten and the machine has been rebooted with the turning off and on of the main power switch.
- If you want to specify encryption of unencrypted data with erase-by-overwrite, select [Random Numbers] as the overwrite method, and set the number of overwrites to "3". The entire process will take up to nine hours. If you specify re-encryption of encrypted data, the entire process will also take up to nine 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.

- Rebooting will be faster if there is no data to carry over to the hard disk and if encryption is set to [Format All Data], even if all the data on the hard disk is formatted. Before you perform encryption, we recommend you back up important data such as the Address Book.
- If the encryption key update was not completed, the printed encryption key will not be valid.

1. **Press the [User Tools] key.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [Machine Data Encryption Settings].**

   If this item is not visible, press [▼Next] to display more settings.

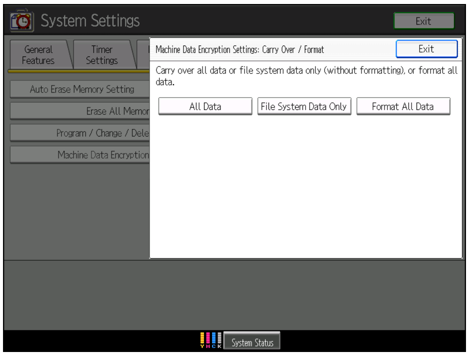
5. **Press [Encrypt].**


Machine Data Encryption Settings

The current data in the machine is not encrypted.

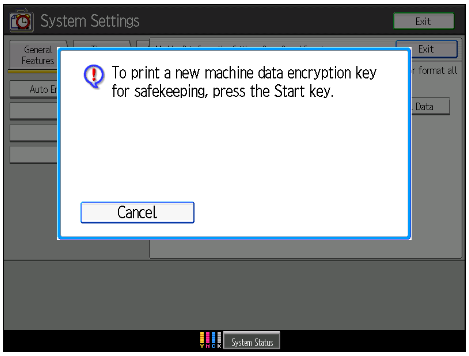
6. **Select the data to be carried over to the hard disk and not be reset.**

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


Machine Data Encryption Settings: Carry Over / Format

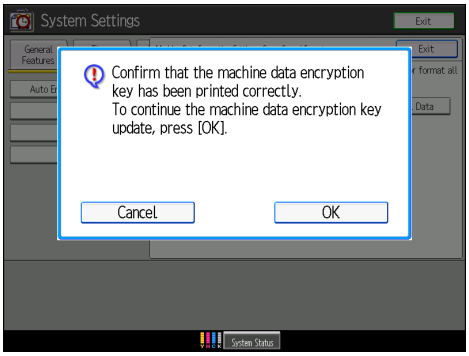
Carry over all data or file system data only (without formatting), or format all data.

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



To print a new machine data encryption key for safekeeping, press the Start key.

8. **Press [OK].**



Confirm that the machine data encryption key has been printed correctly.
To continue the machine data encryption key update, press [OK].

9. **Press [Exit].**

10. **Press [Exit].**

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

12. **Turn off the power and the main power switch, and then turn the main power switch back on.**

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

Printing the Encryption Key

Use the following procedure to print the key again if it has been lost or misplaced.

Important

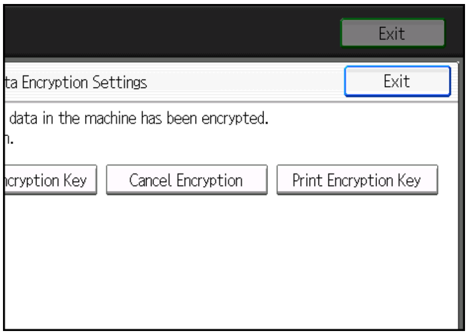
- The encryption key is required for data recovery if the machine malfunctions. Be sure to store the encryption key safely for retrieving backup data.
- If the encryption key update was not completed, the printed encryption key will not be valid.

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

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

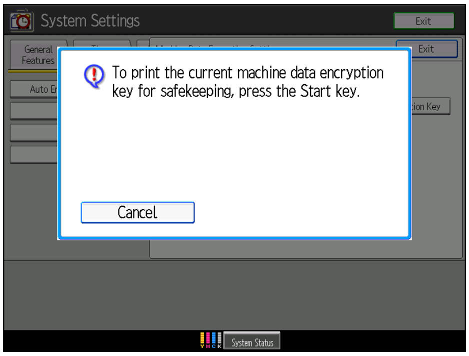
3. **Press [Administrator Tools].**
4. **Press [Machine Data Encryption Settings].**

   If this item is not visible, press [▼Next] to display more settings.
5. **Press [Print Encryption Key].**



data in the machine has been encrypted.
n.

6. **Press the [Start] key.**



To print the current machine data encryption key for safekeeping, press the Start key.

7. **Press [Exit].**

Updating the Encryption Key

You can update the encryption key and create a new key. Updates are possible when the machine is functioning normally.

Important

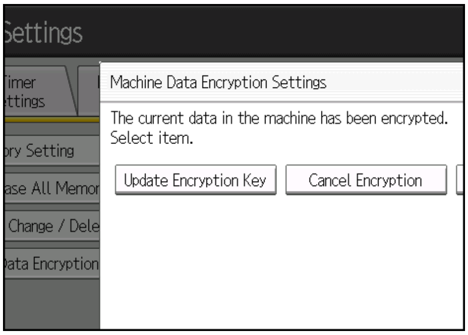
- The encryption key is required for recovery if the machine malfunctions. Be sure to store the encryption key safely for retrieving backup data.
- When the encryption key is updated, encryption is performed using the new key. After completing the procedure on the machine's control panel, turn off the power and restart the machine to enable the new settings. Restarting can be slow when there is data to be carried over to the hard disk.

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

3. **Press [Administrator Tools].**
4. **Press [Machine Data Encryption Settings].**

   If this item is not visible, press [▼Next] to display more settings.

5. **Press [Update Encryption Key].**



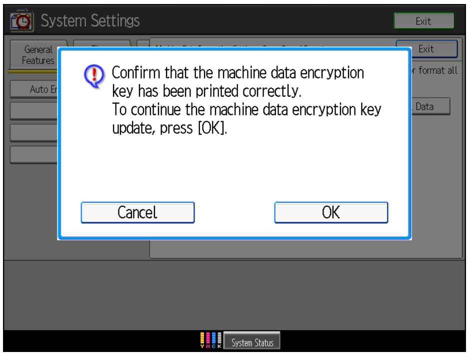
Machine Data Encryption Settings

The current data in the machine has been encrypted.
Select item.

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

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

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



Confirm that the machine data encryption key has been printed correctly.
To continue the machine data encryption key update, press [OK].

9. **Press [Exit].**
10. **Press [Exit].**
11. **Press the [User Tools] key.**
12. **Turn off the power and the main power switch, and then turn the main power switch back on.**

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

Canceling Data Encryption

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

Important

- After completing this procedure on the machine's control panel, turn off the power and restart the machine to enable the new settings. Restarting can be slow when there is data to be carried over to the hard disk.
- Before disposing of a hard disk, note that even if [Format All Data] is selected and encryption is canceled, data stored on the hard disk is not erased.

1. **Press the [User Tools] key.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [Machine Data Encryption Settings].**

   If this item is not visible, press [▼Next] to display more settings.
5. **Press [Cancel Encryption].**
6. **Select the data to be carried over to the hard disk and not be reset.**

   To carry all of the data over to the hard disk, select [All Data]. To carry over only the machine settings data, select [File System Data Only]. To reset all of the data, select [Format All Data].
7. **Press [OK].**
8. **Press [Exit].**
9. **Press [Exit].**
10. **Press the [User Tools] key.**
11. **Turn off the power and the main power switch, and then turn the main power switch back on.**

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

Deleting Data on the Hard Disk

This can be specified by the machine administrator. For details about logging in and logging out with administrator authentication, see p.28 "Logging in Using Administrator Authentication" and p.30 "Logging out Using Administrator Authentication".

Data that will be stored on the hard disk of this machine includes the following: the Address Book data, and code counter data.

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

Conditions for Use

When you use the erase-by-overwrite function, make sure to use it under the following conditions:

Operating Environment

- The machine is used in its normal state (i.e. it is neither damaged, modified nor are there missing components).
- The machine is managed by an administrator who has carefully read and understood this manual, and can ensure the safe and effective use of this machine by general users.

Note

- Customer engineers dispatched from the manufacturer and its affiliated companies are trained in the maintenance of this machine.

Instructions for Use

- Before turning off the main power of the machine, always make sure that the Data Overwrite icon has turned to "Clear".
- If the machine enters Energy Saver mode when overwriting is in progress, press the [Energy Saver] key to revive the display in order to check the icon.
- The machine will not enter Low Power mode or Off mode (Sleep mode) until overwriting has been completed.
- Should the Data Overwrite icon continue to be "Dirty" even after you have made sure that there is no data to be overwritten, turn off the main power of your machine. Turn it on again and see if the icon changes to "Clear". If it does not, contact your sales or service representative.

Auto Erase Memory

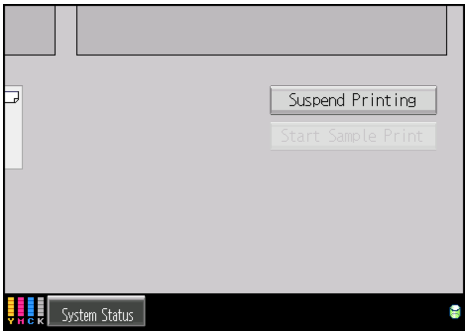
A print data sent from a printer driver is temporarily stored on the machine's hard disk. Even after the job is completed, it remains in the hard disk as temporary data. Auto Erase Memory erases the temporary data on the hard disk by overwriting.

Overwriting starts automatically once the job is completed.

The printer function takes priority over the Auto Erase Memory function. If a print job is in progress, overwriting will only be done once the job is finished.

Overwrite Icon

When Auto Erase Memory is set to [On], the Data Overwrite icon will be indicated in the bottom right hand corner of the panel display of your machine.



🟧	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 has been set to [Off]. If the icon is not displayed even though Auto Erase Memory is [On], contact your service representative.

Methods of Overwriting

You can select a method of overwriting from the following:

- NSA

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

- DoD

  Temporary data is overwritten with a fixed value, the fixed value's complement, and random numbers. When completed, the overwriting 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.

Note

- The default method for overwriting is "Random Numbers", and the default number of overwrites is 3.
- NSA stands for "National Security Agency", U.S.A.
- DoD stands for "Department of Defense", U.S.A.

Using Auto Erase Memory

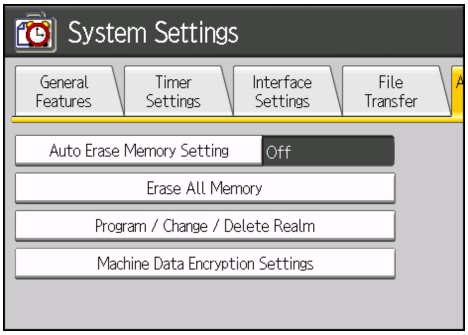
Important

- When Auto Erase Memory is set to [On], temporary data that remained on the hard disk when Auto Erase Memory was set to [Off] might not be overwritten.
- 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 on, and then repeat from step 1.

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

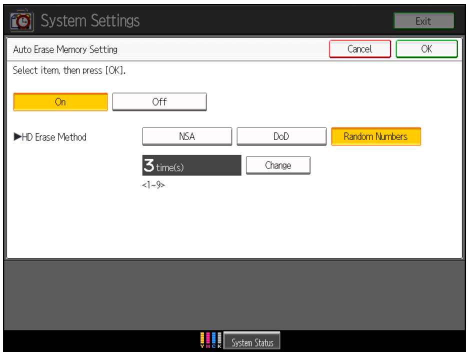
   If this item is not visible, press [▼Next] to display more settings.

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



5. **Press [On].**

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



Select item, then press [OK].

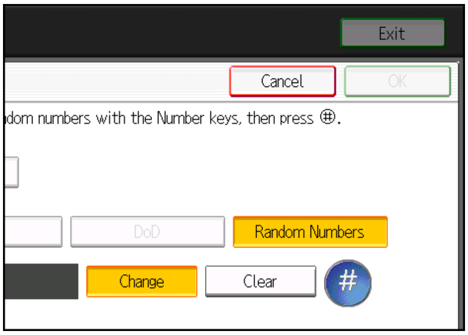
If you select [NSA] or [DoD], proceed to step 9.

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

For details about the methods of overwriting, see p.79 "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].**

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

Note

- If you specify to both overwrite and encrypt the data, the data will all be encrypted.

Canceling Auto Erase Memory

1. **Follow steps 1 to 4 in "Using Auto Erase Memory".**
2. **Press [Off].**
3. **Press [OK].**
4. **Press [Exit].**
5. **Press the [User Tools] key.**

Note

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

Types of Data that Can or Cannot Be Overwritten

The following are 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

  Data stored in the Address Book can be encrypted for security. For details, see p.67 "Protecting the Address Book".

- Counters stored under each user code

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

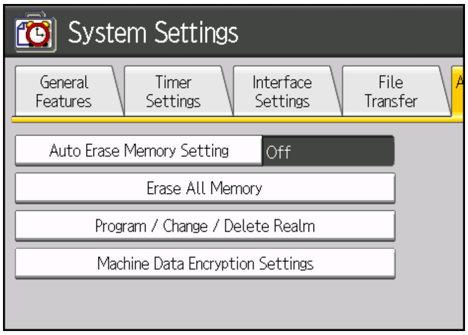
- Document data stored using the printer function will not be erased by Auto Erase Memory.
- If you select "Erase All Memory", you can delete the following: user codes, counters under each user code, data stored in the Address Book, and the machine's network settings.

- 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 up to two and a half 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

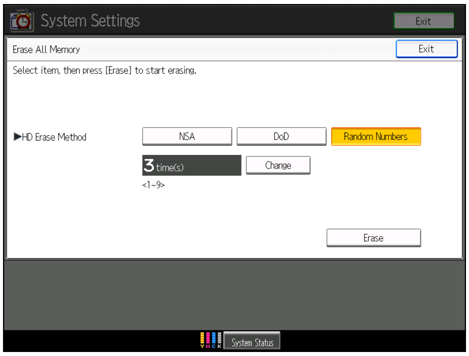
1. **Disconnect communication cables connected to the machine.**
2. **Press the [User Tools] key.**
3. **Press [System Settings].**
4. **Press [Administrator Tools].**

   If this item is not visible, press [▼Next] to display more settings.
5. **Press [Erase All Memory].**



Auto Erase Memory Setting Off

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



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

▶HD Erase Method Random Numbers

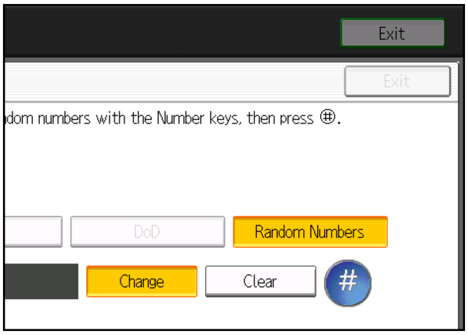
3 time(s) <1~9>

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

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

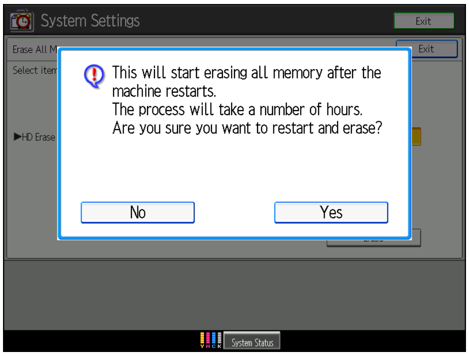
For details about the methods of overwriting, see p.79 "Methods of Overwriting".

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?

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

Before turning the power off, see "Turning On 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 on again, and then repeat from step 2.
- If you specify to both overwrite and encrypt the data, the data will all be encrypted.

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].**
3. **Turn off the main power.**

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

Note

- To resume overwriting, turn on the main power.

5. Managing Access to the Machine

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

Preventing Changes to Machine Settings

The administrator type determines which machine settings can be modified. Users cannot change the administrator settings. In "Available Settings" under "Administrator Authentication Management", the administrator can select which settings users cannot specify. For details about the administrator roles, see p.21 "Administrators".

Register the administrators before using the machine. For instructions on registering the administrator, see p.26 "Registering the Administrator".

Type of Administrator

Register the administrator on the machine, and then authenticate the administrator using the administrator's login user name and password. The administrator can also specify [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

  For a list of settings that the user administrator can specify, see p.189 "User Administrator Settings".

- Machine Administrator

  For a list of settings that the machine administrator can specify, see p.191 "Machine Administrator Settings".

- Network Administrator

  For a list of settings that the network administrator can specify, see p.196 "Network Administrator Settings".

- File Administrator

  For a list of settings that the file administrator can specify, see p.199 "File Administrator Settings".

Limiting Available Functions

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

Available Functions

Printer

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

Note

- Printer job authentication is possible only if user code authentication is enabled. For details, see p.37 "User Code Authentication".

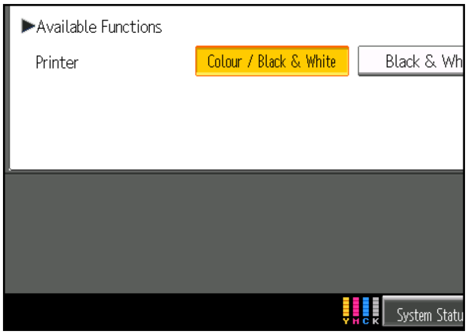
Specifying Which Functions are Available

This can be specified by the user administrator. For details about logging in and logging out with administrator authentication, see p.28 "Logging in Using Administrator Authentication" and p.30 "Logging out Using Administrator Authentication".

Specify which functions will be available to users registered in the Address Book when they log in to the machine.

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.**



▶Available Functions

Printer

If this item is not visible, press [▼Next] to display more settings.

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

Managing Log Files

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

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

The logs can be viewed using Web Image Monitor. Collected logs can be downloaded all at once from Web Image Monitor as CSV files. You cannot directly read the log files on the hard disk.

Log types

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

- Job Log

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

- Access Log

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

Note

- The log of jobs printed by the printer function cannot be collected.

Using Web Image Monitor to Manage Log Files

This can be specified by the machine administrator.

Using Web Image Monitor, you can carry out the following log-related operations:

- Specifying the types of log to store in the machine and the log collection level
- Encrypting log files
- Batch deleting log files
- Downloading log files

Specifying log collect settings

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

Job Log Collect Level

Level 1

User Settings

Access Log Collect Level

Level 1

Level 2

User Settings

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

   The machine administrator can log in.

   Enter the login user name and login password.
4. **Click [Configuration], and then click [Logs] under "Device Settings".**
5. **To specify the Job Log settings, set "Collect Job Logs" to "Active"; to specify the Access Log settings, set "Collect Access Logs" to "Active".**
6. **Specify the recording levels for either "Job Log Collect Level" or "Access Log Collect Level".**

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

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

Note

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

Specifying log encryption

Use the following procedure to enable/disable log encryption.

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

   The machine administrator can log in.

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

5. **Select [Active] under "Encrypt Logs".**

   To disable log encryption, select [Inactive].

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

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

Note

- In order to enable encryption, either "Collect Job Logs" or "Collect Access Logs", or both must be set to [Active].
- If the data stored in the machine has been encrypted, the log files will still be encrypted, regardless of this setting.

Deleting all logs

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

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

   The machine administrator can log in.

   Enter the login user name and login password.

4. **Click [Configuration], and then click [Logs] under "Device Settings".**
5. **Click [Delete] under "Delete All Logs".**
6. **Click [OK].**
7. **Click [OK].**
8. **Click [Logout].**

Note

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

Downloading logs

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

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

3. **Click [Login].**

   The machine administrator can log in.

   Enter the login user name and login password.

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

Note

- Downloaded logs contain data recorded up till the time you click the [Download] button. Any logs recorded after the [Download] button is clicked will not be downloaded. The "Result" field of the log entry for uncompleted jobs will be blank.
- Download time may vary depending on the number of logs.
- If an error occurs while the CSV file is downloading or being created, the download is canceled and details of the error are included at the end of the file.
- If a log is downloaded successfully, "Download completed." will appear in the last line of the log file.
- For details about saving CSV log files, see your browser's Help.
- Downloaded log files use UTF-8 character encoding. To view a log file, open it using an application that supports UTF-8.
- To collect logs, set "Collect Job Logs" and "Collect Access Logs" to [Active]. This setting can be specified in [Logs] under [Configuration] in Web Image Monitor.
- For details about the items contained in the logs, see p.99 "Attributes of logs you can download".

Note concerning downloading logs

When the number of stored logs reaches the maximum, the oldest logs will be overwritten by newer logs. This applies to both job and access logs and occurs regardless of whether or not the logs have been downloaded.

Overwritten old logs will not be included in downloaded log files.

For this reason, we recommend you take note of the information in the table below and perform regular log management using Web Image Monitor.

Maximum number of logs that can be stored in the machine

Job logs	Access logs
2,000	6,000

Estimated number of logs created per day

Job logs	Access logs
100 (100 logs per day)	300 This figure is based on 100 operations such as initialization and access operations over the Web and 200 access log entries (two entries per job: one login and one logout).

If the daily estimates are not exceeded, the machine can store logs for 20 days without having to overwrite older logs. However, we recommend that you download the logs every 10 days. This will prevent unwanted overwriting and ensure all logs are preserved, even if the daily estimate is exceeded.

It is the responsibility of the machine administrator to deal downloaded log files appropriately.

Note

- If you change the [Collect] / [Do not Collect] setting for log collection, you must perform a batch deletion of the logs.
- After downloading the logs, perform a batch deletion of the logs.
- During log downloads, do not perform operations that will create log entries, as logs that are in the process of downloading cannot be updated with new entries.
- Logs can be batch deleted via Web Image Monitor.

Notes on operation when the number of log entries reaches maximum

The machine reads the number of access and job logs and begins overwriting the oldest log entries to make space for the new logs as they arrive.

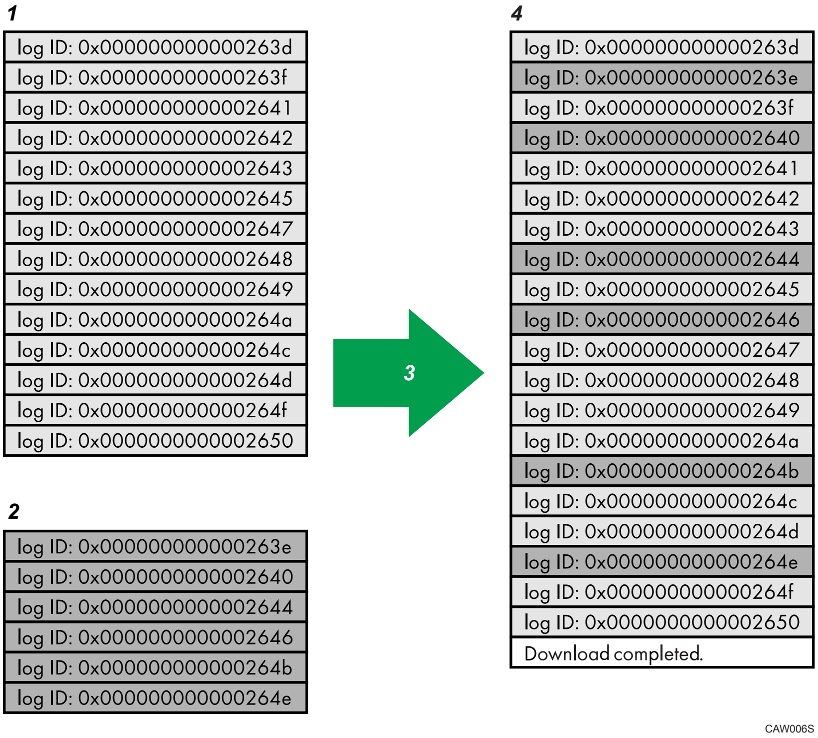
Downloaded log files include both access and job logs, with some log entries incomplete.

The following illustration shows an example in which logs are downloaded during access log overwriting.

In this example, some of the access log entries are incomplete.

Logs are overwritten in reverse priority order, meaning logs of lowest priority are overwritten first and logs of highest priority are overwritten last. This way, if the overwrite is canceled, there is a chance that logs of higher priority will still be available.

If logs are downloaded without overwriting



1

```
log ID: 0x000000000000263d
log ID: 0x000000000000263f
log ID: 0x0000000000002641
log ID: 0x0000000000002642
log ID: 0x0000000000002643
log ID: 0x0000000000002645
log ID: 0x0000000000002647
log ID: 0x0000000000002648
log ID: 0x0000000000002649
log ID: 0x000000000000264a
log ID: 0x000000000000264c
log ID: 0x000000000000264d
log ID: 0x000000000000264f
log ID: 0x0000000000002650
```

2

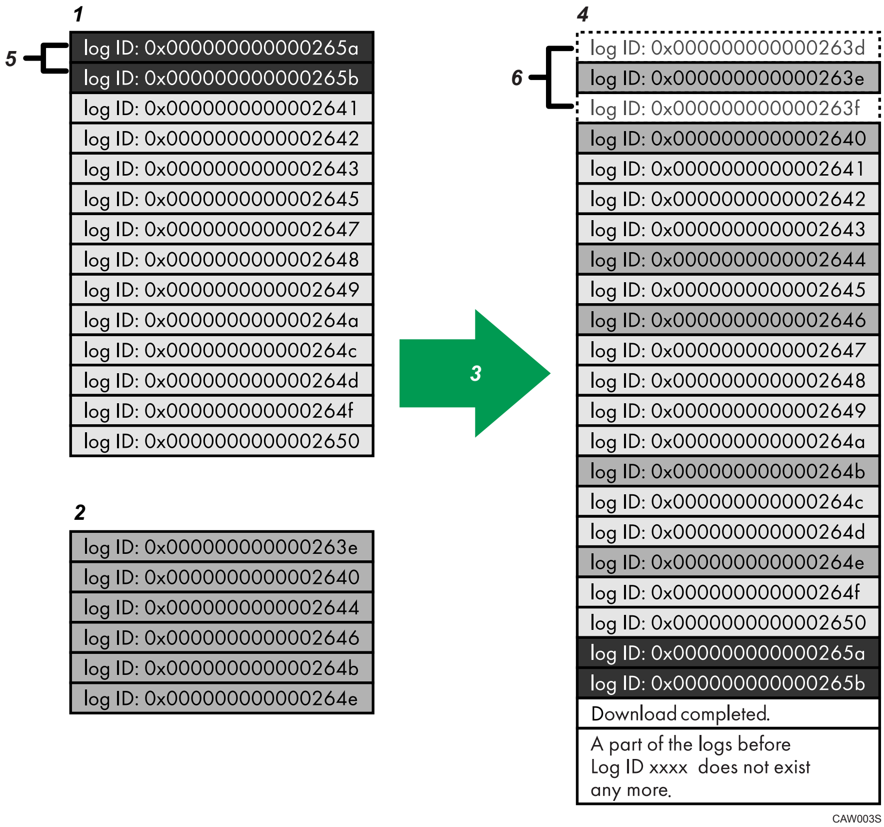
```
log ID: 0x000000000000263e
log ID: 0x0000000000002640
log ID: 0x0000000000002644
log ID: 0x0000000000002646
log ID: 0x000000000000264b
log ID: 0x000000000000264e
```

4

```
log ID: 0x000000000000263d
log ID: 0x000000000000263e
log ID: 0x000000000000263f
log ID: 0x0000000000002640
log ID: 0x0000000000002641
log ID: 0x0000000000002642
log ID: 0x0000000000002643
log ID: 0x0000000000002644
log ID: 0x0000000000002645
log ID: 0x0000000000002646
log ID: 0x0000000000002647
log ID: 0x0000000000002648
log ID: 0x0000000000002649
log ID: 0x000000000000264a
log ID: 0x000000000000264b
log ID: 0x000000000000264c
log ID: 0x000000000000264d
log ID: 0x000000000000264e
log ID: 0x000000000000264f
log ID: 0x0000000000002650
Download completed.
```

1. **Access log**
2. **Job log**
3. **Download**
4. **Downloaded logs**

If logs are downloaded during overwriting



```
log ID: 0x000000000000265a
log ID: 0x000000000000265b
log ID: 0x0000000000002641
log ID: 0x0000000000002642
log ID: 0x0000000000002643
log ID: 0x0000000000002645
log ID: 0x0000000000002647
log ID: 0x0000000000002648
log ID: 0x0000000000002649
log ID: 0x000000000000264a
log ID: 0x000000000000264c
log ID: 0x000000000000264d
log ID: 0x000000000000264f
log ID: 0x0000000000002650
```

```
log ID: 0x000000000000263e
log ID: 0x0000000000002640
log ID: 0x0000000000002644
log ID: 0x0000000000002646
log ID: 0x000000000000264b
log ID: 0x000000000000264e
```

```
log ID: 0x000000000000263d
log ID: 0x000000000000263e
log ID: 0x000000000000263f
log ID: 0x0000000000002640
log ID: 0x0000000000002641
log ID: 0x0000000000002642
log ID: 0x0000000000002643
log ID: 0x0000000000002644
log ID: 0x0000000000002645
log ID: 0x0000000000002646
log ID: 0x0000000000002647
log ID: 0x0000000000002648
log ID: 0x0000000000002649
log ID: 0x000000000000264a
log ID: 0x000000000000264b
log ID: 0x000000000000264c
log ID: 0x000000000000264d
log ID: 0x000000000000264e
log ID: 0x000000000000264f
log ID: 0x0000000000002650
log ID: 0x000000000000265a
log ID: 0x000000000000265b
Download completed.
A part of the logs before
Log ID xxxx  does not exist
any more.
```

1. **Access log**
2. **Job log**
3. **Download**
4. **Downloaded logs**
5. **Overwriting**
6. **Deleted by overwriting**

To determine whether or not overwriting occurred while the logs were downloading, check the message in the last line of the downloaded logs.

- If overwriting did not occur, the last line will contain the following message: Download completed.
- If overwriting did occur, the last line will contain the following message: Download completed. A part of the logs before Log ID xxxx does not exist any more.

Note

- Examine logs following "Log ID xxxx".

Logs That Can Be Managed Using Web Image Monitor

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

Logs that can be collected

The following tables explain the items in the job log and access log that the machine creates when you enable log collection using Web Image Monitor. If you require log collection, use Web Image Monitor to configure it. This setting can be specified in [Logs] under [Configuration] in Web Image Monitor.

Only the settings shown in the following table are available on the machine.

Job log information items

Job Log Item	Log Type Attribute	Content
Report Printing	Report Printing	Details of reports printed from the control panel.

Access log information items

Access Log Item	Log Type Attribute	Content
Login	Login	Times of login and identity of logged in users.
Logout	Logout	Times of logout and identity of logged out users.
HDD Format	HDD Format	Details of hard disk formatting.
All Logs Deletion	All Logs Deletion	Details of deletions of all logs.
Log Setting Change	Log Setting Change	Details of changes made to log settings.
Log Collection Item Change	Log Collection Item Change	Details of changes to job log collection levels, access log collection levels, and types of logs collected.
Collect Encrypted Communication Logs	Collect Encrypted Communication Logs	Details of encrypted communication with the utility software, Web Image Monitor, or external devices.
Access Violation	Access Violation	Details of failed access attempts.
Lockout	Lockout	Details of lockout activation.

Access Log Item	Log Type Attribute	Content
Firmware: Update	Firmware: Update	Details of firmware updates.
Firmware: Structure Change	Firmware: Structure Change	Details of structure changes that occurred when an SD card was inserted or removed, or when an unsupported SD card was inserted.
Firmware: Structure	Firmware: Structure	Details of checks for changes to firmware module structure made at times such as when the machine was switched on.
Machine Data Encryption Key Change	Machine Data Encryption Key Change	Details of changes made to encryption keys using the Machine Data Encryption setting.
Firmware: Invalid	Firmware: Invalid	Details of checks for firmware validity made at times such as when the machine was switched on.
Date/Time Change	Date/Time Change	Details of changes made to date and time settings.
Password Change	Password Change	Details of changes made to the login password.
Administrator Change	Administrator Change	Details of changes of administrator.
Address Book Change	Address Book Change	Details of changes made to Address Book entries.

There is no "Login" log made for SNMPv3.

If the hard disk is formatted, all the log entries up to the format are deleted and a log entry indicating the completion of the format is made.

"Access Violation" indicates the system has experienced frequent remote DoS attacks involving logon attempts through user authentication.

Note

- If "Job Log Collect Level" is set to "Level 1", all job logs are collected.
- If "Access Log Collect Level" is set to "Level 1", the following information items are recorded in the access log:
    - HDD Format
    - All Logs Deletion
    - Log Setting Change

- Log Collection Item Change

- If "Access Log Collect Level" is set to "Level 2", all access logs are collected.
- The first log made following power on is the "Firmware: Structure" log.

Attributes of logs you can download

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

Note that a blank field indicates an item is not featured in a log.

File output format

- Character Code Set: UTF-8
- Output Format: CSV (Comma-Separated Values)
- File Name: "Device Name + _log.csv"

Order of log entries

Log entries are printed in ascending order according to Log ID.

File structure

The data title is printed in the first line (header line) of the file.

The difference between the output format of access log and job log

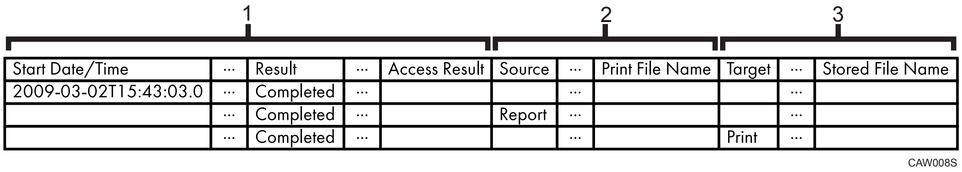
The output format of the access log and job log are different.

- Access log

  Items in the list and access log entries appear on separate lines.

- Job log

  Multiple lines appear in the order of All, Source (job input data), and Target (job output data). The same log ID is assigned to all lines corresponding to a single job log entry.


1
2
3
CAW008S

Start Date/Time	…	Result	…	Access Result	Source	…	Print File Name	Target	…	Stored File Name
2009-03-02T15:43:03.0	…	Completed	…			…			…	
	…	Completed	…		Report	…			…	
	…	Completed	…			…		Print	…	

1. **All**

   Each item in the list is displayed on a separate line.

2. **Source**

   Displays details of the job log entry and the "Result" and "Status" of each item.

   If there are multiple sources, multiple lines are displayed.

3. **Target**

   Displays details of the job log entry and the "Result" and "Status" of each item.

If there are multiple targets, multiple lines are displayed.

Job and access log information items

Item	Content
Start Date/Time	For a job log entry, indicates the start date and time of the operation. If the job has not been completed, this is blank. For an access log entry, indicates the same date and time as shown by "End Date/Time". This is in Item 1 of the CSV file.
End Date/Time	For a job log entry, indicates the end date and time of the operation. If the operation is still in progress, this will be blank. For an access log entry, indicates the same date and time as shown by "Result". This is Item 2 of the CSV file.
Log Type	Details of the log type. Access logs are classified under "Access Log Type". For details about the information items contained in each type of log, see p.97 "Logs that can be collected". This is Item 3 of the CSV file.
Result	Indicates the result of an operation or event: • If "Succeeded" is displayed for a job log entry, the operation completed successfully; "Failed" indicates the operation was unsuccessful. If the operation is still in progress, this will be blank. • If "Succeeded" is displayed for an access log entry, the event completed successfully; "Failed" indicates the event was unsuccessful.

Item	Content
Status	Indicates the status of an operation or event: • If "Completed" is displayed for a job log entry, the operation completed successfully; "Failed" indicates the operation was unsuccessful; "Processing" indicates the operation is still in progress. • If "Completed" is displayed for "Source" or "Target" in a job log entry, the operation completed successfully; "Failed" indicates the operation was unsuccessful; "Processing" indicates the operation is still in progress; "Error" indicates an error occurred; "Suspended" indicates the operation is currently suspended. • If "Succeeded" is displayed for an access log entry, the operation completed successfully; if any of the following are displayed, the operation was unsuccessful: "Password Mismatch", "User Not Programmed", "Other Failures", "User Locked Out", "File Password Mismatch", "No Privileges", "Failed to Access File", "Communication Failure", or "Communication Result Unknown".

Item	Content
User Entry ID	Indicates the user's entry ID. This is a hexadecimal ID that identifies users who performed job or access log-related operations: For supervisors, only "0xffffff86" is available; for administrators, "0xffffff87", "0xffffff88", "0xffffff89", and "0xffffff8a" are available. For general users, any value between "0x00000001" and "0xfffffeff" is available. "0x00000000", "0xffffff80", and "0xffffff81" indicate system operations related to user authentication. IDs "0xffffff80" and "0xffffff81" indicate system operations related to the Address Book; "0x00000000" indicates other operations. "0xffffff80" indicates operations related to changing their access permissions. Displays Address Book updates when Auto registration of users is enabled through Windows authentication, LDAP authentication, or another authentication system. "0x00000000" and "0xffffff81" indicate operations that do not require user authentication and that were performed by non-authenticated users. ID "0xffffff81" indicates operations related to the Address Book and job logs; "0x00000000" indicates other operations.
User Code/User Name	Identifies the user code or user name of the user who performed the operation. If an administrator performed the operation, this ID will contain the login name of that administrator.
Log ID	Identifies the ID that is assigned to the log. This is a hexadecimal ID that identifies the log.

Access log information items

Item	Content
Access Log Type	Indicates the type of access: "Authentication" indicates a user authentication access. "System" indicates a system access. "Network Attack Detection/Encrypted Communication" indicates a network attack or encrypted communication access. "Firmware" indicates a firmware verification access. "Address Book" indicates an Address Book access.
Authentication Server Name	Indicates the name of the server where authentication was last attempted.
No. of Authentication Server Switches	Indicates the number of times server switching occurred when the authentication server was unavailable. You can determine whether or not authentication server availability is detected. The number of server switches is indicated as 0 to 4. A value of 0 indicates the authentication server is available.
Logout Mode	Mode of logout. The remark "by User's Operation" indicates manual logout by the user; "by Auto Logout Timer" indicates automatic logout following a timeout.
Login Method	Identifies the method of login (authorization): "Control Panel" indicates the login was performed through the control panel; "via Network" indicates the login was performed remotely through a network computer; and "Others" indicates the login was performed through another method.

Item	Content
Login User Type	Indicates the type of login user: "User" indicates the logged in user was a registered general user. "Guest" indicates the logged in user was a guest user. "User Administrator" indicates the logged in user was a registered user administrator. "File Administrator" indicates the logged in user was a registered file administrator. "Machine Administrator" indicates the logged in user was a registered machine administrator. "Network Administrator" indicates the logged in user was a registered network administrator. "Supervisor" indicates the logged in user was a registered supervisor. "Custom Engineer (Service Mode)" indicates the logged in user was a customer engineer. "Others" indicates the logged in user did not belong to any of the above types of user.
Target User Entry ID	Indicates the entry ID of the target user is. This is a hexadecimal ID that indicates users to whom the following settings are applied: • Lockout • Password Change
Target User Code/User Name	User code or user name of the user whose data was accessed. If the administrator's data was accessed, the administrator's user name is logged.
Lockout/Release	The mode of operation access. "Lockout" indicates activation of password lockout; "Release" indicates deactivation of password lockout.
Lockout/Release Method	"Manual" is recorded if the machine is unlocked manually. "Auto" is recorded if the machine is unlocked by the lockout release timer.

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

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

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

Item	Content
Parts Number	Firmware module part number.
Version	Firmware version.
Machine Data Encryption Key Operation	Indicates the type of encryption key operation performed: "Back Up Machine Data Encryption Key" indicates an encryption key backup was performed. "Restore Machine Data Encryption Key" indicates an encryption key was restored. "Clear NVRAM" indicates the NVRAM was cleared. "Start Updating Machine Data Encryption Key" indicates an encryption key update was started. "Finish Updating Machine Data Encryption Key" indicates an encryption key update was finished.
Machine Data Encryption Key Type	Identifies the type of the encryption key as "Encryption Key for Hard Disk", "Encryption Key for NVRAM", or "Device Certificate".
Validity Error File Name	Indicates the name of the file in which a validity error was detected.
Access Result	Indicates the results of logged operations: "Completed" indicates an operation completed successfully; "Failed" indicates an operation completed unsuccessfully.

Job log information items

Input information

Item	Content
Source	Indicates the source of the job file: "Report" indicates the job file was a printed report.

Output information

Item	Content
Target	Type of the job target. "Print" indicates a print file.

Item	Content
Start Date/Time	Dates and times "Print" operations started. This is Item 58 of the CSV file.
End Date/Time	Dates and times "Print" operations ended. This is Item 59 of the CSV file.

Note

- Only the settings shown in the table are available on the machine.

6. Enhanced Network Security

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

Preventing Unauthorized Access

You can limit IP addresses, disable ports and protocols, or use Web Image Monitor to specify the network security level to prevent unauthorized access over the network and protect the Address Book, 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, SSH/SFTP, Bonjour, SMB, 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.**
3. **Click [Login].**

   The machine administrator can log in.

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

Enabling and Disabling Protocols

This can be specified by the network administrator. For details about logging in and logging out with administrator authentication, see p.28 "Logging in Using Administrator Authentication" and p.30 "Logging out Using Administrator Authentication".

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

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

Protocol	Port	Setting Method	When Disabled
ssh/sftp	TCP: 22	• Web Image Monitor • telnet	Functions that require sftp cannot be used. You can restrict personal information from being displayed by making settings on the control panel using "Restrict Display of User Information".
telnet	TCP: 23	• Web Image Monitor	Commands using telnet are disabled.
SMTP	TCP: 25 (variable)	• Control Panel • Web Image Monitor	E-mail notification function 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 cannot be used. You can also make settings to require SSL transmission using the control panel or Web Image Monitor.
SMB	TCP: 139	• Control Panel • Web Image Monitor • telnet	SMB printing functions cannot be used.
NBT	UDP: 137 UDP: 138	• telnet	SMB printing functions via TCP/IP, as well as NetBIOS designated functions on the WINS server cannot be used.

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

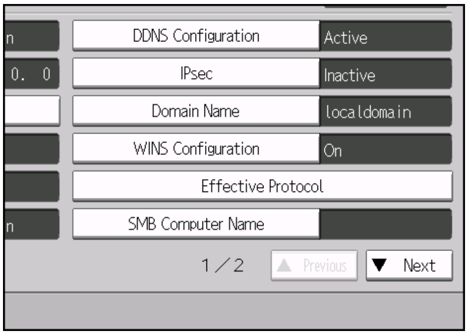
Protocol	Port	Setting Method	When Disabled
RFU	TCP: 10021	• telnet	You can attempt to update firmware via FTP.

Note

- "Restrict Display of User Information" is one of the Extended Security features. For details about making this setting, see p.155 "Specifying the Extended Security Functions".

Enabling and Disabling Protocols Using the Control Panel

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



DDNS Configuration Active

IPsec Inactive

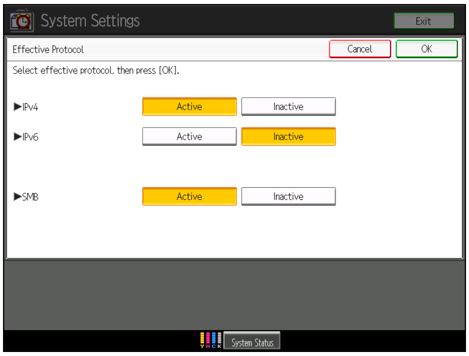
Domain Name localdomain

WINS Configuration On

Effective Protocol

SMB Computer Name

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



System Settings

Effective Protocol

Select effective protocol, then press [OK].

▶IPv4 Active [✓] Inactive

▶IPv6 Active Inactive [✓]

▶SMB Active [✓] Inactive

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

Enabling and Disabling Protocols Using Web Image Monitor

1. **Open a Web browser.**
2. **Enter "http://(the machine's IP address or host name)/" in the address bar.**
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".**
5. **Set the desired protocols to active/inactive (or open/close).**
6. **Click [OK].**
7. **Click [OK].**
8. **Click [Logout].**

Specifying Network Security Level

This can be specified by the network administrator. For details about logging in and logging out with administrator authentication, see p.28 "Logging in Using Administrator Authentication" and p.30 "Logging out Using Administrator Authentication".

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.

Network Security Levels

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

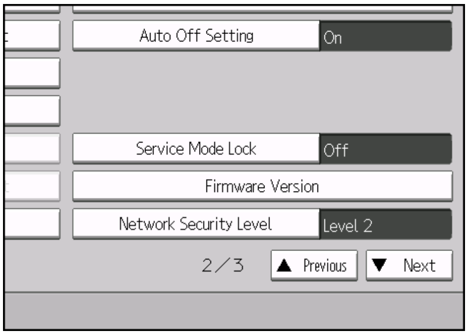
Security Level	Description
[Level 0]	Select [Level 0] to use all features. Use this setting when you have no information that needs to be protected from external threats.
[Level 1]	Select [Level 1] for moderate security to protect important information. Use this setting if the machine is connected to a local area network (LAN).
[Level 2]	Select [Level 2] for maximum security to protect confidential information. Use this setting when it is necessary to protect information from external threats.

Specifying Network Security Level Using the Control Panel

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

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

4. **Press [Network Security Level].**



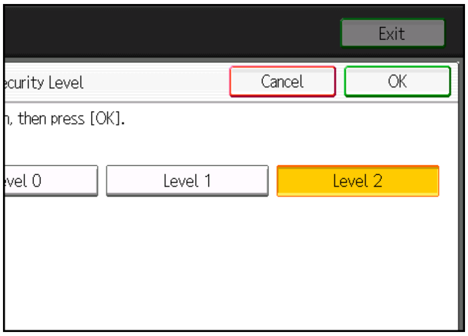
Auto Off Setting On

Service Mode Lock Off

Network Security Level Level 2

If this item is not visible, press [▼Next] to display more settings.

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



curity Level

n, then press [OK].

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

6. **Press [OK].**

7. **Press [Exit].**

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

Specifying Network Security Level Using Web Image Monitor

1. **Open a Web browser.**

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

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".**

5. **Select the network security level in "Security Level".**

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

Status of Functions under Each Network Security Level

Tab Name: TCP/IP*1

Function	Level 0	Level 1	Level 2
TCP/IP*2	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
SSL/TLS version>SSL2.0*2	Active	Active	Active
SSL/TLS version>SSL3.0*2	Active	Active	Active
SSL/TLS version>TLS*2	Active	Active	Active
Encryption Strength Setting>AES*2	Active	Active	Active
Encryption Strength Setting>3DES*2	Active	Active	Active
Encryption Strength Setting>DES*2	Active	Active	Active
Encryption Strength Setting>RC4	Active	Active	Active
Encryption Strength Setting>RC2*2	Active	Active	Active
FTP	Active	Active	Active
sftp	Active	Active	Active
ssh	Active	Active	Active
RSH/RCP	Active	Active	Inactive
TELNET	Active	Inactive	Inactive
Bonjour	Active	Active	Inactive
SSDP	Active	Active	Inactive

Function	Level 0	Level 1	Level 2
SMB	Active	Active	Inactive
NetBIOS over TCP/IPv4	Active	Active	Inactive

The same settings are applied to IPv4 and IPv6.

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

*1 The same settings are applied to IPv4 and IPv6.

*2 This setting is not governed by the security level. Manually specify whether to activate or inactivate this setting.

Protection Using Encryption

Establish encrypted transmission on this machine using SSL, SNMPv3, and IPsec. By encrypting transmitted data and safeguarding the transmission route, you can prevent sent data from being intercepted, analyzed, and tampered with.

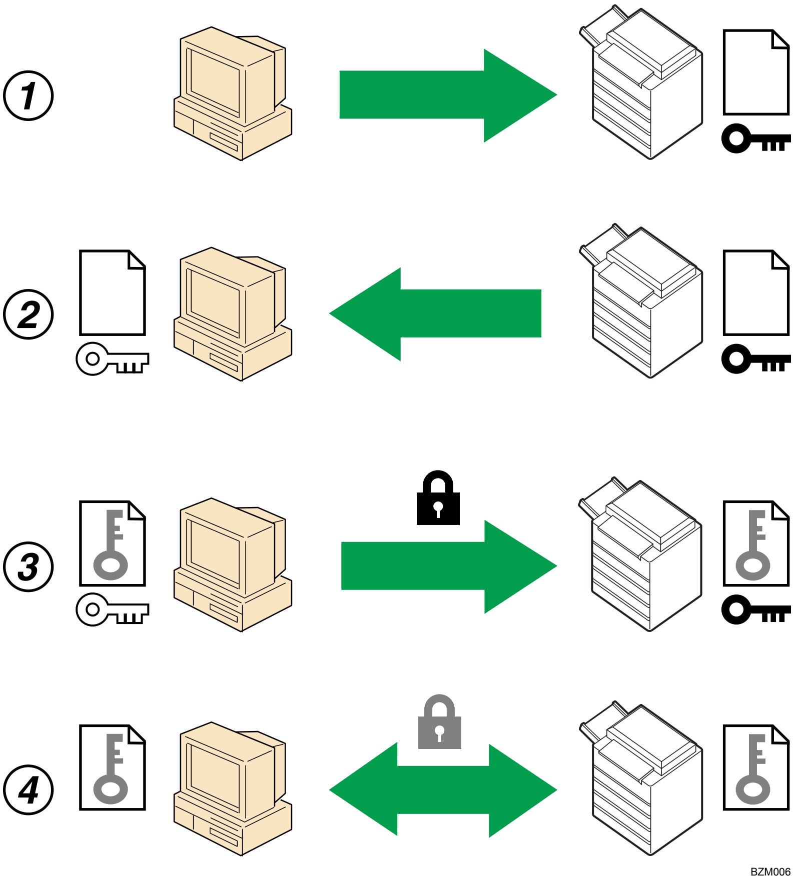
SSL (Secure Sockets Layer) Encryption

This can be specified by the network administrator.

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

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

SSL (Secure Sockets Layer)



1. **To access the machine from a user's computer, request the SSL device certificate and public key.**

2. **The device certificate and public key are sent from the machine to the user's computer.**
3. **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.

Use this procedure to create a self-signed device certificate.

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

   If a security warning dialog box appears, read the message, and then click [OK].

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

Note

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

Creating the Device Certificate (Issued by a Certificate Authority)

Create the device certificate using Web Image Monitor.

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

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

   "Requesting" appears under "Certificate Status".
10. **Click [OK].**
11. **Click [Logout].**

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

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

    For the application, click Web 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 (Issued by a Certificate Authority)

Install the device certificate using Web Image Monitor.

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

1. **Open a Web browser.**
2. **Enter "http://(the machine's IP address or host name)/" in the address bar.**
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".**
5. **Click [Certificate1].**
6. **Click [Install].**
7. **Enter the contents of the device certificate.**

    In the certificate box, enter the details of the device certificate issued by the certificate authority.

    For details about the displayed items and selectable items, see Web Image Monitor Help.
8. **Click [OK].**
9. **Wait a moment for the device to restart, and then click [OK].**

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

After installing the device certificate in the machine, enable the SSL/TLS 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.**
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".**
5. **Click [Active] for the protocol version used in "SSL/TLS".**
6. **Select the encryption communication mode for "Permit SSL/TLS Communication".**
7. **If you want to disable a protocol, click [Inactive] next to "SSL2.0", "SSL3.0", or "TLS".**

   Note that if you have selected [Active] in step 5, at least one of these protocols must be enabled.
8. **In "Encryption Strength Setting", select the encryption strength (key length) for AES, 3DES, DES, RC4, and RC2.**

   You must specify at least one encryption standard by selecting at least one key length.

   Depending on whether "SSL2.0", "SSL3.0", and "TLS" is set to "Active" or "Inactive", the items you can check vary.
9. **Click [OK].**
10. **Click [OK].**
11. **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.
- The TLS version is 1.0.

- If you set [Permit SSL/TLS Communication] to [Ciphertext Only], communication will not be possible if you select a protocol that does not support a Web browser, or specify an encryption strength setting only. If this is the case, enable communication by setting [Permit SSL / TLS Communication] to [Ciphertext / Cleartext] using the machine's control panel, and then specify the correct protocol and encryption strength.
- The SSL/TLS version and encryption strength settings can be changed, even under [Network Security].
- Depending on the states you specify for "SSL2.0", "SSL3.0", and "TLS", the machine might not be able to connect to an external LDAP server.
- Communication via @Remote and Integration Server authentication is always encrypted by SSL 3.0.

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.

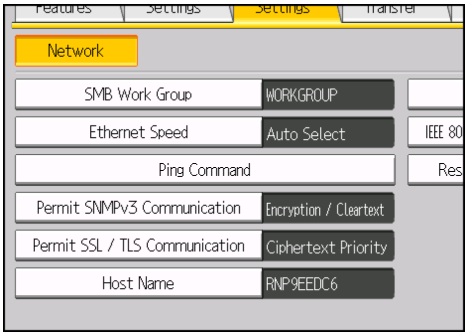
Ciphertext Priority	Performs encrypted communication if encryption is possible. If encryption is not possible, the machine communicates without it.
Ciphertext/Cleartext	Communicates with or without encryption, according to the setting.

Specifying the SSL/TLS Encryption Mode

This can be specified by the network administrator. For details about logging in and logging out with administrator authentication, see p.28 "Logging in Using Administrator Authentication" and p.30 "Logging out Using Administrator Authentication".

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

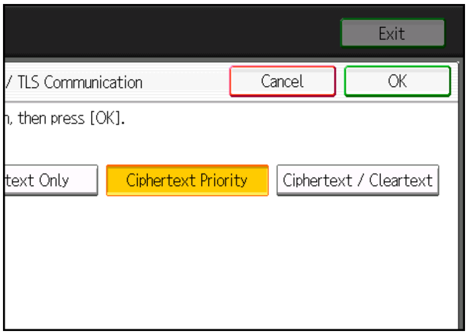
1. **Press the [User Tools] key.**
2. **Press [System Settings].**
3. **Press [Interface Settings].**
4. **Press [Permit SSL / TLS Communication].**



SMB Work Group WORKGROUP
Ethernet Speed Auto Select
Ping Command
Permit SNMPv3 Communication Encryption / Cleartext
Permit SSL / TLS Communication Ciphertext Priority
Host Name RNP9EEDC6

If this item is not visible, press [▼Next] to display more 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.

SNMPv3 Encryption

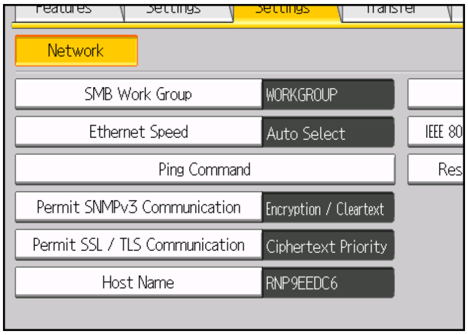
This can be specified by the network administrator. For details about logging in and logging out with administrator authentication, see p.28 "Logging in Using Administrator Authentication" and p.30 "Logging out Using Administrator Authentication".

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.

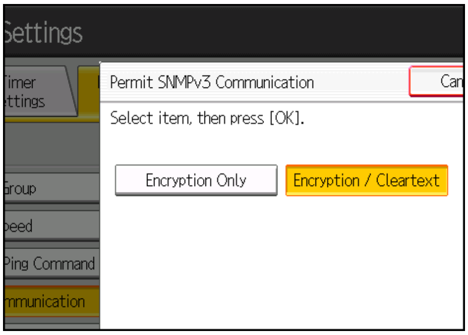
1. **Press the [User Tools] key.**
2. **Press [System Settings].**
3. **Press [Interface Settings].**

4. **Press [Permit SNMPv3 Communication].**



If this item is not visible, press [▼Next] to display more settings.

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



6. **Press [OK].**

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

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 p.26 "Registering the Administrator".

Transmission Using IPsec

This can be specified by the network administrator.

For communication security, this machine supports IPsec. IPsec transmits secure data packets at the IP protocol level using the shared key encryption method, where both the sender and receiver retain the same key. This machine has two methods that you can use to specify the shared encryption key for both parties: encryption key auto exchange and encryption key manual settings. Using the auto exchange setting, you can renew the shared key exchange settings within a specified validity period, and achieve higher transmission security.

Important

- When "Inactive" is specified for "Exclude HTTPS Communication", access to Web Image Monitor can be lost if the key settings are improperly configured. In order to prevent this, you can specify IPsec to exclude HTTPS transmission by selecting "Active". When you want to include HTTPS transmission, we recommend that you select "Inactive" for "Exclude HTTPS Communication" after confirming that IPsec is properly configured. When "Active" is selected for "Exclude HTTPS Communication", even though HTTPS transmission is not targeted by IPsec, Web Image Monitor might become unusable when TCP is targeted by IPsec from the computer side. If you cannot access Web Image Monitor due to IPsec configuration problems, disable IPsec in System Settings on the control panel, and then access Web Image Monitor. For details about enabling and disabling IPsec using the control panel, see "System Settings", Network and System Settings Reference.
- IPsec is not applied to data obtained through DHCP, DNS, or WINS.
- IPsec compatible operating systems are Windows XP SP2, Windows Vista/7, Windows Server 2003/2003 R2/2008/2008 R2, Mac OS X 10.4 and later, RedHat Linux Enterprise WS 4.0, and Solaris 10. However, some setting items are not supported depending on the operating system. Make sure the IPsec settings you specify are consistent with the operating system's IPsec settings.

Encryption and Authentication by IPsec

IPsec consists of two main functions: the encryption function, which ensures the confidentiality of data, and the authentication function, which verifies the sender of the data and the data's integrity. This machine's IPsec function supports two security protocols: the ESP protocol, which enables both of the IPsec functions at the same time, and the AH protocol, which enables only the authentication function.

ESP Protocol

The ESP protocol provides secure transmission through both encryption and authentication. This protocol does not provide header authentication.

- For successful encryption, both the sender and receiver must specify the same encryption algorithm and encryption key. If you use the encryption key auto exchange method, the encryption algorithm and encryption key are specified automatically.
- For successful authentication, the sender and receiver must specify the same authentication algorithm and authentication key. If you use the encryption key auto exchange method, the authentication algorithm and authentication key are specified automatically.

AH Protocol

The AH protocol provides secure transmission through authentication of packets only, including headers.

- For successful authentication, the sender and receiver must specify the same authentication algorithm and authentication key. If you use the encryption key auto exchange method, the authentication algorithm and authentication key are specified automatically.

AH Protocol + ESP Protocol

When combined, the ESP and AH protocols provide secure transmission through both encryption and authentication. These protocols provide header authentication.

- For successful encryption, both the sender and receiver must specify the same encryption algorithm and encryption key. If you use the encryption key auto exchange method, the encryption algorithm and encryption key are specified automatically.
- For successful authentication, the sender and receiver must specify the same authentication algorithm and authentication key. If you use the encryption key auto exchange method, the authentication algorithm and authentication key are specified automatically.

Note

- Some operating systems use the term "Compliance" in place of "Authentication".

Encryption Key Auto Exchange Settings and Encryption Key Manual Settings

This machine provides two key setting methods: manual and auto exchange. Using either of these methods, agreements such as the IPsec algorithm and key must be specified for both sender and receiver. Such agreements form what is known as an SA (Security Association). IPsec communication is possible only if the receiver's and sender's SA settings are identical.

If you use the auto exchange method to specify the encryption key, the SA settings are auto configured on both parties' machines. However, before setting the IPsec SA, the ISAKMP SA (Phase 1) settings are auto configured. After this, the IPsec SA (Phase 2) settings, which allow actual IPsec transmission, are auto configured.

Also, for further security, the SA can be periodically auto updated by applying a validity period (time limit) for its settings. This machine only supports IKEv1 for encryption key auto exchange.

If you specify the encryption key manually, the SA settings must be shared and specified identically by both parties. To preserve the security of your SA settings, we recommend that they are not exchanged over a network.

Note that for both the manual and auto method of encryption key specification, multiple settings can be configured in the SA.

Settings 1-4 and Default Setting

Using either the manual or auto exchange method, you can configure four separate sets of SA details (such as different shared keys and IPsec algorithms). In the default settings of these sets, you can include settings that the fields of sets 1 to 4 cannot contain.

When IPsec is enabled, set 1 has the highest priority and 4 has the lowest. You can use this priority system to target IP addresses more securely. For example, set the broadest IP range at the lowest priority (4), and then set specific IP addresses at a higher priority level (3 and higher). This way, when IPsec transmission is enabled for a specific IP address, the higher level security settings will be applied.

IPsec Settings

IPsec settings for this machine can be made on Web Image Monitor. The following table explains individual setting items.

Encryption Key Auto Exchange / Manual Settings - Shared Settings

Setting	Description	Setting Value
IPsec	Specify whether to enable or disable IPsec.	• Active • Inactive
Exclude HTTPS Communication	Specify whether to enable IPsec for HTTPS transmission.	• Active • Inactive Specify "Active" if you do not want to use IPsec for HTTPS transmission.
Encryption Key Manual Settings	Specify whether to enable Encryption Key Manual Settings, or use Encryption Key Auto Exchange Settings only.	• Active • Inactive Specify "Active" if you want to use "Encryption Key Manual Settings".

The IPsec setting can also be made from the control panel.

Encryption Key Auto Exchange Security Level

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

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

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

Setting	Authentication Only	Authentication and Low Level Encryption	Authentication and High Level Encryption
Security Policy	Apply	Apply	Apply
Encapsulation Mode	Transport	Transport	Transport
IPsec Requirement Level	Use When Possible	Use When Possible	Always Require
Authentication Method	PSK	PSK	PSK
Phase 1 Hash Algorithm	MD5	SHA1	SHA1

Setting	Authentication Only	Authentication and Low Level Encryption	Authentication and High Level Encryption
Phase 1 Encryption Algorithm	DES	3DES	3DES
Phase 1 Diffie-Hellman Group	2	2	2
Phase 2 Security Protocol	AH	ESP	ESP
Phase 2 Authentication Algorithm	HMAC-MD5-96/ HMAC-SHA1-96	HMAC-MD5-96/ HMAC-SHA1-96	HMAC-SHA1-96
Phase 2 Encryption Algorithm	Cleartext (NULL encryption)	DES/3DES/ AES-128/AES-192/ AES-256	3DES/AES-128/ AES-192/AES-256
Phase 2 PFS	Inactive	Inactive	2

Encryption Key Auto Exchange Settings Items

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

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

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

Setting	Description	Setting Value
Remote Address	Specify the address of the IPsec transmission partner. You can also specify an address range.	The IPsec transmission partner's IPv4 or IPv6 address. If you are not setting an address range, enter 32 after an IPv4 address, or enter 128 after an IPv6 address.
Security Policy	Specify how IPsec is handled.	• Apply • Bypass • Discard
Encapsulation Mode	Specify the encapsulation mode. (auto setting)	• Transport • Tunnel (Tunnel beginning address - Tunnel ending address) Select the transport mode (this has no bearing on the security level). If you specify "Tunnel", you must then specify the "Tunnel End Point", which are the beginning and ending IP addresses. Set the same address for the beginning point as you set in "Local Address".
IPsec Requirement Level	Specify whether to only transmit using IPsec, or to allow cleartext transmission when IPsec cannot be established. (auto setting)	• Use When Possible • Always Require

Setting	Description	Setting Value
Authentication Method	Specify the method for authenticating transmission partners. (auto setting)	• PSK • Certificate If you specify "PSK", you must then set the PSK text (using ASCII characters). If you are using "PSK", specify a PSK password using up to 32 ASCII characters. If you specify "Certificate", the certificate for IPsec must be installed and specified before it can be used.
PSK Text	Specify the pre-shared key for PSK authentication.	Enter the pre-shared key required for PSK authentication.
Phase 1 Hash Algorithm	Specify the Hash algorithm to be used in phase 1. (auto setting)	• MD5 • SHA1
Phase 1 Encryption Algorithm	Specify the encryption algorithm to be used in phase 1. (auto setting)	• DES • 3DES
Phase 1 Diffie-Hellman Group	Select the Diffie-Hellman group number used for IKE encryption key generation. (auto setting)	• 1 • 2 • 14
Phase 1 Validity Period	Specify the time period for which the SA settings in phase 1 are valid.	Set in seconds from 300 sec. (5 min.) to 172800 sec. (48 hrs.).

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

Encryption Key Manual Settings Items

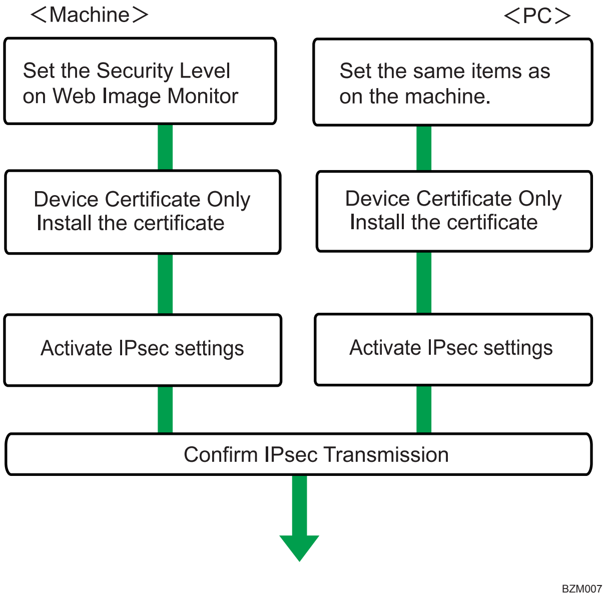
Setting	Description	Setting Value
Address Type	Specify the address type for which IPsec transmission is used.	• Inactive • IPv4 • IPv6 • IPv4/IPv6 (Default Settings only)
Local Address	Specify the machine's address. If you are using multiple IPv6 addresses, you can also specify an address range.	The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

Setting	Description	Setting Value
SPI (Input)	Specify the same value as your transmission partner's SPI output value.	Any number between 256 and 4095
Security Protocol	To apply both encryption and authentication to sent data, specify "ESP" or "ESP+AH". To apply authentication data only, specify "AH".	• ESP • AH • ESP+AH
Authentication Algorithm	Specify the authentication algorithm.	• HMAC-MD5-96 • HMAC-SHA1-96
Authentication Key	Specify the key for the authentication algorithm.	Specify a value within the ranges shown below, according to the encryption algorithm. Hexadecimal value 0-9, a-f, A-F • If HMAC-MD5-96, set 32 digits • If HMAC-SHA1-96, set 40 digits ASCII • IF HMAC-MD5-96, set 16 characters • If HMAC-SHA1-96, set 20 characters
Encryption Algorithm	Specify the encryption algorithm.	• Cleartext (NULL encryption) • DES • 3DES • AES-128 • AES-192 • AES-256

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

Encryption Key Auto Exchange Settings Configuration Flow

This can be specified by the network administrator.


<Machine>
<PC>
Set the Security Level on Web Image Monitor
Set the same items as on the machine.
Device Certificate Only Install the certificate
Device Certificate Only Install the certificate
Activate IPsec settings
Activate IPsec settings
Confirm IPsec Transmission
BZM007

Note

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

Specifying Encryption Key Auto Exchange Settings

This can be specified using Web Image Monitor.

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

   The network administrator can log in.

   Enter the login user name and login password.
4. **Click [Configuration], and then click [IPsec] under "Security".**
5. **Click [Edit] under "Encryption Key Auto Exchange Settings".**
6. **Make encryption key auto exchange settings in [Settings 1].**

   If you want to make multiple settings, select the settings number and add settings.

7. **Click [OK].**
8. **Select [Active] for "IPsec" in "IPsec".**
9. **Set "Exclude HTTPS Communication" to [Active] if you do not want to use IPsec for HTTPS transmission.**
10. **Click [OK].**
11. **Click [OK].**
12. **Click [Logout].**

Note

- To change the transmission partner authentication method for encryption key auto exchange settings to "Certificate", you must first install and assign a certificate. For details about creating and installing a device certificate, see p.120 "Protection Using Encryption".

Selecting the Certificate for IPsec

This can be specified by the network administrator.

Using Web Image Monitor, select the certificate to be used for IPsec. You must install the certificate before it can be used.

1. **Open a Web browser.**
2. **Enter "http://(the machine's IP address or host name)/" in the address bar.**
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".**
5. **Select the certificate to be used for IPsec from the drop down box in "IPsec" under "Certification".**
6. **Click [OK].**
7. **Click [OK].**
8. **Click [Logout].**

Specifying IPsec Settings on the Computer

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

1. **On the [Start] menu, click [Control Panel], click [Performance and Maintenance], and then click [Administrative Tools].**
2. **Double-click [Local Security Policy].**
3. **Click [IP Security Policies on Local Computer].**
4. **In the "Action" menu, click [Create IP Security Policy].**

   The IP Security Policy Wizard appears.
5. **Click [Next].**
6. **Enter a security policy name in "Name", and then click [Next].**
7. **Clear the "Activate the default response rule" check box, and then click [Next].**
8. **Select "Edit properties", and then click [Finish].**
9. **In the "General" tab, click [Advanced].**
10. **In "Authenticate and generate a new key after every", enter the same validity period (in minutes) that is specified on the machine in Encryption Key Auto Exchange Settings Phase 1, and then click [Methods].**
11. **Confirm that the hash algorithm ("Integrity"), encryption algorithm ("Encryption") and "Diffie-Hellman Group" settings in "Security method preference order" all match those specified on the machine in Encryption Key Auto Exchange Settings Phase 1.**

    If the settings are not displayed, click [Add].
12. **Click [OK] twice.**
13. **Click [Add] in the "Rules" tab.**

    The Security Rule Wizard appears.
14. **Click [Next].**
15. **Select "This rule does not specify a tunnel", and then click [Next].**
16. **Select the type of network for IPsec, and then click [Next].**
17. **Select the authentication method, and then click [Next].**

    If you select "Certificate" for authentication method in Encryption Key Auto Exchange Settings on the machine, specify the device certificate. If you select "PSK", enter the same PSK text specified on the machine with the pre-shared key.
18. **Click [Add] in the IP Filter List.**
19. **In [Name], enter an IP Filter name, and then click [Add].**

    The IP Filter Wizard appears.
20. **Click [Next].**
21. **Select "My IP Address" in "Source address", and then click [Next].**
22. **Select "A specific IP Address" in "Destination address", enter the machine's IP address, and then click [Next].**

23. **Select the protocol type for IPsec, and then click [Next].**
24. **Click [Finish].**
25. **Click [OK].**
26. **Select the IP filter that was just created, and then click [Next].**
27. **Select the IPsec security filter, and then click [Edit].**
28. **In the "Security Methods" tab, check "Negotiate security" and then click [Add].**
29. **Select "Custom" and click [Settings].**
30. **In "Integrity algorithm", select the authentication algorithm that was specified on the machine in Encryption Key Auto Exchange Settings Phase 2.**
31. **In "Encryption algorithm", select the encryption algorithm that specified on the machine in Encryption Key Auto Exchange Settings Phase 2.**
32. **In Session key settings, select "Generate a new key every", and enter the validity period (in seconds) that was specified on the machine in Encryption Key Auto Exchange Settings Phase 2.**
33. **Click [OK] three times.**
34. **Click [Next].**
35. **Click [Finish].**

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

36. **Click [OK].**
37. **Click [Close].**

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

38. **Select the security policy that was just created, right click, and then click [Assign].**

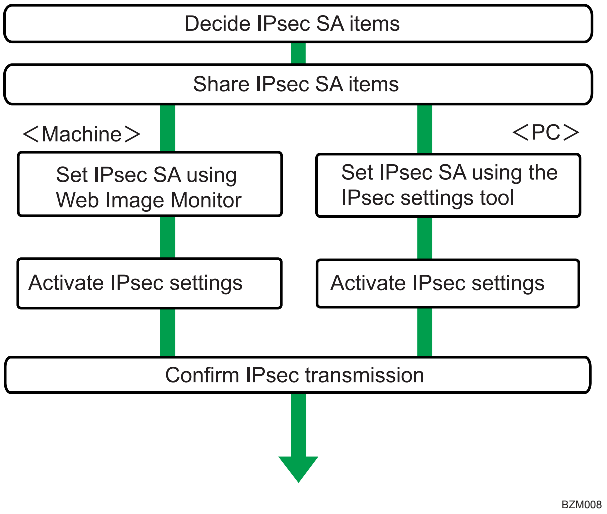
    IPsec settings on the computer are enabled.

Note

- To disable the computer's IPsec settings, select the security policy, right click, and then click [Unassign].
- If you specify the "Authentication and High Level Encryption" security level in encryption key auto exchange settings, also select the "Master key perfect forward secrecy (PFS)" check box in the Security Filter Properties screen (which appears in step 27). If using PFS in Windows XP, the PFS group number used in phase 2 is automatically negotiated in phase 1 from the Diffie-Hellman group number (set in step 11). Consequently, if you change the security level specified automatic settings on the machine and "User Setting" appears, you must set the same group number for "Phase 1 Diffie-Hellman Group" and "Phase 2 PFS" on the machine to establish IPsec transmission.

Encryption Key Manual Settings Configuration Flow

This can be specified by the network administrator.



Note

- Before transmission, SA information is shared and specified by the sender and receiver. To prevent SA information leakage, we recommend that this exchange is not performed over the network.
- After configuring IPsec, you can use "Ping" command to check if the connection is established correctly. However, you cannot use "Ping" command when ICMP is excluded from IPsec transmission. Also, because the response is slow during initial key exchange, it may take some time to confirm that transmission has been established.

Specifying Encryption Key Manual Settings

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

   The network administrator can log in.

   Enter the login user name and login password.
4. **Click [Configuration], and then click [IPsec] under "Security".**
5. **Select [Active] for "Encryption Key Manual Settings".**
6. **Click [Edit] under "Encryption Key Manual Settings".**

7. **Set items for encryption key manual settings in [Settings 1].**

   If you want to make multiple settings, select the settings number and add settings.

8. **Click [OK].**
9. **Select [Active] for "IPsec" in "IPsec".**
10. **Set "Exclude HTTPS Communication" to [Active] if you do not want to use IPsec for HTTPS communication.**
11. **Click [OK].**
12. **Click [OK].**
13. **Click [Logout].**

telnet Setting Commands

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

Important

- If you are using a certificate as the authentication method in encryption key auto exchange settings (IKE), install the certificate using Web Image Monitor. A certificate cannot be installed using telnet.

ipsec

To display IPsec related settings information, use the "ipsec" command.

Display current settings

```
msh> ipsec
```

Displays the following IPsec settings information:

- IPsec shared settings values
- Encryption key manual settings, SA setting 1-4 values
- Encryption key manual settings, default setting values
- Encryption key auto exchange settings, IKE setting 1-4 values
- Encryption key auto exchange settings, IKE default setting values

Display current settings portions

```
msh> ipsec -p
```

- Displays IPsec settings information in portions.

ipsec manual mode

To display or specify encryption key manual settings, use the "ipsec manual_mode" command.

Display current settings

```
msh> ipsec manual_mode
```

- Displays the current encryption key manual settings.

Specify encryption key manual settings

```
msh> ipsec manual_mode {on|off}
```

- To enable encryption key manual settings, set to [on]. To disable settings, set to [off].

ipsec exclude

To display or specify protocols excluded by IPsec, use the "ipsec exclude" command.

Display current settings

```
msh> ipsec exclude
```

- Displays the protocols currently excluded from IPsec transmission.

Specify protocols to exclude

```
msh> ipsec exclude {https|dns|dhcp|wins|all} {on|off}
```

- Specify the protocol, and then enter [on] to exclude it, or [off] to include it for IPsec transmission. Entering [all] specifies all protocols collectively.

ipsec manual

To display or specify the encryption key manual settings, use the "ipsec manual" command.

Display current settings

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

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

Disable settings

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

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

Specify the local/remote address for settings 1-4

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

- Enter the separate setting number [1-4] and specify the local address and remote address.

- To specify the local or remote address value, specify masklen by entering [/] and an integer 0-32 if you are specifying an IPv4 address. If you are specifying an IPv6 address, specify masklen by entering [/] and an integer 0-128.
- Not specifying an address value displays the current setting.

Specify the address type in default setting

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

- Specify the address type for the default setting.
- To specify both IPv4 and IPv6, enter [any].

Security protocol setting

```
msh> ipsec manual {1|2|3|4|default} proto {ah|esp|dual}
```

- Enter the separate setting number [1-4] or [default] and specify the security protocol.
- To specify AH, enter [ah]. To specify ESP, enter [esp]. To specify AH and ESP, enter [dual].
- Not specifying a protocol displays the current setting.

SPI value setting

```
msh> ipsec manual {1|2|3|4|default} spi SPI input value SPI output value
```

- Enter the separate setting number [1-4] or [default] and specify the SPI input and output values.
- Specify a decimal number between 256-4095, for both the SPI input and output values.

Encapsulation mode setting

```
msh> ipsec manual {1|2|3|4|default} mode {transport|tunnel}
```

- Enter the separate setting number [1-4] or [default] and specify the encapsulation mode.
- To specify transport mode, enter [transport]. To specify tunnel mode, enter [tunnel].
- If you have set the address type in the default setting to [any], you cannot use [tunnel] in encapsulation mode.
- Not specifying an encapsulation mode displays the current setting.

Tunnel end point setting

```
msh> ipsec manual {1|2|3|4|default} tunneladdar beginning IP address ending IP
address
```

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

Authentication algorithm and authentication key settings

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

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

Encryption algorithm and encryption key setting

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

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

Reset setting values

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

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

ipsec ike

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

Display current settings

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

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

Disable settings

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

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

Specify the local/remote address for settings 1-4

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

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

Specify the address type in default setting

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

- Specify the address type for the default setting.
- To specify both IPv4 and IPv6, enter [any].

Security policy setting

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

- Enter the separate setting number [1-4] or [default] and specify the security policy for the address specified in the selected setting.
- To apply IPsec to the relevant packets, specify [apply]. To not apply IPsec, specify [bypass].
- If you specify [discard], any packets to which IPsec can be applied are discarded.
- Not specifying a security policy displays the current setting.

Security protocol setting

```
msh> ipsec ike {1|2|3|4|default} proto {ah|esp|dual}
```

- Enter the separate setting number [1-4] or [default] and specify the security protocol.
- To specify AH, enter [ah]. To specify ESP, enter [esp]. To specify AH and ESP, enter [dual].
- Not specifying a protocol displays the current setting.

IPsec requirement level setting

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

- Enter the separate setting number [1-4] or [default] and specify the IPsec requirement level.
- If you specify [require], data will not be transmitted when IPsec cannot be used. If you specify [use], data will be sent normally when IPsec cannot be used. When IPsec can be used, IPsec transmission is performed.
- Not specifying a requirement level displays the current setting.

Encapsulation mode setting

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

- Enter the separate setting number [1-4] or [default] and specify the encapsulation mode.
- To specify transport mode, enter [transport]. To specify tunnel mode, enter [tunnel].
- If you have set the address type in the default setting to [any], you cannot use [tunnel] in encapsulation mode.

- Not specifying an encapsulation mode displays the current setting.

Tunnel end point setting

```
msh> ipsec ike {1|2|3|4|default} tunneladdar beginning IP address ending IP
address
```

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

IKE partner authentication method setting

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

- Enter the separate setting number [1-4] or [default] and specify the authentication method.
- Specify [psk] to use a shared key as the authentication method. Specify [rsasig] to use a certificate at the authentication method.
- You must also specify the PSK character string when you select [psk].
- Note that if you select "Certificate", the certificate for IPsec must be installed and specified before it can be used. To install and specify the certificate use Web Image Monitor.

PSK character string setting

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

- If you select PSK as the authentication method, enter the separate setting number [1-4] or [default] and specify the PSK character string.
- Specify the character string in ASCII characters. There can be no abbreviations.

ISAKMP SA (phase 1) hash algorithm setting

```
msh> ipsec ike {1|2|3|4|default} ph1 hash {md5|sha1}
```

- Enter the separate setting number [1-4] or [default] and specify the ISAKMP SA (phase 1) hash algorithm.
- To use MD5, enter [md5]. To use SHA1, enter [sha1].
- Not specifying the hash algorithm displays the current setting.

ISAKMP SA (phase 1) encryption algorithm setting

```
msh> ipsec ike {1|2|3|4|default} ph1 encrypt {des|3des}
```

- Enter the separate setting number [1-4] or [default] and specify the ISAKMP SA (phase 1) encryption algorithm.
- To use DES, enter [des]. To use 3DES, enter [3des].
- Not specifying an encryption algorithm displays the current setting.

ISAKMP SA (phase 1) Diffie-Hellman group setting

```
msh> ipsec ike {1|2|3|4|default} ph1 dhgroup {1|2|14}
```

- Enter the separate setting number [1-4] or [default] and specify the ISAKMP SA (phase 1) Diffie-Hellman group number.
- Specify the group number to be used.
- Not specifying a group number displays the current setting.

ISAKMP SA (phase 1) validity period setting

```
msh> ipsec ike {1|2|3|4|default} ph1 lifetime validity period
```

- Enter the separate setting number [1-4] or [default] and specify the ISAKMP SA (phase 1) validity period.
- Enter the validity period (in seconds) from 300 to 172800.
- Not specifying a validity period displays the current setting.

IPsec SA (phase 2) authentication algorithm setting

```
msh> ipsec ike {1|2|3|4|default} ph2 auth {hmac-md5|hmac-sha1}
```

- Enter the separate setting number [1-4] or [default] and specify the IPsec SA (phase 2) authentication algorithm.
- Separate multiple encryption algorithm entries with a comma (,). The current setting values are displayed in order of highest priority.
- Not specifying an authentication algorithm displays the current setting.

IPsec SA (phase 2) encryption algorithm setting

```
msh> ipsec ike {1|2|3|4|default} ph2 encrypt {null|des|3des|aes128|aes192|
aes256}
```

- Enter the separate setting number [1-4] or [default] and specify the IPsec SA (phase 2) encryption algorithm.
- Separate multiple encryption algorithm entries with a comma (,). The current setting values are displayed in order of highest priority.
- Not specifying an encryption algorithm displays the current setting.

IPsec SA (phase 2) PFS setting

```
msh> ipsec ike {1|2|3|4|default} ph2 pfs {none|1|2|14}
```

- Enter the separate setting number [1-4] or [default] and specify the IPsec SA (phase 2) Diffie-Hellman group number.
- Specify the group number to be used.
- Not specifying a group number displays the current setting.

IPsec SA (phase 2) validity period setting

```
msh> ipsec ike {1|2|3|4|default} ph2 lifetime validity period
```

- Enter the separate setting number [1-4] or [default] and specify the IPsec SA (phase 2) validity period.

- Enter the validity period (in seconds) from 300 to 172800.
- Not specifying a validity period displays the current setting.

Reset setting values

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

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

Authentication by IEEE802.1X

IEEE802.1X enables authentication in an Ethernet environment. For details, see "Configuring IEEE 802.1X", Network and System Settings Reference.

7. Specifying the Extended Security Functions

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

Specifying the Extended Security Functions

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

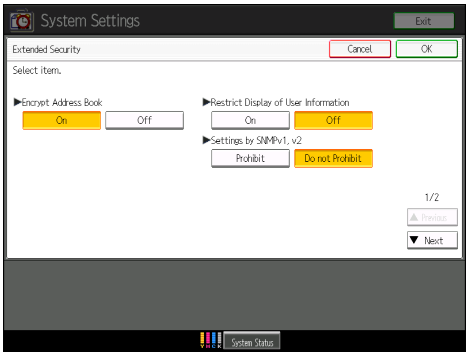
For details about when to use each function, see the corresponding chapters.

Changing the Extended Security Functions

Administrators can change the extended security functions according to their role. For details about logging in and logging out with administrator authentication, see p.28 "Logging in Using Administrator Authentication" and p.30 "Logging out Using Administrator Authentication".

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

   If this item is not visible, press [▼Next] to display more settings.
5. **Press the setting you want to change, and change the setting.**



Extended Security

Select item.

▶Encrypt Address Book: [✓ On] Off

▶Restrict Display of User Information: On [✓ Off]

▶Settings by SNMPv1, v2: Prohibit [✓ Do not Prohibit]

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

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 p.67 "Protecting the Address Book".

Default: [Off]

Restrict Display of User Information

This can be specified by the machine administrator.

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, 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

This can be specified by the machine administrator.

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

Default: [**Do not Prohibit**]

Update Firmware

This can be specified by the machine administrator.

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

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

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

Default: [**Do not Prohibit**]

Change Firmware Structure

This can be specified by the machine administrator.

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

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

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

When Change Firmware Structure is set to [Prohibit], administrator authentication must be enabled.

After [Prohibit] is specified, turn off administrator authentication once, and the next time administrator authentication is specified, the setting will return to the default, [Do not Prohibit].

If you select [Do not Prohibit], firmware structure change detection is disabled.

Default: [**Do not Prohibit**]

Other Security Functions

This section explains 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.

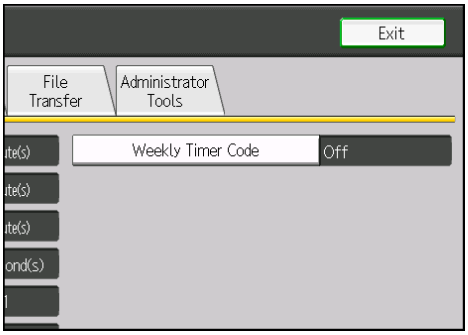
Weekly Timer Code

This can be specified by the machine administrator. For details about logging in and logging out with administrator authentication, see p.28 "Logging in Using Administrator Authentication" and p.30 "Logging out Using Administrator Authentication".

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.

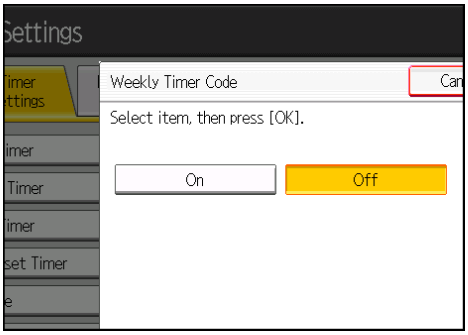
Specifying Weekly Timer Code

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



Weekly Timer Code Off

5. **Press [On].**



Settings

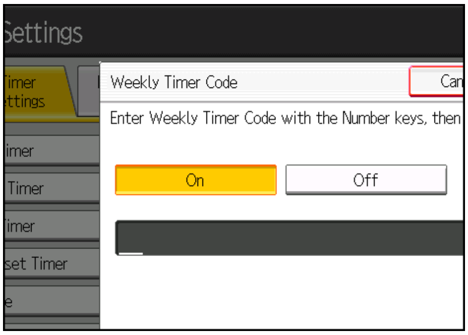
imer
ttings

Weekly Timer Code

Can

Select item, then press [OK].

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



Settings

imer
ttings

Weekly Timer Code

Can

Enter Weekly Timer Code with the Number keys, then

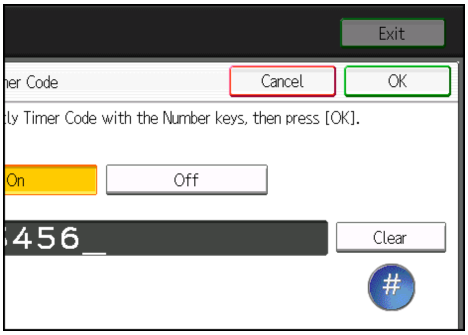
The weekly timer code must be one to eight digits long.

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

Canceling Weekly Timer Code

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

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



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

Limiting Machine Operations to Customers Only

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

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

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

Use the following settings.

- Service Mode Lock

Settings

This can be specified by the machine administrator. For details about logging in and logging out with administrator authentication, see p.28 "Logging in Using Administrator Authentication" and p.30 "Logging out Using Administrator Authentication".

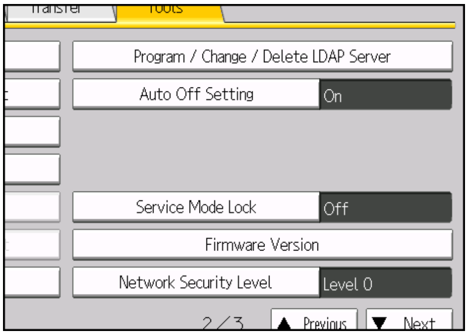
Service Mode Lock

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

Specifying Service Mode Lock

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

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



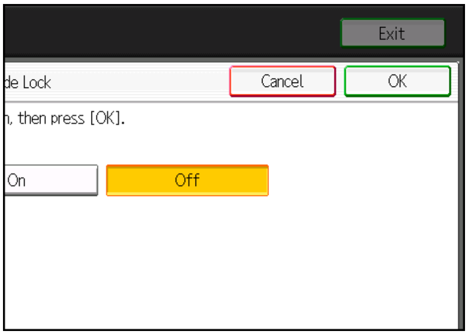
Auto Off Setting On

Service Mode Lock Off

Network Security Level Level 0

If this item is not visible, press [▼Next] to display more settings.

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

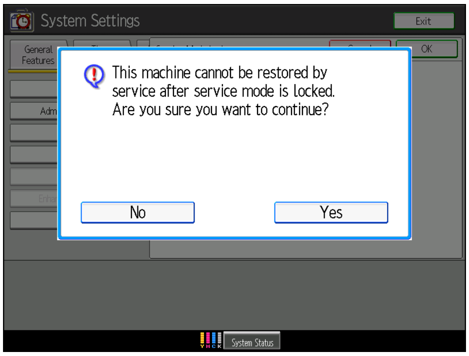


de Lock

n, 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?

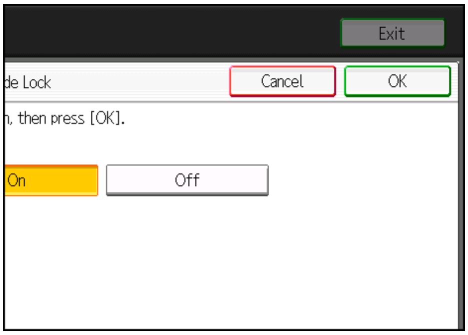
7. **Press the [User Tools] key.**

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.

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

   If this item is not visible, press [▼Next] to display more settings.
5. **Press [Off], and then press [OK].**



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

   The service representative can switch to service mode.

Additional Information for Enhanced Security

This section explains the settings that you can configure to enhance the machine's security.

Settings You Can Configure Using the Control Panel

Use the control panel to configure the security settings shown in the following table.

Menu	Tab	Item	Setting
System Settings	Timer Settings	Auto Logout Timer	On: 180 seconds or less. You cannot change the Web Image Monitor auto logout time. See p.63 "Auto Logout".
System Settings	Administrator Tools	Administrator Authentication Management/User Management	Select [On], and then select [Administrator Tools] for "Available Settings". See p.24 "Enabling Administrator Authentication".
System Settings	Administrator Tools	Administrator Authentication Management/ Machine Management	Select [On], and then select [Timer Settings], [Interface Settings], [File Transfer], and [Administrator Tools] for "Available Settings". See p.24 "Enabling Administrator Authentication".
System Settings	Administrator Tools	Administrator Authentication Management/ Network Management	Select [On], and then select [Interface Settings], [File Transfer], and [Administrator Tools] for "Available Settings". See p.24 "Enabling Administrator Authentication".
System Settings	Administrator Tools	Administrator Authentication Management/File Management	Select [On], and then select [Administrator Tools] for "Available Settings". See p.24 "Enabling Administrator Authentication".

Menu	Tab	Item	Setting
System Settings	Administrator Tools	Extended Security/ Settings by SNMPv1, v2	Prohibit See p.155 "Specifying the Extended Security Functions".
System Settings	Administrator Tools	Extended Security/ Password Policy	"Complexity Setting": Level 1 or higher, "Minimum Character No.": 8 or higher See p.155 "Specifying the Extended Security Functions".
System Settings	Administrator Tools	Network Security Level	Level 2 To acquire the machine status through Web Image Monitor, set "SNMP" to Active on Web Image Monitor. See p.116 "Specifying Network Security Level".
System Settings	Administrator Tools	Service Mode Lock	On See p.161 "Limiting Machine Operations to Customers Only".
System Settings	Administrator Tools	Machine Data Encryption Settings	Select [Encrypt], and then select [All Data] for "Carry over all data or file system data only (without formatting), or format all data" If [Encrypt] is already selected, further encryption settings are not necessary. See p.71 "Encrypting Data on the Hard Disk".

Note

- The SNMP setting can be specified in [SNMP] under [Configuration] in Web Image Monitor.

Settings You Can Configure Using Web Image Monitor

Use Web Image Monitor to configure the security settings shown in the following table.

Category	Item	Setting
Device Settings/ Logs	Collect Job Logs	Active
Device Settings/ Logs	Collect Access Logs	Active
Security/User Lockout Policy	Lockout	Active
Security/User Lockout Policy	Number of Attempts before Lockout	5 times or less. See p.61 "User Lockout Function".
Security/User Lockout Policy	Lockout Release Timer	Set to Active or Inactive. When setting to Active, set the Lockout release timer to 60 minutes or more. See p.61 "User Lockout Function".
Security/User Lockout Policy	Lock Out User for	When setting "Lockout Release Timer" to[Active], set the Lockout release timer to 60 minutes or more. See p.61 "User Lockout Function".
Network/ SNMPv3	SNMPv3 Function	Inactive To use SNMPv3 functions, set "SNMPv3 Function" to [Active], and set "Permit SNMPv3 Communication" to [Encryption Only]. Because SNMPv3 enforces authentication for each packet, Login log will be disabled as long as SNMPv3 is active.
Security/Network Security	FTP	Inactive Before specifying this setting, set "Network Security Level" to [Level 2] on the control panel.

8. Troubleshooting

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

If Authentication Fails

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

If a Message is Displayed

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

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

Messages	Cause	Solutions
"You do not have 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.

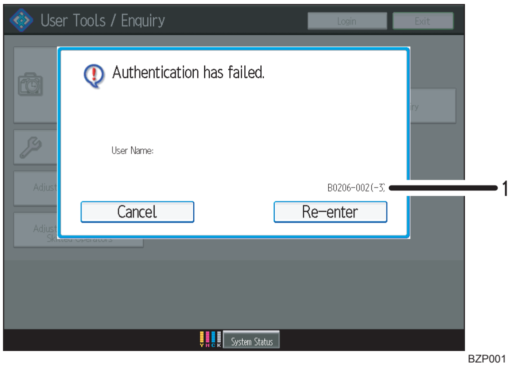
Messages	Cause	Solutions
"Failed to obtain URL."	The machine cannot connect to the server or cannot establish communication.	Make sure the server's settings, such as the IP address and host name, are specified correctly on the machine. Make sure the host name of the UA Server is specified correctly.
"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 0104-000 B, W, L, I 0206-003 W, L, I 0406-003
"Authentication has failed."	Authentication failed because no more users can be registered. (The number of users registered in the Address Book has reached capacity.)	Delete unnecessary user addresses. See the error codes below for possible solutions: W, L, I 0612-005
"Authentication has failed."	Cannot access the authentication server when using Windows authentication, LDAP authentication, or Integration Server authentication.	A network or server error may have occurred. Confirm the network in use with the LAN administrator. If an error code appears, follow the instructions next to the error code in the table below.

Messages	Cause	Solutions
"Administrator Authentication for User Management must be set to on before this selection can be made."	User administrator privileges have not been enabled in Administrator Authentication Management.	To specify basic authentication, Windows authentication, LDAP authentication, or Integration Server authentication, you must first enable user administrator privileges in Administrator Authentication Management. For details about authentication settings, see p.35 "Configuring User Authentication".

If an Error Code is Displayed

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

Error Code Display Position



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.
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.
B0208-000	A login attempt was made using a login user account that was disabled with the User Lockout function.	Release the locked out user account.

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.

Error Code	Cause	Solution
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.
W0406-101	Authentication cannot be completed because of the high number of authentication attempts.	Wait a few minutes and then try again. If the situation does not return to normal, make sure that an authentication attack is not occurring. Notify the administrator of the screen message by e-mail, and check the system log for signs of an authentication attack.
W0400-102	Kerberos authentication failed because the server or security module is not functioning correctly.	1. Make sure that the server is functioning properly. 2. Make sure that the security module is installed.
W0406-104	1. Cannot connect to the authentication server.	Make sure that connection to the authentication server is possible. Use the PING Command to check the connection.
W0406-104	2. A login name or password error occurred.	Make sure that the user is registered on the server. Use a registered login user name and password.

Error Code	Cause	Solution
W0406-104	3. A domain name error occurred.	Make sure that the Windows authentication domain name is specified correctly.
W0406-104	4. Cannot resolve the domain name.	Specify the IP address in the domain name and confirm that authentication is successful. If authentication was successful: 1. If the top-level domain name is specified in the domain name (such as domainname.xxx.com), make sure that DNS is specified in "Interface Settings". 2. If a NetBIOS domain name is specified in domain name (such as DOMAINNAME), make sure that WINS is specified in "Interface Settings".

Error Code	Cause	Solution
W0406-104	4. Cannot resolve the domain name.	Specify the IP address in the domain name and confirm that authentication is successful. If authentication was unsuccessful: 1. Make sure that Restrict LM/NTLM is not set in either "Domain Controller Security Policy" or "Domain Security Policy". 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 the Windows firewall, open the Properties window for "Network Connections", and then click "Settings" on the "Advanced" tab. On the "Exceptions" tab, specify ports 137 and 139 as exceptions. In the Properties window for "Network Connections", open TCP/IP properties. Then click detail settings, WINS, and then check the "Enable NetBIOS over TCP/IP" box and set number 137 to "Open".

Error Code	Cause	Solution
W0406-104	5. Kerberos authentication failed.	1. Kerberos authentication settings are not correctly configured. Make sure the realm name, KDC (Key Distribution Center) name and corresponding domain name are specified correctly. 2. The KDC and machine timing do not match. Authentication will fail if the difference between the KDC and machine timing is more than 5 minutes. Make sure the timing matches. 3. Kerberos authentication will fail if the realm name is specified in lower-case letters. Make sure the realm name is specified in capital letters. 4. Kerberos authentication will fail if automatic retrieval for KDC fails. Ask your service representative to make sure the KDC retrieval settings are set to "automatic retrieval". If automatic retrieval is not functioning properly, switch to manual retrieval.

Error Code	Cause	Solution
W0400-105	1. The UserPrincipleName (user@domainname.xxx.com) form is being used for the login user name.	The user group cannot be obtained if the UserPrincipleName (user@domainname.xxx.com) form is used. Use "sAMAccountName(user)" to log in, because this account allows you to obtain the user group.
W0400-105	2. Current settings do not allow group retrieval.	Make sure the user group's group scope is set to "Global Group" and the group type is set to "Security" in group properties. Make sure the account has been added to user group. Make sure the user group name registered on the 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 Login" 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.

Error Code	Cause	Solution
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.
W0406-003	An authentication error occurred because the user name contains a space, colon (:), or quotation mark (").	Recreate the account if the account name contains any of these prohibited characters. If the account name was entered incorrectly, enter it correctly and log on again.
W0409-000	Authentication timed out because the server did not respond.	Check the network configuration, or settings on the authenticating server.
W0511-000	The authentication server login name is the same as a user name already registered on the 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.

Error Code	Cause	Solution
W0612-005	Authentication failed because no more users can be registered. (The number of users registered in the Address Book has reached capacity.)	Ask the user administrator to delete unused user accounts in the Address Book.
W0707-001	An authentication error occurred because the Address Book is being used at another location.	Wait a few minutes and then try again.

LDAP Authentication

Error Code	Cause	Solution
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.

Error Code	Cause	Solution
L0307-001	An authentication error occurred because the Address Book is being used at another location.	Wait a few minutes and then try again.
L0406-200	Authentication cannot be completed because of the high number of authentication attempts.	Wait a few minutes and then try again. If the situation does not return to normal, make sure that an authentication attack is not occurring. Notify the administrator of the screen message by e-mail, and check the system log for signs of an authentication attack.
L0406-201	Authentication is disabled in the LDAP server settings.	Change the LDAP server settings in administrator tools, in "System Settings".
L0406-202 L0406-203	1. There is an error in the LDAP authentication settings, LDAP server, or network configuration.	1. Make sure that a connection test is successful with the current LDAP server configuration. If connection is not successful, there might be an error in the network settings. Check the domain name or DNS settings in "Interface Settings". 2. Make sure the LDAP server is specified correctly in the LDAP authentication settings. 3. Make sure the login name attribute is entered correctly in the LDAP authentication settings. 4. Make sure the SSL settings are supported by the LDAP server.

Error Code	Cause	Solution
L0406-202 L0406-203	2. A login user name or password error occurred.	1. Make sure the login user name and password are entered correctly. 2. Make sure a usable login name is registered on the 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.
L0406-202 L0406-203	3. There is an error in the simple encryption method.	1. Authentication will fail if the password is left blank in simple authentication mode. To allow blank passwords, contact your service representative. 2. In simple authentication mode, the DN of the login user name is obtained in the user account. Authentication fails if the DN cannot be obtained. Make sure there are no errors in the server name, login user name/password, or information entered for the search filter.

Error Code	Cause	Solution
L0406-204	Kerberos authentication failed.	1. Kerberos authentication settings are not correctly configured. Make sure the realm name, KDC (Key Distribution Center) name, and supporting domain name are specified correctly. 2. The KDC and machine timing do not match. Authentication will fail if the difference between the KDC and machine timing is more than 5 minutes. Make sure the timing matches. 3. Kerberos authentication will fail if the realm name is specified in lower-case letters. Make sure the realm name is specified in capital letters.
L0400-210	Failed to obtain user information in LDAP search.	The login attribute's search criteria might not be specified or the specified search information is unobtainable. Make sure the login name attribute is specified correctly.
L0406-003	An authentication error occurred because the user name contains a space, colon (:), or quotation mark (").	Recreate the account if the account name contains any of these prohibited characters. If the account name was entered incorrectly, enter it correctly and log in again.
L0409-000	Authentication timed out because the server did not respond.	Contact the server or network administrator. If the situation does not return to normal, contact your service representative.

Error Code	Cause	Solution
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.
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.

Error Code	Cause	Solution
I0206-003	An authentication error occurred because the user name contains a space, colon (:), or quotation mark (").	Recreate the account if the account name contains any of these prohibited characters. If the account name was entered incorrectly, enter it correctly and log 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.
I0406-301	2. A login user name or password error occurred.	1. Make sure the login user name and password are entered correctly. 2. Make sure that a usable login name is registered on the 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.

Error Code	Cause	Solution
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.
I0612-005	Authentication failed because no more users can be registered. (The number of users registered in the Address Book has reached capacity.)	Ask the user administrator to delete unused user accounts in the Address Book.
I0707-001	An authentication error occurred because the Address Book is being used at another location.	Wait a few minutes and then try again.

If the Machine Cannot Be Operated

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

Condition	Cause	Solution
User authentication is disabled, yet destinations specified using the machine do not appear.	User authentication might have been disabled without "All Users" being selected for "Protect Destination".	Re-enable user authentication, and select [All Users] as the access permission setting of the destinations you want to display. For details, see p.67 "Protecting the Address Book".
Cannot print when user authentication has been enabled.	User code authentication may not be specified in the printer driver.	Specify user code authentication in the printer driver. For details, see the printer driver Help.
After you execute "Encrypt Address Book", the "Exit" message does not appear.	The hard disk may be faulty. The file may be corrupt.	Contact your service representative.

9. Appendix

Supervisor Operations

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

If any of the administrators forgets their password or if any of the administrators changes, the supervisor can assign a new password. If logged 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 characters that the password can contain, see p.155 "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 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.

Logging in as the Supervisor

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.

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

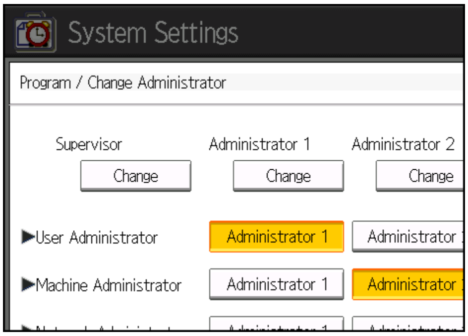
Changing the Supervisor

To do this, you must enable the user administrator's privileges through the settings under "Administrator Authentication Management". For details, see p.24 "Specifying Administrator Privileges".

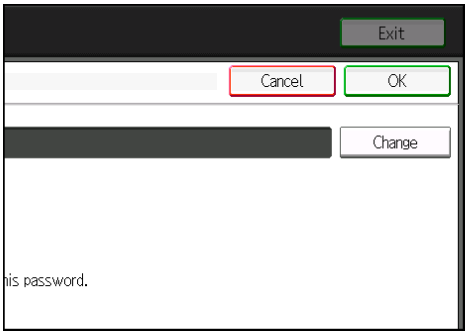
1. **Press the [User Tools] key.**
2. **Press the [Login/Logout] key.**
3. **Log in as the supervisor.**

   For details about logging in as the supervisor, see p.185 "Logging in as the Supervisor".
4. **Press [System Settings].**
5. **Press [Administrator Tools].**
6. **Press [Program / Change Administrator].**

   If this item is not visible, press [▼Next] to display more 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.**

Resetting the Administrator's Password

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

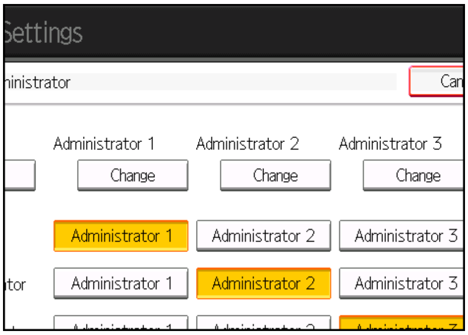
1. **Press the [User Tools] key.**
2. **Press the [Login/Logout] key.**
3. **Log in as the supervisor.**

    For details about logging in as the supervisor, see p.185 "Logging in as the Supervisor".

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

    If this item is not visible, press [▼Next] to display more 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.**

User Administrator Settings

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

System Settings

Interface Settings

- Network

  DNS Configuration

  You can perform a connection test.

Administrator Tools

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

  Clear the counter for all user's jobs

  Clear the counter for each user's jobs
- Administrator Authentication Management

  User Management

  User administrator authentication cannot be disabled while user authentication is enabled.
- Program / Change Administrator

  User Administrator
- Extended Security

  Encrypt Address Book

  Password Policy

Adjustment Settings for Operators

Adjustment Settings for Operators

All the settings can be specified.

Settings via Web Image Monitor

Address Book

All the settings can be specified.

Device Settings

- Administrator Authentication Management

  User Administrator Authentication

  Available Settings for User Administrator

  User administrator authentication cannot be disabled while user authentication is enabled.

- 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

Machine Administrator Settings

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

System Settings

General Features

All the settings can be specified.

Timer Settings

All the settings can be specified.

Interface Settings

- Network

  DNS Configuration

  You can perform a connection test.

File Transfer

- SMTP Authentication
- POP before SMTP
- Reception Protocol
- POP3 / IMAP4 Settings
- Administrator's E-mail Address

Administrator Tools

- 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
- Key Counter Management
- External Charge Unit Management
- Enhanced External Charge Unit Management
- Extended Security

  Restrict Display of User Information

  @Remote Service

  Update Firmware

  Change Firmware Structure
- Program / Change / Delete LDAP Server
- Auto Off Setting
- Service Test Call
- Notify Machine Status
- Service Mode Lock
- Auto Erase Memory Setting
- Erase All Memory
- Program / Change / Delete Realm
- Machine Data Encryption Settings

Maintenance

- Colour Registration

  All the settings can be specified.

Adjustment Settings for Operators

Adjustment Settings for Operators

All the settings can be specified.

Adjustment Settings for Skilled Operators

Adjustment Settings for Skilled Operators

All the settings can be specified.

For details about the settings, contact your service representative.

Tray Paper Settings

Tray Paper Settings

All the settings can be specified.

For details about the settings, contact your service representative.

Settings via Web Image Monitor

Home

- Reset Device

Job

All the settings can be specified.

Device Settings

- System

  Print Priority

  Function Reset Timer

  Permit Firmware Update

  Permit Firmware Structure Change

  Display IP Address on Device Display Panel

  Output Tray

  Paper Tray Priority

- Paper

  All the settings can be specified.

- Custom Paper

  All the settings can be specified.

- Date/Time

  All the settings can be specified.

- Timer

All the settings can be specified.

- Logs

  All the settings can be specified.

- Download Logs
- E-mail

  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 for the machine administrator.

Login User Name

Login Password

Encryption Password

- LDAP Server

  All the settings can be specified.

- Firmware Update

  All the settings can be specified.

- Program/Change Realm

  All the settings can be specified.

Network

- SNMPv3

  Access Type (Machine Administrator)

Security

- User Lockout Policy

  All the settings can be specified.

RC Gate

All the settings can be specified.

Webpage

- Webpage

  Download Help File

Network Administrator Settings

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

System Settings

Interface Settings

If DHCP is enabled, the settings that are automatically obtained via DHCP cannot be specified.

- Print List
- Network

  All the settings can be specified.

File Transfer

- SMTP Server
- E-mail Communication Port
- 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, v2
- Network Security Level

Adjustment Settings for Operators

Adjustment Settings for Operators

All the settings can be specified.

Settings via Web Image Monitor

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.

- Administrator Authentication Management

  Network Administrator Authentication

  Available Settings for Network Administrator

- Program/Change Administrator

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

  Login User Name

  Login Password

  Encryption Password

Interface

- Interface Settings

  Ethernet Security

  Ethernet Speed

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.

- Bonjour

  All the settings can be specified.

Security

- Network Security

  All the settings can be specified.

- Access Control

  All the settings can be specified.

- SSL/TLS

  All the settings can be specified.

- ssh

  All the settings can be specified.

- Site Certificate

  All the settings can be specified.

- Device Certificate

  All the settings can be specified.

- IPsec

  All the settings can be specified.

- IEEE 802.1X

  All the settings can be specified.

Webpage

All the settings can be specified.

File Administrator Settings

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

System Settings

Interface Settings

- Network

  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

Adjustment Settings for Operators

Adjustment Settings for Operators

All the settings can be specified.

Settings via Web Image Monitor

Device Settings

- Administrator Authentication Management

  File Administrator Authentication

  Available Settings for File Administrator

- Program/Change Administrator

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

Login User Name

Login Password

Encryption Password

Webpage

- Webpage

  Download Help File

The Privilege for User Account Settings in the Address Book

The authorities for using the Address Book are as follows:

- Abbreviations in the table heads
    - Read-only (User) = This is a user assigned "Read-only" privilege.
    - Edit (User) = This is a user assigned "Edit" privilege.
    - Edit / Delete (User) = This is a user assigned "Edit / Delete" privilege.
    - Full Control (User) = This is a user assigned "Full Control" privilege.
    - 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
Login User Name	N/A	N/A	N/A	N/A	R	R/W

Settings	Read-only (User)	Edit (User)	Edit / Delete (User)	Full Control (User)	Registered User	User Admin.
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.
Protect Destination: 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.

Note

- Settings that are not in the list can only be viewed, regardless of whether "Available Settings" has been specified.

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
Screen Colour Setting	R/W	R
Output Tray Setting	R/W	R
Output: Printer	R/W	R
Paper Tray Priority: Printer	R/W	R
Key Repeat	R/W	R
System Status Display Time	R/W	R
Status Indicator	R/W	R
Z-fold Position	R/W	R

Settings	Not Specified	Specified
Half Fold Position	R/W	R
Letter Fold-out Position	R/W	R
Letter Fold-in Position	R/W	R
Double Parallel Fold Position	R/W	R
Gate Fold Position	R/W	R

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	R/W	R
Weekly Timer Code	R/W	R

Interface Settings

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

Network

Settings	Not Specified	Specified
Machine IPv4 Address	R/W	R
IPv4 Gateway Address	R/W	R
IPv6 Stateless Address Autoconfiguration	R/W	R
DNS Configuration	R/W	R
DDNS Configuration	R/W	R
IPsec	R/W	R
Domain Name	R/W	R
WINS Configuration	R/W	R
Effective Protocol	R/W	R
SMB Computer Name	R/W	R
SMB Work Group	R/W	R
Ethernet Speed	R/W	R
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
IEEE 802.1X Authentication for Ethernet	R/W	R
Restore IEEE 802.1X Authentication to Defaults	R/W	N/A

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

Settings	Not Specified	Specified
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
Key Counter Management	R/W	R
External Charge Unit Management	R/W	R

Settings	Not Specified	Specified
Enhanced External Charge Unit Management	R/W	R
Extended Security	R/W	R
Program / Change / Delete LDAP Server	R/W	R
Auto Off Setting	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
Program / Change / Delete Realm	R/W	R

Some settings under "Extended Security" are not allowed for general users to specify.

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

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.

Note

- Settings that are not in the list can only be viewed, regardless of whether "Available Settings" has been specified.

Settings	Not Specified	Specified
Colour Registration	R/W	N/A

Adjustment Settings for Operators

Users authorized by user authentication can access all adjustment settings for operators.

Tray Paper 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.

Note

- Settings that are not in the list can only be viewed, regardless of whether "Available Settings" has been specified.

Settings	Not Specified	Specified
Tray Paper Settings: Tray 1	R/W	R
Tray Paper Settings: Tray 2	R/W	R
Tray Paper Settings: Tray 3	R/W	R
Tray Paper Settings: Tray 4	R/W	R
Tray Paper Settings: Tray 5	R/W	R
Tray Paper Settings: Tray 6	R/W	R
Tray Paper Settings: Interposer Upper Tray	R/W	R
Tray Paper Settings: Interposer Lower Tray	R/W	R
Paper Library	R/W*1	R
Custom Paper	R/W*2	R

*1 Saved Paper Library cannot be deleted. For details, contact your service representative.

*2 Advanced Settings cannot be changed. For details, 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.

Note

- Settings that are not in the list can only be viewed, regardless of whether "Available Settings" has been specified.

Home

Settings	Not Specified	Specified
Reset Device	R/W	N/A

System

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

Paper

Settings	Not Specified	Specified
Tray 1: Select Tray Paper Settings	R/W	R
Tray 1: Tray Paper Settings	R/W	R
Tray 2: Select Tray Paper Settings	R/W	R
Tray 2: Tray Paper Settings	R/W	R
Tray 3: Select Tray Paper Settings	R/W	R
Tray 3: Tray Paper Settings	R/W	R
Tray 4: Select Tray Paper Settings	R/W	R
Tray 4: Tray Paper Settings	R/W	R
Tray 5: Select Tray Paper Settings	R/W	R
Tray 5: Tray Paper Settings	R/W	R
Tray 6: Select Tray Paper Settings	R/W	R
Tray 6: Tray Paper Settings	R/W	R
Interposer Upper Tray: Paper Size	R/W	R
Interposer Upper Tray: Custom Paper Size	R/W	R
Interposer Lower Tray: Paper Size	R/W	R
Interposer Lower Tray: Custom Paper Size	R/W	R

Custom Paper

Settings	Not Specified	Specified
Program/Change	R/W	N/A
Delete	R/W	N/A

Date/Time

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

Timer

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

Logs

Settings	Not Specified	Specified
Collect Job Logs	R/W	R
Job Log Collect Level	R/W	R
Collect Access Logs	R/W	R
Access Log Collect Level	R/W	R
Encrypt Logs	R/W	R

Settings	Not Specified	Specified
Delete All Logs	R/W	N/A

E-mail

Settings	Not Specified	Specified
Administrator E-mail Address	R/W	R
Reception Protocol	R/W	R
E-mail Reception Interval	R/W	R
E-mail Storage in Server	R/W	R
SMTP Server Name	R/W	R
SMTP Port No.	R/W	R
SMTP Authentication	R/W	R
SMTP Auth. E-mail Address	R/W	R
SMTP Auth. User Name	R/W	N/A
SMTP Auth. Password	R/W	N/A
SMTP Auth. Encryption	R/W	R
POP before SMTP	R/W	R
POP E-mail Address	R/W	R
POP User Name	R/W	N/A
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

Settings	Not Specified	Specified
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

The passwords for "SMTP Auth. Password" and "POP Password" can only be entered but not changed.

User Authentication Management

Settings	Not Specified	Specified
User Authentication Management	R/W	R
User Code Authentication - User Code Authentication Settings	R/W	R
Basic Authentication - Basic Authentication Settings	R/W	R
Windows Authentication - Windows Authentication Settings	R/W	R
Windows Authentication - Group Settings for Windows Authentication	R/W	R
LDAP Authentication - LDAP Authentication Settings	R/W	R
Integration Server Authentication - Integration Server Authentication Settings	R/W	R
Integration Server Authentication - Group Settings for Integration Server Authentication	R/W	R

LDAP Server

Settings	Not Specified	Specified
Program/Change/Delete	R/W	N/A

Interface

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

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

User privileges are as follows:

- Abbreviations in the table heads

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

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

- Abbreviations in the table columns

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

  R (Read) = Reading only.

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

Note

- Settings that are not in the list can only be viewed, regardless of whether "Available Settings" has been specified.

Interface

Settings	Not Specified	Specified
Ethernet Security	R/W	R
Ethernet Speed	R/W	R

Network

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

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

User privileges are as follows:

- Abbreviations in the table heads

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

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

- Abbreviations in the table columns

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

  R (Read) = Reading only.

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

Note

- Settings that are not in the list can only be viewed, regardless of whether "Available Settings" has been specified.

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

Settings	Not Specified	Specified
DNS Server	R/W	R
RSH/RCP	R/W	R
FTP	R/W	R
sftp	R/W	R

IPv6

Settings	Not Specified	Specified
IPv6	R/W	R
Host Name	R/W	R
Domain Name	R/W	R
Stateless Address	R/W	R
Manual Configuration Address	R/W	R
DHCPv6-lite	R/W	R
DDNS	R/W	R
Default Gateway Address	R/W	R
DNS Server	R/W	R
RSH/RCP	R/W	R
FTP	R/W	R
sftp	R/W	R

SMB

Settings	Not Specified	Specified
SMB	R/W	R
Workgroup Name	R/W	R

Settings	Not Specified	Specified
Computer Name	R/W	R
Comment	R/W	R
Notify Print Completion	R/W	R

Bonjour

Settings	Not Specified	Specified
Bonjour	R/W	R
Computer Name	R/W	R
Location	R/W	R

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.

Note

- Settings that are not in the list can only be viewed, regardless of whether "Available Settings" has been specified.

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

Trademarks

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

Bonjour and Mac OS are trademarks of Apple Inc., registered in the U.S. and other countries.

LINUX® is the registered trademark of Linus Torvalds in the U.S. and other countries.

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

RED HAT is a registered trademark of Red Hat, Inc.

Solaris is a trademark or registered trademark of Sun Microsystems, Inc. in the United States and other countries.

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 XP are as follows:

  Microsoft® Windows® XP Professional Edition

  Microsoft® Windows® XP Home Edition

  Microsoft® Windows® XP Media Center Edition

  Microsoft® Windows® XP Tablet PC Edition

- The product names of Windows Vista are as follows:

  Microsoft® Windows Vista® Ultimate

  Microsoft® Windows Vista® Business

  Microsoft® Windows Vista® Home Premium

  Microsoft® Windows Vista® Home Basic

  Microsoft® Windows Vista® Enterprise

- The product names of Windows 7 are as follows:

  Microsoft® Windows® 7 Home Premium

  Microsoft® Windows® 7 Professional

  Microsoft® Windows® 7 Ultimate

Microsoft® Windows® 7 Enterprise

- The product names of Windows Server 2003 are as follows:

  Microsoft® Windows Server® 2003 Standard Edition

  Microsoft® Windows Server® 2003 Enterprise Edition

- The product names of Windows Server 2003 R2 are as follows:

  Microsoft® Windows Server® 2003 R2 Standard Edition

  Microsoft® Windows Server® 2003 R2 Enterprise Edition

- The product names of Windows Server 2008 are as follows:

  Microsoft® Windows Server® 2008 Standard

  Microsoft® Windows Server® 2008 Enterprise

- The product names of Windows Server 2008 R2 are as follows:

  Microsoft® Windows Server® 2008 R2 Standard

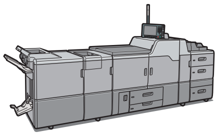
  Microsoft® Windows Server® 2008 R2 Enterprise

INDEX

MEMO

MEMO

Operating Instructions Security Reference



EN (US) M044-7537