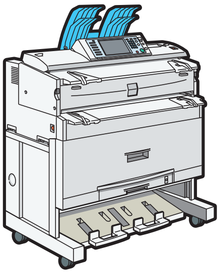
3406WD
GWD3006
LW426
Aficio™ MP W3601

Operating Instructions
Security Reference



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

TABLE OF CONTENTS

3. Configuring User Authentication

4. Protecting Data from Information Leaks

5. Securing Information Sent over the Network or Stored on Hard Disk

6. Managing Access to the Machine

7. Enhanced Network Security

8. Specifying the Extended Security Functions

9. Troubleshooting

10. 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 CD-ROMs provided, and how to replace paper, toner, and other consumables.

Troubleshooting

Provides a guide for resolving common usage-related problems.

Copy and Document Server Reference

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

Printer Reference

Explains Printer functions and operations.

Scanner Reference

Explains Scanner functions and operations.

Network and System Settings Reference

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

Security Reference

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

VM Card Extended Feature Settings Device Reference

Explains how to set up the extended features settings with the machine.

VM Card Extended Feature Settings Web Reference

Explains how to set up the extended features settings using Web Image Monitor.

Other manuals

- Unix Supplement
- Quick Reference Copy Guide
- Quick Reference Printer Guide
- Quick Reference Scanner Guide

Note

- Manuals provided are specific to machine types.
- For "UNIX Supplement", please visit our Web site or consult an authorized dealer. This manual includes descriptions of functions and settings that might not be available on this machine.
- The following software products are referred to using general names:

Product name	General name
DeskTopBinder Lite and DeskTopBinder Professional *[1]	DeskTopBinder
ScanRouter EX Professional *[1] and ScanRouter EX Enterprise *[1]	the ScanRouter delivery software
Remote Communication Gate S Pro for @Remote Enterprise *[1] and Remote Communication Gate S *[1]	Remote Communication Gate S

*1 Optional

Notice

Important

In no event will the company be liable for direct, indirect, special, incidental, or consequential damages as a result of handling or operating the machine.

For good copy quality, the manufacturer recommends that you use genuine toner from the manufacturer.

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

How to Read This Manual

Symbols

This manual uses the following symbols:

★ 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.**

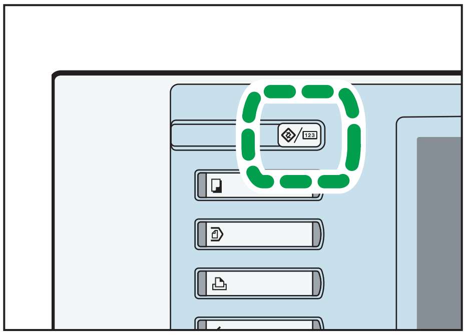
1. To prevent this machine being stolen or willfully damaged, etc., install it in a secure location.
2. Purchasers of this machine must make sure that people who use it do so appropriately, in accordance with operations determined by the machine administrator and supervisor. If the administrator or supervisor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

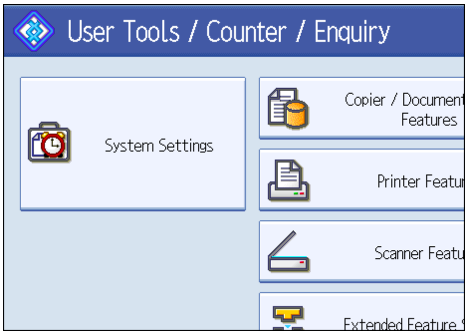
Enabling security

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

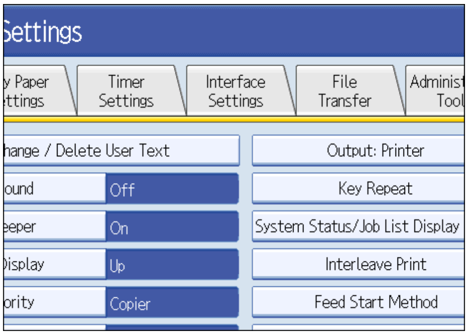


CAU012S

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



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



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 "Using Web Image Monitor to Configure Administrator Authentication".

8. **On the Configuration screen, click [E-mail] under "Device Setting", and then specify the administrator address in "Administrator E-mail Address".**

9. **Install the device certificate.**

   For information on how to install the device certificate, see "Protection Using Encryption".

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

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

    For details about enabling SSL, see "Protection Using Encryption".

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

    For details about specifying administrators' user names and passwords, see "Registering the Administrator".

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

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

    You will be automatically logged out.

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

Enabling enhanced security

1. **Configure the security settings for the machine by following steps 1 to 11 in the previous section, "Enabling security".**

2. **To use only the ports that have high security, set [Network Security Level] to [Level 2].**

   If [Network Security Level] is set to [Level 2], some functions will be unavailable.

   For details, see "Specifying Network Security Level" and "Enabling and Disabling Protocols".

3. **In Web Image Monitor, log in to the machine as the network administrator and set [FTP], which has weak security, to [Inactive] and also set [SNMPv3 Function] to [Inactive].**

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

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

5. **Press [System Settings].**

6. **Press [Administrator Tools].**
7. **Press [Extended Security].**
8. **If you are not using [@Remote Service], set [@Remote Service] to [Prohibit].**

   For details about "Update Firmware", see the following "Firmware Update Cautions".
9. **Press [OK].**
10. **Press the [User Tools/Counter] key.**
11. **Disconnect this machine from the administrator-only access network, and then connect it to the general usage network environment.**

Firmware Update Cautions

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

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

Reference

- p.35 "Using Web Image Monitor to Configure Administrator Authentication"
- p.186 "Protection Using Encryption"
- p.30 "Registering the Administrator"
- p.179 "Specifying Network Security Level"
- p.172 "Enabling and Disabling Protocols"

Enhanced Security

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

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

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

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

Authentication and Access Limits

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

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

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

For details about the administrator, see "Administrators".

For details about the user, see "Users".

Encryption Technology

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

Reference

- p.23 "Administrators"
- p.37 "Users"

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, such as copying and printing.

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, such as copying and printing.

File Creator (Owner)

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

Registered User

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

Administrator Authentication

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

User Authentication

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

The user's login user name and password, as well as such personal information items as e-mail address, 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 "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 "Basic Authentication".

Specifying Which Functions are Available

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

Reference

- p.39 "Configuring User Authentication"
- p.45 "Basic Authentication"
- p.143 "Limiting Available Functions"

Ensuring Information Security

Printing Confidential files

Using the printer's Locked Print, you can store files in the machine as confidential files and then print them. You can print a file using the machine's control panel and collect it on the spot to prevent others from seeing it. For details about printing confidential files, see "Printing a Confidential Document".

Protecting Stored Files from Unauthorized Access

You can specify who is allowed to use and access scanned files and the files in Document Server. You can prevent activities such as the printing of stored files by unauthorized users. For details about protecting stored files from unauthorized access, see "Configuring Access Permissions for Stored Files".

Protecting Stored Files from Theft

You can specify who is allowed to use and access scanned files and the files in Document Server. You can prevent activities such as the sending and downloading of stored files by unauthorized users.

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

Preventing Data Leaks Due to Unauthorized Transmission

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

You can also limit the direct entry of destinations to prevent files from being sent to destinations not registered in the Address Book. For details about preventing data leaks due to unauthorized transmission, see "Preventing Information Leakage Due to Unauthorized Transmission".

Using S/MIME to Protect E-mail Transmission

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

Protecting Registered Information in the Address Book

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

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

Managing Log Files

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

To transfer the log data, Remote Communication Gate S is required. For details about managing log files, see "Managing Log Files".

Encrypting Data on the Hard Disk

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

Reference

- p.89 "Printing a Confidential Document"
- p.95 "Configuring Access Permissions for Stored Files"
- p.107 "Preventing Information Leakage Due to Unauthorized Transmission"
- p.109 "Using S/MIME to Protect E-mail Transmission"
- p.117 "Protecting the Address Book"

- p.145 "Managing Log Files"
- p.121 "Encrypting Data on the Hard Disk"
- p.127 "Deleting Data on the Hard Disk"

Limiting and Controlling Access

Preventing Modification or Deletion of Stored Data

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

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

Preventing Modification of Machine Settings

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

Register the administrators so that users cannot change the administrator settings. For details about preventing modification of machine settings, see "Preventing 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 "Limiting Available Functions".

Reference

- p.95 "Configuring Access Permissions for Stored Files"
- p.137 "Preventing Changes to Machine Settings"
- p.143 "Limiting Available Functions"

Enhancing Network Security

Preventing Unauthorized Access

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

Encrypting Transmitted Passwords

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

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

Safer Communication Using SSL, SNMPv3 and IPsec

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

Reference

- p.171 "Preventing Unauthorized Access"
- p.183 "Encrypting Transmitted Passwords"
- p.186 "Protection Using Encryption"
- p.195 "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. Administrators cannot use functions such as copying and printing. To use these functions, the administrator must be authenticated as the user.

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

Important

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

Reference

- p.30 "Registering the Administrator"
- p.261 "Supervisor Operations"
- p.37 "Users"

User Administrator

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

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

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

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

Machine Administrator

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

Network Administrator

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

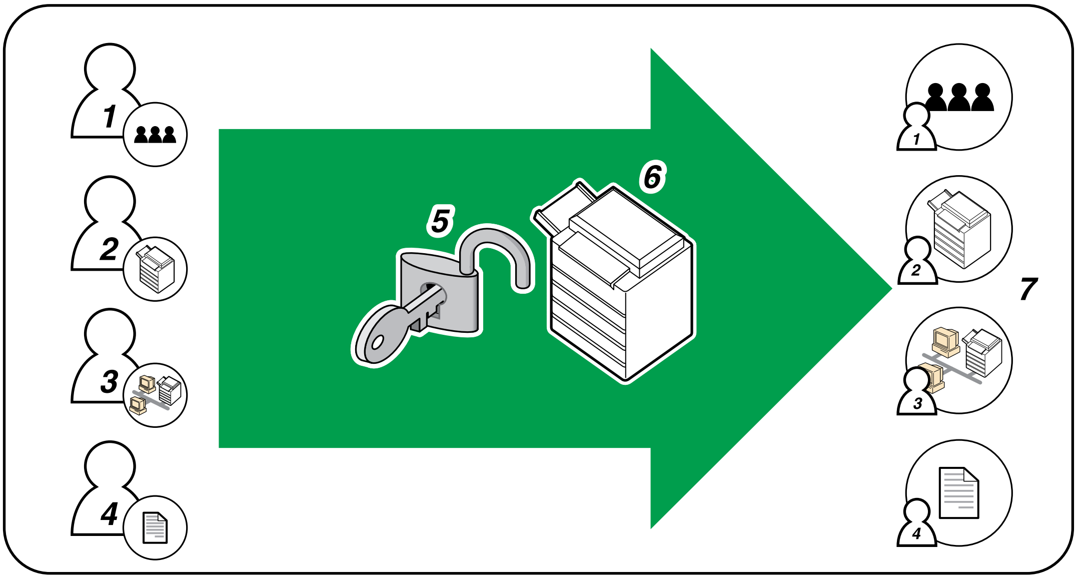
Supervisor

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

About Administrator Authentication

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

For details about each administrator, see "Administrators".



1. **User Administrator**

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

2. **Machine Administrator**

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

3. **Network Administrator**

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

4. **File Administrator**

   This administrator manages permission to access stored files. You can specify passwords for Locked Print files stored in Document Server so that only authorized users can view and change them.

5. **Authentication**

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

6. **This machine**

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

Reference

- p.23 "Administrators"

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 "Registering the Administrator".

You can specify the login user name, login password, and encryption password for each administrator. The encryption password is used for encrypting data transmitted via SNMPv3. It is also used by applications such as SmartDeviceMonitor for Admin that use SNMPv3. Administrators are limited to managing the machine's settings and controlling user access, so they cannot use functions such as copying and printing. To use these functions, the administrator must register as a user in the Address Book and then be authenticated as the user. Specify administrator authentication, and then specify user authentication. For details about specifying authentication, see "Configuring User Authentication".

Note

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

Reference

- p.30 "Registering the Administrator"
- p.37 "Configuring User Authentication"

Specifying Administrator Privileges

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

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

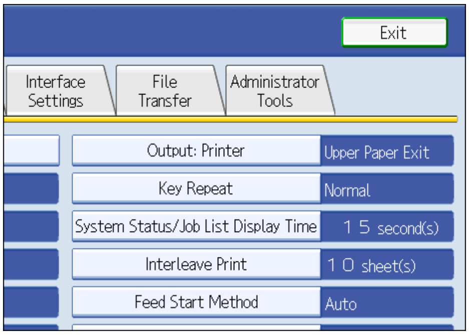
The defaults are "admin" for the login name and blank for the password. For details about changing the administrator password using the supervisor's authority, see "Supervisor Operations".

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

Important

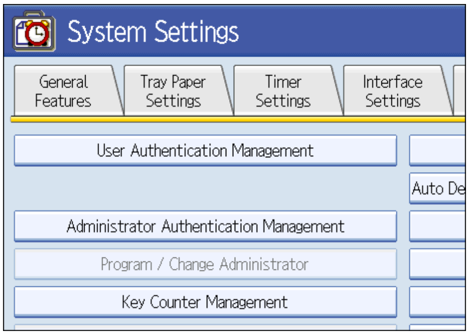
- If you have enabled "Administrator Authentication Management", make sure not to forget the administrator login user name and login password. If an administrator login user name or login password is forgotten, a new password must be specified using the supervisor's authority. For instructions on registering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

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



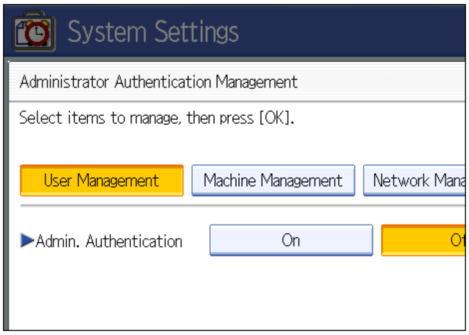
Output: Printer	Upper Paper Exit
Key Repeat	Normal
System Status/Job List Display Time	1 5 second(s)
Interleave Print	1 0 sheet(s)
Feed Start Method	Auto

4. Press [Administrator Authentication 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.**

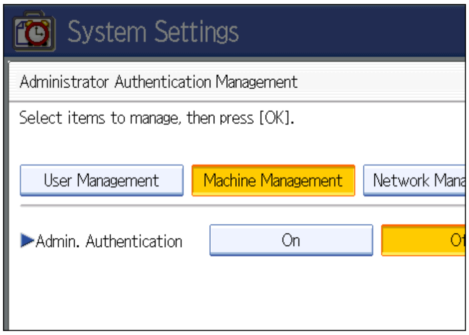


System Settings

Administrator Authentication Management

Select items to manage, then press [OK].

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



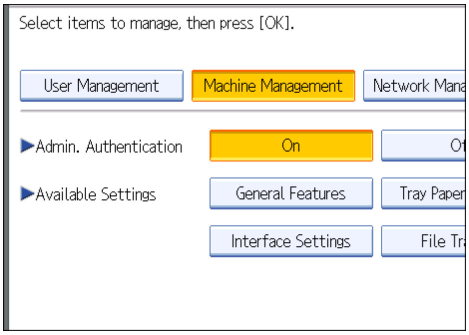
System Settings

Administrator Authentication Management

Select items to manage, then press [OK].

"Available Settings" appears.

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



Select items to manage, then press [OK].

The selected settings will be unavailable to users.

"Available Settings" varies depending on the administrator.

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

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

8. **Press [OK].**

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

Reference

- p.261 "Supervisor Operations"
- p.33 "Logging in Using Administrator Authentication"
- p.34 "Logging out Using Administrator Authentication"
- p.143 "Limiting Available Functions"

Registering the Administrator

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

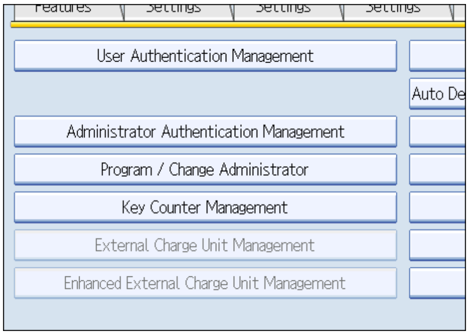
The sharing of administrator tasks eases the burden on individual administrators while also limiting unauthorized operation by a single administrator. You can register up to four login user names (Administrators 1-4) to which you can grant administrator privileges.

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

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

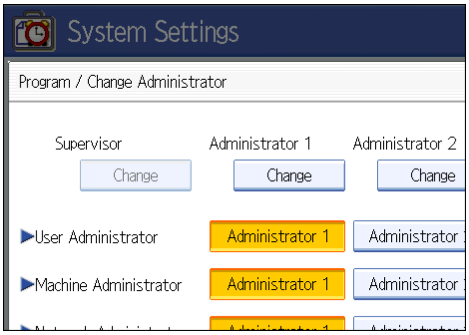
For details about logging in and logging out with administrator authentication, see "Logging in Using Administrator Authentication" and "Logging out Using Administrator Authentication".

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

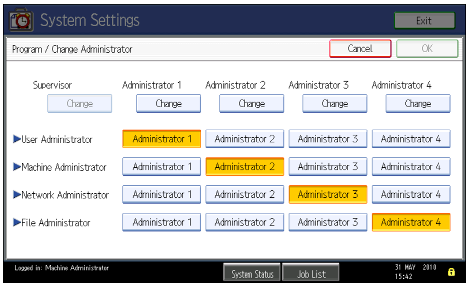

Features
Settings
Settings
Settings
User Authentication Management
Auto De
Administrator Authentication Management
Program / Change Administrator
Key Counter Management
External Charge Unit Management
Enhanced External Charge Unit Management

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

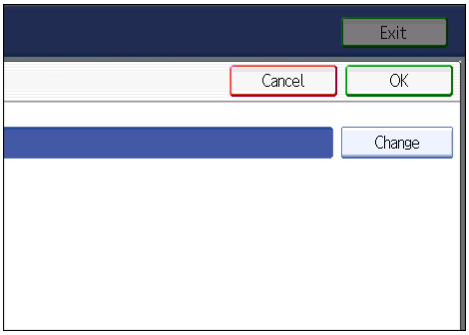
5. In the line for the administrator whose authority you want to specify, press [Administrator 1], [Administrator 2], [Administrator 3] or [Administrator 4], and then press [Change].



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

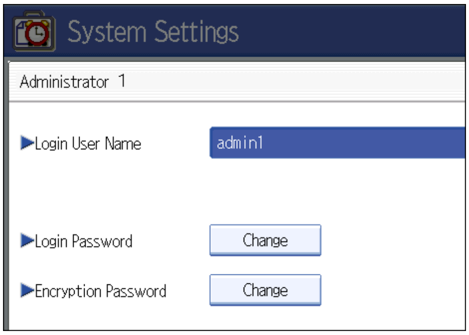


6. Press [Change] for the login user name.



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

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



System Settings

Administrator 1

▶Login User Name admin1

▶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 "Specifying the Extended Security Functions".

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

    You will be automatically logged out.

15. **Press the [User Tools/Counter] 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 "Specifying the Extended Security Functions".

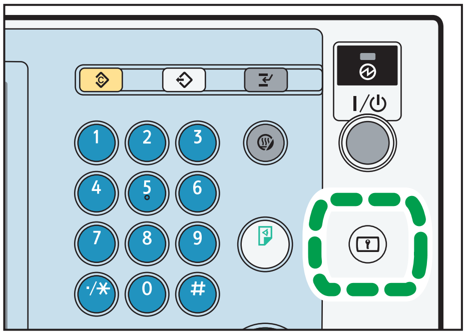
Reference

- p.33 "Logging in Using Administrator Authentication"
- p.34 "Logging out Using Administrator Authentication"
- p.221 "Specifying the Extended Security Functions"

Logging in Using Administrator Authentication

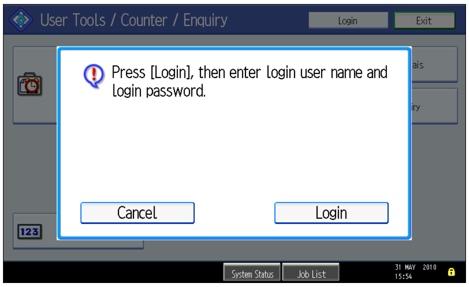
If administrator authentication has been specified, log in using an administrator's user name and password. This section describes how to log in. When you log in with a user name that has multiple administrator privileges, one of the administrator privileges associated with that name is displayed.

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



CAN001S

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



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

3. **Press [Login].**

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

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

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

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

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

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

Note

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

- If you log in using administrator authority, the name of the administrator logging 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/Counter] key to change the default.

Logging out Using Administrator Authentication

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

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

Changing the Administrator

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

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

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

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

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

Reference

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

Using Web Image Monitor to Configure Administrator Authentication

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

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

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

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

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

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

Note

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

Specifying Administrative Settings Using Web Printing Tool

Administrative settings for GL/2 & TIFF Filter can be changed, system logs can be collected, etc. using Web Printing Tool.

1. **Open a Web browser.**
2. **Enter "http://(the machine's IP address)/webprint/index.html" in the address bar.**

   The top page of Web Printing Tool appears.

3. **Click the link to the administrator's page in the header area on the upper-right hand of the screen.**

   To change administrative settings (GL/2 & TIFF Initial Configuration), click 🔧.

   To collect system logs, click 📄.

4. **Enter the administrator password, and then click [OK].**
5. **Make settings as desired.**

Note

- When logging in to Web Printing Tool, the default password is set as "admin". To differentiate from the administrator password set in the machine, use a password unique to Web Printing Tool for login.
- If the password authentication fails three times in a row, you will be returned to the Web Printing Tool top page. To return to the login page again, click the link in the header area on the upper-right hand of the screen.
- The password can be changed in "Change Administrator Password:" under the "Administrator Password" tab on the administrator settings (GL/2 & TIFF Initial Configuration) screen. Click [On] to activate the password entry fields. The password must be 4 to 8 characters long.
- For details about Web Printing Tool, see the Web Printing Tool Help.

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, such as copying and printing. Users are managed using the personal information in the machine's Address Book, and can use only the functions they are permitted to access by administrators. By enabling user authentication, you can allow only people registered in the Address Book to use the machine. Users can be managed in the Address Book by the user administrator. For details about administrator, see "Administrators". For details about 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.**

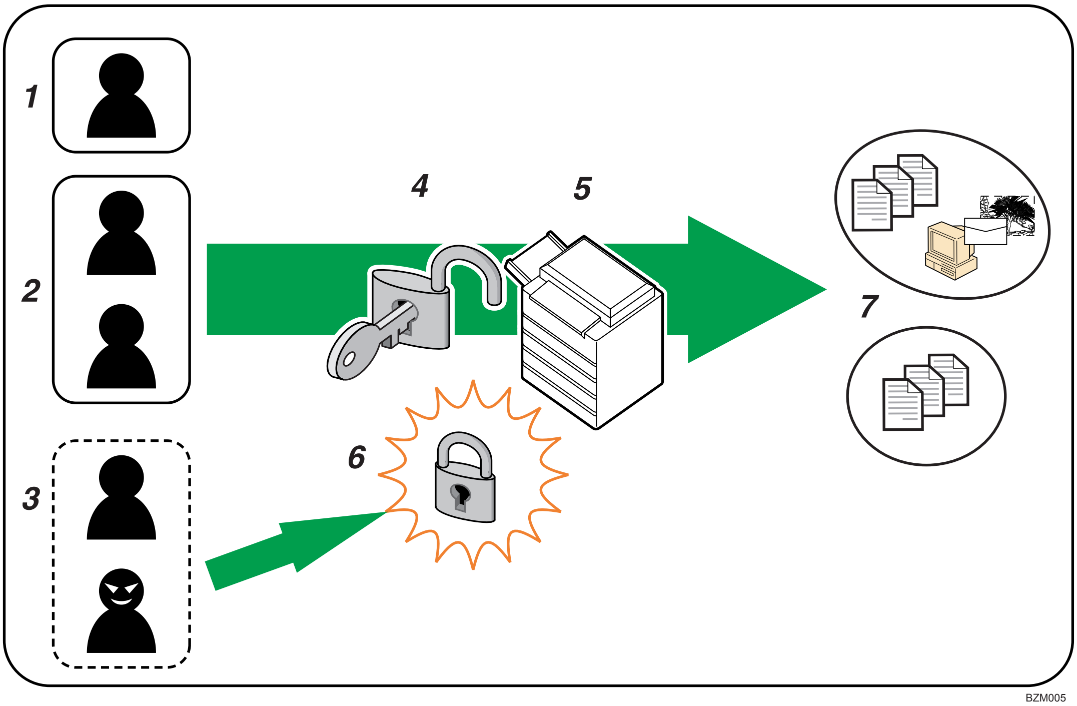
Reference

- p.23 "Administrators"

About User Authentication

This machine has an authentication function to prevent unauthorized access.

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



1. **User**

   A user performs normal operations on the machine, such as copying and printing.

2. **Group**

   A group performs normal operations on the machine, such as copying and printing.

3. **Unauthorized User**

4. **Authentication**

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

5. **This Machine**

6. **Access Limit**

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

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

Configuring User Authentication

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

Administrator authentication	Specify administrator privileges. Register administrators.
User authentication	Specify user authentication. Five types of user authentication are available: • User Code Authentication • Basic Authentication • Windows Authentication • LDAP Authentication • Integration Server Authentication

Note

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

Reference

- p.27 "Enabling Administrator Authentication"
- p.40 "Enabling User Authentication"
- p.27 "Specifying Administrator Privileges"
- p.30 "Registering the Administrator"
- p.41 "User Code Authentication"
- p.45 "Basic Authentication"
- p.52 "Windows Authentication"
- p.64 "LDAP Authentication"
- p.72 "Integration Server Authentication"

Enabling User Authentication

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

Note

- User Code authentication is used for authenticating on the basis of a user code, and Basic authentication, Windows authentication, LDAP authentication, and Integration Server authentication are used for authenticating individual users.
- You can specify User Code authentication without specifying administrator authentication.
- A user code account, that has no more than eight digits and is used for User Code authentication, can be carried over and used as a login user name even after the authentication method has switched from User Code authentication to Basic authentication, Windows authentication, LDAP authentication, or Integration Server authentication. In this case, since the User Code authentication does not have a password, the login password is set as blank.
- When authentication switches to an external authentication method (Windows authentication, LDAP authentication, or Integration Server authentication), authentication will not occur, unless the external authentication device has the carried over user code account previously registered. However, the user code account will remain in the Address Book of the machine despite an authentication failure.
- From a security perspective, when switching from User Code authentication to another authentication method, we recommend that you delete accounts you are not going to use, or set up a login password. For details about deleting accounts, see "Deleting a Registered Name", Network and System Settings Reference. For details about changing passwords, see "Specifying Login User Names and Passwords".
- You cannot use more than one authentication method at the same time.
- User authentication can also be specified via Web Image Monitor. For details, see Web Image Monitor Help.
- When enabling user authentication, all users in the address book can access and change all the settings on the GL/2 & TIFF screen.

Reference

- p.48 "Specifying Login User Names and Passwords"

User Code Authentication

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

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

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

Important

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

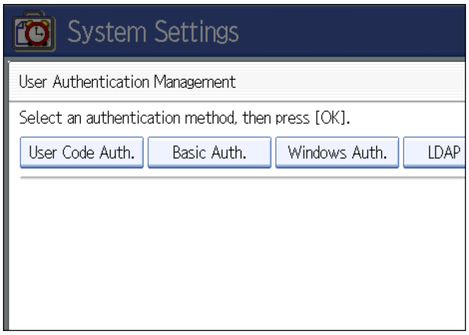
Specifying User Code Authentication

This can be specified by the machine administrator.

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

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

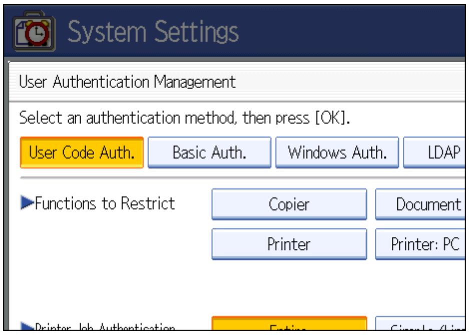
   System Settings

   User Authentication Management

   Select an authentication method, then press [OK].

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

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



System Settings

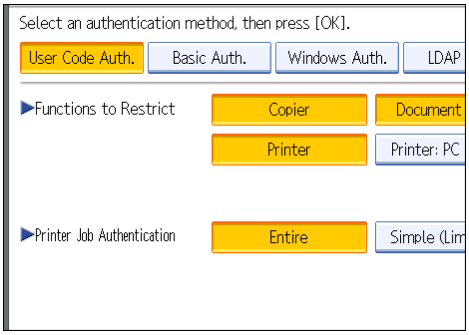
User Authentication Management

Select an authentication method, then press [OK].

The selected settings will be unavailable to users.

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

7. **Select the "Printer Job Authentication" level.**



Select an authentication method, then press [OK].

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

If you select [Entire] or [Simple (All)], proceed to "Selecting Entire or Simple (All)".

If you select [Simple (Limitation)], proceed to "Selecting Simple (Limitation)".

For a description of the printer job authentication levels, see "Printer Job Authentication".

Reference

- p.33 "Logging in Using Administrator Authentication"
- p.34 "Logging out Using Administrator Authentication"
- p.143 "Limiting Available Functions"
- p.43 "Selecting Entire or Simple (All)"
- p.43 "Selecting Simple (Limitation)"
- p.79 "Printer Job Authentication"

Selecting Entire or Simple (All)

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

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

1. **Press [Entire] or [Simple (All)].**
2. **Press [OK].**
3. **Press [Exit].**

   A confirmation message appears.

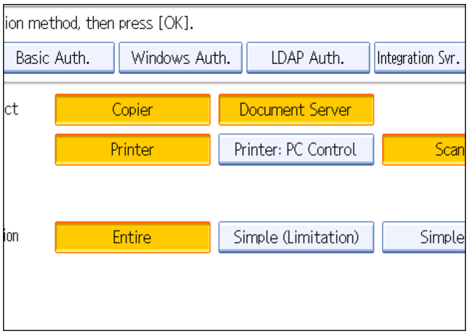
   If you press [Yes], you will be automatically logged out.
4. **Press the [User Tools/Counter] key.**

Selecting Simple (Limitation)

If you select [Simple (Limitation)], you can specify clients for which printer job authentication is not required. Specify [USB: Simple] and the clients' IPv4 address range in which printer job authentication is not required. Specify this setting if you want to print using unauthenticated printer drivers or without any printer driver. Authentication is required for printing with non-specified devices.

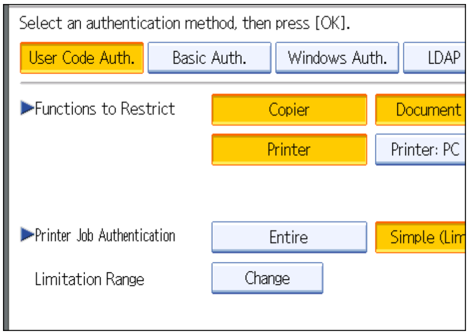
If you select [Simple (Limitation)], you can print even with unauthenticated printer drivers or devices. Specify this setting if you want to print with a printer driver or device that cannot be identified by the machine or if you do not require authentication for printing. However, note that, because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

1. **Press [Simple (Limitation)].**



ion method, then press [OK].

2. **Press [Change].**



Select an authentication method, then press [OK].

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

   You can specify the IPv4 address range to which this setting is applied, and whether or not to apply the setting to the USB interface.

4. **Press [Exit].**
5. **Press [OK].**
6. **Press [Exit].**

   A confirmation message appears.

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

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

Basic Authentication

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

Reference

- p.47 "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".

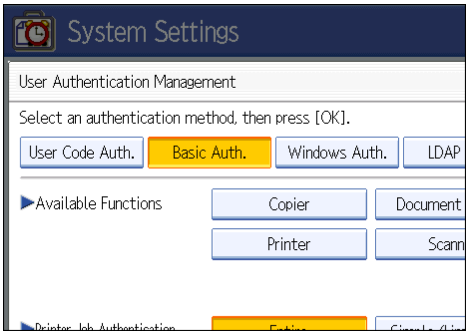
This can be specified by the machine administrator.

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

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

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

   System Settings

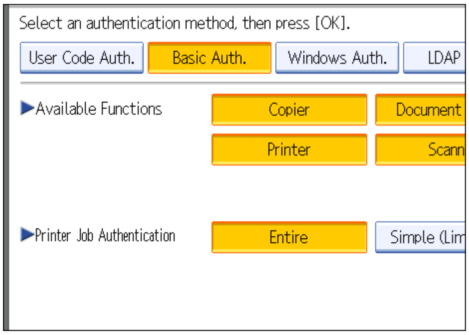
   User Authentication Management

   Select an authentication method, then press [OK].

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

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

7. **Select the "Printer Job Authentication" level.**



Select an authentication method, then press [OK].

If you select [Entire] or [Simple (All)], proceed to "Selecting Entire or Simple (All)".

If you select [Simple (Limitation)], proceed to "Selecting Simple (Limitation)".

For a description of the printer job authentication levels, see "Printer Job Authentication".

Reference

- p.33 "Logging in Using Administrator Authentication"
- p.34 "Logging out Using Administrator Authentication"
- p.143 "Limiting Available Functions"
- p.46 "Selecting Entire or Simple (All)"
- p.47 "Selecting Simple (Limitation)"
- p.79 "Printer Job Authentication"

Selecting Entire or Simple (All)

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

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

1. **Press [Entire] or [Simple (All)].**
2. **Press [OK].**
3. **Press [Exit].**

   A confirmation message appears.

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

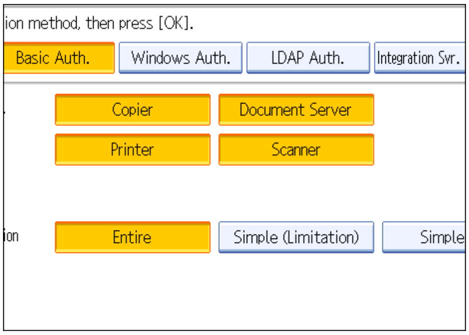
4. **Press the [User Tools/Counter] key.**

Selecting Simple (Limitation)

If you select [Simple (Limitation)], you can specify clients for which printer job authentication is not required. Specify [USB: Simple] and the clients' IPv4 address range in which printer job authentication is not required. Specify this setting if you want to print using unauthenticated printer drivers or without any printer driver. Authentication is required for printing with non-specified devices.

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

1. **Press [Simple (Limitation)].**



ion method, then press [OK].

2. **Press [Change].**
3. **Specify the range in which [Simple (Limitation)] is applied to "Printer Job Authentication".**

   You can specify the IPv4 address range to which this setting is applied, and whether or not to apply the setting to the USB interface.

4. **Press [Exit].**
5. **Press [OK].**
6. **Press [Exit].**

   A confirmation message appears.

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

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

Authentication Information Stored in the Address Book

This can be specified by the user administrator.

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

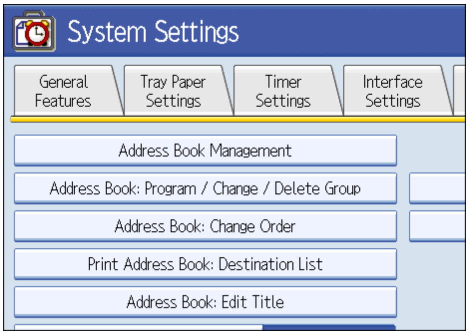
Reference

- p.33 "Logging in Using Administrator Authentication"
- p.34 "Logging out Using Administrator Authentication"
- p.143 "Limiting Available Functions"

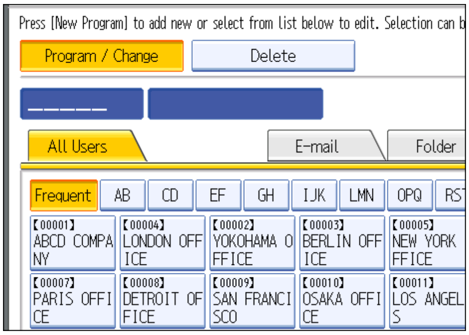
Specifying Login User Names and Passwords

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

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

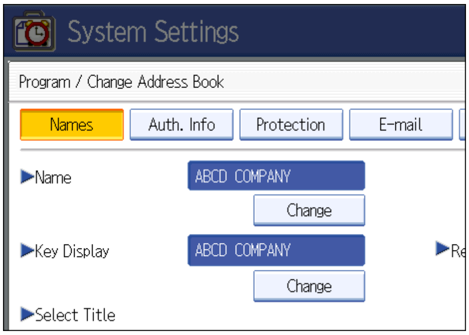


5. **Select the user.**

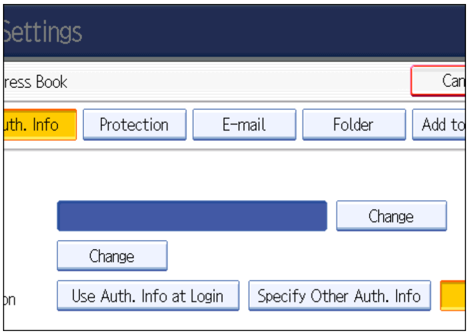


Press [New Program] to add new or select from list below to edit. Selection can b

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

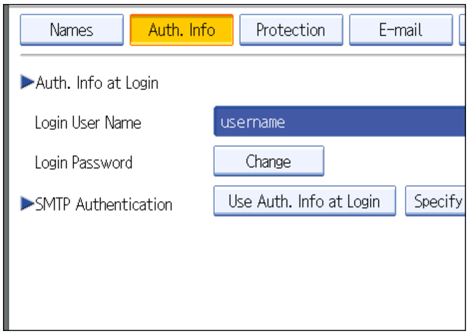


7. **Press [Change] for "Login User Name".**



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

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



▶Auth. Info at Login

Login User Name: username

Login Password: Change

▶SMTP Authentication: Use Auth. Info at Login | Specify

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

Note

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

Reference

- p.221 "Specifying the Extended Security Functions"

Specifying Login Details

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

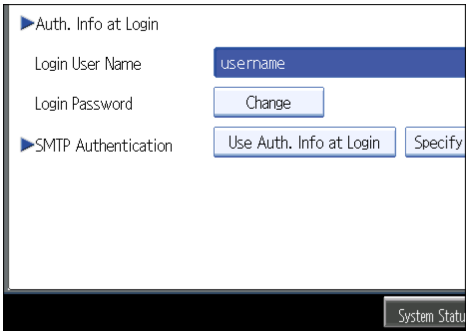
If you do not want to use the login user name and password specified in "Address Book Management" for "SMTP Authentication", "Folder Authentication", or "LDAP Authentication", see "Registering Folders" and "Registering SMTP and LDAP Authentication", Network and System Settings Reference.

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

Important

- **When using "Use Auth. Info at Login" for "SMTP Authentication", "Folder Authentication", or "LDAP Authentication", a user name other than "other", "admin", "supervisor" or "HIDE***" must be specified. The symbol "***" represents any character.**
- **To use "Use Auth. Info at Login" for "SMTP Authentication", a login password up to 128 characters in length must be specified.**

1. **Press the [User Tools/Counter] key.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [Address Book Management].**
5. **Select the user.**
6. **Press [Auth. Info].**
7. **Select [Use Auth. Info at Login] in "SMTP Authentication".**



▶Auth. Info at Login

Login User Name: username

Login Password: Change

▶SMTP Authentication: Use Auth. Info at Login | Specify

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

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

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

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

Reference

- p.48 "Specifying Login User Names and Passwords"

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. Obtaining user information can prevent the use of false identities because the sender's address (From:) is determined by the authentication system when scanned data is sent.

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, such as the user's e-mail address, is automatically registered in the machine. If user information on the server is changed, information registered in the machine may be overwritten when authentication is performed.**
- **Users managed in other domains are subject to user authentication, but they cannot obtain items such as e-mail addresses.**
- **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.**
- **If Kerberos authentication and SSL encryption are set at the same time, e-mail addresses cannot be obtained.**

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.
- When accessing the machine subsequently, you can use all the functions available to your group and to you as an individual user.
- Users who are registered in multiple groups can use all the functions available to those groups.
- A user registered in two or more global groups can use all the functions available to members of those groups.
- If the "Guest" account on the Windows server is enabled, even users not registered in the domain controller can be authenticated. When this account is enabled, users are registered in the Address Book and can use the functions available under "*Default Group".

Specifying Windows Authentication

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

This can be specified by the machine administrator.

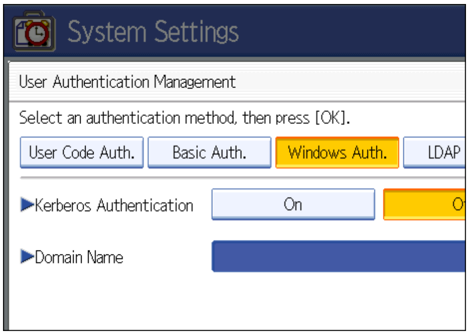
For details about logging in and logging out with administrator authentication, see "Logging in Using Administrator Authentication" and "Logging out Using Administrator Authentication".

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

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



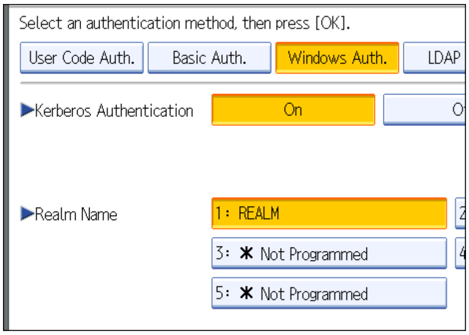
System Settings

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.**

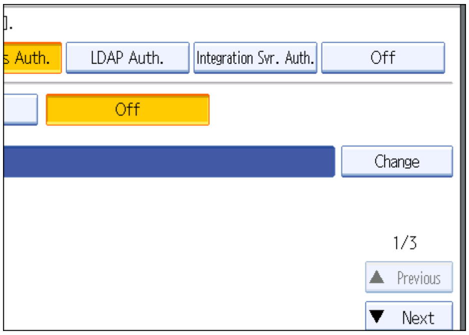


Select an authentication method, then press [OK].

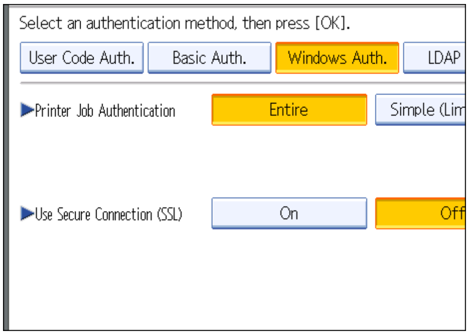
To enable Kerberos authentication, a realm must be registered beforehand. The realm name must be registered in capital letters. For details about registering a realm, see "Programming the Realm", Network and System Settings Reference.

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. **Select the "Printer Job Authentication" level.**



Select an authentication method, then press [OK].

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

If you select [Entire] or [Simple (All)], proceed to "Selecting Entire or Simple (All)".

If you select [Simple (Limitation)], proceed to "Selecting Simple (Limitation)".

For a description of the printer job authentication levels, see "Printer Job Authentication".

Reference

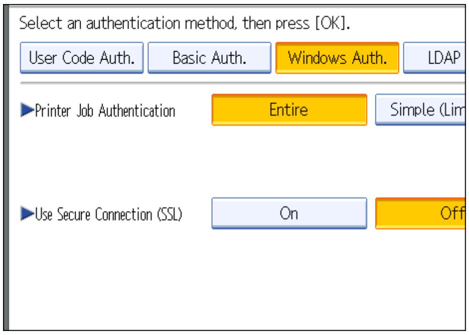
- p.33 "Logging in Using Administrator Authentication"
- p.34 "Logging out Using Administrator Authentication"
- p.55 "Selecting Entire or Simple (All)"
- p.58 "Selecting Simple (Limitation)"
- p.79 "Printer Job Authentication"

Selecting Entire or Simple (All)

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

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

1. **Press [Entire] or [Simple (All)].**
2. **Press [On] for "Use Secure Connection (SSL)".**



Select an authentication method, then press [OK].

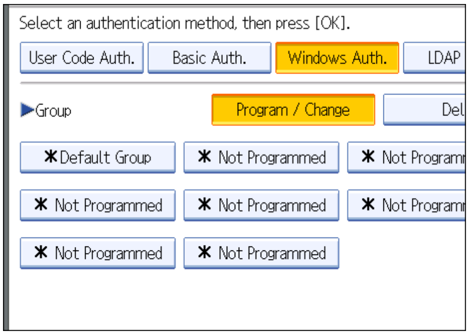
If you are not using secure sockets layer (SSL) for authentication, press [Off].

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

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

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

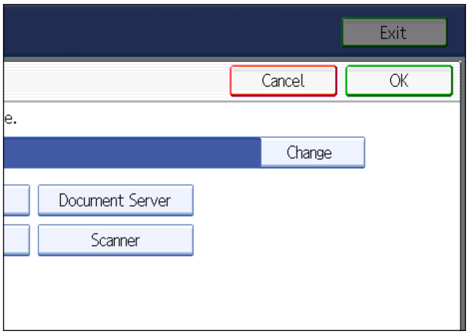
3. **Under "Group", press [Program / Change], and then press [* Not Programmed].**



Select an authentication method, then press [OK].

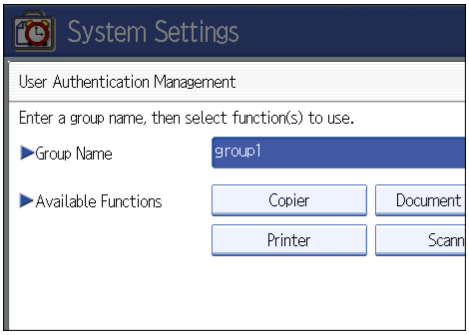
If this item is not visible, press [▼Next] to display more settings.

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



5. **Press [OK].**

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



User Authentication Management

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

▶Group Name: group1

▶Available Functions

Windows Authentication will be applied to the selected functions.

Users can use the selected functions only.

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

7. **Press [OK] twice.**

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

A confirmation message appears.

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

Note

- Under Windows Authentication, you can select whether or not to use secure sockets layer (SSL) authentication.
- To automatically register user information such as e-mail addresses under Windows authentication, it is recommended that communication between the machine and domain controller be encrypted using SSL.
- Under Windows Authentication, you do not have to create a server certificate unless you want to automatically register user information such as e-mail addresses using SSL.

Reference

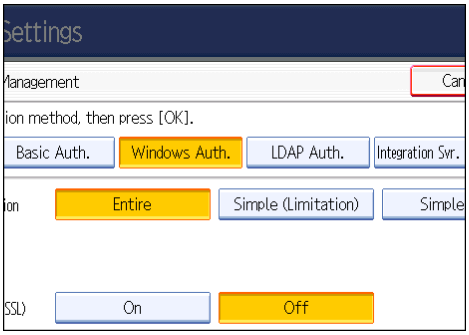
- p.143 "Limiting Available Functions"

Selecting Simple (Limitation)

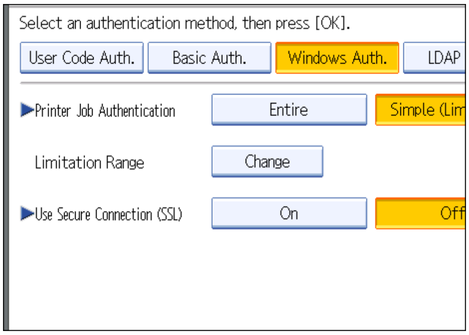
If you select [Simple (Limitation)], you can specify clients for which printer job authentication is not required. Specify [USB: Simple] and the clients' IPv4 address range in which printer job authentication is not required. Specify this setting if you want to print using unauthenticated printer drivers or without any printer driver. Authentication is required for printing with non-specified devices.

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

1. **Press [Simple (Limitation)].**



2. **Press [Change].**

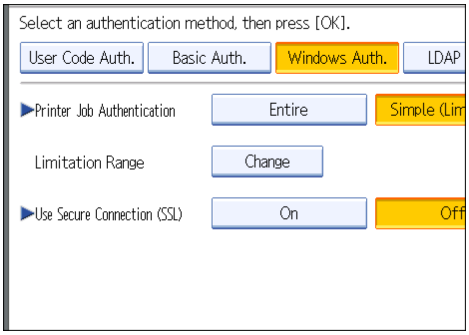

Select an authentication method, then press [OK].
User Code Auth.
Basic Auth.
Windows Auth.
LDAP
Printer Job Authentication
Entire
Simple (Lim
Limitation Range
Change
Use Secure Connection (SSL)
On
Off

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

   You can specify the IPv4 address range to which this setting is applied, and whether or not to apply the setting to the USB interface.

4. **Press [Exit].**

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



Select an authentication method, then press [OK].

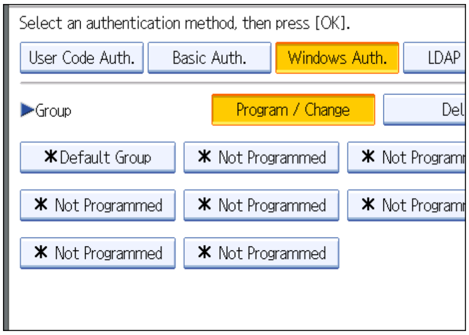
If you are not using secure sockets layer (SSL) for authentication, press [Off].

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

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

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

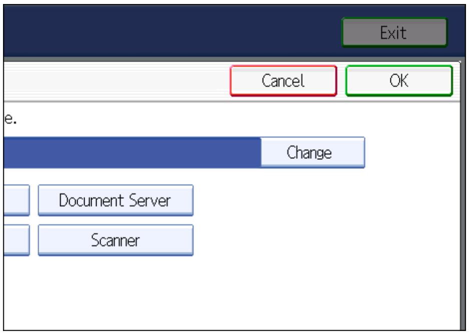
6. **Under "Group", press [Program / Change], and then press [* Not Programmed].**



Select an authentication method, then press [OK].

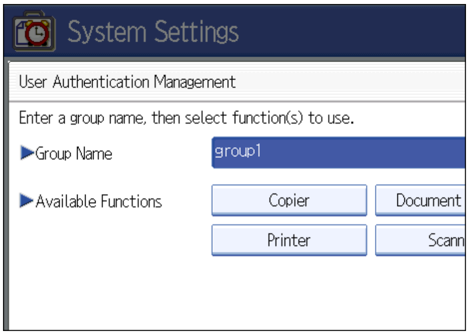
If this item is not visible, press [▼Next] to display more settings.

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



8. **Press [OK].**

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


System Settings

User Authentication Management

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

▶Group Name: group1

Windows Authentication will be applied to the selected functions.

Users can use the selected functions only.

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

10. **Press [OK] twice.**

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

A confirmation message appears.

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

Note

- Under Windows Authentication, you can select whether or not to use secure sockets layer (SSL) authentication.
- To automatically register user information such as e-mail addresses under Windows authentication, it is recommended that communication between the machine and domain controller be encrypted using SSL.
- Under Windows Authentication, you do not have to create a server certificate unless you want to automatically register user information such as e-mail addresses using SSL.

Reference

- p.143 "Limiting Available Functions"

Installing Internet Information Services (IIS) and Certificate Services

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

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

Install the components, and then create the server certificate.

If they are not installed, install them as follows:

Windows Server 2008 R2 is used to illustrate the procedure.

1. **On the [Start] menu, point to [Administrator Tools], and then click [Server Manager].**
2. **Click [Roles] in the left column, click [Add Roles] from the [Action] menu.**
3. **Click [Next>].**
4. **Select the "Web Server (IIS)" and "Active Directory Certificate Services" check boxes, and then click [Next>].**
5. **Read the content information, and then click [Next>].**
6. **Confirm that [Certification Authority] is checked, and then click [Next>].**
7. **Select [Enterprise], and then click [Next>].**
8. **Select [Root CA], and then click [Next>].**
9. **Select [Create a new private key], and then click [Next>].**
10. **Select a cryptographic service provider, key length, and hash algorithm to create a new private key, and then click [Next>].**
11. **In "Common name for this CA:", enter the Certificate Authority name, and then click [Next>].**
12. **Select the validity period, and then click [Next>].**
13. **Leave the "Certificate database location:" and the "Certificate database log location:" settings set to their defaults, and then click [Next>].**
14. **Read the notes, and then click [Next>].**
15. **Select the role service you want to use, and then click [Next>].**
16. **Click [Install].**
17. **When the installation is complete, click [Close].**
18. **Close [Server Manager].**

Creating the Server Certificate

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

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)

Install the device certificate using Web Image Monitor.

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

Enter the device certificate contents issued by the certificate authority.

Installation of the certificate is especially necessary for users who want to print via IPP -SSL from Windows Vista/7, Windows Server 2008/2008 R2.

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

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

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

   The network administrator can log in.

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

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

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

   In the certificate 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 [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. Otherwise, validation by the certificate authority will not be performed correctly. In this case, a warning message may appear when you try to add a printer using IPP-SSL under Windows Vista/7, Windows Server 2008/2008 R2 or when the destination user receives an e-mail with an S/MIME signature. A warning message might also appear if you attempt to access this machine through Web Image Monitor with SSL enabled. To enable authentication from the client computer, install the intermediate certificate on the client computer, and then reestablish connection.
- Intermediate certificates cannot be installed on this machine.

LDAP Authentication

Specify this authentication method when using the LDAP server to authenticate users who have their accounts on the LDAP server. Users cannot be authenticated if they do not have their accounts on the LDAP server. The Address Book stored in the LDAP server can be registered to the machine, enabling user authentication without first using the machine to register individual settings in the Address Book. When using LDAP authentication, to prevent the password information being sent over the network unencrypted, it is recommended that communication between the machine and LDAP server be encrypted using SSL. You can specify on the LDAP server whether or not to enable SSL. To do this, you must create a server certificate for the LDAP server. For details about creating a server certificate, see "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, such as the user's e-mail address, is automatically registered in the machine. If user information on the server is changed, information registered in the machine may be overwritten when authentication is performed.**
- **Under LDAP authentication, you cannot specify access limits for groups registered in the LDAP server.**
- **Enter the user's login user name using up to 128 characters, and 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.**
- **If using ActiveDirectory in LDAP authentication when Kerberos authentication and SSL are set at the same time, e-mail addresses cannot be obtained.**

Operational Requirements for LDAP Authentication

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

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

Select either Kerberos, DIGEST, or Cleartext authentication.

- User Name

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

- Password

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

Note

- When you select Cleartext authentication, LDAP Simplified authentication is enabled. Simplified authentication can be performed with a user attribute (such as cn, or uid), instead of the DN.
- 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.
- The reference function is not available for SSL servers when a search for LDAP is in progress.

Reference

- p.62 "Creating the Server Certificate"

Specifying LDAP Authentication

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

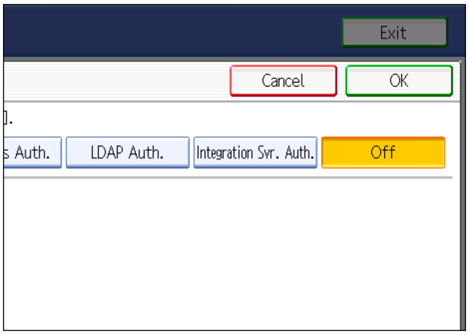
This can be specified by the machine administrator.

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

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

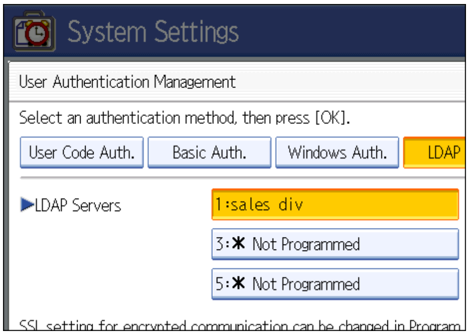
   If this item is not visible, press [▼Next] to display more settings.

5. **Select [LDAP Auth.].**



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

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



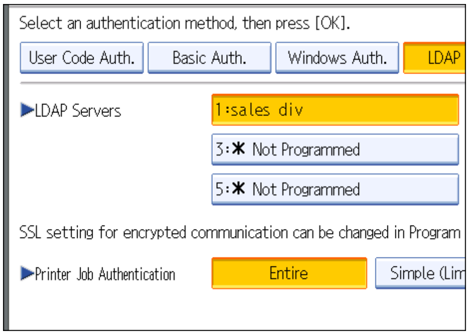
Select an authentication method, then press [OK].

▶LDAP Servers: 1:sales div

SSL setting for encrypted communication can be changed in Program

7. **Select the "Printer Job Authentication" level.**

   You can specify the IPv4 address range to which this setting is applied, and whether or not to apply the setting to the USB interface.



Select an authentication method, then press [OK].

▶LDAP Servers: 1:sales div

SSL setting for encrypted communication can be changed in Program

▶Printer Job Authentication: Entire

If you select [Entire] or [Simple (All)], proceed to "Selecting Entire or Simple (All)".

If you select [Simple (Limitation)], proceed to "Selecting Simple (Limitation)".

For a description of the printer job authentication levels, see "Printer Job Authentication".

Reference

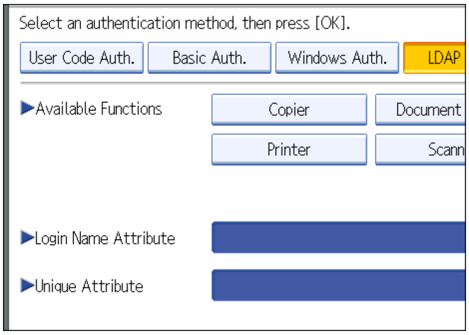
- p.33 "Logging in Using Administrator Authentication"
- p.34 "Logging out Using Administrator Authentication"
- p.67 "Selecting Entire or Simple (All)"
- p.69 "Selecting Simple (Limitation)"
- p.79 "Printer Job Authentication"

Selecting Entire or Simple (All)

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

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

1. **Press [Entire] or [Simple (All)].**
2. **Select which of the machine's functions you want to permit.**



Select an authentication method, then press [OK].

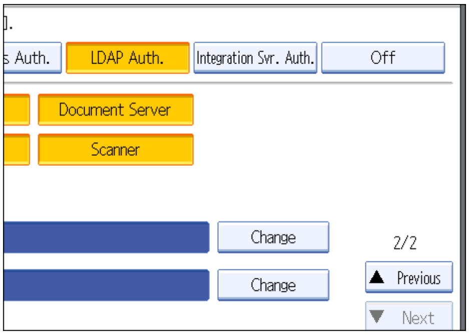
If this item is not visible, press [▼Next] to display more settings.

LDAP Authentication will be applied to the selected functions.

Users can use the selected functions only.

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

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



4. **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.

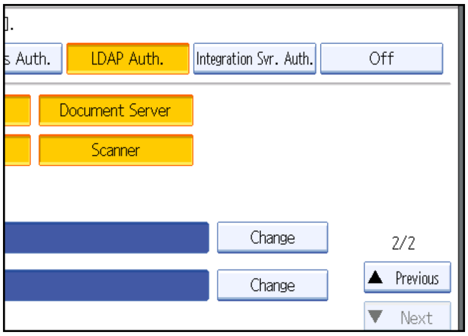
   To specify multiple login attributes, place a comma (,) between them. The search will return hits for either or both attributes.

   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.

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



6. **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.

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

   A confirmation message appears.

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

Reference

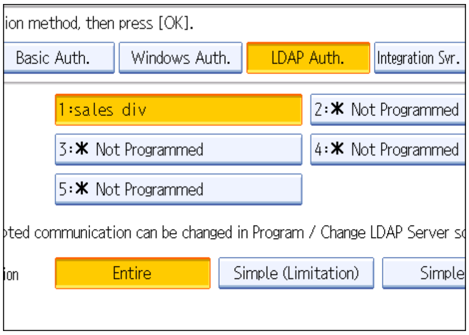
- p.143 "Limiting Available Functions"

Selecting Simple (Limitation)

If you select [Simple (Limitation)], you can specify clients for which printer job authentication is not required. Specify [USB: Simple] and the clients' IPv4 address range in which printer job authentication is not required. Specify this setting if you want to print using unauthenticated printer drivers or without any printer driver. Authentication is required for printing with non-specified devices.

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

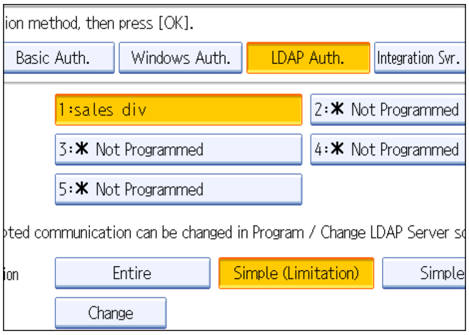
1. **Press [Simple (Limitation)].**



ion method, then press [OK].

ted communication can be changed in Program / Change LDAP Server s

2. **Press [Change].**



ion method, then press [OK].

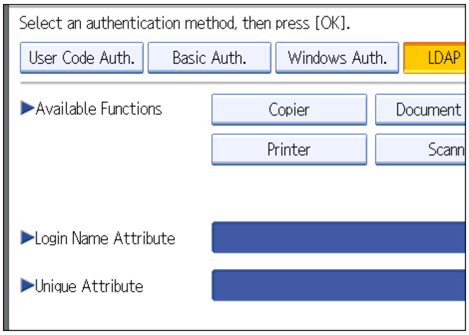
ted communication can be changed in Program / Change LDAP Server s

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

   You can specify the IPv4 address range to which this setting is applied, and whether or not to apply the setting to the USB interface.

4. **Press [Exit].**

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

   Select an authentication method, then press [OK].

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

   LDAP Authentication will be applied to the selected functions.

   Users can use the selected functions only.

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

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

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

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

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

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

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

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

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

9. **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.

10. **Press [OK].**

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

    A confirmation message appears.

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

Reference

- p.143 "Limiting Available Functions"

Integration Server Authentication

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

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

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

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

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

★ Important

- **During Integration Server Authentication, the data registered in the server, such as the user's e-mail address, is automatically registered in the machine.**
- **If user information on the server is changed, information registered in the machine may be overwritten when authentication is performed.**
- **The default administrator name for ScanRouter System and Remote Communication Gate S is "Admin". This is different from the default administrator name for the machine, which is "admin".**

Specifying Integration Server Authentication

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

This can be specified by the machine administrator.

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

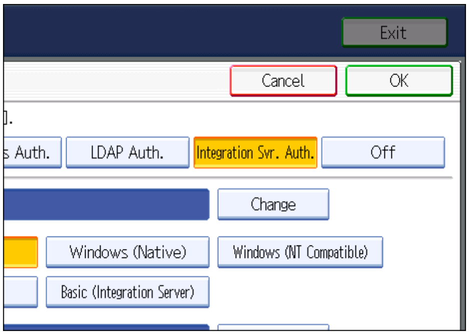
1. **Press the [User Tools/Counter] key.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [User Authentication Management].**

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

5. **Select [Integration Svr. Auth.].**

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

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

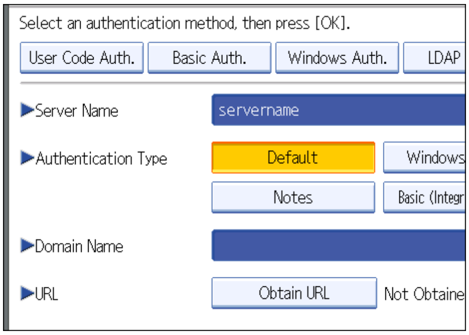


   Specify the name of the server for external authentication.

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

   Enter the IPv4 address or host name.

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



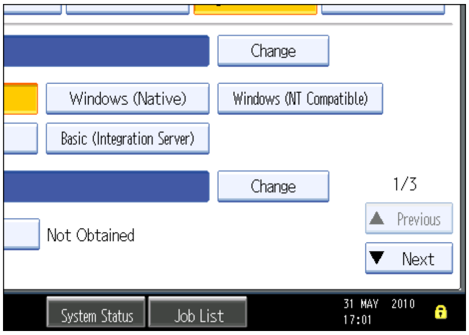
Select an authentication method, then press [OK].

▶Server Name: servername

▶Authentication Type: Default

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

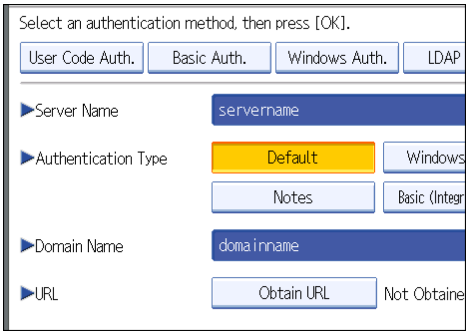
9. **Press [Change] for "Domain Name".**



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].**

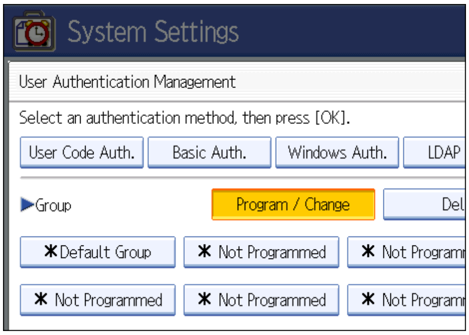
    In the "Authentication Type", if you have not registered a group, proceed to step 18.

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

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

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

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



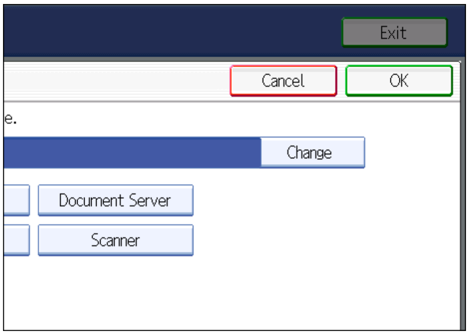
System Settings

User Authentication Management

Select an authentication method, then press [OK].

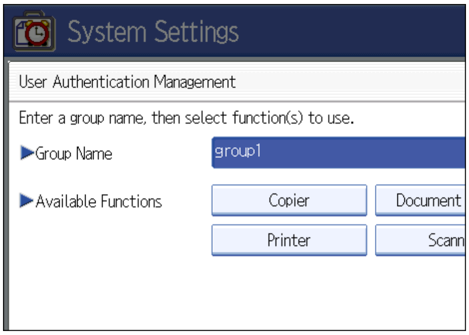
If this item is not visible, press [▼Next] to display more settings.

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



15. **Press [OK].**

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



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

Group Name: group1

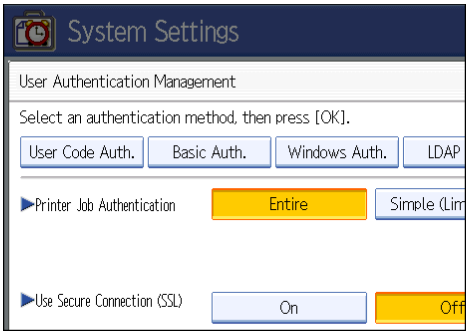
Authentication will be applied to the selected functions.

Users can use the selected functions only.

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

17. **Press [OK].**

18. **Select the "Printer Job Authentication" level.**



Select an authentication method, then press [OK].

Printer Job Authentication: Entire

Use Secure Connection (SSL): Off

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

If you select [Entire] or [Simple (All)], proceed to "Selecting Entire or Simple (All)".

If you select [Simple (Limitation)], proceed to "Selecting Simple (Limitation)".

For a description of the printer job authentication levels, see "Printer Job Authentication".

Reference

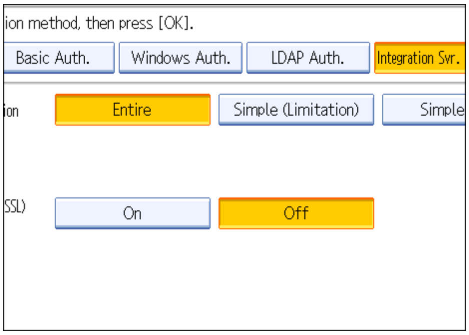
- p.33 "Logging in Using Administrator Authentication"
- p.34 "Logging out Using Administrator Authentication"
- p.143 "Limiting Available Functions"
- p.76 "Selecting Entire or Simple (All)"
- p.77 "Selecting Simple (Limitation)"
- p.79 "Printer Job Authentication"

Selecting Entire or Simple (All)

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

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

1. **Press [Entire] or [Simple (All)].**
2. **Press [On] for "Use Secure Connection (SSL)", and then press [OK].**



ion method, then press [OK].

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

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

A confirmation message appears.

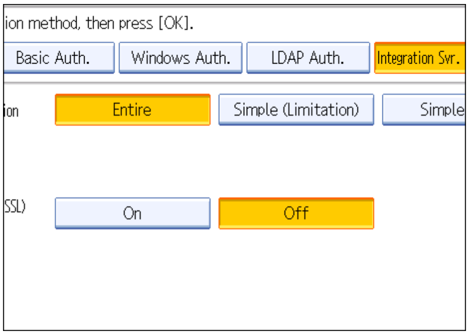
If you press [Yes], you will be automatically logged out.

Selecting Simple (Limitation)

If you select [Simple (Limitation)], you can specify clients for which printer job authentication is not required. Specify [USB: Simple] and the clients' IPv4 address range in which printer job authentication is not required. Specify this setting if you want to print using unauthenticated printer drivers or without any printer driver. Authentication is required for printing with non-specified devices.

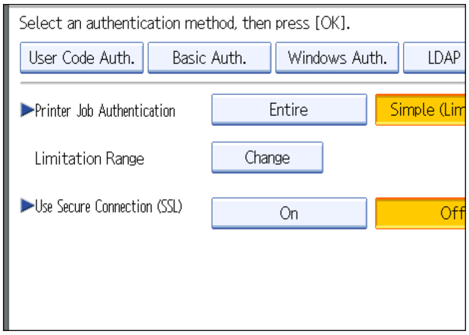
If you select [Simple (Limitation)], you can print even with unauthenticated printer drivers or devices. Specify this setting if you want to print with a printer driver or device that cannot be identified by the machine or if you do not require authentication for printing. However, note that, because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

1. **Press [Simple (Limitation)].**



ion method, then press [OK].

2. **Press [Change].**



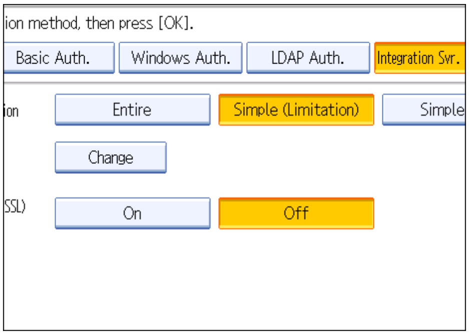
Select an authentication method, then press [OK].

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

   You can specify the IPv4 address range to which this setting is applied, and whether or not to apply the setting to the USB interface.

4. **Press [Exit].**

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



ion method, then press [OK].

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

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

A confirmation message appears.

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

Printer Job Authentication

This section explains the relationship between printer job authentication levels and printer job types.

Depending on the combination of printer job authentication level and printer job type, the machine may not print properly. Set an appropriate combination according to the operating environment.

When user authentication is disabled, printing is possible for all job types.

Printer Job Authentication Levels and Printer Job Types

User Authentication Management	Specified	Specified
Printer Job Authentication	Simple (All)	Entire
Printer Job Type 1	A	B
Printer Job Type 2	A	X
Printer Job Type 3	A	X
Printer Job Type 4	B	B

A: Printing is possible regardless of user authentication.

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

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

Printer Job Authentication

- Entire

  The machine authenticates all printer jobs and remote settings, and cancels jobs and settings that fail authentication.

  Printer Jobs: Job Reset

  Settings: Disabled

- Simple (All)

  The machine authenticates printer jobs and remote settings that have authentication information, and cancels the jobs and settings that fail authentication.

  Printer jobs and settings without authentication information are performed without being authenticated.

- Simple (Limitation)

  You can specify the range to apply [Simple (Limitation)] to by specifying [USB: Simple] and the client's IPv4 address.

Printer Job Types

1. The printer job contains user code information. Personal authentication information is not added to the printer job but the user code information is. This also applies to recovery/parallel printing using a PCL printer driver that does not support authentication.
2. The printer job does not contain user code information. Neither personal authentication information nor user code information is added to the printer job. This also applies to recovery/parallel printing using a PCL printer driver that does not support authentication.
3. A printer job or PDF file is sent from a host computer without a printer driver and is printed via LPR. Personal authentication information is not added to the printer job.
4. A PDF file is printed via ftp. Personal authentication is performed using the user ID and password used for logging in via ftp. However, the user ID and password are not encrypted.

Reference

- p.221 "Specifying the Extended Security Functions"

If User Authentication is Specified

When user authentication (User Code Authentication, Basic Authentication, Windows Authentication, LDAP Authentication, or Integration Server Authentication) is set, the authentication screen is displayed. 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 "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.

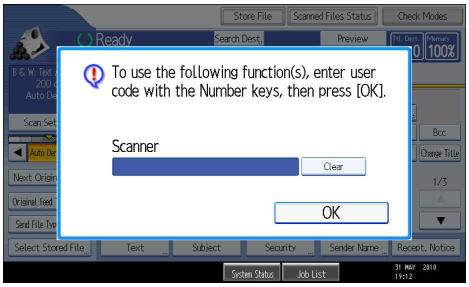
Reference

- p.86 "Auto Logout"

If User Code Authentication is Specified

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

The scanner screen is used as an example.



To use the following function(s), enter user code with the Number keys, then press [OK].

Scanner

Enter your user code.

Logging in Using the Control Panel

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

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

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

Note

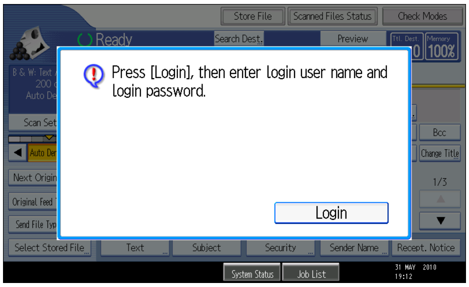
- To log out, do one of the following:
  - Press the operation switch.
  - Press the [Energy Saver] key after jobs are completed.
  - Press the [Clear/Stop] key and the [Clear Modes] key at the same time.

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].**

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

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

Logging out Using the Control Panel

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

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

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

Note

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

Logging in Using Web Image Monitor

This section explains how to log in to the machine via Web Image Monitor.

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

Note

- For user code authentication, enter a user code in "Login User Name", and then click [Login].

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.**

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

The top page of Web Image Monitor appears.

3. **Click [Login].**

   The machine administrator can log in.

   Enter the login user name and login password.

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

   The User Lockout Policy page appears.

5. **Set "Lockout" to [Active].**
6. **In the drop down menu, select the number of login attempts to permit before applying lockout.**
7. **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].**

   User Lockout Policy is set.

10. **Click [Logout].**

Canceling Password Lockout

This section explains how to cancel user password lockout. User password lockout is configured by the user administrator.

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

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

   The top page of Web Image Monitor appears.

3. **Click [Login].**

   The administrator or supervisor with unlocking privileges can log in.

   Enter the login user name and login password.

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

   The Address Book page appears.

5. **Select the locked out user's account.**
6. **Click [Change].**
7. **Set "Lockout" to [Inactive] under "Authentication Information".**
8. **Click [OK].**
9. **Click [Logout].**

Note

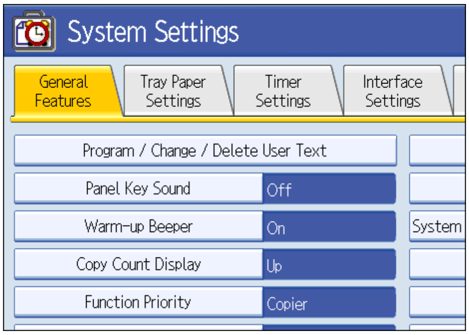
- You can cancel the administrator and supervisor password lockout by turning the power off and then turning it back on again, or by canceling the setting in [Program/Change Administrator] under [Configuration] in Web Image Monitor.

Auto Logout

This can be specified by the machine administrator. For details about logging in and logging out with administrator authentication, see "Logging in Using Administrator Authentication" and "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/Counter] key.**
2. **Press [System Settings].**
3. **Press [Timer Settings].**



System Settings

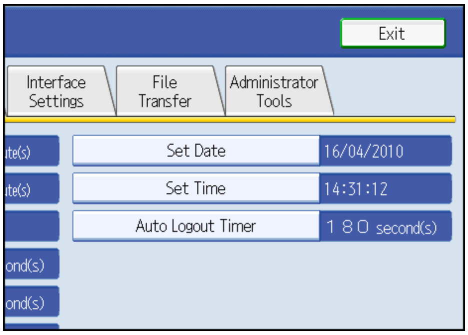
Panel Key Sound: Off

Warm-up Beeper: On

Copy Count Display: Up

Function Priority: Copier

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

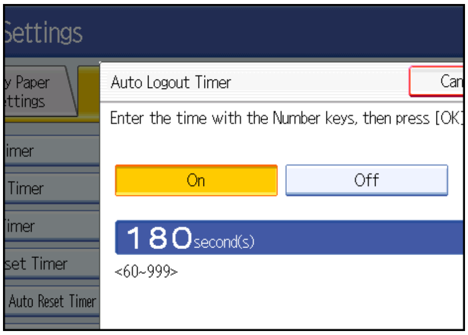


Set Date: 16/04/2010

Set Time: 14:31:12

Auto Logout Timer: 180 second(s)

5. **Select [On].**



Auto Logout Timer

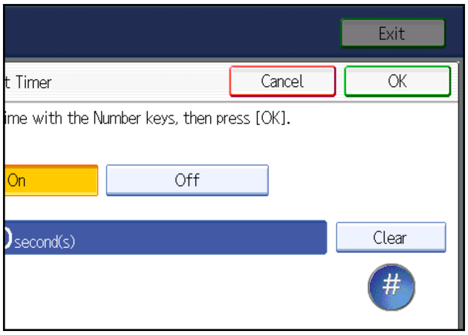
Enter the time with the Number keys, then press [OK]

180 second(s)

<60~999>

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/Counter] key.**

A confirmation message appears.

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

Note

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

Reference

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

Authentication Using an External Device

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

For details, contact your sales representative.

4. Protecting Data from Information Leaks

This chapter describes how to protect document data.

Printing a Confidential Document

Depending on the location of the machine, it is difficult to prevent unauthorized persons from viewing prints lying in the machine's output trays. When printing confidential documents, use the Locked Print function.

Locked Print

- Using the printer's Locked Print function, store files in the machine as Locked Print files and then print them from the control panel and retrieve them immediately, preventing others from viewing them.
- Confidential documents can be printed regardless of the User Authentication settings.

Note

- To store files temporarily, select [Stored Print] in the printer driver.

Specifying Locked Print File

Using the printer driver, specify a Locked Print file.

If User Code authentication has been enabled, you must enter the appropriate user code using the printer driver. For details about logging in, see the printer driver Help.

Locked Print is allowed even if user authentication is not yet configured. For configuring this setting, see "Locked Print", Printer Reference.

1. **Open the printing preferences dialog box.**
2. **In the "Job Type:" list, click [Locked Print].**
3. **Click [Details...].**
4. **Enter the user ID and password.**

   Enter the user ID using up to 8 alphanumeric characters.

   Enter the password using 4 to 8 numbers.

   The password entered here lets you use the Locked Print function.

   To print a Locked Print file, enter the same password on the control panel.

   The password is encrypted during data transmission.
5. **Click [OK].**
6. **Click [OK].**

7. **Print the locked document.**

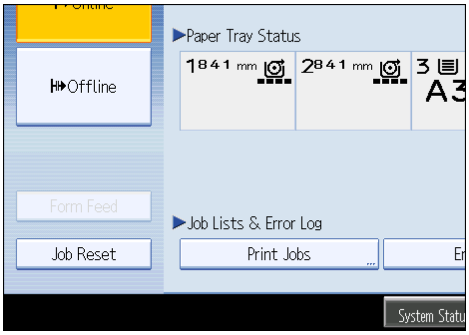
Printing a Locked Print File

To print a Locked Print file, you must be at the machine and print the file using the control panel.

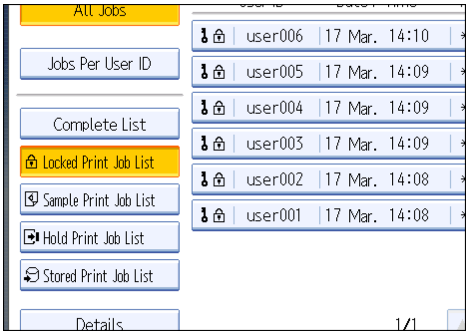
To print Locked Print files, the password is required. If you do not enter the correct password, you cannot print the files. The file administrator can change the user password if it is forgotten.

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

1. **Press the [Printer] key.**
2. **Press [Print Jobs].**



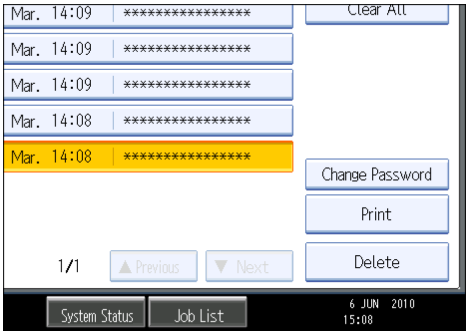
3. **Press [Locked Print Job List].**



🔒	user006	17 Mar. 14:10
🔒	user005	17 Mar. 14:09
🔒	user004	17 Mar. 14:09
🔒	user003	17 Mar. 14:09
🔒	user002	17 Mar. 14:08
🔒	user001	17 Mar. 14:08

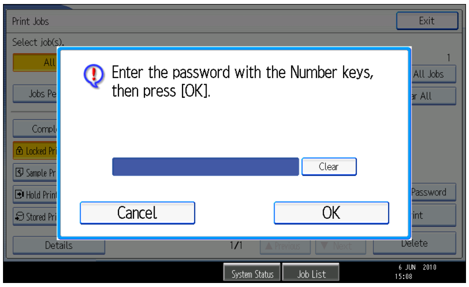
4. **Select the Locked Print file to print.**

5. **Press [Print].**



Mar. 14:09 ****************
Mar. 14:09 ****************
Mar. 14:09 ****************
Mar. 14:08 ****************
Mar. 14:08 ****************

6. **Enter the password for the stored file, and then press [OK].**



Enter the password with the Number keys, then press [OK].

Enter the password specified in step 4 of "Specifying a Locked Print File".

7. **Press [Yes].**

Note

- For details about logging in and logging out with user authentication, see "If User Authentication is Specified".

Reference

- p.81 "If User Authentication is Specified"

Deleting Locked Print Files

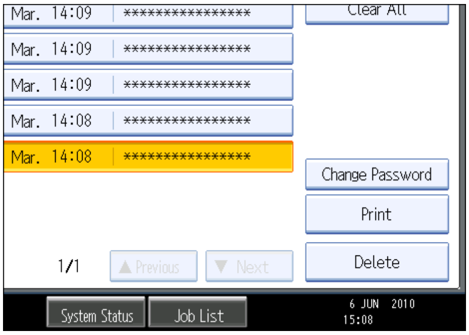
This can be specified by the file creator (owner).

To delete Locked Print files, you must enter the password for the files. If the password has been forgotten, ask the file administrator to change the password.

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

1. **Press the [Printer] key.**
2. **Press [Print Jobs].**
3. **Press [Locked Print Job List].**

4. **Select the file.**
5. **Press [Delete].**


Mar. 14:09 ****************
Mar. 14:09 ****************
Mar. 14:09 ****************
Mar. 14:08 ****************
Mar. 14:08 ****************
Clear All
Change Password
Print
Delete
1/1
▲ Previous
▼ Next
System Status
Job List
6 JUN 2010
15:08

6. **Enter the password of the Locked Print file, and then press [OK].**

   The password entry screen does not appear if the file administrator is logged in.

7. **Press [Yes].**

Note

- You can configure this machine to delete stored files automatically by setting the "Auto Delete Temporary Print Jobs" option to [On]. For details about "Auto Delete Temporary Print Jobs", see "System", Printer Reference.
- Locked Print files can also be deleted by the file administrator.

Changing the Password of a Locked Print File

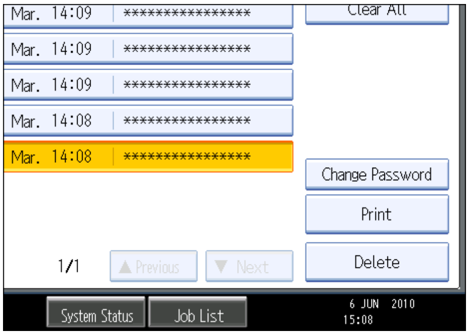
This can be specified by the file creator (owner) or file administrator.

If the password has been forgotten, the file administrator changes the password to restore access.

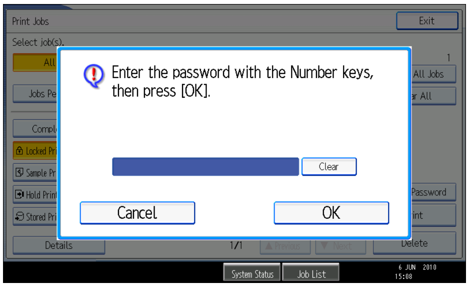
This can also be specified via Web Image Monitor. For details, see Web Image Monitor Help.

1. **Press the [Printer] key.**
2. **Press [Print Jobs].**
3. **Press [Locked Print Job List].**
4. **Select the file.**

5. **Press [Change Password].**

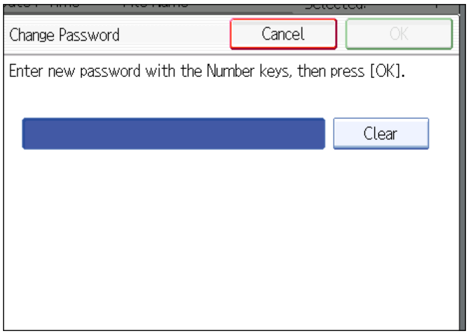

Mar. 14:09 ****************
Mar. 14:09 ****************
Mar. 14:09 ****************
Mar. 14:08 ****************
Mar. 14:08 ****************
Clear All
Change Password
Print
Delete
1/1
▲ Previous
▼ Next
System Status
Job List
6 JUN 2010
15:08

6. **Enter the password for the stored file, and then press [OK].**


Enter the password with the Number keys, then press [OK].

The password entry screen will not appear if the file administrator is logged in.

7. **Enter the new password for the stored file, and then press [OK].**


Change Password

Enter new password with the Number keys, then press [OK].

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

The password entry screen does not appear if the file administrator is logged in.

Unlocking a Locked Print File

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

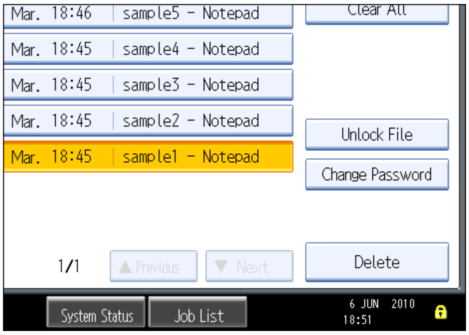
"Enhance File Protection" is one of the extended security functions. For details about this and other extended security functions, see "Specifying the Extended Security Functions".

Only the file administrator can unlock files. For details about logging in and logging out with administrator authentication, see "Logging in Using Administrator Authentication" and "Logging out Using Administrator Authentication".

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

1. **Press the [Printer] key.**
2. **Press [Print Jobs].**
3. **Press [Locked Print Job List].**
4. **Select the file.**

   The ⊘ icon appears next to a file locked by the Enhance File Protection function.
5. **Press [Unlock File].**



Mar. 18:46 | sample5 - Notepad
Mar. 18:45 | sample4 - Notepad
Mar. 18:45 | sample3 - Notepad
Mar. 18:45 | sample2 - Notepad
Mar. 18:45 | sample1 - Notepad

6. **Press [Yes].**

   The ⊘ icon disappears.

Note

- You can use the same procedure to unlock stored print files also.

Reference

- p.221 "Specifying the Extended Security Functions"
- p.33 "Logging in Using Administrator Authentication"
- p.34 "Logging out Using Administrator Authentication"

Configuring Access Permissions for Stored Files

This section describes how to specify access permissions for stored files.

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

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

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

Access Permission

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

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

Password for Stored Files

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

Note

- For details about assigning a password to a stored file, see "Specifying Passwords for Stored Files".
- Files can be stored by any user who is allowed to use Document Server, copy function, or scanner function.
- Using Web Image Monitor, you can check the content of stored files. For details, see Web Image Monitor Help.
- Access permission to documents sent from the printer driver and stored on the machine can only be set on Web Image Monitor. For details, see Web Image Monitor Help.
- The default access permission for the file creator (owner) is "Read-only". You can also specify the access permission.
- The file administrator can also delete stored files. For details, see "Deleting a Stored Document", Copy and Document Server Reference.

Reference

- p.104 "Specifying Passwords for Stored Files"

Specifying User and Access Permissions for Stored Files

This can be specified by the file creator (owner) or file administrator. For details about logging in and logging out with administrator authentication, see "Logging in Using Administrator Authentication" and "Logging out Using Administrator Authentication".

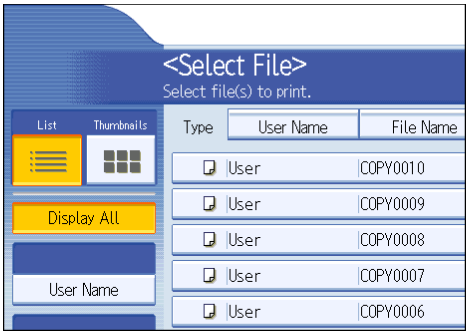
Specify the users and their access permissions for each stored file.

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

Important

- **If files become inaccessible, reset their access permission as the file creator (owner). This can also be done by the file administrator. If you want to access a file but do not have access permission, ask the file creator (owner).**
- **The file administrator can change the owner of a document using the document's [Change Access Priv.] setting. This setting also allows the file administrator to change the access privileges of the owner and other users. The document owner and users with the [Full Control] privilege for the document can change the access privileges of the owner and other users under the [Change Access Priv.] setting.**

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

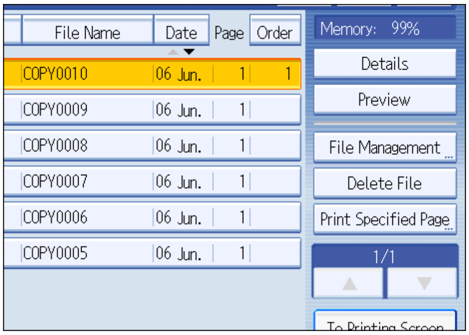


<Select File>

Select file(s) to print.

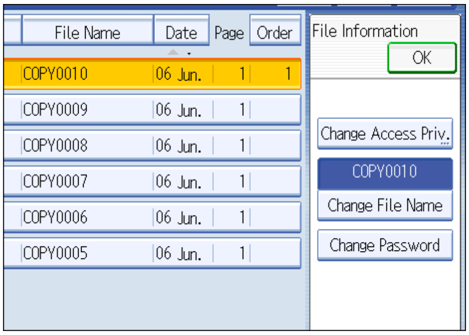
Type	User Name	File Name
	User	COPY0010
	User	COPY0009
	User	COPY0008
	User	COPY0007
	User	COPY0006

3. **Press [File Management].**



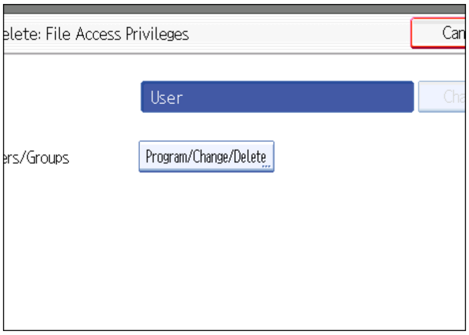
File Name	Date	Page	Order
COPY0010	06 Jun.	1	1
COPY0009	06 Jun.	1	
COPY0008	06 Jun.	1	
COPY0007	06 Jun.	1	
COPY0006	06 Jun.	1	
COPY0005	06 Jun.	1	

4. **Press [Change Access Priv.].**

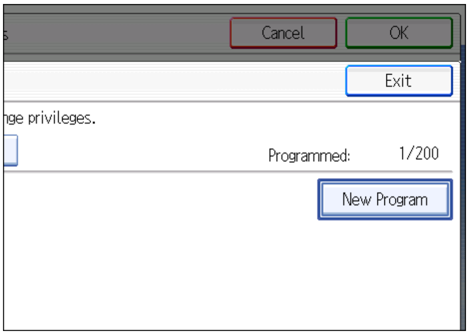


File Name	Date	Page	Order
COPY0010	06 Jun.	1	1
COPY0009	06 Jun.	1	
COPY0008	06 Jun.	1	
COPY0007	06 Jun.	1	
COPY0006	06 Jun.	1	
COPY0005	06 Jun.	1	

5. **Press [Program/Change/Delete].**



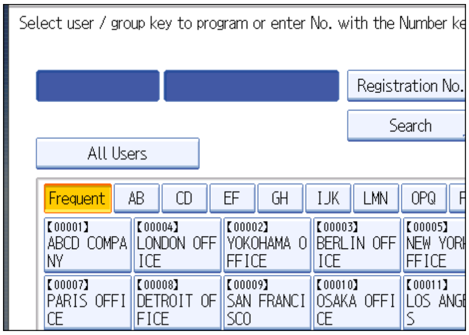
6. **Press [New Program].**



nge privileges.

Programmed: 1/200

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



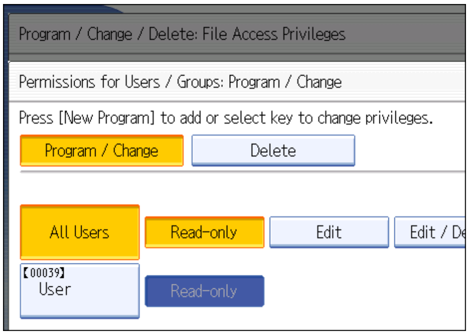
Select user / group key to program or enter No. with the Number ke

You can select more than one user.

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

8. **Press [Exit].**

9. **Select the user to whom you want to assign access permission, and then select the permission.**



Program / Change / Delete: File Access Privileges

Permissions for Users / Groups: Program / Change

Press [New Program] to add or select key to change privileges.

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

10. **Press [Exit].**

11. **Press [OK].**

Note

- The "Edit", "Edit / Delete", and "Full Control" access permissions allow a user to perform high level operations that could result in loss of or changes to sensitive information. We recommend you grant only the "Read-only" permission to general users.

Reference

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

Changing the Owner of a Document

Use this procedure to change the owner of a document.

Only the file administrator can change the owner of a document.

1. **Press the [Document Server] key.**
2. **Select the file.**
3. **Press [File Management].**
4. **Press [Change Access Priv.].**
5. **Under "Owner", press [Change].**
6. **Select the user you want to register.**
7. **Press [Exit].**
8. **Press [OK] twice.**

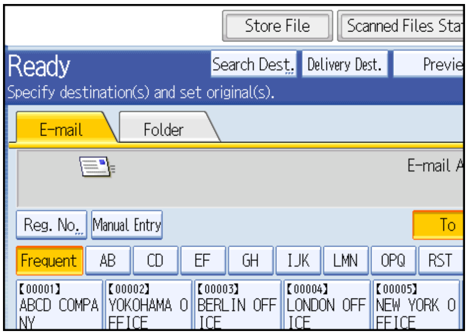
Specifying Access Permissions for Files Stored Using the Scanner Function

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

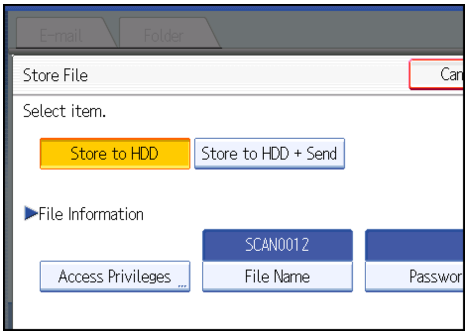
Specifying Access Permissions When Storing a File

This section explains how to specify the access privileges and then store a file in Document Server under the scanner function.

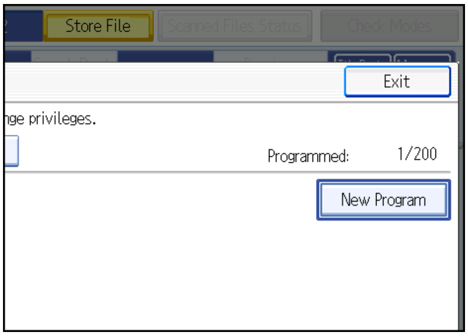
1. **Press [Store File].**



2. **Press [Access Privileges].**



3. **Press [New Program].**



4. **Select the users or groups to whom you want to assign permission.**

   You can select more than one user.

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

5. **Press [Exit].**

6. **Select the user to whom you want to assign access permission, and then select the permission.**

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

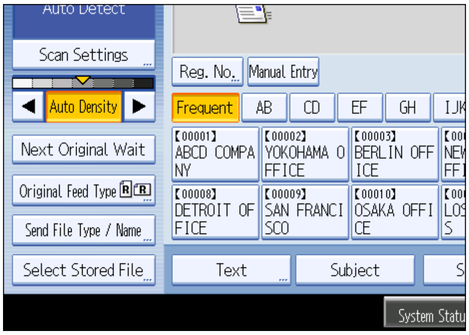
7. **Press [Exit].**

8. **Press [OK].**
9. **Store files in Document Server.**

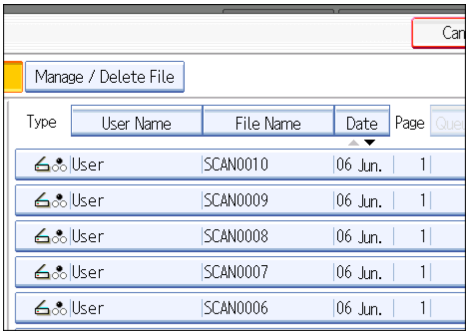
Specifying Access Permissions for Stored Files

This section explains how to change access privileges for a file stored in Document Server under the scanner function.

1. **Press [Select Stored File].**

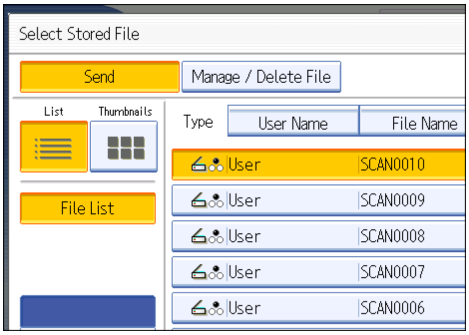


2. **Select the file.**



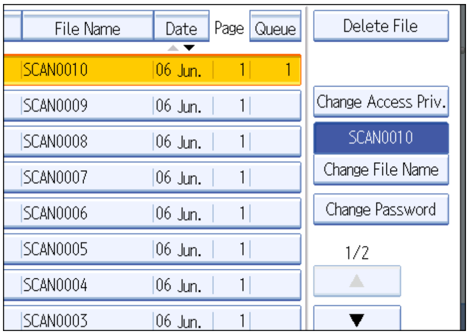
Type	User Name	File Name	Date	Page	Que
	User	SCAN0010	06 Jun.	1	
	User	SCAN0009	06 Jun.	1	
	User	SCAN0008	06 Jun.	1	
	User	SCAN0007	06 Jun.	1	
	User	SCAN0006	06 Jun.	1	

3. **Press [Manage / Delete File].**



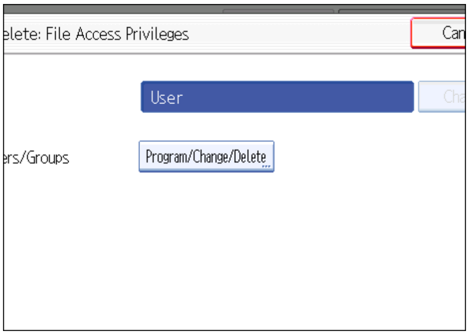
Type	User Name	File Name
	User	SCAN0010
	User	SCAN0009
	User	SCAN0008
	User	SCAN0007
	User	SCAN0006

4. **Press [Change Access Priv.].**

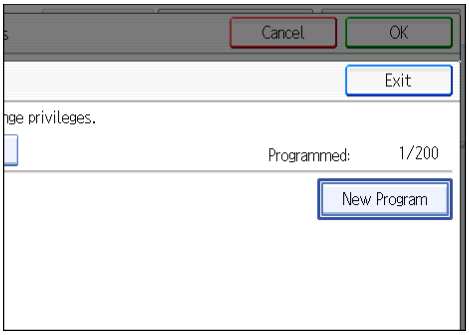


File Name	Date	Page	Queue
SCAN0010	06 Jun.	1	1
SCAN0009	06 Jun.	1	
SCAN0008	06 Jun.	1	
SCAN0007	06 Jun.	1	
SCAN0006	06 Jun.	1	
SCAN0005	06 Jun.	1	
SCAN0004	06 Jun.	1	
SCAN0003	06 Jun.	1	

5. **Press [Program/Change/Delete].**



6. **Press [New Program].**



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

   You can select more than one user.

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

8. **Press [Exit].**

9. **Select the user to whom you want to assign access permission, and then select the permission.**

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

10. **Press [Exit].**

11. Press [OK].

Note

- The "Edit", "Edit / Delete", and "Full Control" access permissions allow a user to perform high level operations that could result in loss of or changes to sensitive information. We recommend you grant only the "Read-only" permission to general users.

Specifying User and Access Permissions for Files Stored by a Particular User

This can be specified by the file creator (owner) or user administrator. For details about logging in and logging out with administrator authentication, see "Logging in Using Administrator Authentication" and "Logging out Using Administrator Authentication".

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

Only those users granted access permission can access stored files.

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

Important

- **If files become inaccessible, be sure to enable the user administrator, so that the user administrator can reset the access permission for the files in question.**

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

2. Press [System Settings].

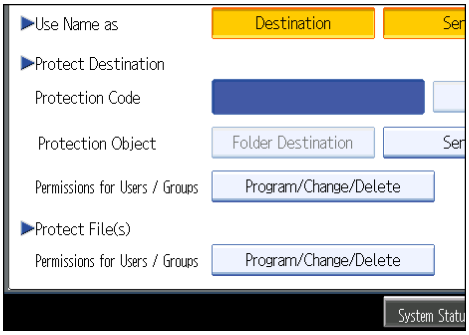
3. Press [Administrator Tools].

4. Press [Address Book Management].

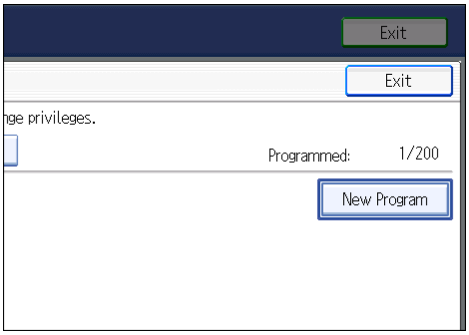
5. Select the user.

6. Press [Protection].

7. Under "Protect File(s)", press [Program/Change/Delete] for "Permissions for Users/ Groups".



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

12. **Press [Exit].**
13. **Press [OK].**
14. **Press [Exit].**
15. **Press the [User Tools/Counter] key.**

Note

- The "Edit", "Edit / Delete", and "Full Control" access permissions allow a user to perform high level operations that could result in loss of or changes to sensitive information. We recommend you grant only the "Read-only" permission to general users.

Reference

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

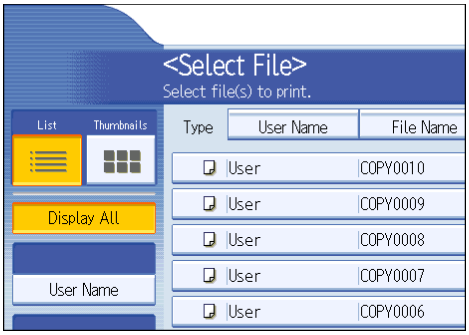
Specifying Passwords for Stored Files

This can be specified by the file creator (owner) or file administrator. For details about logging in and logging out with administrator authentication, see "Logging in Using Administrator Authentication" and "Logging out Using Administrator Authentication".

Specify passwords for stored files.

This provides increased protection against unauthorized use of files.

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

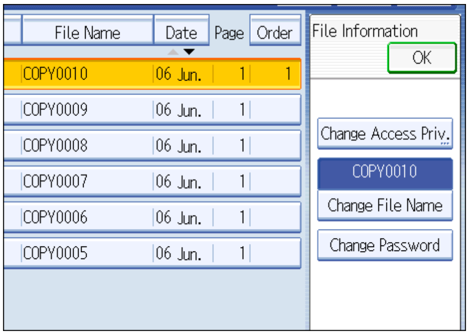


<Select File>

Select file(s) to print.

Type	User Name	File Name
	User	COPY0010
	User	COPY0009
	User	COPY0008
	User	COPY0007
	User	COPY0006

3. **Press [File Management].**
4. **Press [Change Password].**



File Name	Date	Page	Order
COPY0010	06 Jun.	1	1
COPY0009	06 Jun.	1	
COPY0008	06 Jun.	1	
COPY0007	06 Jun.	1	
COPY0006	06 Jun.	1	
COPY0005	06 Jun.	1	

File Information

5. **Enter the password using the number keys.**

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

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

   The 🔑 icon appears next to a stored file protected by password.

9. **Press [OK].**

Reference

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

Unlocking Files

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

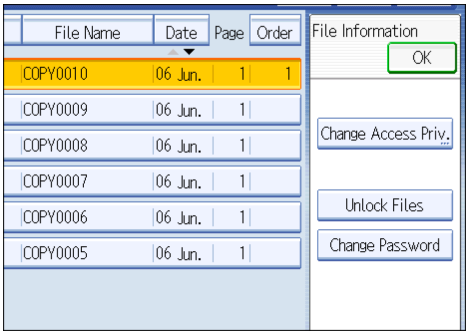
"Enhance File Protection" is one of the extended security functions. For details about this and other extended security functions, see "Specifying the Extended Security Functions".

Only the file administrator can unlock files.

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

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

   The 🔒 icon appears next to a file locked by the Enhance File Protection function.
3. **Press [File Management].**
4. **Press [Unlock Files].**



File Name	Date	Page	Order
COPY0010	06 Jun.	1	1
COPY0009	06 Jun.	1	
COPY0008	06 Jun.	1	
COPY0007	06 Jun.	1	
COPY0006	06 Jun.	1	
COPY0005	06 Jun.	1	

5. **Press [Yes].**

   The 🔒 icon changes to the 🔑 icon.
6. **Press [OK].**

Reference

- p.221 "Specifying the Extended Security Functions"
- p.33 "Logging in Using Administrator Authentication"
- p.34 "Logging out Using Administrator Authentication"

5. Securing Information Sent over the Network or Stored on Hard Disk

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

Preventing Information Leakage Due to Unauthorized Transmission

This section describes Preventing Data Leaks Due to Unauthorized Transmission.

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

You can also limit the direct entry of destinations to prevent files from being sent to destinations not registered in the Address Book.

Restricting Destinations

This can be specified by the user administrator.

Make the setting to disable the direct entry of e-mail addresses under the scanner function.

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

If you set "Restrict Use of Destinations" to [On], users will not be able to directly enter e-mail addresses and folder paths as file destinations on the scanner screen. If you set "Restrict Use of Destinations" to [Off], "Restrict Adding of User Destinations" will appear. Note that selecting [On] for "Restrict Adding of User Destinations" will prevent users registering destinations entered using the scanner screen in the Address Book.

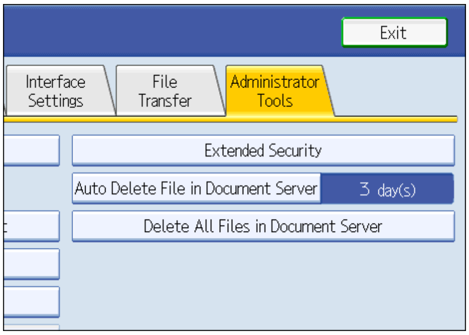
If you set "Restrict Adding of User Destinations" to [Off], users will be able to directly enter e-mail addresses, and folder paths as file destinations using "Prg. Dest." on the scanner screen. If you set these settings to [On], the [Prg. Dest.] key will not appear. Users will still be able to enter a destination directly using the scanner screen, but cannot then register that destination in the Address Book by pressing [Prg. Dest.]. Note too that if you set these functions to [On], only the user administrator can register new users in the Address Book and change the passwords and other information of existing registered users.

"Restrict Use of Destinations" and "Restrict Adding of User Destinations" are extended security functions. For more information about these and the extended security functions, see "Specifying the Extended Security Functions".

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

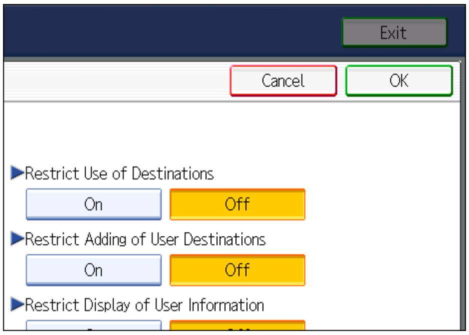
For details about logging in and logging out with administrator authentication, see "Logging in Using Administrator Authentication" and "Logging out Using Administrator Authentication".

1. **Press the [User Tools/Counter] 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 "Restrict Use of Destinations".**


Exit
Cancel
OK
▶Restrict Use of Destinations
On
Off
▶Restrict Adding of User Destinations
On
Off
▶Restrict Display of User Information

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

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

Reference

- p.221 "Specifying the Extended Security Functions"
- p.33 "Logging in Using Administrator Authentication"
- p.34 "Logging out Using Administrator Authentication"

Using S/MIME to Protect E-mail Transmission

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

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

For details about using S/MIME with the scanner function, see "Security Settings to E-mails", Scanner Reference.

Compatible Mailer Applications

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

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

Important

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

Note

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

E-mail Encryption

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

E-mail Encryption

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

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

Note

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

Specifying the User Certificate

This can be specified by the user administrator.

Each user certificate must be prepared in advance.

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

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

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

   The user administrator can log in.

   Enter the login user name and login password.
4. **Click [Address Book].**

   The Address Book page appears.
5. **Select the user for whom the certificate will be installed, and then click [Change].**

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

   The user certificate is installed.
10. **Click [OK].**
11. **Click [Logout].**

Specifying the Encryption Algorithm

This can be specified by the network administrator.

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

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

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

   The network administrator can log in.

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

   The S/MIME settings page appears.
5. **Select the encryption algorithm from the drop down menu next to "Encryption Algorithm" under "Encryption".**
6. **Click [OK].**

   The algorithm for S/MIME is set.
7. **Click [Logout].**

Attaching an Electronic Signature

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

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

Important

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

Electronic Signature

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

Configuration flow (self-signed certificate)

1. Create and install the device certificate using Web Image Monitor.
2. Make settings for the certificate to be used for S/MIME using Web Image Monitor.
3. Make settings for the electronic signature using Web Image Monitor.

Configuration flow (certificate issued by a certificate authority)

1. Create the device certificate using Web Image Monitor.

   The application procedure for a created certificate depends on the certificate authority. Follow the procedure specified by the certificate authority.
2. Install the device certificate using Web Image Monitor.
3. Make settings for the certificate to be used for S/MIME using Web Image Monitor.
4. Make settings for the electronic signature using Web Image Monitor.

Creating and Installing the Self-Signed Certificate

This can be specified by the network administrator.

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

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

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

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

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

   The network administrator can log in.

   Enter the login user name and login password.
4. **Click [Configuration], and then click [Device Certificate] under "Security".**
5. **Check the radio button next to the number of the certificate you want to create.**
6. **Click [Create].**
7. **Make the necessary settings.**
8. **Click [OK].**

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

   A security warning dialog box appears.

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

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

11. **Click [Logout].**

Note

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

Creating the Device Certificate (Issued by a Certificate Authority)

This can be specified by the network administrator.

Create the device certificate using Web Image Monitor. For details about the displayed and selectable items and settings, see Web Image Monitor Help.

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

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

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

    The top page of Web Image Monitor appears.

3. **Click [Login].**

    The network administrator can log in.

    Enter the login user name and login password.

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

    The Device Certificate page appears.

5. **Check the radio button next to the number of the certificate you want to request.**
6. **Click [Request].**
7. **Make the necessary settings.**
8. **Click [OK].**
9. **Click [OK].**

    "Requesting" appears for "Certificate Status".

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

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

    For application details, click the Web Image Monitor Details icon and use the information shown 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)

This can be specified by the network administrator.

Install the device certificate using Web Image Monitor. For details about displayed and selectable items and settings, see Web Image Monitor Help.

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

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

Installation of the certificate is especially necessary for users who want to print via IPP -SSL from Windows Vista/7, Windows Server 2008/2008 R2.

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

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

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

   The network administrator can log in.

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

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

   In the certificate 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 [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. Otherwise, validation by the certificate authority will not be performed correctly. In this case, a warning message may appear when you try to add a printer using IPP-SSL under Windows Vista/7, Windows Server 2008/2008 R2 or when the destination user receives an e-mail with an S/MIME signature. A warning message might also appear if you attempt to access this machine through Web Image Monitor with SSL enabled. To enable authentication from the client computer, install the intermediate certificate on the client computer, and then reestablish connection.
- Intermediate certificates cannot be installed on this machine.

Selecting the Device Certificate

This can be specified by the network administrator.

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

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

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

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

   The network administrator can log in.

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

   The Device Certificate page appears.
5. **Select the certificate to be used for the electronic signature from the drop down box in "S/MIME" under "Certification".**
6. **Click [OK].**

   The certificate to be used for the S/MIME electronic signature is set.
7. **Click [OK].**
8. **Click [Logout].**

Specifying the Electronic Signature

This can be specified by the network administrator.

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

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

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

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

   The network administrator can log in.

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

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

   The settings for the S/MIME electronic signature are enabled.
9. **Click [Logout].**

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.

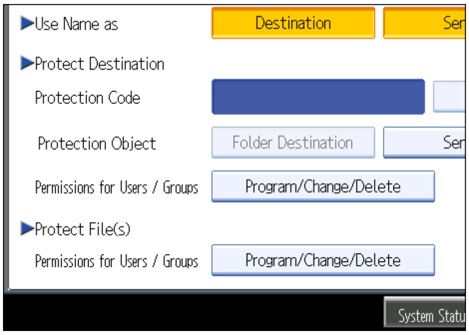
Access permission can also be specified by a user granted full control or the user administrator.

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

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

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

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



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

   You can select more than one user.

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

10. **Press [Exit].**
11. **Select the user 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/Counter] key.**

Note

- The "Edit", "Edit / Delete", and "Full Control" access permissions allow a user to perform high level operations that could result in loss of or changes to sensitive information. We recommend you grant only the "Read-only" permission to general users.

Reference

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

Encrypting Data in the Address Book

This can be specified by the user administrator.

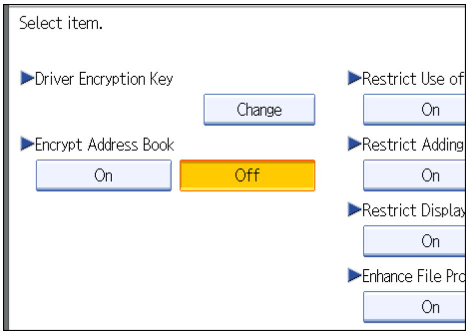
You can encrypt the data in the Address Book using the extended security function, "Encrypt Address Book". For details about this and other extended security functions, see "Specifying the Extended Security Functions".

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

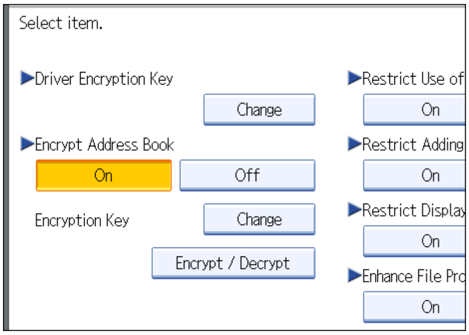
1. **Press the [User Tools/Counter] key.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [Extended Security].**

   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".**

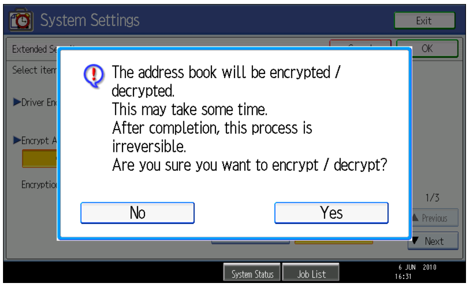


7. **Enter the encryption key, and then press [OK].**

   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/Counter] 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.

Reference

- p.33 "Logging in Using Administrator Authentication"
- p.34 "Logging out Using Administrator Authentication"
- p.221 "Specifying the Extended Security Functions"

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 "Logging in Using Administrator Authentication" and "Logging out Using Administrator Authentication".

Prevent information leakage by encrypting the Address Book, authentication information, and stored documents as the data is written. 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
- Data stored in Document Server
- Temporary stored documents
- Logs
- Network I/F setting information
- System settings information

Reference

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

Enabling the Encryption Settings

Use the following procedure to enable the encryption settings at initial set up, or after encryption settings have been canceled and settings must be made again.

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.**
- **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 about seven hours. If there is encrypted data on the hard disk that must be re-encrypted, rebooting will also take about seven hours. If both the**

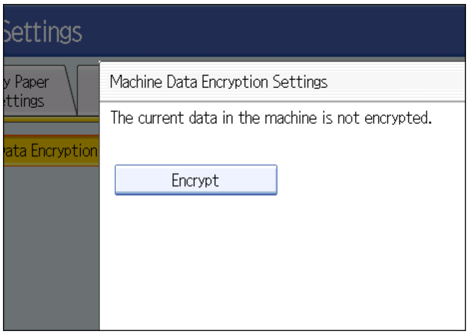
erase-by-overwrite function and the encryption function are specified, encryption begins after the data that is stored on the hard disk has been overwritten and the machine has been rebooted with the turning off and on of the main power switch.

- 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 about nine hours. If you specify re-encryption of encrypted data, the entire process will also take about 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 and all data stored in Document Server.
- If the encryption key update was not completed, the printed encryption key will not be valid.

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

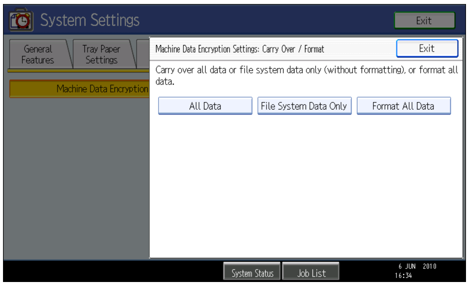
5. **Press [Encrypt].**



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].

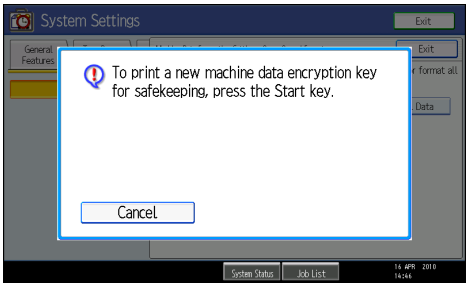


Machine Data Encryption Settings: Carry Over / Format

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

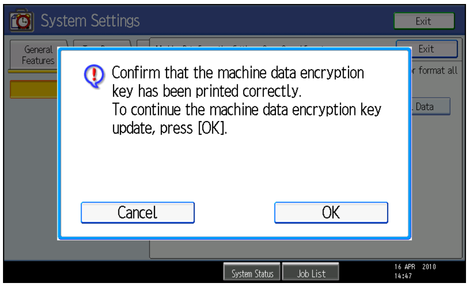
7. **Press the [Start] key.**

   The encryption key for backup data is printed.



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/Counter] 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.

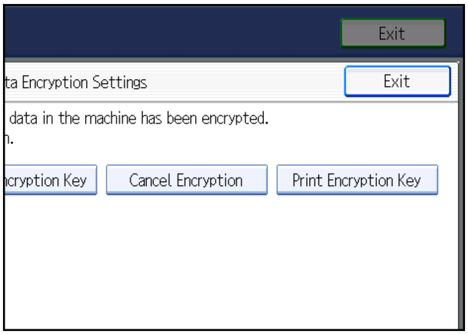
Important

- **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/Counter] 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].**

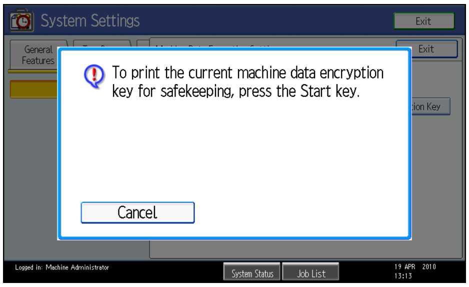


ta Encryption Settings

data in the machine has been encrypted.
n.

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

   The encryption key for retrieving backup data is printed.



System Settings

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

Logged in: Machine Administrator

19 APR 2010 13:13

7. **Press [Exit].**

Updating the Encryption Key

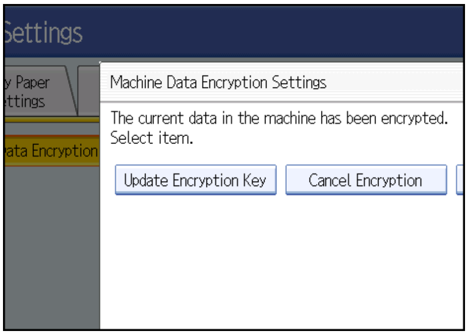
You can update the encryption key and create a new key. Updates are possible when the machine is functioning normally.

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/Counter] 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].**



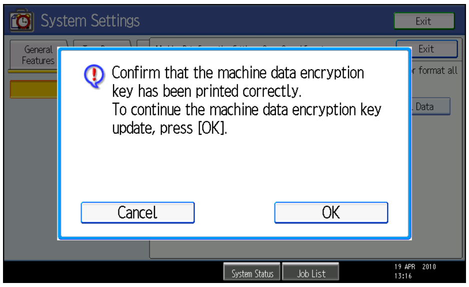
Machine Data Encryption Settings

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.**

   The encryption key for retrieving the backup data is printed.
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/Counter] 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/Counter] 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/Counter] 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.

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

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

Note

- Network TWAIN scanner data are recorded in the memory installed on this machine. This information is not overwritten with the Hard Disk 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

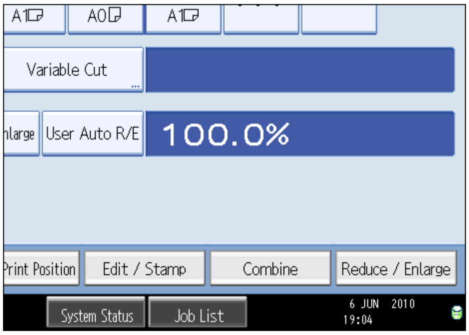
A document scanned in copier, or scanner mode, or print data sent from a printer driver is temporarily stored on the machine's hard disk. Even after the job is completed, it remains in the hard disk as temporary data. Auto Erase Memory erases the temporary data on the hard disk by writing over it.

Overwriting starts automatically once the job is completed.

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

Overwrite Icon

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.

Important

- **The Data Overwrite icon will indicate "Clear" when there is a Sample Print/Locked Print/Hold Print/ Stored Print job.**

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

This can be specified by the machine administrator.

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

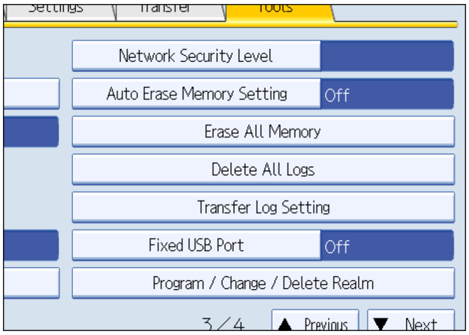
Important

- **When Auto Erase Memory 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/Counter] key.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**

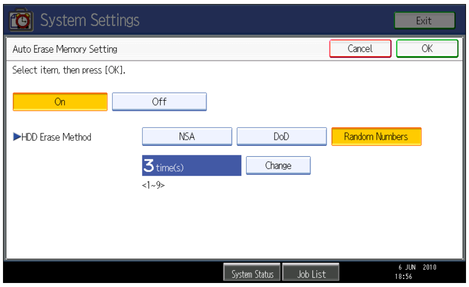
   Press [▼Next] repeatedly until [Auto Erase Memory Setting] appears.

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



5. **Press [On].**

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



Auto Erase Memory Setting

Select item, then press [OK].

▶HDD Erase Method

3 time(s)

<1~9>

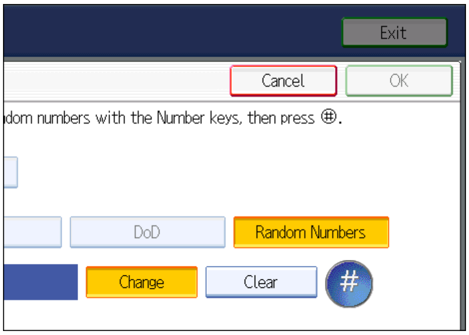
If you select [NSA] or [DoD], proceed to step 9.

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

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

7. **Press [Change].**

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



dom numbers with the Number keys, then press ⊕.

9. **Press [OK].**

Auto Erase Memory is set.

Note

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

Reference

- p.33 "Logging in Using Administrator Authentication"
- p.34 "Logging out Using Administrator Authentication"
- p.129 "Methods of Overwriting"

Canceling Auto Erase Memory

This can be specified by the machine administrator.

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

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

   Auto Erase Memory is disabled.

Note

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

Reference

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

Types of Data that Can or Cannot Be Overwritten

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

Data Overwritten by Auto Erase Memory

Copier

- Copy jobs

Printer

- Print jobs
- Sample Print /Locked Print/Hold Print/Stored Print jobs

  A Sample Print/Locked Print/Hold Print job can only be overwritten after it has been executed. A Stored Print job is overwritten after it has been deleted.
- Spool Printing jobs

- PDF Direct Print data

Scanner

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

Data scanned with network TWAIN scanner will not be overwritten by Auto Erase Memory.

Data Not Overwritten by Auto Erase Memory

- Documents stored by the user in Document Server using the Copier, Printer, or Scanner functions

  A stored document can only be overwritten after it has been printed or deleted from Document Server.

- Information registered in the Address Book

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

- Counters stored under each user code

Reference

- p.117 "Protecting the Address Book"

Erase All Memory

This can be specified by the machine administrator.

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

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

Important

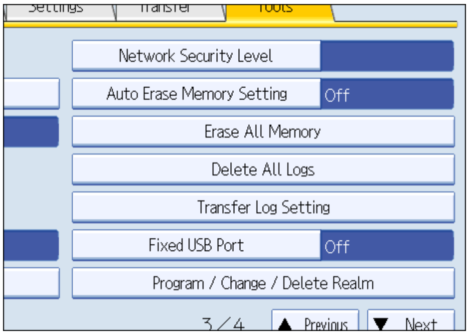
- **If you select "Erase All Memory", the following are also deleted: user codes, counters under each user code, user stamps, data stored in the Address Book, printer fonts downloaded by users, applications using Embedded Software Architecture, SSL server certificates, and the machine's network settings.**
- **If the main power switch is turned off before "Erase All Memory" is completed, overwriting will be stopped and data will be left on the hard disk.**
- **Do not stop the overwrite mid-process. Doing so will damage the hard disk.**
- **We recommend that before you erase the hard disk, you use SmartDeviceMonitor for Admin to back up the user codes, the counters for each user code, and the Address Book. The Address Book can also be backed up using Web Image Monitor. For details, see SmartDeviceMonitor for Admin Help or Web Image Monitor Help.**

- Other than pausing, no operations are possible during the "Erase All Memory" process. If [Random Numbers] is specified and the number of overwrites set to "3", the erase process will take about two 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/Counter] key.**
3. **Press [System Settings].**
4. **Press [Administrator Tools].**

   Press [▼Next] repeatedly until [Erase All Memory] appears.
5. **Press [Erase All Memory].**



Settings | Transfer | Tools

Network Security Level

Auto Erase Memory Setting: Off

Erase All Memory

Delete All Logs

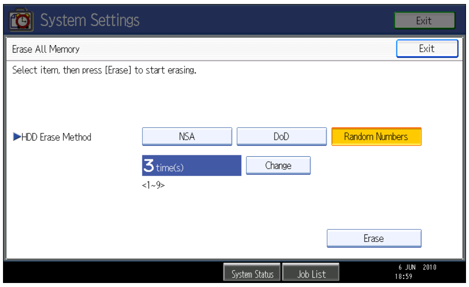
Transfer Log Setting

Fixed USB Port: Off

Program / Change / Delete Realm

3/4 ▲ Previous ▼ Next

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



System Settings Exit

Erase All Memory Exit

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

▶HDD Erase Method: NSA | DoD | Random Numbers

3 time(s) Change

<1~9>

Erase

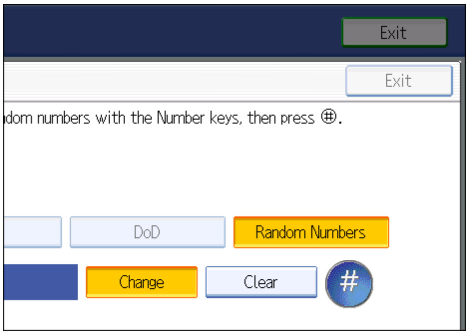
System Status | Job List 6 JUN 2010 18:59

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

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

   For details about the methods of overwriting, see "Methods of Overwriting".
7. **Press [Change].**

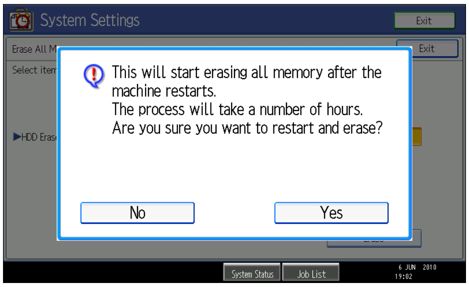
8. **Enter the number of times that you want to overwrite using the number keys, and then press [#].**



dom numbers with the Number keys, then press ⊕.

9. **Press [Erase].**

10. **Press [Yes].**



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

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.

Reference

- p.33 "Logging in Using Administrator Authentication"
- p.34 "Logging out Using Administrator Authentication"
- p.129 "Methods of Overwriting"

Suspending Erase All Memory

The overwriting process can be suspended temporarily.

Important

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

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

   Erase All Memory is suspended.
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.

6. 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

This section describes preventing modification of machine settings.

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

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

Type of Administrator

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

- Machine Administrator

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

- Network Administrator

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

- File Administrator

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

Menu Protect

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

You can specify Menu Protect for the following settings:

- Copier / Document Server Features
- Printer Features
- Scanner Features

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

Reference

- p.23 "Administrators"
- p.30 "Registering the Administrator"
- p.265 "User Administrator Settings"
- p.267 "Machine Administrator Settings"
- p.275 "Network Administrator Settings"
- p.279 "File Administrator Settings"
- p.286 "User Settings - Control Panel Settings"
- p.304 "User Settings - Web Image Monitor Settings"

Menu Protect

The administrator can also limit users' access permission to the machine's settings. The machine's "System Settings" menu and the printer's regular menus can be locked so they cannot be changed. This function is also effective when management is not based on user authentication. For a list of settings that users can specify according to the Menu Protect level, see "User Settings - Control Panel Settings", or "User Settings - Web Image Monitor Settings".

Reference

- p.286 "User Settings - Control Panel Settings"
- p.304 "User Settings - Web Image Monitor Settings"

Enabling Menu Protect

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

For details about specifying "Menu Protect", see "Specifying Menu Protect".

Reference

- p.139 "Specifying Menu Protect"

Disabling Menu Protect

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

For details about canceling "Menu Protect", see "Specifying Menu Protect".

Reference

- p.139 "Specifying Menu Protect"

Specifying Menu Protect

This can be specified by the machine administrator.

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

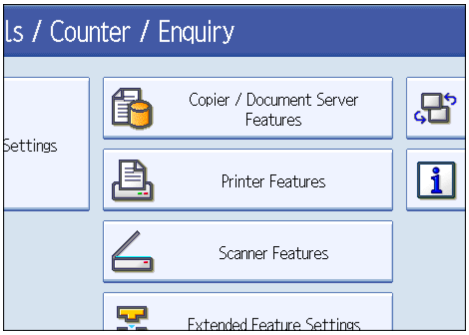
Reference

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

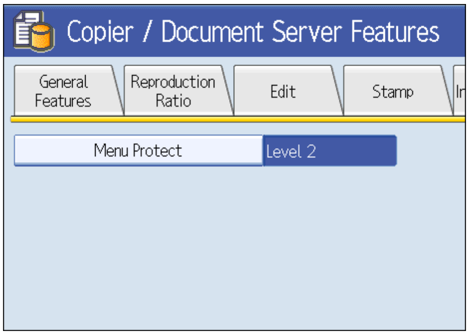
Copy Function

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

1. **Press the [User Tools/Counter] key.**
2. **Press [Copier / Document Server Features].**

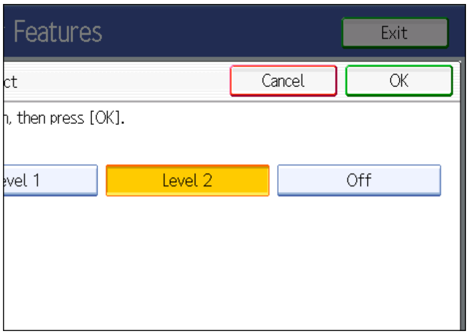


3. **Press [Administrator Tools].**
4. **Press [Menu Protect].**



Menu Protect Level 2

5. **Select the menu protect level, and then press [OK].**



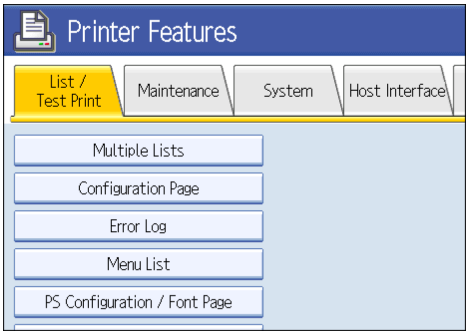
n, then press [OK].

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

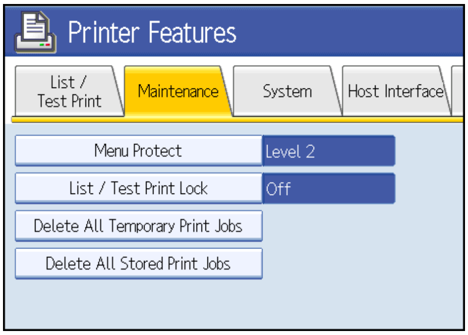
Printer Function

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

1. **Press the [User Tools/Counter] key.**
2. **Press [Printer Features].**
3. **Press [Maintenance].**



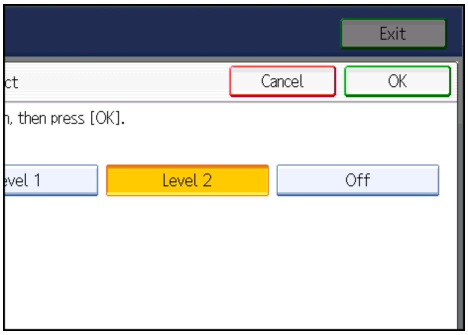
4. **Press [Menu Protect].**



Menu Protect: Level 2

List / Test Print Lock: Off

5. **Select the menu protect level, and then press [OK].**



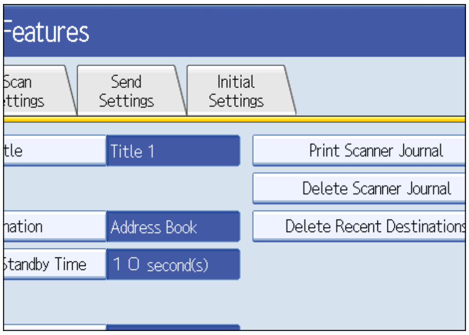
n, then press [OK].

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

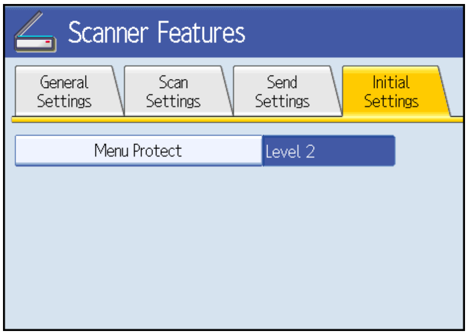
Scanner Function

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

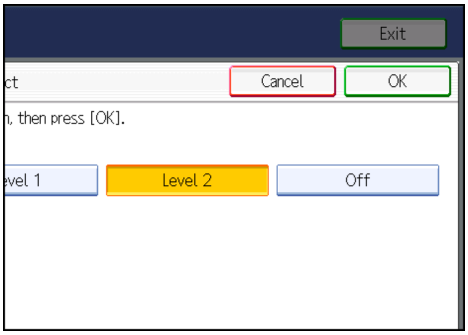
1. **Press the [User Tools/Counter] key.**
2. **Press [Scanner Features].**
3. **Press [Initial Settings].**



4. **Press [Menu Protect].**



5. **Select the menu protect level, and then press [OK].**



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

Limiting Available Functions

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

Available Functions

Specify the available functions from the copier, Document Server, scanner, and printer functions.

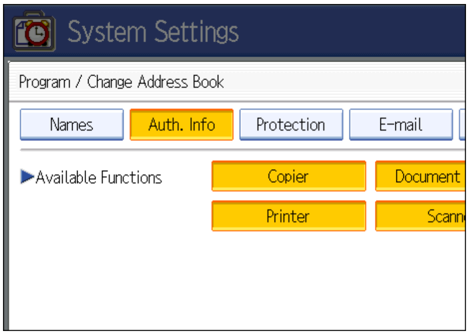
Specifying Which Functions are Available

This can be specified by the user administrator.

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

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

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



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

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

Reference

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

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 or Remote Communication Gate S. Collected logs can be downloaded all at once from Web Image Monitor as CSV files. To use Remote Communication Gate S you must specify the log transfer setting under Remote Communication Gate S in advance.

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 copying, printing, and saving in Document Server, and control panel operations such as sending scan files and printing reports (the configuration list, for example).

- Access Log

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

Note

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

Using the Control Panel to Specify Log File Settings

This can be specified by the machine administrator.

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

You can specify settings such as whether or not to transfer logs to Remote Communication Gate S and whether or not to delete all logs.

Reference

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

Disabling log transfer to Remote Communication Gate S

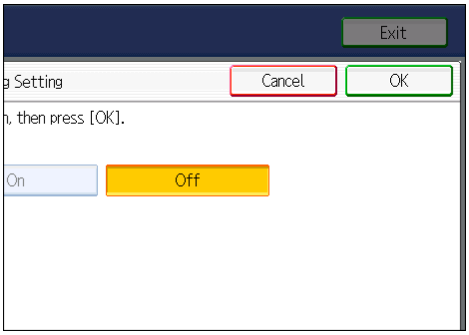
Use the following procedure to disable log transfer from the machine to Remote Communication Gate S. Note that you can change the log transfer setting to [Off] only if it is already set to [On].

For details about Remote Communication Gate S, contact your sales representative.

For details about the transfer log setting, see Remote Communication Gate S manual.

1. **Press the [User Tools/Counter] key.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [Transfer Log Setting].**

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



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

Specifying Delete All Logs

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

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

1. **Press the [User Tools/Counter] key.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [Delete All Logs].**

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

   The confirmation screen appears.
5. **Press [Yes].**

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

Using Remote Communication Gate S to Manage Log Files

For details about using Remote Communication Gate S to manage Log Files, see the manual supplied with Remote Communication Gate S.

Using Web Image Monitor to Manage Log Files

This can be specified by the machine administrator.

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

You can specify the types of log to store in the machine and the log collection level. You can also encrypt, bulk delete, or download log files.

Reference

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

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.**

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

   The top page of Web Image Monitor appears.

3. **Click [Login].**

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

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

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

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

7. **Click [OK] twice.**

   Changes are also reflected in related log settings.

8. **Click [Logout].**

Note

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

Disabling log transfer to Remote Communication Gate S

Use the following procedure to disable log transfer to Remote Communication Gate S. Note that you can change the log transfer setting to [Inactive] only if it is already set to [Active].

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

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

   The top page of Web Image Monitor appears.

3. **Click [Login].**

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

4. **Click [Configuration], and then click [Logs] under "Device Settings".**
5. **Select [Inactive] under "Transfer Logs".**
6. **Click [OK].**
7. **Click [Logout].**

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.**

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

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

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

   To disable log encryption, select [Inactive].

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

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

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

Note

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

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

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

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

6. **Click [Back].**

   All job logs and device access log records are cleared.

7. **Click [Logout].**

Note

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

Downloading logs

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. **In the Web browser's address bar, enter "http://(the machine's IP address or host name)/ " to access the machine.**

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

   The top page of Web Image Monitor appears.

3. **Click [Login].**

   Log in using an administrator's user name and password.

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

Note

- Downloaded logs contain data recorded up till the time you click the [Download] button. Any logs recorded after the [Download] button is clicked will not be downloaded. 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 "Attributes of logs you can download".

Reference

- p.159 "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.
- Batch deletion of logs can be performed from the control panel or through 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.

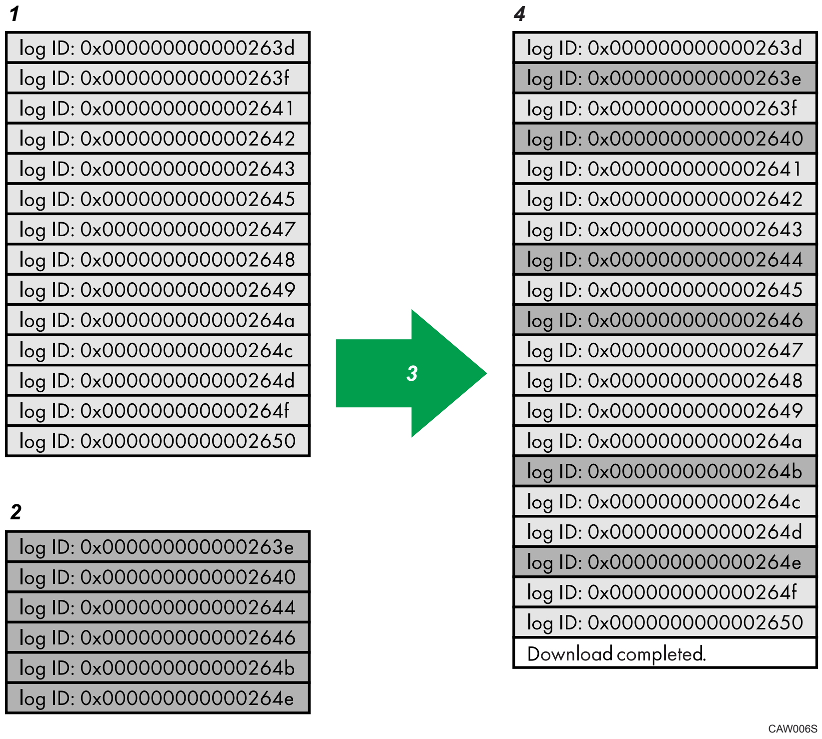
Downloaded log files include both access and job logs, with some log entries incomplete.

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
```

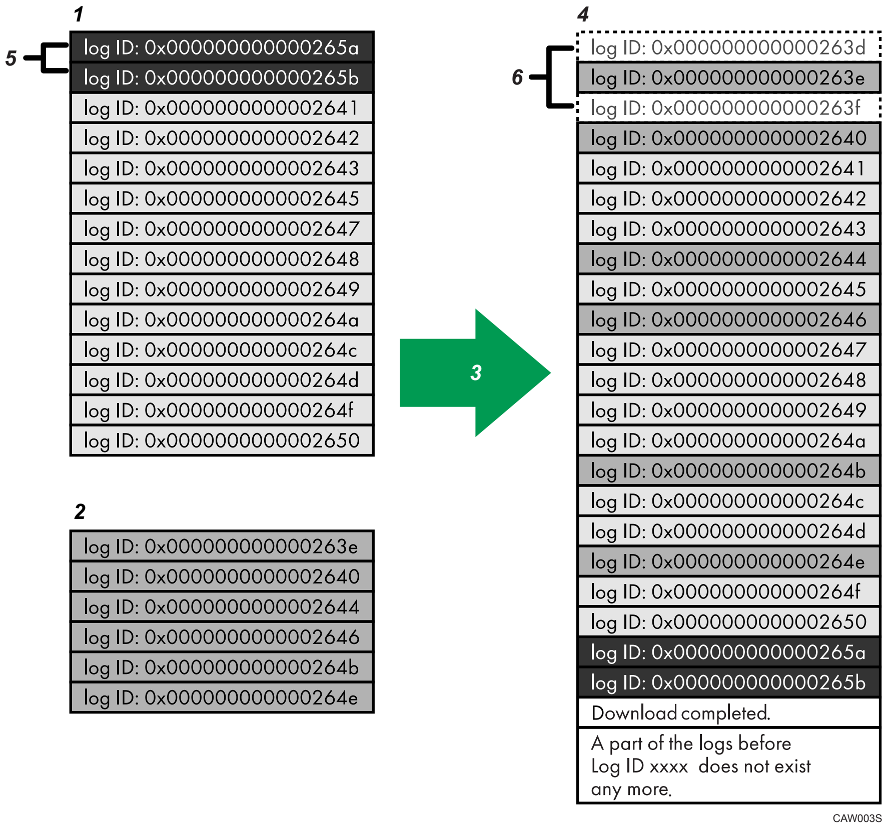
4

```
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".

Detailed explanation of print job-related log entries

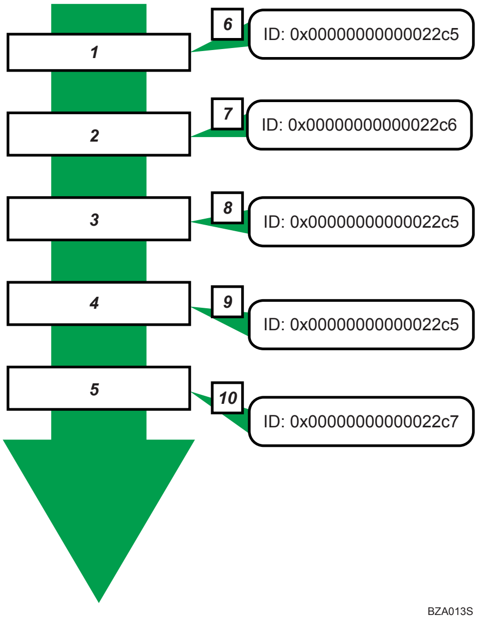
Print Log entries are made before the login entry is made in the Access Log.

Details of series of jobs (including reception, processing, and output of the jobs' data) are combined into single entries.

When the machine receives a print job, it creates an ID for the job and records this in the job log. The machine then creates a login ID for the print job and records this in the access log. It then creates a job log entry detailing the job's processing and outputting (under the same login ID). When the machine has finished processing the job, it creates a logout entry and places this in the access log.

Entries detailing the reception, processing, and output of a series of print jobs are created in the job log first, and then the login and logout details of those jobs are recorded in the access log.

Print job flowchart



1. **Print job data is received.**
2. **Authentication (login) data is received.**
3. **Print job is processed.**
4. **Print job is output.**
5. **Authentication (login) data is received.**
6. **An ID is assigned to the print job and recorded as an entry in the Job Log.**

7. **Authentication (login) data is recorded as an entry in the Access Log.**
8. **Information about the processing of the print job is recorded as an entry in the Job Log (using the same ID).**
9. **Information about the outputting of the print job is recorded as an entry in the Job Log (using the same ID).**
10. **Authentication (logout) data is recorded as an entry in the Access Log.**

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.

Job log information items

Job Log Item	Log Type Attribute	Content
Copier: Copying	Copier: Copying	Details of normal and Sample Copy jobs.
Copier: Copying and Storing	Copier: Copying and Storing	Details of files stored in Document Server that were also copied at the time of storage.
Document Server: Storing	Document Server: Storing	Details of files stored using the Document Server screen.
Document Server: Stored File Downloading	Document Server: Stored File Downloading	Details of files stored in Document Server and downloaded using Web Image Monitor or DeskTopBinder.
Stored File Printing	Stored File Printing	Details of files printed using the Document Server screen.
Scanner: Sending	Scanner: Sending	Details of sent scan files.
Scanner: URL Link Sending and Storing	Scanner: URL Link Sending and Storing	Details of scan files stored in Document Server and whose URLs were sent by e-mail at the time of storage.

Job Log Item	Log Type Attribute	Content
Scanner: Sending and Storing	Scanner: Sending and Storing	Details of scan files stored in Document Server that were also sent at the time of storage.
Scanner: Storing	Scanner: Storing	Details of scan files stored in Document Server.
Scanner: Stored File Downloading	Scanner: Stored File Downloading	Details of scan files stored in Document Server and downloaded using Web Image Monitor, DeskTopBinder or Desk Top Editor For Production.
Scanner: Stored File Sending	Scanner: Stored File Sending	Details of stored scan files that were also sent.
Scanner: Stored File URL Link Sending	Scanner: Stored File URL Link Sending	Details of stored scan files whose URLs were sent by e-mail.
Printer: Printing	Printer: Printing	Details of normal print jobs.
Printer: Locked Print (Incomplete)	Printer: Locked Print (Incomplete)	Log showing Locked Print documents temporarily stored on the machine.
Printer: Locked Print	Printer: Locked Print	Log showing Locked Print documents temporarily stored on the machine and then printed from the control panel or through Web Image Monitor.
Printer: Sample Print (Incomplete)	Printer: Sample Print (Incomplete)	Log showing Sample Print documents temporarily stored on the machine.
Printer: Sample Print	Printer: Sample Print	Log showing Sample Print documents temporarily stored on the machine and then printed from the control panel or through Web Image Monitor.
Printer: Hold Print (Incomplete)	Printer: Hold Print (Incomplete)	Log showing Hold Print documents temporarily stored on the machine.
Printer: Hold Print	Printer: Hold Print	Log showing Hold Print documents temporarily stored on the machine and then printed from the control panel or through Web Image Monitor.
Printer: Stored Print	Printer: Stored Print	Details of Stored Print files stored on the machine.

Job Log Item	Log Type Attribute	Content
Printer: Store and Normal Print	Printer: Store and Normal Print	Details of Stored Print files that were printed at the time of storage (when "Job Type:" was set to "Store and Print" in printer properties).
Printer: Stored File Printing	Printer: Stored File Printing	Details of Stored Print files printed from the control panel or Web Image Monitor.
Printer: Document Server Sending	Printer: Document Server Sending	Details of files stored in Document Server when "Job Type:" was set to "Document Server" in printer properties.
Report Printing	Report Printing	Details of reports printed from the control panel.
Scanner: TWAIN Driver Scanning	Scanner: TWAIN Driver Scanning	Details of stored scan files that were sent using Network TWAIN Scanner.

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.
File Storing	File Storing	Details of files stored in Document Server.
Stored File Deletion	Stored File Deletion	Details of files deleted from Document Server.
All Stored Files Deletion	All Stored Files Deletion	Details of deletions of all Document Server files.
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.
Transfer Log Error	Transfer Log Error	Details of changes made to log settings.
Log Collection Item Change	Log Collection Item Change	Details of changes made to log settings.
Collect Encrypted Communication Logs	Collect Encrypted Communication Logs	Details of changes to job log collection levels, access log collection levels, and types of log collected.

Access Log Item	Log Type Attribute	Content
Access Violation	Access Violation	Details of failed access attempts.
Lockout	Lockout	Details of lockout activation.
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.
File Access Privilege Change	File Access Privilege Change	Log for changing the access privilege to the stored files.
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.
Capture Error	Capture Error	Details of file capture errors.

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

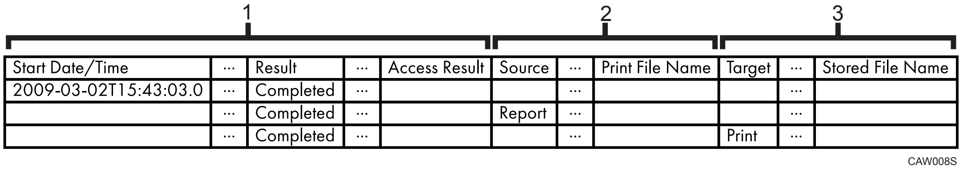
The output format of the access log and job log are different.

- 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.



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 "Logs that can be collected". This is Item 3 of the CSV file.

Item	Content
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.
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", "File Limit Exceeded", "Transfer Cancelled", "Power Failure", "Lost File", "Functional Problem", "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 stored files and the address book; "0x00000000" indicates other operations. "0xffffff80" indicates operations related to deleting Hold Print, Locked Print, and Stored Print jobs, or 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. ID "0xffffff81" indicates operations related to creating Hold Print, Locked Print, and Stored Print jobs that can be deleted using system operations. "0x00000000" and "0xffffff81" indicate operations that do not require user authentication (such as copying and scanning) and that were performed by non-authenticated users. ID "0xffffff81" indicates operations related to stored files, 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.

The following log items are recorded only when the logged operations are executed successfully: "Document Server: Stored File Downloading", "Stored File Printing", "Scanner: Storing", "Scanner:

Stored File Sending", "Printer: Stored File Printing", and "File Storing" and "Stored File Deletion" (Access logs).

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. "Stored File" indicates a stored file 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. "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.
Stored File ID	Identifies a created or deleted file. This is a hexadecimal ID that indicates created or deleted stored files.
Stored File Name	Name of a created or deleted file.

Item	Content
File Location	Region of all file deletion. "Document Server" indicates a deletion of all files from the machine's hard disk.
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.
Transfer Logs	Indicates the status of the log transfer setting: "Active" indicates log transfer is enabled. "Inactive" indicates log transfer is disabled. "Not Changed" indicates no changes have been made to the log transfer setting.
Encrypt Logs	Indicates the status of the log encryption setting: "Active" indicates log encryption is enabled. "Inactive" indicates log encryption is disabled. "Not Changed" indicates no changes have been made to the log encryption setting.
Log Type	If a log's collection level setting has been changed, this function indicates details of the change: "Job Log" indicates the Job Log's collection level has been changed. "Access Log" indicates the Access Log's collection level has been changed. "Level 1" indicates a level 1 collection setting. "Level 2" indicates a level 2 collection setting. "User Settings" indicates a user-specified collection level setting. This is Item 24 of the CSV file.

Item	Content
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.
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 update. "Added with SD Card" indicates an SD card was used to add the firmware update. "Deleted with SD Card" indicates an SD card was used to delete the firmware update. "Moved to Another SD Card" indicates the firmware update was moved to another SD card. "Updated via Remote" indicates the firmware update was updated remotely from a computer. "Updated for Other Reasons" indicates the firmware updated 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: "Scan File" indicates the job file was scanned in; "Stored File" indicates the job file was stored on the hard disk; "Printer" indicates the job file was sent from the printer driver; "Report" indicates the job file was a printed report.
Start Date/Time	Dates and times "Scan File", "Received File" and "Printer" operations started. This is Item 52 of the CSV file.

Item	Content
End Date/Time	Dates and times "Scan File", "Received File" and "Printer" operations ended. This is Item 53 of the CSV file.
Stored File Name	Names of "Stored File" files.
Stored File ID	Indicates the ID of data that is output as a stored file. This is a decimal ID that identifies the stored file.
Print File Name	Name of "Printer" files.

Output information

Item	Content
Target	Type of the job target. "Print" indicates a print file; "Store" indicates a stored file; "Send" indicates a sent file.
Start Date/Time	Dates and times "Print", "Store", and "Send" operations started. This is Item 58 of the CSV file.
End Date/Time	Dates and times "Print", "Store", and "Send" operations ended. This is Item 59 of the CSV file.
Destination Name	Names of "Send" destinations.
Destination Address	IP address, path, or e-mail address of "Send" destinations.
Stored File ID	Indicates the ID of data that is output as a store file. This is a decimal ID that identifies the stored file.
Stored File Name	If the Target Type is "Store", the file name of the stored file is recorded.

Reference

- p.155 "Logs that can be collected"

7. Enhanced Network Security

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

Preventing Unauthorized Access

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

Access Control

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

For details, see Web Image Monitor Help.

The machine can control TCP/IP access.

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

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

Important

- **Using access control, you can limit access involving LPR, RCP/RSH, FTP, SSH/SFTP, Bonjour, SMB, WSD (Device), WSD (Printer), IPP, DIPRINT, Web Image Monitor, SmartDeviceMonitor for Client or DeskTopBinder. You cannot limit the monitoring of SmartDeviceMonitor for Client. You cannot limit access involving telnet, or SmartDeviceMonitor for Admin, when using the SNMPv1 monitoring.**

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

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

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

   The network administrator can log in using the appropriate login user name and login password.
4. **Click [Configuration], and then click [Access Control] under "Security".**

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

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

6. **Click [OK].**

   Access control is set.

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

Enabling and Disabling Protocols

This can be specified by the network administrator.

Specify whether to enable or disable the function for each protocol. By making this setting, you can specify which protocols are available and so prevent unauthorized access over the network. Network settings can be specified on the control panel, or using Web Image Monitor, telnet, SmartDeviceMonitor for Admin or Remote Communication Gate S. If you use SmartDeviceMonitor for Admin, start Web Image Monitor from SmartDeviceMonitor for Admin and configure the settings from there. For details about making settings using SmartDeviceMonitor for Admin or Remote Communication Gate S, see the manual for each application. 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.

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

Protocol	Port	Setting Method	When Disabled
IPv4	-	• Control Panel • Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Remote Communication Gate S	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 • SmartDeviceMonitor for Admin • Remote Communication Gate S	All applications that operate over IPv6 cannot be used.

Protocol	Port	Setting Method	When Disabled
IPsec	-	• Control Panel • Web Image Monitor • telnet • SmartDeviceMonitor for Admin	Encrypted transmission using IPsec is disabled.
FTP	TCP:21	• Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Remote Communication Gate S	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".
ssh/sftp	TCP:22	• Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Remote Communication Gate S	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 • SmartDeviceMonitor for Admin	Commands using telnet are disabled.
SMTP	TCP:25 (variable)	• Control Panel • Web Image Monitor • SmartDeviceMonitor for Admin • Remote Communication Gate S	E-mail notification function that require SMTP reception cannot be used.

Protocol	Port	Setting Method	When Disabled
HTTP	TCP:80	• Web Image Monitor • telnet • SmartDeviceMonitor for Admin	Functions that require HTTP cannot be used. Cannot print using IPP on port 80.
HTTPS	TCP:443	• Web Image Monitor • telnet • SmartDeviceMonitor for Admin	Functions that require HTTPS cannot be used. @Remote cannot be used. You can also make settings to require SSL transmission using the control panel or Web Image Monitor.
SMB	TCP:139	• Control Panel • Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Remote Communication Gate S	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.
SNMPv1,v2	UDP:161	• Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Remote Communication Gate S	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.

Protocol	Port	Setting Method	When Disabled
SNMPv3	UDP:161	• Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Remote Communication Gate S	Functions that require SNMPv3 cannot be used. You can also make settings to require SNMPv3 encrypted transmission and restrict the use of other transmission methods using the control panel, Web Image Monitor, or telnet.
RSH/RCP	TCP:514	• Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Remote Communication Gate S	Functions that require RSH and network TWAIN functions cannot be used. You can restrict personal information from being displayed by making settings on the control panel using "Restrict Display of User Information".
LPR	TCP:515	• Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Remote Communication Gate S	LPR functions cannot be used. You can restrict personal information from being displayed by making settings on the control panel using "Restrict Display of User Information".

Protocol	Port	Setting Method	When Disabled
IPP	TCP:631	• Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Remote Communication Gate S	IPP functions cannot be used.
SSDP	UDP:1900	• Web Image Monitor • telnet • SmartDeviceMonitor for Admin	Device discovery using UPnP from Windows cannot be used.
Bonjour	UDP:5353	• Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Remote Communication Gate S	Bonjour functions cannot be used.
@Remote	TCP:7443 TCP:7444	• telnet	@Remote cannot be used.
DIPRINT	TCP:9100	• Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Remote Communication Gate S	DIPRINT functions cannot be used.
RFU	TCP:10021	• telnet	You can attempt to update firmware via FTP.

Protocol	Port	Setting Method	When Disabled
NetWare	(IPX/SPX)	• Control Panel • Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Remote Communication Gate S	Cannot print with NetWare. SNMP over IPX cannot be used.
WSD (Device)	TCP:53000 (variable)	• Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Remote Communication Gate S	WSD (Device) functions cannot be used.
WSD (Printer)	TCP:53001 (variable)	• Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Remote Communication Gate S	WSD (Printer) functions cannot be used.
WS-Discovery	UDP/TCP:3702	• telnet • Remote Communication Gate S	WSD (Device, Printer) search function cannot be used.

Note

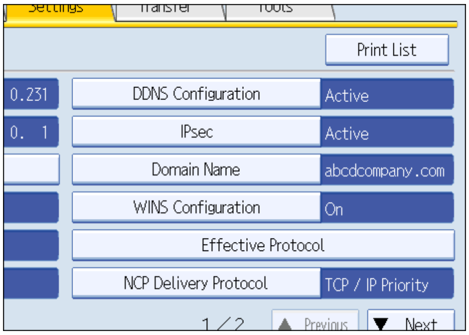
- "Restrict Display of User Information" is one of the Extended Security features. For details about making this setting, see "Specifying the Extended Security Functions".

Reference

- p.33 "Logging in Using Administrator Authentication"
- p.34 "Logging out Using Administrator Authentication"
- p.221 "Specifying the Extended Security Functions"

Enabling and Disabling Protocols Using the Control Panel

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



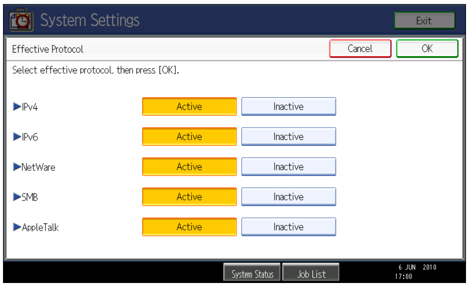
Settings | Transfer | Tools

Print List

0.231	DDNS Configuration	Active
0. 1	IPsec	Active
	Domain Name	abcdcompany.com
	WINS Configuration	On
	Effective Protocol	
	NCP Delivery Protocol	TCP / IP Priority

1 / 2 ▲ Previous ▼ Next

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



System Settings Exit

Effective Protocol Cancel OK

Select effective protocol, then press [OK].

▶IPv4	Active	Inactive
▶IPv6	Active	Inactive
▶NetWare	Active	Inactive
▶SMB	Active	Inactive
▶AppleTalk	Active	Inactive

System Status Job List 6 JUN 2010 17:00

6. **Press [OK].**
7. **Press the [User Tools/Counter] 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.**

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

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

   The network administrator can log in.

   Enter the login user name and login password.

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

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

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

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

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

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

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

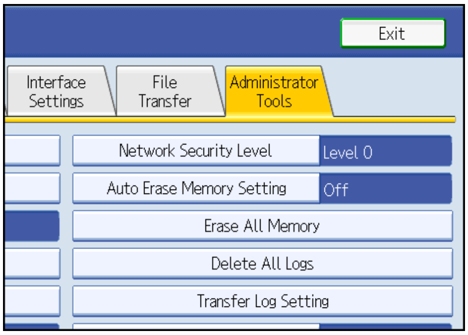
Reference

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

Specifying Network Security Level Using the Control Panel

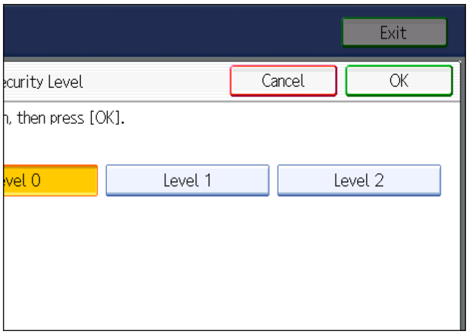
1. **Press the [User Tools/Counter] key.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**

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



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

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



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

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

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

   The top page of Web Image Monitor appears.

3. **Click [Login].**

   The network administrator can log in.

   Enter the login user name and login password.

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

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

Status of Functions under Each Network Security Level

Tab Name:TCP/IP

Function	Level 0	Level 1	Level 2
TCP/IP	Active	Active	Active
HTTP> Port 80	Open	Open	Open
IPP> Port 80	Open	Open	Open
IPP> Port 631	Open	Open	Close
SSL/TLS> Port 443	Open	Open	Open
SSL/TLS> Permit SSL/TLS Communication	Ciphertext Priority	Ciphertext Priority	Ciphertext Only
DIPRINT	Active	Active	Inactive
LPR	Active	Active	Inactive
FTP	Active	Active	Active
sftp	Active	Active	Active
ssh	Active	Active	Active
RSH/RCP	Active	Active	Inactive
TELNET	Active	Inactive	Inactive
Bonjour	Active	Active	Inactive
SSDP	Active	Active	Inactive
SMB	Active	Active	Inactive
NetBIOS over TCP/IPv4	Active	Active	Inactive
WSD (Device)	Active	Active	Inactive

Function	Level 0	Level 1	Level 2
WSD (Printer)	Active	Active	Inactive

The same settings are applied to IPv4 and IPv6.

Tab Name:NetWare

Function	Level 0	Level 1	Level 2
NetWare	Active	Active	Inactive

If NetWare is not used on your network, the above settings are not applicable.

Tab Name:SNMP

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

Encrypting Transmitted Passwords

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

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

Driver Encryption Key

Encrypt the password transmitted when specifying user authentication.

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

Password for IPP Authentication

To encrypt the IPP Authentication password on Web Image Monitor, set "Authentication" to [DIGEST], and then specify the IPP Authentication password set on the machine.

You can use telnet or FTP to manage passwords for IPP authentication, although it is not recommended.

Specifying a Driver Encryption Key

This can be specified by the network administrator.

Specify the driver encryption key on the machine.

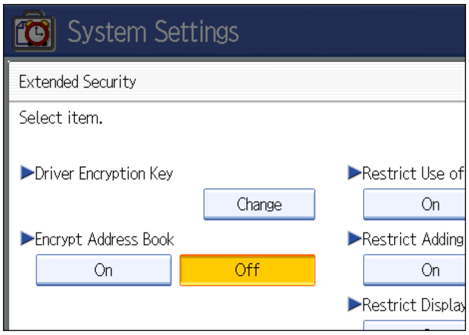
You can enhance security to make login passwords harder to break.

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

1. **Press the [User Tools/Counter] 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. **For "Driver Encryption Key", press [Change].**



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

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

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

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

7. **Press [OK].**

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

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

Reference

- p.33 "Logging in Using Administrator Authentication"
- p.34 "Logging out Using Administrator Authentication"
- p.221 "Specifying the Extended Security Functions"

Specifying an IPP Authentication Password

This can be specified by the network administrator.

Specify the IPP authentication passwords for the machine using Web Image Monitor.

You can enhance security to make IPP authentication passwords harder to break.

1. **Open a Web browser.**

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

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

The top page of Web Image Monitor appears.

3. **Click [Login].**

   The network administrator can log in. Enter the login user name and login password.

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

   The IPP Authentication page appears.

5. **Select [DIGEST] from the "Authentication" list.**
6. **Enter the user name in the "User Name" box.**
7. **Enter the password in the "Password" box.**
8. **Click [OK].**

   IPP authentication is specified.

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

Note

- When using the IPP port under Windows XP/Vista/7, Windows Server 2003/2003 R2/2008/2008 R2, you can use the operating system's standard IPP port.

Protection Using Encryption

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

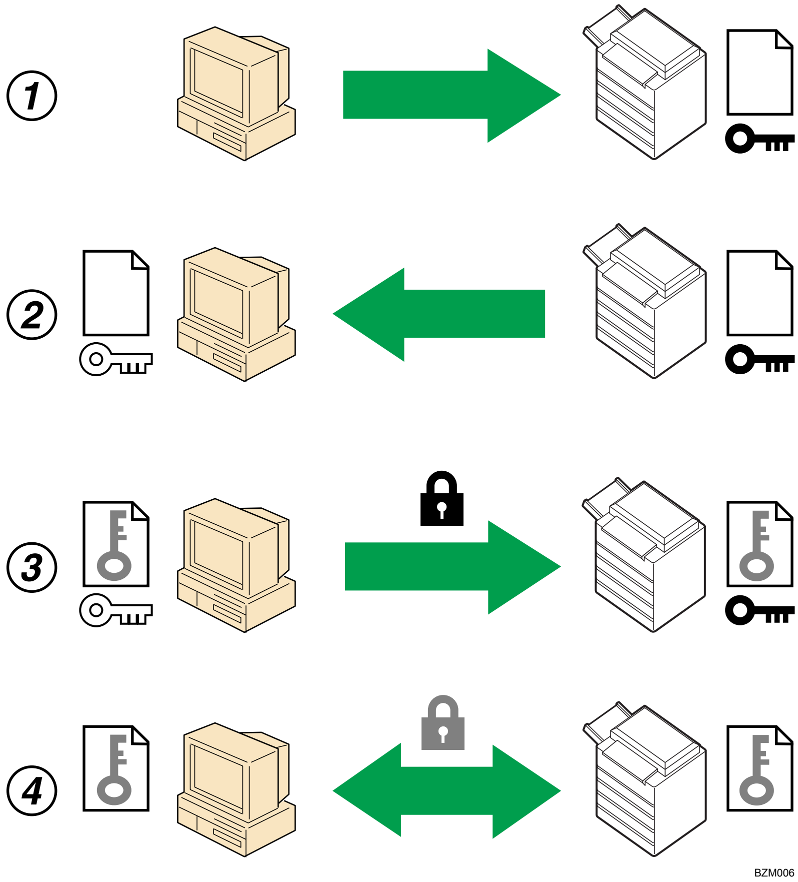
SSL (Secure Sockets Layer) Encryption

This can be specified by the network administrator.

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

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

SSL (Secure Sockets Layer)



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

2. **The device certificate and public key are sent from the machine to the user's computer.**
3. **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.
- If you enable SSL for IPP (printer functions), sent data is encrypted, preventing it from being intercepted, analyzed, or tampered with.

Creating and Installing the Self-Signed Certificate

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

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

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

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

   The top page of Web Image Monitor appears.

3. **Click [Login].**

   The network administrator can log in.

   Enter the login user name and login password.

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

   The Device Certificate page appears.

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

   The setting is changed.

9. **Click [OK].**

   A security warning dialog box appears.

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

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

11. **Click [Logout].**

Note

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

Creating the Device Certificate (Issued by a Certificate Authority)

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

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

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

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

   The top page of Web Image Monitor appears.

3. **Click [Login].**

   The network administrator can log in.

   Enter the login user name and login password.

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

   The Device Certificate page appears.

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

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

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

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

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

Note

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

Installing the Device Certificate (Issued by a Certificate Authority)

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

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

Enter the device certificate contents issued by the certificate authority.

Installation of the certificate is especially necessary for users who want to print via IPP -SSL from Windows Vista/7, Windows Server 2008/2008 R2.

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

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

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

   The network administrator can log in.

Enter the login user name and login password.

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

   The Device Certificate page appears.

5. **Click [Certificate1].**
6. **Click [Install].**
7. **Enter the contents of the device certificate.**

   In the certificate 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 [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. Otherwise, validation by the certificate authority will not be performed correctly. In this case, a warning message may appear when you try to add a printer using IPP-SSL under Windows Vista/7, Windows Server 2008/2008 R2 or when the destination user receives an e-mail with an S/MIME signature. A warning message might also appear if you attempt to access this machine through Web Image Monitor with SSL enabled. To enable authentication from the client computer, install the intermediate certificate on the client computer, and then reestablish connection.
- Intermediate certificates cannot be installed on this machine.

Enabling SSL

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

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

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

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

   The top page of Web Image Monitor appears.

3. **Click [Login].**

   The network administrator can log in.

   Enter the login user name and login password.

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

   The SSL/TLS page appears.

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

   The SSL setting is enabled.

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

Note

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

User Settings for SSL (Secure Sockets Layer)

We recommend that after installing the self-signed certificate or device certificate from a private certificate authority on the main unit and enabling SSL (communication encryption), you instruct users to install the certificate on their computers. Installation of the certificate is especially necessary for users who want to print via IPP-SSL from Windows Vista/7, Windows Server 2008/2008 R2. 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 when accessing the machine using IPP, see Web Image Monitor Help.
- If a certificate issued by a certificate authority is installed in the machine, confirm the certificate store location with the certificate authority.
- Printing via the standard IPP port under Windows Vista/7, Windows Server 2008/2008 R2 is possible only after the hostname or IP address is specified in the device certificate's [Common Name] setting. If the host name or IP address has changed, the user must delete the printer installed on the client computer. The printer must be reinstalled if the client computer's device certificate has been updated. Also, if a user's authentication information (login user name and password) has changed, the printer must be deleted, then the user's information settings must be updated, and then the printer must be reinstalled.

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.

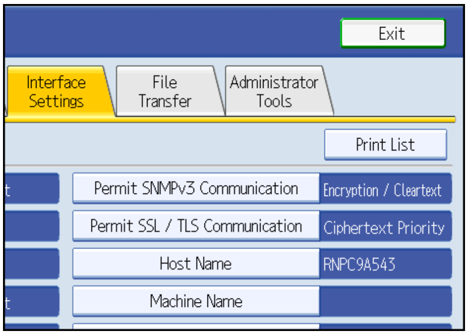
Specifying the SSL/TLS Encryption Mode

This can be specified by the network administrator.

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

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

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



Permit SNMPv3 Communication: Encryption / Cleartext

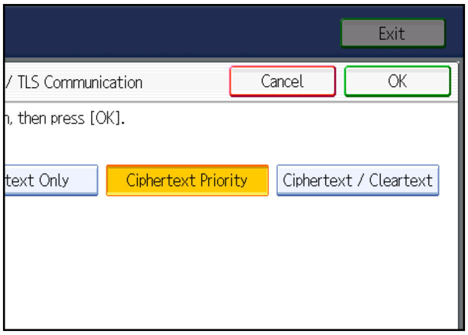
Permit SSL / TLS Communication: Ciphertext Priority

Host Name: RNPC9A543

Machine Name

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/Counter] key.**

Note

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

Reference

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

SNMPv3 Encryption

This can be specified by the network administrator.

When using SmartDeviceMonitor for Admin or another application to make various settings, you can encrypt the data transmitted.

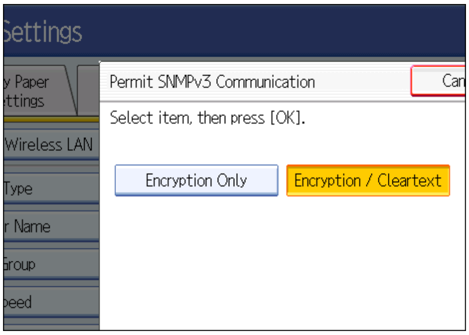
By making this setting, you can protect data from being tampered with.

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

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



Permit SNMPv3 Communication

Select item, then press [OK].

Encryption Only | Encryption / Cleartext

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

Note

- To use SmartDeviceMonitor for Admin for encrypting the data for specifying settings, you need to specify the network administrator's [Encryption Password] setting and [Encryption Password] in [SNMP Authentication Information] in SmartDeviceMonitor for Admin, in addition to specifying [Permit SNMPv3 Communication] on the machine. For details about specifying [Encryption Password] in SmartDeviceMonitor for Admin, see SmartDeviceMonitor for Admin Help.
- If network administrator's [Encryption Password] setting is not specified, the data for transmission may not be encrypted or sent. For details about specifying the network administrator's [Encryption Password] setting, see "Registering the Administrator".

Reference

- p.33 "Logging in Using Administrator Authentication"
- p.34 "Logging out Using Administrator Authentication"
- p.30 "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
Phase 1 Encryption Algorithm	DES	3DES	3DES
Phase 1 Diffie-Hellman Group	2	2	2

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

Encryption Key Auto Exchange 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

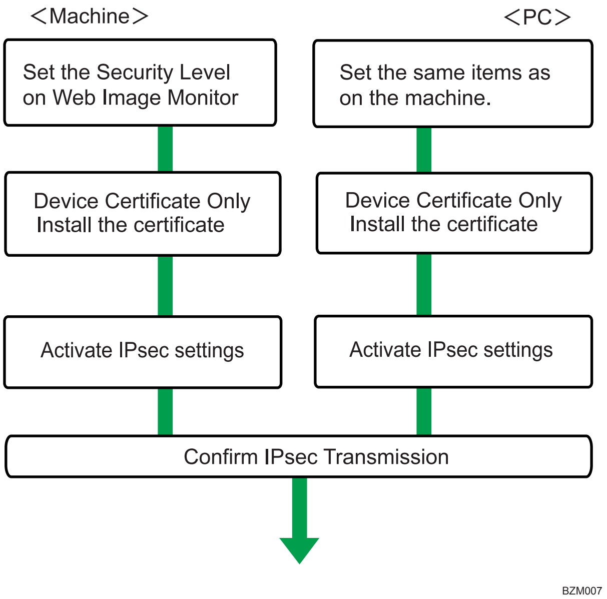
Setting	Description	Setting Value
SPI (Input)	Specify the same value as your transmission partner's SPI output value.	Any number between 256 and 4095
Security Protocol	To apply both encryption and authentication to sent data, specify "ESP" or "ESP+AH". To apply authentication data only, specify "AH".	• 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 section explains the procedure for specifying Encryption Key Auto Exchange Settings.

This can be specified by the network administrator.



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

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

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

   The network administrator can log in.

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

   The IPsec settings page appears.

5. **Click [Edit] under "Encryption Key Auto Exchange Settings".**
6. **Make encryption key auto exchange settings in [Settings 1].**

   If you want to make multiple settings, select the settings number and add settings.
7. **Click [OK].**
8. **Select [Active] for "IPsec" 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 "Using S/MIME to Protect E-mail Transmission".

Reference

- p.109 "Using S/MIME to Protect E-mail Transmission"

Selecting the Certificate for IPsec

This can be specified by the network administrator.

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

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

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

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

   The network administrator can log in.

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

   The Device Certificate page appears.
5. **Select the certificate to be used for IPsec from the drop down box in "IPsec" under "Certification".**

6. **Click [OK].**

   The certificate for IPsec is specified.

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

Specifying IPsec Settings on the Computer

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

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.

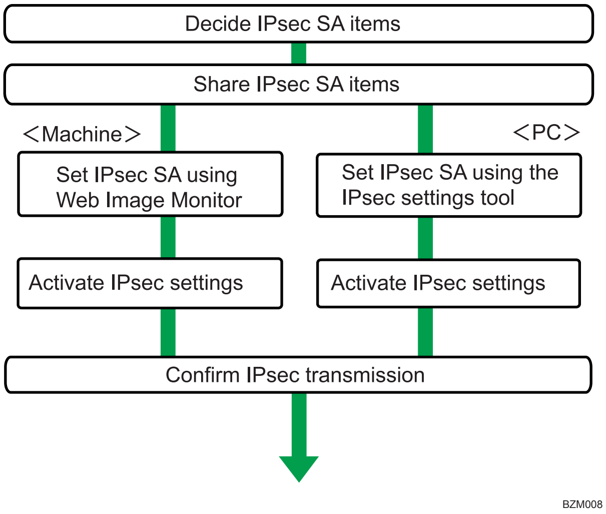
Note

- 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 the group number for "Phase 1 Diffie-Hellman Group" and "Phase 2 PFS" on the machine to establish IPsec transmission.

Encryption Key Manual Settings Configuration Flow

This section explains the procedure for specifying encryption key manual settings.

This can be specified by the network administrator.



Note

- Before transmission, SA information is shared and specified by the sender and receiver. To prevent SA information leakage, we recommend that this exchange is not performed over the network.
- After configuring IPsec, you can use "Ping" command to check if the connection is established correctly. However, you cannot use "Ping" command when ICMP is excluded from IPsec transmission. Also,

because the response is slow during initial key exchange, it may take some time to confirm that transmission has been established.

Specifying Encryption Key Manual Settings

This can be specified using Web Image Monitor.

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

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

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

   The network administrator can log in.

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

   The IPsec settings page appears.
5. **Select [Active] for "Encryption Key Manual Settings".**
6. **Click [Edit] under "Encryption Key Manual Settings".**
7. **Set items for encryption key manual settings in [Settings 1].**

   If you want to make multiple settings, select the settings number and add settings.
8. **Click [OK].**
9. **Select [Active] for "IPsec" in "IPsec".**
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 manual {1|2|3|4|default} disable
```

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

Specify the local/remote address for settings 1-4

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

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

Specify the address type in default setting

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

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

Security policy setting

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

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

This section explains Authentication by telnet. When using telnet, the default login name for administrator login is "admin" and the password is blank. For details on how to login to telnet, see "Using telnet", Network and System Settings Reference.

"authfree" Command

Use the "authfree" command to display and configure authentication exclusion control settings. If you use the "authfree" command in telnet, you can exclude printer job authentication and specify an IP address range. The authentication exclusion control display and setting methods are explained below.

View Settings

```
msh> authfree
```

If print job authentication exclusion is not specified, authentication exclusion control is not displayed.

IPv4 address settings

```
msh> authfree "ID" range_addr1 range_addr2
```

IPv6 address settings

```
msh> authfree "ID" range6_addr1 range6_addr2
```

IPv6 address mask settings

```
msh> authfree "ID" mask6_addr1 masklen
```

USB settings

```
msh> authfree usb [on|off]
```

- To enable authfree, specify "on". To disable authfree, specify "off".
- Always specify the interface.

Authentication exclusion control initialization

```
msh> authfree flush
```

Note

- In both IPv4 and IPv6 environments, up to five access ranges can be registered and selected.

Authentication by IEEE802.1X

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

8. Specifying the Extended Security Functions

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

Specifying the Extended Security Functions

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

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

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

Changing the Extended Security Functions

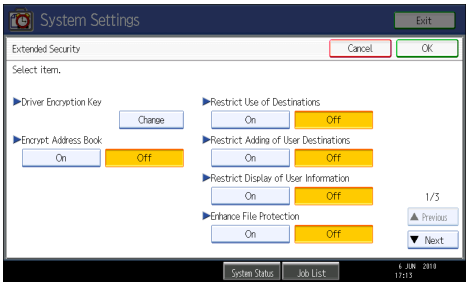
This section describes how to change the Extended Security Functions.

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

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

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



System Settings

Extended Security

Select item.

▶Driver Encryption Key

▶Encrypt Address Book: On [✓ Off]

▶Restrict Use of Destinations: On [✓ Off]

▶Restrict Adding of User Destinations: On [✓ Off]

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

▶Enhance File Protection: On [✓ Off]

1/3

6 JUN 2010 17:13

6. **Press [OK].**

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

Reference

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

Extended Security Settings

Driver Encryption Key

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

Encrypt Address Book

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

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

Default: [Off]

Restrict Use of Destinations

This can be specified by the user administrator.

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

A user cannot directly enter the destinations for transmission.

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

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

For details about preventing unauthorized transmission, see "Preventing Information Leakage Due to Unauthorized Transmission".

Default: [Off]

Restrict Adding of User Destinations

This can be specified by the user administrator.

If you set "Restrict Adding of User Destinations" to [Off], users will be able to register a scanner destination in the Address Book simply by entering the destination and then pressing [Prg. Dest.]. If you set these functions to [On], the [Prg. Dest.] key will not appear. Users will still be able to enter a destination directly using the scanner screen, but cannot then register that destination in the Address Book by pressing [Prg. Dest.]. Note too that if you set these functions to [On], only the user administrator can register new users in the Address Book and change the passwords and other information of existing registered users.

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 "*********". For example, when someone not authenticated as an administrator checks the job history using SNMP in SmartDeviceMonitor for Admin, personal information can be displayed as "*********" so that users cannot be identified. Because information identifying registered users cannot be viewed, unauthorized users are prevented from obtaining information about the registered files.

Default: [**Off**]

Enhance File Protection

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

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

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

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

Default: [**Off**]

Settings by SNMPv1, v2

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

Default: [**Do not Prohibit**]

Restrict Use of Simple Encryption

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

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

Default: [**Off**]

Authenticate Current Job

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

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

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

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

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

Default: [**Off**]

Password Policy

This can be specified by the user administrator.

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

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

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

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

Default: [**Off**]

Passwords can contain the following characters:

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

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

@Remote Service

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**]

Reference

- p.117 "Protecting the Address Book"
- p.107 "Preventing Information Leakage Due to Unauthorized Transmission"
- p.191 "Setting the SSL/TLS Encryption Mode"

Other Security Functions

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

Scanner Function

Print & Delete Scanner Journal

When user authentication is enabled, "Print & Delete Scanner Journal" is automatically set to [Do not Print: Disable Send] in order to prevent personal information in transmission/delivery history from being automatically printed. In this case, the scanner is automatically disabled when the journal history exceeds 250 transmissions/deliveries. When this happens, click [Print Scanner Journal] or [Delete Scanner Journal]. To print the scanner journal automatically, set [On] for "Print & Delete Scanner Journal". For details, see "Scanner Features", Scanner Reference.

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.

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 "Logging in Using Administrator Authentication" and "Logging out Using Administrator Authentication".

Service Mode Lock

This can be specified by the machine administrator. Service mode is used by a service representative for inspection or repair. If you set "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.

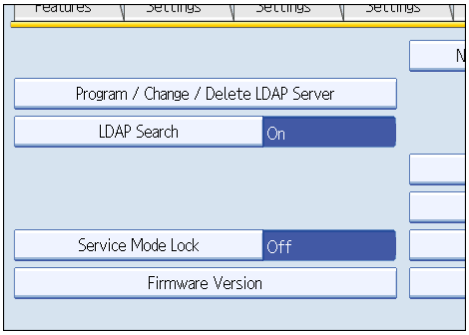
Reference

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

Specifying Service Mode Lock

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

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

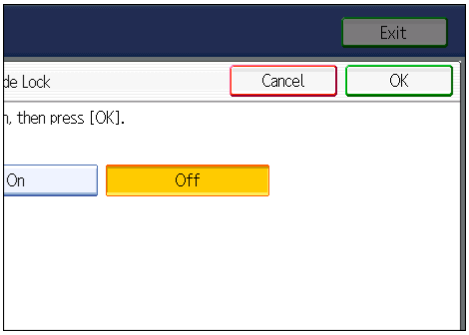


LDAP Search On

Service Mode Lock Off

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

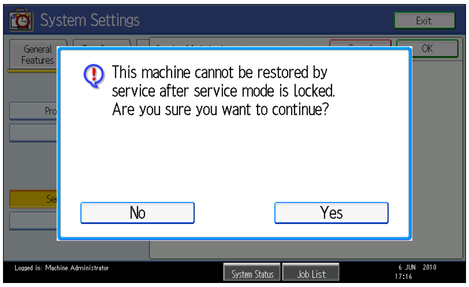
5. **Press [On], and then press [OK].**



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/Counter] key.**

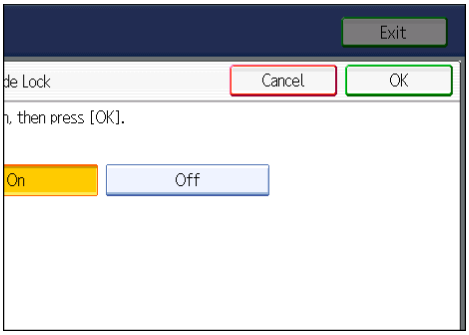
Canceling Service Mode Lock

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/Counter] 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].**



de Lock

n, then press [OK].

6. **Press the [User Tools/Counter] 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 "Auto Logout".
System Settings	Administrator Tools	User Authentication Management	Select [Basic Auth.], and then set "Printer Job Authentication" to [Entire]. See "Basic Authentication".
System Settings	Administrator Tools	Administrator Authentication Management/User Management	Select [On], and then select [Administrator Tools] for "Available Settings". See "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 "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 "Enabling Administrator Authentication".

Menu	Tab	Item	Setting
System Settings	Administrator Tools	Administrator Authentication Management/File Management	Select [On], and then select [Administrator Tools] for "Available Settings". See "Enabling Administrator Authentication".
System Settings	Administrator Tools	Extended Security/ Settings by SNMPv1, v2	Prohibit See "Specifying the Extended Security Functions".
System Settings	Administrator Tools	Extended Security/ Restrict Use of Simple Encryption	Off See "Specifying the Extended Security Functions".
System Settings	Administrator Tools	Extended Security/ Authenticate Current Job	Access Privilege See "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 "Specifying the Extended Security Functions".
System Settings	Administrator Tools	Network Security Level	Level 2 To acquire the machine status through printer driver or Web Image Monitor, set "SNMP" to Active on Web Image Monitor. See "Specifying Network Security Level".
System Settings	Administrator Tools	Service Mode Lock	On See "Limiting Machine Operations to Customers Only".

Menu	Tab	Item	Setting
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 "Encrypting Data on the Hard Disk".

Menu	Tab	Item	Setting
Scanner Features	Initial Settings	Menu Protect	Level 2 See "Menu Protect".

Note

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

Reference

- p.86 "Auto Logout"
- p.45 "Basic Authentication"
- p.27 "Enabling Administrator Authentication"
- p.221 "Specifying the Extended Security Functions"
- p.179 "Specifying Network Security Level"
- p.227 "Limiting Machine Operations to Customers Only"
- p.121 "Encrypting Data on the Hard Disk"
- p.139 "Menu Protect"
- p.226 "Other Security Functions"

Settings You Can Configure Using Web Image Monitor

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

Category	Item	Setting
Device Settings/ Logs	Collect Job Logs	Active

Category	Item	Setting
Device Settings/ Logs	Collect Access Logs	Active
Security/User Lockout Policy	Lockout	Active
Security/User Lockout Policy	Number of Attempts before Lockout	5 times or less. See "User Lockout Function".
Security/User Lockout Policy	Lockout Release Timer	Set to Active or Inactive. When setting to Active, set the Lockout release timer to 60 minutes or more. See "User Lockout Function".
Security/User Lockout Policy	Lock Out User for	When setting "Lockout Release Timer" to[Active], set the Lockout release timer to 60 minutes or more. See "User Lockout Function".
Network/ SNMPv3	SNMPv3 Function	Inactive To use SNMPv3 functions, set "SNMPv3 Function" to [Active], and set "Permit SNMPv3 Communication" to [Encryption Only]. Because SNMPv3 enforces authentication for each packet, Login log will be disabled as long as SNMPv3 is active.
Security/Network Security	FTP	Inactive Before specifying this setting, set "Network Security Level" to [Level 2] on the control panel.
Security	S/MIME	"Encryption Algorithm": 3DES-168 bit You must register the user certificate in order to use S/MIME.
Address Book/E-mail	User Certificate	You must register the user certificate in order to use S/MIME.

Note

- For details about specifying an encryption algorithm and registering a user certificate, see "Using S/MIME to Protect Email Transmission".

Reference

- p.83 "User Lockout Function"
- p.109 "Using S/MIME to Protect E-mail Transmission"

Settings You Can Configure When IPsec Is Available/Unavailable

All communication to and from machines on which IPsec is enabled is encrypted.

If your network supports IPsec, we recommend you enable it.

Settings you can configure when IPsec is available

If IPsec is available, configure the settings shown in the following table to enhance the security of the data traveling on your network.

Control panel settings

Menu	Tab	Item	Setting
System Settings	Interface Settings	IPsec	Active
System Settings	Interface Settings	Permit SSL / TLS Communication	Ciphertext Only

8

Web Image Monitor settings

Category	Item	Setting
Security/IPsec	Encryption Key Manual Settings	Inactive
Security/IPsec	Encryption Key Auto Exchange Settings/ Security Level	Authentication and High Level Encryption

Note

- You can set "IPsec" and "Permit SSL/TLS Communication" using either Web Image Monitor or the machine's control panel.

Settings you can configure when IPsec is unavailable

If IPsec is not available, configure the settings shown in the following table to enhance the security of the data traveling on your network.

Control panel settings

Menu	Tab	Item	Setting
System Settings	Interface Settings	IPsec	Inactive
System Settings	Interface Settings	Permit SSL / TLS Communication	Ciphertext Only

Securing data when IPsec is unavailable

The following procedures make user data more secure when IPsec is unavailable.

Administrators must inform users to carry out these procedures.

- Printer

  To use the printer functions, specify "SFTP" as the protocol, or specify "IPP" and enable SSL.

  For details about SFTP, see "Special Operations under Windows", Network and System Settings Reference.

  For details about IPP settings, see "Installing the Printer Driver for the Selected Port", Printer Reference.

  For details about SSL settings, see "Protection Using Encryption".

- Scanner

  Send the URL of scanned files to destinations by configuring [Send Settings] in [Scanner Features], instead of sending the actual scanned files. Use Web Image Monitor through your network to view, delete, send, and download scanned files.

  When sending scanned files attached to e-mail, protect them by applying an S/MIME certificate. To do this, configure the "Security" settings prior to sending. For details about sending e-mail from the scanner, see "Sending Scan Files by E-mail", Scanner Reference.

Note

- For details about enabling and disabling IPsec using the control panel, see "System Settings", Network and System Settings Reference.
- For details about the setting for permitting SSL/TLS communication, see "Setting the SSL/TLS Encryption Mode".
- For details about specifying the IPsec setting via Web Image Monitor, see "Transmission Using IPsec".

Reference

- p.186 "Protection Using Encryption"
- p.191 "Setting the SSL/TLS Encryption Mode"
- p.195 "Transmission Using IPsec"

9. 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 "Configuring User Authentication".
"The selected file(s) contained file (s) without access privileges. Only file(s) with access privileges will be deleted."	You have tried to delete files without the authority to do so.	Files can be deleted by the file creator (owner) or file administrator. To delete a file which you are not authorized to delete, contact the file creator (owner).

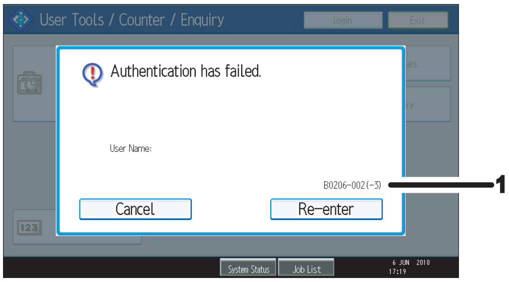
Reference

- p.39 "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



User Tools / Counter / Enquiry

Authentication has failed.

User Name:

B0206-002(-3)

CAN002S

1. **error code**

   An error code appears.

Basic Authentication

Error Code	Cause	Solution
B0103-000	A TWAIN operation occurred during authentication.	Make sure no other user is logged on to the machine, and then try again.
B0104-000	Failed to decrypt password.	1. A password error occurred. Make sure the password is entered correctly. 2. "Restrict Use of Simple Encryption" is enabled. The administrator has restricted use of simple encryption. You can use the encryption key if it has been specified in the driver. 3. A driver encryption key error occurred. Make sure that the encryption key is correctly specified on the driver.
B0105-000	A login user name was not specified but a DeskTopBinder operation was performed.	Specify the DeskTopBinder login user name correctly.
B0206-002	1. A login user name or password error occurred.	Make sure the login user name and password are entered correctly and then log in.
B0206-002	2. The user attempted authentication from an application on the "System Settings" screen, where only the administrator has authentication ability.	Only the administrator has login privileges on this screen. Log in as a general user from the application's login screen.

Error Code	Cause	Solution
B0206-003	An authentication error occurred because the user name contains a space, colon (:), or quotation mark (").	Recreate the account if the account name contains any of these prohibited characters. If the account name was entered incorrectly, enter it correctly and log in again.
B0207-001	An authentication error occurred because the Address Book is being used at another location.	Wait a few minutes and then try again.
B0208-000	The account is locked because you have reached the maximum number of failed authentication attempts allowed.	Ask the user administrator to unlock the account.

Windows Authentication

Error Code	Cause	Solution
W0103-000	A TWAIN operation occurred during authentication.	Make sure no other user is logged in to the machine, and then try again.
W0104-000	Failed to encrypt password.	1. A password error occurred. Make sure the password is entered correctly. 2. "Restrict Use of Simple Encryption" is enabled. The administrator has restricted use of simple encryption. You can use the encryption key if it has been specified in the driver. 3. A driver encryption key error occurred. Make sure that the encryption key is correctly specified on the driver.

Error Code	Cause	Solution
W0105-000	A login user name was not specified but a DeskTopBinder operation was performed.	Set the DeskTopBinder login user name correctly.
W0206-002	The user attempted authentication from an application on the "System Settings" screen, where only the administrator has authentication ability.	Only the administrator has login privileges on this screen. Log in as a general user from the application's login screen.
W0206-003	An authentication error occurred because the user name contains a space, colon (:), or quotation mark (").	Recreate the account if the account name contains any of these prohibited characters. If the account name was entered incorrectly, enter it correctly and log in again.
W0207-001	An authentication error occurred because the Address Book is being used at another location.	Wait a few minutes and then try again.
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.

Error Code	Cause	Solution
W0406-104	1. Cannot connect to the authentication server.	Make sure that connection to the authentication server is possible. Use the PING Command to check the connection.
W0406-104	2. A login name or password error occurred.	Make sure that the user is registered on the server. Use a registered login user name and password.
W0406-104	3. A domain name error occurred.	Make sure that the Windows authentication domain name is specified correctly.
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
L0103-000	A TWAIN operation occurred during authentication.	Make sure no other user is logged in to the machine, and then try again.
L0104-000	Failed to encrypt password.	1. A password error occurred. Make sure the password is entered correctly. 2. "Restrict Use of Simple Encryption" is enabled. The administrator has restricted use of simple encryption. You can use the encryption key if it has been specified in the driver. 3. A driver encryption key error occurred. Make sure that the encryption key is correctly specified on the driver.
L0105-000	A login user name was not specified but a DeskTopBinder operation was performed.	Set the DeskTopBinder login user name correctly.

Error Code	Cause	Solution
L0206-002	A user attempted authentication from an application on the "System Settings" screen, where only the administrator has authentication ability.	Only the administrator has login privileges on this screen. Log in as a general user from the application's login screen.
L0206-003	An authentication error occurred because the user name contains a space, colon (:), or quotation mark (").	Recreate the account if the account name contains any of these prohibited characters. If the account name was entered incorrectly, enter it correctly and log in again.
L0207-001	An authentication error occurred because the Address Book is being used at another location.	Wait a few minutes and then try again.
L0306-018	The LDAP server is not correctly configured.	Make sure that a connection test is successful with the current LDAP server configuration.
L0307-001	An authentication error occurred because the Address Book is being used at another location.	Wait a few minutes and then try again.
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".

Error Code	Cause	Solution
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.
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.

Error Code	Cause	Solution
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.
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.

Error Code	Cause	Solution
L0400-210	Failed to obtain user information in LDAP search.	The login attribute's search criteria might not be specified or the specified search information is unobtainable. Make sure the login name attribute is specified correctly.
L0406-003	An authentication error occurred because the user name contains a space, colon (:), or quotation mark (").	Recreate the account if the account name contains any of these prohibited characters. If the account name was entered incorrectly, enter it correctly and log in again.
L0409-000	Authentication timed out because the server did not respond.	Contact the server or network administrator. If the situation does not return to normal, contact your service representative.
L0511-000	The authentication server login name is the same as a user name already registered on the machine. (Names are distinguished by the unique attribute specified in the LDAP authentication settings.)	1. Delete the old, duplicated name or change the login name. 2. If the authentication server has just been changed, delete the old name on the server.
L0607-001	An authentication error occurred because the Address Book is being used at another location.	Wait a few minutes and then try again.
L606-004	Authentication failed because the user name contains language that cannot be used by general users.	Do not use "other", "admin", "supervisor" or "HIDE*" in general user accounts.
L0612-005	Authentication failed because no more users can be registered. (The number of users registered in the Address Book has reached capacity.)	Ask the user administrator to delete unused user accounts in the Address Book.

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

Integration Server Authentication

Error Code	Cause	Solution
I0103-000	A TWAIN operation occurred during authentication.	Make sure no other user is logged in to the machine, and then try again.
I0104-000	Failed to decrypt password.	1. A password error occurred. Make sure the password is entered correctly. 2. "Restrict Use of Simple Encryption" is enabled. The administrator has restricted use of simple encryption. You can use the encryption key if it has been specified in the driver. 3. A driver encryption key error occurred. Make sure that the encryption key is correctly specified on the driver.
I0105-000	A login user name was not specified but a DeskTopBinder operation was performed.	Set the DeskTopBinder login user name correctly.
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
Cannot connect with the TWAIN driver.	User authentication has been rejected.	Confirm the user name and login name with the administrator of the network in use if using Windows authentication, LDAP authentication, or Integration Server authentication. Confirm with the user administrator if using Basic authentication.
Cannot connect with the TWAIN driver.	The encryption key specified in the driver does not match the machine's driver encryption key.	Specify the driver encryption key registered in the machine. See "Specifying a Driver Encryption Key".
Cannot connect with the TWAIN driver.	The SNMPv3 account, password, and encryption algorithm do not match settings specified on this machine.	Specify the account, password and the encryption algorithm of SNMPv3 registered in the machine using network connection tools.
Cannot authenticate using the TWAIN driver.	Another user is logging in to the machine.	Wait for the user to log out.
Cannot authenticate using the TWAIN driver.	Authentication is taking time because of operating conditions.	Make sure the LDAP server setting is correct. Make sure the network settings are correct.
Cannot authenticate using the TWAIN driver.	Authentication is not possible while the machine is editing the Address Book data.	Wait until editing of the Address Book data is complete.
After starting "User Management Tool" or "Address Management Tool" in SmartDeviceMonitor for Admin and entering the correct login user name and password, a message that an incorrect password has been entered appears.	"Restrict Use of Simple Encryption" is not set correctly. Alternatively, "SSL/TLS" has been enabled although the required certificate is not installed in the computer.	Set "Restrict Use of Simple Encryption" to [On]. Alternatively, enable "SSL/TLS", install the server certificate in the machine, and then install the certificate in the computer. See "Setting the SSL/TLS Encryption Mode".

Condition	Cause	Solution
Cannot log in to the machine using [Document Server (MFP): Authentication/Encryption] in DeskTopBinder.	"Restrict Use of Simple Encryption" is not set correctly. Alternatively, "SSL/TLS" has been enabled although the required certificate is not installed in the computer.	Set "Restrict Use of Simple Encryption" to [On]. Alternatively, enable "SSL/TLS", install the server certificate in the machine, and then install the certificate in the computer. See "Setting the SSL/TLS Encryption Mode".
Cannot access the machine using ScanRouter EX Professional V3 / ScanRouter EX Enterprise V2.	"Restrict Use of Simple Encryption" is not set correctly. Alternatively, "SSL/TLS" has been enabled although the required certificate is not installed in the computer.	Set "Restrict Use of Simple Encryption" to [On]. Alternatively, enable "SSL/TLS", install the server certificate in the machine, and then install the certificate in the computer. See "Setting the SSL/TLS Encryption Mode".
Cannot connect to the ScanRouter delivery software.	The ScanRouter delivery software may not be supported by the machine.	Update to the latest version of the ScanRouter delivery software.
Cannot access the machine using ScanRouter EX Professional V2.	ScanRouter EX Professional V2 does not support user authentication.	ScanRouter EX Professional V2 does not support user authentication.
Cannot log out when using the copying or scanner functions.	The original has not been scanned completely.	When the original has been scanned completely, press [#], remove the original, and then log out.
"Prg. Dest." does not appear on the scanner screen for specifying destinations.	"Restrict Adding of User Destinations" is set to [On] in "Restrict Use of Destinations" under "Extended Security", so only the user administrator can register destinations in the Address Book on the scanner screen.	Registration must be done by the user administrator.

Condition	Cause	Solution
User authentication is disabled, yet stored files do not appear.	User authentication might have been disabled without "All Users" being selected for user access to stored files.	Re-enable user authentication, and select [All Users] as the access permission setting of the files you want to display. For details, see "Configuring Access Permissions for Stored Files".
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 "Protecting the Address Book".
Cannot print when user authentication has been enabled.	User Code authentication may not be specified in the printer driver. Print jobs might not be sent successfully if Basic, Windows, LDAP or Integration Server authentication has been enabled.	Specify User Code authentication in the printer driver. For details, see the printer driver Help. Set the Printer Job Authentication level to [Simple (All)] or [Simple (Limitation)]. For details about the Printer Job Authentication level, see "Printer Job Authentication".
If you try to interrupt a job while copying or scanning, an authentication screen appears.	With this machine, you can log out while copying or scanning. If you try to interrupt copying or scanning after logging out, an authentication screen appears.	Only the user who executed a copying or scanning job can interrupt it. Wait until the job has completed or consult an administrator or the user who executed the job.
After you execute "Encrypt Address Book", the "Exit" message does not appear.	The hard disk may be faulty. The file may be corrupt.	Contact your service representative.

Reference

- p.183 "Specifying a Driver Encryption Key"
- p.191 "Setting the SSL/TLS Encryption Mode"

- p.95 "Configuring Access Permissions for Stored Files"
- p.117 "Protecting the Address Book"
- p.79 "Printer Job Authentication"

10. 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 "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.

Reference

- p.221 "Specifying the Extended Security Functions"

Logging in as the Supervisor

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

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

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

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

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

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

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

Logging out as the Supervisor

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

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

Changing the Supervisor

This section describes how to change the supervisor's login name and password.

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

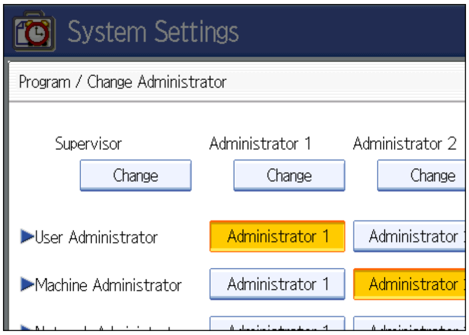
1. **Press the [User Tools/Counter] key.**
2. **Press the [Login/Logout] key.**
3. **Log in as the supervisor.**

   You can log in the same way as an administrator.

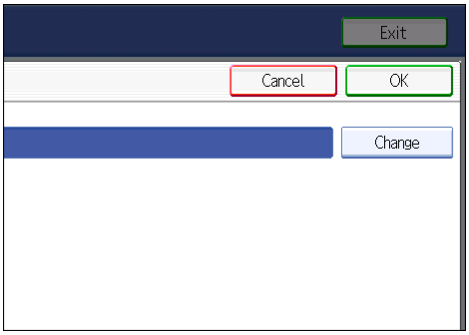
4. **Press [System Settings].**
5. **Press [Administrator Tools].**
6. **Press [Program / Change Administrator].**

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

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



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



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

    You will be automatically logged out.

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

Reference

- p.27 "Specifying Administrator Privileges"
- p.261 "Supervisor Operations"

Resetting the Administrator's Password

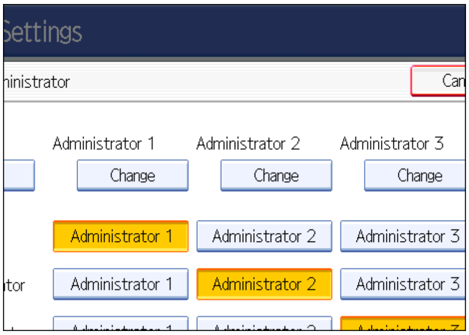
This section describes how to reset the administrators' passwords. Administrator login names cannot be changed.

For details about logging in and logging out as the supervisor, see "Supervisor Operations".

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

   You can log in the same way as an administrator.
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 the login password.**
9. **Enter the login password, and then press [OK].**
10. **If a password reentry screen appears, enter the login password, and then press [OK].**
11. **Press [OK] twice.**

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

Reference

- p.261 "Supervisor Operations"

User Administrator Settings

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

System Settings

The following settings can be specified.

Administrator Tools

- Address Book Management
- Address Book: Program / Change / Delete Group
- Address Book: Change Order
- Print Address Book: Destination List
- Address Book: Edit Title
- Address Book: Switch Title
- Back Up / Restore Address Book
- Data Carry-over Setting for Address Book Auto-program
- Display / Clear / Print Counter per User

  All Users: Clear

  Per User: Clear
- 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

  Encryption Key

  Encrypt / Decrypt

  Restrict Use of Destinations

  Restrict Adding of User Destinations

  Password Policy

Extended Feature Settings

The following settings can be specified.

GL/2 & TIFF

All the settings can be specified.

Settings via Web Image Monitor

The following settings can be specified.

Address Book

All the settings can be specified.

Device Settings

- Administrator Authentication Management

  User Administrator Authentication

  Available Settings for User Administrator

  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

The following settings can be specified.

General Features

All the settings can be specified.

Tray Paper Settings

All the settings can be specified.

Timer Settings

All the settings can be specified.

Interface Settings

The following settings can be specified.

- Network

  DNS Configuration

  You can perform a connection test.

File Transfer

The following settings can be specified.

- Delivery Option
- Capture Server IPv4 Address
- SMTP Authentication
- POP before SMTP
- Reception Protocol
- POP3 / IMAP4 Settings
- Administrator's E-mail Address
- Default User Name / Password (Send)
- Program / Change / Delete E-mail Message

Administrator Tools

The following settings can be specified.

- Address Book Management

  Search

  Switch Title

- Address Book: Program / Change / Delete Group

  Search

  Switch Title
- Display / Print Counter

  Print Counter List
- Display / Clear / Print Counter per User

  All Users: Print Counter List

  Per User: Print Counter List
- User Authentication Management

  You can specify which authentication to use.

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

  Machine Management
- Program / Change Administrator

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

  Restrict Display of User Information

  Authenticate Current Job

  @Remote Service

  Update Firmware

  Change Firmware Structure
- Capture Priority
- Capture: Delete All Unsent Files
- Capture: Ownership
- Capture: Public Priority
- Capture: Owner Defaults
- Program / Change / Delete LDAP Server
- LDAP Search
- Service Mode Lock

- Auto Erase Memory Setting
- Erase All Memory
- Delete All Logs
- Transfer Log Setting

  This setting can be changed only when it is set to [On].
- Fixed USB Port
- Program / Change / Delete Realm
- Machine Data Encryption Settings

Copier / Document Server Features

The following settings can be specified.

General Features

All the settings can be specified.

Reproduction Ratio

All the settings can be specified.

Edit

All the settings can be specified.

Stamp

All the settings can be specified.

Input / Output

All the settings can be specified.

Administrator Tools

All the settings can be specified.

Printer Features

The following settings can be specified.

List / Test Print

All the settings can be specified.

Maintenance

The following settings can be specified.

- Menu Protect
- List / Test Print Lock

System

The following settings can be specified.

- Print Error Report
- Auto Continue
- Memory Overflow
- Rotate by 180 Degrees
- Initial Print Job List
- Memory Usage
- Copies
- Blank Page Print
- Reserved Job Waiting Time
- Printer Language
- Sub Paper Size
- Tray Setting Priority
- Edge to Edge Print
- Default Printer Language
- Tray Switching
- Extended Auto Tray Switching

Host Interface

All the settings can be specified.

PS Menu

All the settings can be specified.

PDF Menu

All the settings can be specified.

Scanner Features

The following settings can be specified.

General Settings

All the settings can be specified.

Scan Settings

All the settings can be specified.

Send Settings

The following settings can be specified.

- Compression (Black & White)
- Compression (Grey Scale / Full Colour)
- Insert Additional E-mail Info
- No. of Digits for Single Page Files
- Stored File E-mail Method
- Default E-mail Subject

Initial Settings

All the settings can be specified.

Extended Feature Settings

The following settings can be specified.

Extended Feature Settings

All the settings can be specified.

GL/2 & TIFF

All the settings can be specified.

Settings via Web Image Monitor

The following settings can be specified.

Top Page

- Reset Device
- Reset Printer Job

Device Settings

- System

  Spool Printing

  Protect Printer Display Panel

  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.

- Date/Time

  All the settings can be specified.

- Timer

  All the settings can be specified.

- Logs

  All the settings can be specified.

  The "Transfer Logs" setting can be changed only when it is set to [Active].

- Download Logs
- E-mail

  All the settings can be specified.

- Auto E-mail Notification

  All the settings can be specified.

- On-demand E-mail Notification

  All the settings can be specified.

- File Transfer

  All the settings can be specified.

- User Authentication Management

  All the settings can be specified.

- Administrator Authentication Management

  Machine Administrator Authentication

  Available Settings for Machine Administrator

- Program/Change Administrator

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

  Login User Name

  Login Password

  Encryption Password

- LDAP Server

  All the settings can be specified.

- Firmware Update

  All the settings can be specified.

- Program/Change Realm

All the settings can be specified.

Printer

- System

  All the settings can be specified except the following.

  Auto Delete Temporary Print Jobs

  Auto Delete Stored Print Jobs

- Host Interface

  All the settings can be specified.

- PS Menu

  All the settings can be specified.

- PDF Menu

  All the settings can be specified.

- Tray Parameters (PS)

  All the settings can be specified.

- PDF Fixed Password

  All the settings can be specified.

Scanner

- General Settings

  All the settings can be specified.

- Scan Settings

  All the settings can be specified.

- Send Settings

  All the settings can be specified except the following.

  Max. E-mail Size

  Divide & Send E-mail

- Initial Settings

  All the settings can be specified.

- Default Settings for Normal Screens on Device

  All the settings can be specified.

- Default Settings for Simplified Screens on Device

  All the settings can be specified.

Interface Settings

- USB

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

Extended Feature Settings

- All the settings can be specified.

Network Administrator Settings

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

System Settings

The following settings can be specified.

Interface Settings

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

- Print List
- Network

  All the settings can be specified.
- Wireless LAN

  All the settings can be specified.

File Transfer

- SMTP Server
- E-mail Communication Port

  All the settings can be specified.
- E-mail Reception Interval
- Max. Reception E-mail Size
- E-mail Storage in Server
- Auto Specify Sender Name
- Scanner Resend Interval Time
- Number of Scanner Resends

Administrator Tools

- Address Book Management

  Search

  Switch Title
- Address Book: Program / Change / Delete Group

  Search

  Switch Title
- Administrator Authentication Management

  Network Management
- Program / Change Administrator

Network Administrator

- Extended Security

  Driver Encryption Key

  Settings by SNMPv1, v2

  Restrict Use of Simple Encryption

- Network Security Level

Scanner Features

The following settings can be specified.

Send Settings

- Max. E-mail Size
- Divide & Send E-mail

Extended Feature Settings

The following settings can be specified.

GL/2 & TIFF

All the settings can be specified.

Settings via Web Image Monitor

The following settings can be specified.

Device Settings

- System

  Device Name

  Comment

  Location

- E-mail

  All the settings can be specified.

- Administrator Authentication Management

  Network Administrator Authentication

  Available Settings for Network Administrator

- Program/Change Administrator

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

Login User Name

Login Password

Encryption Password

Scanner

- Send Settings

  Max. E-mail Size

  Divide & Send E-mail

Interface

- Interface Settings

  LAN Type

  Ethernet Security

  Ethernet Speed

- Wireless LAN Settings

  LAN Type

  Communication Mode

  SSID

  Channel

  Security Method

  WEP Authentication

  WEP Key Number

  WEP Key

  WPA Encryption Method

  WPA Authentication Method

  WPA-PSK/WPA2-PSK

Network

- IPv4

  All the settings can be specified.

- IPv6

  All the settings can be specified.

- NetWare

  All the settings can be specified.

- SMB

All the settings can be specified.

- SNMP

  All the settings can be specified.

- SNMPv3

  All the settings can be specified.

- SSDP

  All the settings can be specified.

- Bonjour

  All the settings can be specified.

Security

- Network Security

  All the settings can be specified.

- Access Control

  All the settings can be specified.

- IPP Authentication

  All the settings can be specified.

- SSL/TLS

  All the settings can be specified.

- 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.

- S/MIME

  All the settings can be specified.

Webpage

All the settings can be specified.

File Administrator Settings

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

System Settings

The following settings can be specified.

Interface Settings

- DNS Configuration

  Connection Test

Administrator Tools

- Address Book Management

  Search

  Switch Title
- Address Book: Program / Change / Delete Group

  Search

  Switch Title
- Administrator Authentication Management

  File Management
- Program / Change Administrator

  File Administrator
- Extended Security

  Enhance File Protection
- Auto Delete File in Document Server
- Delete All Files in Document Server

Printer Features

The following settings can be specified.

Maintenance

- Delete All Temporary Print Jobs
- Delete All Stored Print Jobs

System

- Auto Delete Temporary Print Jobs

- Auto Delete Stored Print Jobs

Extended Feature Settings

The following settings can be specified.

GL/2 & TIFF

All the settings can be specified.

Settings via Web Image Monitor

The following settings can be specified.

Document Server

All the settings can be specified.

Printer: Print Jobs

The file administrator can edit/delete "Print Job List" and unlock the print job.

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

Printer

- System

  Auto Delete Temporary Print Jobs

  Auto Delete Stored Print Jobs

Webpage

- Webpage

  Download Help File

Document Server File Permissions

The authorities for using the files stored in Document Server are as follows.

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

- Read-only

  This is a user assigned "Read-only" authority.

- Edit

  This is a user assigned "Edit" authority.

- Edit / Delete

  This is a user assigned "Edit / Delete" authority.

- Full Control

  This is a user granted full control.

- Owner

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

- File Administrator

  This is the file administrator.

A = Granted authority to operate.

- = Not granted authority to operate.

Settings	Read-only	Edit	Edit / Delete	Full Control	Owner	File Admin.
Viewing Details About Stored Files	A	A	A	A	A*1	A
Viewing Preview	A	A	A	A	A*1	-
Print/Transmission	A	A	A	A	A*1	-
Changing File Name	-	A	A	A	A *1	-
Deleting Files	-	-	A	A	A *1	A
Specifying File Password	-	-	-	-	A	A
Specifying Permissions for Users/Groups	-	-	-	A	A	A

Settings	Read-only	Edit	Edit / Delete	Full Control	Owner	File Admin.
Unlocking Files	-	-	-	-	-	A
Changing Owner	-	-	-	-	-	A

*1 The owner can change the authorities for these settings as necessary.

The Privilege for User Account Settings in the Address Book

The authorities for using the Address Book are as follows:

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

- Abbreviations in the table heads

  Read-only (User) = This is a user assigned "Read-only" authority.

  Edit (User) = This is a user assigned "Edit" authority.

  Edit / Delete (User) = This is a user assigned "Edit / Delete" authority.

  User Admin. = This is the user administrator.

  Registered User = This is a user that has personal information registered in the Address Book and has a login password and user name.

  Full Control = This is a user granted full control.

- Abbreviations in the table columns

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

  R (Read) = Reading only.

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

Tab Name: Names

Settings	Read-only (User)	Edit (User)	Edit / Delete (User)	Full Control	Registered User	User Admin.
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	Registered User	User Admin.
User Code	N/A	N/A	N/A	N/A	N/A	R/W

Settings	Read-only (User)	Edit (User)	Edit / Delete (User)	Full Control	Registered User	User Admin.
Login User Name	N/A	N/A	N/A	N/A	R	R/W
Login Password	N/A	N/A	N/A	N/A	R/W*1	R/W*1
SMTP Authentication	N/A	N/A	N/A	N/A	R/W*1	R/W*1
Folder Authentication	R	R/W*1	R/W*1	R/W*1	R/W*1	R/W*1
LDAP Authentication	N/A	N/A	N/A	N/A	R/W*1	R/W*1
Available Functions	N/A	N/A	N/A	N/A	R	R/W

*1 The password for "Login Password", "SMTP Authentication", or "LDAP Authentication" can be entered or changed but not displayed.

Tab Name: Protection

Settings	Read-only (User)	Edit (User)	Edit / Delete (User)	Full Control	Registered User	User Admin.
Use Name as	R	R/W	R/W	R/W	R/W	R/W
Protection Code	N/A	N/A	N/A	R/W*2	R/W*2	R/W*2
Protection Object	N/A	R/W	R/W	R/W	R/W	R/W
Protect Destination: Permissions for Users / Groups	N/A	N/A	N/A	R/W	R/W	R/W
Protect File(s): Permissions for Users / Groups	N/A	N/A	N/A	R/W	R/W	R/W

*2 The code for "Protection Code" can be entered or changed but not displayed.

Tab Name: E-mail

Settings	Read-only (User)	Edit (User)	Edit / Delete (User)	Full Control	Registered User	User Admin.
E-mail Address	R	R/W	R/W	R/W	R/W	R/W

Tab Name: Folder

Settings	Read-only (User)	Edit (User)	Edit / Delete (User)	Full Control	Registered User	User Admin.
SMB/FTP/NCP	R	R/W	R/W	R/W	R/W	R/W
SMB: Path	R	R/W	R/W	R/W	R/W	R/W
FTP: Server Name	R	R/W	R/W	R/W	R/W	R/W
FTP: Path	R	R/W	R/W	R/W	R/W	R/W
FTP: Port Number	R	R/W	R/W	R/W	R/W	R/W
NCP: Path	R	R/W	R/W	R/W	R/W	R/W
NCP: Connection Type	R	R/W	R/W	R/W	R/W	R/W

Tab Name: Add to Group

Settings	Read-only (User)	Edit (User)	Edit / Delete (User)	Full Control	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 explains which functions and system settings are available to users when administrator authentication is specified. The administrator's configuration of Menu Protect and Available Settings determines which functions and system settings are available to users. If user authentication is specified, system settings and functions are available to authorized users only, who must log in to access them.

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
Copy Count Display	R/W	R
Function Priority	R/W	R
Print Priority	R/W	R
Function Reset Timer	R/W	R
Output: Printer	R/W	R
Key Repeat	R/W	R
System Status / Job List Display Time	R/W	R
Interleave Print	R/W	R

Settings	Not Specified	Specified
Feed Start Method	R/W	R
Original Feed Delay 2	R/W	R
Original Feed Delay 1	R/W	R
Fine Ratio Adjustment: Copier	R/W	R
Fine Ratio Adjustment: Printer	R/W	R
Adjust Scan Position	R/W	R
Preview Area Settings	R/W	R
Print Image Priority	R/W	R

Tray Paper Settings

Settings	Not Specified	Specified
Paper Tray Priority: Copier	R/W	R
Paper Tray Priority: Printer	R/W	R
Tray Paper Size: Tray 1-3	R/W	R
Printer Bypass Paper Size	R/W	R
Paper Type: Bypass Tray	R/W	R
Paper Type: Tray 1-3	R/W	R
Paper Thickness: Paper Tray	R/W	R
Paper Thickness: Paper Bypass	R/W	R
Paper Volume	R/W	R

Timer Settings

Settings	Not Specified	Specified
Auto Off Timer	R/W	R

Settings	Not Specified	Specified
Energy Saver Timer	R/W	R
Panel Off Timer	R/W	R
System Auto Reset Timer	R/W	R
Copier / Document Server Auto Reset Timer	R/W	R
Printer Auto Reset Timer	R/W	R
Scanner Auto Reset Timer	R/W	R
Set Date	R/W	R
Set Time	R/W	R
Auto Logout Timer	R/W	R

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
Machine IPv6 Address	R/W	R
IPv6 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

Settings	Not Specified	Specified
Domain Name	R/W	R
WINS Configuration	R/W	R
Effective Protocol	R/W	R
NCP Delivery Protocol	R/W	R
NW Frame Type	R/W	R
SMB Computer Name	R/W	R
SMB Work Group	R/W	R
Ethernet Speed	R/W	R
LAN Type	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", "Machine IPv6 Address", "DNS Configuration", "Domain Name", or "WINS Configuration" to "Auto-Obtain (DHCP)", you can only display the settings.

Wireless LAN

Settings	Not Specified	Specified
Communication Mode	R/W	R
SSID Setting	R/W	R
Ad-hoc Channel	R/W	R
Security Method	R/W	R

Settings	Not Specified	Specified
Restore Factory Defaults	R/W	N/A

File Transfer

Settings	Not Specified	Specified
Delivery Option	R/W	R
Capture Server IPv4 Address	R/W	R
SMTP Server	R/W	R
SMTP Authentication	R/W	R
POP before SMTP	R/W	R
Reception Protocol	R/W	R
POP3 / IMAP4 Settings	R/W	R
Administrator's E-mail Address	R/W	R
E-mail Communication Port	R/W	R
E-mail Reception Interval	R/W	R
Max. Reception E-mail Size	R/W	R
E-mail Storage in Server	R/W	R
Default User Name / Password (Send)	R/W	R
Program / Change / Delete E-mail Message	R/W	R/W
Auto Specify Sender Name	R/W	R
Scanner Resend Interval Time	R/W	R
Number of Scanner Resends	R/W	R

The settings made for "Primary Delivery Server IPv4 Address" and "Secondary Delivery Server IPv4 Address" in "Delivery Option" can only be displayed, not changed.

The passwords for "SMTP Authentication" and "Default User Name / Password (Send)" can be entered or changed but not displayed.

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
Print Address Book: Destination List	R/W	R/W
Address Book: Edit Title	R/W	N/A
Address Book: Switch Title	R/W	R
Back Up / Restore Address Book	R/W	N/A
Data Carry-over Setting for Address Book Auto-program	R/W	R
Display / Print Counter	R/W	R/W
Display / Clear / Print Counter per User	R/W	N/A
User Authentication Management	R/W	R
Enhanced Authentication Management	R/W	R
Administrator Authentication Management	R/W	N/A
Key Counter Management	R/W	R
External Charge Unit Management	R/W	R
Enhanced External Charge Unit Management	R/W	R
Extended Security	R/W	R
Auto Delete File in Document Server	R/W	R
Delete All Files in Document Server	R/W	N/A
Capture Priority	R/W	R
Capture: Delete All Unsent Files	R/W	N/A
Capture: Ownership	R/W	R
Capture: Public Priority	R/W	R

Settings	Not Specified	Specified
Capture: Owner Defaults	R/W	R
Program / Change / Delete LDAP Server	R/W	R
LDAP Search	R/W	R
Service Mode Lock	R/W	R
Auto Erase Memory Setting	R/W	R
Erase All Memory	R/W	R
Delete All Logs	R/W	N/A
Transfer Log Setting	R/W	N/A
Fixed USB Port	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.

"Transfer Log Setting" can be changed only when it is set to [On].

Copier / Document Server Features

When administrator authentication is enabled, the administrator's configuration of Menu Protect determines which functions and settings are available to users.

User privileges are as follows:

- Abbreviations in the table columns

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

  R (Read) = Reading only.

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

When "Menu Protect" is set to [Off], all the following settings can be viewed and modified.

Note

- The default for "Menu Protect" is [Level 2].
- Settings that are not in the list can only be viewed, regardless of the menu protect level setting.

General Features

Settings	Level 1	Level 2
Auto Image Density Priority	R	R
Original Photo Type Priority	R	R
Max. Copy Quantity	R	R
Auto Tray Switching	R	R
Job End Call	R	R

Reproduction Ratio

Settings	Level 1	Level 2
User Reduce/Enlarge Ratio	R	R
Reproduction Ratio	R	R
Reduce/Enlarge Ratio Priority	R	R
User Auto Reduce/Enlarge: A0-B4 JIS	R	R

Edit

Settings	Level 1	Level 2
Adjust Position	R	R
Erase Border Width	R	R
Erase Original Shadow in Combine	R/W	R
Image Repeat Separation Line	R/W	R
Double Copies Separation Line	R/W	R
Separation Line in Combine	R/W	R
Copy Order in Combine	R/W	R
Program / Delete Format	R/W	R
Margin Adjustment Priority	R	R
Partial Copy Size	R	R

Stamp

Background Numbering

Settings	Level 1	Level 2
Size	R/W	R
Density	R/W	R

Preset Stamp

Settings	Level 1	Level 2
Stamp Language	R/W	R
Stamp Priority	R	R
Stamp Format: COPY	R/W	R
Stamp Format: URGENT	R/W	R
Stamp Format: PRIORITY	R/W	R
Stamp Format: For Your Info.	R/W	R

Settings	Level 1	Level 2
Stamp Format: PRELIMINARY	R/W	R
Stamp Format: For Internal Use Only	R/W	R
Stamp Format: CONFIDENTIAL	R/W	R
Stamp Format: DRAFT	R/W	R

If you select [Level 1] in "Stamp Format", you can only specify "Adjust Stamp Position".

User Stamp

Settings	Level 1	Level 2
Program / Delete Stamp	R/W	R
Stamp Format: 1-40	R/W	R

Date Stamp

Settings	Level 1	Level 2
Format	R	R
Font	R/W	R
Size	R/W	R
Superimpose	R/W	R
Stamp Setting	R/W	R

If you select [Level 1] in "Stamp Setting", you can only specify "Adjust Stamp Position".

Page Numbering

Settings	Level 1	Level 2
Stamp Format	R	R
Font	R/W	R
Size	R/W	R
Page Numbering in Combine	R/W	R
Stamp Position:P1,P2...	R/W	R

Settings	Level 1	Level 2
Stamp Position:1/5,2/5...	R/W	R
Stamp Position:-1-,-2-...	R/W	R
Stamp Position:P.1,P.2...	R/W	R
Stamp Position:1,2...	R/W	R
Stamp Position:1-1,1-2...	R/W	R
Superimpose	R/W	R
Page Numbering Initial Letter	R/W	R

If you select [Level 1] in "Stamp Position", you can only specify "Adjust Stamp Position".

Input / Output

Settings	Level 1	Level 2
Rotate Sort: Auto Paper Continue	R	R

Printer Functions

When administrator authentication is enabled, the administrator's configuration of Menu Protect determines which functions and settings are available to users.

User privileges are as follows:

- Abbreviations in the table columns

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

  R (Read) = Reading only.

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

When "Menu Protect" is set to [Off], all the following settings can be viewed and modified.

Note

- The default for "Menu Protect" is [Level 2].
- Settings that are not in the list can only be viewed, regardless of the menu protect level setting.

Normal Printer Screen

Functions	Level 1	Level 2
Print Jobs	R/W	R/W
Spooling Job List	R/W	R/W

Printer Features

When administrator authentication is enabled, the administrator's configuration of Menu Protect determines which functions and settings are available to users.

User privileges are as follows:

- Abbreviations in the table columns

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

  R (Read) = Reading only.

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

When "Menu Protect" is set to [Off], all the following settings can be viewed and modified.

Note

- The default for "Menu Protect" is [Level 2].
- Settings that are not in the list can only be viewed, regardless of the menu protect level setting.

List / Test Print

Settings	Level 1	Level 2
Multiple Lists	R/W	R/W
Configuration Page	R/W	R/W
Error Log	R/W	R/W
Menu List	R/W	R/W
PS Configuration / Font Page	R/W	R/W
PDF Configuration / Font Page	R/W	R/W
Hex Dump	R/W	R/W

System

Settings	Level 1	Level 2
Print Error Report	R	R
Auto Continue	R	R
Memory Overflow	R	R
Rotate by 180 Degrees	R	R

Settings	Level 1	Level 2
Auto Delete Temporary Print Jobs	R	R
Auto Delete Stored Print Jobs	R	R
Initial Print Job List	R	R
Memory Usage	R	R
Copies	R	R
Blank Page Print	R	R
Reserved Job Waiting Time	R	R
Printer Language	R	R
Sub Paper Size	R	R
Tray Setting Priority	R	R
Edge to Edge Print	R	R
Default Printer Language	R	R
Tray Switching	R	R
Extended Auto Tray Switching	R	R

Host Interface

Settings	Level 1	Level 2
I/O Buffer	R	R
I/O Timeout	R	R

PS Menu

Settings	Level 1	Level 2
Job Timeout	R	R
Wait Timeout	R	R
Data Format	R	R
Resolution	R	R

Settings	Level 1	Level 2
Orientation Auto Detect	R	R

PDF Menu

Settings	Level 1	Level 2
Change PDF Password	R	R
Reverse Order Printing	R	R
Resolution	R	R
Orientation Auto Detect	R	R

Scanner Features

When administrator authentication is enabled, the administrator's configuration of Menu Protect determines which functions and settings are available to users.

User privileges are as follows:

- Abbreviations in the table columns

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

  R (Read) = Reading only.

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

When "Menu Protect" is set to [Off], all the following settings can be viewed and modified.

Note

- The default for "Menu Protect" is [Level 2].
- Settings that are not in the list can only be viewed, regardless of the menu protect level setting.

General Settings

Settings	Level 1	Level 2
Switch Title	R	R
Update Delivery Server Destination List	R/W	R
Search Destination	R	R
PC Scan Command Standby Time	R	R
Destination List Display Priority 1	R	R
Destination List Display Priority 2	R	R
Print & Delete Scanner Journal	R	R
Print Scanner Journal	N/A	N/A
Delete Scanner Journal	N/A	N/A
Delete Recent Destinations	N/A	N/A

Scan Settings

Settings	Level 1	Level 2
Next Original Wait Setting	R	R

10

Send Settings

Settings	Level 1	Level 2
Compression (Black & White)	R/W	R
Compression (Grey Scale / Full Colour)	R/W	R
Insert Additional E-mail Info	R/W	R
No. of Digits for Single Page Files	R/W	R
Stored File E-mail Method	R/W	R
Default E-mail Subject	R	R

User Settings - Web Image Monitor Settings

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

Device Settings

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

Top Page

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
General Settings : Spool Printing	R/W	R
Output Tray : Printer	R/W	R
Paper Tray Priority : Copier	R/W	R
Paper Tray Priority : Printer	R/W	R

Paper

Settings	Not Specified	Specified
Tray 1 : Paper Size	R/W	R
Tray 1 : Paper Type	R/W	R
Tray 1: Apply Auto Paper Select	R/W	R
Tray 2: Paper Size	R/W	R
Tray 2: Paper Type	R/W	R
Tray 2: Apply Auto Paper Select	R/W	R
Tray 3: Paper Size	R/W	R
Tray 3: Paper Type	R/W	R
Tray 3: Apply Auto Paper Select	R/W	R
Bypass Tray : Paper Size	R/W	R
Bypass Tray : Custom Paper Size	R/W	R
Bypass Tray : Paper Type	R/W	R

Date/Time

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

Timer

Settings	Not Specified	Specified
Auto Off Timer	R/W	R
Energy Saver Timer	R/W	R
Panel Off Timer	R/W	R
System Auto Reset Timer	R/W	R
Copier/Document Server Auto Reset Timer	R/W	R
Scanner Auto Reset Timer	R/W	R
Printer Auto Reset Timer	R/W	R
Auto Logout 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
Transfer Logs	R/W	R
Encrypt Logs	R/W	R
Classification Code	R/W	R
Delete All Logs	R/W	N/A

"Transfer Logs" can be changed only when it is set to [Active].

E-mail

Settings	Not Specified	Specified
Administrator E-mail Address	R/W	R
Reception Protocol	R/W	R
E-mail Reception Interval	R/W	R
Max. Reception E-mail Size	R/W	R
E-mail Storage in Server	R/W	R
SMTP Server Name	R/W	R
SMTP Port No.	R/W	R
SMTP Authentication	R/W	R
SMTP Auth. E-mail Address	R/W	R
SMTP Auth. User Name	R/W	N/A
SMTP Auth. Password	R/W	N/A
SMTP Auth. Encryption	R/W	R
POP before SMTP	R/W	R
POP E-mail Address	R/W	R
POP User Name	R/W	N/A
POP Password	R/W	N/A
Timeout setting after POP Auth.	R/W	R
POP3/IMAP4 Server Name	R/W	R
POP3/IMAP4 Encryption	R/W	R
POP3 Reception Port No.	R/W	R
IMAP4 Reception Port No.	R/W	R
E-mail Notification E-mail Address	R/W	R
Receive E-mail Notification	R/W	N/A

Settings	Not Specified	Specified
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.

File Transfer

Settings	Not Specified	Specified
SMB User Name	R/W	N/A
SMB Password	R/W	N/A
FTP User Name	R/W	N/A
FTP Password	R/W	N/A
NCP User Name	R/W	N/A
NCP Password	R/W	N/A

The passwords for "SMB Password", "FTP Password", and "NCP Password" can be entered or changed but not displayed.

User Authentication Management

Settings	Not Specified	Specified
User Authentication Management	R/W	R
User Code Authentication - Printer Job Authentication Settings	R/W	R
User Code Authentication - User Code Authentication Settings	R/W	R
Basic Authentication - Printer Job Authentication Settings	R/W	R
Basic Authentication - Basic Authentication Settings	R/W	R
Windows Authentication - Printer Job Authentication Settings	R/W	R
Windows Authentication - Windows Authentication Settings	R/W	R

Settings	Not Specified	Specified
Windows Authentication - Group Settings for Windows Authentication	R/W	R
LDAP Authentication - Printer Job Authentication Settings	R/W	R
LDAP Authentication - LDAP Authentication Settings	R/W	R
Integration Server Authentication - Printer Job 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
LDAP Search	R/W	N/A
Program/Change/Delete	R/W	N/A

Printer

If you have enabled administrator authentication, the menu protection setting determines which functions and settings are available.

User privileges are as follows:

- Abbreviations in the table columns

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

  R (Read) = Reading only.

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

When "Menu Protect" is set to [Off], all the following settings can be viewed and modified.

Note

- The default for "Menu Protect" is [Level 2].
- Settings that are not in the list can only be viewed, regardless of the menu protect level setting.

Printer Basic Settings

System

Settings	Level 1	Level 2
Print Error Report	R	R
Auto Continue	R	R
Memory Overflow	R	R
Auto Delete Temporary Print Jobs	R	R
Auto Delete Stored Print Jobs	R	R
Initial Print Job List	R	R
Rotate by 180 Degrees	R	R
Memory Usage	R	R
Copies	R	R
Blank Page Print	R	R
Reserved Job Waiting Time	R	R
Printer Language	R	R
Sub Paper Size	R	R

Settings	Level 1	Level 2
Tray Setting Priority	R	R
Edge to Edge Print	R	R
Default Printer Language	R	R
Tray Switching	R	R
Extended Auto Tray Switching	R	R

Host Interface

Settings	Level 1	Level 2
I/O Buffer	R	R
I/O Timeout	R	R

PS Menu

Settings	Level 1	Level 2
Job Timeout	R	R
Wait Timeout	R	R
Data Format	R	R
Resolution	R	R
Orientation Auto Detect	R	R

PDF Menu

Settings	Level 1	Level 2
Reverse Order Printing	R	R
Resolution	R	R
Orientation Auto Detect	R	R

PDF Temporary Password

Settings	Level 1	Level 2
PDF Temporary Password	R/W	R/W
Confirm Password	R/W	R/W

PDF Fixed Password

Settings	Level 1	Level 2
Current PDF Fixed Password	N/A	N/A
New PDF Fixed Password	N/A	N/A
Confirm Password	N/A	N/A

Scanner

If you have enabled administrator authentication, the menu protection setting determines which functions and settings are available.

User privileges are as follows:

- Abbreviations in the table columns

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

  R (Read) = Reading only.

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

When "Menu Protect" is set to [Off], all the following settings can be viewed and modified.

Note

- The default for "Menu Protect" is [Level 2].
- Settings that are not in the list can only be viewed, regardless of the menu protect level setting.

General Settings

Settings	Level 1	Level 2
Switch Title	R	R
Search Destination	R	R
PC Scan Command Standby Time	R	R
Destination List Display Priority 1	R	R
Destination List Display Priority 2	R	R
Print & Delete Scanner Journal	R	R

Scan Settings

Settings	Level 1	Level 2
Wait Time for Next Original(s)	R	R

Send Settings

Settings	Level 1	Level 2
Compression (Black & White)	R/W	R
Compression (Gray Scale/Full Color)	R/W	R

Settings	Level 1	Level 2
Insert Additional E-mail Info	R/W	R
No. of Digits for Single Page Files	R/W	R
Stored File E-mail Method	R/W	R
Default E-mail Subject	R	R

Default Settings for Normal Screens on Device

Settings	Level 1	Level 2
Store File	R	R
Preview	R	R
Original Type	R	R
Resolution	R	R
Auto Density	R	R
Send File Type	R	R

Default Settings for Simplified Screens on Device

Settings	Level 1	Level 2
Original Type	R	R
Resolution	R	R
Send File Type	R	R

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

Settings	Not Specified	Specified
Network : LAN Type	R	N/A
Ethernet : Ethernet Security	R/W	R
Ethernet : Ethernet Speed	R/W	R
USB	R/W	R

Wireless LAN Settings

Settings	Not Specified	Specified
LAN Type	R/W	N/A
Communication Mode	R/W	R
SSID	R/W	R
Channel	R/W	N/A

Settings	Not Specified	Specified
Security Method	R/W	R
WEP Authentication	R/W	N/A
WEP Key Number	R/W	R
WEP Key	R/W	R
WPA Encryption Method	R/W	R
WPA Authentication Method	R/W	R
WPA-PSK/WPA2-PSK	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
LPR	R/W	R
RSH/RCP	R/W	R
DIPRINT	R/W	R
FTP	R/W	R
sftp	R/W	R
WSD (Device)	R/W	R
WSD (Printer)	R/W	R
IPP	R/W	R
WSD (Printer)/IPP Timeout	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
LPR	R/W	R
RSH/RCP	R/W	R

Settings	Not Specified	Specified
DIPRINT	R/W	R
FTP	R/W	R
sftp	R/W	R
WSD (Device)	R/W	R
WSD (Printer)	R/W	R
IPP	R/W	R
WSD (Printer)/IPP Timeout	R/W	R

NetWare

Settings	Not Specified	Specified
NetWare	R/W	R
Print Server Name	R/W	R
Logon Mode	R/W	R
File Server Name	R/W	R
NDS Tree	R/W	N/A
NDS Context Name	R/W	R
Operation Mode	R/W	R
Remote Printer No.	R/W	N/A
Job Timeout	R/W	N/A
Frame Type	R/W	R
Print Server Protocol	R/W	R
NCP Delivery Protocol	R/W	R

SMB

Settings	Not Specified	Specified
SMB	R/W	R
Workgroup Name	R/W	R
Computer Name	R/W	R
Comment	R/W	R
Notify Print Completion	R/W	R

Bonjour

Settings	Not Specified	Specified
Bonjour	R/W	R
Computer Name	R/W	R
Location	R/W	R
DIPRINT	R/W	R
LPR	R/W	R
IPP	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
Language1	R/W	R
Language2	R/W	R
URL1	R/W	R
URL2	R/W	R
Set Help URL Target	R/W	R
WSD/UPnP Setting	R/W	R
Download Help File	R/W	R/W

Trademarks

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

Apple, Bonjour, Macintosh, 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.

NetWare is a registered trademark of Novell, Inc.

PowerPC® is a trademark of International Business Machines Corporation in the United States, other countries, or both.

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 2008 R2 are as follows:

  Microsoft® Windows Server® 2008 R2 Standard

  Microsoft® Windows Server® 2008 R2 Enterprise

INDEX

MEMO

MEMO

Operating Instructions Security Reference