Operating Instructions

Security Guide

For safe and correct use, be sure to read the Safety Information in Read This First before using the machine.

TABLE OF CONTENTS

3. Restricting Machine Usage

4. Preventing Leakage of Information from Machines

5. Enhanced Network Security

6. Preventing the Leaking of Documents

7. Managing the Machine

8. Troubleshooting

9. List of Operation Privileges for Settings

Functions That Require Options

The following functions require certain options and additional functions.

- Detect Data Security for Copying

  Copy Data Security Unit

Region A (mainly Europe)

You can use Copy Data Security Unit on Type 1, 2, or 3 machines only.

Region B (mainly North America)

You can use Copy Data Security Unit on Type 1*, 2, or 3 machines only.

* The printer and scanner functions are not available on Pro 8200EX.

For details about other functions that require options, see "Functions Requiring Optional Configurations", Getting Started.

1. Getting Started

This chapter describes the precautions to take when using the machine's security features and how to configure the administrator settings.

Before Configuring the Security Function Settings

Important

- **If the security settings are not configured, the data in the machine is vulnerable to attack.**
- To prevent this machine being stolen or willfully damaged, etc., install it in a secure location.
- 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.
- Before setting this machine's security features and to ensure appropriate operation by users, administrators must read the Security Guide completely and thoroughly, paying particular attention to the section entitled "Before Configuring the Security Function Settings".
- Administrators must inform users regarding proper usage of the security functions.
- If this machine is connected to a network, its environment must be protected by a firewall or similar.
- 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.
- Administrators should routinely examine the machine's logs to check for irregular and unusual events.

Before Using This Machine

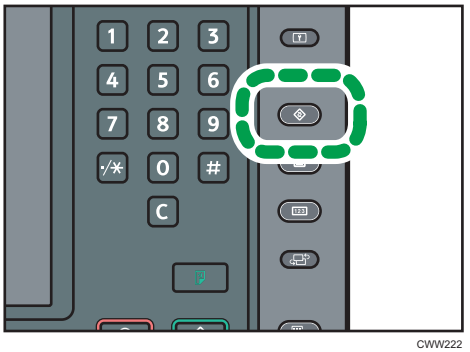
1

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.

1. **Turn the machine on.**

   For details about turning on the main power, see "Turning On/Off the Power", Getting Started.

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



CWW222

3. **Press [System Settings].**
4. **Press [Interface Settings].**
5. **Specify IPv4 Address.**

   For details on how to specify the IPv4 address, see "Interface Settings", Connecting the Machine/ System Settings.

6. **Press [File Transfer] in [System Settings].**
7. **Press [Administrator's E-mail Address], and then specify the e-mail address of the administrator of this machine.**
8. **Create and install the device certificate from the control panel.**

   For information on how to install the device certificate, see page 119 "Protecting the Communication Path via a Device Certificate".

   As the e-mail address for the device certificate, enter the address specified in Step 7.

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

   For details about specifying administrators' user names and passwords, see page 16 "Registering and Changing Administrators".

10. **Connect the machine to the general usage network environment.**

Note

- To enable higher security, see page 252 "Additional Information for Enhanced Security".

Administrators and Users

This section explains the terms "administrator", "supervisor", "user", and "owner" as used in this manual.

Administrator

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

Their main role is to specify the settings for operating the machine. Their access privileges depend on the administrator type. Administrators cannot perform normal operations, such as copying and printing.

Supervisor

There is only one supervisor. The supervisor can specify each administrator's password. For normal operations, a supervisor is not required, because administrators specify their own passwords.

User

Users are people using the machine for normal operations, such as copying and printing.

Owner

A user who has registered files in the machine under the copier, printer, or other functions is called an owner.

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 role of administrator for this machine is divided into four categories according to their function: user administrator, machine administrator, network administrator, and file administrator. Sharing administrator tasks eases the burden on individual administrators while at the same time limiting unauthorized operations by an administrator. Multiple administrator roles can be assigned to one administrator and one role can also be shared by more than one administrator. A supervisor can also be set up, who can then change the administrators' passwords.

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 page 16 "Registering and Changing Administrators", and for instructions on changing the administrator's password, see page 23 "Supervisor". For details on Users, see page 27 "Users".

Important

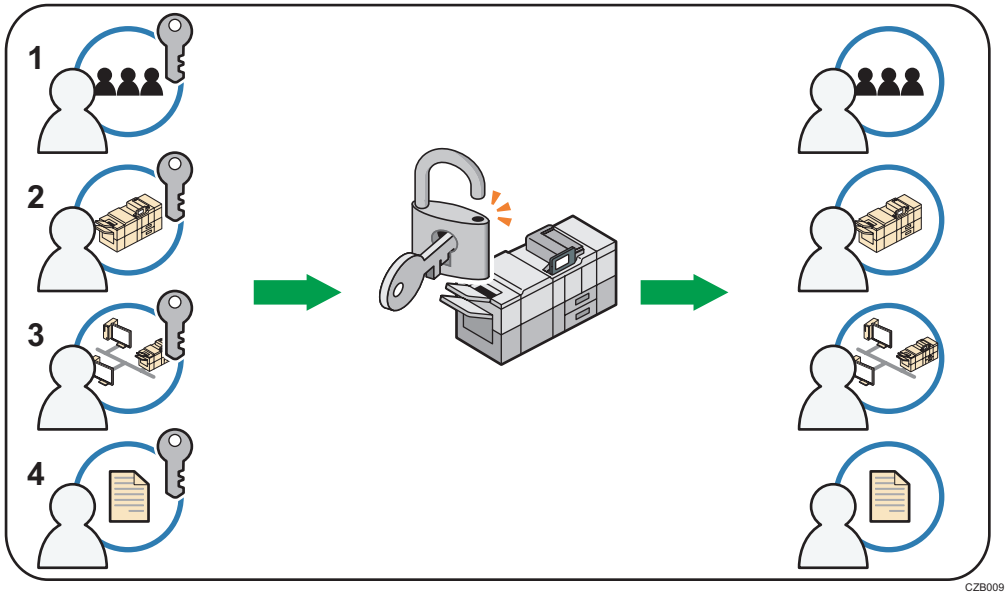
- **If user authentication is not possible because of a problem with the hard disk or network, you can use the machine by accessing it using administrator authentication and disabling user authentication. Do this if, for instance, you need to use the machine urgently.**

Configuring Administrator Authentication

Administrator authentication requires the login user name and password for verifying administrators attempting to specify the machine's settings or access them from a network. 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 privileges are granted to a single login user name. For instructions on registering the administrator, see page 16 "Registering and Changing Administrators".

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 Device Manager NX Lite 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 page 29 "Configuring User Authentication".

Roles of each administrator



1. **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.

2. **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.

3. **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.

4. **File administrator**

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

Note

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

Specifying Administrator Privileges

To specify administrator authentication, set "Administrator Authentication Management" to [On]. If this setting is enabled, administrators will be able to configure only settings allocated to them.

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

When you log in as an administrator, the default login user name is "admin". The password is not configured by default.

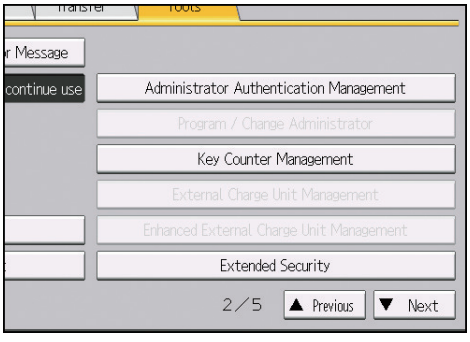
For details about logging in and logging out with administrator authentication, see page 20 "Administrator Login Method" and page 22 "Administrator Logout Method".

Important

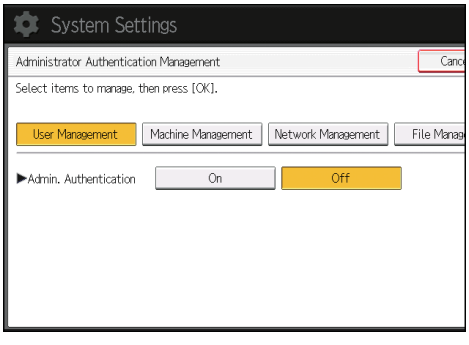
- **If you have enabled "Administrator Authentication Management", make sure not to forget the administrator login user name and login password. If an administrator login user name or login password is forgotten, a new password must be specified using the supervisor's privilege. For details on supervisor privileges, see page 23 "Supervisor".**

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

2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼Next].**
5. **Press [Administrator Authentication Management].**



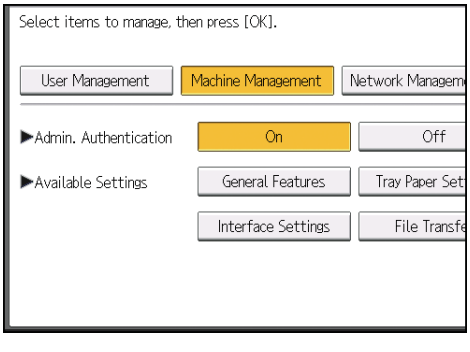
6. **Press [User Management], [Machine Management], [Network Management], or [File Management] to select which settings to manage.**



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

   "Available Settings" appears.

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



   The selected settings will be unavailable to users.

   The available settings depend on the administrator type.

To specify administrator authentication for more than one category, repeat Steps 6 to 8.

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

Registering and Changing Administrators

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

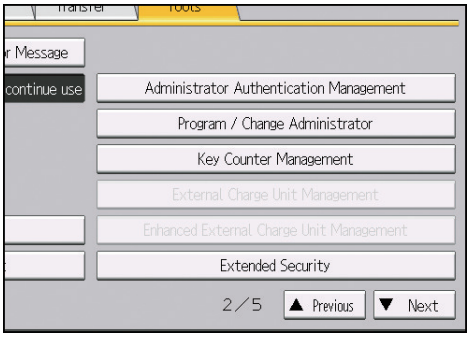
The sharing of administrator tasks eases the burden on individual administrators while also restricting unauthorized operations by a single administrator. You can register up to four login user names (Administrators 1-4) to which you can grant administrator privileges.

An administrator's privileges can only be changed by an administrator with the relevant privileges.

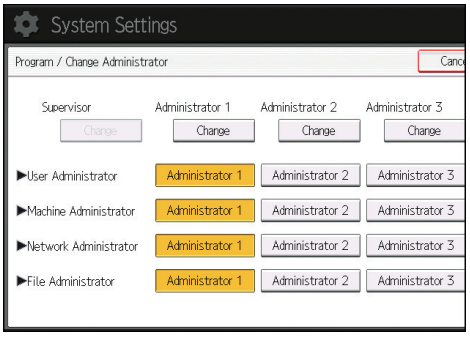
Be sure to assign all administrator privileges so that each administrator privilege is associated with at least one administrator.

For details about logging in and logging out with administrator authentication, see page 20 "Administrator Login Method" and page 22 "Administrator Logout Method".

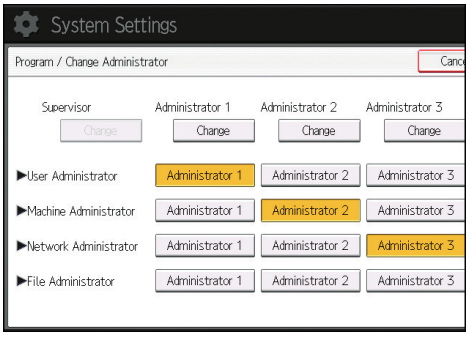
1. **Log in as an administrator from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼Next].**
5. **Press [Program / Change Administrator].**



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



When allocating administrators' privileges to one person each, select one administrator under each category as shown below.



To combine the privileges of multiple administrators, assign multiple administrators to a single administrator.

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

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

    Follow the password policy to strengthen the login password.

    For details about the password policy and how to specify it, see page 243 "Specifying the Extended Security Functions".
11. **Re-enter the login password for confirmation, and then press [OK].**
12. **Press [Change] for "Encryption Password".**
13. **Enter the encryption password, and then press [OK].**

14. **Re-enter the encryption password for confirmation, and then press [OK].**
15. **Press [OK] twice.**

    You will be automatically logged out.

1

Note

- For the characters that can be used for login user names and passwords, see page 18 "Usable characters for user names and passwords".

Usable characters for user names and passwords

The following characters can be used for login user names and passwords. Names and passwords are case sensitive.

- 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)

Login user name

- Cannot contain spaces, colons or quotation marks.
- Cannot be comprised of numbers only or cannot be left blank.
- Can be up to 32 characters long.

Login password

- The maximum password length for administrators and supervisors is 32 characters; for users it is 128 characters.
- There are no restrictions on the types of characters that can be used for a password. For security, it is recommended to create passwords consisting of uppercase or lowercase characters, numbers, and symbols. A password consisting of a large number of characters is less easily guessed by others.
- If the password's complexity and minimum length have been configured in [Password Policy] in [Extended Security], only passwords meeting the requirements can be specified. For details about specifying the password policy, see "Password Policy" in page 243 "Specifying the Extended Security Functions".

Using Web Image Monitor to Configure Administrator Authentication

Using Web Image Monitor, you can log in to the machine and change the administrator settings. For details about logging in and logging out with administrator authentication, see page 20 "Administrator Login Method" and page 22 "Administrator Logout Method".

1. **Log in as an administrator from Web Image Monitor.**
2. **Point to [Device Management], and then click [Configuration].**
3. **Click [Administrator Authentication Management] or [Program/Change Administrator] under "Device Settings".**
4. **Change the settings as desired.**
5. **Log out.**

Note

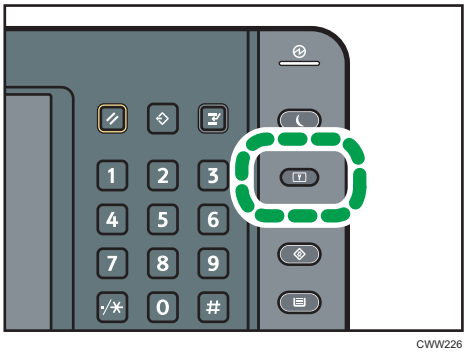
- For details about Web Image Monitor, see Web Image Monitor Help.

Administrator Login Method

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

Logging in Using the Control Panel

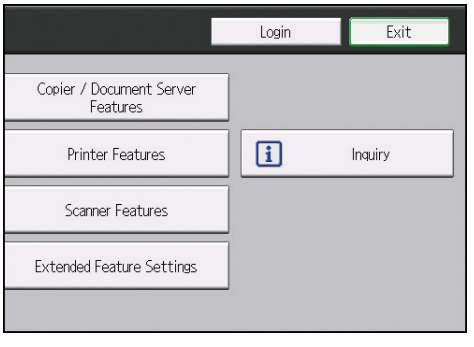
1. **Press the [User Tools] key.**
2. **Press the [Login/Logout] key.**



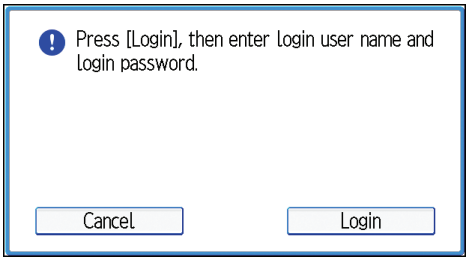
CWW226

The login screen appears.

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



3. **Press [Login].**



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

   The default login name for administrators is "admin" and "supervisor" for supervisors.

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

   There is no preset default password for administrators or supervisors. Therefore, leave the password field blank and press [OK].

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

Note

- If user authentication has already been specified, a screen for authentication appears. To log in as an administrator, enter the administrator's login user name and login password.
- If you log in using administrator privilege, the name of the administrator logging in appears. When you log in with a user name that has multiple administrator privileges, one of the administrator privileges associated with that name is displayed.
- If you try to log in from an operating screen, "You do not have the privileges to use this function. You can only change setting(s) as an administrator." appears. Press the [User Tools] key to change the default.

Logging in Using Web Image Monitor

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

   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.

   Enter the IPv6 address with brackets before and after, like this: [2001:db8::9abc].

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

3. **Click [Login] at the top right of the window.**
4. **Enter the login name and password of an administrator, and then click [Login].**

   The default login name for administrators is "admin" and that for supervisors is "supervisor". No login password is set up.

Note

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

Administrator Logout Method

If administrator authentication has been specified, be sure to log out after completing settings.
Supervisors log out in the same way.

Logging out Using the Control Panel

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

Note

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

Logging out Using Web Image Monitor

1. **Click [Logout] at the top right of the window.**

Note

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

Supervisor

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 you have logged in using the supervisor's user name and password, you cannot use normal functions or specify system settings. The methods for logging in and out are the same as for administrators. See page 20 "Administrator Login Method" and page 22 "Administrator Logout Method".

Important

- **The default login user name is "supervisor". No login password is set up. We recommend changing the login user name and login password.**
- **For the characters that can be used for login user names and passwords, see page 18 "Usable characters for user names and passwords".**
- **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 the machine setting data, counters, logs and other data being lost; consequently, the service call may not be free of charge.**

Note

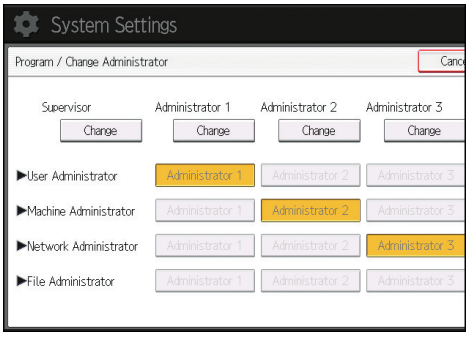
- You cannot specify the same login user name for the supervisor and the administrators.
- Using Web Image Monitor, you can log in as the supervisor and delete an administrator's password or specify a new one.

Resetting the Administrator's Password

1. **Log in as the supervisor from the control panel.**

   For details on how to log in, see page 20 "Administrator Login Method".
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼Next].**
5. **Press [Program / Change Administrator].**

6. **Press [Change] for the administrator you wish to reset.**



7. **Press [Change] for "Login Password".**
8. **Enter the login password, and then press [OK].**
9. **Re-enter the login password for confirmation, and then press [OK].**
10. **Press [OK] twice.**

    You will be automatically logged out.

Note

- The supervisor can change the administrators' login passwords but not their login user names.

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 page 14 "Specifying Administrator Privileges".

1. **Log in as the supervisor from the control panel.**

   For details on how to log in, see page 20 "Administrator Login Method".
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼Next].**
5. **Press [Program / Change Administrator].**
6. **Under "Supervisor", press [Change].**
7. **Press [Change] for "Login User Name".**
8. **Enter the login user name, and then press [OK].**
9. **Press [Change] for "Login Password".**
10. **Enter the login password, and then press [OK].**
11. **Re-enter the login password for confirmation, and then press [OK].**

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

    You will be automatically logged out.

2. Configuring User Authentication

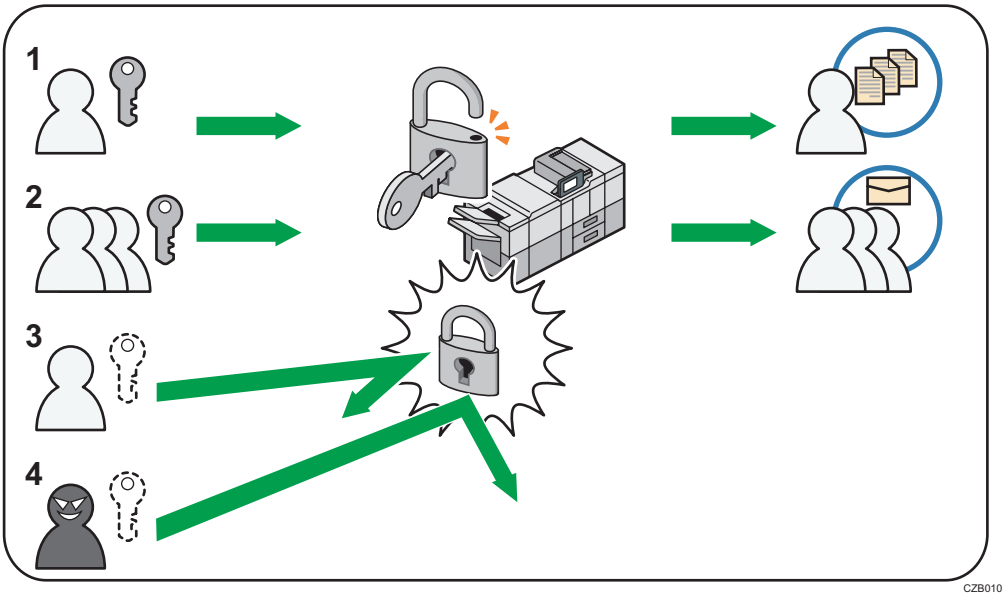
This chapter describes how to specify user authentication and explains the functions that are enabled by user authentication.

Users

A user performs normal operations on the machine, such as copying and printing. Users are managed using the information in the machine's Address Book, and can only use 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 page 12 "Administrators". For details about user registration in the Address Book, see "Registering User Information", Connecting the Machine/ System Settings or Web Image Monitor Help.

About User Authentication

User authentication is a system requiring the login user name and password for verifying users to operate the machine or access the machine over the network.



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. **Unauthorized access**

Configuring User Authentication

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

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.**
- **You cannot use more than one authentication method at the same time.**

User authentication configuration flow

Configuration procedure	Details
Configuring administrator authentication	page 14 "Specifying Administrator Privileges" page 16 "Registering and Changing Administrators"
Configuring user authentication	Specify user authentication. Five types of user authentication are available: • page 32 "User Code Authentication" • page 35 "Basic Authentication" • page 40 "Windows Authentication" • page 49 "LDAP Authentication" • page 54 "Integration Server Authentication"

User authentication methods

Type	Details
User Code authentication	Authentication is performed using eight-digit user codes. Authentication is applied to each user code, not to each user. It is necessary to register the user code in the machine's address book in advance.

Type	Details
Basic authentication	Authentication is performed using the machine's address book. It is necessary to register users in the machine's address book in advance. Authentication can be applied to each user.
Windows authentication	Authentication is performed using the domain controller of the Windows server on the same network as the machine. Authentication can be applied to each user.
LDAP authentication	Authentication is performed using the LDAP server on the same network as the machine. Authentication can be applied to each user.
Integration Server authentication	Authentication is performed using an external authentication server on the same network as the machine. This establishes an environment in which authentication is applied collectively to users of devices (such as MFPs and computers) over the network. Authentication can be applied to each user. To create an external authentication server, software including Authentication Manager is required.

A user's e-mail address obtained via Windows, LDAP, or Integration Server authentication can be used as the sender's fixed address ("From") when sending e-mails in the scanner mode in order to prevent ID fraud. You can use the scanner function on Type 1, 2, or 3 machines only.

If the user authentication method is switched halfway

- 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", Connecting the Machine/ System Settings. For details about changing passwords, see page 37 "Specifying Login User Names and Passwords".

Note

- After turning the main power on, extended features may not appear in the list of user authentication items in the User Authentication Management menu. If this happens, wait a while and then open the User Authentication Management menu again.
- User authentication can also be specified via Web Image Monitor. For details, see Web Image Monitor Help.

User Code Authentication

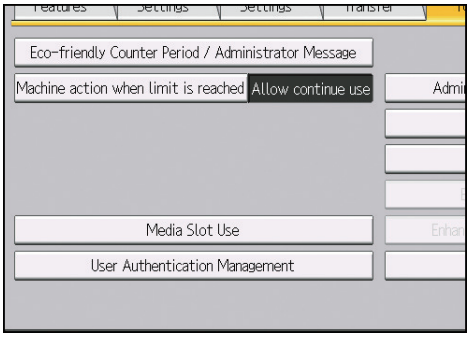
This is an authentication method for limiting access to functions according to a user code. The same user code can be used by more than one user.

For details about specifying user codes, see "Registering a User Code", Connecting the Machine/ System Settings.

For details about specifying the user code on the printer driver or TWAIN driver, see the driver help.

You can use the Document Server function and TWAIN driver on Type 1, 2, or 3 machines only.

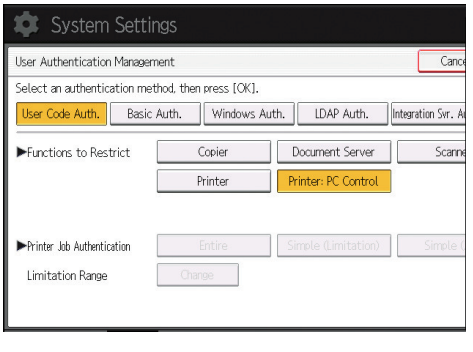
1. **Log in as the machine administrator from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼Next].**
5. **Press [User Authentication Management].**



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

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

7. **In "Functions to Restrict" and "Extended Features to Restrict", select the functions you want to restrict.**



The selected functions are subject to User Code authentication. User Code authentication is not applied to the functions not selected.

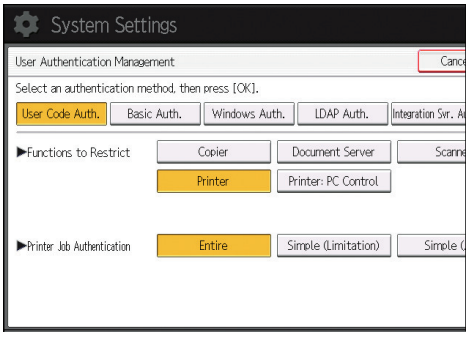
The Extended Features to Restrict menu appears only if an extended feature is installed in the machine.

For details about limiting available functions for individuals or groups, see page 76 "Limiting Available Functions".

8. **Under "Functions to Restrict", either deselect [Printer: PC Control] or select [Printer].**

   If you do not want to specify printer job authentication, proceed to step 14.

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

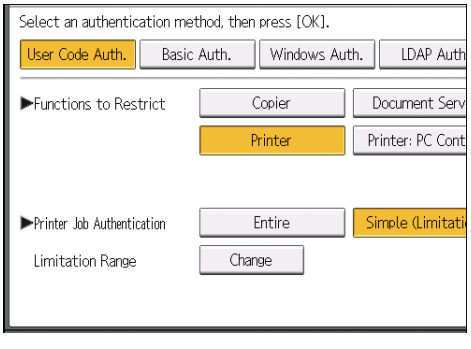


   For a description of the printer job authentication levels, see page 59 "Printer Job Authentication".

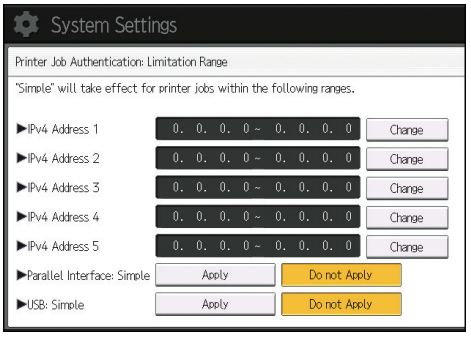
   If you select [Entire] or [Simple (All)], proceed to step 13.

   If you select [Simple (Limitation)], proceed to step 10.

10. **Press [Change].**



11. **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 parallel and USB interfaces.

12. **Press [Exit].**

13. **Press [OK].**

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

A confirmation message appears.

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

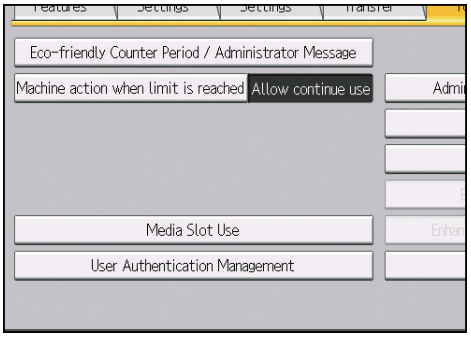
Basic Authentication

Specify this authentication method when using the machine's Address Book to authenticate each user. Using Basic authentication, you can not only manage the machine's available functions but also limit access to stored files and to 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 page 37 "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".

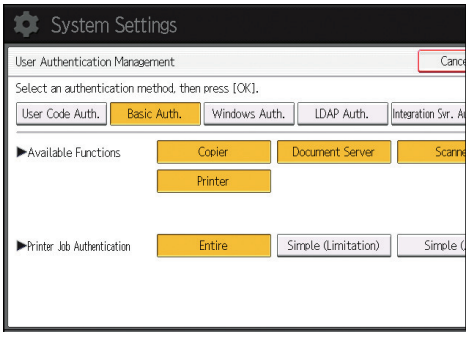
1. **Log in as the machine administrator from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼Next].**
5. **Press [User Authentication Management].**



6. **Select [Basic Auth.].**

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

7. **In "Available Functions" and "Available Extended Features", select the machine functions you want to permit.**



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

The Available Extended Features menu appears only if an extended feature is installed in the machine.

For details about specifying available functions for individuals or groups, see page 76 "Limiting Available Functions".

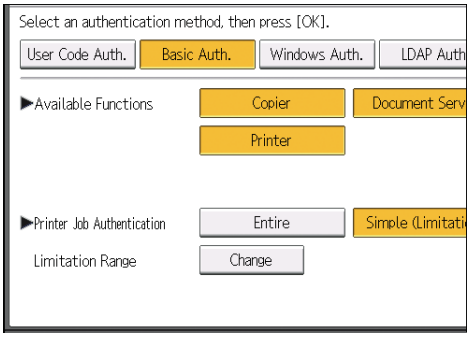
8. **Select the "Printer Job Authentication" level.**

For a description of the printer job authentication levels, see page 59 "Printer Job Authentication".

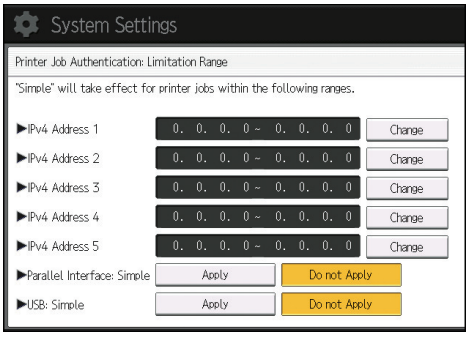
If you select [Entire] or [Simple (All)], proceed to step 12.

If you select [Simple (Limitation)], proceed to step 9.

9. **Press [Change].**



10. **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 parallel and USB interfaces.

11. **Press [Exit].**
12. **Press [OK].**
13. **Press the [Login/Logout] key.**

A confirmation message appears.

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

Authentication Information Stored in the Address Book

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 page 76 "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 in the Address Book, see "Registering User Information", Connecting the Machine/ System Settings.

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

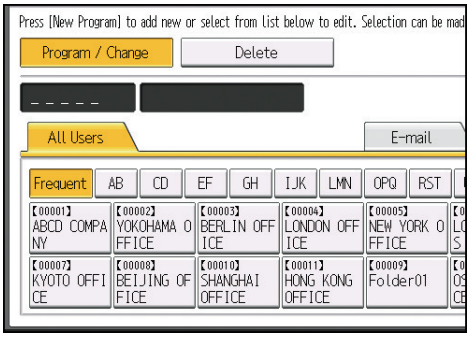
Specifying Login User Names and Passwords

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

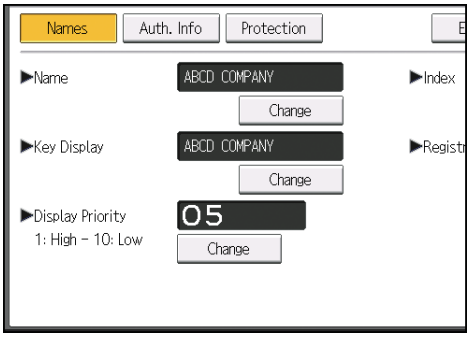
For the characters that can be used for login user names and passwords, see page 18 "Usable characters for user names and passwords".

1. **Log in as the user administrator from the control panel.**

2. **Press [Address Book Mangmnt].**
3. **Select the user.**



4. **Press [Auth. Info].**



5. **Press [Change] for "Login User Name".**
6. **Enter a login user name, and then press [OK].**
7. **Press [Change] for "Login Password".**
8. **Enter a login password, and then press [OK].**
9. **Re-enter the login password for confirmation, and then press [OK].**
10. **Press [OK].**
11. **Press [Exit].**
12. **Log out.**

Specifying Login Details

You can specify this setting on Type 1, 2, or 3 machines only.

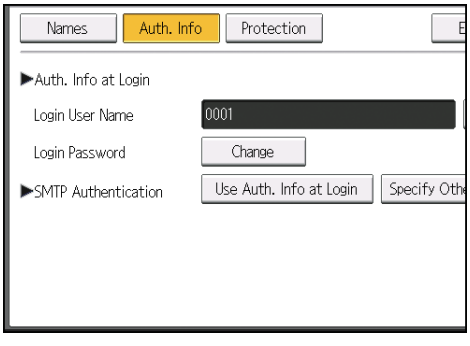
The login user name and password specified in "Address Book Management" can be used as the login information for "SMTP Authentication", "Folder Authentication", and "LDAP Authentication".

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", Connecting the Machine/ System Settings.

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.**

1. **Log in as the user administrator from the control panel.**
2. **Press [Address Book Mangmnt].**
3. **Select the user.**
4. **Press [Auth. Info].**
5. **Select [Use Auth. Info at Login] in "SMTP Authentication".**



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

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

If the function you want to select is not displayed, press [▼Next].

6. **Press [OK].**
7. **Press [Exit].**
8. **Log out.**

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.

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.

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. To do this, you must create a server certificate for the domain controller. For details about creating a server certificate, see page 47 "Creating the Server Certificate".

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 or SSLv3.
    - Windows Server 2008/2008 R2
    - Windows Server 2012/2012 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 or SSLv3. Compatible operating systems are listed below.
    - Windows Server 2008/2008 R2
    - Windows Server 2012/2012 R2

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

- Transmission between the machine and the KDC server is encrypted if Kerberos authentication is enabled. For details about specifying encrypted transmission, see page 163 "Kerberos Authentication Encryption Setting".

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.**
- **When Type 1, 2, or 3 is used and if Kerberos authentication and SSL encryption are set at the same time, e-mail addresses cannot be obtained.**
- **If you created a new user in the domain controller and selected "User must change password at next logon" at password configuration, first log on to the computer and change the password.**
- **If the authenticating server only supports NTLM when Kerberos authentication is selected on the machine, the authenticating method will automatically switch to NTLM.**
- **When using Windows authentication, the login name is case sensitive. If you make a mistake, the user's login name will be added to the address book. You should delete the added user.**
- **If the "Guest" account on the Windows server is enabled, even users not registered in the domain controller can be authenticated. When this account is enabled, users are registered in the Address Book and can use the functions available under "*Default Group".**

Note

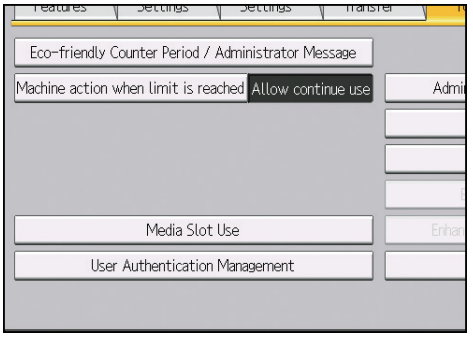
- For the characters that can be used for login user names and passwords, see page 18 "Usable characters for user names and passwords".
- When accessing the machine subsequently, you can use all the functions available to your group and to you as an individual user.
- Users who are registered in multiple groups can use all the functions available to those groups.
- 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.

Specifying Windows Authentication

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

1. **Log in as the machine administrator from the control panel.**
2. **Press [System Settings].**

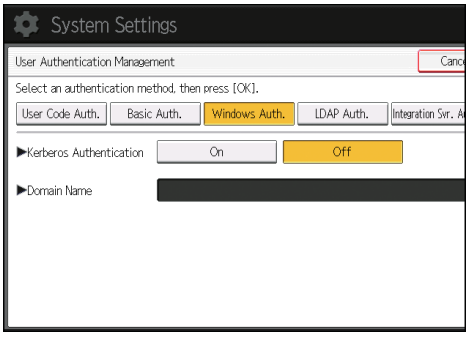
3. **Press [Administrator Tools].**
4. **Press [▼Next].**
5. **Press [User Authentication Management].**



6. **Select [Windows Auth.].**

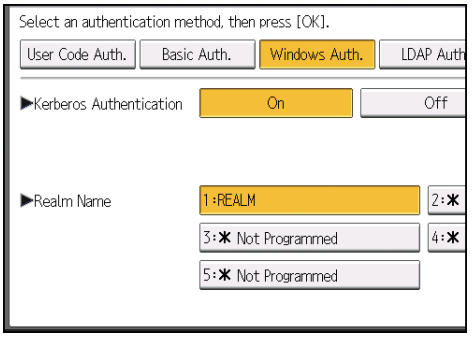
   If you do not want to use user authentication management, select [Off].

7. **If you want to use Kerberos authentication, press [On].**



   If you want to use NTLM authentication, press [Off] and proceed to step 9.

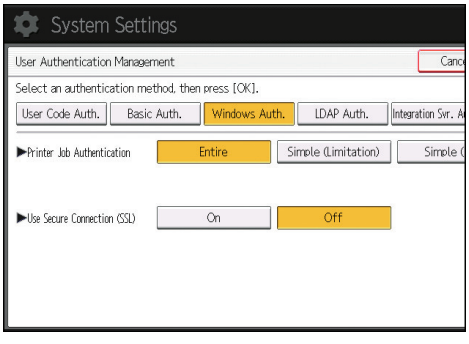
8. **Select Kerberos authentication realm and proceed to step 10.**



   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", Connecting the Machine/ System Settings.

Up to 5 realms can be registered.

9. **Press [Change] for "Domain Name", enter the name of the domain controller to be authenticated, and then press [OK].**
10. **Press [▼Next].**
11. **Select the "Printer Job Authentication" level.**

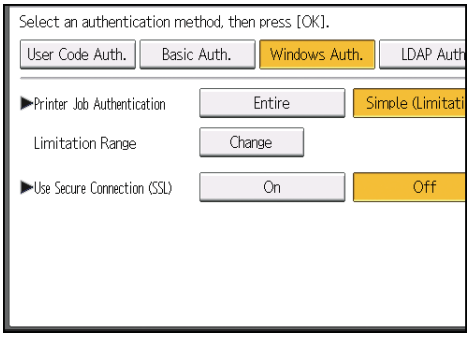


For a description of the printer job authentication levels, see page 59 "Printer Job Authentication".

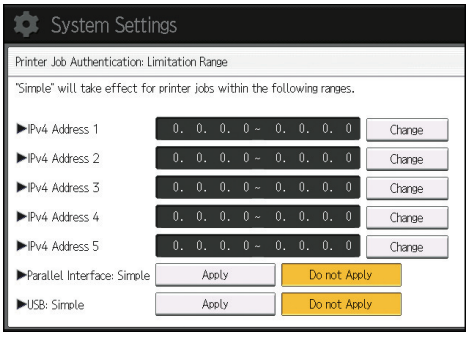
If you select [Entire] or [Simple (All)], proceed to step 15.

If you select [Simple (Limitation)], proceed to step 12.

12. **Press [Change].**



13. **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 parallel and USB interfaces.

14. **Press [Exit].**
15. **Press [On] for "Use Secure Connection (SSL)".**

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

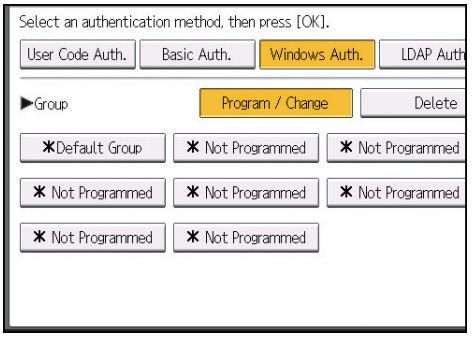
    If you have not registered a global group, proceed to step 22.

    If you have registered a global group, proceed to step 16.

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

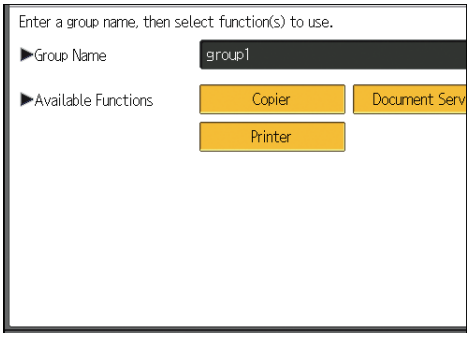
    You need to create global groups in the Windows server in advance and register in each group the users to be authenticated. You also need to register in the machine the functions available to the global group members. Create global groups in the machine by entering the names of the global groups registered 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.
16. **Press [▼Next].**
17. **Under "Group", press [Program / Change], and then press [* Not Programmed].**



18. **Press [Change] for "Group Name", and then enter the group name.**
19. **Press [OK].**

20. **In "Available Functions" and "Available Extended Features", select the machine functions you want to permit.**



Windows Authentication will be applied to the selected functions.

Users can use the selected functions only.

The Available Extended Features menu appears only if an extended feature is installed in the machine.

For details about specifying available functions for individuals or groups, see page 76 "Limiting Available Functions".

21. **Press [OK].**
22. **Press [OK].**
23. **Press the [Login/Logout] key.**

A confirmation message appears.

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

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:

Installation under Windows Server 2008 R2

1. **On the [Start] menu, point to [Administrative 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>].**

   If a confirmation message appears, click [Add Features].
5. **Read the content information, and then click [Next>].**
6. **Check 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].**

Installation under Windows Server 2012 R2

1. **On the Start screen, click [Server Manager].**
2. **On the [Manage] menu, click [Add Roles and Features].**
3. **Click [Next>].**
4. **Select [Role-based or feature-based installation], and then click [Next>].**
5. **Select a server.**
6. **Select the "Active Directory Certificate Services" and "Web Server (IIS)" check boxes, and then click [Next>].**

   If a confirmation message appears, click [Add Features].
7. **Check the features you want to install, and then click [Next>].**
8. **Read the content information, and then click [Next>].**

9. **Make sure that [Certification Authority] is selected in the [Role Services] area in [Active Directory Certificate Services], and then click [Next>].**
10. **Read the content information, and then click [Next>].**
11. **Check the role services you want to install under [Web Server (IIS)], and then click [Next>].**
12. **Click [Install].**
13. **After completing the installation, click the Server Manager's Notification icon , and then click [Configure Active Directory Certificate Services on the destination server].**
14. **Click [Next>].**
15. **Click [Certification Authority] in the [Role Services] area, and then click [Next>].**
16. **Select [Enterprise CA], and then click [Next>].**
17. **Select [Root CA] , and then click [Next>].**
18. **Select [Create a new private key], and then click [Next>].**
19. **Select a cryptographic provider, key length, and hash algorithm to create a new private key, and then click [Next>].**
20. **In "Common name for this CA:", enter the Certificate Authority name, and then click [Next>].**
21. **Select the validity period, and then click [Next>].**
22. **Leave the "Certificate database location:" and the "Certificate database log location:" settings set to their defaults, and then click [Next>].**
23. **Click [Configure].**
24. **If the message "Configuration succeeded" appears, click [Close].**

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 [Administrative Tools], and then click [Internet Information Services (IIS) Manager].**

   Under Windows Server 2012/2012 R2, click [Internet Information Services (IIS) Manager] on the Start screen.

   When the confirmation message appears, click [Yes].
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].

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 page 47 "Creating the Server Certificate". The setting for using SSL can be specified in the LDAP server setting.

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

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.

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", Connecting the Machine/ System Settings.

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 directory server.**
- **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 Active Directory in LDAP authentication when Kerberos authentication and SSL are set at the same time, e-mail addresses cannot be obtained.**
- **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.**

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 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".

For details about registering an LDAP server, see "Programming the LDAP server", Connecting the Machine/ System Settings.

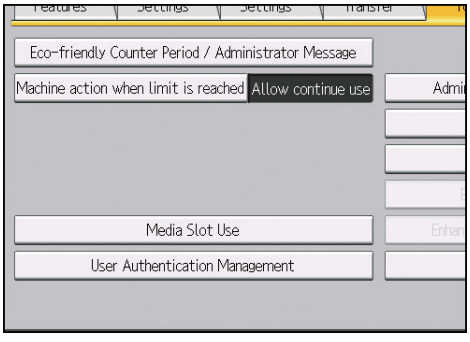
Note

- For the characters that can be used for login user names and passwords, see page 18 "Usable characters for user names and passwords".
- In LDAP simple authentication mode, authentication will fail if the password is left blank. To allow blank passwords, contact your service representative.
- 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.
- Transmission between the machine and the KDC server is encrypted if Kerberos authentication is enabled. For details about specifying encrypted transmission, see page 163 "Kerberos Authentication Encryption Setting".

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

1. **Log in as the machine administrator from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**

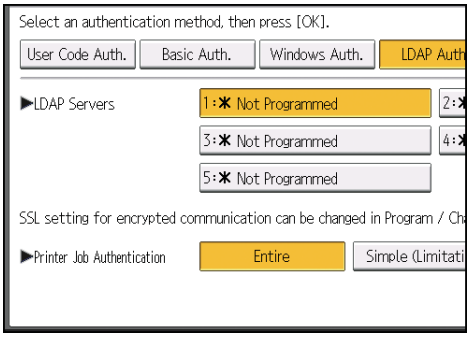
4. **Press [▼Next].**
5. **Press [User Authentication Management].**



6. **Select [LDAP Auth.].**

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

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



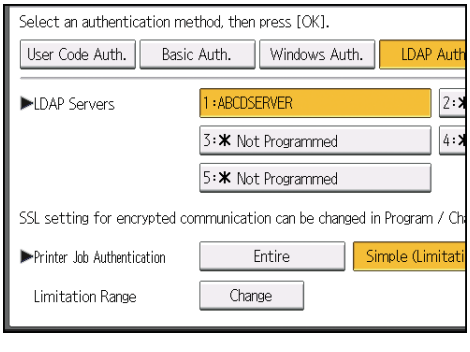
8. **Select the "Printer Job Authentication" level.**

   For a description of the printer job authentication levels, see page 59 "Printer Job Authentication".

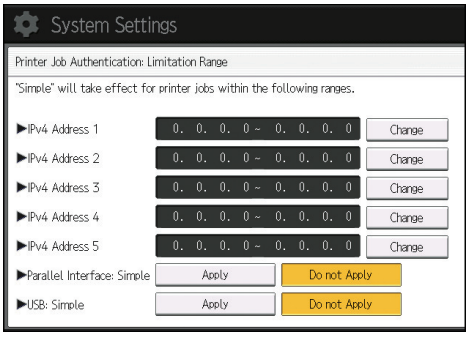
   If you select [Entire] or [Simple (All)], proceed to step 12.

   If you select [Simple (Limitation)], proceed to step 9.

9. **Press [Change].**

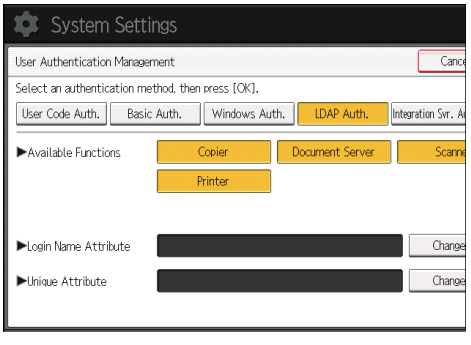


10. **Specify the range in which [Simple (Limitation)] is applied to "Printer Job Authentication".**



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

11. **Press [Exit].**
12. **Press [▼Next].**
13. **In "Available Functions" and "Available Extended Features", select the machine functions you want to permit.**



LDAP authentication will be applied to the selected functions.

Users can use the selected functions only.

The Available Extended Features menu appears only if an extended feature is installed in the machine.

For details about specifying available functions for individuals or groups, see page 76 "Limiting Available Functions".

14. **Press [Change] for "Login Name Attribute".**
15. **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.

16. **Press [Change] for "Unique Attribute".**
17. **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.
18. **Press [OK].**
19. **Press the [Login/Logout] key.**

    A confirmation message appears.

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

Integration Server Authentication

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

To use the Integration Server authentication, software featuring Authentication Manager is required. For details about supported software, contact your sales representative.

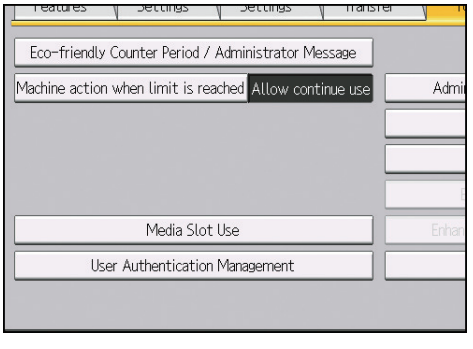
Using Web Image Monitor, you can specify that the server reliability and site certificate are checked every time you access the SSL server. For details about specifying SSL using Web Image Monitor, see Web Image Monitor Help.

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".**

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

1. **Log in as the machine administrator from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼Next].**
5. **Press [User Authentication Management].**



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

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

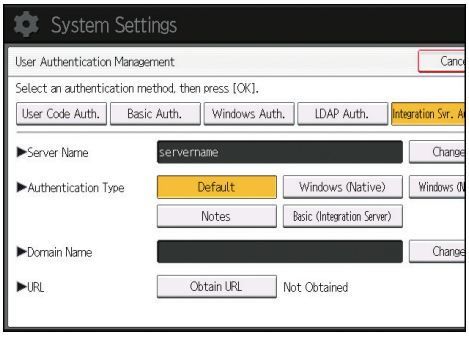
7. **Press [Change] for "Server Name".**

   Specify the name of the server for external authentication.

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

   Enter the IPv4 address or host name.

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



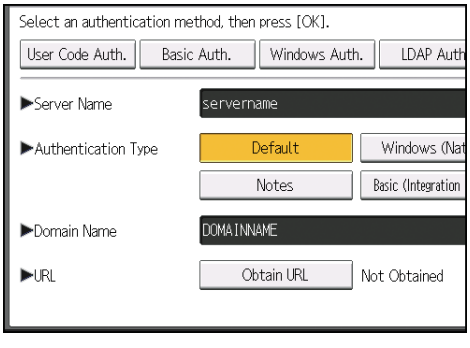
   Select an available authentication system. For general usage, select [Default].

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

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

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

12. **Press [Obtain URL].**



    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".

13. **Press [Exit].**

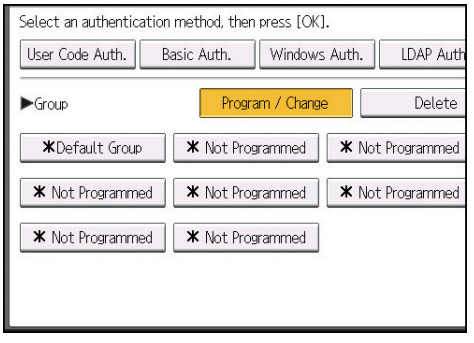
    If you have not registered a group on the external authentication system being used, proceed to Step 20.

    If you have registered a group, proceed to step 14.

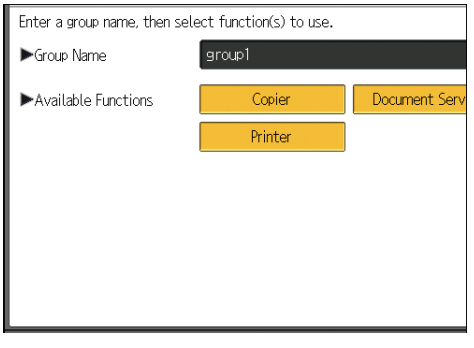
    If you set "Authentication Type" to [Windows (Native)] or [Windows (NT Compatible)], you can use the global group.

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.

14. **Press [▼Next].**
15. **Press [Program / Change] for "Group", and then press [* Not Programmed].**



16. **Press [Change] for "Group Name", and then enter the group name.**
17. **Press [OK].**
18. **In "Available Functions" and "Available Extended Features", select the machine functions you want to permit.**



Authentication will be applied to the selected functions.

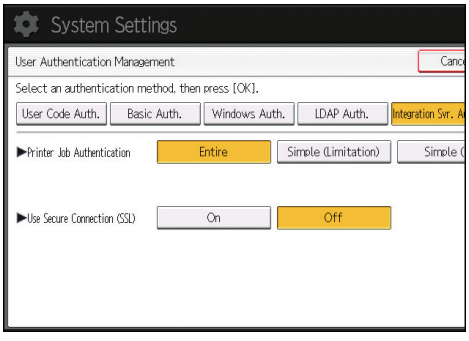
Users can use the selected functions only.

The Available Extended Features menu appears only if an extended feature is installed in the machine.

For details about specifying available functions for individuals or groups, see page 76 "Limiting Available Functions".

19. **Press [OK].**
20. **Press [▼Next].**

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



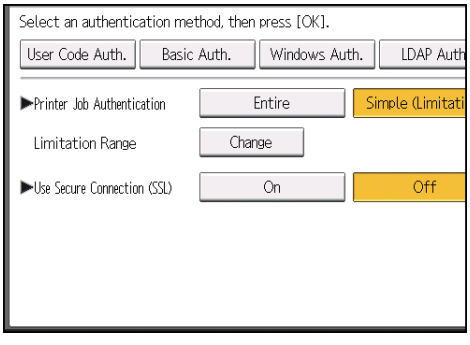
If you cannot see this item, press [▼Next] to display more settings.

For a description of the printer job authentication levels, see page 59 "Printer Job Authentication".

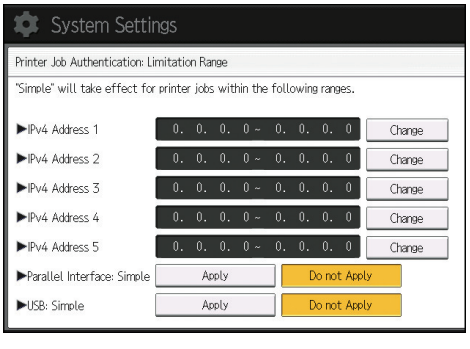
If you select [Entire] or [Simple (All)], proceed to step 25.

If you select [Simple (Limitation)], proceed to step 22.

22. **Press [Change].**



23. **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 parallel and USB interfaces.

24. **Press [Exit].**

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

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

26. **Press [OK].**

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

    A confirmation message appears.

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

Printer Job Authentication

Printer job authentication is a function allowing user authentication to be applied to print jobs.

User authentication is supported by the PCL and PostScript3 drivers. The PostScript3 driver supports User Code authentication only.

Printer Job Authentication Levels

The security level for "Entire" is the highest, followed by "Simple (Limitation)", and at the bottom, "Simple (All)".

- Entire

  Select this to authenticate all print jobs and remote configuration.

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

  To print in an environment that does not support authentication, select [Simple (All)] or [Simple (Limitation)].

- Simple (Limitation)

  Select this to restrict the range of [Simple (All)].

  The specified range can be printed regardless of the authentication. Authentication will be applied to addresses outside this range.

  You can specify whether to apply [Simple (All)] to parallel connection, USB connection, and the user's IPv4 address. The range of application to IPv6 addresses can be configured from Web Image Monitor.

- Simple (All)

  Select this if you want to print with a printer driver or device that cannot be identified by the machine or if authentication is not required for printing.

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

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

  Unauthorized users may be able to use the machine since printing is allowed without user authentication.

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 types: A printer job is specified when:

1. The [User Authentication] check box is selected in the PCL printer driver or in the PCL universal driver.
2. The [User Authentication] and [With Encryption] check boxes are selected in the PCL mini-driver*.

   * The authentication function cannot be used with IA-64 OS.
3. The [User Authentication] check box is selected in the PCL mini-driver.
4. The [User Authentication] check box is not selected in the PCL printer driver or in the PCL mini-driver*.

   * The authentication function cannot be used with IA-64 OS.
5. When the User Code is entered using the PostScript 3 printer driver or PS3 universal driver.

   This also applies to recovery/parallel printing using a PCL printer driver that does not support authentication.
6. When the User Code is not entered using the PostScript 3 printer driver or PS3 universal driver. This also applies to recovery/parallel printing using a PCL printer driver that does not support authentication.
7. A printer job or PDF file is sent from a host computer without a printer driver and is printed via LPR. This can be also applied to Mail to Print.
8. 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.

Printer job authentication levels and printer job types

Printer Job Authentication	Simple (All)	Simple (All)	Simple (All)	Entire	Entire	Entire
Driver Encryption Key:Encryption Strength	Simple Encryption	DES	AES	Simple Encryption	DES	AES
Printer Job Type 1	C*1	C*1	C*1	C*1	C*1	C*1
Printer Job Type 2	C*1	C*1	X*1	C*1	C*1	X*1

Printer Job Authentication	Simple (All)	Simple (All)	Simple (All)	Entire	Entire	Entire
Driver Encryption Key:Encryption Strength	Simple Encryption	DES	AES	Simple Encryption	DES	AES
Printer Job Type 3	B	X*1	X*1	B	X*1	X*1
Printer Job Type 4	X	X	X	X	X	X
Printer Job Type 5	A	A	A	B	B	B
Printer Job Type 6	A	A	A	X	X	X
Printer Job Type 7	A	A	A	X	X	X
Printer Job Type 8	B	B	B	B	B	B

*1 Printing with User Code authentication is classified as 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.

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

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

Note

- For details about "Driver Encryption Key:Encryption Strength", see page 243 "Specifying the Extended Security Functions".

"authfree" Command

If [Simple (Limitation)] is selected under printer job authentication, the telnet authfree command can be used to specify exceptions to the printer job authentication.

The default user name for logging into telnet is "admin". The password is not configured by default. For details about logging into and using telnet, see "Remote Maintenance Using telnet", Connecting the Machine/ System Settings.

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 "start-address" "end-address"
```

IPv6 address settings

```
msh> authfree "ID" range6 "start-address" "end-address"
```

IPv6 address mask settings

```
msh> authfree "ID" mask6 "base-address" "masklen"
```

Parallel/USB settings

```
msh> authfree [parallel|usb] [on|off]
```

- To exclude parallel and USB connections from printer job authentication, set this to "on". The default setting is "off".
- Always specify either "parallel" or "USB".

  "parallel" can be specified when an optional IEEE 1284 interface board is installed.

Authentication exclusion control initialization

```
msh> authfree flush
```

Note

- In both IPv4 and IPv6 environments, up to five access ranges can be registered and selected.

Auto Registration to the Address Book

The personal information of users logging in via Windows, LDAP or Integration Server authentication is automatically registered in the Address Book. Any other information may be specified by copying from other registered users.

When using Type 1, 2, or 3, items for the copier function, Document Server function, scanner function, E-mail address, and Protect File(s) are registered automatically.

You can use Data Carry-over Setting for Address Book Auto-program on Type 1, 2, or 3 machines only.

Automatically Registered Address Book Items

- Login User Name
- Login Password
- Registration No.
- Name*1
- Key Display*1
- E-mail Address*2
- Protect File(s)

  Permissions for Users / Groups*3

*1 If this information cannot be obtained, the login user name is registered in this field.

*2 If this information cannot be obtained, auto registration does not work.

*3 If [Data Carry-over Setting for Address Book Auto-program] is set to [Carry-over Data], it has priority.

Note

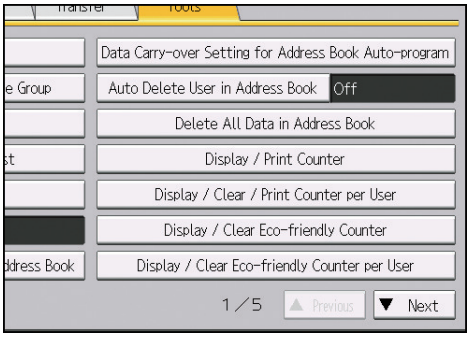
- You can automatically delete old user accounts when performing auto registration if the amount of data registered in the address book has reached the limit. For details, see page 242 "Managing the Address Book".

Data Carry-over Setting for Address Book Auto-program

Information that is not automatically registered in the Address Book can be copied from an already registered user and then registered.

1. **Log in as the user administrator from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**

4. **Press [Data Carry-over Setting for Address Book Auto-program].**



5. **Press [Carry-over Data].**
6. **Use the number keys to enter the registration number of the Address Book to apply the specified setting, and then press [#].**
7. **Press [OK].**
8. **Press the [Login/Logout] key.**

   A confirmation message appears.

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

Locked out user	Unlocking administrator
supervisor	machine administrator

Specifying the User Lockout Function

1. **Log in as the machine administrator from Web Image Monitor.**
2. **Point to [Device Management], and then click [Configuration].**
3. **Click [User Lockout Policy] under "Security".**
4. **Set "Lockout" to [Active].**
5. **In the drop-down menu, select the number of login attempts to permit before applying lockout.**
6. **After lockout, if you want to cancel lockout after a specified time elapses, set "Lockout Release Timer" to [Active].**
7. **In the "Lock Out User for" field, enter the number of minutes until lockout is disabled.**
8. **Click [OK].**

   User Lockout Policy is set.
9. **Log out.**

Canceling Password Lockout

1. **Log in as the user administrator from Web Image Monitor.**
2. **Point to [Device Management], and then click [Address Book].**
3. **Select the locked out user's account.**
4. **Click [Detail Input], and then click [Change].**
5. **Set "Lockout" to [Inactive] under "Authentication Information".**
6. **Click [OK].**
7. **Log out.**

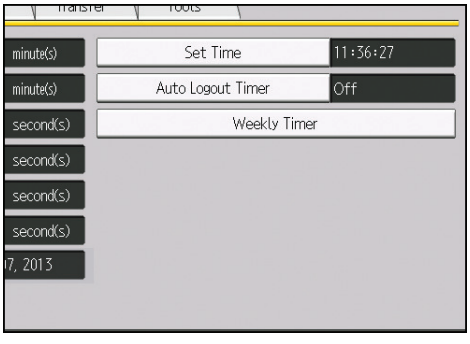
Note

- You can cancel the administrator and supervisor password lockout by turning the main 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

After you log in, the machine automatically logs you out if you do not use the control panel within a given time. This feature is called "Auto Logout". Specify how long the machine is to wait before performing Auto Logout.

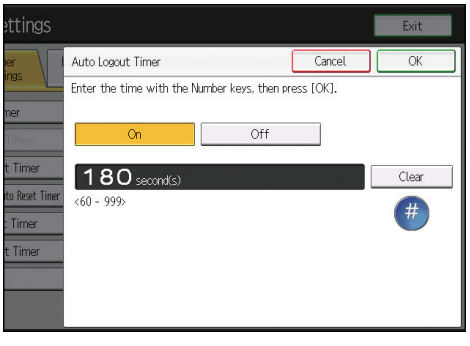
1. **Log in as the machine administrator from the control panel.**
2. **Press [System Settings].**
3. **Press [Timer Settings].**
4. **Press [Auto Logout Timer].**



5. **Select [On].**

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

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



   If you make a mistake, press [Clear].

7. **Press [OK].**
8. **Press the [Login/Logout] 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.
- You can specify the Auto Logout setting for Web Image Monitor in [Webpage]. For details, see the Web Image Monitor Help.

Authentication Using an External Device

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

For details, contact your sales representative.

3. Restricting Machine Usage

This chapter explains how to restrict use of the machine by the user.

Restricting Usage of the Destination List

The use of the destination list can be restricted under the scanner function.

You can use the scanner function on Type 1, 2, or 3 machines only.

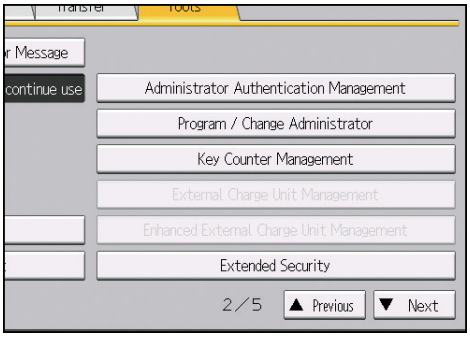
Restrict Use of Destinations

You can prohibit the sending scanned documents to addresses other than those registered in the Address Book. By enabling this, you can prohibit users from manually entering the e-mail address or folder destination.

Restrict Adding of User Destinations

With regard to the addresses manually entered for sending scanned documents, you can prohibit the their registration into the Address Book using [Prg. Dest.]. Also note that with this setting, only the user administrator can register new users in the Address Book and change the passwords and other information of existing registered users. Also, note that even if you set these functions to [On], the user registered as destination can change their password. Only the user administrator can change items other than the password.

1. **Log in as the user administrator from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼Next].**
5. **Press [Extended Security].**



6. **Press [▼Next].**
7. **Set "Restrict Use of Destinations" or "Restrict Adding of User Destinations" to [On].**

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

8. **Press [OK].**
9. **Press the [Login/Logout] key.**

   A confirmation message appears.

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

Preventing Changes to Administrator Settings

Limiting the Settings that Can Be Changed by Each Administrator

The settings that can be made for this machine vary depending on the type of administrator, allowing the range of operations that can be made to be divided among the administrators.

The following administrators are defined for this machine.

- User administrator
- Machine administrator
- Network administrator
- File administrator

For details on the settings that can be made by each administrator, see page 279 "List of Operation Privileges for Settings".

Register the administrators before using the machine. For instructions on registering the administrator, see page 16 "Registering and Changing Administrators".

Prohibiting Users from Making Changes to Settings

Makes it possible to prohibit users from changing administrator settings.

Select the item under "Available Settings" in "Administrator Authentication Management" to prevent such changes.

For details on selections in "Available Settings", see page 13 "Configuring Administrator Authentication".

Specifying Menu Protect

Menu Protect allows you to limit user permission to access the settings in the User Tools menu except for the System Settings. This setting can be used regardless of user authentication. To change the menu protect setting, first enable administrator authentication. For details on how to set administrator authentication, see page 13 "Configuring Administrator Authentication". For a list of settings that users can specify according to the menu protect level, see page 279 "List of Operation Privileges for Settings".

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.

If you want to disable "Menu Protect", specify it to [Off].

You can specify the items for the copier and scanner functions on Type 1, 2, and 3 machines only.

Copy Function

1. **Log in as the machine administrator from the control panel.**
2. **Press [Copier / Document Server Features].**
3. **Press [Administrator Tools].**
4. **Press [Menu Protect].**
5. **Select the menu protect level, and then press [OK].**
6. **Log out.**

Printer Function

1. **Log in as the machine administrator from the control panel.**
2. **Press [Printer Features].**
3. **Press [Data Management].**
4. **Press [Menu Protect].**
5. **Select the menu protect level, and then press [OK].**
6. **Log out.**

Scanner Function

1. **Log in as the machine administrator from the control panel.**
2. **Press [Scanner Features].**

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

Limiting Available Functions

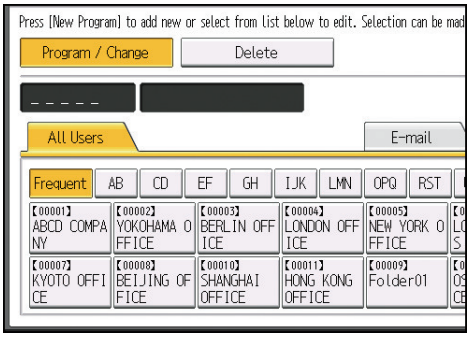
To prevent unauthorized operation, you can specify who is allowed to access each of the machine's functions.

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

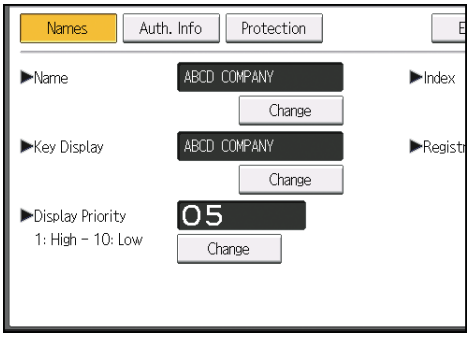
When using Type 1, 2, or 3, you can place limitations on the use of the copier, Document Server, scanner, printer, and extended features.

When using Type 4 or 5, you can place limitations on the use of the printer function and extended features.

1. **Log in as the user administrator from the control panel.**
2. **Press [Address Book Mangmnt].**
3. **Select the user.**

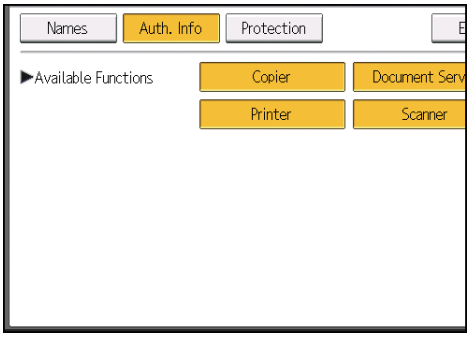


4. **Press [Auth. Info].**



5. **Press ▼[Next] twice.**

6. **In "Available Functions" and "Available Extended Features", select the machine functions you want to permit.**



The Available Extended Features menu appears only if an extended feature is installed in the machine.

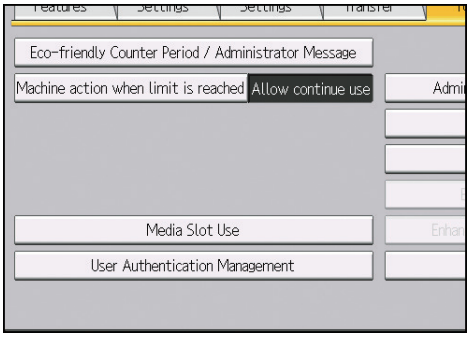
7. **Press [OK].**
8. **Log out.**

Restricting Media Slot Access

Specify on the control panel whether or not to allow users to use the media slots. With this setting, you can restrict storing scanned files on a removable memory device, and also restrict printing of files stored on a removable memory device.

You can store files on a removable memory device on Type 1, 2, and 3 machines.

1. **Log in as the machine administrator from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼Next].**
5. **Press [Media Slot Use].**



6. **To restrict storing files on a removable memory device, press [Prohibit] under "Store to Memory Device".**
7. **To restrict printing of files stored on a removable memory device, press [Prohibit] under "Print from Memory Storage Device".**
8. **Press [OK].**
9. **Log out.**

Note

- If you select [Prohibit] under "Store to Memory Device", the [Store to Memory Device] button is not displayed on the Store File screen of the scanner function.
- If you select [Prohibit] under "Print from Memory Storage Device", the [Print from Memory Storage Device] button is not displayed on the printer function's initial screen.

Managing Print Volume per User

This function limits how much each user can print. If users reach their maximum print volume, their print jobs are canceled and/or a message indicating so is displayed.

Print volume

The print volume is calculated by multiplying the number of pages by a unit count.

The unit count can be specified according to the printing condition. For example, if one page is printed with a unit count of 10, the print volume would be 10.

The print volume is tracked for each user.

Setting Items

Item	Explanation	Setting
Machine action when limit is reached	Specify whether to limit print volume and the method for limiting prints. • Stop Job When the maximum print volume is reached, both the current job and waiting jobs are canceled. • Finish Job and Limit When the maximum print volume is reached, the current job is allowed to finish, but waiting jobs are canceled. • Allow Continue Use Print volume is not limited.	• Stop Job • Finish Job and Limit • **Allow Continue Use** (Default setting)
Print Volume Use Limitation: Unit Count Setting	For each of the print conditions, specify a per-page unit count between 0 and 200. A print condition is a combination of paper size and function. The default per-page unit count for every print condition is 1. The paper size "Others" refers to paper sizes other than A3 and DLT (11 × 17 in).	**When using Type 1, 2, or 3** • Copier:A3/DLT • Printer:A3/DLT • Copier:Others • Printer:Others **When using Type 4 or 5** • Printer:A3/DLT • Printer:Others

Things to note when limiting print volume

If the following occurs, the user will not be able to print:

- The login user name or user code registered in the Address Book is changed while the user is logged in and authenticated.

If the following occurs, print volume management will not function correctly:

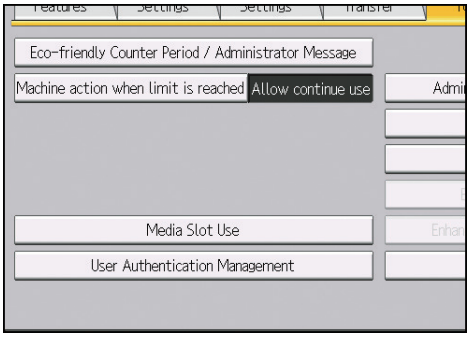
- Under Windows or LDAP authentication, a user logs in to the same user account by using multiple login user names, and these multiple login names are registered in the Address Book as separate users.

The following operations are exempt from print volume limitation:

- Printing from an operating system that does not support the current authentication method

Specifying Limitations for Print Volume

1. **Log in as the machine administrator from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **When using Type 1, 2, or 3, press [▼Next].**
5. **Press [Machine action when limit is reached].**

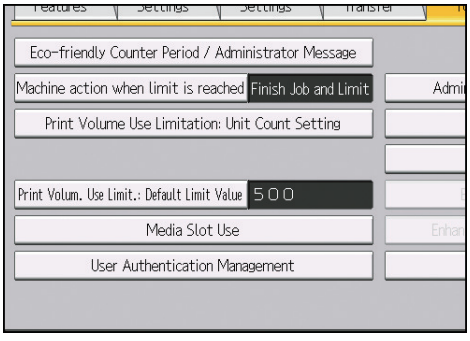


6. **Select [Stop Job] or [Finish Job and Limit], and then press [OK].**

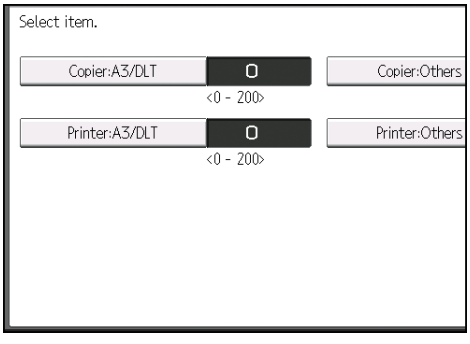
   If you do not want to limit print volume, select [Allow Continue Use].

7. **When using Type 4 or 5, press [▼Next].**

8. **Press [Print Volume Use Limitation: Unit Count Setting].**



9. **For each print condition, use the number keys to enter a per-page unit count between "0" and "200", and then press [#].**



If you specify "0" for a print condition, no volume restriction is applied to jobs matching that condition.

10. **Press [OK].**
11. **Log out.**

Note

- Limitations for print volume can also be specified in [Print Volume Use Limitation] under "Configuration" in Web Image Monitor.

Restrictions When User Code Authentication is Enabled

When User Code authentication is enabled, the following restrictions apply to the print volume limitation settings:

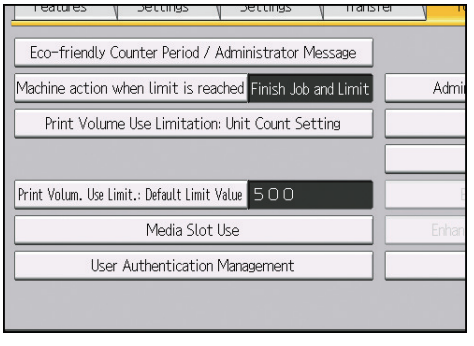
- If [PC Control] is selected for the printer function, the values specified for print volume use units might not be applied to users' print counters. Do not select [PC Control] if you want to limit print volume when running User Code authentication.
- Under Basic, Windows, and LDAP authentication, figures displayed on the lower left of the control panel show users how many of the total prints allotted to them by the administrator they have used.

Under User Code authentication, users cannot check the print volume they have made, using either the control panel or Web Image Monitor. Under User Code authentication, administrators can inform users of the print volume they have made.

- Log information related to print use limitations is not recorded in the Job Log or Access Log.
- Depending on the settings configured for User Code authentication, users might be able to make prints before logging in, regardless of the print volume limitation set by the administrator. Restrict all functions via "Functions to Restrict" in [User Code Auth.] in [User Authentication Management].

Specifying the Default Maximum Use Count

1. **Log in as the machine administrator from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼Next].**
5. **Press [Print Volum. Use Limit.: Default Limit Value].**



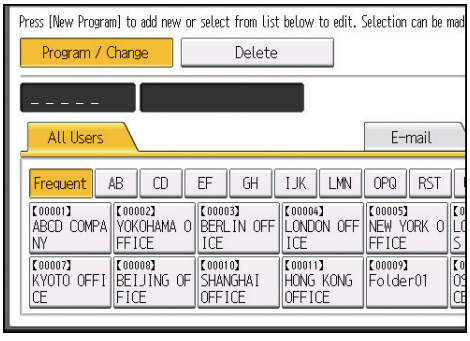
[Print Volum. Use Limit.: Default Limit Value] does not appear if you have selected [Allow Continue Use] in "Machine action when limit is reached".

6. **Use the number keys to enter a value between "0" and "999,999" as the maximum available print volume, and then press [#].**
7. **Press [OK].**
8. **Log out.**

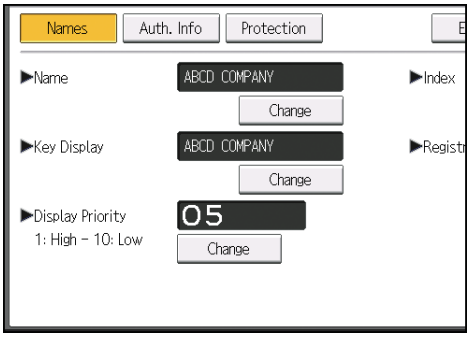
Specifying the Maximum Use Count per User

1. **Log in as the machine administrator from the control panel.**
2. **Press [Address Book Mangmnt].**

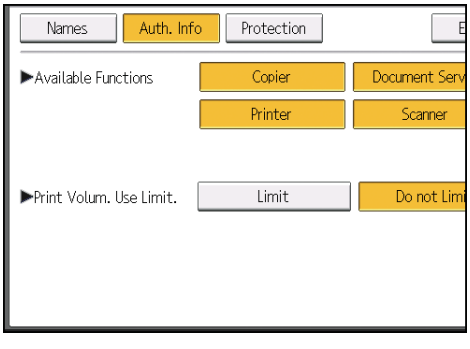
3. **Select the user whose maximum available print volume you want to specify.**



4. **Press [Auth. Info].**



5. **When using Type 1, 2, or 3, press [▼Next] twice. When using Type 4 or 5, press [▼Next].**
6. **Press [Limit] in "Print Volum. Use Limit.".**



"Print Volum. Use Limit." does not appear if you have selected [Allow Continue Use] in "Machine action when limit is reached".

If you do not want to limit user's print volume, press [Do not Limit].

7. **Press [Change], and then use the number keys to enter a value between "0" and "999,999" as the maximum available print volume, and then press [#].**

A user whose maximum print volume is set to "0" can only print jobs whose print conditions match those with a unit value of "0".

8. **Press [OK].**
9. **Log out.**

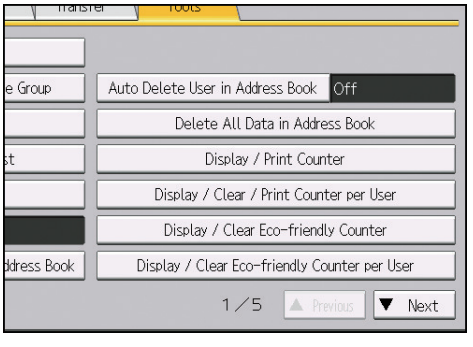
Note

- The maximum print volume for an individual user can also be specified in [Address Book] in Web Image Monitor.

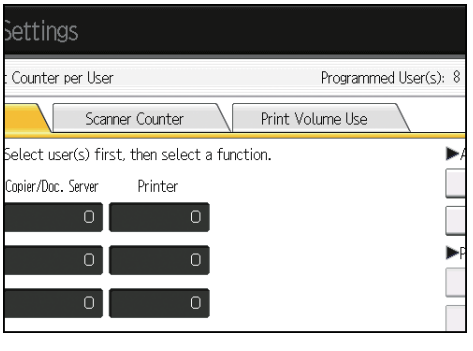
Checking Print Volume per User

This procedure can be done by any administrator.

1. **Log in as the administrator from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [Display / Clear / Print Counter per User].**



5. **Press [Print Volume Use].**



Each user's print volume limit and print volume used to date are displayed.

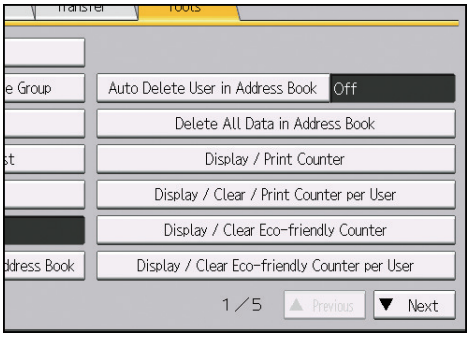
6. **After confirming the settings, log out.**

Note

- Authorized users and the user administrator can also use [Address Book] in Web Image Monitor to check users' print volume use counters.

Printing a List of Print Volume Use Counters

1. **Log in as the machine administrator from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [Display / Clear / Print Counter per User].**

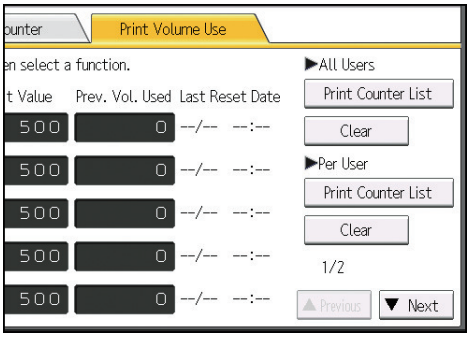


5. **Press [Print Volume Use].**

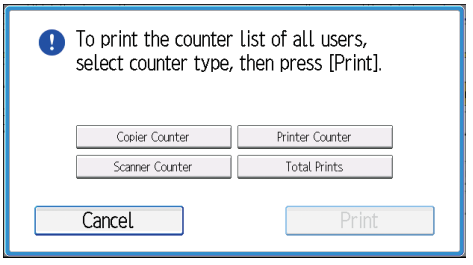
   A list of users' print volume use counters is displayed.

   To select all the users displayed on the page, press [Select All on the Page].

6. **To print a list of the volume use counters of every user, press [Print Counter List] under "All Users". To print a list of the volume use counters of selected users only, select the users whose counters you want to print, and then press [Print Counter List] under "Per User".**



7. **Select the counter you want to print in the list, and then press [Print].**



8. **Log out.**

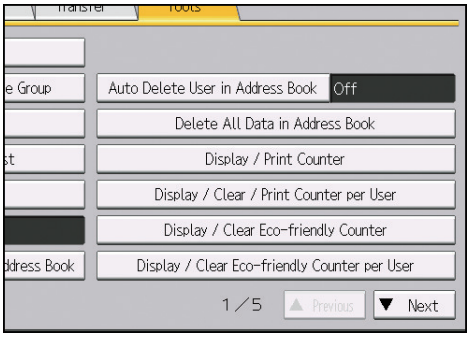
Note

- Print volume use counter lists can be printed only if the following paper sizes is loaded in the paper tray: A4, 8 $^{1}/_{2}$ × 11 in, B4, 8 $^{1}/_{2}$ × 14 in, A3, or 11 × 17 in.

Clearing Print Volume Use Counters

Clearing a user's print volume counter or increasing a user's print volume limit allows the user to continue printing beyond his/her original print volume limit.

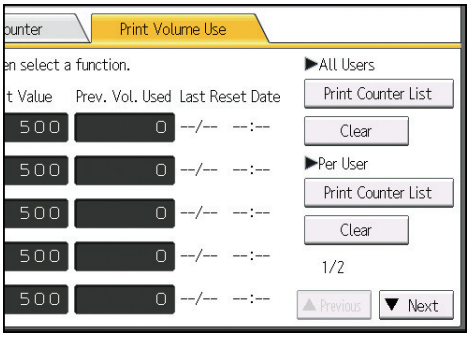
1. **Log in as the user administrator from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [Display / Clear / Print Counter per User].**



5. **Press [Print Volume Use].**

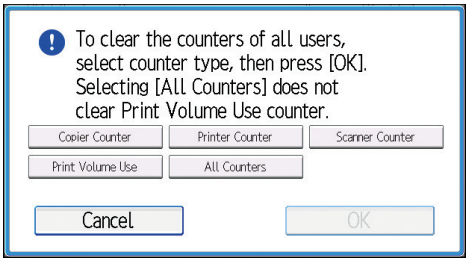
   A list of users' print volume use counters is displayed.

6. **To clear the print volume use counters of every user, press [Clear] under "All Users". To clear the print volume use counters of selected users only, select the users whose counters you want to clear, and then press [Clear] under "Per User".**



To select all the users displayed on the page, press [Select All on the Page].

7. **Select [Print Volume Use], and then press [OK].**



8. **Log out.**

Note

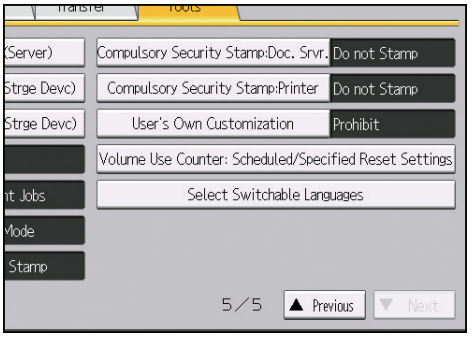
- You can also use [Address Book] in Web Image Monitor to clear the print volume use counters. However if you want to clear the print volume use counters of all users simultaneously, use the control panel.

Configuring the Auto-Reset Function

The print volume counter can be reset at a specified time.

Options	Details
Every Month	Resets the print volume at the specified time/date each month.
Specify Date	Resets the print volume (only once) at the specified time/date.
Specify Cycle	Resets after the specified interval from a reference date, then resets thereafter at the same interval.

1. **Log in as the machine administrator from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **When using Type 1, 2, or 3, press [▼Next] four times. When using Type 4 or 5, press [▼Next] three times.**
5. **Press [Volume Use Counter: Scheduled/Specified Reset Settings].**



6. **Select one of [Every Month], [Specify Date] and [Specify Cycle].**
7. **Configure the conditions.**
8. **Press [OK].**
9. **Log out.**

Note

- If the machine is turned off at the specified time on the specified date, the print volume will be reset when the power is turned on.
- If you select in [Every Month] a date, such as the 31st, which is missing on some months, the print volume will be reset at 0:00 on the 1st of the month following such a month.

4. Preventing Leakage of Information from Machines

This chapter explains how to protect information if it is stored in the machine's memory or on the hard disk.

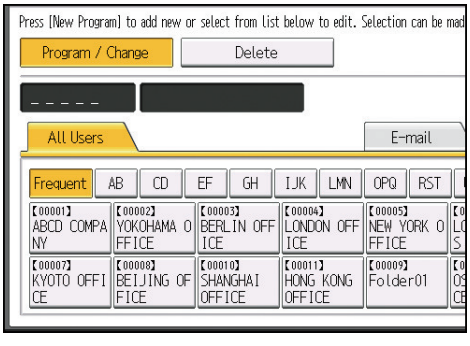
Protecting the Address Book

You can specify who is allowed to access the data in the Address Book. To protect the data from unauthorized reading, you can also encrypt the data in the Address Book.

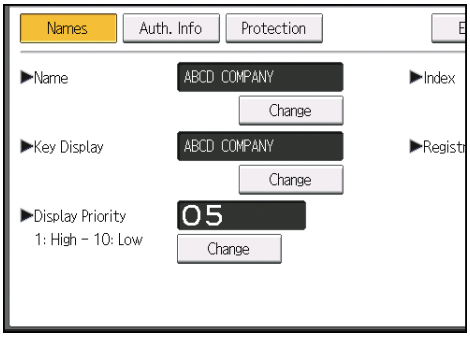
Specifying Address Book Access Permissions

These access permissions can be specified by the users registered in the Address Book, users with full control privileges, and user administrator.

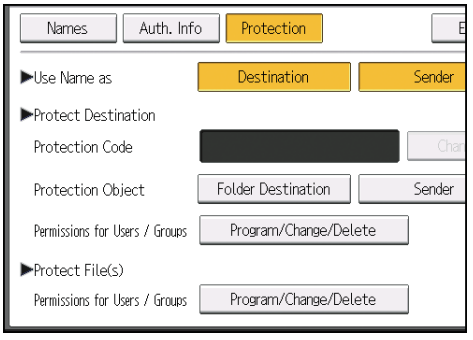
1. **Log in as the user administrator from the control panel.**
2. **Press [Address Book Mangmnt].**
3. **Select the user whose access permission you want to change.**



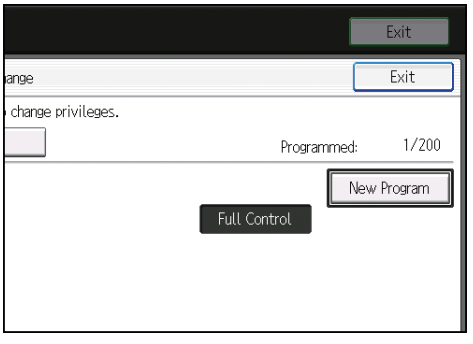
4. **Press [Protection].**



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



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



7. **Select the users or groups to which to apply the access 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 permission, from [Read-only], [Edit], [Edit / Delete], or [Full Control].

10. **Press [Exit].**
11. **Press [OK].**
12. **Log out.**

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.

Encrypting Data in the Address Book

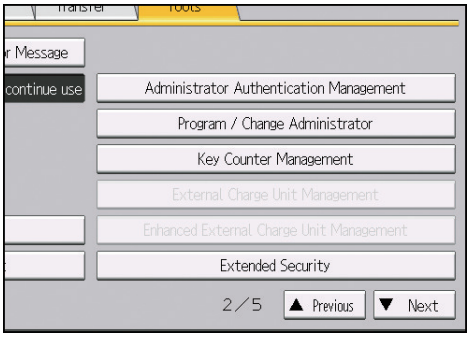
Important

- **The machine cannot be used during encryption.**

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

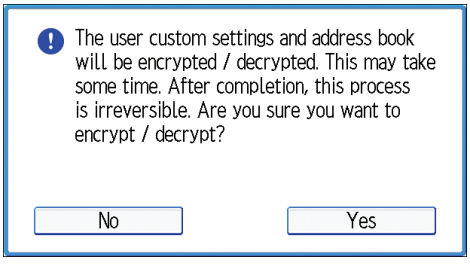
Encrypting the data in the Address Book may take a long time.

1. **Log in as the user administrator from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼Next].**
5. **Press [Extended Security].**



6. **Press [On] for "Encrypt User Custom Settings & Address Book".**
7. **Press [Change] for "Encryption Key".**
8. **Enter the encryption key, and then press [OK].**

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



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

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

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

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

11. **Press [Exit].**
12. **Press [OK].**
13. **Log out.**

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", Connecting the Machine/ System Settings.

Encrypting Data on the Hard Disk

⚠CAUTION

- Keep SD cards or USB flash memory devices out of reach of children. If a child accidentally swallows an SD card or USB flash memory device, consult a doctor immediately.

Prevent information leakage by encrypting the Address Book, authentication information, and stored documents as the data is written.

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.

You can use the copy function and Document Server function on Type 1, 2, or 3 machines only.

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

Note

- If the machine needs to be replaced, the existing data can be transferred to a new machine, even if the data is encrypted. To transfer data, contact your service representative.
- You can back up the machine's data encryption key to an SD card. For details about SD card handling, see "Inserting/Removing a Memory Storage Device", Getting Started.

Time required for encryption

When setting up encryption, specify whether to start encryption after deleting data (initialize) or encrypt existing data and retain it. If data is retained, it may take some time to encrypt it.

Setting	Data to be kept	Data to be initialized	Required time
File System Data Only	• Embedded Software Architecture applications' program/log • Address Book • Registered fonts • Job logs/access logs • Thumbnails of stored documents • Sent/received e-mail • Documents forwarded to the capture server • Spooled jobs	• Stored documents (stored documents in Document Server, Locked Print files / Sample Print files / Stored Print files / Hold Print files • Registered stamps	Approx. 1 hour 45 minutes
All Data	All Data: Both the data to be kept and data not kept when [File System Data Only] is specified	None	Approx. 4 hours 30 minutes
Format All Data	None	All Data: Both the data to be kept and data not kept when [File System Data Only] is specified	Several minutes

Things to note when enabling encryption settings

- If you use Embedded Software Architecture application or App2Me, be sure to specify [File System Data Only] or [All Data].
- Note that the machine's settings will not be initialized to their system defaults even if [Format All Data], [File System Data Only], or [All Data] is specified.

Enabling the Encryption Settings

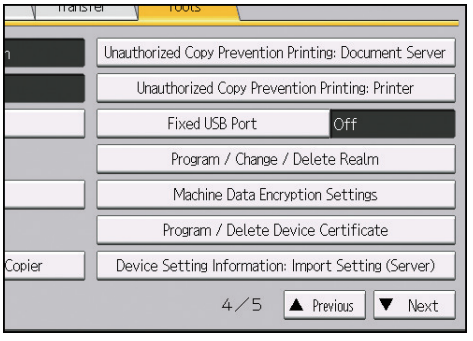
Important

- **The machine cannot be operated while data is being encrypted.**

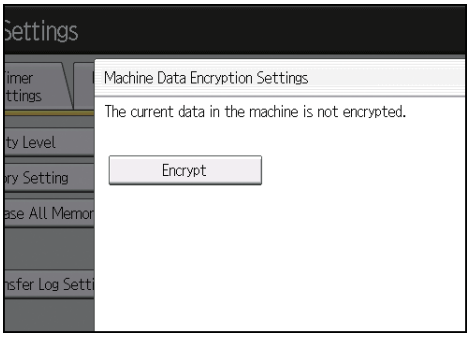
- Once the encryption process begins, it cannot be stopped. Make sure that the machine's main power is not turned off while the encryption process is in progress. If the machine's main power is turned off while the encryption process is in progress, the hard disk will be damaged and all data on it will be unusable.
- The encryption key is required for data recovery if the machine malfunctions. Be sure to store the encryption key safely for retrieving backup data.
- Encryption begins after you have completed the control panel procedure and rebooted the machine by turning off and on the main power switch. If 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 use hard disk erase-by-overwrite and encryption simultaneously, and select overwrite three times for "Random Numbers", the process will take the following amount of time. Re-encrypting from an already encrypted state takes the same amount of time.
  - When using Type 1, 2, or 3: Up to 10 hours 15 minutes
  - When using Type 4 or 5: Up to 11 hours 30 minutes
- 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. Log in as the machine administrator from the control panel.
2. Press [System Settings].
3. Press [Administrator Tools].
4. When using Type 1, 2, or 3, press [▼Next] three times. When using Type 4 or 5, press [▼Next] twice.

5. **Press [Machine Data Encryption Settings].**



6. **Press [Encrypt].**



7. **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].

8. **Select the backup method.**

   If you have selected [Save to SD Card], load an SD card into the media slot on the side of the control panel and press [OK] to back up the machine's data encryption key.

   For details about inserting the SD card, see "Inserting/Removing a Memory Storage Device", Getting Started.

   If you have selected [Print on Paper], press the [Start] key and print out the machine's data encryption key.

9. **Press [OK].**
10. **Press [Exit].**
11. **Press [Exit].**
12. **Log out.**

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

    The machine will start to convert the data on the memory after you turn on the machine. Wait until the message "Memory conversion complete. Turn the main power switch off." appears, and then turn the main power switches off again.

    For details about turning off the main power, see "Turning On/Off the Power", Getting Started.

Backing Up the Encryption Key

The encryption key can be backed up. Select whether to save it to an SD card or to print it.

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.**

1. **Log in as the machine administrator from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **When using Type 1, 2, or 3, press [▼Next] three times. When using Type 4 or 5, press [▼Next] twice.**
5. **Press [Machine Data Encryption Settings].**
6. **Press [Back Up Encryption Key].**
7. **Select the backup method.**

   If you have selected [Save to SD Card], load an SD card into the media slot on the side of the control panel and press [OK]; once the machine's data encryption key is backed up, press [Exit].

   For details about inserting the SD card, see "Inserting/Removing a Memory Storage Device", Getting Started.

   If you have selected [Print on Paper], press the [Start] key and print out the machine's data encryption key.
8. **Press [Exit].**
9. **Log out.**

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 main 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.**
- **If the encryption key update was not completed, the printed encryption key will not be valid.**

1. **Log in as the machine administrator from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **When using Type 1, 2, or 3, press [▼Next] three times. When using Type 4 or 5, press [▼Next] twice.**
5. **Press [Machine Data Encryption Settings].**
6. **Press [Update Encryption Key].**
7. **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].
8. **Select the backup method.**

   If you have selected [Save to SD Card], load an SD card into the media slot on the side of the control panel and press [OK] to back up the machine's data encryption key.

   For details about inserting the SD card, see "Inserting/Removing a Memory Storage Device", Getting Started.

   If you have selected [Print on Paper], press the [Start] key and print out the machine's data encryption key.
9. **Press [OK].**
10. **Press [Exit].**
11. **Press [Exit].**
12. **Log out.**
13. **Turn off the main power switch, and then turn the main power switch back on.**

    The machine will start to convert the data on the memory after you turn on the machine. Wait until the message "Memory conversion complete. Turn the main power switch off." appears, and then turn the main power switches off again.

    For details about turning off the main power, see "Turning On/Off the Power", Getting Started.

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 main 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.
- When disposing of a machine, completely erase the memory. For details on erasing all of the memory, see page 100 "Deleting Data on the Hard Disk".

1. **Log in as the machine administrator from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **When using Type 1, 2, or 3, press [▼Next] three times. When using Type 4 or 5, press [▼Next] twice.**
5. **Press [Machine Data Encryption Settings].**
6. **Press [Cancel Encryption].**
7. **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].
8. **Press [OK].**
9. **Press [Exit].**
10. **Press [Exit].**
11. **Log out.**
12. **Turn off the main power switch, and then turn the main power switch back on.**

    For details about turning off the main power, see "Turning On/Off the Power", Getting Started.

Deleting Data on the Hard Disk

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.

You can use the copy function, Document Server function, and scanner function on Type 1, 2, or 3 machines only.

Conditions for Use

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

- 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.

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 Low Power 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 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

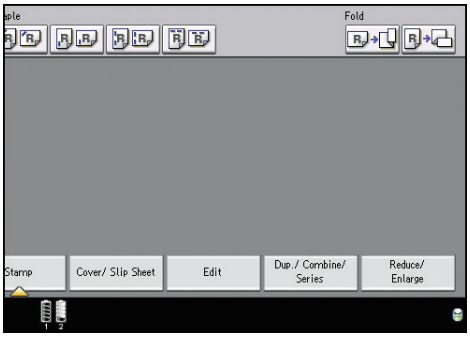
A document scanned in copier, or scanner mode, or print data sent from a printer driver is temporarily stored on the machine's hard disk. Even after the job is completed, it remains in the hard disk as temporary data. Auto Erase Memory erases the temporary data on the hard disk by writing over it.

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.



Icon	Icon name	Explanation
	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

  Each item of data is overwritten by a random number, then by its complement, then by another random number, and is then verified.

- Random Numbers

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

Note

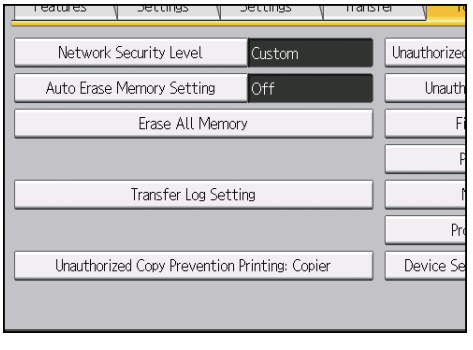
- The default method for overwriting is "Random Numbers", and the default number of overwrites is 3.
- NSA stands for "National Security Agency", U.S.A.
- DoD stands for "Department of Defense", U.S.A.

Using Auto Erase Memory

Important

- When Auto Erase Memory is set to [On], temporary data that remained on the hard disk when Auto Erase Memory was set to [Off] might not be overwritten.
- If the main power switch is turned off before Auto Erase Memory is completed, overwriting will stop and data will be left on the hard disk.
- Do not stop the overwrite mid-process. Doing so will damage the hard disk.
- Should the main power switch be turned off before Auto Erase Memory is completed, overwriting will continue once the main power switch is turned back on.
- If an error occurs before overwriting is completed, turn off the main power. Turn it on, and then repeat from step 1.

1. Log in as the machine administrator from the control panel.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [▼Next] three times.
5. Press [Auto Erase Memory Setting].



6. Press [On].

7. **Select the method of overwriting.**

   If you select [NSA] or [DoD], proceed to step 10.

   If you select [Random Numbers], proceed to step 8.

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

    Auto Erase Memory is set.

11. **Log out.**

Note

- If you enable both overwriting and data encryption, the overwriting data will also be encrypted.

Canceling Auto Erase Memory

1. **Log in as the machine administrator from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼Next] three times.**
5. **Press [Auto Erase Memory Setting].**
6. **Press [Off].**
7. **Press [OK].**

   Auto Erase Memory is disabled.

8. **Log out.**

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

Scanner

- Scanned files sent by e-mail
- Files sent by Scan to Folder
- Documents sent using Web Image Monitor
- Network TWAIN scanner

  Data scanned with the network TWAIN scanner when the TWAIN driver's "ADF(Read-ahead)" function is checked will be overwritten by Auto Erase Memory. Data scanned when the "ADF(Read-ahead)" function is not checked will not be overwritten.

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 page 89 "Protecting the Address Book".
- Counters stored under each user code

Erase All Memory

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

The following data will also be erased by Erase All Memory. For details about using the machine after executing Erase All Memory, contact your sales representative.

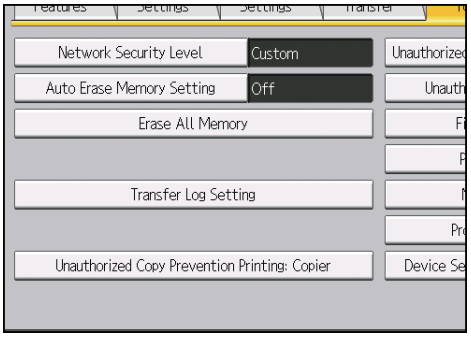
- User codes
- Counters under each user code
- User stamps
- Data stored in the Address Book
- Printer fonts downloaded by users
- Applications using Embedded Software Architecture
- SSL server certificates
- Machine's network settings

Important

- 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 Device Manager NX Lite 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 Device Manager NX Lite Help or Web Image Monitor Help.
- The only operation possible during the "Erase All Memory" process is pausing. If "Random Numbers" is selected and overwrite three times is set, the "Erase All Memory" process takes the following amount of time:
  - When using Type 1, 2, or 3: Up to 3 hours 45 minutes
  - When using Type 4 or 5: Up to 7 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. Log in as the machine administrator from the control panel.
3. Press [System Settings].
4. Press [Administrator Tools].
5. Press [▼Next] three times.
6. Press [Erase All Memory].

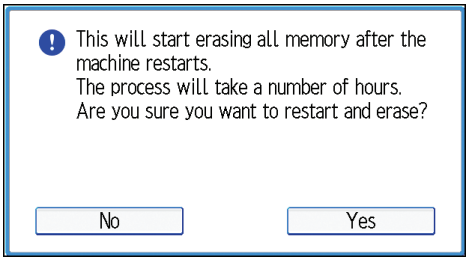


7. Select the method of overwriting.

   If you select [NSA] or [DoD], proceed to step 10.

   If you select [Random Numbers], proceed to step 8.

8. **Press [Change].**
9. **Enter the number of times that you want to overwrite using the number keys, and then press [#].**
10. **Press [Erase].**
11. **Press [Yes].**



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

    For details about turning off the main power, see "Turning On/Off the Power", Getting Started.

Note

- Should the main power switch be turned off before "Erase All Memory" is completed, overwriting will start over when 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.

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.**

   For details about turning off the main power, see "Turning On/Off the Power", Getting Started.

Note

- To resume overwriting, turn on the main power.

5. Enhanced Network Security

This chapter describes the functions for enhancing security when the machine is connected to the network.

Access Control

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].

You can use the scanner function on Type 1, 2, or 3 machines only.

Important

- **Using access control, you can limit access involving LPR, RCP/RSH, FTP, ssh/sftp, Bonjour, SMB, WSD (Device), WSD (Printer), WSD (Scanner)/DSM, IPP, DIPRINT, RHPP or Web Image Monitor. You cannot limit access involving telnet, or Device Manager NX Lite, when using the SNMPv1 monitoring.**

1. **Log in as the network administrator from Web Image Monitor.**
2. **Point to [Device Management], and then click [Configuration].**
3. **Click [Access Control] under "Security".**
4. **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".
5. **Click [OK].**
6. **"Updating..." appears. Wait for about one or two minutes, and then click [OK].**

   If the previous screen does not reappear after you click [OK], wait for a while, and then click the web browser's refresh button.
7. **Log out.**

Enabling and Disabling Protocols

Specify whether to enable or disable the function for each protocol. By making this setting, you can specify which protocols are available and so prevent unauthorized access over the network. Network settings can be specified on the control panel or by using Web Image Monitor, telnet or Device Manager NX Lite. In the case of Device Manager NX Lite, use it to start Web Image Monitor and configure the settings from there.

You can use the scanner function and network TWAIN function on Type 1, 2, or 3 machines only.

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

Protocol	Port	Setting method	When disabled
ssh/sftp	TCP:22	• Web Image Monitor • telnet • Device Manager NX Lite	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 • Device Manager NX Lite	Commands using telnet are disabled.
SMTP	TCP:25 (variable)	• Control panel • Web Image Monitor • Device Manager NX Lite	E-mail notification functions that require SMTP reception cannot be used.
HTTP	TCP:80	• Web Image Monitor • telnet • Device Manager NX Lite	Functions that require HTTP cannot be used. Cannot print using IPP on port 80.
HTTPS	TCP:443	• Web Image Monitor • telnet • Device Manager NX Lite	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 • Device Manager NX Lite	SMB printing functions cannot be used.

Protocol	Port	Setting method	When disabled
NBT	UDP:137 UDP:138	• telnet	SMB printing functions via TCP/IP, as well as NetBIOS designated functions on the WINS server cannot be used.
SNMPv1,v2	UDP:161	• Web Image Monitor • telnet • Device Manager NX Lite	Functions that require SNMPv1, v2 cannot be used. Using the control panel, Web Image Monitor or telnet, you can specify that SNMPv1, v2 settings are read-only, and cannot be edited.
SNMPv3	UDP:161	• Web Image Monitor • telnet • Device Manager NX Lite	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 • Device Manager NX Lite	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 • Device Manager NX Lite	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 • Device Manager NX Lite	IPP functions cannot be used.
SSDP	UDP:1900	• Web Image Monitor • telnet • Device Manager NX Lite	Device discovery using UPnP from Windows cannot be used.
Bonjour	UDP:5353	• Web Image Monitor • telnet • Device Manager NX Lite	Bonjour functions cannot be used.
@Remote	TCP:7443 TCP:7444	• Control panel • telnet	@Remote cannot be used.
DIPRINT	TCP:9100	• Web Image Monitor • telnet • Device Manager NX Lite	DIPRINT functions cannot be used.
RFU	TCP:10021	• Control panel • telnet	You can attempt to update firmware via FTP.
WSD (Device)	TCP:53000 (variable)	• Web Image Monitor • telnet • Device Manager NX Lite	WSD (Device) functions cannot be used.
WSD (Printer)	TCP:53001 (variable)	• Web Image Monitor • telnet • Device Manager NX Lite	WSD (Printer) functions cannot be used.

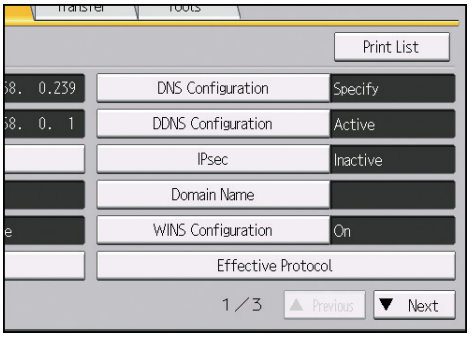
Protocol	Port	Setting method	When disabled
WSD (Scanner)/DSM	TCP-53002 (variable)	• Web Image Monitor • telnet • Device Manager NX Lite	WSD (Scanner) and DSM functions cannot be used.
WS-Discovery	UDP/TCP: 3702	• telnet	WSD (Device, Printer, Scanner) search function cannot be used.
RHPP	TCP:59100	• Web Image Monitor • telnet • Device Manager NX Lite	Cannot print with RHPP.
LLTD	-	• telnet	Device search function using LLTD cannot be used.
LLMNR	UDP:5355	• Web Image Monitor • telnet	Name resolution requests using LLMNR cannot be respond.

Note

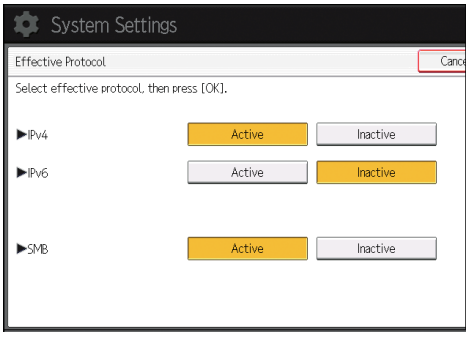
- "Restrict Display of User Information" is one of the Extended Security features. For details about making this setting, see page 243 "Specifying the Extended Security Functions".

Enabling and Disabling Protocols Using the Control Panel

1. **Log in as the network administrator from the control panel.**
2. **Press [System Settings].**
3. **Press [Interface Settings].**
4. **Press [Effective Protocol].**



5. Set the desired protocols to active/inactive.



6. Press [OK].
7. Log out.

Enabling and Disabling Protocols Using Web Image Monitor

1. Log in as the network administrator from Web Image Monitor.
2. Point to [Device Management], and then click [Configuration].
3. Click [Network Security] under "Security".
4. Set the desired protocols to active/inactive (or open/close).
5. Click [OK].
6. "Updating..." appears. Wait for about one or two minutes, and then click [OK].

   If the previous screen does not reappear after you click [OK], wait for a while, and then click the web browser's refresh button.
7. Log out.

Specifying Network Security Level

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.

You can use the scanner function and S/MIME on Type 1, 2, or 3 machines only.

Important

- **With some utilities, communication or login may fail depending on the network security level.**

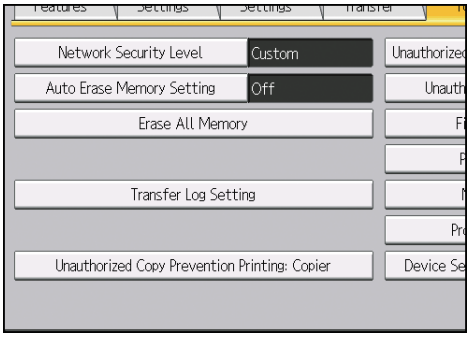
Network Security Levels

Security Level	Description
[Level 0]	Select [Level 0] to use all features. Use this setting when you have no information that needs to be protected from external threats.
[Level 1]	Select [Level 1] for moderate security to protect important information. Use this setting if the machine is connected to a local area network (LAN).
[FIPS140]	Provides a security strength intermediate between [Level 1] and [Level 2]. You can only use codes recommended by the U.S. government as its coding/authentication algorithm. Settings other than the algorithm are the same as [Level 2].
[Level 2]	Select [Level 2] for maximum security to protect confidential information. Use this setting when it is necessary to protect information from external threats.
[Custom]	For configurations other than the levels above. Configure using Web Image Monitor.

Specifying Network Security Level Using the Control Panel

1. **Log in as the network administrator from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼Next] three times.**

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



6. **Select the network security level.**

   Select [Level 0], [Level 1], [Level 2], or [FIPS140].

7. **Press [OK].**

8. **Log out.**

Specifying Network Security Level Using Web Image Monitor

1. **Log in as the network administrator from Web Image Monitor.**
2. **Point to [Device Management], and then click [Configuration].**
3. **Click [Network Security] under "Security".**
4. **Select the network security level in "Security Level".**
5. **Click [OK].**
6. **"Updating..." appears. Wait for about one or two minutes, and then click [OK].**

   If the previous screen does not reappear after you click [OK], wait for a while, and then click the web browser's refresh button.

7. **Log out.**

Status of Functions under Each Network Security Level

TCP/IP

Function	Level 0	Level 1	FIPS 140	Level 2
TCP/IP	Active	Active	Active	Active
HTTP > Port 80	Open	Open	Open	Open
IPP > Port 80	Open	Open	Open	Open

Function	Level 0	Level 1	FIPS 140	Level 2
IPP > Port 631	Open	Open	Close	Close
SSL/TLS > Port 443	Open	Open	Open	Open
SSL/TLS > Permit SSL/TLS Communication	Ciphertext Priority	Ciphertext Priority	Ciphertext Only	Ciphertext Only
SSL/TLS Version > TLS1.2	Active	Active	Active	Active
SSL/TLS Version > TLS1.1	Active	Active	Active	Active
SSL/TLS Version > TLS1.0	Active	Active	Active	Active
SSL/TLS Version > SSL3.0	Active	Inactive	Inactive	Inactive
Encryption Strength Setting > AES	128bit/ 256bit	128bit/ 256bit	128bit/ 256bit	128bit/ 256bit
Encryption Strength Setting > 3DES	168bit	168bit	168bit	-
Encryption Strength Setting > RC4	-	-	-	-
DIPRINT	Active	Active	Inactive	Inactive
LPR	Active	Active	Inactive	Inactive
FTP	Active	Active	Active	Active
sftp	Active	Active	Active	Active
ssh	Active	Active	Active	Active
RSH/RCP	Active	Active	Inactive	Inactive
TELNET	Active	Inactive	Inactive	Inactive
Bonjour	Active	Active	Inactive	Inactive
SSDP	Active	Active	Inactive	Inactive
SMB	Active	Active	Inactive	Inactive
NetBIOS over TCP/IPv4	Active	Active	Inactive	Inactive
WSD (Device)	Active	Active	Active	Active
WSD (Printer)	Active	Active	Active	Active

Function	Level 0	Level 1	FIPS 140	Level 2
WSD (Scanner)/DSM	Active	Active	Active	Active
WSD (Encrypted Communication of Device)	Inactive	Inactive	Active	Active
RHPP	Active	Active	Inactive	Inactive

The same settings are applied to IPv4 and IPv6.

TCP/IP setting is not governed by the security level. Manually specify whether to activate or inactivate this setting.

SNMP

Function	Level 0	Level 1	FIPS 140	Level 2
SNMP	Active	Active	Active	Active
Permit Settings by SNMPv1 and v2	On	Off	Off	Off
SNMPv1,v2 Function	Active	Active	Inactive	Inactive
SNMPv3 Function	Active	Active	Active	Active
Permit SNMPv3 Communication	Encryption/ Cleartext	Encryption/ Cleartext	Encryption Only	Encryption Only

TCP/IP Encryption Strength Setting

Function	Level 0	Level 1	FIPS 140	Level 2
ssh > Encryption Algorithm	DES/3DES/ AES-128/ AES-192/ AES-256/ Blowfish/ Arcfour	3DES/ AES-128/ AES-192/ AES-256/ Arcfour	3DES/ AES-128/ AES-192/ AES-256	3DES/ AES-128/ AES-192/ AES-256
S/MIME > Encryption Algorithm	3DES-168 bit	3DES-168 bit	3DES-168 bit	AES-256 bit
S/MIME > Digest Algorithm	SHA1	SHA1	SHA1	SHA-256 bit

Function	Level 0	Level 1	FIPS 140	Level 2
SNMPv3 > Authentication Algorithm	MD5	SHA1	SHA1	SHA1
SNMPv3 > Encryption Algorithm	DES	DES	AES-128	AES-128
Kerberos Authentication > Encryption Algorithm	AES256-CTS-HMAC-SHA1-96/ AES128-CTS-HMAC-SHA1-96/ DES3-CBC-SHA1/RC4-HMAC/DES-CBC-MD5	AES256-CTS-HMAC-SHA1-96/ AES128-CTS-HMAC-SHA1-96/ DES3-CBC-SHA1/RC4-HMAC	AES256-CTS-HMAC-SHA1-96/ AES128-CTS-HMAC-SHA1-96/ DES3-CBC-SHA1	AES256-CTS-HMAC-SHA1-96/ AES128-CTS-HMAC-SHA1-96
Driver Encryption Key > Encryption Strength	Simple Encryption	DES	AES	AES

Protecting the Communication Path via a Device Certificate

This machine can protect its communication path and establish encrypted communications using SSL/TLS, IPsec, S/MIME, or IEEE 802.1X. It can also protect PDFs by means of a PDF or PDF/A digital signature.

To use these functions, it is necessary to create and install a device certificate for the machine in advance.

The following types of device certificate can be used:

- Self-signed certificate created by the machine
- Certificate issued by a certificate authority

You can use S/MIME, PDF Digital Signature, and PDF/A Digital Signature on Type 1, 2, or 3 machines only.

Important

- **The administrator is required to manage the expiration of certificates and renew the certificates before they expire.**
- **The administrator is required to check that the issuer of the certificate is valid.**

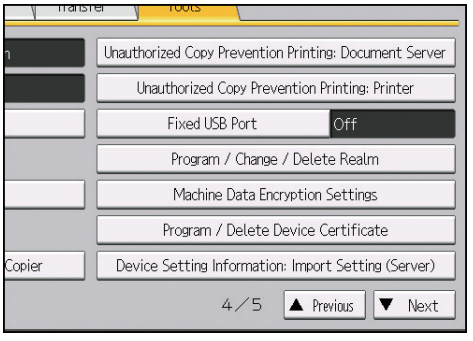
Creating and Installing a Device Certificate from the Control Panel (Self-Signed Certificate)

Create and install the device certificate using control panel.

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

1. **Log in as the network administrator from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼Next] three times.**

5. **Press [Program / Delete Device Certificate].**



6. **Check that [Program] is selected.**
7. **Press [Certificate 1].**

   Only [Certificate 1] can be created from the control panel.

8. **Make the necessary settings.**

   To use the device certificate for S/MIME, PDF Digital Signature, or PDF/A Digital Signature, enter the machine's administrator's e-mail address in the e-mail address setting.

9. **Press [OK].**

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

10. **Log out.**

Note

- Select [Delete] to delete the device certificate from the machine.
- To use the device certificate created on the machine for S/MIME or PDF/A Digital Signature, set "Certification" in Web Image Monitor to [Certificate 1].

Creating and Installing a Device Certificate from Web Image Monitor (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. **Log in as the network administrator from Web Image Monitor.**
2. **Point to [Device Management], and then click [Configuration].**
3. **Click [Device Certificate] under "Security".**

4. **Check the radio button next to the number of the certificate you want to create.**

   To use SSL/TLS, select [Certificate 1]. To use any other protocol, select the certificate number desired.

5. **Click [Create].**

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

6. **Make the necessary settings.**

   To use the device certificate for S/MIME, PDF Digital Signature, or PDF/A Digital Signature, enter the machine's administrator's e-mail address in the e-mail address setting.

7. **Click [OK].**

   The setting is changed.

8. **Click [OK].**

9. **If a security warning message appears, check the details, and then select "Continue to this website".**

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

10. **Log out.**

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. **Log in as the network administrator from Web Image Monitor.**
2. **Point to [Device Management], and then click [Configuration].**
3. **Click [Device Certificate] under "Security".**
4. **Check the radio button next to the number of the certificate you want to create.**

   To use SSL/TLS, select [Certificate 1]. To use any other protocol, select the certificate number desired.

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

   The setting is changed.

8. **Click [OK].**

   "Requesting" appears for "Certificate Status".

9. **Log out.**

10. **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.
- Web Image Monitor can be used for creating the device certificate but not for requesting the certificate to the certificate authority.
- 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.

1. **Log in as the network administrator from Web Image Monitor.**
2. **Point to [Device Management], and then click [Configuration].**
3. **Click [Device Certificate] under "Security".**
4. **Check the radio button next to the number of the certificate you want to install.**

    To use SSL/TLS, select [Certificate 1]. To use any other protocol, select the certificate number desired.
5. **Click [Install].**
6. **Enter the contents of the device certificate.**

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

    If you are installing an intermediate certificate, enter the contents of the intermediate certificate also.

    For details about the displayed items and selectable items, see Web Image Monitor Help.
7. **Click [OK].**
8. **Wait for about one or two minutes, and then click [OK].**

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

Installing an Intermediate Certificate (Issued by a Certificate Authority)

This section explains how to use Web Image Monitor to install an intermediate certificate issued by a certificate authority.

If you do not have the intermediate certificate issued by the certificate authority, a warning message will appear during communication. If the certificate authority has issued an intermediate certificate, we recommend installing the intermediate certificate.

1. **Log in as the network administrator from Web Image Monitor.**
2. **Point to [Device Management], and then click [Configuration].**
3. **Click [Device Certificate] under "Security".**
4. **Check the radio button next to the number of the certificate you want to install.**
5. **Click [Install Intermediate Certificate].**
6. **Enter the contents of the intermediate certificate.**

   In the certificate box, enter the contents of the intermediate certificate issued by the certificate authority. For details about the items and settings of a certificate, see Web Image Monitor Help.
7. **Click [OK].**
8. **Wait for about one or two minutes, and then click [OK].**

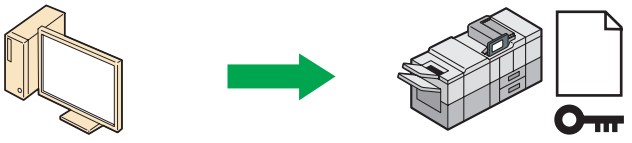
   The intermediate certificate will be installed on the device. The "Certificate Details" screen will inform you whether or not the installation of the intermediate certificate was successful. For details about the "Certificate Details" screen, see Web Image Monitor Help.
9. **Log out.**

Configuring SSL/TLS

Configuring the machine to use SSL/TLS enables encrypted communication. Doing so helps prevent data from being intercepted, cracked or tampered with during transmission.

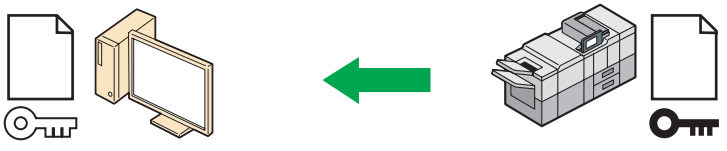
Flow of SSL/TLS encrypted communications

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



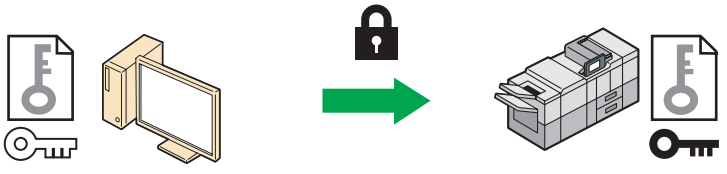
CZB002

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



CZB003

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.



CZB004

4. The shared key is used for data encryption and decryption, thus achieving secure transmission.

CZB005

Configuration flow when using a self-signed certificate

1. Creating and installing the device certificate

Create and install a device certificate from the control panel or Web Image Monitor.

2. Enabling SSL/TLS

   Enable the SSL/TLS setting using Web Image Monitor.

Configuration flow when using an authority issued certificate

1. Creating a device certificate and applying to the authority

   After creating a device certificate on Web Image Monitor, apply to the certificate authority.

   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/TLS

   Enable the SSL/TLS setting using Web Image Monitor.

Note

- To confirm whether SSL/TLS 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/TLS configuration is invalid.
- If you enable SSL/TLS for IPP (printer functions), sent data is encrypted, preventing it from being intercepted, analyzed, or tampered with.

Enabling SSL/TLS

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

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

1. **Log in as the network administrator from Web Image Monitor.**
2. **Point to [Device Management], and then click [Configuration].**
3. **Click [SSL/TLS] under "Security".**
4. **For IPv4 and IPv6, select "Active" if you want to enable SSL/TLS.**
5. **Select the encryption communication mode for "Permit SSL/TLS Communication".**
6. **If you want to disable a protocol, click [Inactive] next to "TLS1.2", "TLS1.1", "TLS1.0", or "SSL3.0".**

   At least one of these protocols must be enabled.

7. **Under "Encryption Strength Setting", specify the strength of encryption to be applied for "AES", "3DES", and/or "RC4". You must select at least one check box.**

   Note that the availability of encryption strengths will vary depending on the settings you have specified for "TLS1.2", "TLS1.1", "TLS1.0", or "SSL3.0".

8. **Click [OK].**
9. **"Updating..." appears. Wait for about one or two minutes, and then click [OK].**

   If the previous screen does not reappear after you click [OK], wait for a while, and then click the web browser's refresh button.

10. **Log out.**

Note

- If you set "Permit SSL/TLS Communication" to [Ciphertext Only], communication will not be possible if you select a protocol that does not support a Web browser, or specify an encryption strength setting only. If this is the case, enable communication by setting [Permit SSL / TLS Communication] to [Ciphertext / Cleartext] using the machine's control panel, and then specify the correct protocol and encryption strength.
- The SSL/TLS version and encryption strength settings can be changed, even under [Network Security].
- Depending on the states you specify for "TLS1.2", "TLS1.1", "TLS1.0", and "SSL3.0", the machine might not be able to connect to an external LDAP server.
- If only TLS1.2 and TLS1.1 are enabled, Integration Server authentication cannot be performed.
- The following types of communication and data are always encrypted by SSL3.0: communication via @Remote, Integration Server authentication and files sent via a delivery server.

User Setting for SSL/TLS

We recommend that after installing the self-signed certificate or device certificate from a private certificate authority on the main unit and enabling SSL/TLS (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/7/8/8.1/10, Windows Server 2008/2008 R2/2012/2012 R2. The network administrator must instruct each user to install the certificate.

Select [Trusted Root Certification Authorities] for the certificate store location when accessing the machine by IPP.

Note

- Take the appropriate steps when you receive a user's inquiry concerning problems such as an expired certificate.
- If a certificate issued by a certificate authority is installed in the machine, confirm the certificate store location with the certificate authority.

- To change the host name or IP address in [Common Name] of the device certificate when using the operating system's standard IPP port under Windows Vista/7/8/8.1/10 or Windows Server 2008/2008 R2/2012/2012 R2, delete any previously configured PC printer beforehand and re-install it after changing [Common Name]. Also, to change the user authentication settings (login user name and password), delete any previously configured PC printer beforehand and re-install it after changing the user authentication settings.

Setting the SSL/TLS Encryption Mode

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

Encrypted communication mode

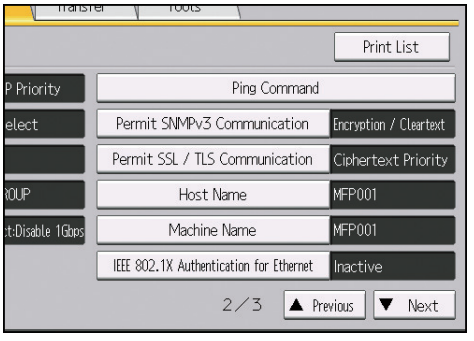
Using the encrypted communication mode, you can specify encrypted communication.

Encrypted communication mode	Description
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.

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

1. **Log in as the network administrator from the control panel.**
2. **Press [System Settings].**
3. **Press [Interface Settings].**
4. **Press [▼Next].**

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



6. **Select the encrypted communication mode.**

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

7. **Press [OK].**

8. **Log out.**

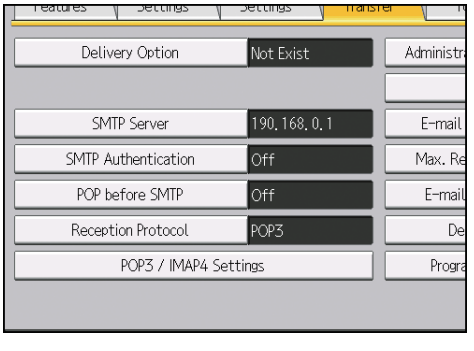
Note

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

Enabling SSL for SMTP Connections

Use the following procedure to enable SSL encryption for SMTP connections.

1. **Log in as the network administrator from the control panel.**
2. **Press [System Settings].**
3. **Press [File Transfer].**
4. **Press [SMTP Server].**



5. **In "Use Secure Connection (SSL)", press [On].**

   If you are not using SSL for SMTP connections, press [Off].

   When "Use Secure Connection (SSL)" is set to [On], the port number is changed to 465.

6. **Press [OK].**

7. **Log out.**

Configuring S/MIME

You can use the S/MIME function on Type 1, 2, or 3 machines only.

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

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

Compatible mailer applications

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

- Microsoft Outlook 98 and later
- Microsoft Outlook Express 5.5 and later
- Thunderbird 3.1.7 and later
- Lotus Notes R5 and later
- Windows Live Mail 2009 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 you send an e-mail to both users whose mail clients support S/MIME and users whose clients lack such support, the e-mail for the S/MIME clients is encrypted, but that for the non-S/MIME clients is left as plaintext.
- When using S/MIME, the e-mail size is larger than normal.
- For details about using S/MIME with the scanner function, see "Security Settings to E-mails", Scan.

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

Each user certificate must be prepared in advance.

1. **Log in as the user administrator from Web Image Monitor.**
2. **Point to [Device Management], and then click [Address Book].**
3. **Select the user for whom the certificate will be installed.**
4. **Click [Detail Input], and then click [Change].**

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

   The user certificate is installed.
9. **"Updating..." appears. Wait for about one or two minutes, and then click [OK].**

   If the previous screen does not reappear after you click [OK], wait for a while, and then click the web browser's refresh button.
10. **Log out.**

Note

- Once the valid period of the selected user certificate elapses, encrypted messages can no longer be sent. Select a certificate that is within its valid period.

Specifying the encryption algorithm

1. **Log in as the network administrator from Web Image Monitor.**
2. **Point to [Device Management], and then click [Configuration].**
3. **Click [S/MIME] under "Security".**
4. **Select the encryption algorithm from the drop-down menu next to "Encryption Algorithm" under "Encryption".**
5. **Click [OK].**

   The algorithm for S/MIME is set.
6. **Log out.**

Note

- Configure the settings taking into consideration the encryption algorithm and digest algorithm supported by the user's e-mail software.

Attaching an Electronic Signature

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

As the device certificate, you can use a self-signed certificate created by the machine or a certificate issued by a certificate authority. For details about creating and installing the device certificate, see page 119 "Protecting the Communication Path via a Device Certificate".

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.

Selecting the device certificate

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

1. **Log in as the network administrator from Web Image Monitor.**
2. **Point to [Device Management], and then click [Configuration].**
3. **Click [Device Certificate] under "Security".**
4. **Select the certificate to be used for the electronic signature from the drop-down box in "S/MIME" under "Certification".**
5. **Click [OK].**

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

6. **"Updating..." appears. Wait for about one or two minutes, and then click [OK].**

   If the previous screen does not reappear after you click [OK], wait for a while, and then click the web browser's refresh button.

7. **Log out.**

Note

- If the selected device certificate expires, signatures cannot be attached to e-mail. Select a certificate that is within its valid period.

Specifying the electronic signature

After installing a device certificate to the machine, configure the conditions for S/MIME signatures. 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. **Log in as the network administrator from Web Image Monitor.**
2. **Point to [Device Management], and then click [Configuration].**
3. **Click [S/MIME] under "Security".**

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

   The settings for the S/MIME electronic signature are enabled.
8. **Log out.**

Note

- Configure the settings taking into consideration the encryption algorithm and digest algorithm supported by the user's e-mail software.

Specifying Checking of the Certificate Valid Period

The validity period of the certificate used with S/MIME is verified when you send e-mail.

You can change the timing at which the valid period is checked.

Operation mode	Description
Security Priority	The validity period is verified at the following timings. **User Certificate** (a). When the address is selected (b). When the [Start] key is pressed **Device certificate** (c). When the first address is selected (d). When the [Start] key is pressed
Performance Priority	Performing (b) and (c) are omitted. If it takes a long time to verify the validity period when the address is selected or when the [Start] key is pressed, the time taken can be shortened by selecting "Performance Priority".

1. **Log in as the network administrator from Web Image Monitor.**
2. **Point to [Device Management], and then click [Configuration].**
3. **Click [S/MIME] under "Security".**

4. **In "Operation Mode", select [Security Priority] or [Performance Priority].**
5. **Click [OK].**
6. **Log out.**

Note

- If a certificate was valid when transmitted but has expired before retrieving the e-mail from the mail server to the client computer, the e-mail may not be retrieved.
- If an error occurs outside the validity period of the certificate when sending an S/MIME e-mail automatically, such as in the case of sending e-mail by Memory Transmission or at a specified time, the error will be reported by e-mail in plain text to the sender's or administrator's e-mail address. The error details can be viewed in the job log. When using S/MIME, be sure to enable the job log collection function. For details about viewing the logs, see page 191 "Managing Log Files".

Configuring PDFs with Electronic Signatures

You can use this function on Type 1, 2, or 3 machines only.

This machine can create PDFs with electronic signatures. PDFs with electronic signatures certify the creator of the PDF document and the date and time of creation. Tampering is also prevented as documents that have been tampered with can be detected.

In order to create PDFs with electronic signatures, first select the certificate to use for the signature from the device certificates that have been created and installed.

As the device certificate, you can use a self-signed certificate created by the machine or a certificate issued by a certificate authority. For details about creating and installing a device certificate, see page 119 "Protecting the Communication Path via a Device Certificate".

Important

- **To create digitally signed PDFs, you must first specify [Administrator's E-mail Address] in [File Transfer] in [System Settings].**
- **To use the device certificate for digitally signed PDFs, you must first specify the administrator's e-mail address so that it is the same as that registered as "Administrator's E-mail Address" in [System Settings].**

Select the certificate to use for signatures.

1. **Log in as the network administrator from Web Image Monitor.**
2. **Point to [Device Management], and then click [Configuration].**
3. **Click [Device Certificate] under "Security".**
4. **Select the certificate to be used for the electronic signature from the drop-down box in "PDF Digital Signature" or "PDF/A Digital Signature" under "Certification".**

   PDF Digital Signature: This can be attached to PDFs in formats other than PDF/A.

   PDF/A Digital Signature: This can be attached to PDFs in the PDF/A format.
5. **Click [OK].**
6. **"Updating..." appears. Wait for about one or two minutes, and then click [OK].**

   If the previous screen does not reappear after you click [OK], wait for a while, and then click the web browser's refresh button.
7. **Log out.**

Note

- If the selected device certificate expires, signatures cannot be attached to PDFs. Select a certificate that is within its valid period.
- The signature algorithm for the device certificate's digital signature that can be attached to PDF/A files is "sha1WithRSA-1024".

Configuring IPsec

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 uses automatic key exchange to configure the pre-shared key for both parties. 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 "Interface Settings", Connecting the Machine/ System Settings.
- IPsec is not applied to data obtained through DHCP, DNS, or WINS.
- IPsec for both IPv4 and IPv6 is supported by Windows Vista/7/8/8.1/10, Windows Server 2008/2008 R2/2012/2012 R2, OS X 10.9 and later, Red Hat Enterprise Linux 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

For key configuration, this machine supports automatic key exchange to specify agreements such as the IPsec algorithm and key 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.

Note that it is possible to configure multiple SAs.

Settings 1-4 and default setting

Using the 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 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.

IPsec settings items

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.

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.

Security level	Security level features
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	SHA256
Phase 1 Encryption Algorithm	DES	3DES	AES-128-CBC
Phase 1 Diffie-Hellman Group	2	2	2
Phase 2 Security Protocol	AH	ESP	ESP

Setting	Authentication Only	Authentication and Low Level Encryption	Authentication and High Level Encryption
Phase 2 Authentication Algorithm	HMAC-SHA1-96/ HMAC-SHA256-128/ HMAC-SHA384-192/ HMAC-SHA512-256	HMAC-SHA1-96/ HMAC-SHA256-128/ HMAC-SHA384-192/ HMAC-SHA512-256	HMAC-SHA256-128/ HMAC-SHA384-192/ HMAC-SHA512-256
Phase 2 Encryption Algorithm Permissions	Cleartext (NULL encryption)	3DES/AES-128/ AES-192/AES-256	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".

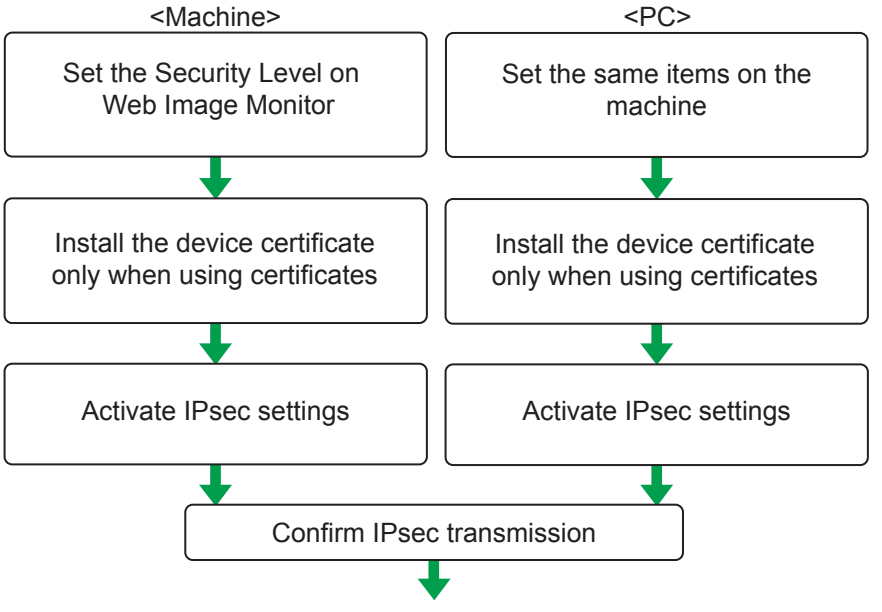
Setting	Description	Setting value
Address Type	Specify the address type for which IPsec transmission is used.	• Inactive • IPv4 • IPv6 • IPv4/IPv6 (Default Settings only)
Local Address	Specify the machine's address. If you are using multiple addresses in IPv6, you can also specify an address range.	The 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 • SHA256 • SHA384 • SHA512
Phase 1 Encryption Algorithm	Specify the encryption algorithm to be used in phase 1. (auto setting)	• DES • 3DES • AES-128-CBC • AES-192-CBC • AES-256-CBC
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 • HMAC-SHA256-128 • HMAC-SHA384-192 • HMAC-SHA512-256
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 Auto Exchange Settings Configuration Flow



CJD015

Important

- 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

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 page 119 "Protecting the Communication Path via a Device Certificate". For the method of assigning installed certificates to IPsec, see page 146 "Selecting the certificate for IPsec".

1. Log in as the network administrator from Web Image Monitor.
2. Point to [Device Management], and then click [Configuration].
3. Click [IPsec] under "Security".
4. Click [Edit] under "Encryption Key Auto Exchange Settings".

5. **Make encryption key auto exchange settings in [Settings 1].**

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

6. **Click [OK].**
7. **Select [Active] for "IPsec" in "IPsec".**
8. **Set "Exclude HTTPS Communication" to [Active] if you do not want to use IPsec for HTTPS transmission.**
9. **Click [OK].**
10. **"Updating..." appears. Wait for about one or two minutes, and then click [OK].**

    If the previous screen does not reappear after you click [OK], wait for a while, and then click the web browser's refresh button.

11. **Log out.**

Selecting the certificate for IPsec

Using Web Image Monitor, select the certificate to be used for IPsec. You must install the certificate before it can be used. For details about creating and installing a device certificate, see page 119 "Protecting the Communication Path via a Device Certificate".

1. **Log in as the network administrator from Web Image Monitor.**
2. **Point to [Device Management], and then click [Configuration].**
3. **Click [Device Certificate] under "Security".**
4. **Select the certificate to be used for IPsec from the drop-down box in "IPsec" under "Certification".**
5. **Click [OK].**

   The certificate for IPsec is specified.

6. **"Updating..." appears. Wait for about one or two minutes, and then click [OK].**

   If the previous screen does not reappear after you click [OK], wait for a while, and then click the web browser's refresh button.

7. **Log out.**

Specifying the computer's IPsec settings

Configure the computer's IPsec SA settings, so that they exactly match 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 7 when the "Authentication and Low Level Encryption" security level is selected.

1. **On the [Start] menu, click [Control Panel], click [System and Security], and then click [Administrative Tools].**

   Under Windows 8, hover the mouse pointer over the top- or bottom-right corner of the screen, and then click [Settings], [Control Panel], [System and Security], and then [Administrative Tools].

2. **Double-click [Local Security Policy].**

   If the "User Account Control" dialog box appears, click [Yes].

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

    The IP Filter Wizard appears.

19. **Click [Next].**
20. **If required, enter a description of the IP filter, and then click [Next].**
21. **Select "My IP Address" in "Source address", and then click [Next].**
22. **Select "A specific IP Address or Subnet" in "Destination address", enter the machine's IP address, and then click [Next].**

23. **Select the protocol type for IPsec, and then click [Next].**

    If you are using IPsec with IPv6, select "58" as the protocol number for the "Other" target protocol type.

24. **Click [Finish].**
25. **Click [OK].**
26. **Select the IP filter that was just created, and then click [Next].**
27. **Click [Add].**

    Filter action wizard appears.

28. **Click [Next].**
29. **In [Name], enter an IP Filter action name, and then click [Next].**
30. **Select "Negotiate security", and then click [Next].**
31. **Select "Allow unsecured communication if a secure connection connect be established.", and then [Next].**
32. **Select "Custom" and click [Settings].**
33. **In "Integrity algorithm", select the authentication algorithm that was specified on the machine in "Encryption Key Auto Exchange Settings Phase 2".**
34. **In "Encryption algorithm", select the encryption algorithm that specified on the machine in "Encryption Key Auto Exchange Settings Phase 2".**
35. **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".**
36. **Click [OK].**
37. **Click [Next].**
38. **Click [Finish].**
39. **Select the filter action that was just created, and then click [Next].**

    If you set "Encryption Key Auto Exchange Settings" to "Authentication and High Level Encryption", select the IP filter action that was just created, click [Edit], and then check "Use session key perfect forward secrecy (PFS)" on the filter action properties dialog box. If using PFS in Windows, 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.

40. **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.

41. **Click [Finish].**

    If you are using IPv6, you must repeat this procedure from Step 13 and add 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].

42. **Click [OK].**

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

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

    The computer's IPsec settings are enabled.

Note

- To disable the computer's IPsec settings, select the security policy, right-click, and then click [Unassign].

telnet Setting Commands

You can use telnet to confirm IPsec settings and make setting changes. This section explains telnet commands for IPsec. The default user name for logging into telnet is "admin". The password is not configured by default. For details about logging in to telnet and telnet operations, see "Remote Maintenance Using telnet", Connecting the Machine/ System Settings.

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 settings 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 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 ike

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

Display current settings

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

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

Disable settings

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

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

Specify the local/remote address for settings 1-4

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

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

Specify the address type in default setting

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

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

Security policy setting

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

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

Security protocol setting

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

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

IPsec requirement level setting

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

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

Encapsulation mode setting

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

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

Tunnel end point setting

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

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

IKE partner authentication method setting

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

- Enter the separate setting number [1-4] or [default] and specify the authentication method.

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

PSK character string setting

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

- If you select PSK as the authentication method, enter the separate setting number [1-4] or [default] and specify the PSK character string.
- Specify the 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|sha256|sha384|sha512}
```

- Enter the separate setting number [1-4] or [default] and specify the ISAKMP SA (phase 1) hash algorithm.
- 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|aes128|aes192|aes256}
```

- Enter the separate setting number [1-4] or [default] and specify the ISAKMP SA (phase 1) encryption algorithm.
- 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|hmac-sha256|hmac-
sha384|hmac-sha512}
```

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

IPsec SA (phase 2) encryption algorithm setting

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

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

IPsec SA (phase 2) PFS setting

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

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

IPsec SA (phase 2) validity period setting

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

- Enter the separate setting number [1-4] or [default] and specify the IPsec SA (phase 2) validity period.
- Enter the validity period (in seconds) from 300 to 172800.
- Not specifying a validity period displays the current setting.

Reset setting values

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

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

Configuring IEEE 802.1X Authentication

IEEE 802.1X is an authentication function that can be used with both wired and wireless networks. Authentication is performed by the authentication server (RADIUS server).

You can select four types of EAP authentication method: EAP-TLS, LEAP, EAP-TTLS and PEAP. Note that each EAP authentication method has different configuration settings and authentication procedures.

Types and requirements of certificates are as follows:

EAP type	Required certificates
EAP-TLS	Site certificate, Device certificate (IEEE 802.1X Client Certificate)
LEAP	-
EAP-TTLS	Site certificate
PEAP	Site certificate
PEAP (Phase 2 is for TLS only)	Site certificate, Device certificate (IEEE 802.1X Client Certificate)

Installing a Site Certificate

Install a site certificate (root CA certificate) for verifying the reliability of the authentication server. You need to have at least a certificate issued by the certificate authority who signed the server certificate or a certificate from a higher certificate authority.

Only PEM (Base64-encoded X.509) site certificates can be imported.

1. **Log in as the network administrator from Web Image Monitor.**
2. **Point to [Device Management], and then click [Configuration].**
3. **Click [Site Certificate] under "Security".**
4. **Click [Browse] for "Site Certificate to Import", and then select the CA certificate you obtained.**
5. **Click [Open].**
6. **Click [Import].**
7. **Check that the imported certificate's [Status] shows "Trustworthy".**

   If [Site Certificate Check] shows [Active], and the [Status] of the certificate shows [Untrustworthy], communication might not be possible.
8. **Click [OK].**
9. **Log out.**

Selecting the Device Certificate

Select the certificate to use under IEEE 802.1X from among the device certificates created and installed in advance on the machine. For details about creating and installing a device certificate, see page 119 "Protecting the Communication Path via a Device Certificate".

1. **Log in as the network administrator from Web Image Monitor.**
2. **Point to [Device Management], and then click [Configuration].**
3. **Click [Device Certificate] under "Security".**
4. **Select the certificate to be used for IEEE 802.1X from the drop-down box in "IEEE 802.1X" under "Certification".**
5. **Click [OK].**
6. **"Updating..." appears. Wait for about one or two minutes, and then click [OK].**

   If the previous screen does not reappear after you click [OK], wait for a while, and then click the web browser's refresh button.
7. **Log out.**

Setting Items of IEEE 802.1X for Ethernet

1. **Log in as the network administrator from Web Image Monitor.**
2. **Point to [Device Management], and then click [Configuration].**
3. **Click [IEEE 802.1X] under "Security".**
4. **In "User Name", enter the user name set in the RADIUS server.**
5. **Enter the domain name in "Domain Name".**
6. **Select "EAP Type". Configurations differ according to the EAP Type.**

   EAP-TLS

   - Make the following settings according to the operating system you are using:
     - Select [On] or [Off] in "Authenticate Server Certificate".
     - Select [On] or [Off] in "Trust Intermediate Certificate Authority".
     - Enter the host name of the RADIUS server on "Server ID".
     - Select [On] or [Off] in "Permit Sub-domain".

   LEAP

   - Click [Change] in "Password", and then enter the password set in the RADIUS server.

   EAP-TTLS

   - Click [Change] in "Password", and then enter the password set in the RADIUS server.

- Click [Change] in "Phase 2 User Name", and then enter the user name set in the RADIUS server.
- Select [CHAP], [MSCHAP], [MSCHAPv2], [PAP], or [MD5] in "Phase 2 Method".

  Certain methods might not be available, depending on the RADIUS server you want to use.
- Make the following settings according to the operating system you are using:
  - Select [On] or [Off] in "Authenticate Server Certificate".
  - Select [On] or [Off] in "Trust Intermediate Certificate Authority".
  - Enter the host name of the RADIUS server in "Server ID".
  - Select [On] or [Off] in "Permit Sub-domain".

PEAP

- Click [Change] in "Password", and then enter the password set in the RADIUS server.

  If [TLS] is selected for "Phase 2 Method", you do not need to specify a password.
- Click [Change] on "Phase 2 User Name", and then enter the user name set in the RADIUS server.
- Select [MSCHAPv2] or [TLS] in "Phase 2 Method".

  When you select [TLS], you must install "IEEE 802.1X Client Certificate".
- Make the following settings according to the operating system you are using:
  - Select [On] or [Off] in "Authenticate Server Certificate".
  - Select [On] or [Off] in "Trust Intermediate Certificate Authority".
  - Enter the host name of the RADIUS server on "Server ID".
  - Select [On] or [Off] in "Permit Sub-domain".

7. **Click [OK].**
8. **"Updating..." appears. Wait for about one or two minutes, and then click [OK].**

   If the previous screen does not reappear after you click [OK], wait for a while, and then click the web browser's refresh button.
9. **Click [Interface Settings] under "Interface".**
10. **Select [Active] in "Ethernet Security".**
11. **Click [OK].**
12. **"Updating..." appears. Wait for about one or two minutes, and then click [OK].**

    If the previous screen does not reappear after you click [OK], wait for a while, and then click the web browser's refresh button.
13. **Log out.**

Note

- If there is a problem with settings, you might not be able to communicate with the machine. In such a case, access [Print List] in [Interface Settings] on the control panel, and then print the network summary to check the status.
- If you cannot identify the problem, execute [Restore IEEE 802.1X Authentication to Defaults] in [Network] in [Interface Settings] on the control panel, and then repeat the procedure.

Setting Items of IEEE 802.1X for Wireless LAN

1. **Log in as the network administrator from Web Image Monitor.**
2. **Point to [Device Management], and then click [Configuration].**
3. **Click [IEEE 802.1X] under "Security".**
4. **In "User Name", enter the user name set in the RADIUS server.**
5. **Enter the domain name in "Domain Name".**
6. **Select "EAP Type". Configurations differ according to the EAP Type.**

   EAP-TLS

   - Make the following settings according to the operating system you are using:
     - Select [On] or [Off] in "Authenticate Server Certificate".
     - Select [On] or [Off] in "Trust Intermediate Certificate Authority".
     - Enter the host name of the RADIUS server on "Server ID".
     - Select [On] or [Off] in "Permit Sub-domain".

   LEAP

   - Click [Change] in "Password", and then enter the password set in the RADIUS server.

   EAP-TTLS

   - Click [Change] in "Password", and then enter the password set in the RADIUS server.
   - Click [Change] in "Phase 2 User Name", and then enter the user name set in the RADIUS server.
   - Select [CHAP], [MSCHAP], [MSCHAPv2], [PAP], or [MD5] in "Phase 2 Method".

     Certain methods might not be available, depending on the RADIUS server you want to use.
   - Make the following settings according to the operating system you are using:
     - Select [On] or [Off] in "Authenticate Server Certificate".
     - Select [On] or [Off] in "Trust Intermediate Certificate Authority".
     - Enter the host name of the RADIUS server in "Server ID".
     - Select [On] or [Off] in "Permit Sub-domain".

PEAP

- Click [Change] in "Password", and then enter the password set in the RADIUS server.

  If [TLS] is selected for "Phase 2 Method", you do not need to specify a password.
- Click [Change] on "Phase 2 User Name", and then enter the user name set in the RADIUS server.
- Select [MSCHAPv2] or [TLS] in "Phase 2 Method".

  When you select [TLS], you must install "IEEE 802.1X Client Certificate".
- Make the following settings according to the operating system you are using:
  - Select [On] or [Off] in "Authenticate Server Certificate".
  - Select [On] or [Off] in "Trust Intermediate Certificate Authority".
  - Enter the host name of the RADIUS server on "Server ID".
  - Select [On] or [Off] in "Permit Sub-domain".

7. **Click [OK].**
8. **"Updating..." appears. Wait for about one or two minutes, and then click [OK].**

   If the previous screen does not reappear after you click [OK], wait for a while, and then click the web browser's refresh button.
9. **Click [Wireless LAN Settings] under "Interface".**
10. **Select [Wireless LAN] in "LAN Type".**
11. **Select [Infrastructure Mode] in "Communication Mode".**
12. **Enter the alphanumeric characters (a-z, A-Z, or 0-9) in [SSID] according to the access point you want to use.**
13. **Select [WPA2] in "Security Method".**
14. **Select [WPA2] in "WPA2 Authentication Method".**
15. **Click [OK].**
16. **"Updating..." appears. Wait for about one or two minutes, and then click [OK].**

    If the previous screen does not reappear after you click [OK], wait for a while, and then click the web browser's refresh button.
17. **Log out.**

Note

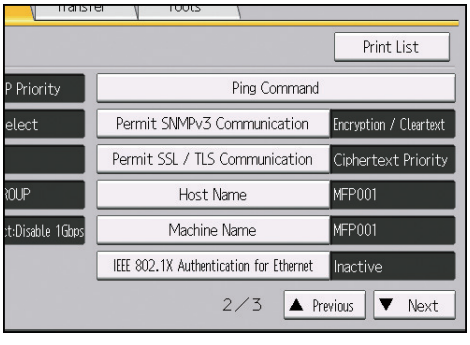
- If there is a problem with settings, you might not be able to communicate with the machine. In such a case, access [Print List] in [Interface Settings] on the control panel, and then print the network summary to check the status.
- If you cannot identify the problem, execute [Restore IEEE 802.1X Authentication to Defaults] in [Network] in [Interface Settings] on the control panel, and then repeat the procedure.

SNMPv3 Encryption

When using Device Manager NX Lite or another application that communicates via SNMPv3, you can encrypt the data transmitted.

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

1. **Log in as the network administrator from the control panel.**
2. **Press [System Settings].**
3. **Press [Interface Settings].**
4. **Press [▼Next].**
5. **Press [Permit SNMPv3 Communication].**



6. **Press [Encryption Only].**
7. **Press [OK].**
8. **Log out.**

Note

- To use Device Manager NX Lite 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 Device Manager NX Lite, in addition to specifying [Permit SNMPv3 Communication] on the machine. For details about specifying [Encryption Password] in Device Manager NX Lite, see Device Manager NX Lite 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 page 16 "Registering and Changing Administrators".

Encrypting Transmitted Passwords

Configuring the driver encryption key and password encryption for IPP authentication enables communication with encrypted passwords as well as increasing the security against password cracking. In order to further enhance security, we recommend using IPsec, SNMPv3 and SSL/TLS all together.

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

Driver Encryption Key

This key is a character string used for encrypting login passwords or document passwords sent from each driver when user authentication is ON.

To encrypt the login password, specify the driver encryption key on the machine and on the printer 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.

You can use the TWAIN driver on Type 1, 2, or 3 machines only.

Note

- For details on encrypting the login passwords used for administrator authentication, see page 16 "Registering and Changing Administrators".

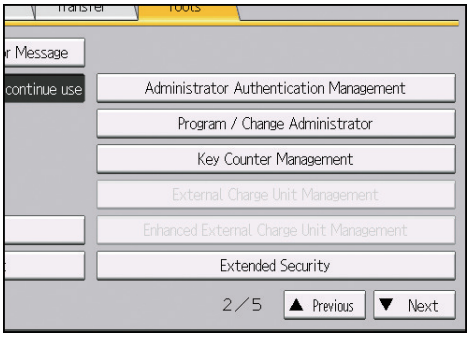
Specifying a Driver Encryption Key

Specify the driver encryption key on the machine.

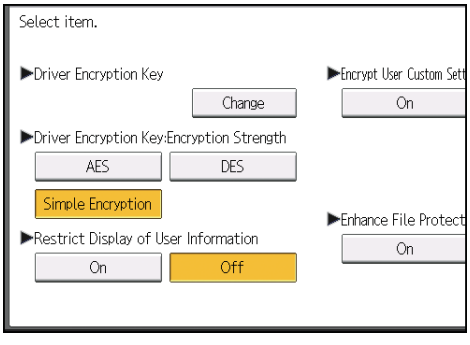
This setting enables encrypted transmission of login passwords and strengthens the security against password cracking.

1. **Log in as the network administrator from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼Next].**

5. **Press [Extended Security].**



6. **For "Driver Encryption Key", press [Change].**



7. **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.

8. **Press [OK].**
9. **Log out.**

Note

- For details about specifying the encryption key on the printer driver or TWAIN driver, see the driver help.

Specifying an IPP Authentication Password

Specify an IPP authentication password for this machine. This setting enables encrypted transmission of IPP authentication passwords and strengthens the security against password cracking.

1. **Log in as the network administrator from Web Image Monitor.**
2. **Point to [Device Management], and then click [Configuration].**

3. **Click [IPP Authentication] under "Security".**
4. **Select [DIGEST] from the "Authentication" list.**
5. **Enter the user name in the "User Name" box.**
6. **Enter the password in the "Password" box.**
7. **Click [OK].**

   IPP authentication is specified.
8. **"Updating..." appears. Wait for about one or two minutes, and then click [OK].**

   If the previous screen does not reappear after you click [OK], wait for a while, and then click the web browser's refresh button.
9. **Log out.**

Kerberos Authentication Encryption Setting

You can specify encrypted transmission between the machine and the key distribution center (KDC) server when Kerberos authentication is enabled.

Using Kerberos authentication with Windows or LDAP authentication, LDAP search, etc., ensures safe communication.

The supported encryption algorithm differs depending on the type of KDC server. Select the algorithm that suits your environment.

KDC server	Supported encryption algorithms
Windows Server 2008	• AES256-CTS-HMAC-SHA1-96 • AES128-CTS-HMAC-SHA1-96 • RC4-HMAC (ARCFOUR-HMAC-MD5) • DES-CBC-MD5
Windows Server 2008 R2/Windows Server 2012/2012 R2	• AES256-CTS-HMAC-SHA1-96 • AES128-CTS-HMAC-SHA1-96 • RC4-HMAC (ARCFOUR-HMAC-MD5) • DES-CBC-MD5*
Heimdal	• AES256-CTS-HMAC-SHA1-96 • AES128-CTS-HMAC-SHA1-96 • DES3-CBC-SHA1 • RC4-HMAC (ARCFOUR-HMAC-MD5) • DES-CBC-MD5

* To use Kerberos authentication, it must be enabled in the operating system settings.

1. **Log in as the network administrator from Web Image Monitor.**
2. **Point to [Device Management], and then click [Configuration].**
3. **Click [Kerberos Authentication] under "Device Settings".**
4. **Select the encryption algorithm you want to enable.**

   One or more encryption algorithm must always be selected.
5. **Click [OK].**
6. **Log out.**

6. Preventing the Leaking of Documents

This chapter explains how to protect document data stored in the machine or printed using the machine.

Managing Folders

You can use this function on Type 1, 2, or 3 machines only.

This section explains how to manage the folders in Document Server: how to delete folders, change their passwords, and unlock them when locked.

Deleting Folders

This can be done by the file administrator or a user.

To delete a folder with icon next to it, the folder's password is required.

If a user has forgotten the password to access the folder, the file administrator can change it.

The file administrator can delete folders without using the password.

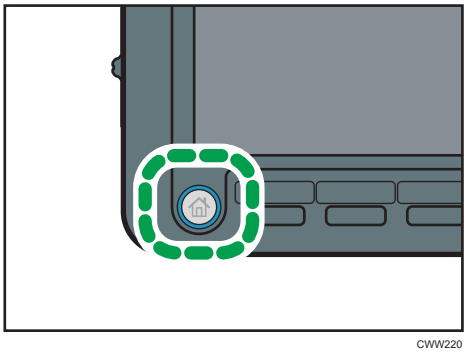
Folders containing files which the user does not have permission to delete cannot be deleted.

The shared folder cannot be deleted.

1. **Log in as the file administrator or a user from the control panel.**
2. **Press the [User Tools] key to close the User Tools menu.**

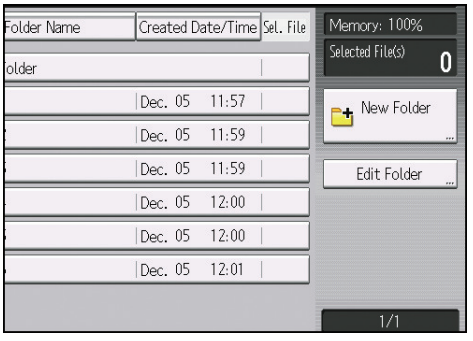
   If the message "You do not have the privileges to use this function." appears, press [Exit].
3. **Press the [Home] key on the control panel, and press the [Document Server] icon on the [Home] screen.**

   If the message "You do not have the privileges to use this function." appears, press [Exit].



CWW220

4. **Press [Edit Folder].**



5. **Select the folder.**
6. **Press [Delete].**
7. **If a password entry screen appears, enter the password of the folder, and then press [OK].**
8. **Press [Delete].**
9. **Log out.**

Note

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

Changing the Password of a Folder

This can be specified by the file administrator or a user.

If the password to access the folder has been forgotten, the file administrator can change it.

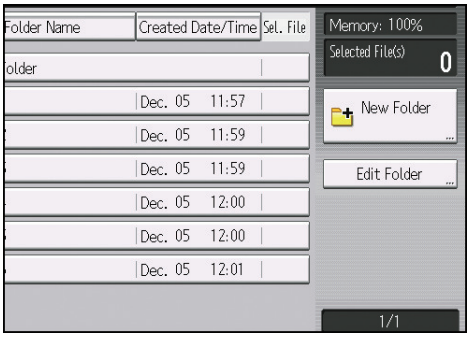
A password cannot be specified for the shared folder.

1. **Log in as the file administrator or a user from the control panel.**
2. **Press the [User Tools] key to close the User Tools menu.**

   If the message "You do not have the privileges to use this function." appears, press [Exit].
3. **Press the [Home] key on the control panel, and press the [Document Server] icon on the [Home] screen.**

   If the message "You do not have the privileges to use this function." appears, press [Exit].

4. **Press [Edit Folder].**



5. **Select the folder.**
6. **Press [Change Password].**
7. **If a password entry screen appears, enter the password of the folder, and then press [OK].**

   The password entry screen does not appear if the file administrator is logged in.
8. **Enter the new password for the folder, and then press [OK].**

   You can use 4 to 8 numbers as the password for the folder.
9. **Re-enter the password for confirmation, and then press [OK].**

   The icon appears next to a folder protected by password.
10. **Log out.**

Note

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

Unlocking Folders

Only the file administrator can unlock folders.

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

"Enhance File Protection" is one of the extended security functions. For details about this and other extended security functions, see page 243 "Specifying the Extended Security Functions".

1. **Log in as the file administrator from the control panel.**
2. **Press the [User Tools] key to close the User Tools menu.**

   If the message "You do not have the privileges to use this function." appears, press [Exit].
3. **Press the [Home] key on the control panel, and press the [Document Server] icon on the [Home] screen.**

   If the message "You do not have the privileges to use this function." appears, press [Exit].

4. **Press [Edit Folder].**
5. **Select the folder.**

   The icon appears next to a folder locked by the Enhance File Protection function.
6. **Press [Unlock].**

   The icon changes to the icon.
7. **Press [Unlock].**
8. **Log out.**

Note

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

Managing Stored Files

You can use this function on Type 1, 2, or 3 machines only.

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.

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

Types of access permission

Access permission	Description
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 administrator or owner. You can obtain greater protection against the unauthorized use of files. For details about assigning a password to a stored file, see page 175 "Specifying Passwords for Stored Files".
- Even if user authentication is not set, passwords for stored files can be set.

Note

- Files can be stored by any user who is allowed to use Document Server, copy function, scanner function, or printer function.
- Using Web Image Monitor, you can check the content of stored files. For details, see Web Image Monitor Help.
- The default access permission for the owner is "Read-only". You can also specify the access permission.
- The file administrator not only configures access permissions, but can also delete stored files. For details on the methods of deleting documents, see "Deleting Stored Documents", Copy/ Document Server.

Configuring Access Permission for Each Stored File

This can be specified by the file administrator or owner.

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

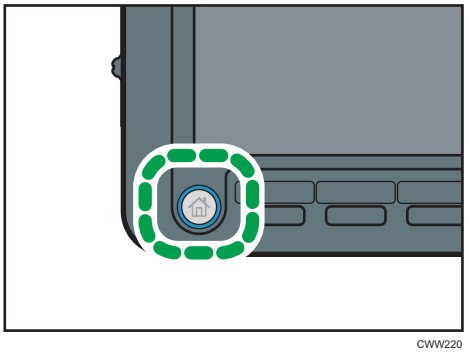
Important

- **If files become inaccessible, reset their access permission as the 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 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. **Log in as the file administrator or the owner from the control panel.**
2. **Press the [User Tools] key to close the User Tools menu.**

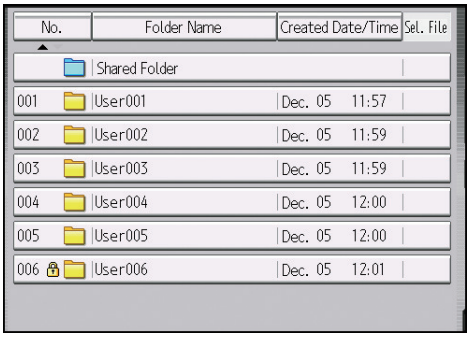
   If the message "You do not have the privileges to use this function." appears, press [Exit].
3. **Press the [Home] key on the control panel, and press the [Document Server] icon on the [Home] screen.**

   If the message "You do not have the privileges to use this function." appears, press [Exit].

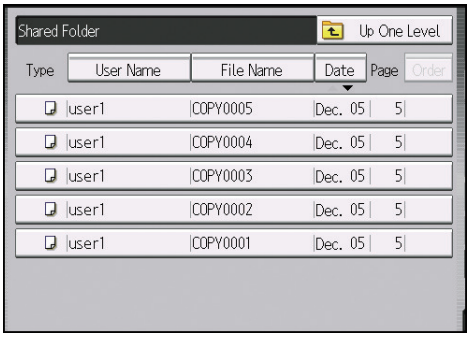


CWW220

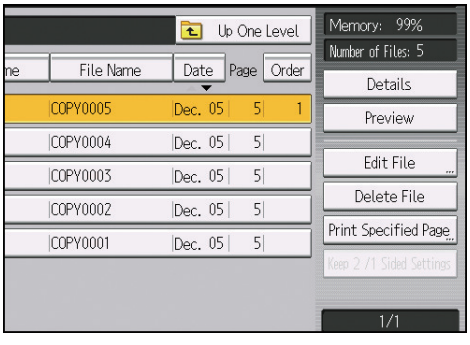
4. **Select the folder.**



5. Select the file.

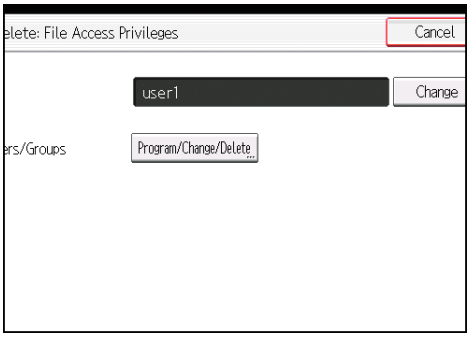


6. Press [Edit File].



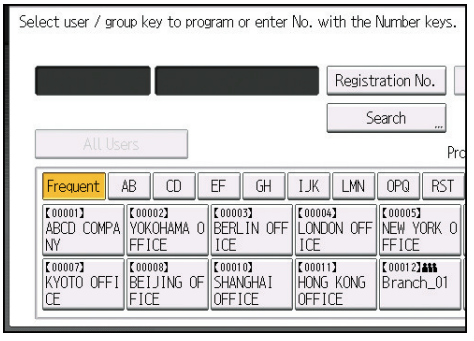
7. Press [Change Access Priv.].

8. Press [Program/Change/Delete].



9. Press [New Program].

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

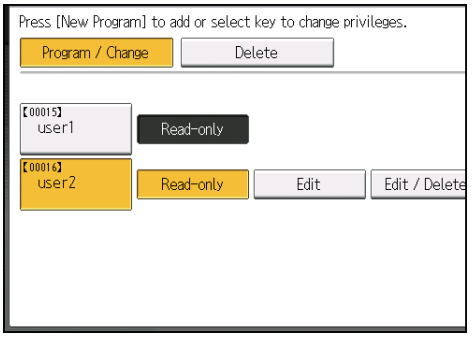


You can select more than one user.

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

11. **Press [Exit].**

12. **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].

13. **Press [Exit].**

14. **Press [OK].**

15. **Log out.**

Note

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

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. **Log in as the file administrator from the control panel.**
2. **Press the [User Tools] key to close the User Tools menu.**

   If the message "You do not have the privileges to use this function." appears, press [Exit].
3. **Press the [Home] key on the control panel, and press the [Document Server] icon on the [Home] screen.**

   If the message "You do not have the privileges to use this function." appears, press [Exit].
4. **Select the folder.**
5. **Select the file.**
6. **Press [Edit File].**
7. **Press [Change Access Priv.].**
8. **Press [Change] for "Owner".**
9. **Select the user you want to register.**
10. **Press [Exit].**
11. **Press [OK].**
12. **Log out.**

Configuring Access Permission for Each User for Stored Files

This can be specified by the user administrator or owner.

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

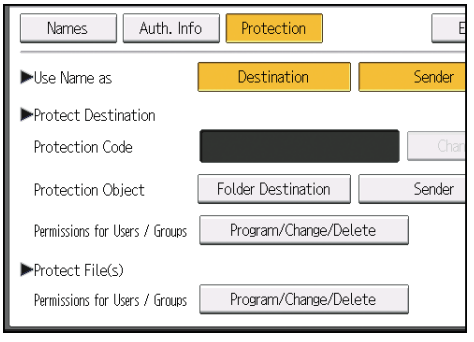
This makes managing access permission easier than specifying and managing access permissions for each stored file.

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. **The user administrator or the owner logs in from the control panel.**
2. **Press [Address Book Mangmnt].**
3. **Select the user.**
4. **Press [Protection].**

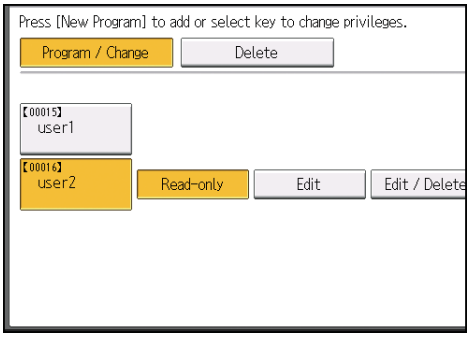
5. **Under "Protect File(s)", press [Program/Change/Delete] for "Permissions for Users / Groups".**



6. **Press [New Program].**
7. **Select the users or groups to register.**

   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].**
12. **Press [Exit].**
13. **Log out.**

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.

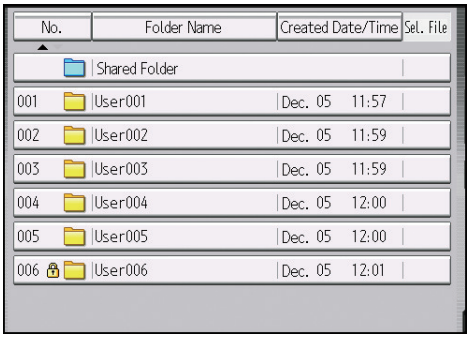
Specifying Passwords for Stored Files

This can be specified by the file administrator or owner.

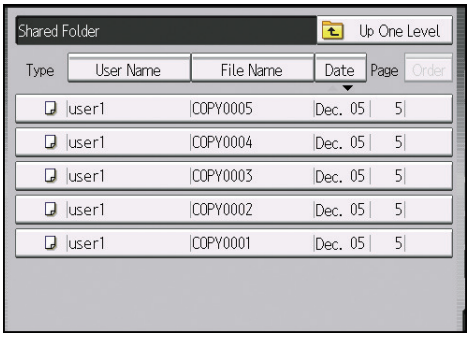
1. **The file administrator or the owner logs in from the control panel.**
2. **Press the [User Tools] key to close the User Tools menu.**

   If the message "You do not have the privileges to use this function." appears, press [Exit].
3. **Press the [Home] key on the control panel, and press the [Document Server] icon on the [Home] screen.**

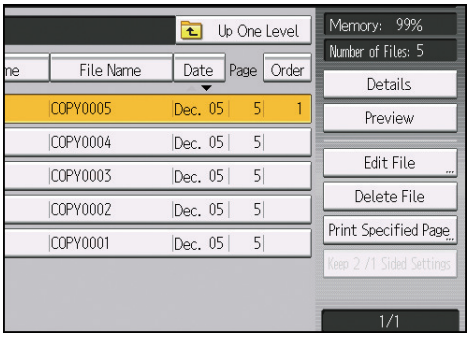
   If the message "You do not have the privileges to use this function." appears, press [Exit].
4. **Select the folder.**



5. **Select the file.**



6. **Press [Edit File].**



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

   You can use 4 to 8 numbers as the password for the stored file.
9. **Re-enter the password for confirmation, and then press [OK].**

   The icon appears next to a stored file protected by password.
10. **Press [OK].**
11. **Log out.**

Unlocking Stored Files

Only the file administrator can unlock 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 page 243 "Specifying the Extended Security Functions".

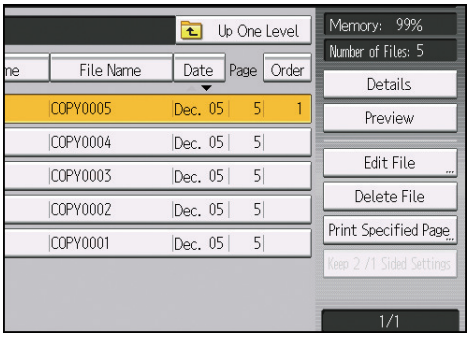
1. **Log in as the file administrator from the control panel.**
2. **Press the [User Tools] key to close the User Tools menu.**

   If the message "You do not have the privileges to use this function." appears, press [Exit].
3. **Press the [Home] key on the control panel, and press the [Document Server] icon on the [Home] screen.**

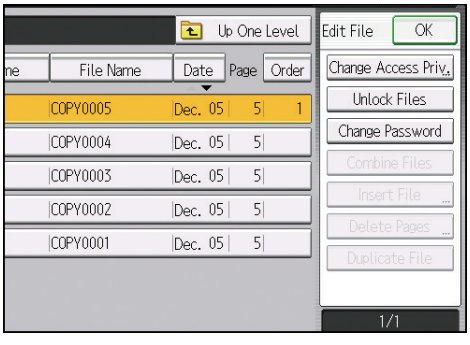
   If the message "You do not have the privileges to use this function." appears, press [Exit].
4. **Select the folder.**
5. **Select the file.**

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

6. **Press [Edit File].**



7. **Press [Unlock Files].**



8. **Press [Yes].**

   The icon changes to the icon.

9. **Press [OK].**

10. **Log out.**

Managing Locked Print Files

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.

Note

- Confidential documents can be printed regardless of the user authentication settings.
- To store files temporarily, select [Stored Print] in the printer driver. If you select [Stored Print (Shared)], you can also share these files.
- For details on how to use the Locked Print function, see "Locked Print", Print.

Deleting Locked Print Files

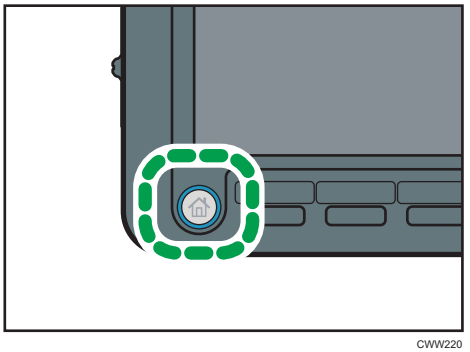
This can be specified by the file administrator or owner.

For the owner to delete a Locked Print file, the password to access the file is required. If the owner has forgotten the password, the file administrator can change it.

The password is not required for the file administrator to delete Locked Print files.

1. **Log in as the file administrator or the owner from the control panel.**
2. **Press the [User Tools] key to close the User Tools menu.**

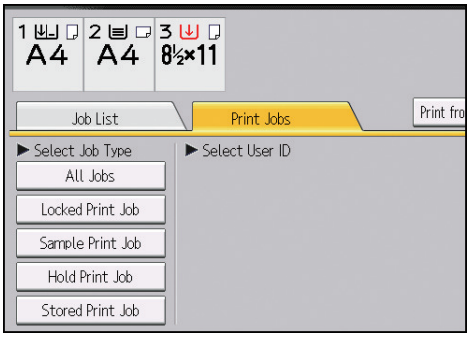
   If the message "You do not have the privileges to use this function." appears, press [Exit].
3. **Press the [Home] key on the control panel, and press the [Printer] icon on the [Home] screen.**



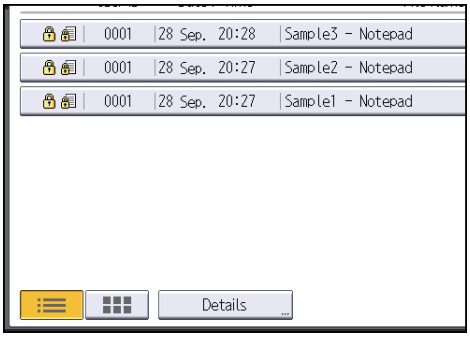
CWW220

4. **Press [Print Jobs].**

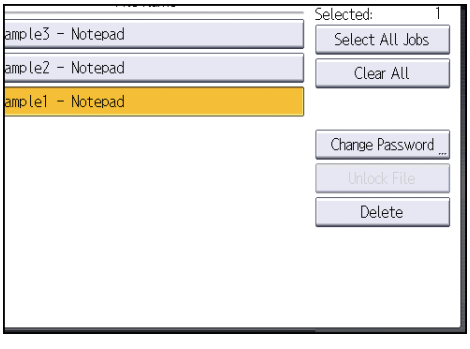
5. **Press [Locked Print Job].**



6. **Select the file.**



7. **Press [Delete].**



8. **If a password entry screen appears, 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.

9. **Press [Yes].**

10. **Log out.**

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 "Data Management", Print.
- This can also be specified via Web Image Monitor. For details, see Web Image Monitor Help.

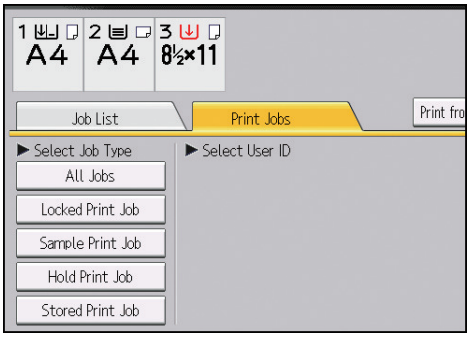
Changing the Password of a Locked Print File

This can be specified by the file administrator or owner.

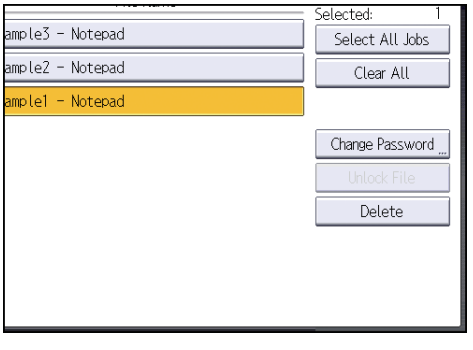
If the owner has forgotten the password, the file administrator can change it.

1. **Log in as the file administrator or the owner from the control panel.**
2. **Press the [User Tools] key to close the User Tools menu.**

   If the message "You do not have the privileges to use this function." appears, press [Exit].
3. **Press the [Home] key on the control panel, and press the [Printer] icon on the [Home] screen.**
4. **Press [Print Jobs].**
5. **Press [Locked Print Job].**



6. **Select the file.**
7. **Press [Change Password].**



8. **If a password entry screen appears, enter the password for the stored file, and then press [OK].**

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

9. **Enter the new password for the stored file, and then press [OK].**
10. **Re-enter the password for confirmation, and then press [OK].**
11. **Log out.**

Note

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

Unlocking a Locked Print File

Only the file administrator can unlock files.

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 page 243 "Specifying the Extended Security Functions".

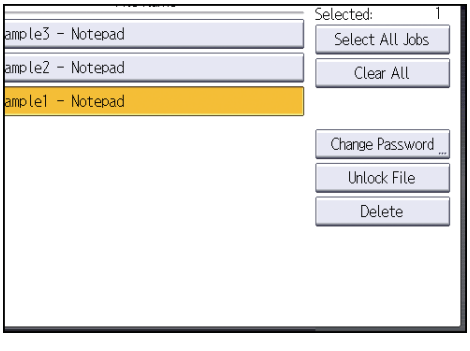
1. **Log in as the file administrator from the control panel.**
2. **Press the [User Tools] key to close the User Tools menu.**

   If the message "You do not have the privileges to use this function." appears, press [Exit].

3. **Press the [Home] key on the control panel, and press the [Printer] icon on the [Home] screen.**
4. **Press [Print Jobs].**
5. **Press [Locked Print Job].**
6. **Select the file.**

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

7. **Press [Unlock File].**



8. **Press [Yes].**

   The icon disappears.

9. **Log out.**

Note

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

Unauthorized Copy Prevention / Data Security for Copying

The copier, Document Server, and printer functions let you embed a pattern in a printed copy to discourage or prevent unauthorized copying.

You can use the copy function, Document Server function, and Detect Data Security for Copying function on Type 1, 2, or 3 machines only.

If the Unauthorized Copy Prevention function is enabled, embedded text patterns (for instance, a warning message such as "No Copying") are displayed when documents are copied illegally. Accordingly, unauthorized copying can be prevented.

If the Data Security for Copying function is used and settings for special patterns embedded in documents are enabled, copies of documents with embedded patterns are printed with gray overprint. Accordingly, information leakage can be prevented. To protect documents by gray overprint, the copier or multi-function printer must be installed with the Copy Data Security Unit.

If a machine installed with the Copy Data Security Unit detects a file protected by the Data Security for Copying function, the machine beeps and logs the unauthorized copying.

For more information, see the information below:

Using Unauthorized Copy Prevention

1. On the machine, enable printing of the embedded pattern. The settings must be configured by the machine administrator. For details about how to configure the setting, see page 184 "Enabling Pattern Printing".
2. Specify the settings for unauthorized copy prevention in the copier, Document Server, or printer function. The privilege to specify the setting depends on the setting specified in [Compulsory Unauthorized Copy Prevention]. For details, see page 184 "Enabling Pattern Printing".

Using Data Security for Copying

1. On the machine, enable the embedded pattern print setting. The settings must be configured by the machine administrator. For details about how to configure the setting, see page 184 "Enabling Pattern Printing".
2. Specify the settings for data security for copying in the copier, Document Server, or printer function. The privilege to specify the setting depends on the setting specified in [Compulsory Unauthorized Copy Prevention]. For details, see page 184 "Enabling Pattern Printing".
3. Configure the "Detect Data Security for Copying" setting for printed copies, so that documents are printed with gray overprint when they are illegally copied, scanned, or stored in the machine. The setting must be configured by the machine administrator. For details about how to configure the setting, see page 185 "Enabling Detect Data Security for Copying".

Note

- When copying, the thickness of an embedded pattern may be uneven due to the original type setting,. If this happens, change the original type setting to [Text] or [Photo].

Enabling Pattern Printing

You can enable embedded pattern printing to discourage or prevent unauthorized copying.

Enabling embedded pattern printing in the Copier/Document Server functions

1. **Log in as the machine administrator from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼Next] three times.**
5. **Select either [Unauthorized Copy Prevention Printing: Copier] or [Unauthorized Copy Prevention Printing: Document Server].**
6. **Press [Change] for "Compulsory Unauthorized Copy Prevention".**
7. **Specify whether or not to make printing of the embedded pattern mandatory.**
   - [Off]

     Printing of the embedded pattern is not mandatory.

     From the Copier/Document Server screen, users can specify whether or not to print with the embedded pattern and can specify its settings.
   - [On:User Can Chng. Some Setg.]

     Printing of the embedded pattern is mandatory.

     From the Copier/Document Server screen, users can specify the embedded pattern settings except for type and thickness.
   - [On:User Cannot Change Settgs.]

     Printing of the embedded pattern is mandatory.

     Users cannot specify the embedded pattern settings from the Copier/Document Server screen.
8. **Press [OK] twice.**
9. **Log out.**

Note

- For details of the settings to specify the pattern using the machine, see "Administrator Tools", Connecting the Machine/ System Settings.

Enabling embedded pattern printing in the Printer function

1. **Log in as the machine administrator from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **When using Type 1, 2, or 3, press [▼Next] three times. When using Type 4 or 5, press [▼Next] twice.**
5. **Press [Unauthorized Copy Prevention Printing: Printer].**
6. **Press [Change] for "Unauthorized Copy Prevention Setting".**
7. **Press [On], and then press [OK].**
8. **Press [Change] for "Compulsory Unauthorized Copy Prevention".**
9. **Specify whether or not to make printing of the embedded pattern mandatory.**
   - [Driver / Command]

     Printing of the embedded pattern is not mandatory.

     Using the printer driver, users can choose whether or not to print with the embedded pattern and can specify its settings.
   - [Driver/Command (Most Settings)]

     Printing of the embedded pattern is mandatory.

     Using the printer driver, users can specify the embedded pattern settings except for type and thickness.
   - [Machine Setting(s)]

     Printing of the embedded pattern is mandatory.

     Users cannot specify the embedded pattern settings using the printer driver.
10. **Press [OK] twice.**
11. **Log out.**

Note

- For details of the settings to specify the pattern using the machine, see "Administrator Tools", Connecting the Machine/ System Settings.

Enabling Detect Data Security for Copying

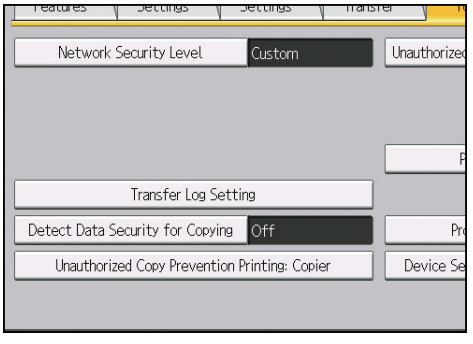
To use this function, the Copy Data Security Unit must be installed.

If a document printed is copied, scanned, or stored in the Document Server, the copy is grayed out.

Important

- If a document that is not copy-guarded is copied, scanned, or stored, the copy or stored file is not grayed out.

1. Log in as the machine administrator from the control panel.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [▼Next] three times.
5. Press [Detect Data Security for Copying].



6. Press [On].

   If you do not want to specify "Detect Data Security for Copying", select [Off].

7. Press [OK].
8. Log out.

Printing User Information on Paper

You can use this function on Type 1, 2, or 3 machines only.

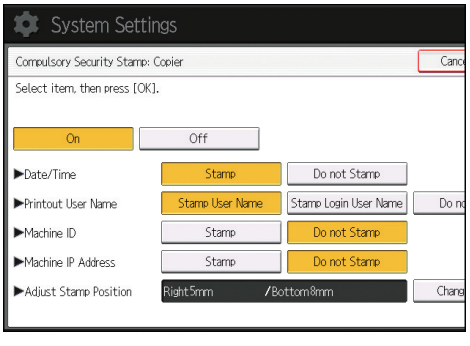
The start time of the print job, information on the person who prints it (name or login user name), machine number and machine's IP address can be compulsorily embedded on printed sheets. This function is called Compulsory Security Stamp.

Always printing out information on the person printing the job is effective for discouraging information leakage. It can also be used for identifying sources of information leakage.

Compulsory Security Stamp can be used with copying, Document Server, and printing.

1. **Log in as the machine administrator from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼Next] four times.**
5. **Select the function(s) for Compulsory Security Stamp.**
   - To set the copy function to be stamped, press [Compulsory Security Stamp:Copier].
   - To set the Document Server to be stamped, press [Compulsory Security Stamp:Doc. Srvr.].
   - To set the printer function to be stamped, press [Compulsory Security Stamp:Printer].
6. **Press [On], and then select the data to be stamped.**

   To turn Compulsory Security Stamp off, press [Off].



   - Date/Time

     The job start time will be printed.
   - Printout User Name

     These will be printed if user authentication is enabled.
     - Stamp User Name

       The "Name" in the "Names" in the Address Book will be printed.
     - Stamp Login User Name

The user code or login user name in "Auth. Info" in the address book will be printed.

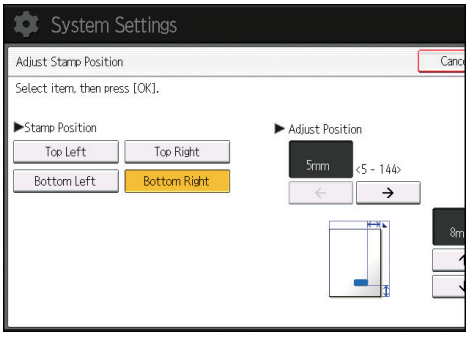
- Machine ID

  The numbers displayed as the "Serial No. of Machine" in [Inquiry] will be printed.

- Machine IP Address

  The machine's IP address will be printed. If there are both IPv4 and IPv6 addresses, the IPv4 address will be printed. If no IP address has been configured, this will be left blank.

7. **Press [Change] for "Adjust Stamp Position".**
8. **Set the stamp position.**



9. **Press [OK] twice.**
10. **Log out.**

Enforced Storage of Documents to be Printed on a Printer

By making it compulsory to keep jobs in the machine before printing them, you can prevent information leakage due to users failing to collect prints or leaving prints unattended. The following print jobs are subject to compulsory storage.

- Normal Print
- Sample Print
- Store and Print

1. **Log in as the machine administrator from the control panel.**
2. **Press [Printer Features].**
3. **Press [System].**
4. **Press [▼Next] twice.**
5. **Press [Restrict Direct Print Jobs].**
6. **Press [Automatclly. Store Jobs].**
7. **Press [OK].**
8. **Log out.**

- If you select [Cncl All Direct Prt Jobs], the print jobs will be cancelled without being stored.
- For information on how to print stored documents, see "Printing Stored Documents", Print.

7. Managing the Machine

This chapter describes the functions for enhancing the security of the machine and operating the machine effectively.

Managing Log Files

Collecting the logs stored in this machine allows you to track detailed data on access to the machine, user identities, usage of the machine's various functions, and error histories.

The logs can be deleted periodically to make hard disk space available, and they can be encrypted to prevent leaking of information.

The logs can be viewed using Web Image Monitor or using the log collection server. Collected logs can be converted to CSV files and downloaded all at once. They cannot be read directly from the hard disk.

Log types

Three types of logs are stored on this machine: the job log, access log, and eco-friendly 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 activities, stored file operations such as creating, editing, and deleting, customer engineer operations such as hard disk formatting, system operations such as viewing log transfer results, and security operations such as specifying settings for encryption, unprivileged access detection, user lockout, and firmware authentication.

- Eco-friendly Log

  Main power ON, OFF, transitions in power status, job run times or time interval between jobs, paper consumption per hour, power consumption.

Note

- For details about the log collection server, see the user's manual of the log collection server.
- When using the log collection server you must configure the log transfer settings on the log collection server.

Using Web Image Monitor to Manage Log Files

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.

Type 1, 2, and 3 machines can collect logs about the copy function, Document Server function, scanner function, Detect Data Security for Copying function, and Result Report Printing/Emailing.

Logs That Can Be Managed Using Web Image Monitor

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.
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.
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.

Job Log Item	Log Type Attribute	Content
Scanner: Stored File Downloading	Scanner: Stored File Downloading	Details of scan files stored in Document Server and downloaded using Web Image Monitor.
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.
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.

Job Log Item	Log Type Attribute	Content
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.
Printer: Hold Print File Printing	Printer: Hold Print File Printing	When a document is held for printing and stored temporarily on the machine, this logs the time a user specifies it be printed via the control panel or Web Image Monitor.

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.
Unauthorized Copying	Unauthorized Copying	Details of documents scanned with "Data Security for Copying".
All Logs Deletion	All Logs Deletion	Details of deletions of all logs.
Log Setting Change	Log Setting Change	Details of changes made to log settings.
Log Collection Item Change	Log Collection Item Change	Details of changes to job log collection levels, access log collection levels, and types of log collected.

Access Log Item	Log Type Attribute	Content
Collect Encrypted Communication Logs	Collect Encrypted Communication Logs	Log of encrypted transmissions between the utility, Web Image Monitor or outside devices.
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 "Machine Data Encryption Key Change" 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.
Machine Configuration	Machine Configuration	Log of changes to the machine's settings.

Access Log Item	Log Type Attribute	Content
Back Up Address Book	Back Up Address Book	Log of when data in the Address Book is backed up.
Restore Address Book	Restore Address Book	Log of when data in the Address Book is restored.
Enhanced Print Volume Use Limitation: Tracking Permission Result	Enhanced Print Volume Use Limitation: Tracking Permission Result	Log of when a tracking error occurs.
Counter Clear Result: Selected User(s)	Counter Clear Result: Selected User(s)	Log of when the counter for an individual user is cleared.
Counter Clear Result: All Users	Counter Clear Result: All Users	Log of when the counters for all users are cleared.
Import Device Setting Information	Import Device Setting Information	Log of when a device setting information file is imported.
Export Device Setting Information	Export Device Setting Information	Log of when a device setting information file is exported.
Creating/Deleting Folders	Creating/Deleting Folders	Log reporting when folders are created and deleted.
Stored File Editing	Stored File Editing	Log for editing a file
Insertion into another File	Insertion into another File	Log for inserting a file into another file

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.

The first log made following power on is the "Firmware: Structure" log.

Eco-friendly log information items

Eco-friendly Log Item	Log Type Attribute	Content
Main Power On	Main Power On	Log of when the main power switch is turned on.

Eco-friendly Log Item	Log Type Attribute	Content
Main Power Off	Main Power Off	Log of when the main power switch is turned off.
Power Status Transition Result	Power Status Transition Result	Log of the results of transitions in power status.
Job Related Information	Job Related Information	Log of job-related information.
Paper Usage	Paper Usage	Log of the amount of paper used.
Power Consumption	Power Consumption	Log of power consumption.

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 Names of Job Logs and Access Logs: "machine name +_log.csv"
- File names for Eco-friendly Logs: "machine name+_ecolog.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.

Differences in log data formatting

- Job log

  Multiple lines appear in the order of common items (job log and access log), 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
1	20XX-12-03T15:43:03.0	···	Completed	···			···			···	
2		···	Completed	···		Report	···			···	
3		···	Completed	···			···		Print	···	

CJD022

1. **Common items**

   Each item in the common items is displayed on a separate line.

2. **Source**

   "Result" and "Status" in the common items and the job log input entry appear.

   If there are multiple sources, multiple lines appear.

3. **Target**

   "Result" and "Status" in the common items and the job log output entry appear.

   If there are multiple targets, multiple lines appear.

- Access log

  The common items and access log entries appear on separate lines.

- Eco-friendly log

  Eco-friendly log entries appear on separate lines.

Common items (Job log and Access log)

Start Date/Time

Indicates the start date and time of an operation or event.

End Date/Time

Indicates the end date and time of an operation or event.

Log Type

Details of the log type.

For details about the information items contained in each type of log, see page 192 "Logs That Can Be Managed Using Web Image Monitor".

Result

Indicates the result of an operation or event.

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" (Job logs) and "File Storing" and "Stored File Deletion" (Access logs).

Value	Content
Succeeded	The operation or event completed successfully.
Failed	The operation or event was unsuccessful.
<Blank>	The operation or event is still in progress.

Operation Method

Indicates the operation procedure.

Value	Content
Control Panel	Control panel
Driver	Driver
Utility	Utility
Web	Web
Email	E-mail

Status

Indicates the status of an operation or event.

Value	Content
Completed	The operation or event completed successfully on a job log entry.
Failed	The operation or event was unsuccessful on a job log entry.
Succeeded	The operation or event completed successfully on an access log entry.
Password Mismatch	An access error has occurred because of a password mismatch.
User Not Programmed	An access error has occurred because the user is not registered.
Other Failures	An access error has occurred because of an unspecified failure.
User Locked Out	An access error has occurred because the user is locked out.
File Limit Exceeded	An access error has occurred because the file limit has been exceeded.
Transfer Cancelled	An access error has occurred because of a transfer cancellation.
Power Failure	An access error has occurred because of a power failure.

Value	Content
Lost File	An access error has occurred because the file has been lost.
Functional Problem	An access error has occurred because of a functional problem.
Communication Failure	An access error has occurred because of a communication failure.
Communication Result Unknown	An access error has occurred because of an unknown communication result.
Failure in some or all parts	Clearing user-specific counter or all-user counter failed.
Importing/Exporting by Other User	Importing or exporting is executing by another user.
Connection Failed with Remote Machine	A connection to an output destination failed.
Write Error to Remote Machine	An error occurred in writing to an output destination.
Specified File: Incompatible	The specified file is incompatible.
Specified File: Format Error	A format error occurred with the specified file.
Specified File: Not Exist	The specified file cannot be found.
Specified File: No Privileges	There are no privileges for operating the specified file.
Specified File: Access Error	An error occurs in accessing the specified file.
Memory Storage Device Full	The external media is full.
Memory Storage Device Error	An abnormality is found in the external media.
Encryption Failed	Encryption failed.
Decoding Failed	Decoding failed.
Common Key Not Exist	There are no common keys.
Connection Error	A communication error occurred.
Processing	The job is being processed.
Error	An error has occurred.
Suspended	The job has been suspended.

Cancelled: Details

Indicates the status in which the operation or event was unsuccessful.

Value	Content
Cancelled by User	A user canceled an operation.
Input Failure	It terminated abnormally during input.
Output Failure	It terminated abnormally during output.
Other Error	An error is detected prior to execution of a job or others.
Power Failure	Power is lost.
External Charge Unit Disconnected	The accounting device is unplugged during operation.
Insufficient No. of Original for Overlay	Pages are missing from a manuscript during execution of the overlaid copying.
Exceed Max. Stored Page (File Storage)	The storage capacity of pages on Document Server is exceeded.
Exceed Max. Stored File (File Storage)	The storage capacity of documents on Document Server is exceeded.
Hard Disk Full (File Storage Memory)	The hard disk capacity on Document Server is exceeded.
Exceeded Max. Email Size	The limit to e-mail size is exceeded.
Exceeded Max. File Size	The size limit for one document is exceeded.
Scanner Error	A read error occurred with the automatic document feed.
Timeout	A time-out occurred.
Exceed Max. Stored Page (Image Area)	The number of pages that can be captured is exceeded.
Hard Disk Full (Image Area)	The hard disk capacity for capture is exceeded.
Specified Folder to Store does not Exist	The specified folder to store cannot be found.
Password for Folder Specified to Store is Incorrect	The password for specified folder to store is incorrect.

Value	Content
Folder is Locked	Folder is locked.
Memory Full	The memory range for processing data becomes full.
Print Data Error	An attempt to use a PDL or a port not configured on the machine has been made.
Data Transfer Interrupted	The following case is recorded; • A different type of driver is used. • A network malfunction occurs.
Over Job Limit	The number of jobs that can be received is exceeded.
Specifying Destination Error	An illegal address or an address with 41 or more digits is specified.
Authentication Failed (Access Restricted)	Device authentication failed.
Exceeded Print Volume Use Limitation	The logged in user exceeds their paper usage limit.
No Privilege	The user does not have permission to access a document or function.
Unavailable Size to Store	The size of paper specified (including irregular sizes) is of a size that cannot be stored.
Transmission Failed (Data Deleted)	A document is deleted or an undelivered document exceeds its wait time and is deleted.
Not Entered Document Password	The password for a document is not input.
Connection Failed with Destination	The specified server or folder is not found.
Authentication Failed with Destination	Authentication with the destination failed.
Transmission Failed with Memory Full	The destination memory is full.

Value	Content
Invalid Device Certificate	The following case is recorded; • There is no device certificate. • Its valid period is elapsed. • If the e-mail address of the administrator and that of the certificate do not match.
Invalid Expiration Date: Destination's Certificate	The valid period of the destination certificate is expired.
Invalid Device/Destination's Certificate	Both the destination certificate and the device certificate are invalid.
Book Function Error	A bookbinding function error has occurred.
Fold Function Error	A folding function error has occurred.
Print Cancelled (Error)	The print job has been cancelled because of a system error.

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.

Value	Content
0x00000000	Indicates other operations
0x00000001 - 0xfffffeff	For general users and user code
0xffffff80	System operations
0xffffff81	System operations, Operations that were performed by non-authenticated users
0xffffff86	Supervisor
0xffffff87	Administrator
0xffffff88	Administrator 1
0xffffff89	Administrator 2
0xffffff8a	Administrator 3
0xffffff8b	Administrator 4

User Code/User Name

Identifies the user code or user name of the user who performed the operation.

If an administrator performed the operation, this ID will contain the login name of that administrator.

Log ID

Identifies the ID that is assigned to the log.

This is a hexadecimal ID that identifies the log.

Access log information items

Access Log Type

Indicates the type of access.

Value	Content
Authentication	User authentication access
Stored File	Stored file access
System	System access
Network Attack Detection/ Encrypted Communication	Network attack or encrypted communication access
Firmware	Firmware verification access
Address Book	Address book access
Device Settings	Changes made to a setting in the User Tools menu.

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 check whether or not the authentication server is available.

The number of server switches is indicated as 0 to 4.

"0" indicates the authentication server is available.

Logout Mode

Mode of logout.

Value	Content
by User's Operation	Manual logout by the user
by Auto Logout Timer	Automatic logout following a timeout

Login Method

Indicates the route by which the authentication request is received.

Value	Content
Control Panel	The login was performed through the control panel.
via Network	The login was performed remotely through a network computer.
Others	The login was performed through another method.

Login User Type

Indicates the type of login user.

Value	Content
User	General user
Guest	Guest user
User Administrator	User administrator
Machine Administrator	Machine administrator
Network Administrator	Network administrator
File Administrator	File administrator
Supervisor	Supervisor
Customer Engineer (Service Mode)	Customer engineer
Others	Login requests from users other than those specified above

Target User Entry ID

Indicates the entry ID of the target user.

This is a hexadecimal ID that indicates users to whom the following settings are applied:

- Lockout
- Password Change

Target User Code/User Name

User code or user name of the user whose data was accessed.

If the administrator's data was accessed, the administrator's user name is logged.

Address Book Registration No.

Indicates the registration number of the user performing the operation.

Address Book Operation Mode

Indicates the method applied for changing the data registered in the Address Book.

Address Book Change Item

Indicates which item in the Address Book is changed.

Address Book Change Request IP Address

Indicates the IP address type (IPv4/IPv6) of the user using the Address Book.

Lockout/Release

Indicates the lockout status.

Value	Content
Lockout	Activation of password lockout
Release	Deactivation of password lockout

Lockout/Release Method

Indicates the method applied for releasing the lockout.

Value	Content
Manual	The machine is unlocked manually.
Auto	The machine is unlocked by the lockout release timer.

Lockout Release Target Administrator

Indicates which administrator(s) is (are) released when releasing the lockout.

Counter to Clear

Indicates which counter is reset for each user.

Export Target

Indicates the settings to be included in the device setting file to be exported.

Value	Content
System Settings	System Settings
Copier Features	Copier Features
Printer Features	Printer Features
Scanner Features	Scanner Features
Program (Copier)	Program (Copier)
Program (Scanner)	Program (Scanner)
Program (Document Server)	Program (Document Server)
Web Image Monitor Setting	Web Image Monitor Setting
Web Service Settings	Web Service Settings
System/Copier SP	System/Copier SP
Scanner SP	Scanner SP
Printer SP	Printer SP

Target File Name

Indicates the name of the device information file to be imported/exported.

Stored File ID

Identifies a created or deleted file.

This is a hexadecimal ID that indicates created or deleted stored files.

Stored File Name

Indicates the name of a created or deleted file.

Delete File Type

Indicates the type of file deletion.

Value	Content
Delete Normal File	Deleting a normal file
Delete Editing File	Deleting a file during editing
Auto Delete	Deleting a file automatically after the prescribed time has passed

Value	Content
Others	Deleting a file for reasons other than those stated above.

Folder Number

Indicates the folder number.

Folder Name

Indicates the folder name.

Creating/Deleting Folders

Indicates the operations performed on folders.

Value	Content
Delete Folder	Folder deleted
New Folder	Folder created

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.

Value	Content
Active	Job log collection setting is enabled.
Inactive	Job log collection setting is disabled.
Not Changed	No changes have been made to the job log collection setting.

Collect Access Logs

Indicates the status of the access log collection setting.

Value	Content
Active	Access log collection setting is enabled.
Inactive	Access log collection setting is disabled.
Not Changed	No changes have been made to the access log collection setting.

Collect Eco-friendly Logs

Indicates the status of the eco-friendly log collection setting.

Value	Content
Active	Eco-friendly log collection setting is enabled.
Inactive	Eco-friendly log collection setting is disabled.
Not Changed	No changes have been made to the eco-friendly log collection setting.

Transfer Logs

Indicates the status of the log transfer setting.

Value	Content
Active	Log transfer setting is enabled.
Inactive	Log transfer setting is disabled.
Not Changed	No changes have been made to the log transfer setting.

Encrypt Logs

Indicates the status of the log encryption setting.

Value	Content
Active	Log encryption setting is enabled.
Inactive	Log encryption setting is disabled.
Not Changed	No changes have been made to the log transfer setting.

Log Type

If a log's collection level setting has been changed, this function indicates details of the change.

Value	Content
Job Log	Job log
Access Log	Access log
Eco-friendly Log	Eco-friendly log

Log Collect Level

Indicates the level of log collection.

Value	Content
Level 1	Level 1
Level 2	Level 2
User Settings	User settings

Encryption/Cleartext

Indicates whether communication encryption is enabled or disabled.

Value	Content
Encryption Communication	Encryption is enabled.
Cleartext Communication	Encryption is disabled.

Machine Port No.

Indicates the machine's port number.

Protocol

Destination protocol.

"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.

Value	Content
Communication Start Request Receiver (In)	The machine received a request to start communication.
Communication Start Request Sender (Out)	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.

Network Attack Status

Indicates the machine's status when network attacks occur.

Value	Content
Violation Detected	An attack on the network was detected.
Recovered from Violation	The network recovered from an attack.
Max. Host Capacity Reached	The machine became inoperable due to the volume of incoming data reaching the maximum host capacity.
Recovered from Max. Host Capacity	The machine became operable again following reduction of the volume of incoming data.

Network Attack Type

Identifies network attack types.

Value	Content
Password Entry Violation	Password entry violation
Device Access Violation	Device access violation

Network Attack Type Details

Indicates details of network attack types.

Value	Content
Authentication Error	Authentication error
Encryption Error	Encryption error

Network Attack Route

Identifies the route of the network attack.

Value	Content
Attack from Control Panel	Attack by an unauthorized operation using the machine's control panel
Attack from Other than Control Panel	Attack by means other than an unauthorized operation using the machine's control panel

Login User Name used for Network Attack

Identifies the login user name that the network attack was performed by.

Add/Update/Delete Firmware

Indicates the method used to add, update, or delete the machine's firmware.

Value	Content
Updated with SD Card	An SD card was used to perform the firmware update.
Added with SD Card	An SD card was used to install the firmware.
Deleted with SD Card	An SD card was used to delete the firmware.
Moved to Another SD Card	The firmware was moved to another SD card.
Updated via Remote	The firmware was updated from a remote computer.
Updated for Other Reasons	The firmware update was performed using a method other than any of the above.

Module Name

Firmware module name.

Parts Number

Firmware module part number.

Version

Firmware version.

Machine Data Encryption Key Operation

Indicates the type of encryption key operation performed.

Value	Content
Back Up Machine Data Encryption Key	An encryption key backup was performed.
Restore Machine Data Encryption Key	An encryption key was restored.
Clear NVRAM	The NVRAM was cleared.
Start Updating Machine Data Encryption Key	An encryption key update was started.
Finish Updating Machine Data Encryption Key	An encryption key update was finished.

Machine Data Encryption Key Type

Identifies the type of the encryption key.

Value	Content
Encryption Key for Hard Disk	Encryption key for hard disk
Encryption Key for NVRAM	Encryption key for NVRAM
Device Certificate	Device certificate

Validity Error File Name

Indicates the name of the file in which a validity error was detected.

Configuration Category

Indicates the categories with changed settings.

Value	Content
User Lockout Policy	User lockout policy
Auto Logout Timer	Auto logout timer
Device Certificate	Device certificate
IPsec	IPsec

Value	Content
Compulsory Security Stamp	Compulsory security stamp
S/MIME	S/MIME
WIM Auto Logout Timer	Web Image Monitor auto logout timer

Configuration Name / Configuration Value

Indicates the attributes of the categories.

Indicates the values of the attributes.

Attribute	Description
Lockout	Whether the lockout is active (Active) or inactive (Inactive) is recorded.
Number of Attempts before Lockout	The number of times a user may enter a login password is recorded.
Lockout Release Timer	Whether the lockout release timer is active (Active) or inactive (Inactive) is recorded.
Lock Out User for	The time until lockout release is recorded.
Auto Logout Timer	Whether Auto Logout Timer is set to (On) or (Off) is recorded.
Auto Logout Timer (seconds)	The time until the auto logout operates is recorded.
Operation Mode	The type of operation is recorded.
Certificate No.	The number of the certificate to be used is recorded.
Certificate No.: IEEE 802.1X (WPA/WPA2)	The number of the certificate for applications is recorded. When a certificate is not used, "Do not Use" is recorded.
Certificate No.: S/MIME	The number of the certificate for applications is recorded. When a certificate is not used, "Do not Use" is recorded.
Certificate No.: IPsec	The number of the certificate for applications is recorded. When a certificate is not used, "Do not Use" is recorded.
Certificate No.: Digital Signature PDF	The number of the certificate for applications is recorded. When a certificate is not used, "Do not Use" is recorded.

Attribute	Description
Certificate No.: Digital Signature PDF/A	The number of the certificate for applications is recorded. When a certificate is not used, "Do not Use" is recorded.
IPsec	Whether IPsec is active (Active) or inactive (Inactive) is recorded.
Encryption Key Auto Exchange: Setting1-4: Remote Address	The remote address is recorded.
Encryption Key Auto Exchange: Setting1-4, Default: Security Level	The security level is recorded. When [Authentication Only] is selected, "Authentication Only" is recorded. When [Authentication and Low Level Encryption] is selected, "Authentication and Low Level Encryption" is recorded. When [Authentication and High Level Encryption] is selected, "Authentication and High Level Encryption" is recorded. When [User Settings] is selected, "User Settings" is recorded.
Encryption Key Auto Exchange: Setting1-4, Default: Authentication Method	The authentication method used for the auto key exchange format is recorded. Either "PSK" or "Certificate" is recorded.
Compulsory Security Stamp	Whether [Compulsory Security Stamp] is set to (On) or (Off) is recorded.
Operation Mode	The mode of operation is recorded.
Scanner: Email Sending	The signature is recorded when the scanner is used for sending e-mail.
Document Server (Utility): Stored File Transferring	The signature is recorded when Document Server (utility) is used for transferring documents stored on it.
WIM Auto Logout Timer (minutes)	Web Image Monitor's auto logout timer log is recorded in increments of one minute.

Destination Server Name

Indicates the name of the destination server to which the tracking information failed to be sent if the log type is "Enhanced Print Volume Use Limitation: Tracking Permission Result".

Indicates the name of the server from which the data export or import request is issued if the log type is import or export of preference information.

HDD Format Partition

Indicates the initial status of each hard disk partition.

Access Result

Indicates the results of logged operations.

Value	Content
Completed	An operation completed successfully.
Failed	An operation completed unsuccessfully.

Job log (source)

Source

Indicates the source of the job file.

Value	Content
Scan File	The job file was scanned.
Stored File	The job file was stored on the hard disk.
Printer	The job file was sent from the printer driver.
Report	The job file was a printed report.

Start Date/Time

Dates and times "Scan File", "Received File" and "Printer" operations started.

End Date/Time

Dates and times "Scan File", "Received File" and "Printer" operations ended.

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.

Stored File Name

Names of "Stored File" files.

Folder Number

Indicates the number of the folder in which the file has been stored.

Folder Name

Indicates the name of the folder in which the file has been stored.

Print File Name

Name of "Printer" files.

Job log (target)

Target

Type of the job target.

Value	Content
Print	Print
Store	Store
Send	Send

Start Date/Time

Dates and times "Print", "Store", and "Send" operations started.

End Date/Time

Dates and times "Print", "Store", and "Send" operations ended.

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

Indicates the name of the stored file when Target Type is "Store".

Folder Number

Indicates the number of the folder in which you have stored the file.

Folder Name

Indicates the name of the folder in which you have stored the file.

Eco-friendly log information items

Start Date/Time

The event start date and time is recorded.

End Date/Time

The event end date and time is recorded.

Log Type

The type of eco-friendly log is recorded.

Value	Content
Main Power On	Main power on
Main Power Off	Main power off
Power Status Transition Result	Power status transition result
Job Related Information	Job related information
Paper Usage	Paper usage
Power Consumption	Power consumption

Log Result

Whether the event has ended or not is displayed.

Value	Content
Completed	Completed
Failed	Failed

Result

The result of the event is recorded.

Value	Content
Succeeded	Succeeded
Failed	Failed

Log ID

Identifies the ID that is assigned to the log. This is a hexadecimal ID that identifies the log.

Power Mode

The power status of the machine (after state transition) is logged.

Value	Content
Standby	Standby status
Low Power	Low power status
Silent	Silent status
HDD On	HDD on status
Engine Off	Engine off status
Controller Off	Controller off status
STR	STR status
Silent Print	Silent print status
Low Power Print	Low power print status
Fusing Unit Off	Fusing unit off status

Log Type

The type of job log is recorded.

Job Interval (seconds)

Indicates the elapsed time from the start of the previous job to the start of the present job.

Job Duration (seconds)

Indicates the elapsed time from the start of a job to its end.

Paper Usage (Large Size)

Indicates the number of one-sided prints per hour on large paper.

Large size means A3 (11 × 17 inches) or larger.

Paper Usage (Small Size)

Indicates the number of one-sided prints per hour on small paper.

Small size means smaller than A3 (11 × 17 inches).

Paper Usage (2 Sided: Large Size)

Indicates the number of two-sided prints per hour on large paper.

Large size means A3 (11 × 17 inches) or larger.

Paper Usage (2 Sided: Small Size)

Indicates the number of two-sided prints per hour on small paper.

Small size means smaller than A3 (11 × 17 inches).

Detected Power

The power consumption status of the machine is measured and registered in the log while the machine is being used.

Value	Content
Controller Standby	Controller standby mode
STR	Suspend to RAM (STR) mode
Main Power Off	The main power is turned off.
Scanning/Printing	Simultaneous scanning and printing
Printing	Machine's printing status
Scanning	Machine's scanning status
Engine Standby	Engine's standby status
Engine Low	Engine's low-power status
Engine Night	Engine's silent status
Engine Total	Machine's total electricity consumption
Fusing Unit Off	Fusing unit off status

Power Consumption(Wh)

Indicates the power consumption in each power state.

Specifying Log Collect Settings

Enable the collection settings for each kind of log and configure the collection level.

Job Log Collect Level

If "Job Log Collect Level" is set to [Level 1], all job logs are collected.

Access Log Collect Level

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.

Eco-friendly Log Collect Level

If "Eco-friendly Log Collect Level" is set to [Level 1], eco-friendly logs are not collected.

If "Eco-friendly Log Collect Level" is set to [Level 2], all eco-friendly logs are collected.

1. **Log in as the machine administrator from Web Image Monitor.**
2. **Point to [Device Management], and then click [Configuration].**
3. **Click [Logs] under "Device Settings".**
4. **Select [Active] for each function: "Collect Job Logs", "Collect Access Logs" and "Collect Eco-friendly Logs".**
5. **Specify the collection level for each function, "Job Log Collect Level", "Access Log Collect Level", and "Eco-friendly Log Collect Level".**

   When a level is changed, the selection status of log details changes according to the level.

   To change individual items of the log details, configure the setting for each item. Even if the collection level is set to [Level 1] or [Level 2], once individual items of the log details are changed, the level changes to [User Settings].
6. **Click [OK].**
7. **"Updating..." appears. Wait for about one or two minutes, and then click [OK].**

   If the previous screen does not reappear after you click [OK], wait for a while, and then click the web browser's refresh button.
8. **Log out.**

Note

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

Specifying Log Encryption

Use the following procedure to enable/disable log encryption.

To encrypt the logs, it is necessary to set the collection setting to active for job log, access log, or eco-friendly log.

If the data stored in the machine has been encrypted, the log files will still be encrypted, regardless of this setting.

1. **Log in as the machine administrator from Web Image Monitor.**
2. **Point to [Device Management], and then click [Configuration].**
3. **Click [Logs] under "Device Settings".**
4. **Select [Active] in the [Encrypt Logs] area under "Common Settings for All Logs".**

   To disable log encryption, select [Inactive].

5. **Click [OK].**

   A confirmation message appears.

6. **Click [OK].**

7. **Log out.**

Downloading Logs

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

To collect logs, set the collection setting for the job log, access log and eco-friendly log to [Active].

This setting can be specified in [Logs] under [Configuration] in Web Image Monitor.

1. **Log in as the machine administrator from Web Image Monitor.**
2. **Point to [Device Management], and then click [Configuration].**
3. **Click [Download Logs] under "Device Settings".**
4. **Click [Logs to Download] and select the type of log to download.**

   The security log includes two kinds of logs: job log and access log.

5. **Click [Download].**
6. **Specify the folder in which you want to save the file.**
7. **Click [Back].**
8. **Log out.**

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.
- For details about the items contained in the logs, see page 197 "Attributes of Logs You Can Download".

Number of Logs That Can Be Kept on the Machine

When the maximum number of job log, access log or eco-friendly log that can be kept on the machine is exceeded and new logs are generated, old logs are overwritten by new ones. If the logs are not downloaded periodically, it may not be possible to record the old logs onto files.

When using Web Image Monitor to manage logs, download the logs at an interval appropriate to the conditions in the table.

After downloading the logs, perform a batch deletion of the logs.

If you change the [Collect] / [Do not Collect] setting for log collection, you must perform a batch deletion of the logs.

Maximum number of logs that can be stored in the machine

Log types	Maximum number of logs
Job logs	4000
Access logs	12000
Eco-friendly logs	4000

Estimated number of logs created per day

Log types	Number of logs created per day
Job logs	100
Access logs	300 This number is based on 100 operations such as initialization and access operations over the Web, and 200 job entries (two entries per job: one login and one logout).
Eco-friendly logs	100

According to these conditions, the machine can maintain logs for 40 days without overwriting, but to be cautious, we recommend downloading after half that time, 20 days, to leave room for error.

Manage downloaded log files appropriately under the responsibility of the machine administrator.

Note

- 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

If the number of logs that can be stored on the machine exceeds the specified maximum limit, old logs are overwritten by new logs. The maximum number of logs that can be stored is defined for each of the job log, access log and eco-friendly log.

The job log and access log are downloaded as one file.

"If logs are downloaded without overwriting" below indicates that the job log and access log are mixed after download.

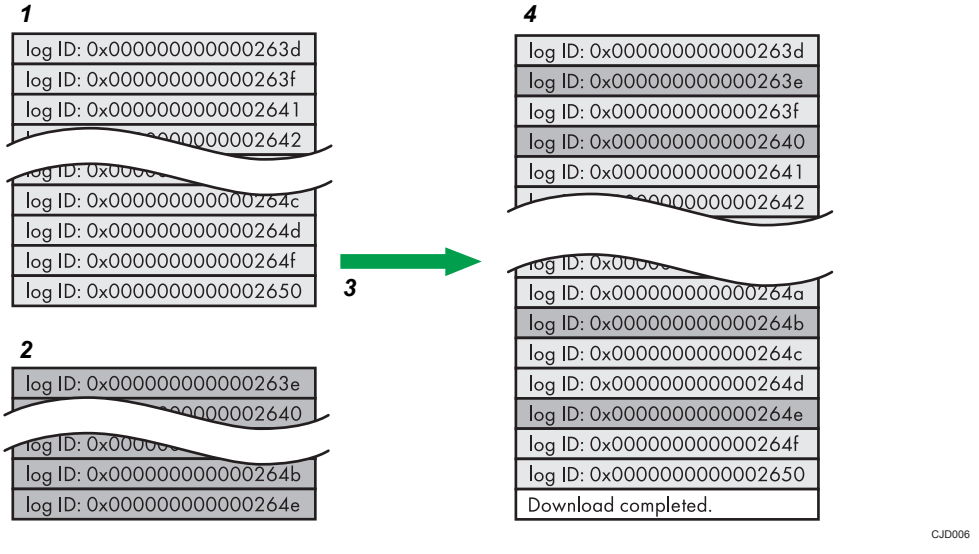
"If logs are downloaded during overwriting" below indicates that part of the access log is overwritten.

In this example, part of the access log is overwritten by a downloaded log and deleted.

The eco-friendly log is downloaded as an independent file.

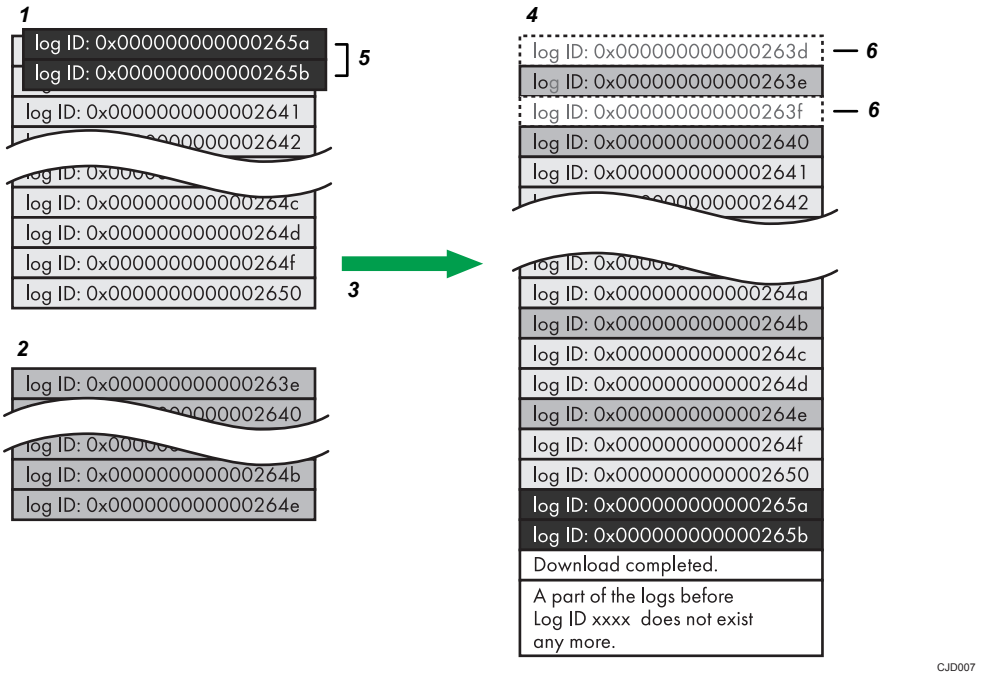
Log entries are overwritten in the order of priority. Log entries with higher priority will not be overwritten or deleted.

If logs are downloaded without overwriting



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

If logs are downloaded during overwriting



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

- If overwriting has occurred, a part of the logs will have been erased by the overwriting, so check the log "Log ID xxxx" and more recent logs.

Printer Job Logs

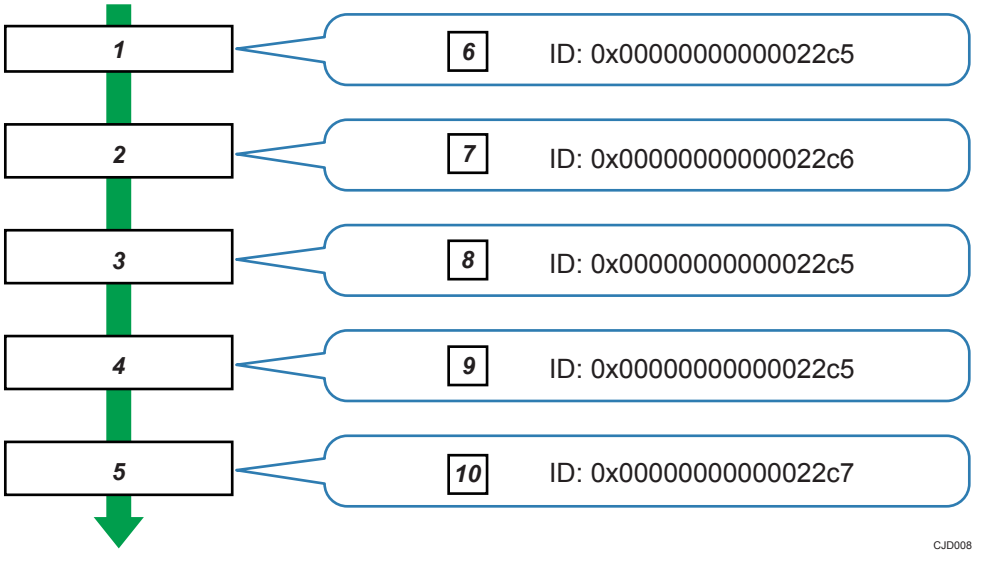
Print Log entries are made before the login entry is made in the Access Log.

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.**

Deleting All Logs

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

"Delete All Logs" appears if one of the job log, access log, or eco-friendly log is set to [Active].

1. **Log in as the machine administrator from Web Image Monitor.**
2. **Point to [Device Management], and then click [Configuration].**
3. **Click [Logs] under "Device Settings".**
4. **Click [Delete] under "Delete All Logs".**
5. **Click [OK].**
6. **Log out.**

Disabling Log Transfer to the Log Collection Server

Use the following procedure to disable log transfer to the log collection server. Note that you can switch the log transfer setting to [Inactive] only if it is already set to [Active].

1. **Log in as the machine administrator from Web Image Monitor.**
2. **Point to [Device Management], and then click [Configuration].**
3. **Click [Logs] under "Device Settings".**
4. **Select [Inactive] in the [Transfer Logs] area under "Common Settings for All Logs".**
5. **Click [OK].**
6. **Log out.**

Managing Logs from the Machine

You can specify settings such as whether or not to transfer logs to the log collection server and whether or not to delete all logs.

Disabling Log Transfer to the Log Collection Server

Use the following procedure to disable log transfer from the machine to the log collection server. Note that you can switch the log transfer setting to [Off] only if it is already set to [On].

For details about the log collection server, contact your sales representative.

For details about the transfer log setting, see the log collection server manual.

1. **Log in as the machine administrator from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **When using Type 1, 2, or 3, press [▼Next] three times. When using Type 4 or 5, press [▼Next] twice.**
5. **Press [Transfer Log Setting].**
6. **Press [Off].**
7. **Press [OK].**
8. **Log out.**

Specifying Delete All Logs

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

Deleting all logs from the machine as a batch can be achieved only if the log collection server is in use or if the Web Image Monitor setting has been specified to collect job log, access log or eco-friendly log.

1. **Log in as the machine administrator from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼Next] three times.**
5. **Press [Delete All Logs].**
6. **Press [Yes].**
7. **Press [Exit].**
8. **Log out.**

Managing Logs from the Log Collection Server

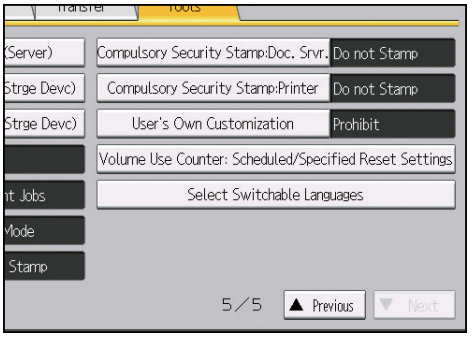
For details about using the log collection server to manage Log Files, see the manual supplied with the log collection server.

Configuring the Home Screen for Individual Users

This allows each user to use their own home screen.

When a user logs in, their personalized home screen is displayed.

1. **Log in as the machine administrator from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **When using Type 1, 2, or 3, press [▼Next] four times. When using Type 4 or 5, press [▼Next] three times.**
5. **Press [User's Own Customization].**



6. **Press [Allow], and then press [OK].**
7. **Log out.**

Note

- This can also be configured from Web Image Monitor. For details, see Web Image Monitor Help.
- The home information for each user is maintained even when "User's Own Customization" is set to [Prohibit]. When the setting is changed back to [Allow], the information can be used again.

Warnings About Using User's Own Home Screens

Consider these warnings before using this function.

- When a user is registered in the Address Book, a home screen is created for that user. At that time, their user's own home screen is configured with the default settings (arrangement of icons).
- If Menu Protect is set to either [Level 1] or [Level 2], the user cannot use that function's program registration, editing or delete. However, there is no restriction on adding icons to the user's own home screen.

- When Menu Protect has been set to [Level 1] or [Level 2], have the administrator create any necessary programs.
- Only the icons of functions an administrator has permitted to be used are displayed.
- When a user is deleted from the Address Book, that user's home screen information is also deleted.
- When a user has edited a program, the changes are reflected to all the users who have the program's icon distributed to their own home screen.
- When a user deletes a program, the icon of the program is deleted from all the user's home screens to which it is distributed.
- Because each user manages and uses their own home screen, the administrator cannot check each user's own home information (customized state of users' own home screens).

Managing Device Information

⚠CAUTION

- Keep SD cards or USB flash memory devices out of reach of children. If a child accidentally swallows an SD card or USB flash memory device, consult a doctor immediately.

The machine's device information can be set by an administrator with privileges to manage everything — devices, users, networks and files.

The machine's device information can be exported to an external device as a device setting information file. By importing an exported device setting information file to the machine, you can use it as a backup file to restore device settings.

You can use the copy function, Document Server function, and scanner function on Type 1, 2, or 3 machines only.

Data that can be imported and exported

- Copier / Document Server Features
- Printer Features
- Scanner Features
- Program (Document Server)
- Program (Copier)
- Program (Scanner)
- Web Image Monitor Setting
- Web Service Settings
- System Settings

Data that cannot be imported or exported

- Some System Settings *1 *2

*1 The setting for the date, settings that require the device certificate, and settings that need to be adjusted for each machine (for example, image adjustment settings) cannot be imported or exported.

*2 Settings only for executing functions and settings only for viewing cannot be imported or exported.

- Extended Feature Settings
- Address book
- Programs (printer function)
- User stamp in Copier / Document Server Features
- Settings that can be specified via telnet
- @Remote-related data
- Counters

- EFI printer unit settings
- Settings that can only be specified via Web Image Monitor or Web Service (for example, Bonjour, SSDP setting)

Note

- The file format for exports is CSV.
- The device configuration of the machine importing the device setting information file must be the same as that of the machine, which exported the device setting information file. Otherwise, the device setting information file cannot be imported.
- Import/export is possible between machines only if their models, region of use, and the following device configuration match.
  - Input Tray
  - Output Tray
  - Whether or not equipped with the duplex function
  - Whether or not equipped with a finisher and the type of finisher
  - Whether or not equipped with a hard disk
- If the device configuration is changed, export the updated device setting information file.
- If there are machines with the same device configuration, you can specify their settings identically by importing the same device setting file.
- If the home screen contains JPG image files, they will also be exported.
- While a user is operating the machine, nothing can be imported or exported until the user completes the operation.
- During export and import, the machine cannot be otherwise operated.
- For details about SD card handling, see "Inserting/Removing a Memory Storage Device", Getting Started.

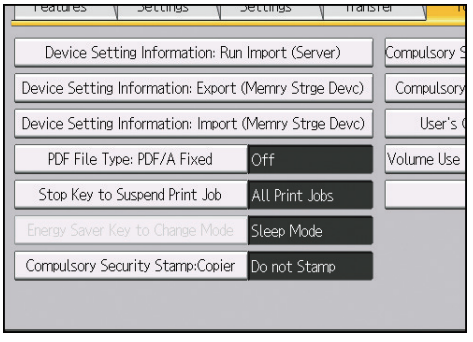
Exporting Device Information

When exporting device information from the control panel, the data is saved on an SD card.

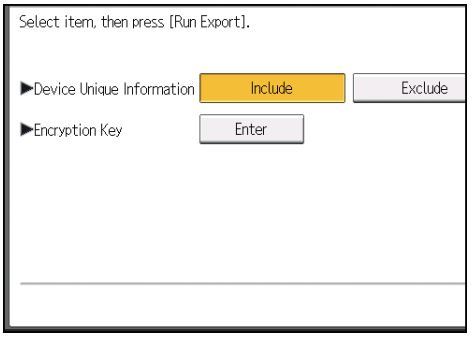
1. **Insert an SD card into the media slot on the side of the control panel.**

   For details about inserting the SD card, see "Inserting/Removing a Memory Storage Device", Getting Started.
2. **Log in from the control panel as an administrator with all privileges.**
3. **Press [System Settings].**
4. **Press [Administrator Tools].**

5. **When using Type 1, 2, or 3, press [▼Next] four times. When using Type 4 or 5, press [▼Next] twice.**
6. **Press [Device Setting Information: Export (Memry Strge Devc)].**



7. **Set the export conditions.**



- Specify whether to [Include] or [Exclude] the "Device Unique Information". "Device Unique Information" includes the IP address, host name, etc.
- Specify an encryption key.

8. **Press [Run Export].**
9. **Press [OK].**
10. **Press [Exit].**
11. **Log out.**

Note

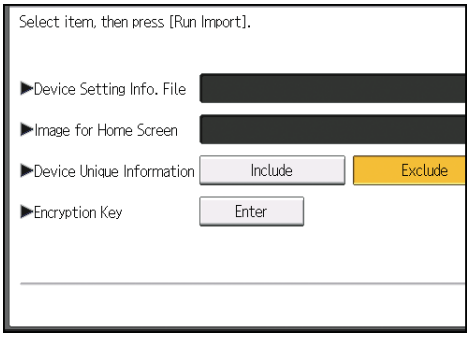
- If import or export fails, you can check the log for the error. The log is stored in the same location as the exported device setting information file.

Importing Device Information

Import device information saved on an SD card.

1. **Insert an SD card into the media slot on the side of the control panel.**

   For details about inserting the SD card, see "Inserting/Removing a Memory Storage Device", Getting Started.
2. **Log in from the control panel as an administrator with all privileges.**
3. **Press [System Settings].**
4. **Press [Administrator Tools].**
5. **When using Type 1, 2, or 3, press [▼Next] four times. When using Type 4 or 5, press [▼Next] twice.**
6. **Press [Device Setting Information: Import (Memry Strge Devc)].**
7. **Configure the import conditions.**



   - Press [Select] of the "Device Setting Info. File" to select the file(s) to import.
   - When adding an image to a home screen, press [Select] for "Image for Home Screen", and then select the file.
   - Specify whether to [Include] or [Exclude] the "Device Unique Information". "Device Unique Information" includes the IP address, host name, etc.
   - Enter the encryption key that was specified when the file was exported.
8. **Press [Run Import].**
9. **Press [OK].**
10. **Press [Exit].**

    The machine restarts.

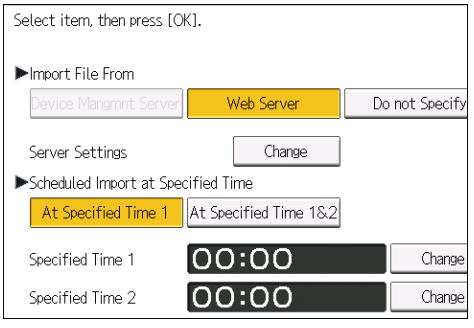
Note

- If import or export fails, you can check the log for the error. The log is stored in the same location as the exported device setting information file.

Periodically Importing Device Information

This setting automatically import the device information stored on a server into the machine.

1. **Log in from the control panel as an administrator with all privileges.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press ▼[Next] 3 times.**
5. **Press [Device Setting Information: Import Setting (Server)].**
6. **Configure the import conditions.**



- Select the source for importing files. Configure settings such as the URL, user name, password, etc., using the detail settings of the server.
- Select the frequency for importing device setting information files and set the time used for a periodic import at the specified time.
- Select whether or not to import a device setting information file if it is identical as compared to the last imported file.
- When the device setting information file to be imported is encrypted, configure an encryption key.
- Select whether or not to send e-mail notification to the machine administrator when importing fails.

7. **Press [OK].**
8. **Log out.**

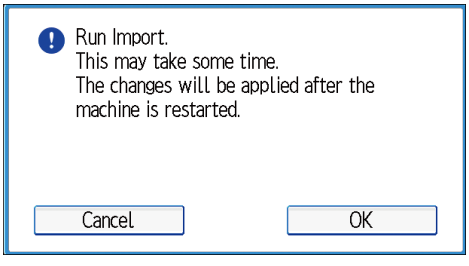
Note

- This can also be configured from Web Image Monitor. For details, see Web Image Monitor Help.
- When the managing device server is used, more detailed import settings can be made. For further details, refer to the user's manual of the managing device server.
- If import or export fails, you can check the log for the error. The log is stored in the same location as the exported device setting information file.

Manually Importing the Device Setting Information File of a Server

Manually import into the machine the device setting information file specified with [Device Setting Information: Import Setting (Server)].

1. **Log in from the control panel as an administrator with all privileges.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press ▼[Next] 4 times.**
5. **Press [Device Setting Information: Run Import (Server)].**
6. **Press [OK].**



7. **Press [Exit].**

   The machine restarts.

Note

- If import or export fails, you can check the log for the error. The log is stored in the same location as the exported device setting information file.

Troubleshooting

If an error occurs, check the log's result code first. Values other than 0 indicate that an error occurred. The result code will appear in the circled area illustrated below.

Example of a log file

CJD023

If you cannot solve the problem or do not know how to solve it after checking the code, write down the error log entry, and then contact your service representative.

ResultCode	Cause	Solutions
2 (INVALID REQUEST)	A file import was attempted between different models or machines with different device configurations.	Import files exported from the same model with the same device configurations.
4 (INVALID OUTPUT DIR)	Failed to write the device information to the destination device.	Check whether the destination device is operating normally.
7 (MODULE ERROR)	An unexpected error has occurred during an import or export.	Turn the power off and then back on, and then try the operation again. If the error persists, contact your service representative.
8 (DISK FULL)	The available storage space on the external medium is insufficient.	Execute the operation again after making sure there is enough storage space.
9 (DEVICE ERROR)	Failed to write or read the log file.	Check whether the path to the folder for storing the file or the folder in which the file is stored is missing.

ResultCode	Cause	Solutions
10 (LOG ERROR)	Failed to write the log file. The hard disk is faulty.	Contact your service representative.
20 (PART FAILED)	Failed to import some settings.	The reason for the failure is logged in "NgName". Check the code. **Reason for the Error (NgName)** 2 INVALID VALUE The specified value exceeds the allowable range. 3 PERMISSION ERROR The permission to edit the setting is missing. 4 NOT EXIST The setting does not exist in the system. 5 INTERLOCK ERROR The setting cannot be changed because of the system status or interlocking with other specified settings. 6 OTHER ERROR The setting cannot be changed for some other reason.
21 (INVALID FILE)	Failed to import the file because it is in the wrong format in the external medium.	Check whether the file format is correct. The log is in the form of a CSV file.
22 (INVALID KEY)	The encryption key is not valid.	Use the correct encryption key.

Managing Eco-friendly Counter

When user authentication is being used, information on the eco-friendly counter is displayed at login.

The eco-friendly counter displays the ratio of use of duplex and combine printing to the total number of printed sheets.

How much toner and paper are being saved is indicated by the eco-friendly index. Higher eco-friendly index leads to greater resource saving.

Note

- When Basic, Windows, LDAP or Integration Server authentication is used for user authentication, the machine compiles the data and displays the eco-friendly counter for each user.
- When user code authentication is used for user authentication, or when user authentication is not in use, the machine compiles the data and displays it's overall eco-friendly counter.

Configuring the Display of Eco-friendly Counters

Set up the period for collecting data for the eco-friendly counter and an administrator's message.

1. **Log in as the machine administrator from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **When using Type 1, 2, or 3, press [▼Next].**
5. **Press [Eco-friendly Counter Period / Administrator Message].**
6. **Change the settings.**
7. **Press [OK].**
8. **Press [Exit].**
9. **Log out.**

Count Period

Set up the period for collecting data for the eco-friendly counter.

When [Specify Days] is selected, data for the eco-friendly counter is compiled for each number of days specified.

Default: [Do not Count]

Administrator Message

Select the message to be displayed when a user logs in.

If you select "Fixed Message", a preset message is displayed.

If you select "User Message", the machine administrator can enter a message to be displayed.

Default: [Fixed Message]

Display Information Screen

Specify whether or not to display the information screen at user login.

Default: [Off]

Display Time

Specify the timing for displaying the information screen.

Default: [Every Time Login]

Clearing a Machine's Eco-friendly Counter

A machine's eco-friendly counter can be cleared.

1. **Log in as the machine administrator from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [Display / Clear Eco-friendly Counter].**
5. **Press [Clear Current Value] or [Clear Crnt. & Prev. Val.].**
6. **Press [OK].**
7. **Log out.**

Clearing Users' Eco-friendly Counters

By clearing the users' eco-friendly counter, all users' eco-friendly counters are cleared.

1. **Log in as the machine administrator from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [Display / Clear Eco-friendly Counter per User].**
5. **Press [Clear Current Value] or [Clear Crnt. & Prev. Val.].**
6. **Press [OK].**
7. **Log out.**

Managing the Address Book

Specifying Auto Deletion of Address Book Data

Specify how the machine handles a request for auto registration after the registered data in the address book has reached the limit.

If you set this to [On], new user accounts are added by automatically deleting old user accounts. Accounts that have not been used for the longest time are deleted first.

If you set this to [Off], old user accounts are not deleted, so new user accounts cannot be added once the limit has been reached.

1. **Log in as the user administrator from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [Auto Delete User in Address Book].**
5. **Select [On], and then press [OK].**
6. **Log out.**

Note

- The data is automatically deleted only when the machine receives a request for data registration. Auto deletion is not executed if user accounts are manually added.
- Only user accounts with user codes or login user names and passwords will be automatically deleted.

Deleting All Data in the Address Book

You can delete all the data registered in the Address Book.

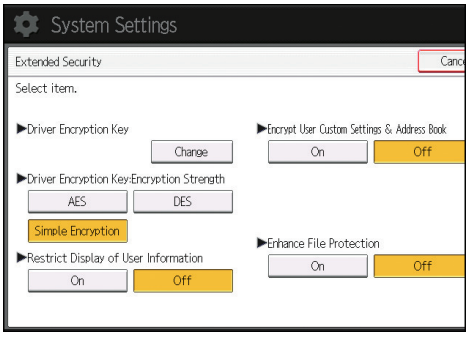
1. **Log in as the user administrator from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [Delete All Data in Address Book].**
5. **Press [Yes], and then press [Exit].**
6. **Log out.**

Specifying the Extended Security Functions

In addition to providing basic security through user authentication and each administrator's specified limits to access the machine, security can also be increased by encrypting transmitted data and data in the Address Book.

You can specify the items for the Document Server function and the scanner function on Type 1, 2, or 3 machines only.

1. **Log in from the control panel as an administrator with privileges.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼Next].**
5. **Press [Extended Security].**
6. **Press the setting you want to change, and change the settings.**



7. **Press [OK].**
8. **Log out.**

Note

- The operation privileges of an administrator differs depending on the setting.

Driver Encryption Key

This can be specified by the network administrator.

Specify the string of text for decrypting the login passwords or file passwords sent from the driver when user authentication is ON.

To specify the driver encryption key, register the encryption key specified using the machine in the driver.

For details, see page 160 "Specifying a Driver Encryption Key".

Driver Encryption Key:Encryption Strength

This can be specified by the network administrator.

Specify the encryption strength for sending jobs from the driver to the machine.

The machine confirms the encryption strength of the password appended to a job and processes it.

If [Simple Encryption] is specified, all jobs that pass user authentication are accepted.

If [DES] is specified, jobs encrypted with DES or AES are accepted.

If [AES] is specified, jobs encrypted with AES are accepted.

If you select [AES] or [DES], specify the encryption settings using the printer driver. For details about specifying the printer driver, see the printer driver Help.

Default: [**Simple Encryption**]

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 Device Manager NX Lite, 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**]

Encrypt User Custom Settings & Address Book

This can be specified by the user administrator.

Encrypt the individual settings of the machine's users and the data in the Address Book.

Even if information on an internal part has been leaked, encryption prevents the individual user settings or the Address Book data from being read.

For details, see page 89 "Protecting the Address Book".

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.

When "Enhance File Protection" is specified, () appears in the lower right corner of the screen.

The locked files can only be unlocked by the file administrator.

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

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, see page 71 "Restricting Usage of the Destination List".

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.].

Also, note that even if you set these functions to [On], users registered in the address book can change their passwords. Only the user administrator can change items other than the password.

Default: [Off]

Settings by SNMPv1, v2

This can be specified by the network administrator.

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

Default: [Do not Prohibit]

Authenticate Current Job

This 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 [Access Privilege] is specified, any user who performed a copy or print job can cancel the job. Also, the machine administrator can cancel the user's copy or print job.

Even if you select [Login Privilege] and log on to the machine, you cannot cancel a copy or print job that is being processed if you are not privileged 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.

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], Minimum required number of characters not specified

@Remote Service

This can be specified by the machine administrator.

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

When setting it to [Prohibit], consult with your service representative.

If it is set to [Proh. Some Services], it becomes impossible to change settings via a remote connection, providing optimally secure operation.

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 a 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, disable administrator authentication. When administrator authentication is enabled again, you can return the setting to [Do not Prohibit].

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

Default: [**Do not Prohibit**]

Password Entry Violation

This can be specified by the machine administrator.

If the number of authentication requests exceeds the setting, the system classifies the access session as a password attack. The access session is recorded in the Access Log and the log data is sent to the machine administrator by e-mail.

If the "Max. Allowed No. of Access" is set to [0], password attacks are not detected.

- Max. Allowed No. of Access

  Specify the maximum number of allowable authentication attempts.

  Use the number keys to enter the number between "0" and "100", and then press [#].

  Default: [**30**]

- Measurement Time

  Specify the interval to count the number of repeated failed authentication attempts. When the measurement time is over, the logged counts of failed authentication attempts are cleared.

  Use the number keys to enter the time between "1" and "10", and then press [#].

  Default: [**5**]

Note

- Depending on the values of the settings for [Max. Allowed No. of Access] and [Measurement Time], you may frequently receive violation detection e-mail.
- If violation detection e-mail is received frequently, check the content and review the setting values.

Security Setting for Access Violation

This can be specified by the machine administrator.

When logging in to the machine via a network application, a user may be locked out erroneously because the number of authentication attempts of the user does not match the number of attempts logged internally.

For example, access may be denied when a print job for multiple sets of pages is sent from an application.

If you select [On] under "Security Setting for Access Violation", you can prevent such authentication errors.

- On
  - Denial Durtn. for Accs. Viol.

    Specify the time to limit repeated access by a user.

    Use the number keys to enter the time between "0" and "60", and then press [#].

    Default: [15]
  - Managed User Host Limit

    Specify the number of user accounts to manage under "Security Setting for Access Violation".

    Use the number keys to enter the number between "50" and "200", and then press [#].

    Default: [200]
  - Password Entry Host Limit

    Specify the number of passwords to manage under "Security Setting for Access Violation".

    Use the number keys to enter the number between "50" and "200", and then press [#].

    Default: [200]
  - Status Monitor Interval

    Specify the monitoring interval of "Managed User Host Limit" and "Password Entry Host Limit".

    Use the number keys to enter the time between "1" and "10", and then press [#].

    Default: [3]
- Off

Default: [Off]

Device Access Violation

This can be specified by the machine administrator.

If the number of log in requests exceeds the setting, the system classifies the access session as an access violation. The access session is recorded in the Access Log and the log data is sent to the machine administrator by e-mail. Also, a message is displayed on the control panel and on Web Image Monitor.

If the "Max. Allowed No. of Access" is set to [0], over access is not detected.

In "Authentication Delay Time", you can specify response delay time for log-in requests to prevent the system from becoming unavailable when an access violation is detected.

In "Simultns. Access Host Limit", you can specify the limit number of hosts accessing the machine at one time. If the number of access exceeds the setting, monitoring becomes unavailable and the detected unavailability is recorded in the Log.

- Max. Allowed No. of Access

  Specify the maximum number of allowable access attempts.

  Use the number keys to enter the number between "0" and "500", and then press [#].

  Default: [100]

- Measurement Time

  Specify the interval to count the number of excessive access. When the measurement time is over, the logged counts of access are cleared.

  Use the number keys to enter the number between "10" and "30", and then press [#].

  Default: [10]

- Authentication Delay Time

  Specify the authentication delay time when an access violation is detected.

  Use the number keys to enter the number between "0" and "9", and then press [#].

  Default: [3]

- Simultns. Access Host Limit

  Specify the number of acceptable authentication attempts when authentications are delayed due to an access violation.

  Use the number keys to enter the number between "50" and "200", and then press [#].

  Default: [200]

Note

- Depending on the values of the settings for [Max. Allowed No. of Access] and [Measurement Time], you may frequently receive violation detection e-mail.
- If violation detection e-mail is received frequently, check the content and review the setting values.

Other Security Functions

This is an explanation of the settings for preventing leakage of information.

It also explains the functions that are restricted when user authentication is used.

Scanner Function

You can use the scanner function on Type 1, 2, or 3 machines only.

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, select [Print Scanner Journal] or [Delete Scanner Journal]. To print the scanner journal automatically, set [Print and Delete All] for "Print & Delete Scanner Journal".

For details, see "Scanner Features", Scan.

WSD scanner function

WSD scanner function is automatically disabled when user authentication is specified. Even if automatically disabled, it can be enabled from "Initial Settings" available in Web Image Monitor.

For details, see "Preparing to Use WSD Scanner (Push Type)" and "Preparing to Use WSD Scanner (Pull Type)", Scan.

System Status

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

Confirming Firmware Validity

When the machine starts up, this function verifies the validity of its firmware.

If an error occurs during the verification, a verification error is displayed on the control panel.

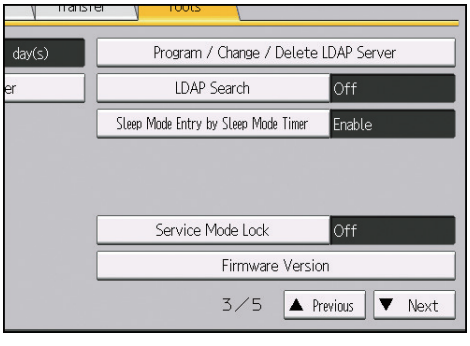
Note that this can also be checked on Web Image Monitor after startup of the machine. If an error occurs in the verification of Web Image Monitor itself, Web Image Monitor cannot be used, so check the display on the control panel.

Restricting a Customer Engineer Operation

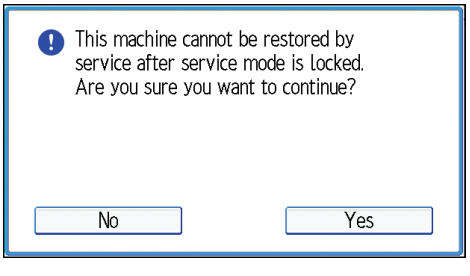
You can restrict the customer engineer's access to the service mode.

Service mode is used by a customer engineer 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 a customer engineer to operate the machine for inspection and repair. This ensures that the inspection and repair are done under the supervision of the machine administrator.

1. **Log in as the machine administrator from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼Next] twice.**
5. **Press [Service Mode Lock].**



6. **Press [On], and then press [OK].**
7. **Press [Yes].**



8. **Log out.**

Additional Information for Enhanced Security

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

You can specify the items for the scanner function and S/MIME on Type 1, 2, or 3 machines only.

Settings You Can Configure Using the Control Panel

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

System Settings

Tab	Item	Setting
Timer Settings	Auto Logout Timer	On: 180 seconds or less. See page 67 "Auto Logout".
Administrator Tools	User Authentication Management	Select [Basic Auth.], and then set "Printer Job Authentication" to [Entire]. See page 35 "Basic Authentication".
Administrator Tools	Administrator Authentication Management→User Management	Select [On], and then select [Administrator Tools] for "Available Settings". See page 13 "Configuring Administrator Authentication".
Administrator Tools	Administrator Authentication Management→Machine Management	Select [On], and then select each of "Available Settings". See page 13 "Configuring Administrator Authentication".
Administrator Tools	Administrator Authentication Management→Network Management	Select [On], and then select [Interface Settings], [File Transfer], and [Administrator Tools] for "Available Settings". See page 13 "Configuring Administrator Authentication".
Administrator Tools	Administrator Authentication Management→File Management	Select [On], and then select [Administrator Tools] for "Available Settings". See page 13 "Configuring Administrator Authentication".

Tab	Item	Setting
Administrator Tools	Extended Security→ Settings by SNMPv1, v2	Prohibit See page 243 "Specifying the Extended Security Functions".
Administrator Tools	Extended Security→Driver Encryption Key:Encryption Strength	AES See page 243 "Specifying the Extended Security Functions"
Administrator Tools	Extended Security→ Authenticate Current Job	Access Privilege See page 243 "Specifying the Extended Security Functions"
Administrator Tools	Extended Security→ Password Policy	"Complexity Setting": Level 1 or higher, "Minimum Character No.": 8 or higher See page 243 "Specifying the Extended Security Functions"
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 page 114 "Specifying Network Security Level".
Administrator Tools	Service Mode Lock	On See page 251 "Restricting a Customer Engineer Operation".
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 page 93 "Encrypting Data on the Hard Disk".

Scanner Features

Tab	Item	Setting
Initial Settings	Menu Protect	Level 2 See page 74 "Specifying Menu Protect".

Note

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

Settings You Can Configure Using Web Image Monitor

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

Category	Item	Setting
Device Settings→Logs	Collect Job Logs	Active
Device Settings→Logs	Collect Access Logs	Active
Security→User Lockout Policy	Lockout	Active For details, see page 65 "User Lockout Function".
Security→User Lockout Policy	Number of Attempts before Lockout	5 times or less. For details, see page 65 "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. For details, see page 65 "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. For details, see page 65 "User Lockout Function".

Category	Item	Setting
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": AES-128 bit, AES-256 bit, or 3DES-168 bit You must register the user certificate in order to use S/MIME.
Address Book→ Detail Input→Add User/Change→ Email	User Certificate	You must register the user certificate in order to use S/MIME.

Note

- The administrator must indicate which strength level is to be specified for the encryption algorithm.
- For details about specifying an encryption algorithm and registering a user certificate, see page 130 "Configuring S/MIME".

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

System Settings

Tab	Item	Setting
Interface Settings	IPsec	Active
Interface Settings	Permit SSL / TLS Communication	Ciphertext Only

Web Image Monitor settings

Category	Item	Setting
Security→IPsec→ Encryption Key Auto Exchange Settings	Edit→Security Level	Authentication and High Level Encryption

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

System Settings

Tab	Item	Setting
Interface Settings	IPsec	Inactive
Interface Settings	Permit SSL / TLS Communication	Ciphertext Only

Note

- You can set "IPsec" and "Permit SSL/TLS Communication" using Web Image Monitor.

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

- Printing with protocols that support encryption

To use the printer functions, specify sftp as the protocol, or specify IPP and enable SSL/TLS.

For details about sftp, see "Printing Files Directly from Windows", Connecting the Machine/ System Settings.

For details about IPP settings, see "Installing the Printer Driver for the Selected Port", Driver Installation Guide.

For details about SSL/TLS settings, see page 124 "Configuring SSL/TLS".

Scanner

- Sending the URL address of stored files

  Send the URL of scanned files to destinations by configuring [Send Settings] in [Scanner Features], instead of sending the actual scanned files. For details, see "Sending the URL by E-mail", Scan.

- Managing scanned files using Web Image Monitor

  Use Web Image Monitor through your network to view, delete, send, and download scanned files.

- S/MIME authentication function

  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 "Security Settings to E-mails", Scan.

Note

- For details about enabling and disabling IPsec using the control panel, see "Interface Settings", Connecting the Machine/ System Settings.
- For details about specifying the IPsec setting via Web Image Monitor, see page 137 "Configuring IPsec".

8. Troubleshooting

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

If a Message is Displayed

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

If a message not shown below is displayed, follow the message to resolve the problem.

"You do not have the privileges to use this function."

The privileges 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 additionally assign the privileges to use the function.

If this appears when trying to specify a machine setting:

- The administrator differs depending on the machine settings you wish to specify.
- Using the list of settings, the administrator responsible must decide whether to additionally assign the privileges to use the function.

"Authentication has failed."

The cause depends on the error code.

For details, see page 261 "If an Error Code is Displayed".

"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, see page 13 "Configuring Administrator Authentication".

"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.

"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 privileges to do so.

- Files can be deleted by the owner or file administrator. To delete a file which you are not privileged to delete, contact the owner.

Note

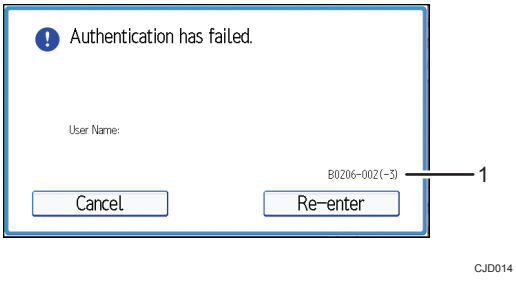
- If a service call message appears, contact your service representative.

If an Error Code is Displayed

When authentication fails, the message "Authentication has failed." appears with an error code. The following lists provide solutions for each error code. If the error code that appears is not on the lists, write down the error code and contact your service representative.

The TWAIN items are displayed on Type 1, 2, or 3 machines only.

Error code display position



1. **Error code**

   An error code appears.

Basic Authentication

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.

- A password error occurred.

  Make sure the password is entered correctly.
- Either [DES] or [AES] is selected for "Driver Encryption Key: Encryption Strength".

  You can make access by specifying the driver encryption key.
- A driver encryption key error occurred.

  Make sure that the encryption key is correctly specified on the driver.

B0206-002 : Case 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 : Case 2

The user attempted authentication from an application on the "System Settings" screen, where only the administrator has authentication ability.

- Only the administrator has login privileges on this screen.
- Log in as a general user from the application's login screen.

B0206-003

An authentication error occurred because the user name contains a space, colon (:), or quotation mark (").

- Recreate the account if the account name contains any of these prohibited characters.
- If the account name was entered incorrectly, enter it correctly and log in again.

B0207-001

An authentication error occurred because the Address Book is being used at another location.

- Wait a few minutes and then try again.

B0208-000 / B0208-002

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

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.

- A password error occurred.

  Make sure the password is entered correctly.
- Either [DES] or [AES] is selected for "Driver Encryption Key: Encryption Strength".

  You can make access by specifying the driver encryption key.
- A driver encryption key error occurred.

  Make sure that the encryption key is correctly specified on the driver.

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.

W0208-000 / W0208-002

The account is locked because you have reached the maximum number of failed authentication attempts allowed.

- Ask the user administrator to unlock the account.

W0400-102

Kerberos authentication failed because the server is not functioning correctly.

- Make sure that the server is functioning properly.

W0400-200

Due to the high number of authentication attempts, all resources are busy.

- Wait a few minutes and then try again.

W0400-202 : Case 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 : Case 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.

W0406-101

Authentication cannot be completed because of the high number of authentication attempts.

- Wait a few minutes and then try again.
- If the situation does not return to normal, make sure that an authentication attack is not occurring.
- Notify the administrator of the screen message by e-mail, and check the system log for signs of an authentication attack.

W0406-107 : Case 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.

W0406-107 : Case 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.

W0406-107 : Case 3

The domain name cannot be resolved.

- Make sure that DNS/WINS is specified in the domain name in "Interface Settings".

W0406-107 : Case 4

Cannot connect to the authentication server.

- Make sure that connection to the authentication server is possible.
- Use the "Ping Command" in "Interface Settings" to check the connection.

W0406-107 : Case 5

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.

W0406-107 : Case 6

A domain name error occurred.

- Make sure that the Windows authentication domain name is specified correctly.

W0406-107 : Case 7

Cannot resolve the domain name.

- Specify the IP address in the domain name and confirm that authentication is successful.

  If authentication was successful:

  - 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".
  - If a NetBIOS domain name is specified in domain name (such as DOMAINNAME), make sure that WINS is specified in "Interface Settings".

  If authentication was unsuccessful:

  - Make sure that Restrict LM/NTLM is not set in either "Domain Controller Security Policy" or "Domain Security Policy".
  - 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 the Windows firewall is activated, create a firewall rule in the Windows firewall's "Advanced settings" to authorize ports 137 and 139.
- 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".

W0406-107 : Case 8

Kerberos authentication failed.

- Kerberos authentication settings are not correctly configured.

  Make sure the realm name, KDC (Key Distribution Center) name and corresponding domain name are specified correctly.
- 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.
- Kerberos authentication will fail if the realm name is specified in lower-case letters. Make sure the realm name is specified in capital letters.
- 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.

W0409-000

Authentication timed out because the server did not respond.

- Check the network configuration, or settings on the authenticating server.

W0511-000

The authentication server login name is the same as a user name already registered on the machine. (Names are distinguished by the unique attribute specified in LDAP authentication settings.)

- Delete the old, duplicated name or change the login name.
- If the authentication server has just been changed, delete the old name on the server.

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.

W0607-001

An authentication error occurred because the Address Book is being used at another location.

- Wait a few minutes and then try again.

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

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.

- A password error occurred.

Make sure the password is entered correctly.

- Either [DES] or [AES] is selected for "Driver Encryption Key: Encryption Strength".

  You can make access by specifying the driver encryption key.

- A driver encryption key error occurred.

  Make sure that the encryption key is correctly specified on the driver.

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.

L0208-000 / L0208-002

The account is locked because you have reached the maximum number of failed authentication attempts allowed.

- Ask the user administrator to unlock the account.

L0307-001

An authentication error occurred because the Address Book is being used at another location.

- Wait a few minutes and then try again.

L0400-210

Failed to obtain user information in LDAP search.

- The login attribute's search criteria might not be specified or the specified search information is unobtainable.
- Make sure the login name attribute is specified correctly.

L0406-003

An authentication error occurred because the user name contains a space, colon (:), or quotation mark (").

- Recreate the account if the account name contains any of these prohibited characters.
- If the account name was entered incorrectly, enter it correctly and log in again.

L0406-200

Authentication cannot be completed because of the high number of authentication attempts.

- Wait a few minutes and then try again.
- If the situation does not return to normal, make sure that an authentication attack is not occurring.
- Notify the administrator of the screen message by e-mail, and check the system log for signs of an authentication attack.

L0406-201

Authentication is disabled in the LDAP server settings.

- Change the LDAP server settings in administrator tools, in "System Settings".

L0406-202 / L0406-203 : Case 1

There is an error in the LDAP authentication settings, LDAP server, or network configuration.

- 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".
- Make sure the LDAP server is specified correctly in the LDAP authentication settings.
- Make sure the login name attribute is entered correctly in the LDAP authentication settings.
- Make sure the SSL settings are supported by the LDAP server.

L0406-202 / L0406-203 : Case 2

A login user name or password error occurred.

- Make sure the login user name and password are entered correctly.
- Make sure a usable login name is registered on the machine.

  Authentication will fail in the following cases:

  If the login user name contains a space, colon (:), or quotation mark (").

  If the login user name exceeds 128 bytes.

L0406-202 / L0406-203 : Case 3

There is an error in the simple encryption method.

- Authentication will fail if the password is left blank in simple authentication mode.

  To allow blank passwords, contact your service representative.
- 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.

- Kerberos authentication settings are not correctly configured.

  Make sure the realm name, KDC (Key Distribution Center) name, and supporting domain name are specified correctly.

- 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.

- Kerberos authentication will fail if the realm name is specified in lower-case letters. Make sure the realm name is specified in capital letters.

L0409-000

Authentication timed out because the server did not respond.

- Contact the server or network administrator.
- If the situation does not return to normal, contact your service representative.

L0511-000

The authentication server login name is the same as a user name already registered on the machine. (Names are distinguished by the unique attribute specified in the LDAP authentication settings.)

- Delete the old, duplicated name or change the login name.
- If the authentication server has just been changed, delete the old name on the server.

L0606-004

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.

L0607-001

An authentication error occurred because the Address Book is being used at another location.

- Wait a few minutes and then try again.

L0612-005

Authentication failed because no more users can be registered. (The number of users registered in the Address Book has reached capacity.)

- Ask the user administrator to delete unused user accounts in the Address Book.

L0707-001

An authentication error occurred because the Address Book is being used at another location.

- Wait a few minutes and then try again.

Integration Server Authentication

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.

- A password error occurred.

  Make sure the password is entered correctly.
- Either [DES] or [AES] is selected for "Driver Encryption Key: Encryption Strength".

  You can make access by specifying the driver encryption key.
- A driver encryption key error occurred.

  Make sure that the encryption key is correctly specified on the driver.

I0206-002

A user attempted authentication from an application on the "System Settings" screen, where only the administrator has authentication ability.

- Only the administrator has login privileges on this screen.
- Log in as a general user from the application's login screen.

I0206-003

An authentication error occurred because the user name contains a space, colon (:), or quotation mark (").

- Recreate the account if the account name contains any of these prohibited characters.
- If the account name was entered incorrectly, enter it correctly and log in again.

I0207-001

An authentication error occurred because the Address Book is being used at another location.

- Wait a few minutes and then try again.

I0208-000 / I0208-002

The account is locked because you have reached the maximum number of failed authentication attempts allowed.

- Ask the user administrator to unlock the account.

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 : Case 1

The URL could not be obtained.

- Obtain the URL using Obtain URL in Integration Server authentication.

I0406-301 : Case 2

A login user name or password error occurred.

- Make sure the login user name and password are entered correctly.
- 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.

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.)

- Delete the old, duplicated name or change the login name.
- If the authentication server has just been changed, delete the old name on the server.

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.

I0607-001

An authentication error occurred because the Address Book is being used at another location.

- Wait a few minutes and then try again.

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.

You can use the copy function, Document Server function, scanner function, and TWAIN driver on Type 1, 2, or 3 machines only.

Condition	Cause	Solution
Cannot perform the following: • Print with the printer driver • Connect with the TWAIN driver	User authentication has been rejected.	Confirm the user name and login name with the administrator of the network in use if using Windows authentication, LDAP authentication, or Integration Server authentication. Confirm with the user administrator if using Basic authentication.
Cannot perform the following: • Print with the printer driver • 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. For details, see page 160 "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.

Condition	Cause	Solution
After starting "User Management Tool" or "Address Management Tool" in Device Manager NX Lite and entering the correct login user name and password, a message that an incorrect password has been entered appears.	"Driver Encryption Key:Encryption Strength" is not set correctly. Alternatively, "SSL/TLS" has been enabled although the required certificate is not installed in the computer.	Set "Driver Encryption Key:Encryption Strength" to [Simple Encryption]. Alternatively, enable "SSL/TLS", install the server certificate in the machine, and then install the certificate in the computer. For details, see page 243 "Specifying the Extended Security Functions" and page 124 "Configuring SSL/TLS".
Cannot access the machine using ScanRouter EX Professional V3 / ScanRouter EX Enterprise V2.	"Driver Encryption Key:Encryption Strength" is not set correctly. Alternatively, "SSL/TLS" has been enabled although the required certificate is not installed in the computer.	Set "Driver Encryption Key:Encryption Strength" to [Simple Encryption]. Alternatively, enable "SSL/TLS", install the server certificate in the machine, and then install the certificate in the computer. For details, see page 243 "Specifying the Extended Security Functions" and page 124 "Configuring SSL/TLS".
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.

Condition	Cause	Solution
"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.
Cannot send e-mail from the scanner. Similarly: • Cannot select an address. • Cannot specify a signature. • Cannot store data in a media.	The following are possible causes: • The validity period of the user certificate (destination certificate) has expired. • The validity period of the device certificate (S/MIME) has expired. • The device certificate (S/MIME) does not exist or is invalid. • The validity period of the device certificate (PDF with digital signature or PDF/A with digital signature) has expired. • The device certificate (PDF with digital signature or PDF/A with digital signature) does not exist or is invalid. • The administrator's e-mail address is incorrect.	• Install a user certificate (destination certificate). You can install a user certificate (destination certificate) from the Web Image Monitor address book. The user certificate (destination certificate) itself must be prepared in advance. • Install a device certificate for S/MIME. • Install a device certificate for PDF with digital signature or PDF/A with digital signature. For details, see page 119 "Protecting the Communication Path via a Device Certificate". • Specify the administrator's e-mail address. For details, see "File Transfer", Connecting the Machine/ System Settings.

Condition	Cause	Solution
User authentication is disabled, yet stored files or stored print 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 page 169 "Managing Stored Files" or Web Image Monitor Help.
User authentication is disabled, yet destinations specified using the machine or users registered in the Address Book 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 or users you want to display. For details, see page 89 "Protecting the Address Book".
Cannot print when user authentication has been enabled.	User authentication may not be specified in the printer driver.	Specify user authentication in the printer driver. For details, see the printer driver Help.
[Finish Job and Limit] is selected in "Machine action when limit is reached", but the current job is canceled before it is finished.	Depending on the application you are using, the machine might recognize a job as multiple jobs, causing cancelation of the job before it is finished.	Reset the print volume use setting for the user by, for example, clearing the print volume use counter, and then perform printing again. For details, see page 86 "Clearing Print Volume Use Counters".
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 check with the user who executed the job. The machine administrator can delete jobs.

Condition	Cause	Solution
After executing "Encrypt User Custom Settings & Address Book", the "Exit" message does not appear despite waiting a long time.	Authentication may be taking time because a large number of items are registered in the address book. Alternatively, a file may be corrupt or the hard disk may be faulty.	If the screen has still not updated even though the "File System Data Only" time specified in accordance with page 93 "Encrypting Data on the Hard Disk" has elapsed, contact your service representative.

9. List of Operation Privileges for Settings

This chapter specifies a list of the administrator and user operation privileges for the machine settings when administrator authentication or user authentication is enabled.

How to Read

Understanding headers

- User

  The user administrator has privileges for this operation.

- Mach

  The machine administrator has privileges for this operation.

- N/W

  The network administrator has privileges for this operation.

- File

  The file administrator has privileges for this operation.

- Unset

  The logged in user has privileges for this operation.

  In cases where no settings are selected in "Available Settings" of [Administrator Authentication Management].

- Set

  The logged in user has privileges for this operation.

  Status when settings are selected in "Available Settings" of [Administrator Authentication Management].

- Lv.1

  In cases where the [Menu Protect] setting is set to [Level 1].

- Lv.2

  In cases where the [Menu Protect] setting is set to [Level 2].

Understanding the symbols

R/W: Execute, change and reading possible.

R: Reading is possible.

-: Execute, change and reading are not possible.

System Settings

When administrator authentication is set, the restrictions to user operations differ depending on the configurations in "Available Settings".

The items you can specify differ depending on the machine you are using.

[General Features]

Settings	User	Mach	N/W	File	Unset	Set
[Program / Change / Delete User Text]	R	R/W	R	R	R/W	R
[Panel Key Sound]	R	R/W	R	R	R/W	R
[Warm-up Beeper]	R	R/W	R	R	R/W	R
[Copy Count Display]	R	R/W	R	R	R/W	R
[Function Priority]	R	R/W	R	R	R/W	R
[Function Key Allocation]	R	R/W	R	R	R/W	R
[Screen Color Setting]	R	R/W	R	R	R/W	R
[Print Priority]	R	R/W	R	R	R/W	R
[Function Reset Timer]	R	R/W	R	R	R/W	R
[Interleave Print]	R	R/W	R	R	R/W	R
[Output: Copier]	R	R/W	R	R	R/W	R
[Output: Document Server]	R	R/W	R	R	R/W	R
[Output: Printer]	R	R/W	R	R	R/W	R
[Key Repeat]	R	R/W	R	R	R/W	R
[System Status/Job List Display Time]	R	R/W	R	R	R/W	R
[Time Interval between Printing Jobs]	R	R/W	R	R	R/W	R
[ADF Original Table Elevation]	R	R/W	R	R	R/W	R
[External Keyboard]	R	R/W	R	R	R/W	R
[Compatible ID]	R	R/W	R	R	R/W	R
[Z-fold Position]	R	R/W	R	R	R/W	R

Settings	User	Mach	N/W	File	Unset	Set
[Half Fold Position]	R	R/W	R	R	R/W	R
[Letter Fold-out Position]	R	R/W	R	R	R/W	R
[Letter Fold-in Position]	R	R/W	R	R	R/W	R
[Double Parallel Fold Position]	R	R/W	R	R	R/W	R
[Gate Fold Position]	R	R/W	R	R	R/W	R
[Paper Tray Priority: Copier]	R	R/W	R	R	R/W	R
[Paper Tray Priority: Printer]	R	R/W	R	R	R/W	R
[Status Indicator]	R	R/W	R	R	R/W	R
[Perfect Binding Cut Fine Adjustment]	R	R/W	R	R	R/W	R
[Auto Detect: Switch Paper Size Detected Legal/Oficio]	R	R/W	R	R	R/W	R

[Timer Settings]

Settings	User	Mach	N/W	File	Unset	Set
[Sleep Mode Timer]	R	R/W	R	R	R/W	R
[Low Power Mode Timer]	R	R/W	R	R	R/W	R
[System Auto Reset Timer]	R	R/W	R	R	R/W	R
[Copier / Document Server Auto Reset Timer]	R	R/W	R	R	R/W	R
[Printer Auto Reset Timer]	R	R/W	R	R	R/W	R
[Scanner Auto Reset Timer]	R	R/W	R	R	R/W	R
[Set Date]	R	R/W	R	R	R/W	R
[Set Time]	R	R/W	R	R	R/W	R
[Auto Logout Timer]	R	R/W	R	R	R/W	R
[Weekly Timer]	R	R/W	R	R	R/W	R
[Binding Glue Heater Auto Off Timer]	R	R/W	R	R	R/W	R

[Interface Settings]

[Network]

Settings	User	Mach	N/W	File	Unset	Set
[Machine IPv4 Address]*1	R	R	R/W	R	R/W	R
[IPv4 Gateway Address]	R	R	R/W	R	R/W	R
[Machine IPv6 Address]	R	R	R	R	R	R
[IPv6 Gateway Address]	R	R	R	R	R	R
[IPv6 Stateless Address Autoconfiguration]	R	R	R/W	R	R/W	R
[DHCPv6 Configuration]	R	R	R/W	R	R/W	R
[DNS Configuration]*2	R	R	R/W	R	R/W	R
[DDNS Configuration]	R	R	R/W	R	R/W	R
[IPsec]	R	R	R/W	R	R/W	R
[Domain Name]*1	R	R	R/W	R	R/W	R
[WINS Configuration]	R	R	R/W	R	R/W	R
[Effective Protocol]	R	R	R/W	R	R/W	R
[SMB Computer Name]	R	R	R/W	R	R/W	R
[SMB Work Group]	R	R	R/W	R	R/W	R
[Ethernet Speed]	R	R	R/W	R	R/W	R
[LAN Type]	R	R	R/W	R	R/W	R
[Ping Command]	–	–	R/W	–	R/W	R
[Permit SNMPv3 Communication]	R	R	R/W	R	R/W	R
[Permit SSL / TLS Communication]	R	R	R/W	R	R/W	R
[Host Name]	R	R	R/W	R	R/W	R
[Machine Name]	R	R	R/W	R	R/W	R
[IEEE 802.1X Authentication for Ethernet]	R	R	R/W	R	R/W	R

Settings	User	Mach	N/W	File	Unset	Set
[Restore IEEE 802.1X Authentication to Defaults]	–	–	R/W	–	R/W	–

*1 When auto-obtain is set, the data is read-only.

*2 All administrators and users can run a test of connections.

[Parallel Interface]

Settings	User	Mach	N/W	File	Unset	Set
[Parallel Timing]	R	R/W	R	R	R/W	R
[Parallel Communication Speed]	R	R/W	R	R	R/W	R
[Selection Signal Status]	R	R/W	R	R	R/W	R
[Input Prime]	R	R/W	R	R	R/W	R
[Bidirectional Communication]	R	R/W	R	R	R/W	R
[Signal Control]	R	R/W	R	R	R/W	R

[Wireless LAN]

Settings	User	Mach	N/W	File	Unset	Set
[Communication Mode]	R	R	R/W	R	R/W	R
[SSID Setting]	R	R	R/W	R	R/W	R
[Ad-hoc Channel]	R	R	R/W	R	R/W	R
[Security Method]	R	R	R/W	R	R/W	R
[Wireless LAN Easy Setup]	–	–	R/W	–	R/W	–
[Wireless LAN Signal]	R	R	R	R	R	R
[Restore Factory Defaults]	–	–	R/W	–	R/W	–

[Print List]

Settings	User	Mach	N/W	File	Unset	Set
[Print List]	–	–	R/W	–	R/W	–

[File Transfer]

Settings	User	Mach	N/W	File	Unset	Set
[Delivery Option]*3	R	R/W	R	R	R/W	R
[Capture Server IPv4 Address]	R	R/W	R	R	R/W	R
[SMTP Server]	R	R	R/W	R	R/W	R
[SMTP Authentication]*4	R	R/W	R	R	R/W	R
[POP before SMTP]	R	R/W	R	R	R/W	R
[Reception Protocol]	R	R/W	R	R	R/W	R
[POP3 / IMAP4 Settings]	R	R/W	R	R	R/W	R
[Administrator's E-mail Address]	R	R/W	R	R	R/W	R
[E-mail Communication Port]	R	R	R/W	R	R/W	R
[E-mail Reception Interval]	R	R	R/W	R	R/W	R
[Max. Reception E-mail Size]	R	R	R/W	R	R/W	R
[E-mail Storage in Server]	R	R	R/W	R	R/W	R
[Auto Email Notify]	–	R/W	–	–	R/W	–
[Default User Name / Password (Send)]*4	R	R/W	R	R	R/W	R
[Program / Change / Delete E-mail Message]	R	R/W	R	R	R/W	R/W
[Auto Specify Sender Name]	R	R	R/W	R	R/W	R
[Scanner Resend Interval Time]	R	R	R/W	R	R/W	R
[Number of Scanner Resends]	R	R	R/W	R	R/W	R

*3 The primary and secondary delivery server addresses are read-only.

*4 Passwords cannot be read.

[Administrator Tools]

Settings	User	Mach	N/W	File	Unset	Set
[Address Book Management]	R/W	R/W *5	R/W *5	R/W *5	R/W *6	R*6
[Address Book: Program / Change / Delete Group]	R/W	R/W *5	R/W *5	R/W *5	R/W *6	R*6
[Address Book: Change Order]	R/W	–	–	–	R/W	–
[Print Address Book: Destination List]	R/W	–	–	–	R/W	R/W
[Address Book: Edit Title]	R/W	–	–	–	R/W	–
[Address Book: Switch Title]	R/W	–	–	–	R/W	R
[Backup/Restore: User Custom Settings & Address Book]	R/W	–	–	–	R/W	–
[Data Carry-over Setting for Address Book Auto-program]	R/W	R	R	R	R/W	R
[Auto Delete User in Address Book]	R/W	–	–	–	R/W	–
[Delete All Data in Address Book]	R/W	–	–	–	R/W	–
[Display / Print Counter]	R	R/W	R	R	R/W	R/W
[Display / Clear / Print Counter per User]	R/W *7	R/W *8	R	R	R/W	–
[Display / Clear Eco-friendly Counter]	–	R/W	–	–	–	–
[Display / Clear Eco-friendly Counter per User]	–	R/W	–	–	–	–
[Eco-friendly Counter Period / Administrator Message]	R	R/W	R	R	R	R
[Machine action when limit is reached]	R	R/W	R	R	R	R
[Print Volume Use Limitation: Unit Count Setting]	R	R/W	R	R	R	R
[Enhanced Print Volume Use Limitation]	R	R/W	R	R	R	R
[Print Volum. Use Limit.: Default Limit Value]	R/W	R	R	R	R	R

Settings	User	Mach	N/W	File	Unset	Set
[Media Slot Use]	R	R/W	R	R	R	R
[User Authentication Management]	R	R/W	R	R	R/W	R
[Enhanced Authentication Management]	R	R/W	R	R	R/W	R
[Administrator Authentication Management]	R/W *9*10	R/W *10	R/W *10	R/W *10	R/W	–
[Program / Change Administrator]	R/W *11	R/W *11	R/W *11	R/W *11	–	–
[Key Counter Management]	R	R/W	R	R	R/W	R
[External Charge Unit Management]	R	R/W	R	R	R/W	R
[Enhanced External Charge Unit Management]	R	R/W	R	R	R/W	R
[Extended Security]						
• [Driver Encryption Key]	–	–	R/W	–	R/W	–
• [Driver Encryption Key:Encryption Strength]	R	R	R/W	R	R/W	R
• [Restrict Display of User Information]	R	R/W	R	R	R/W	R
• [Encrypt User Custom Settings & Address Book]	R/W	R	R	R	R	R
• [Enhance File Protection]	R	R	R	R/W	R	R
• [Restrict Use of Destinations]	R/W	R	R	R	R	R
• [Restrict Adding of User Destinations]	R/W	R	R	R	R	R
• [Settings by SNMPv1, v2]	R	R	R/W	R	R/W	R
• [Authenticate Current Job]	R	R/W	R	R	R/W	R
• [Password Policy]	R/W	–	–	–	–	–
• [@Remote Service]	R	R/W	R	R	R/W	R
• [Update Firmware]	R	R/W	R	R	–	–
• [Change Firmware Structure]	R	R/W	R	R	–	–

Settings	User	Mach	N/W	File	Unset	Set
• [Password Entry Violation]	–	R/W	–	–	–	–
• [Security Setting for Access Violation]	–	R/W	–	–	–	–
• [Device Access Violation]	–	R/W	–	–	–	–
[Auto Delete File in Document Server]	R	R	R	R/W	R/W	R
[Delete All Files in Document Server]	–	–	–	R/W	R/W	–
[Capture Priority]	–	R/W	–	–	R/W	R
[Capture: Delete All Unsent Files]	–	R/W	–	–	R/W	–
[Capture: Ownership]	–	R/W	–	–	R/W	R
[Capture: Public Priority]	–	R/W	–	–	R/W	R
[Capture: Owner Defaults]	–	R/W	–	–	R/W	R
[Program / Change / Delete LDAP Server]*4	–	R/W	–	–	R/W	R
[LDAP Search]	R	R/W	R	R	R/W	R
[Sleep Mode Entry by Sleep Mode Timer]	R	R/W	R	R	R/W	R
[Service Test Call]	–	R/W	–	–	R/W	–
[Notify Machine Status]	–	R/W	–	–	R/W	–
[Service Mode Lock]	R	R/W	R	R	R/W	R
[Firmware Version]	R	R	R	R	R	R
[Network Security Level]	R	R	R/W	R	R	R
[Auto Erase Memory Setting]	R	R/W	R	R	R	R
[Erase All Memory]	–	R/W	–	–	–	–
[Delete All Logs]	–	R/W	–	–	R/W	–
[Transfer Log Setting]*12	R	R/W	R	R	R/W	R
[Detect Data Security for Copying]	R	R/W	R	R	R/W	R
[Unauthorized Copy Prevention Printing: Copier]	R	R/W	R	R	R/W	R

Settings	User	Mach	N/W	File	Unset	Set
[Unauthorized Copy Prevention Printing: Document Server]	R	R/W	R	R	R/W	R
[Unauthorized Copy Prevention Printing: Printer]	R	R/W	R	R	R/W	R
[Fixed USB Port]	R	R/W	R	R	R/W	R
[Program / Change / Delete Realm]	–	R/W	–	–	R/W	R
[Machine Data Encryption Settings]	–	R/W	–	–	–	–
[Program / Delete Device Certificate]	–	–	R/W	–	–	–
[Device Setting Information: Import Setting] [(Server)]*13	–	–	–	–	–	–
[Device Setting Information: Run Import] [(Server)]*13	–	–	–	–	–	–
[Device Setting Information: Export (Memry Strge Devc)]*13	–	–	–	–	–	–
[Device Setting Information: Import (Memry Strge Devc)]*13	–	–	–	–	–	–
[PDF File Type: PDF/A Fixed]	R	R/W	R	R	R/W	R
[Stop Key to Suspend Print Job]	R	R/W	R	R	R/W	R
[Energy Saver Key to Change Mode]	R	R/W	R	R	R/W	R
[Compulsory Security Stamp:Copier]	R	R/W	R	R	R/W	R
[Compulsory Security Stamp:Doc. Srvr.]	R	R/W	R	R	R/W	R
[Compulsory Security Stamp:Printer]	R	R/W	R	R	R/W	R
[User's Own Customization]	R	R/W	R	R	R/W	R
[Volume Use Counter: Scheduled/Specified Reset Settings]	R	R/W	R	R	R	R
[Select Switchable Languages]	–	R/W	–	–	R/W	–

*4 Passwords cannot be read.

*5 Only changing headings and user searches are possible.

*6 The items that can be executed, changed and read differ according is set to access privilege.

*7 Can only be cleared.

*8 Can only be printed.

*9 Cannot be changed when using the individual authentication function.

*10 Only the administrator privilege settings can be changed.

*11 Administrators can only change their own accounts.

*12 Can only be changed to [Off].

*13 R/W is the administrator with all privileges that include user administrator, machine administrator, network administrator, and file administrator privileges.

Tray Paper Settings

This section lists the settings displayed by pressing the [Paper Setting] key on the control panel.

When administrator authentication is set, the restrictions to user operations differ depending on the configurations in "Available Settings".

You can specify [Cover/Designation/Slip/Separation Sheet] on Type 1, 2, or 3 machines only.

[Tray Paper Settings]

Settings	User	Mach	N/W	File	Unset	Set
[Paper Tray]	R	R/W	R	R	R/W	R
[Cover/Designation/Slip/Separation Sheet]	R	R/W	R	R	R/W	R
[Edit Custom Paper]	–	R/W	–	–	R/W	–

Edit Home

When administrator authentication is set, the restrictions to user operations differ depending on the configurations in "Available Settings".

[Edit Home]

Settings	User	Mach	N/W	File	Unset	Set
[Move Icon]	R	R/W	R	R	R/W	R
[Delete Icon]	R	R/W	R	R	R/W	R
[Add Icon]	–	R/W	–	–	R/W	–
[Restore Default Icon Display]	–	R/W	–	–	R/W	–
[Insert Image on Home Screen]	–	R/W	–	–	R/W	–

Adjustment Settings for Operators

Settings	User	Mach	N/W	File	Unset	Set
[Adjustment Settings for Operators]	R/W	R/W	R/W	R/W	R/W	R/W

Adjustment Settings for Skilled Operators

Settings	User	Mach	N/W	File	Unset	Set
[Adjustment Settings for Skilled Operators]	–	R/W	–	–	–	–

Copier / Document Server Features

You can use the copy function and Document Server function on Type 1, 2, or 3 machines only.

When administrator authentication is set, the restrictions to user operations differ depending on the "Menu Protect" setting.

[General Features]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Auto Image Density Priority]	R	R/W	R	R	R	R
[Original Photo Type Priority]	R	R/W	R	R	R	R
[Original Orientation in Duplex Mode]	R	R/W	R	R	R	R
[Copy Orientation in Duplex Mode]	R	R/W	R	R	R	R
[Reserve Job Mode]	R	R/W	R	R	R	R
[Reservation Screen Auto-off Timer]	R	R/W	R	R	R	R
[Max. Copy Quantity]	R	R/W	R	R	R	R
[Manual Original Counter Reset]	R	R/W	R	R	R	R
[Auto Tray Switching]	R	R/W	R	R	R	R
[Dark Background]	R	R/W	R	R	R	R
[Panel Features Default]	R	R/W	R	R	R	R
[Image Adjustment Priority]	R	R/W	R	R	R	R
[Paper Display]	R	R/W	R	R	R	R
[Original Type Display]	R	R/W	R	R	R	R
[Alert Sound: Original left on Exposure Glass]	R	R/W	R	R	R	R
[Job End Call]	R	R/W	R	R	R	R
[Connect Copy Key Display]	R	R/W	R	R	R	R
[Switch Original Counter Display]	R	R/W	R	R	R	R
[Paper Settings Screen for Tray 7]	R	R/W	R	R	R	R
[Customize Function: Copier]	R	R/W	R	R	R/W	R

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Customize Function: Document Server Storage]	R	R/W	R	R	R/W	R

[Reproduction Ratio]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Shortcut Reduce/Enlarge]	R	R/W	R	R	R	R
[Reproduction Ratio]	R	R/W	R	R	R	R
[Reduce/Enlarge Ratio Priority]	R	R/W	R	R	R	R
[Ratio for Create Margin]	R	R/W	R	R	R	R

[Edit]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Front Margin: Left / Right]	R	R/W	R	R	R	R
[Back Margin: Left / Right]	R	R/W	R	R	R	R
[Front Margin: Top / Bottom]	R	R/W	R	R	R	R
[Back Margin: Top / Bottom]	R	R/W	R	R	R	R
[1 Sided→2 Sided Auto Margin: TtoT]	R	R/W	R	R	R	R
[1 Sided→2 Sided Auto Margin: TtoB]	R	R/W	R	R	R	R
[Creep Setting for Magazine]	R	R/W	R	R	R	R
[Erase Border Width]	R	R/W	R	R	R	R
[Erase Original Shadow in Combine]	R	R/W	R	R	R/W	R
[Erase Center Width]	R	R/W	R	R	R	R
[Front Cover Copy in Combine]	R	R/W	R	R	R/W	R
[Copy Order in Combine]	R	R/W	R	R	R/W	R
[Orientation: Booklet, Magazine]	R	R/W	R	R	R/W	R
[Copy on Designating Page in Combine]	R	R/W	R	R	R/W	R

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Image Repeat Separation Line]	R	R/W	R	R	R/W	R
[Double Copies Separation Line]	R	R/W	R	R	R/W	R
[Separation Line in Combine]	R	R/W	R	R	R/W	R
[Copy Back Cover]	R	R/W	R	R	R/W	R
[Double Copies Position]	R	R/W	R	R	R/W	R

[Stamp]

[Background Numbering]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Size]	R	R/W	R	R	R/W	R
[Density]	R	R/W	R	R	R/W	R

[Preset Stamp]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Stamp Language]	R	R/W	R	R	R/W	R
[Stamp Priority]	R	R/W	R	R	R	R
[Stamp Format]: COPY	R	R/W	R	R	R/W *1	R
[Stamp Format]: URGENT	R	R/W	R	R	R/W *1	R
[Stamp Format]: PRIORITY	R	R/W	R	R	R/W *1	R
[Stamp Format]: For Your Info.	R	R/W	R	R	R/W *1	R
[Stamp Format]: PRELIMINARY	R	R/W	R	R	R/W *1	R
[Stamp Format]: For Internal Use Only	R	R/W	R	R	R/W *1	R

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Stamp Format]: CONFIDENTIAL	R	R/W	R	R	R/W *1	R
[Stamp Format]: DRAFT	R	R/W	R	R	R/W *1	R

*1 Only adjustments to print position can be set. The print position itself cannot be configured.

[User Stamp]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Program / Delete Stamp]	R	R/W	R	R	R/W	R
[Stamp Format]: 1-5	R	R/W	R	R	R/W	R

[Date Stamp]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Format]	R	R/W	R	R	R	R
[Font]	R	R/W	R	R	R/W	R
[Size]	R	R/W	R	R	R/W	R
[Superimpose]	R	R/W	R	R	R/W	R
[Stamp Setting]	R	R/W	R	R	R/W *2	R

*2 Only adjustments to print position can be set. The print position itself cannot be configured.

[Page Numbering]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Stamp Format]	R	R/W	R	R	R	R
[Font]	R	R/W	R	R	R/W	R
[Size]	R	R/W	R	R	R/W	R
[Duplex Back Page Stamping Position]	R	R/W	R	R	R/W	R
[Page Numbering in Combine]	R	R/W	R	R	R/W	R

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Stamp on Designating Slip Sheet]	R	R/W	R	R	R/W	R
[Stamp Position:P1,P2...]	R	R/W	R	R	R/W *3	R
[Stamp Position:1/5,2/5...]	R	R/W	R	R	R/W *3	R
[Stamp Position:-1-,-2-...]	R	R/W	R	R	R/W *3	R
[Stamp Position:P.1,P.2...]	R	R/W	R	R	R/W *3	R
[Stamp Position:1,2...]	R	R/W	R	R	R/W *3	R
[Stamp Position:1-1,1-2...]	R	R/W	R	R	R/W *3	R
[Superimpose]	R	R/W	R	R	R/W	R
[Page Numbering Initial Letter]	R	R/W	R	R	R	R

*3 Only adjustments to print position can be set. The print position itself cannot be configured.

[Stamp Text]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Font]	R	R/W	R	R	R/W	R
[Size]	R	R/W	R	R	R/W	R
[Superimpose]	R	R/W	R	R	R/W	R
[Stamp Setting]	R	R/W	R	R	R/W	R
[Change Job Serial No. for First Job]	R	R/W	R	R	R	R

[Input / Output]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[SADF Auto Reset]	R	R/W	R	R	R	R

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Copy Eject Face Method in Glass Mode]	R	R/W	R	R	R	R
[Memory Full Auto Scan Restart]	R	R/W	R	R	R	R
[Sort/ Stack Shift Tray Setting]	R	R/W	R	R	R	R
[Insert Separation Sheet]	R	R/W	R	R	R	R
[Letterhead Setting]	R	R/W	R	R	R	R
[Fore Edge Cut Setting]	R	R/W	R	R	R	R
[Staple Position]	R	R/W	R	R	R/W	R
[Punch Type]	R	R/W	R	R	R/W	R
[Ring Binding / Fold Type]	R	R/W	R	R	R/W	R
[Fold Type]	R	R/W	R	R	R/W	R
[Finisher: Staple Position]	R	R/W	R	R	R/W	R
[Finisher: Punch Type]	R	R/W	R	R	R/W	R
[Finisher: Ring Binding Type]	R	R/W	R	R	R/W	R
[Simplified Screen: Finishing Types]	R	R/W	R	R	R/W	R
[Half Fold Settings (Finisher: Booklet Tray)]	R	R/W	R	R	R	R
[Z-fold Output Tray]	R	R/W	R	R	R	R
[Half Fold Settings]	R	R/W	R	R	R	R
[Letter Fold-out Settings]	R	R/W	R	R	R	R
[Letter Fold-in Settings]	R	R/W	R	R	R	R
[Double Parallel Fold Settings]	R	R/W	R	R	R	R
[Gate Fold Settings]	R	R/W	R	R	R	R

[Administrator Tools]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Menu Protect]	R	R/W	R	R	R	R

Printer Functions

This section lists the printer function items that appear if [Printer] on the Home screen is pressed.

When administrator authentication is set, the restrictions to user operations differ depending on the "Menu Protect" setting.

Printer Functions

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Job List]	R	R	R	R	R	R
[Print Jobs]	R	R	R	R/W	R/W	R/W
[Print from Memory Storage Device]	–	–	–	–	R/W	R/W
[Job Reset]	R/W	R/W	R/W	R/W	R/W	R/W
[Job Operation]	R/W	R/W	R/W	R/W	R/W	R/W
[Form Feed]	R/W	R/W	R/W	R/W	R/W	R/W
[Spooling Job List]	R	R/W	R	R	R	R
[Error Log]	–	R	–	–	R	R

Printer Features

When administrator authentication is set, the restrictions to user operations differ depending on the "Menu Protect" setting.

You can specify [Reserved Job Waiting Time] on Type 1, 2, or 3 machines only.

[List / Test Print]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Multiple Lists]	–	R/W	–	–	R/W	R/W
[Configuration Page]	–	R/W	–	–	R/W	R/W
[Error Log]	–	R/W	–	–	R/W	R/W
[PCL Configuration / Font Page]	–	R/W	–	–	R/W	R/W
[PS Configuration / Font Page]	–	R/W	–	–	R/W	R/W
[PDF Configuration / Font Page]	–	R/W	–	–	R/W	R/W
[Hex Dump]	–	R/W	–	–	R/W	R/W

[Data Management]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Menu Protect]	R	R/W	R	R	R	R
[List / Test Print Lock]	R	R/W	R	R	R	R
[Delete All Temporary Print Jobs]	–	–	–	R/W	–	–
[Delete All Stored Print Jobs]	–	–	–	R/W	–	–
[Auto Delete Temporary Print Jobs]	R	R	R	R/W	R	R
[Auto Delete Stored Print Jobs]	R	R	R	R/W	R	R

[System]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Print Error Report]	R	R/W	R	R	R	R
[Auto Continue]	R	R/W	R	R	R	R

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Store and Skip Errored Job]	R	R/W	R	R	R	R
[Memory Overflow]	R	R/W	R	R	R	R
[Auto Cancel Conf. for PDL Error Job]	R	R/W	R	R	R	R
[Auto Cancel for Print Job(s) on Error]	R	R/W	R	R	R	R
[Job Separation]	R	R/W	R	R	R	R
[Rotate Sort: Auto Paper Continue]	R	R/W	R	R	R	R
[Rotate by 180 Degrees]	R	R/W	R	R	R	R
[Print Compressed Data]	R	R/W	R/W	R	R	R
[Memory Usage]	R	R/W	R/W	R	R	R
[Duplex]	R	R/W	R	R	R	R
[Copies]	R	R/W	R	R	R	R
[Blank Page Print]	R	R/W	R	R	R	R
[Toner Saving]	R	R/W	R	R	R	R
[Spool Image]	R	R/W	R	R	R	R
[Reserved Job Waiting Time]	R	R/W	R	R	R	R
[Printer Language]	R	R/W	R	R	R	R
[Sub Paper Size]	R	R/W	R	R	R	R
[Page Size]	R	R/W	R	R	R	R
[Letterhead Setting]	R	R/W	R	R	R	R
[Tray Setting Priority]	R	R/W	R	R	R	R
[Edge to Edge Print]	R	R/W	R	R	R	R
[Default Printer Language]	R	R/W	R	R	R	R
[Tray Switching]	R	R/W	R	R	R	R
[Extended Auto Tray Switching]	R	R/W	R	R	R	R
[Jobs Not Printed As Machn. Was Off]	R	R/W	R	R	R	R

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Restrict Direct Print Jobs]	R	R/W	R	R	R	R
[Switch Initial Screen]	R	R/W	R	R	R	R

[Host Interface]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[I/O Buffer]	R	R/W	R	R	R	R
[I/O Timeout]	R	R/W	R	R	R	R

[PCL Menu]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Orientation]	R	R/W	R	R	R	R
[Form Lines]	R	R/W	R	R	R	R
[Font Source]	R	R/W	R	R	R	R
[Font Number]	R	R/W	R	R	R	R
[Point Size]	R	R/W	R	R	R	R
[Font Pitch]	R	R/W	R	R	R	R
[Symbol Set]	R	R/W	R	R	R	R
[Courier Font]	R	R/W	R	R	R	R
[Extend A4 Width]	R	R/W	R	R	R	R
[Append CR to LF]	R	R/W	R	R	R	R
[Resolution]	R	R/W	R	R	R	R

[PS Menu]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Job Timeout]	R	R/W	R	R	R	R
[Wait Timeout]	R	R/W	R	R	R	R

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Paper Selection Method]	R	R/W	R	R	R	R
[Swtchng. btwn. 1&2 Sided Prt. Func.]	R	R/W	R	R	R	R
[Data Format]	R	R/W	R	R	R	R
[Resolution]	R	R/W	R	R	R	R
[Orientation Auto Detect]	R	R/W	R	R	R	R

[PDF Menu]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Change PDF Password]	R	R/W	R	R	R	R
[PDF Group Password]	R	R/W	R	R	R	R
[Reverse Order Printing]	R	R/W	R	R	R	R
[Resolution]	R	R/W	R	R	R	R
[Orientation Auto Detect]	R	R/W	R	R	R	R

Scanner Features

You can use the scanner function on Type 1, 2, or 3 machines only.

When administrator authentication is set, the restrictions to user operations differ depending on the "Menu Protect" setting.

[General Settings]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Switch Title]	R	R/W	R	R	R	R
[Update Delivery Server Destination List]	–	R/W	–	–	–	–
[Search Destination]	R	R/W	R	R	R	R
[Ext. Auth.: Folder Path Overwrite Setting]	R	R/W	R	R	R	R
[PC Scan Command Standby Time]	R	R/W	R	R	R	R
[Destination List Display Priority 1]	R	R/W	R	R	R	R
[Destination List Display Priority 2]	R	R/W	R	R	R	R
[Print & Delete Scanner Journal]	R	R/W	R	R	R	R
[Print Scanner Journal]	R	R/W	R	R	R	R
[Delete Scanner Journal]	R	R/W	R	R	R	R
[Delete Recent Destinations]	R	R/W	R	R	R	R
[Use WSD or DSM]	R	R/W	R	R	R/W	R
[Use a Destination List that is not DSM]	R	R/W	R	R	R/W	R
[Program Setting for Destinations]	R	R/W	R	R	R	R

[Scan Settings]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[A.C.S. Sensitivity Level]	R	R/W	R	R	R	R
[Wait Time for Next Orig.: Exposure Glass]	R	R/W	R	R	R	R
[Wait Time for Next Original(s): SADF]	R	R/W	R	R	R	R

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Background Density of ADS (Full Color)]	R	R/W	R	R	R	R
[Blank Page Detect]	R	R/W	R	R	R	R
[Reproduction Ratio]	R	R/W	R	R	R	R
[Program / Change / Delete Scan Size]	R	R/W	R	R	R	R

[Send Settings]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Compression (Black & White)]	R	R/W	R	R	R/W	R
[Compression Method (Black & White)]	R	R/W	R	R	R/W	R
[Compression (Gray Scale / Full Color)]	R	R/W	R	R	R/W	R
[Compression Method for High Compression PDF]	R	R/W	R	R	R/W	R
[High Compression PDF Level]	R	R/W	R	R	R/W	R
[OCR Scanned PDF: Blank Page Sensitivity]	R	R/W	R	R	R/W	R
[Max. Email Size]	R	R	R/W	R	R	R
[Divide & Send Email]	R	R	R/W	R	R	R
[Insert Additional Email Info]	R	R/W	R	R	R/W	R
[No. of Digits for Single Page Files]	R	R/W	R	R	R/W	R
[Stored File Email Method]	R	R/W	R	R	R/W	R
[Default Email Subject]	R	R/W	R	R	R	R

[Initial Settings]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Menu Protect]	R	R/W	R	R	R	R

Extended Feature Settings

[Extended Feature Settings]

Settings	User	Mach	N/W	File	Unset	Set
[Startup Setting]	R	R/W	R	R	R	R
[Install]	R	R/W	R	R	R	R
[Uninstall]	R	R/W	R	R	R	R
[Extended Feature Info]	R	R/W	R	R	R	R
[Administrator Tools]	–	R/W	–	–	–	–
[Add.Program Startup Setting]	R	R/W	R	R	R	R
[Install Add.Program]	R	R/W	R	R	R	R
[Uninstall Add.Program]	R	R/W	R	R	R	R
[Add.Program Info]	R	R/W	R	R	R	R

Web Image Monitor: Display Eco-friendly Counter

These settings are in [Status/Information].

Each user can only view his or her own counter.

Settings	User	Mach	N/W	File	Unset	Set
[Download]	–	R/W	–	–	–	–
[Device Total Counter]	–	R	–	–	–	–
[Counter per User]	–	R	–	–	R	R

Web Image Monitor: Job

These settings are in [Status/Information].

Users can only change jobs they themselves executed.

You can specify [Document Server] on Type 1, 2, or 3 machines only.

[Job List]

Settings	User	Mach	N/W	File	Unset	Set
[Current/Waiting Jobs]: [Change Order]	–	R/W	–	–	–	–
[Current/Waiting Jobs]: [Suspend Printing]/ [Resume Printing]	–	R/W	–	–	–	–
[Current/Waiting Jobs]: [Delete Reservation]	–	R/W	–	–	–	R/W
[Job History]	–	R	–	–	R	R*1

*1 Can be viewed if user code authentication is used for the user authentication method.

[Printer]

Settings	User	Mach	N/W	File	Unset	Set
[Spool Printing]: [Delete]	–	R/W	–	–	R	R/W
[Job History]	R	R/W	R	R	R	R
[Error Log]	–	R	–	–	R	R

[Document Server]

Settings	User	Mach	N/W	File	Unset	Set
[Print Job History]	–	R	–	–	R	R*1
[Scanner Remote Send History]	–	R	–	–	R	R*1

*1 Can be viewed when using user code authentication for the user authentication method.

Web Image Monitor: Device Settings

These settings are in [Configuration] in [Device Management].

When administrator authentication is set, the restrictions to user operations differ depending on the configurations in "Available Settings".

The items you can specify differ depending on the machine you are using.

[System]

Settings	User	Mach	N/W	File	Unset	Set
[Device Name]	R	R	R/W	R	R/W	R
[Comment]	R	R	R/W	R	R/W	R
[Location]	R	R	R/W	R	R/W	R
[Display Panel Language]	R	R/W	R	R	R/W	R
[Spool Printing]	R	R/W	R	R	R/W	R
[Protect Printer Display Panel]	R	R/W	R	R	–	–
[Print Priority]	R	R/W	R	R	R/W	R
[Function Reset Timer]	R	R/W	R	R	R/W	R
[Energy Saver Key to Change Mode]	R	R/W	R	R	R/W	R
[Stop Key to Suspend Print Job]	R	R/W	R	R	R/W	R
[Permit Firmware Update]	R	R/W	R	R	–	–
[Permit Firmware Structure Change]	R	R/W	R	R	–	–
[Display IP Address on Device Display Panel]	R	R/W	R	R	–	–
[Media Slot Use]	R	R/W	R	R	R	R
[Compatible ID]	R	R/W	R	R	R/W	R
[PDF File Type: PDF/A Fixed]	R	R/W	R	R	R/W	R
[Output Tray]	R	R/W	R	R	R/W	R
[Paper Tray Priority]	R	R/W	R	R	R/W	R
[Front Cover Sheet Tray]	R	R/W	R	R	R/W	R

Settings	User	Mach	N/W	File	Unset	Set
[Back Cover Sheet Tray]	R	R/W	R	R	R/W	R
[Slip Sheet Tray]	R	R/W	R	R	R/W	R
[Designation Sheet 1-9 Tray]	R	R/W	R	R	R/W	R
[Separation Sheet Tray]	R	R/W	R	R	R/W	R

[Function Key Allocation/Function Priority]

Settings	User	Mach	N/W	File	Unset	Set
[Function Key Allocation]	R	R/W	R	R	R/W	R
[Function Priority]	R	R/W	R	R	R/W	R

[Paper]

Settings	User	Mach	N/W	File	Unset	Set
[Tray 1-7]	R	R/W	R	R	R/W	R
[Tray T1-T4]	R	R/W	R	R	R/W	R
[Interposer Upper Tray]	R	R/W	R	R	R/W	R
[Interposer Lower Tray]	R	R/W	R	R	R/W	R
[Perfect Binder Interposer Upper Tray]	R	R/W	R	R	R/W	R
[Perfect Binder Interposer Lower Tray]	R	R/W	R	R	R/W	R

[Custom Paper]

Settings	User	Mach	N/W	File	Unset	Set
[Program/Change]	–	R/W	–	–	R/W	–
[Delete]	–	R/W	–	–	R/W	–
[Recall Paper Library]	–	R/W	–	–	R/W	–

[Date/Time]

Settings	User	Mach	N/W	File	Unset	Set
[Set Date]	R	R/W	R	R	R/W	R
[Set Time]	R	R/W	R	R	R/W	R
[SNTP Server Name]	R	R/W	R	R	R/W	R
[SNTP Polling Interval]	R	R/W	R	R	R/W	R
[Time Zone]	R	R/W	R	R	R/W	R

[Timer]

Settings	User	Mach	N/W	File	Unset	Set
[Sleep Mode Timer]	R	R/W	R	R	R/W	R
[Low Power Mode Timer]	R	R/W	R	R	R/W	R
[System Auto Reset Timer]	R	R/W	R	R	R/W	R
[Copier/Document Server Auto Reset Timer]	R	R/W	R	R	R/W	R
[Scanner Auto Reset Timer]	R	R/W	R	R	R/W	R
[Printer Auto Reset Timer]	R	R/W	R	R	R/W	R
[Auto Logout Timer]	R	R/W	R	R	R/W	R
[Weekly Timer]	R	R/W	R	R	R/W	R

[Logs]

Settings	User	Mach	N/W	File	Unset	Set
[Job Log]	R	R/W	R	R	R/W	R
[Access Log]	R	R/W	R	R	R/W	R
[Eco-friendly Logs]	R	R/W	R	R	R/W	R
[Transfer Logs]*1	R	R/W	R	R	R/W	R
[Encrypt Logs]	R	R/W	R	R	R/W	R
[Classification Code]	R	R/W	R	R	R/W	R

Settings	User	Mach	N/W	File	Unset	Set
[Delete All Logs]	–	R/W	–	–	R/W	–

*1 Can only be changed to [Inactive].

[Download Logs]

Settings	User	Mach	N/W	File	Unset	Set
[Logs to Download]	–	R/W	–	–	–	–
[Download]	–	R/W	–	–	–	–

[Email]

Settings	User	Mach	N/W	File	Unset	Set
[Administrator Email Address]	–	R/W	–	–	R/W	R
[Signature]	–	R/W	–	–	R/W	R
[Reception Protocol]	–	R/W	–	–	R/W	R
[Email Reception Interval]	–	–	R/W	–	R/W	R
[Max. Reception Email Size]	–	–	R/W	–	R/W	R
[Email Storage in Server]	–	–	R/W	–	R/W	R
[SMTP Server Name]	–	–	R/W	–	R/W	R
[SMTP Port No.]	–	–	R/W	–	R/W	R
[Use Secure Connection (SSL)]	–	–	R/W	–	R/W	R
[SMTP Authentication]	–	R/W	–	–	R/W	R
[SMTP Auth. Email Address]	–	R/W	–	–	R/W	R
[SMTP Auth. User Name]	–	R/W	–	–	R/W	–
[SMTP Auth. Password]*2	–	R/W	–	–	R/W	–
[SMTP Auth. Encryption]	–	R/W	–	–	R/W	R
[POP before SMTP]	–	R/W	–	–	R/W	R
[POP Email Address]	–	R/W	–	–	R/W	R

Settings	User	Mach	N/W	File	Unset	Set
[POP User Name]	–	R/W	–	–	R/W	–
[POP Password]*2	–	R/W	–	–	R/W	–
[Timeout setting after POP Auth.]	–	R/W	–	–	R/W	R
[POP3/IMAP4 Server Name]	–	R/W	–	–	R/W	R
[POP3/IMAP4 Encryption]	–	R/W	–	–	R/W	R
[POP3 Reception Port No.]	–	–	R/W	–	R/W	R
[IMAP4 Reception Port No.]	–	–	R/W	–	R/W	R
[Email Notification E-mail Address]	–	R/W	–	–	R/W	R
[Receive Email Notification]	–	R/W	–	–	R/W	–
[Email Notification User Name]	–	R/W	–	–	R/W	–
[Email Notification Password]*2	–	R/W	–	–	R/W	–

*2 Passwords cannot be read.

[Auto Email Notification]

Settings	User	Mach	N/W	File	Unset	Set
[Notification Message]	R	R/W	R	R	R/W	R
[Groups to Notify]	R	R/W	R	R	R/W	R
[Select Groups/Items to Notify]	R	R/W	R	R	R/W	R
[Detailed Settings of Each Item]	R	R/W	R	R	R/W	R

[On-demand Email Notification]

Settings	User	Mach	N/W	File	Unset	Set
[Notification Subject]	R	R/W	R	R	R/W	R
[Notification Message]	R	R/W	R	R	R/W	R
[Access Restriction to Information]	R	R/W	R	R	R/W	R

Settings	User	Mach	N/W	File	Unset	Set
[Receivable Email Address/Domain Name Settings]	R	R/W	R	R	R/W	R

[File Transfer]

Settings	User	Mach	N/W	File	Unset	Set
[SMB User Name]	–	R/W	–	–	R/W	–
[SMB Password]*2	–	R/W	–	–	R/W	–
[FTP User Name]	–	R/W	–	–	R/W	–
[FTP Password]*2	–	R/W	–	–	R/W	–

*2 Passwords cannot be read.

[User Authentication Management]

Settings	User	Mach	N/W	File	Unset	Set
[User Authentication Management]	R	R/W	R	R	R/W	R
[Printer Job Authentication Settings]	R	R/W	R	R	R/W	R
[User Code Authentication Settings]	R	R/W	R	R	R/W	R
[Basic Authentication Settings]	R	R/W	R	R	R/W	R
[Windows Authentication Settings]	R	R/W	R	R	R/W	R
[Group Settings for Windows Authentication]	R	R/W	R	R	R/W	R
[LDAP Authentication Settings]	R	R/W	R	R	R/W	R
[Integration Server Authentication Settings]	R	R/W	R	R	R/W	R
[Group Settings for Integration Server Authentication]	R	R/W	R	R	R/W	R

[Administrator Authentication Management]

Settings	User	Mach	N/W	File	Unset	Set
[User Administrator Authentication]	R/W	R	R	R	R	R

Settings	User	Mach	N/W	File	Unset	Set
[Available Settings for User Administrator]	R/W	R	R	R	R	R
[Machine Administrator Authentication]	R	R/W	R	R	R	R
[Available Settings for Machine Administrator]	R	R/W	R	R	R	R
[Network Administrator Authentication]	R	R	R/W	R	R	R
[Available Settings for Network Administrator]	R	R	R/W	R	R	R
[File Administrator Authentication]	R	R	R	R/W	R	R
[Available Settings for File Administrator]	R	R	R	R/W	R	R

[Program/Change Administrator]

Settings	User	Mach	N/W	File	Unset	Set
[User Administrator]	R/W	R	R	R	–	–
[Machine Administrator]	R	R/W	R	R	–	–
[Network Administrator]	R	R	R/W	R	–	–
[File Administrator]	R	R	R	R/W	–	–
[Login User Name]*1	R/W	R/W	R/W	R/W	–	–
[Login Password]*1	R/W	R/W	R/W	R/W	–	–
[Encryption Password]*1	R/W	R/W	R/W	R/W	–	–

*1 Administrators can only change their own accounts.

[Print Volume Use Limitation]

Settings	User	Mach	N/W	File	Unset	Set
[Machine Action When Limit is Reached]	R	R/W	R	R	R	R
[Print Volume Use Limitation: Unit Count Setting]	R	R/W	R	R	R	R

Settings	User	Mach	N/W	File	Unset	Set
[Volume Use Counter: Scheduled/Specified Reset Settings]	R	R/W	R	R	R	R

[LDAP Server]

Settings	User	Mach	N/W	File	Unset	Set
[LDAP Search]	–	R/W	–	–	R/W	–
[Change]	–	R/W	–	–	R/W	–
[Delete]	–	R/W	–	–	R/W	–

[Firmware Update]

Settings	User	Mach	N/W	File	Unset	Set
[Update]	–	R/W	–	–	–	–
[Firmware Version]	–	R	–	–	–	–

[Kerberos Authentication]

Settings	User	Mach	N/W	File	Unset	Set
[Encryption Algorithm]	–	R/W	–	–	–	–
[Realm 1-5]	–	R/W	–	–	–	–

[Device Setting Information: Import Setting (Server)]

Settings	User	Mach	N/W	File	Unset	Set
[Import File From]*5	–	–	–	–	–	–
[Scheduled Import at Specified Time]*5	–	–	–	–	–	–
[Comparing New File to Last Import File]*5	–	–	–	–	–	–
[Email Failure Notification]*5	–	–	–	–	–	–
[Number of Retries]*5	–	–	–	–	–	–
[Retry Interval]*5	–	–	–	–	–	–

Settings	User	Mach	N/W	File	Unset	Set
[Encryption Key]*5	–	–	–	–	–	–

*5 R/W is the administrator with all privileges that include user administrator, machine administrator, network administrator, and file administrator privileges.

[Import Test]

Settings	User	Mach	N/W	File	Unset	Set
[Start]*5	–	–	–	–	–	–

*5 R/W is the administrator with all privileges that include user administrator, machine administrator, network administrator, and file administrator privileges.

[Eco-friendly Counter Period/Administrator Message]

Settings	User	Mach	N/W	File	Unset	Set
[Display Information Screen]	R	R/W	R	R	R/W	R
[Display Time]	R	R/W	R	R	R/W	R
[Count Period]	R	R/W	R	R	R/W	R
[Count Period (Days)]	R	R/W	R	R	R/W	R
[Administrator Message]	R	R/W	R	R	R/W	R

[Compulsory Security Stamp]

Settings	User	Mach	N/W	File	Unset	Set
[Copier]	R	R/W	R	R	R	R
[Document Server]	R	R/W	R	R	R	R
[Printer]	R	R/W	R	R	R	R

[Unauthorized Copy Prevention: Copier]

Settings	User	Mach	N/W	File	Unset	Set
[Compulsory Unauthorized Copy Prevention]	R	R/W	R	R	R	R
[Unauthorized Copy Prevention Type]	R	R/W	R	R	R	R

Settings	User	Mach	N/W	File	Unset	Set
[Mask Type for Pattern/Density/Effect]	R	R/W	R	R	R	R
[Prevention Text Settings]	R	R/W	R	R	R	R

[Unauthorized Copy Prevention: Document Server]

Settings	User	Mach	N/W	File	Unset	Set
[Compulsory Unauthorized Copy Prevention]	R	R/W	R	R	R	R
[Unauthorized Copy Prevention Type]	R	R/W	R	R	R	R
[Mask Type for Pattern/Density/Effect]	R	R/W	R	R	R	R
[Prevention Text Settings]	R	R/W	R	R	R	R

[Unauthorized Copy Prevention: Printer]

Settings	User	Mach	N/W	File	Unset	Set
[Unauthorized Copy Prevention Setting]	R	R/W	R	R	R	R
[Compulsory Unauthorized Copy Prevention]	R	R/W	R	R	R	R
[Unauthorized Copy Prevention Type]	R	R/W	R	R	R	R
[Mask Type for Pattern/Density/Effect]	R	R/W	R	R	R	R
[Prevention Text Settings]	R	R/W	R	R	R	R

Web Image Monitor: Printer

These settings are in [Configuration] in [Device Management].

When administrator authentication is set, the restrictions to user operations differ depending on the "Menu Protect" setting.

You can specify [Reserved Job Waiting Time] on Type 1, 2, or 3 machines only.

[Basic Settings]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Print Error Report]	R	R/W	R	R	R	R
[Auto Continue]	R	R/W	R	R	R	R
[Memory Overflow]	R	R/W	R	R	R	R
[Auto Cancel Confirmation for PDL Error Job]	R	R/W	R	R	R	R
[Auto Cancel for Print Job(s) on Error]	R	R/W	R	R	R	R
[Job Separation]	R	R/W	R	R	R	R
[Rotate Sort: Auto Paper Continue]	R	R/W	R	R	R	R
[Auto Delete Temporary Print Jobs]	R	R	R	R/W	R	R
[Auto Delete Stored Print Jobs]	R	R	R	R/W	R	R
[Jobs Not Printed As Machine Was Off]	R	R/W	R	R	R	R
[Rotate by 180 Degrees]	R	R/W	R	R	R	R
[Print Compressed Data]	R	R/W	R/W	R	R	R
[Memory Usage]	R	R/W	R	R	R	R
[Duplex]	R	R/W	R	R	R	R
[Copies]	R	R/W	R	R	R	R
[Blank Page Print]	R	R/W	R	R	R	R
[Toner Saving]	R	R/W	R	R	R	R
[Spool Image]	R	R/W	R	R	R	R
[Reserved Job Waiting Time]	R	R/W	R	R	R	R

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Printer Language]	R	R/W	R	R	R	R
[Sub Paper Size]	R	R/W	R	R	R	R
[Page Size]	R	R/W	R	R	R/W	R
[Letterhead Setting]	R	R/W	R	R	R	R
[Tray Setting Priority]	R	R/W	R	R	R	R
[Store and Skip Errored Job]	R	R/W	R	R	R	R
[Edge to Edge Print]	R	R/W	R	R	R	R
[Default Printer Language]	R	R/W	R	R	R	R
[Tray Switching]	R	R/W	R	R	R	R
[List/Test Print Lock]	R	R/W	R	R	R	R
[Extended Auto Tray Switching]	R	R/W	R	R	R	R
[Virtual Printer]	R	R/W	R	R	R	R
[Restrict Direct Print Jobs]	R	R/W	R	R	R	R
[Initial screen switch setting]	R	R/W	R	R	R	R
[Host Interface]	R	R/W	R	R	R	R
[PCL Menu]	R	R/W	R	R	R	R
[PS Menu]	R	R/W	R	R	R	R
[PDF Menu]	R	R/W	R	R	R	R

[Tray Parameters (PCL)]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Tray Parameters (PCL)]	–	R/W	–	–	–	–

[Tray Parameters (PS)]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Tray Parameters (PS)]	–	R/W	–	–	–	–

[PDF Temporary Password]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[PDF Temporary Password]	–	–	–	–	R/W	R/W

[PDF Group Password]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[PDF Group Password]	–	R/W	–	–	–	–

[PDF Fixed Password]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[PDF Fixed Password]	–	R/W	–	–	–	–

[Virtual Printer Settings]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Virtual Printer Name]	R	R/W	R	R	R	R
[Protocol]	R	R/W	R	R	R	R
[Print Error Report]	R	R/W	R	R	R	R
[Job Separation]	R	R/W	R	R	R	R
[Rotate by 180 Degrees]	R	R/W	R	R	R	R
[Memory Usage]	R	R/W	R	R	R	R
[Duplex]	R	R/W	R	R	R	R
[Copies]	R	R/W	R	R	R	R
[Blank Page Print]	R	R/W	R	R	R	R
[Toner Saving]	R	R/W	R	R	R	R
[Sub Paper Size]	R	R/W	R	R	R	R
[Input Tray]	R	R/W	R	R	R/W	R/W
[Page Size]	R	R/W	R	R	R/W	R

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Paper Type]	R	R/W	R	R	R/W	R/W
[Output Tray]	R	R/W	R	R	R/W	R/W
[Letterhead Setting]	R	R/W	R	R	R	R
[Edge to Edge Print]	R	R/W	R	R	R	R
[PCL Menu]	R	R/W	R	R	R	R
[PS Menu]	R	R/W	R	R	R	R
[PDF Menu]	R	R/W	R	R	R	R
[RHPP Settings]	R	R/W	R	R	R/W	R/W

[Permissions for Printer Language to Operate File System]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[PJL]	R	R/W	R	R	R	R
[PDF, PostScript]	R	R/W	R	R	R	R

Web Image Monitor: Scanner

You can specify this setting on Type 1, 2, or 3 machines only.

These settings are in [Configuration] in [Device Management].

When administrator authentication is set, the restrictions to user operations differ depending on the "Menu Protect" setting.

[General Settings]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Switch Title]	R	R/W	R	R	R	R
[Search Destination]	R	R/W	R	R	R	R
[PC Scan Command Standby Time]	R	R/W	R	R	R	R
[Destination List Display Priority 1]	R	R/W	R	R	R	R
[Destination List Display Priority 2]	R	R/W	R	R	R	R
[Print & Delete Scanner Journal]	R	R/W	R	R	R	R
[External Authentication: Folder Path Overwrite Setting]	R	R/W	R	R	R	R

[Scan Settings]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[A.C.S. Sensitivity Level]	R	R/W	R	R	R	R
[Wait Time for Next Original(s)]	R	R/W	R	R	R	R
[Background Density of ADS (Full Color)]	R	R/W	R	R	R	R
[Blank Page Detect]	R	R/W	R	R	R	R

[Send Settings]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Compression (Black & White)]	R	R/W	R	R	R/W	R
[Compression (Gray Scale/Full Color)]	R	R/W	R	R	R/W	R
[OCR Scanned PDF: Blank Page Sensitivity]	R	R/W	R	R	R/W	R

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[High Compression PDF Level]	R	R/W	R	R	R/W	R
[Compression Method for High Compression PDF]	R	R/W	R	R	R/W	R
[Max. Email Size]	R	R	R/W	R	R*1	R*1
[Divide & Send Email]	R	R	R/W	R	R*1	R*1
[Insert Additional Email Info]	R	R/W	R	R	R/W	R
[No. of Digits for Single Page Files]	R	R/W	R	R	R/W	R
[Stored File Email Method]	R	R/W	R	R	R/W	R
[Default Email Subject]	R	R/W	R	R	R	R

*1 When [Network Management] in [Administrator Authentication Management] is set to [Off], user privilege becomes R/W.

[Initial Settings]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Menu Protect]	R	R/W	R	R	R	R
[Use WSD or DSM]	R	R/W	R	R	R	R
[Display WSD Destination List]	R	R/W	R	R	R	R
[Prohibit WSD Scan Command]	R	R/W	R	R	R	R
[Use a Destination List that is not DSM]	R	R/W	R	R	R	R

[Default Settings for Normal Screens on Device]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Store File]	–	R/W	–	–	R	R
[Preview]	–	R/W	–	–	R	R
[Scan Settings]	–	R/W	–	–	R	R
[Send File Type]	–	R/W	–	–	R	R

[Default Settings for Simplified Screens on Device]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Scan Settings]	–	R/W	–	–	R	R
[Send File Type]	–	R/W	–	–	R	R

Web Image Monitor: Interface

These settings are in [Configuration] in [Device Management].

When administrator authentication is set, the restrictions to user operations differ depending on the configurations in "Available Settings".

[Interface Settings]

Settings	User	Mach	N/W	File	Unset	Set
[LAN Type]	–	–	R/W	–	R	–
[Network]	R	R	R	R	R	R
[MAC Address]	R	R	R	R	R	R
[Ethernet Security]	R	R	R/W	R	R/W	R
[Ethernet Speed]	R	R	R/W	R	R/W	R
[Operation Mode]	R	R	R/W	R	R/W	R
[USB]	R	R/W	R	R	R/W	R
[USB Host]	R	R	R	R	R	R

[Wireless LAN Settings]

Settings	User	Mach	N/W	File	Unset	Set
[LAN Type]	–	–	R/W	–	R	–
[Network]	R	R	R	R	R	R
[MAC Address]	R	R	R	R	R	R
[Available Wireless LAN]	R	R	R	R	R	R
[Communication Mode]	R	R	R/W	R	R/W	R
[SSID]	R	R	R/W	R	R/W	R
[Channel]	R	R	R/W	R	R/W	–
[Security Method]	R	R	R/W	R	R/W	R
[WEP Settings]	R	R	R/W	R	R/W	R

Settings	User	Mach	N/W	File	Unset	Set
[WPA2 Settings]	R	R	R/W	R	R/W	R

Web Image Monitor: Network

These settings are in [Configuration] in [Device Management].

When administrator authentication is set, the restrictions to user operations differ depending on the configurations in "Available Settings".

[IPv4]

Settings	User	Mach	N/W	File	Unset	Set
[IPv4]	R	R	R/W *1	R	R/W *1	R
[Host Name]	R	R	R/W	R	R/W	R
[DHCP]	R	R	R/W	R	R/W	R
[Domain Name]	R	R	R/W	R	R/W	R
[IPv4 Address]	R	R	R/W	R	R/W	R
[Subnet Mask]	R	R	R/W	R	R/W	R
[DDNS]	R	R	R/W	R	R/W	R
[WINS]	R	R	R/W	R	R/W	R
[Primary WINS Server]	R	R	R/W	R	R/W	R
[Secondary WINS Server]	R	R	R/W	R	R/W	R
[LLMNR]	R	R	R/W	R	R/W	R
[Scope ID]	R	R	R/W	R	R/W	R
[Details]	R	R	R/W	R	R/W	R

*1 IPv4 cannot be disabled from Web Image Monitor when using IPv4 transmission.

[IPv6]

Settings	User	Mach	N/W	File	Unset	Set
[IPv6]	R	R	R/W	R	R/W	R
[Host Name]	R	R	R/W	R	R/W	R
[Domain Name]	R	R	R/W	R	R/W	R

Settings	User	Mach	N/W	File	Unset	Set
[Link-local Address]	R	R	R	R	R	R
[Stateless Address]	R	R	R/W	R	R/W	R
[Manual Configuration Address]	R	R	R/W	R	R/W	R
[DHCPv6]	R	R	R/W	R	R/W	R
[DHCPv6 Address]	R	R	R	R	R	R
[DDNS]	R	R	R/W	R	R/W	R
[LLMNR]	R	R	R/W	R	R/W	R
[Details]	R	R	R/W	R	R/W	R

[SMB]

Settings	User	Mach	N/W	File	Unset	Set
[SMB]	R	R	R/W	R	R/W	R
[Protocol]	R	R	R	R	R	R
[Workgroup Name]	R	R	R/W	R	R/W	R
[Computer Name]	R	R	R/W	R	R/W	R
[Comment]	R	R	R/W	R	R/W	R
[Share Name]	R	R	R	R	R	R
[Notify Print Completion]	R	R	R/W	R	R/W	R

[SNMP]

Settings	User	Mach	N/W	File	Unset	Set
[SNMP]	–	–	R/W	–	–	–
[Protocol]	–	–	R/W	–	–	–
[SNMPv1,v2 Setting]	–	–	R/W	–	–	–
[Community]	–	–	R/W	–	–	–

[SNMPv3]

Settings	User	Mach	N/W	File	Unset	Set
[SNMP]	–	–	R/W	–	–	–
[Protocol]	–	–	R/W	–	–	–
[SNMPv3 Setting]	–	–	R/W	–	–	–
[SNMPv3 Trap Communication Setting]	–	–	R/W	–	–	–
[Account] [(User)]	–	–	R/W	–	–	–
[Account] [(Network Administrator)]	–	–	R/W	–	–	–
[Account] [(Machine Administrator)]	–	R/W	–	–	–	–

[SSDP]

Settings	User	Mach	N/W	File	Unset	Set
[SSDP]	–	–	R/W	–	–	–
[UUID]	–	–	R	–	–	–
[Profile Expires]	–	–	R/W	–	–	–
[TTL]	–	–	R/W	–	–	–

[Bonjour]

Settings	User	Mach	N/W	File	Unset	Set
[Bonjour]	R	R	R/W	R	R/W	R
[Local Hostname]	R	R	R	R	R	R
[Details]	R	R	R/W	R	R/W	R
[Print Order Priority]	R	R	R/W	R	R/W	R

[System Log]

Settings	User	Mach	N/W	File	Unset	Set
[System Log]	R	R	R	R	R	–

Web Image Monitor: Security

You can specify the items for the scanner function and S/MIME on Type 1, 2, or 3 machines only.

These settings are in [Configuration] in [Device Management].

Settings	User	Mach	N/W	File	Unset	Set
[Network Security]	–	–	R/W	–	–	–
[Access Control]	–	–	R/W	–	–	–
[IPP Authentication]	–	–	R/W	–	–	–
[SSL/TLS]	–	–	R/W	–	–	–
[ssh]	–	–	R/W	–	R	R
[Site Certificate]	–	–	R/W	–	–	–
[Device Certificate]	–	–	R/W	–	–	–
[S/MIME]	–	–	R/W	–	–	–
[IPsec]	–	–	R/W	–	–	–
[User Lockout Policy]	–	R/W	–	–	–	–
[IEEE 802.1X]	–	–	R/W	–	–	–

Web Image Monitor: @Remote

These settings are in [Configuration] in [Device Management].

Settings	User	Mach	N/W	File	Unset	Set
[Setup RC Gate]	–	R/W	–	–	–	–
[Update RC Gate Firmware]	–	R/W	–	–	–	–
[RC Gate Proxy Server]	–	R/W	–	–	–	–
[Notify Functional Problems of Device]	–	R/W	–	–	–	–

Web Image Monitor: Webpage

These settings are in [Configuration] in [Device Management].

When administrator authentication is set, the restrictions to user operations differ depending on the configurations in "Available Settings".

[Webpage]

Settings	User	Mach	N/W	File	Unset	Set
[Webpage Language]	R	R	R/W	R	R/W	R
[Web Image Monitor Auto Logout]	R	R	R/W	R	R/W	R
[Set URL Target of Link Page]	R	R	R/W	R	R/W	R
[Set Help URL Target]	R	R	R/W	R	R/W	R
[WSD/UPnP Setting]	R	R	R/W	R	R/W	R
[Download Help File]	R/W	R/W	R/W	R/W	R/W	R/W

Web Image Monitor: Extended Feature Settings

These settings are in [Configuration] in [Device Management].

Settings	User	Mach	N/W	File	Unset	Set
[Startup Setting]	–	R/W	–	–	–	–
[Extended Feature Info]	R	R	R	R	R	R
[Install]	–	R/W	–	–	–	–
[Uninstall]	–	R/W	–	–	–	–
[Administrator Tools]	–	R/W	–	–	–	–
[Additional Program Startup Setting]	–	R/W	–	–	–	–
[Install Additional Program]	–	R/W	–	–	–	–
[Uninstall Additional Program]	–	R/W	–	–	–	–
[Copy Extended Features]	–	R/W	–	–	–	–
[Copy Card Save Data]	–	R/W	–	–	–	–

Web Image Monitor: Address Book

You can specify [Data Carry-over Setting for Address Book Auto-program] on Type 1, 2, or 3 machines only.

These settings are in [Device Management].

Settings	User	Mach	N/W	File	Unset	Set
[Add User]	R/W	–	–	–	R/W *1	R/W *1
[Change]	R/W	–	–	–	R/W *1	R/W *1
[Delete]	R/W	–	–	–	R/W *1	R/W *1
[Add Group]	R/W	–	–	–	R/W *1	R/W *1
[Data Carry-over Setting for Address Book Auto-program]	R/W	–	–	–	R/W *1	R/W *1
[Maintenance]	R/W	–	–	–	R/W *1	R/W *1

*1 When Type 1, 2, or 3 is used, and if [Restrict Adding of User Destinations] of [Extended Security] is set to [On], when the machine is configured for basic authentication, users can only change the password of their own account.

Web Image Monitor: Reset Printer Job

These settings are in [Device Management].

Settings	User	Mach	N/W	File	Unset	Set
[Reset Current Job]	–	R/W	–	–	–	–
[Reset All Jobs]	–	R/W	–	–	–	–

Web Image Monitor: Reset the Machine

These settings are in [Device Management].

When administrator authentication is set, the restrictions to user operations differ depending on the configurations in "Available Settings".

Settings	User	Mach	N/W	File	Unset	Set
[Reset the Machine]	–	R/W	–	–	R/W	–

Web Image Monitor: Device Home Management

These settings are in [Device Management].

When administrator authentication is set, the restrictions to user operations differ depending on the configurations in "Available Settings".

Settings	User	Mach	N/W	File	Unset	Set
[Edit Icons]	R	R/W	R	R	R/W	R
[Restore Default Icon Display]	–	R/W	–	–	R/W	–
[Home Screen Settings]	R	R/W	R	R	R/W	R

Web Image Monitor: Screen Monitoring

These settings are in [Device Management].

Settings	User	Mach	N/W	File	Unset	Set
[Display Device's Screen]	–	R/W	–	–	–	–

Web Image Monitor: Customize Screen per User

This appears if [User's Own Customization] is set to [Allow].

Users can change only their own settings.

Settings	User	Mach	N/W	File	Unset	Set
[Edit Icons]	–	–	–	–	–	R/W
[Restore Default Icon Display]	–	–	–	–	–	R/W
[Function Priority per User]	–	–	–	–	–	R/W

Web Image Monitor: Document Server

You can specify this setting on Type 1, 2, or 3 machines only.

These settings are in [Print Job/Stored File].

What users can do with stored files depends on their access privileges. For details, see page 344 "List of Operation Privileges for Stored Files".

Settings	User	Mach	N/W	File	Unset	Set
[New Folder]	–	–	–	R/W	R/W	R/W
[Edit Folder]	–	–	–	R/W	R/W	R/W
[Delete Folder]	–	–	–	R/W	R/W	R/W
[Unlock Folder]	–	–	–	R/W	–	–
[Print]	–	–	–	–	R/W	R/W
[Send]	–	–	–	–	R/W	R/W
[Delete]	–	–	–	R/W	R/W	R/W
[Edit detailed information]	–	–	–	R/W	R/W	R/W
[Download]	–	–	–	–	R/W	R/W
[Unlock File]	–	–	–	R/W	–	–

Web Image Monitor: Printer: Print Jobs

These settings are in [Print Job/Stored File].

Users can use the printer documents stored themselves or stored when user authentication is off.

The printer documents stored by other users are not displayed.

Settings	User	Mach	N/W	File	Unset	Set
[Print]	–	–	–	–	R/W *1	R/W *1
[Delete]	–	–	–	R/W	R/W *1	R/W *1
[Edit detailed information]	–	–	–	R/W	R/W *1	R/W *1
[Unlock Job]	–	–	–	R/W	–	–

*1 Access to saved documents may be restricted, depending on the user's access privileges.

List of Operation Privileges for Stored Files

You can specify the items for the Document Server function on Type 1, 2, or 3 machines only.

Understanding headers

- Read

  Users configured for read privileges.
- Edit

  Users configured for editing privileges.
- E/D

  Users configured for edit/delete privileges.
- Full

  Users configured for full control privileges.
- Owner

  Either the user who registered a document or a user set up as the owner.
- File

  The file administrator.

Understanding the symbols

R/W: Can execute.

–: Cannot execute.

This table lists the Web Image Monitor access privileges for Type 4 or 5.

Settings	Read	Edit	E/D	Full	Owner	File
[Printing]	R/W	R/W	R/W	R/W	R/W	–
[Details]	R/W	R/W	R/W	R/W	R/W	R/W
[Preview]	R/W	R/W	R/W	R/W	R/W	–
When using Type 1, 2, or 3: [Change Access Priv.]: [Owner] **When using Type 4 or 5:** Change owner	–	–	–	–	–	R/W

Settings	Read	Edit	E/D	Full	Owner	File
When using Type 1, 2, or 3: [Change Access Priv.]: [Permissions for Users/Groups] **When using Type 4 or 5:** [Access Privilege]: [Permissions for Users/Groups]	–	–	–	R/W	R/W*1	R/W
[Change File Name]	–	R/W	R/W	R/W	R/W*1	–
[Change Password]	–	–	–	–	R/W	R/W
[Unlock Files]	–	–	–	–	–	R/W
[Combine Files]	–	–	R/W	R/W	R/W*1	–
[Insert File]	–	–	R/W	R/W	R/W*1	–
[Delete Pages]	–	–	R/W	R/W	R/W*1	–
[Duplicate File]	R/W	R/W	R/W	R/W	R/W	–
[Delete File]	–	–	R/W	R/W	R/W*1	R/W
[Print Specified Page]	R/W	R/W	R/W	R/W	R/W	–
[Keep 2 /1 Sided Settings]	R/W	R/W	R/W	R/W	R/W	–

*1 The owner can change operation privileges.

[Combine Files] and [Insert File] can be applied to files with the "Edit / Delete" access permission.

When executing [Combine Files] or [Insert File], the access permission configured for the initially selected file is applied to the newly created file.

List of Operation Privileges for Address Books

You can specify the items for the scanner function, SMTP Authentication, Folder Authentication, and LDAP Authentication on Type 1, 2, or 3 machines only.

Understanding headers

- Read

  Users configured for read privileges.

- Edit

  Users configured for editing privileges.

- E/D

  Users configured for edit/delete privileges.

- Full

  Users configured for full control privileges.

- Entry

  User whose personal information is registered in the Address Book. The person who knows the user login name and password.

- User

  The user administrator.

Understanding the symbols

R/W: Execute, change and reading possible.

R: Reading is possible.

–: Execute, change and reading are not possible.

[Names]

Settings	Read	Edit	E/D	Full	Entry	User
[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
[Display Priority]	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

[Auth. Info]

Settings	Read	Edit	E/D	Full	Entry	User
[User Code]	–	–	–	–	–	R/W
[Login User Name]	–	–	–	–	R	R/W
[Login Password]	–	–	–	–	R/W *1	R/W *1
[SMTP Authentication]	–	–	–	–	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]	–	–	–	–	R/W *1	R/W *1
[Available Functions]	–	–	–	–	R	R/W
[Print Volum. Use Limit.]	–	–	–	–	R	R/W

*1 Passwords cannot be read.

[Protection]

Settings	Read	Edit	E/D	Full	Entry	User
[Use Name as]	R	R/W	R/W	R/W	R/W	R/W
[Protect Destination]: [Protection Code]	–	–	–	R/W *2	R/W *2	R/W *2
[Protect Destination]: [Protection Object]	–	R/W	R/W	R/W	R/W	R/W
[Protect Destination]: [Permissions for Users / Groups]	–	–	–	R/W	R/W	R/W
[Protect File(s)]: [Permissions for Users / Groups]	–	–	–	R/W	R/W	R/W

*2 The code for [Protection Code] cannot be read.

[E-mail]

Settings	Read	Edit	E/D	Full	Entry	User
[E-mail Address]	R	R/W	R/W	R/W	R/W	R/W

[Folder]

Settings	Read	Edit	E/D	Full	Entry	User
[SMB/FTP]	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
[Connection Test]	R	R/W	R/W	R/W	R/W	R/W

[Add to Group]

Settings	Read	Edit	E/D	Full	Entry	User
[Registration No.]	R	R/W	R/W	R/W	R/W	R/W
[Search]	R	R/W	R/W	R/W	R/W	R/W
[Switch Title]	R/W	R/W	R/W	R/W	R/W	R/W

Note

- When [Restrict Adding of User Destinations] of [Extended Security] is set to [On], regardless of the user's operation privileges, access to the Address Book is rescinded from any user other than the user administrator.

Trademarks

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

OS X and Bonjour are trademarks of Apple Inc., registered in the U.S. and other countries.

LINUX is a registered trademark of Linus Torvalds.

Lotus Notes is a trademark of International Business Machines Corporation, registered in may jurisdictions worldwide.

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

PCL® is a registered trademark of Hewlett-Packard Company.

Red Hat is a registered trademark of Red Hat, Inc.

Solaris is a trademark or registered trademark of Oracle Corporation and/or its affiliates.

Thunderbird is a registered trademark of the Mozilla Foundation.

UPnP is a trademark of 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 Internet Explorer 6 is Microsoft® Internet Explorer® 6.

The proper names of the Windows operating systems are as follows:

- 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 8 are as follows:

  Microsoft® Windows® 8

  Microsoft® Windows® 8 Pro

Microsoft® Windows® 8 Enterprise

- The product names of Windows 8.1 are as follows:

  Microsoft® Windows® 8.1

  Microsoft® Windows® 8.1 Pro

  Microsoft® Windows® 8.1 Enterprise

- The product names of Windows 10 are as follows:

  Microsoft® Windows® 10 Home

  Microsoft® Windows® 10 Pro

  Microsoft® Windows® 10 Enterprise

  Microsoft® Windows® 10 Education

- 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

- The product names of Windows Server 2012 are as follows:

  Microsoft® Windows Server® 2012 Foundation

  Microsoft® Windows Server® 2012 Essentials

  Microsoft® Windows Server® 2012 Standard

- The product names of Windows Server 2012 R2 are as follows:

  Microsoft® Windows Server® 2012 R2 Foundation

  Microsoft® Windows Server® 2012 R2 Essentials

  Microsoft® Windows Server® 2012 R2 Standard

INDEX

P

R

S

T

U

W

EN GB EN US EN AU D270-7484