Pro C9100/C9110

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

1. Getting Started

2. Configuring User Authentication

3. Restricting Machine Usage

4. Preventing Leakage of Information from Machines

5. Enhanced Network Security

6. Managing the Machine

7. Troubleshooting

8. List of Operation Privileges for Settings

1. Getting Started

This chapter describes the precautions you need 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 from being stolen or willfully damaged, 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 regularly examine the machine's logs to check for irregular and unusual events.

Before Using This Machine

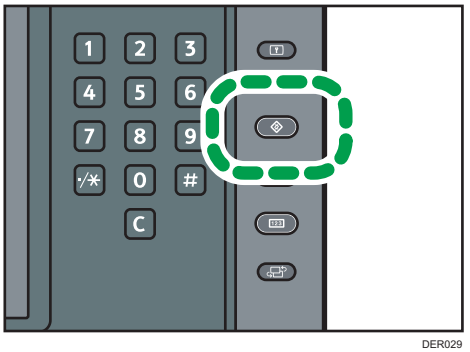
1

This section explains how to encrypt 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.**



DER029

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 Email 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 81 "Protecting Communication Paths 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 login user name and password.**

   For details about specifying administrators' login user names and passwords, see page 14 "Registering and Changing Administrators".

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

Note

- To enable higher security, see page 170 "Additional Information for Enhanced Security".

Administrators and Users

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

Administrator

There are 4 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 printing documents.

Supervisor

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

User

Users are people who use the machine for normal operations, such as printing documents.

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 password are required in order to use the machine. The role of administrator for this machine is divided into 4 categories according to their function: user administrator, machine administrator, network administrator, and file administrator. Sharing administrator tasks facilitates each administrator's tasks while at the same time preventing unauthorized administrator operations. 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 available to users, such as printing documents. To use these functions, the administrator must be authenticated as the user.

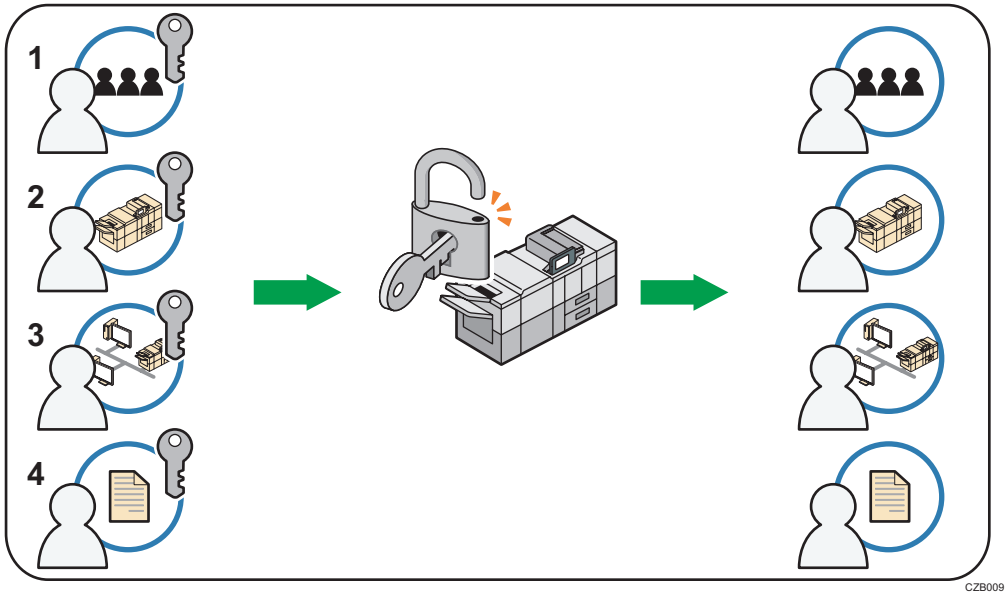
For instructions on registering the administrator, see page 14 "Registering and Changing Administrators", and for instructions on changing the administrator's password, see page 20 "Supervisor". For details on Users, see page 23 "Users".

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 managed differently from the users registered in the Address Book. Windows authentication and LDAP 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 14 "Registering and Changing Administrators".

You can specify the login user name and 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 that use SNMPv3. Administrators can only manage the machine's settings and control user access, Administrators can only manage the machine's settings and control user access; they cannot use functions such as printing documents. To use this function, the administrator must register as a user in the Address Book, and then be authenticated. Specify administrator authentication, and then specify user authentication. For details about specifying authentication, see page 25 "Configuring User Authentication".

Roles of each administrator



1. **User administrator**

   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 a user forgets their password, the user administrator can delete it and create a new one, allowing the user to access the machine again.

2. **Machine administrator**

   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 users from changing the settings and allow the machine to be used securely by its users.

3. **Network administrator**

   Manages the network settings. You can set the machine so that network settings such as the IP address and settings for sending and receiving e-mail can 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**

   Manages permission to access files.

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 can configure only settings allocated to them.

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

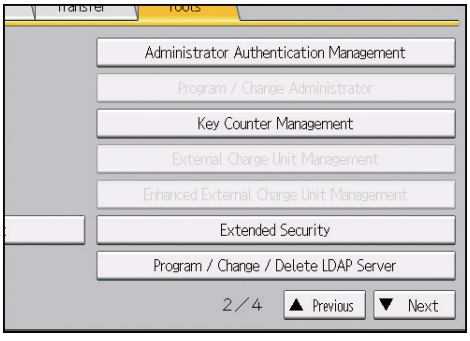
For details about logging in and logging out with administrator authentication, see page 17 "Administrator Login Method" and page 19 "Administrator Logout Method".

Important

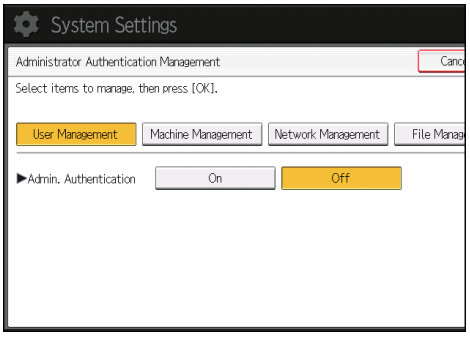
- **If you have enabled "Administrator Authentication Management", make sure not to forget the administrator login user name and password. If you forget an administrator login user name or password, you must specify a new password using the supervisor's privilege. For details on supervisor privileges, see page 20 "Supervisor".**

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

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



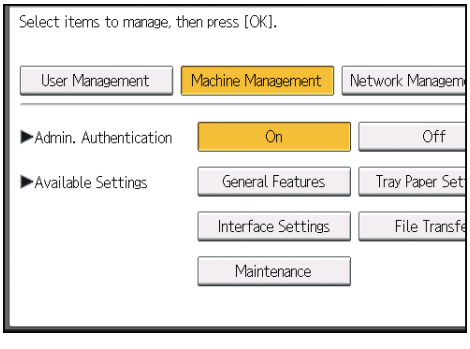
6. **Press [User Management], [Machine Management], [Network Management], or [File Management] to select which settings to manage.**



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 is specified, we recommend only one person take each administrator role.

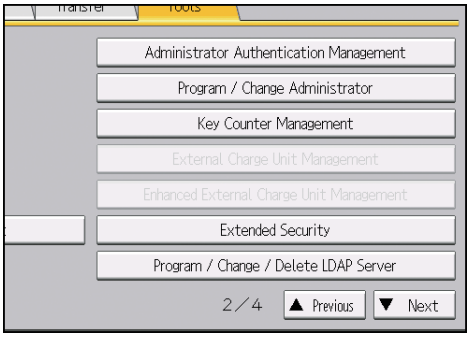
Sharing administrator tasks facilitates each administrator's tasks while also preventing unauthorized administrator operations. You can register up to 4 login user names (Administrators 1-4) to which you can grant administrator privileges.

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

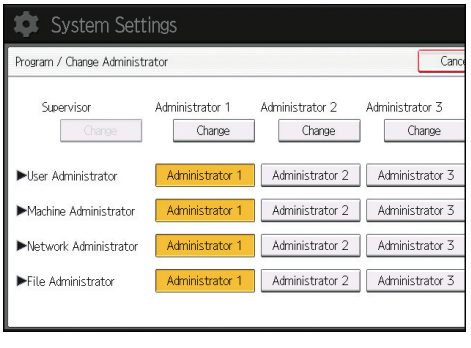
Be sure to assign all administrator privileges so that each administrator privilege is associated with at least one administrator.

For details about logging in and logging out with administrator authentication, see page 17 "Administrator Login Method" and page 19 "Administrator Logout Method".

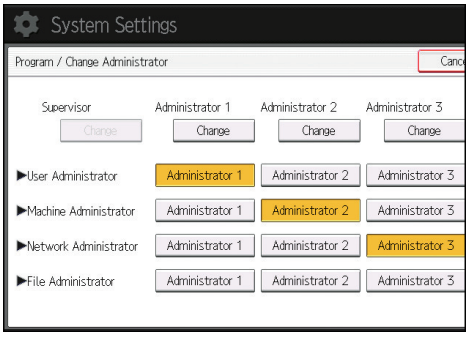
1. **Log in as an administrator from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼Next].**
5. **Press [Program / Change Administrator].**



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 multiple administrator privileges, assign multiple administrator privileges to a single administrator.

For example, to assign machine administrator privileges and user administrator privileges 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 162 "Specifying the Extended Security Functions".
11. **Enter the login password for confirmation again, and then press [OK].**
12. **Press [Change] for "Encryption Password".**
13. **Enter the encryption password, and then press [OK].**
14. **Enter the encryption password for confirmation again, and then press [OK].**
15. **Press [OK] twice.**

    You will be automatically logged out.

Note

- For the characters that can be used for login user names and passwords, see page 15 "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 left blank.
- Can be up to 32 characters long.
- The login user name of an administrator must contain characters other than numerical characters (numbers) if it is up to 8 characters. If it is consists only numbers, 9 or more must be used.

Login password

- The maximum password length for administrators and supervisors is 32 characters and 128 characters for users.
- 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.
- In [Password Policy] in [Extended Security], you can specify a password consisting of uppercase or lowercase characters, numbers, and symbols, as well as the minimum number of characters to be used for the password. For details about specifying the password policy, see "Password Policy" in page 162 "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 17 "Administrator Login Method" and page 19 "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.

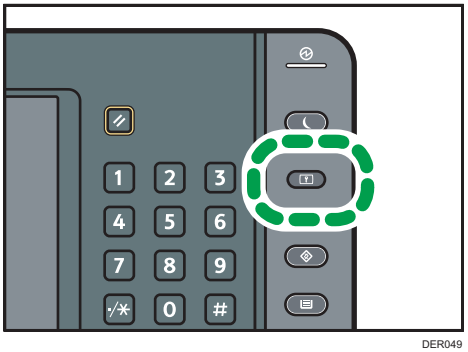
Administrator Login Method

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

For information about the user name and password for the administrator and supervisor, ask the administrator.

Logging in Using the Control Panel

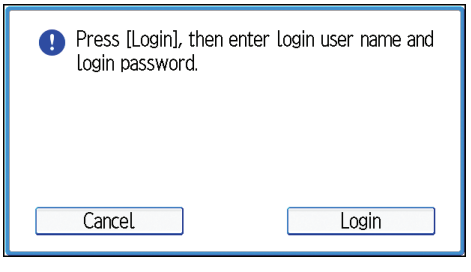
1. **Press the [User Tools] key.**
2. **Press the [Login/Logout] key.**



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

"Authenticating... Please wait." appears, followed by the initial settings screen.

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 password.

- If you log in using administrator privileges, 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 display the initial settings screen.

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 user name and password of an administrator, and then click [Login].**

Note

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

Administrator Logout Method

If administrator authentication is specified, be sure to log out after changes to settings are completed. Supervisors log out in the same way.

Logging out Using the Control Panel

1. **Press the [Login/Logout] key, and then 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 an administrator forgets or changes his or her password, the supervisor can assign a new password to the administrator. If you log 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 those for administrators. See page 17 "Administrator Login Method" and page 19 "Administrator Logout Method".

Important

- **Be sure not to forget the supervisor login user name and password. If you 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. The service call may not be free of charge.**

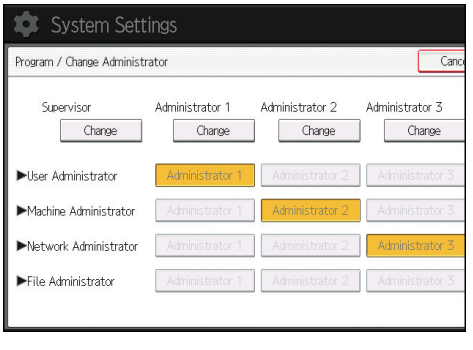
Note

- For the characters that can be used for login user names and passwords, see page 15 "Usable characters for user names and passwords".
- 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 17 "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 want to reset.**



7. **Press [Change] for "Login Password".**
8. **Enter the login password, and then press [OK].**
9. **Enter the login password for confirmation again, 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 user 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 12 "Specifying Administrator Privileges".

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

   For details on how to log in, see page 17 "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. **Enter the login password for confirmation again, and then press [OK].**
12. **Press [OK] twice.**

    You will be automatically logged out.

2. Configuring User Authentication

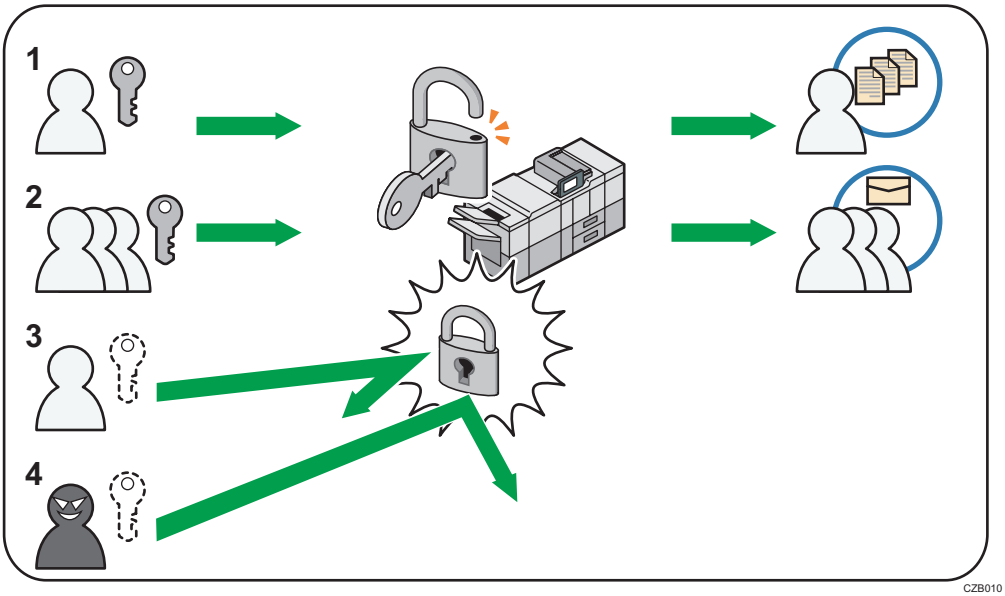
This chapter describes how to specify user authentication and explains the functions that are enabled by user authentication.

Users

A user performs normal operations on the machine, such as 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 administrators, see page 10 "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 printing.

2. **Group**

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

3. **Unauthorized user**

4. **Unauthorized access**

Configuring User Authentication

There are 4 types of user authentication methods: User Code authentication, Basic authentication, Windows authentication, and LDAP 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 cannot be enabled 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 12 "Specifying Administrator Privileges" page 14 "Registering and Changing Administrators"
Configuring user authentication	Specify user authentication. 4 types of user authentication are available: • page 27 "User Code Authentication" • page 29 "Basic Authentication" • page 32 "Windows Authentication" • page 39 "LDAP 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.
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.

Type	Details
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.

If the user authentication method is switched halfway

- A user code account that has no more than 8 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, or LDAP authentication. In this case, since no password is provided for the User Code authentication, the login password is set as blank.
- When authentication switches to an external authentication method (Windows authentication or LDAP authentication), authentication cannot be enabled unless the external authentication device has the carried over user code account previously registered. However, the user code account will be stored in the machine's Address Book even if an authentication failure occurs.
- From a security perspective, when switching from User Code authentication to another authentication method, we recommend that you delete accounts you do not 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 30 "Specifying Login User Names and Passwords".

Note

- After the main power turns 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.

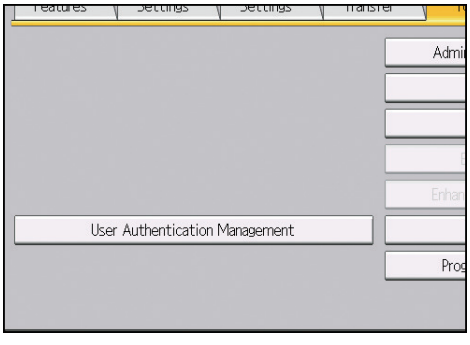
User Code Authentication

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

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, see the driver Help.

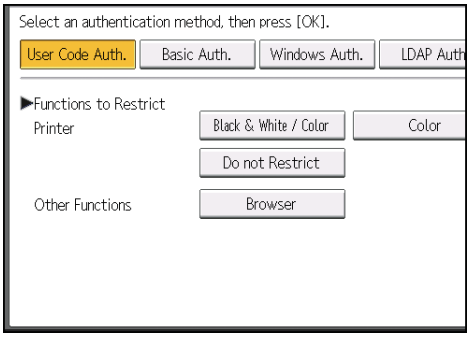
1. **Log in as the machine administrator from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼Next].**
5. **Press [User Authentication Management].**



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

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

7. **In "Functions to Restrict", select the functions that you want to restrict.**



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

For details about limiting available functions for individuals or groups, see page 50 "Limiting Available Functions".

8. **To specify printer job authentication, select [Black & White / Color] or [Color] for "Printer" under "Functions to Restrict".**

   For details about printer job authentication, see page 43 "Printer Job Authentication".

9. **Press [OK].**

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

    A confirmation message appears. If you press [Yes], you will be automatically logged out.

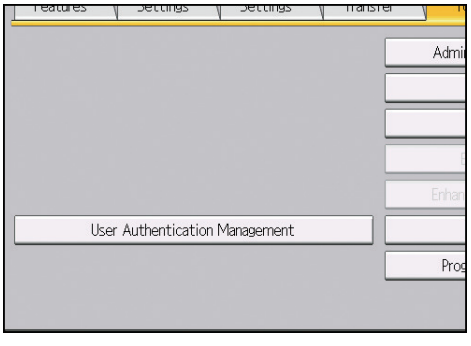
Basic Authentication

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 the personal data in the Address Book. Under Basic authentication, the administrator must specify the functions available to each user registered in the Address Book. For details about how to limit functions, see page 30 "Authentication Information Stored in the Address Book".

Specifying Basic Authentication

Before configuring 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 enable user authentication, select [Off].

7. **In "Other Functions", select which of the machine's functions you want to permit.**

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

   For details about specifying available functions for individuals or groups, see page 50 "Limiting Available Functions".

8. **Press [OK].**
9. **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 the functions that can be limited, see page 50 "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.

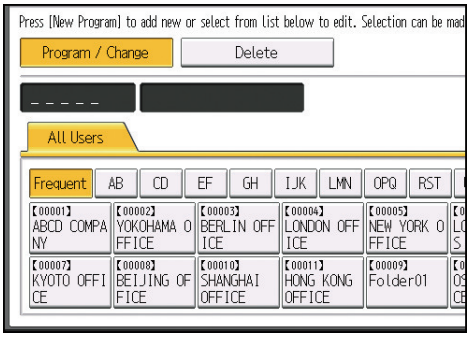
User authentication can also be specified via Web Image Monitor. For details, see Web Image Monitor Help.

Specifying Login User Names and Passwords

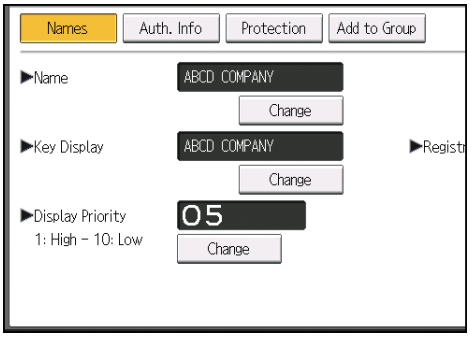
In "Address Book Management", specify the login user name and password to be used for "User Authentication Management".

For the characters that can be used for login user names and passwords, see page 15 "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.

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.

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 functions that are available only to certain users, first make settings in advance in the Address Book.

To automatically register user information under Windows authentication, it is recommended to encrypt communication between the machine and domain controller by using SSL. To do this, you must create a server certificate for the domain controller. For details about creating a server certificate, see page 38 "Creating the Server Certificate".

Important

- **If you use Windows authentication, user information registered in the directory server is automatically registered in the machine's address book. Even if the user information automatically registered in the machine's address book is edited on the machine, it is overwritten by the information from the directory server when authentication is performed.**
- **Users managed in other domains are subject to user authentication, but they cannot obtain items such as user names.**
- **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 Windows authentication is used, the login user name is case-sensitive. A wrongly entered login user name will be added to the Address Book. If this is the case, delete the added user.**
- **If the "Guest" account on the Windows server is enabled, 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".**

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.
- Set up a domain controller in the domain you want to use.

- This function is supported by the operating systems listed below. To obtain user information when Active Directory is running, use LDAP. If you are using LDAP, we recommend you use SSL to encrypt communication between the machine and the LDAP server. SSL encryption is possible only if the LDAP server supports TLSv1 or SSLv3.
  - Windows Server 2003/2003 R2
  - 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:

- Set up a domain controller in the domain you want to use.
- The operating system must support KDC (Key Distribution Center). To obtain user information when Active Directory is running, use LDAP. If you are using LDAP, we recommend you use SSL to encrypt communication between the machine and the LDAP server. SSL encryption is possible only if the LDAP server supports TLSv1 or SSLv3. Compatible operating systems are listed below:
  - Windows Server 2003/2003 R2
  - Windows Server 2008/2008 R2
  - Windows Server 2012/2012 R2

  To use Kerberos authentication under Windows Server 2008, install Service Pack 2 or later.
- Data transmission between the machine and the KDC server is encrypted if Kerberos authentication is enabled. For details about specifying encrypted transmission, see page 113 "Kerberos Authentication Encryption Setting".

Note

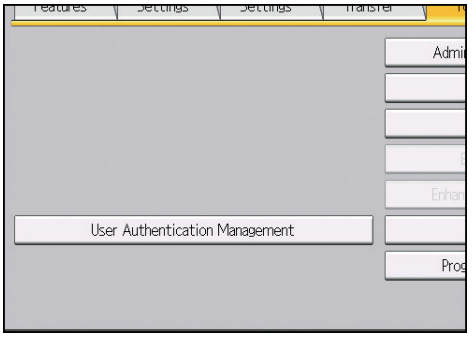
- For the characters that can be used for login user names and passwords, see page 15 "Usable characters for user names and passwords".
- When accessing the machine subsequently, you can use all the functions available to your group and to you as an individual user.
- Users who are registered in multiple groups can use all functions available to those groups.
- Under Windows Authentication, you do not need to create a server certificate unless you want to automatically register user information such as user names using SSL.

Specifying Windows Authentication

Before configuring 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.**

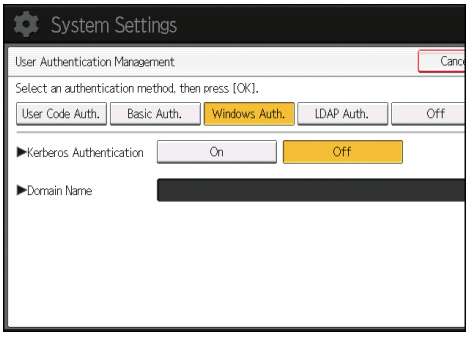
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼Next].**
5. **Press [User Authentication Management].**



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

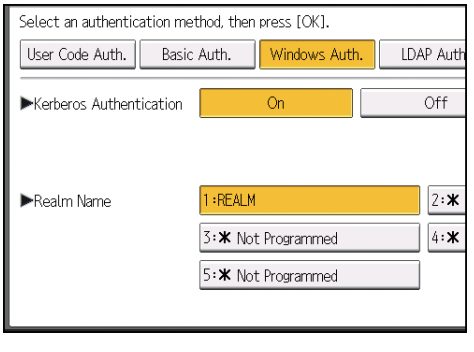
   If you do not want to enable user authentication, select [Off].

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 the Kerberos authentication realm and proceed to Step 10.**



To enable Kerberos authentication, a realm must be registered beforehand. A 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. **Press [On] for "Use Secure Connection (SSL)".**

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

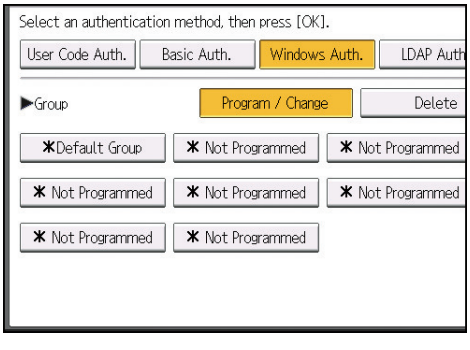
    If you have not registered a global group, proceed to Step 18.

    If you have registered a global group, proceed to Step 12.

    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 functions specified in [*Default Group]. If global groups are specified, users not registered in global groups can use the 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.
12. **Press [▼Next].**
13. **Under "Group", press [Program / Change], and then press [* Not Programmed].**



14. **Press [Change] for "Group Name", and then enter the group name.**
15. **Press [OK].**
16. **In "Other Functions", select which of the machine's functions you want to permit.**

    Windows Authentication will be applied to the selected functions.

Users can use the selected functions only.

For details about specifying available functions for individuals or groups, see page 50 "Limiting Available Functions".

17. **Press [OK].**
18. **Press [OK].**
19. **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 user informations registered in Active Directory.

We recommend you install Internet Information Services (IIS) and Certificate services as 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 selected, 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. Set the "Certificate database location:" and the "Certificate database log location:" settings 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

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, and then click [Next>].
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. **Set the "Certificate database location:" and the "Certificate database log location:" settings 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 show the procedure.

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

   Under Windows Server 2012, 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 from being sent over the network unencrypted, it is recommended to encrypt communication between the machine and LDAP server by 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 38 "Creating the Server Certificate". SSL settings can be specified in the LDAP server setting.

Using Web Image Monitor, you can enable a function to check that the SSL server is trusted. 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 in advance. A realm must be configured in capital letters. For details about registering a realm, see "Programming the Realm", Connecting the Machine/ System Settings.

Important

- **If you use LDAP authentication, user information registered in the LDAP server is automatically registered in the machine's address book. Even if the user information automatically registered in the machine's address book is edited on the machine, it is overwritten by the information from the LDAP server 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 Active Directory in LDAP authentication is used when Kerberos authentication and SSL are set at the same time, user informations 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 be able to access the server.**
- **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:

- Configure the network so that the machine can detect the LDAP server.
- When SSL is being used, TLSv1 or SSLv3 can run on the LDAP server.

- Register the LDAP server to the machine.
- To register the LDAP server, specify the following settings:
  - 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 need 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.

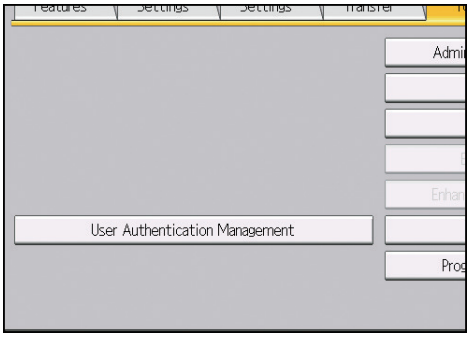
Note

- For the characters that can be used for login user names and passwords, see page 15 "Usable characters for user names and passwords".
- In LDAP simple authentication mode, authentication will fail if the password is left blank. To use 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 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 is enabled when the user accesses the machine.
- Data transmission between the machine and the KDC server is encrypted if Kerberos authentication is enabled. For details about specifying encrypted transmission, see page 113 "Kerberos Authentication Encryption Setting".

Before configuring 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].**

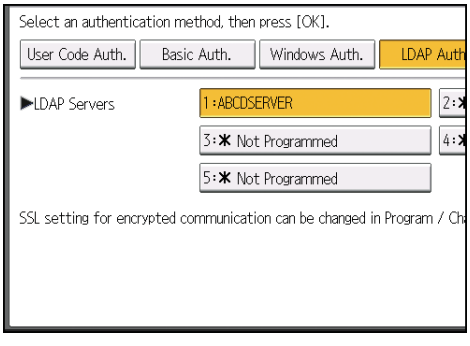
5. **Press [User Authentication Management].**



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

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

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



8. **Press [▼Next].**
9. **In "Other Functions", select which of the machine's functions you want to permit.**

   LDAP authentication will be applied to the selected functions.

   Users can use the selected functions only.

   For details about specifying available functions for individuals or groups, see page 50 "Limiting Available Functions".

10. **Press [▼Next].**
11. **Press [Change] for "Login Name Attribute".**
12. **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.

13. **Press [Change] for "Unique Attribute".**
14. **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.
15. **Press [OK].**
16. **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 to apply user authentication to print jobs.

User code authentication can be used for printer job authentication.

A job can be printed if the user code entered in the printer properties dialog box matches a user code registered in the machine's Address Book and the job is authenticated. However, even if the user code matches, the job will be canceled if the user is not authorized to use printer functions. For details about specifying available functions for each user, see page 50 "Limiting Available Functions".

Combination Table

User Authentication Management	User Code matching	User Code non-matching
[User Code Auth.] : [Black & White / Color]	B	C
[User Code Auth.] : [Color]	B	C
[User Code Auth.] : [PC Control]	A	A
[User Code Auth.] : [Do not Restrict]	A	A

A: Printing is possible.

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

C: Printing is not possible.

Note

- Of various types of user authentication, only user code authentication supports authentication of print jobs. Under basic authentication, Windows authentication, LDAP authentication, and Integration Server authentication, all jobs can be printed regardless of the user authentication settings.
- If you have enabled user code authentication on the machine, be sure to enter the user code in the printer properties dialog box.
- If you try to print without entering the user code, the print job will be unauthorized and it will be canceled.
- For details about entering the user code in the printer properties dialog box, see the printer driver Help.

Auto Registration to the Address Book

The personal information of users logging in via Windows or LDAP authentication is automatically registered in the Address Book.

Automatically Registered Address Book Items

- Login User Name
- Login Password
- Registration No.
- Name*1
- Key Display*1

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

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 161 "Managing the Address Book".

User Lockout Function

If an incorrect password is entered several times, the User Lockout function prevents further login attempts under the same login 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.**

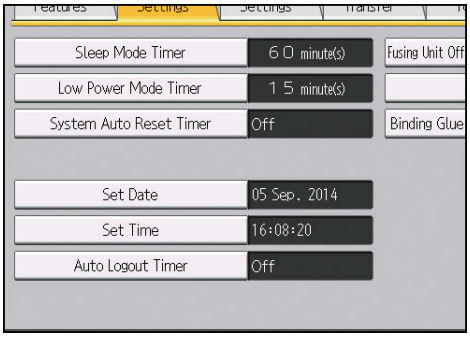
Note

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

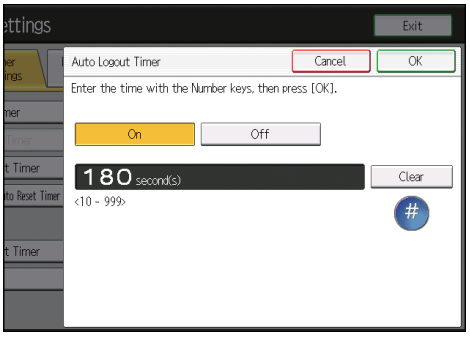
1. **Log in as the machine administrator from the control panel.**
2. **Press [System Settings].**
3. **Press [Timer Settings].**
4. **Press [Auto Logout Timer].**



5. **Select [On].**

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

6. **Enter "10" 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

- You can specify Auto Logout settings for Web Image Monitor in [Webpage]. For details, see the Web Image Monitor Help.

3. Restricting Machine Usage

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

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 shared 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 187 "List of Operation Privileges for Settings".

Register the administrators before using the machine. For instructions on registering administrators, see page 14 "Registering and Changing Administrators".

Prohibiting Users from Making Changes to Settings

It is possible to prohibit users from changing administrator settings.

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

For details about items that can be selected in "Available Settings", see page 11 "Configuring Administrator Authentication".

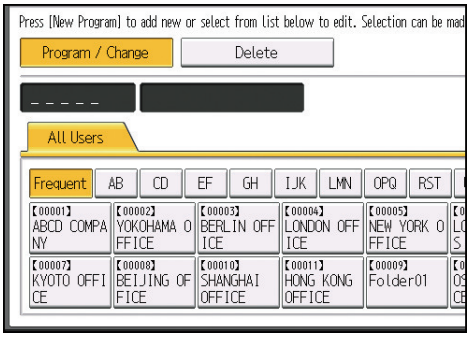
Limiting Available Functions

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

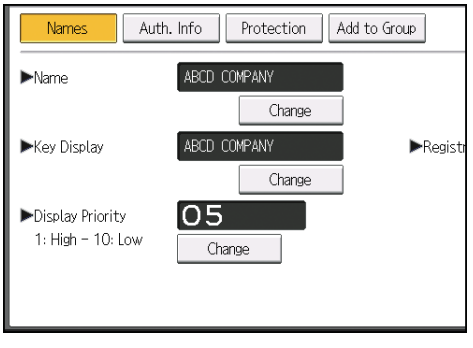
Specify the functions available to registered users. By configuring this setting, you can limit the functions available to users.

You can place limitations on the use of the printer, browser functions 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. **In "Printer" and "Other Functions", select which of the machine's functions you want to permit.**

   "Printer" is displayed if user code authentication is being applied for user authentication. For details about specifying user code authentication, see page 27 "User Code Authentication".

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

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.

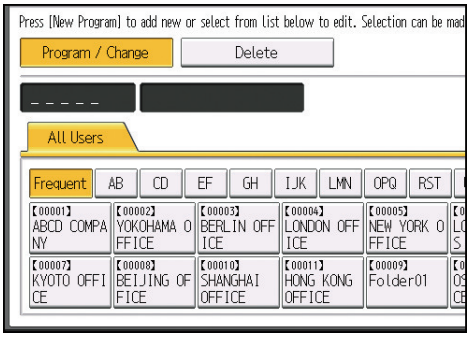
Protecting the Address Book

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

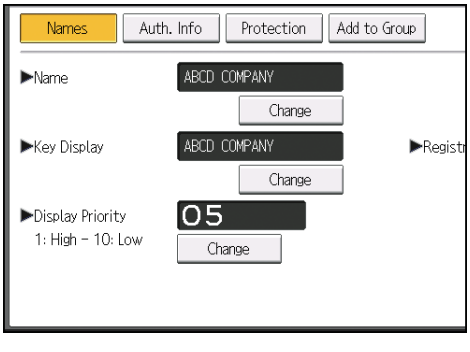
Specifying Address Book Access Permissions

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

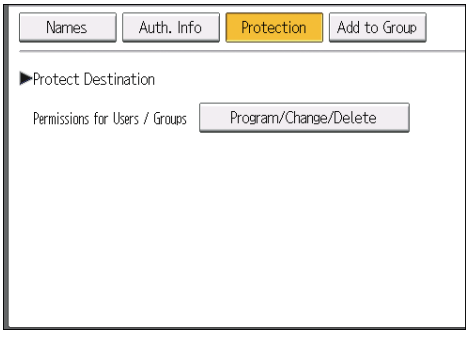
1. **Log in as the user administrator from the control panel.**
2. **Press [Address Book Mangmnt].**
3. **Select the user whose access permission you want to change.**



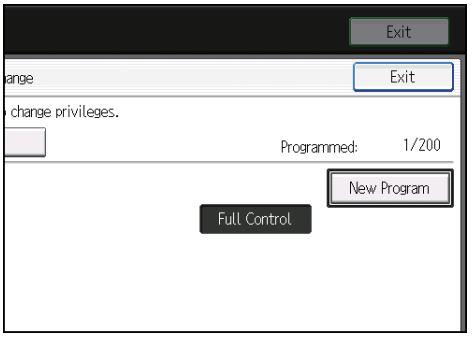
4. **Press [Protection].**



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 access permissions.**

   You can select multiple users.

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

8. **Press [Exit].**
9. **Select the user to whom you want to assign access permissions, and then specify the permission.**

   Select one of [Read-only], [Edit], [Edit / Delete], or [Full Control].

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

Note

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

Encrypting Data in the Address Book

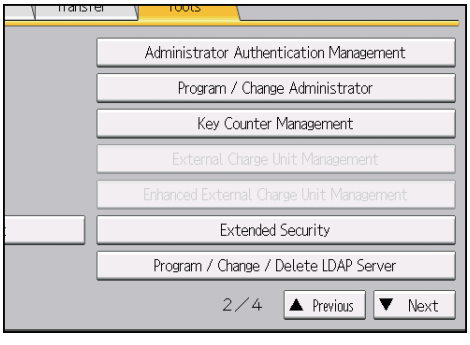
Important

- **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.

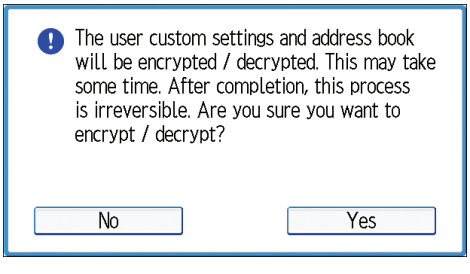
Encrypting the data in the Address Book may take longer.

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 turn 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 is not decrypted.

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, their data is also encrypted.
- The backup copy of the Address Book data stored in the SD card is encrypted. For details about backing up and restoring the Address Book using an SD card, see "Administrator Tools", Connecting the Machine/ System Settings.

Encrypting Data on the Machine

⚠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.

Even if the memory device or hard disk is stolen, data leakage can be prevented by encrypting the data on the machine, such as Address Book, authentication data, and files.

Once encryption is enabled, all data subsequently stored on the machine will be encrypted.

You can also choose to encrypt or delete the data currently stored on the machine.

The encryption algorithm is AES-256.

Data that is encrypted

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

The following data is encrypted:

NVRAM

- System settings information
- Network I/F setting information
- Browser Features
- User code information
- Counter information

Hard disk

- Address Book
- Embedded Software Architecture applications' program/log
- Logs (Job log/access log/Eco-friendly log)
- Sent/received e-mail

Type of Encryption

Specify whether to encrypt existing data and keep it on the hard disk or delete (format) it.
Encryption takes time if a large amount of data is to be kept. The NVRAM data will not be deleted (initialized).

Setting	Data to be kept	Data to be initialized	Required time
File System Data Only	• Address Book • Embedded Software Architecture applications' program/log • Logs • Sent/received e-mail	None	Approx. 2 hours and 45 minutes
All Data	All Data: Data to be kept when [File System Data Only] is specified	None	Approx. 3 hours
Format All Data	None	All Data: Data to be kept when [File System Data Only] is specified	Several minutes

Notes for enabling encryption settings

- If you use Embedded Software Architecture application, 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.

Restoring Data

- To transfer data to a new machine, restore the encrypted data. For details, ask the service representative.
- The encryption key used for data encryption is required to restore the data.
- You can specify whether to print the encryption key or store it on an SD card.
- You can change the encryption key later.

Enabling the Encryption Settings

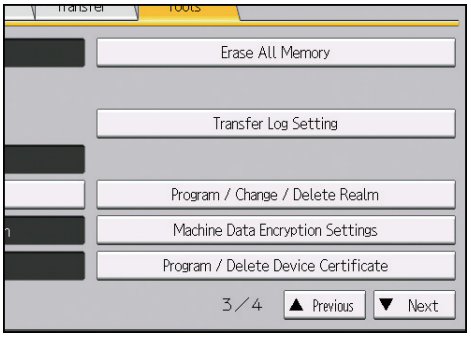
Important

- **The machine cannot be operated while data is being encrypted.**
- **Once the encryption process starts, 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**

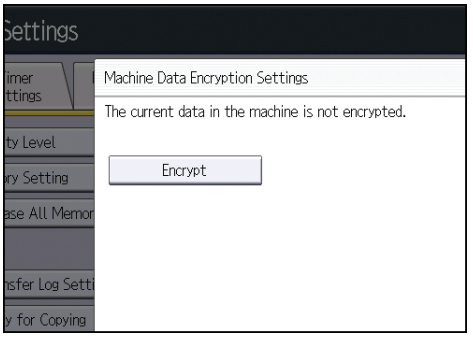
off while the encryption process is in progress, the hard disk will be damaged and all data on it will be unusable.

- 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 starts after you have completed the control panel procedure and rebooted the machine by turning the main power switch off and on. If both the Erase All Memory function and the encryption function are specified, encryption starts after the data that is stored on the hard disk has been overwritten and the machine has been rebooted by turning the main power switch on and off.
- If you use Erase All Memory and encryption simultaneously, and select overwrite 3 times for "Random Numbers", the process will take up to 7 hours and 45 minutes. Re-encrypting from an already encrypted state takes 7 hours and 15 minutes.
- The "Erase All Memory" function also clears the machine's security settings, so that neither machine nor user administration will be possible. 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 data on the hard disk is formatted. Before you perform encryption, we recommend you back up important data such as the Address Book.

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 [Machine Data Encryption Settings].



6. **Press [Encrypt].**



7. **Select the data to be carried over to the hard disk and the one not to be deleted.**

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

8. **Specify how to back up the encryption key.**

   If you have selected [Save to SD Card], insert 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 handling and 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 on the main power switch again.**

    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.

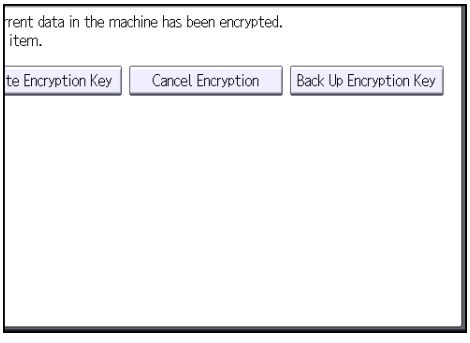
Backing Up the Encryption Key

You can back up the encryption key without changing the encryption setting.

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. **Press [▼Next] twice.**
5. **Press [Machine Data Encryption Settings].**
6. **Press [Back Up Encryption Key].**



7. **Specify how to back up the encryption key.**

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

   For details about handling and 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

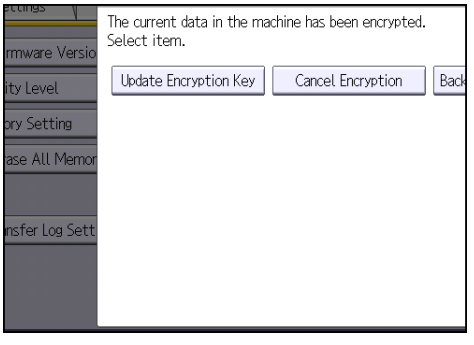
You can update the encryption key. Applying the new encryption key takes the same amount of time as that for starting encryption. Updates are possible when the machine is working normally.

Important

- **The machine cannot be used while the encryption key is being updated.**
- **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.**

- Once the updating of the encryption key starts, 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.
- If the encryption key update was not completed, the created 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. **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 the one not to be deleted.**

   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 delete all data, select [Format All Data].

8. **Specify how to back up the encryption key.**

   If you have selected [Save to SD Card], insert 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 handling and 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 on the main power switch again.**

    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. Enabling and disabling the encryption settings takes equally long.

Important

- **The machine cannot be used while data encryption is being cancelled.**
- **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.**
- **Once the canceling of data encryption starts, 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.**
- **When disposing of a machine, completely erase the memory. For details about erasing all the memory, see page 63 "Deleting Data on the Machine".**

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 [Machine Data Encryption Settings].**
6. **Press [Cancel Encryption].**
7. **Select the data to be carried over to the hard disk and the one not to be deleted.**

   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 delete all 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 on the main power switch again.**

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

Deleting Data on the Machine

You can prevent data leakage by overwriting the data stored on the machine.

There are two kinds of overwriting as follows:

Auto Erase Memory

When you edit or delete data on the machine's hard disk, the data is automatically erased by overwriting so that unnecessary data is not retained. For details, see page 63 "Auto Erase Memory".

Erase All Memory

All data stored on the machine's hard disk is erased by overwriting over it. The device settings stored on the machine's memory are initialized. Execute this to erase all data and settings when you relocate or dispose of the machine. For details, see page 66 "Erase All Memory".

Auto Erase Memory

To completely erase any unnecessary left behind after you edit or delete data on the machine's hard disk, the data must be deleted by overwriting. If you use Auto Erase Memory, overwriting is done automatically.

Types of data that can or cannot be overwritten by Auto Erase Memory

Data overwritten by Auto Erase Memory

- Information registered in the Address Book

  Data stored in the Address Book can only be overwritten after it has been changed or deleted.

- Applications using Embedded Software Architecture

  Embedded Software Architecture programs' data can only be overwritten after it has been deleted.

Data Not overwritten by Auto Erase Memory

- Counters stored under each user code

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.

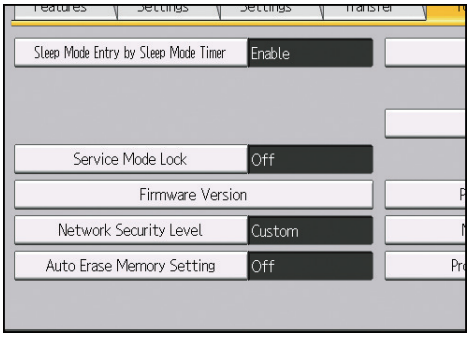
Using Auto Erase Memory

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.
- If the main power switch is 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.
- The machine will not enter Sleep mode until overwriting has been completed.

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 [Auto Erase Memory Setting].**



6. **Press [On].**
7. **Select the overwriting method you want to use.**

   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.

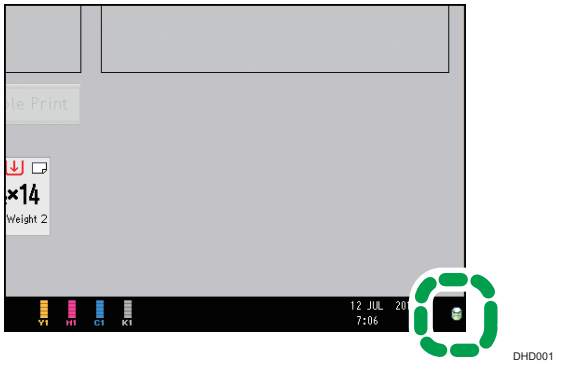
Canceling Auto Erase Memory

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

   Auto Erase Memory is disabled.
8. **Log out.**

Overwrite icon

When Auto Erase Memory is enabled, 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 flashes during overwriting.
	Clear	This icon is lit when there is no temporary data to be overwritten.

Note

- If the Data Overwrite icon is not displayed, first check if Auto Erase Memory has been set to [Off]. If the icon is not displayed even though Auto Erase Memory is [On], contact your service representative.
- 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.
- If the Data Overwrite icon continues to be "Dirty" when there is no data to be overwritten, turn off the machine's main power. Turn it on again and see if the icon changes to "Clear". If it does not, contact your sales or service representative.

Erase All Memory

Overwrite and erase all data stored on the hard disk when you relocate or dispose of the machine. The device settings stored on the machine's memory are initialized.

For details about using the machine after executing Erase All Memory, contact your sales representative.

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 to back up the Address Book. The Address Book can also be backed up using Web Image Monitor. For details, see Device Manager NX 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 3 times is set, the "Erase All Memory" process takes up to 4 hours and 45 minutes.
- The "Erase All Memory" function also clears the machine's security settings, so that neither machine nor user administration will be possible. Ensure that users do not save any data on the machine after "Erase All Memory" has completed.

Types of data that can be overwritten by Erase All Memory

- Information registered in the Address Book
- Counters stored under each user code
- Applications using Embedded Software Architecture

System Settings or other settings related to the device are initialized.

Methods of erasing

You can select a method of erasing from the following:

- NSA

  Data is overwritten twice with random numbers and once with zeros.

- DoD

  Data is overwritten by a random number, then by its complement, then by another random number, and is then verified.

- Random Numbers

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

- BSI/VSITR

  Data is overwritten 7 times with the following patterns: 0x00, 0xFF, 0x00, 0xFF, 0x00, 0xFF, 0xAA.

- Secure Erase

  Data is overwritten using an algorithm that is built in to the hard disk drive.

- Format

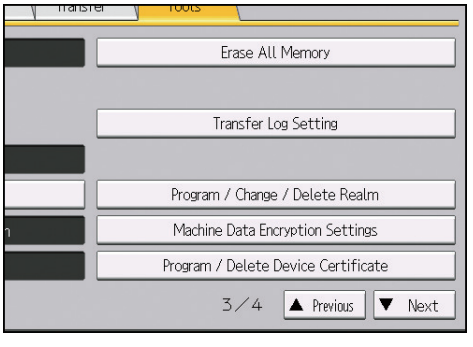
  The hard disk is formatted. Data is not overwritten.

Note

- The default method for erasing 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 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] twice.**
6. **Press [Erase All Memory].**



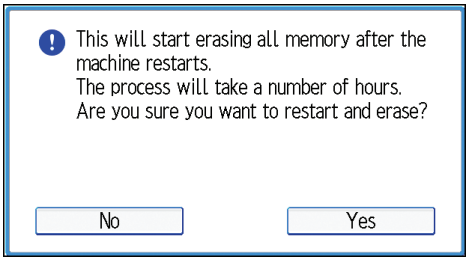
7. **Select the method of erasing.**

   If you select [NSA], [DoD], [BSI/VSITR], [Secure Erase], or [Format], 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 erasing 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

- If the main power switch is 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

To turn off the machine's power while Erase All Memory is enabled, suspend Erase All Memory in advance. Erase All Memory will resume when you turn on the main power.

Important

- **If [Secure Erase] or [Format] has been selected, the process cannot be suspended.**
- **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.

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 an access control range.

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

Important

- **Using access control, you can limit accesses from RCP/RSH, FTP, ssh/sftp, Bonjour, SMB, or Web Image Monitor. You cannot limit accesses from telnet or Device Manager NX when using SNMPv1 for 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 an IPv4 address, enter an IP address that has access to the machine in "Access Control Range".**

   To specify an 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 appear again 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, Device Manager NX, or Remote Communication Gate S.

Protocol	Port	Setting method	When disabled
IPv4	-	• Control panel • Web Image Monitor • telnet	All applications that operate over IPv4 cannot be used. IPv4 cannot be disabled from Web Image Monitor when using IPv4 transmission.
IPv6	-	• Control panel • Web Image Monitor • telnet	All applications that operate over IPv6 cannot be used.
IPsec	-	• Control panel • Web Image Monitor • telnet	Encrypted transmission using IPsec is disabled.
FTP	TCP:21	• Web Image Monitor • telnet • Device Manager NX • Remote Communication Gate S	Functions that require FTP cannot be used. You can restrict personal information from being displayed by making settings on the control panel using "Restrict Display of User Information".
ssh/sftp	TCP:22	• Web Image Monitor • telnet • Device Manager NX • Remote Communication Gate S	Functions that require sftp cannot be used. You can restrict personal information from being displayed by making settings on the control panel using "Restrict Display of User Information".
telnet	TCP:23	• Web Image Monitor • Device Manager NX	Commands using telnet are disabled.

Protocol	Port	Setting method	When disabled
SMTP	TCP:25 (variable)	• Control panel • Web Image Monitor • Device Manager NX • Remote Communication Gate S	E-mail notification function that require SMTP reception cannot be used.
HTTP	TCP:80	• Web Image Monitor • telnet	Functions that require HTTP cannot be used.
HTTPS	TCP:443	• Web Image Monitor • telnet	Functions that require HTTPS cannot be used. @Remote cannot be used. You can also make settings to require SSL transmission using the control panel or Web Image Monitor.
SMB	TCP:139	• Control panel • Web Image Monitor • telnet • Device Manager NX • Remote Communication Gate S	SMB printing functions cannot be used.
NBT	UDP:137 UDP:138	• telnet	SMB printing functions via TCP/IP, as well as NetBIOS designated functions on the WINS server cannot be used.
SNMPv1,v2	UDP:161	• Web Image Monitor • telnet • Device Manager NX • Remote Communication Gate S	Functions that require SNMPv1, v2 cannot be used. Using the control panel, Web Image Monitor or telnet, you can specify that SNMPv1, v2 settings are read-only, and cannot be edited.

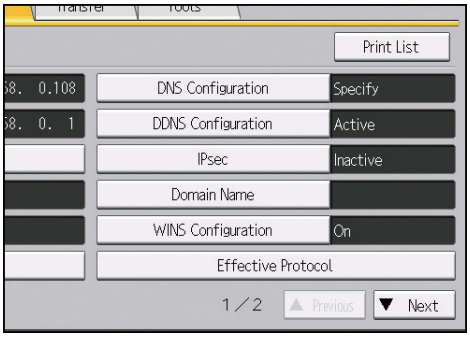
Protocol	Port	Setting method	When disabled
SNMPv3	UDP:161	• Web Image Monitor • telnet • Device Manager NX • Remote Communication Gate S	Functions that require SNMPv3 cannot be used. You can also specify settings to require SNMPv3 encrypted transmission and restrict the use of other transmission methods using the control panel, Web Image Monitor, or telnet.
RSH/RCP	TCP:514	• Web Image Monitor • telnet • Device Manager NX • Remote Communication Gate S	Functions that require RSH cannot be used. You can restrict personal information from being displayed by making settings on the control panel using "Restrict Display of User Information".
SSDP	UDP:1900	• Web Image Monitor • telnet	Device discovery using UPnP from Windows cannot be used.
Bonjour	UDP:5353	• Web Image Monitor • telnet	Bonjour functions cannot be used.
@Remote	TCP:7443 TCP:7444	• Control panel • telnet	@Remote cannot be used.
RFU	TCP:10021	• Control panel • telnet	You can update firmware via FTP.
LLTD	-	• telnet	Device search function using LLTD cannot be used.
LLMNR	UDP:5355	• Web Image Monitor • telnet	Name resolution requests using LLMNR cannot be responded.

Note

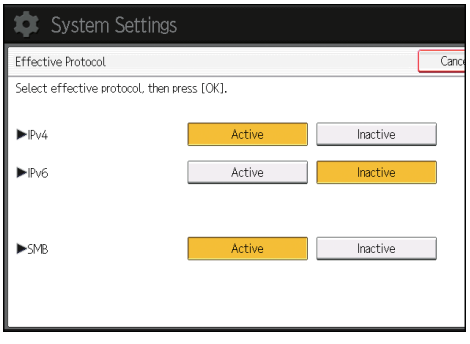
- "Restrict Display of User Information" is one of the Extended Security features. For details about making this setting, see page 162 "Specifying the Extended Security Functions".

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. Select the protocol you want to enable or disable.



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. Select the protocol you want to enable or disable, or select the port you want to open or close.
5. Click [OK].

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

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

7. **Log out.**

Specifying Network Security Levels

This setting allows you to change security levels to limit unauthorized access. You can configure network security level settings using the control panel or Web Image Monitor. Note that the protocols that can be specified differ.

Important

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

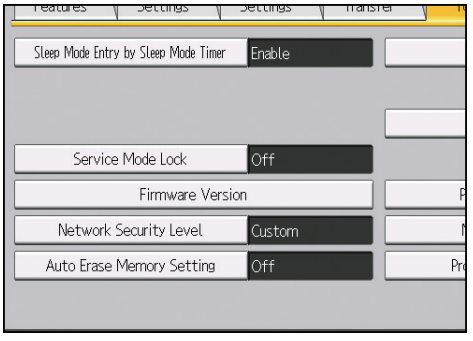
Network Security Levels

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 Levels 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] twice.**

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



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

   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 appear again 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
SSL/TLS > Port 443	Open	Open	Open	Open

Function	Level 0	Level 1	FIPS 140	Level 2
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	Active	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	-	-	-	-
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

The same settings are applied to IPv4 and IPv6.

TCP/IP setting is not controlled by the security level. Manually specify whether to enable or disable 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

Function	Level 0	Level 1	FIPS 140	Level 2
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
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

Protecting Communication Paths via a Device Certificate

This machine can protect its communication paths and establish encrypted communications using SSL/TLS, IPsec, or IEEE 802.1X.

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

Important

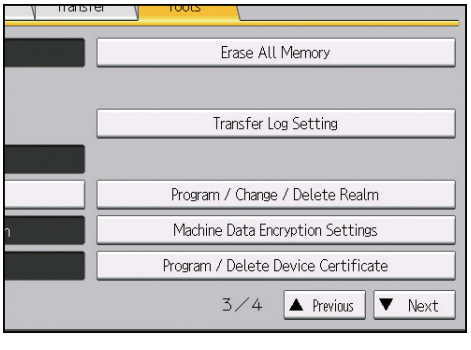
- **The administrator is required to manage the expiration of certificates and renew the certificates before they expire.**
- **The administrator is required to check that the issuer of the certificate is valid.**

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] twice.**
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. **Configure the necessary settings.**
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.

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 you want to use.

5. **Click [Create].**

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

6. **Configure the necessary settings.**
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 a 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 you want to use.
5. **Click [Request].**
6. **Configure 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 2 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 a 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 you want to use.
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 indicate whether or not the intermediate certificate has been installed. For details about the "Certificate Details" screen, see Web Image Monitor Help.

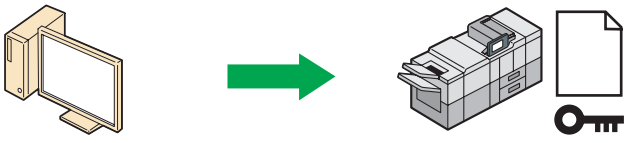
9. **Log out.**

Configuring SSL/TLS Settings

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

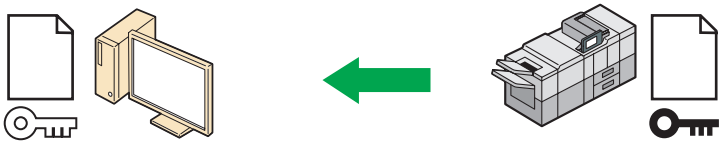
Flow of SSL/TLS encrypted communications

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.

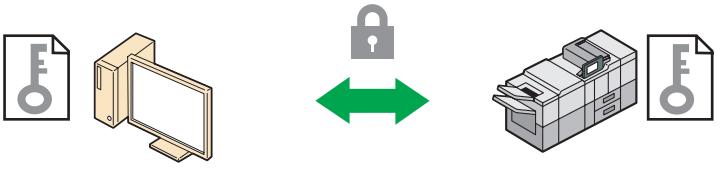


CZB003

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 check 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.

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 appear again 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.
- The following types of communication and data are always encrypted by SSL3.0: communication via @Remote and logs transferred to Remote Communication Gate S.

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. The network administrator must instruct each user to install the certificate.

Note

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

Setting SSL/TLS Encryption Mode

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

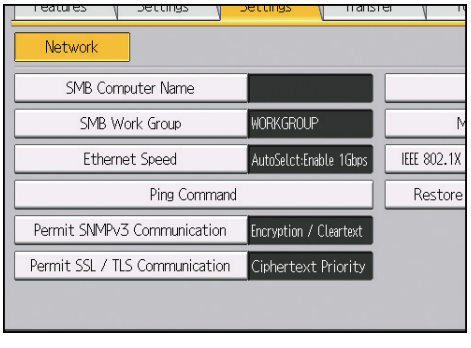
Encrypted communication mode

Using 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 a device certificate, specify SSL/TLS encrypted communication mode. By configuring 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 you want to use.**

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

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

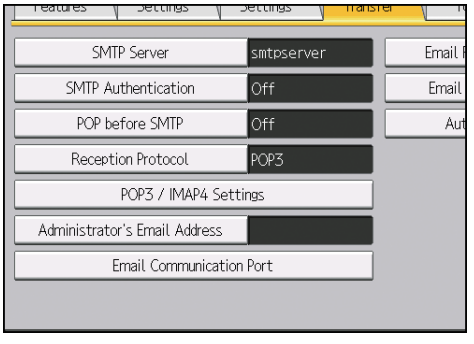
Note

- 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 changes to 465.
6. **Press [OK].**
7. **Log out.**

Configuring IPsec Settings

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.**

Supported operating systems

Operating systems	Note
• Windows Server 2003/2003 R2	IPsec over IPv4 can be used.
• Windows Vista/7/8/8.1 • Windows Server 2008/2008 R2/2012/2012 R2 • Mac OS X 10.4.8 or later • Red Hat Enterprise Linux WS 4.0 • Solaris 10	IPsec over both IPv4 and IPv6 can be used.

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 2 main functions: the encryption function, which ensures data confidentiality, and the authentication function, which verifies the sender of the data and the data's integrity. This machine's IPsec

function supports 2 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 set 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 configured 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 cleartext, data packets are vulnerable to eavesdropping attacks. Do not select this if you are exchanging sensitive information.
Authentication and Low Level Encryption	Select this level if you want to encrypt the data packets as well as authenticate the transmission partner and prevent unauthorized packet tampering. Packet encryption helps prevent eavesdropping attacks. This level provides less security than "Authentication and High Level Encryption".
Authentication and High Level Encryption	Select this level if you want to encrypt the data packets as well as authenticate the transmission partner and prevent unauthorized packet tampering. Packet encryption helps prevent eavesdropping attacks. This level provides higher security than "Authentication and Low Level Encryption".

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

Setting	Authentication Only	Authentication and Low Level Encryption	Authentication and High Level Encryption
Security Policy	Apply	Apply	Apply
Encapsulation Mode	Transport	Transport	Transport
IPsec Requirement Level	Use When Possible	Use When Possible	Always Require
Authentication Method	PSK	PSK	PSK
Phase 1 Hash Algorithm	MD5	SHA1	SHA256
Phase 1 Encryption Algorithm	DES	3DES	AES-128-CBC

Setting	Authentication Only	Authentication and Low Level Encryption	Authentication and High Level Encryption
Phase 1 Diffie-Hellman Group	2	2	2
Phase 2 Security Protocol	AH	ESP	ESP
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".

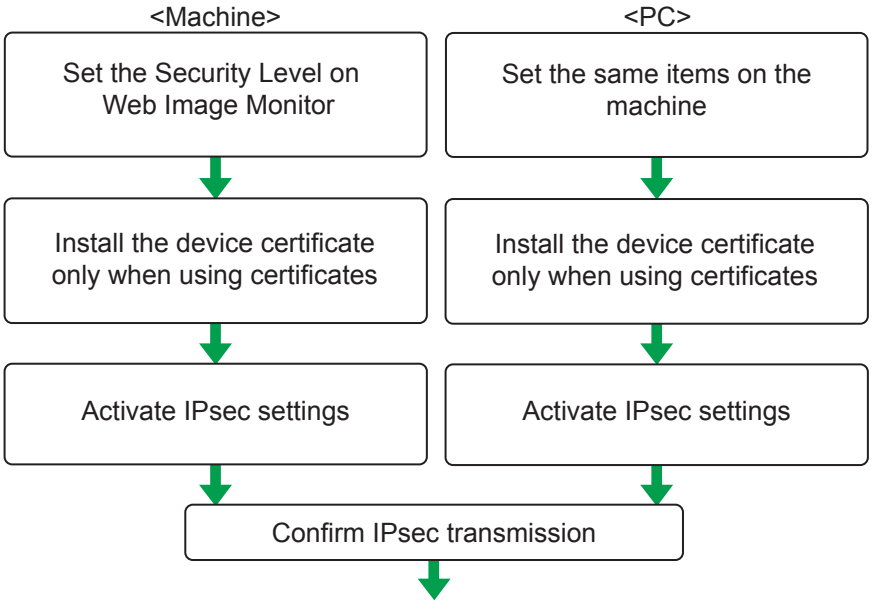
Setting	Description	Setting value
Address Type	Specify the address type for which IPsec transmission is used.	• Inactive • IPv4 • IPv6 • IPv4/IPv6 (Default Settings only)

Setting	Description	Setting value
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.
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 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



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 81 "Protecting Communication Paths via a Device Certificate". For the method of assigning installed certificates to IPsec, see page 100 "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 1 or 2 minutes, and then click [OK].**

    If the previous screen does not appear again 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 81 "Protecting Communication Paths 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 1 or 2 minutes, and then click [OK].**

   If the previous screen does not appear again 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 cannot be established.", and then click [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].**
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. For information about the user name and password for logging into telnet, ask the administrator. 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 user-specific local address / remote address.

```
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 standard and it uses the authentication server (RADIUS server).

You can select 4 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 you want 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 81 "Protecting Communication Paths 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 1 or 2 minutes, and then click [OK].**

   If the previous screen does not appear again 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 1 or 2 minutes, and then click [OK].**

   If the previous screen does not appear again 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 1 or 2 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

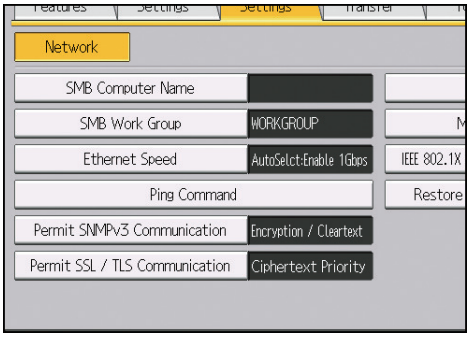
- If there is a problem with settings, you might not be able to communicate with the machine. In such a case, access [Print List] in [Interface Settings] on the control panel, and then print the network summary to check the status.
- If you cannot identify the problem, execute [Restore IEEE 802.1X Authentication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

SNMPv3 Encryption

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

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 for encrypting the data for specifying settings, you need to specify the network administrator's [Encryption Password] setting and [Encrypted Password] in [SNMP Account Setting] in Device Manager NX, in addition to specifying [Permit SNMPv3 Communication] on the machine. For details about specifying [Encrypted Password] in Device Manager NX, see Device Manager NX 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 14 "Registering and Changing Administrators".

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, 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 2003 Active Directory	• RC4-HMAC (ARCFOUR-HMAC-MD5) • DES-CBC-MD5
Windows Server 2008	• AES256-CTS-HMAC-SHA1-96 • AES128-CTS-HMAC-SHA1-96 • RC4-HMAC (ARCFOUR-HMAC-MD5) • DES-CBC-MD5
Windows Server 2008 R2/2012/2012 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, enable it in the operating system settings.

1. **Log in as the machine 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.**

   Be sure to select one or more encryption algorithm.
5. **Click [OK].**
6. **Log out.**

6. 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 access data 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.

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

3 types of logs are stored in this machine: job log, access log, and eco-friendly log.

- Job Log

  Stores details of control panel operations such as printing reports (the configuration list, for example).

- Access Log

  Stores details of login and logout activities, 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

  Stores details of 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 on the machine and the log collection level. You can also bulk delete or download log files.

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
Report Printing	Report Printing	Details of reports printed from the control panel.

Access log information items

Access Log Item	Log Type Attribute	Content
Login	Login	Times of login and identity of logged in users.
Logout	Logout	Times of logout and identity of logged out users.
HDD Format	HDD Format	Details of hard disk formatting.
All Logs Deletion	All Logs Deletion	Details of deletions of all logs.
Log Setting Change	Log Setting Change	Details of changes made to log settings.
Transfer Log Result	Transfer Log Result	Log of the result of log transfer to Remote Communication Gate S.
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.
Collect Encrypted Communication Logs	Collect Encrypted Communication Logs	Log of encrypted transmissions between the utility, Web Image Monitor or outside devices.

Access Log Item	Log Type Attribute	Content
Access Violation	Access Violation	Details of failed access attempts.
Lockout	Lockout	Details of lockout activation.
Firmware: Update	Firmware: Update	Details of firmware updates.
Firmware: Structure Change	Firmware: Structure Change	Details of structure changes that occurred when an SD card was inserted or removed, or when an unsupported SD card was inserted.
Firmware: Structure	Firmware: Structure	Details of checks for changes to firmware module structure made at times such as when the machine was switched on.
Machine Data Encryption Key Change	Machine Data Encryption Key Change	Details of changes made to encryption keys using "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.
Password Change	Password Change	Details of changes made to the login password.
Administrator Change	Administrator Change	Details of changes of administrators.
Address Book Change	Address Book Change	Details of changes made to address book entries.
Machine Configuration	Machine Configuration	Log of changes to the machine's settings.
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.
Counter Clear Result: Selected User(s)	Counter Clear Result: Selected User(s)	Log of when the counter for an individual user is cleared.

Access Log Item	Log Type Attribute	Content
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.

There is no "Login" log made for SNMPv3.

If the hard disk is formatted, all the log entries up to the time of 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 created after the power is turned 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.
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 116 "Logs That Can Be Managed Using Web Image Monitor".

Result

Indicates the result of an operation or event.

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.

Value	Content
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.
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	The privilege to access the specified file is missing.
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	The common key is missing.

Value	Content
Connection Error	A communication error occurred.
Specified Server Error	An access error has occurred because the server is not configured correctly.
Specified Client Error	An access error has occurred because the client is not configured correctly.
Authentication Settings Mismatch	Address book specifications do not match.
Authentication Method Mismatch	Authentication methods do not match.
Maximum Limit of Registered Number	The maximum number of machines that can be registered.
Invalid Password	The entered password is not valid.
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	An input was terminated abnormally.
Output Failure	An output was terminated abnormally.
Other Error	An error was detected prior to execution of a job or other errors have occurred.
Power Failure	Power was lost.
External Charge Unit Disconnected	The accounting device was unplugged during operation.
Timeout	A time-out occurred.

Value	Content
Memory Full	The memory range for processing data is full.
Print Data Error	An attempt to use a PDL or a port not installed on the machine has been made.
Data Transfer Interrupted	Cases to be recorded are as follows: • The driver being used is not matching. • A network malfunction occurs.
Over Job Limit	The limit of jobs that can be received was exceeded.
Authentication Failed (Access Restricted)	Device authentication failed.
No Privilege	The user does not have permission to access a document or function.
Not Entered Document Password	The password for a document was not entered.
Invalid Device Certificate	Cases to be recorded are as follows: • The device certificate is missing. • The valid period has expired. • If the e-mail address of the administrator and that of the certificate do not match.
Book Function Error	A bookbinding function error has occurred.
Fold Function Error	A folding function error has occurred.
Print Cancelled (Error)	The print job was canceled 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	System operations, Operations that were performed by non-authenticated users
0x00000001 - 0xfffffeff	For general users and user code

Value	Content
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 name of the user who performed the operation.

If an administrator performed the operation, his or her ID contains the login user name of the 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
System	System access
Network Attack Detection/ Encrypted Communication	Network attack or encrypted communication access
Firmware	Firmware verification access
Address Book	Address book access

Value	Content
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 using the control panel.
via Network	The login was performed remotely using a network computer.
Others	The login was performed using another method.

Login User Type

Indicates the type of login user.

Value	Content
User	General user
Guest	Guest user
User Administrator	User administrator

Value	Content
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 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 was 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 a lockout release occurs.

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
Web Image Monitor Setting	Web Image Monitor Setting
Web Service Settings	Web Service Settings
System/Copier SP	System SP

Target File Name

Indicates the name of the device information file to be imported or exported.

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.

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 protocol of the destination is not identified.

IP Address

Destination IP address.

Port No.

Destination port number.

Port numbers are indicated in decimal numbers.

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 cracking
Device Access Violation	Denial-of-Service attack (DoS)
Request Falsification Violation	Request forgery

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
WIM Auto Logout Timer	Web Image Monitor auto logout timer
Extended Security	Extended Security
Firmware Update Start	Firmware Update

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 no certificate is used, "Do not Use" is recorded.
Certificate No.: IPsec	The number of the certificate for applications is recorded. When no certificate is 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.

Attribute	Description
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.
WIM Auto Logout Timer (minutes)	Web Image Monitor's auto logout timer log is recorded in increments of one minute.
Update Firmware	A log entry reporting changes to the [Update Firmware] setting is recorded. "Prohibit" or "Do not Prohibit" is recorded.
Change Firmware Structure	A log entry reporting changes to the [Change Firmware Structure] setting is recorded. "Prohibit" or "Do not Prohibit" is recorded.
Firmware Update Start	A log entry reporting firmware update is recorded.

Destination Server Name

Indicates the name of the server from which the data export or import request was issued when the log type is for importing or exporting preference information.

HDD Format Partition

Indicates the reason for formatting the hard disk.

Value	Content
HDD Exchange	The hard disk has been replaced.
Problem with HDD Encryption Key	There is a problem with the hard disk encryption key.
Problem with Disk Label	The disk label cannot be read.

Value	Content
Problem with File System	There is a problem with the file system.

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
Report	The job file was a printed report.

Job log (target)

Target

Type of the job target.

Value	Content
Print	Print

Start Date/Time

Indicates when "Print" operation started.

End Date/Time

Indicates when "Print" operation ended.

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 time that has elapsed from the start of the previous job to that of the present job.

Job Duration (seconds)

Indicates the time that has elapsed from the start of a job to the end of it.

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.
Printing	Machine's printing 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 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 each item of the log details is changed, the level changes to [User Settings].
6. **Click [OK].**
7. **"Updating..." appears. Wait for about 1 or 2 minutes, and then click [OK].**

   If the previous screen does not appear again 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.

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, configure the collection setting for 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. **Select the type of log to download from the drop-down box in "Logs to Download".**

   The security log includes 2 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 to the time you click the [Download] button. Any logs recorded after you click the [Download] button 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 being downloaded or 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 118 "Attributes of Logs You Can Download".

Number of Logs That Can Be Kept on the Machine

When the limit 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 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 shown 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 numbers 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 numbers 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 (2 entries per job: 1 login and 1 logout).
Eco-friendly logs	100

According to these conditions, the machine can maintain logs for 40 days without overwriting. We recommend downloading logs every 20 days in case errors may occur.

The machine administrator must manage downloaded log files appropriately.

Note

- While logs are being downloaded, do not perform operations that will create log entries because as the logs that are being downloaded cannot record 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 the Maximum

If the number of logs that can be stored on the machine exceeds the specified 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 combined after they are downloaded.

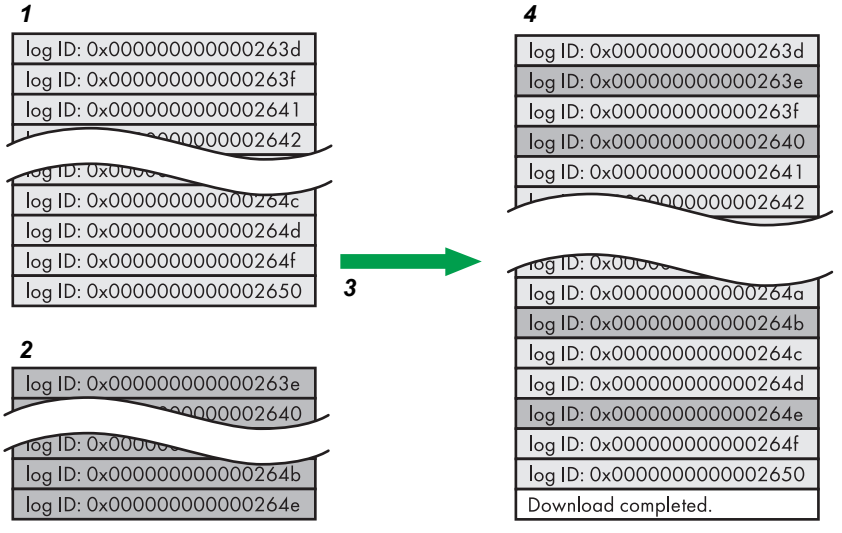
"If logs are downloaded during overwriting" below indicates that part of the access log is overwritten.

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.

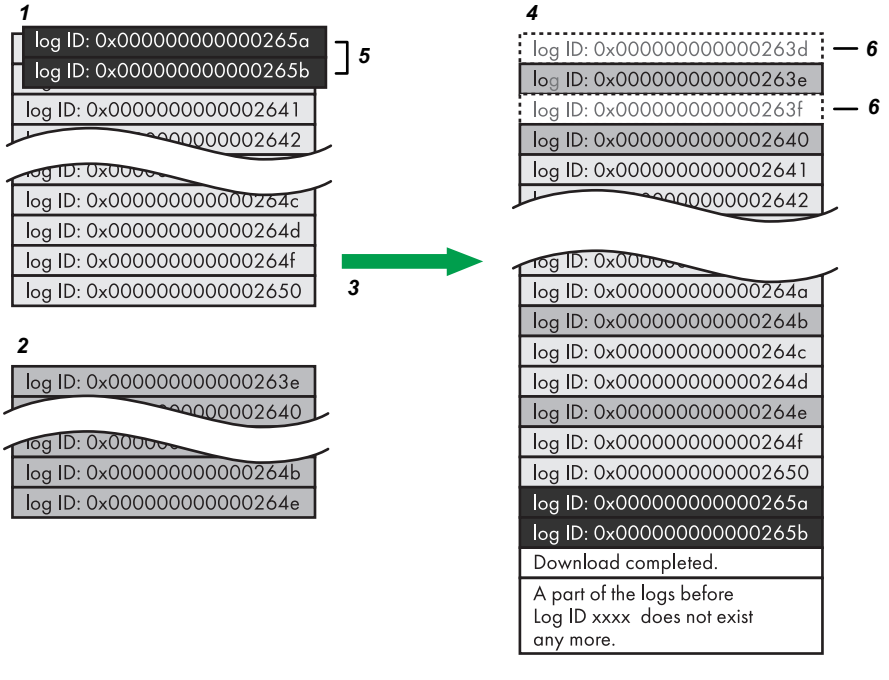
Log entries are overwritten in the order of priority. Log entries with higher priority will not be overwritten or deleted.

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**

Check the message in the last line of the downloaded logs to determine whether or not overwriting occurred while the logs were downloading,

- 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 occurs, part of the logs will be deleted by the overwriting, so check the log "Log ID xxxx" and more recent logs.

Deleting All Logs

Use the following procedure to delete all logs stored on 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 the log collection setting, whether or not to transfer logs to the log collection server, and whether or not to delete all logs.

Specifying Log Collect Settings

Enable the collection settings for each log type.

1. **Log in as the machine administrator from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼Next] 3 times.**
5. **Press [Collect Logs].**
6. **Select [Active] for each function: "Job Log", "Access Log" and "Eco-friendly Logs".**
7. **Press [OK].**
8. **Log out.**
9. **Turn off the main power switch, and then turn on the main power switch again.**

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 currently 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. **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 on the machine.

Deleting all logs from the machine as a batch can be performed 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] twice.**
5. **Press [Delete All Logs].**
6. **Press [Yes].**
7. **Press [Exit].**
8. **Log out.**

Managing Logs from the Log Collection Server

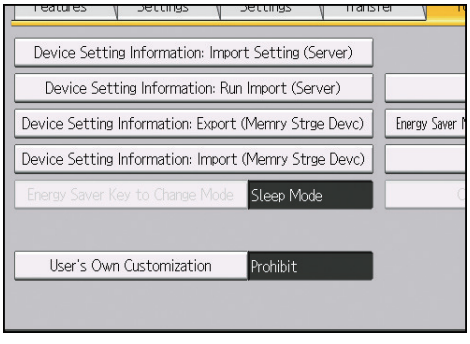
For details about using the log collection server to manage log files, see the manual supplied with the log collection server.

Configuring the Home Screen for Individual Users

This allows each user to use his or her home screen.

When a user logs in, the 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. **Press [▼Next] 3 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 a User's Own Home Screens

Note these warnings before using this function.

- When a user is registered in the Address Book, a home screen is created for that user. The user's own home screen is configured with the default settings (arrangement of icons).
- Only the icons of the functions the user has permission to use are displayed.
- When a user is deleted from the Address Book, the home screen information of the user is also deleted.

- Because each user can customize his or her home screen, the administrator cannot check the home information of each user.

Configuring the Browser Settings

Precautions for Using the Browser Function

Communication between the machine and the server via a web browser is exposed to eavesdropping and data tampering. Because of this, it is recommended to install the site certificates issued for the websites the machine is allowed to browse and enable the machine's Site Certificate Check function in advance. Access to unauthorized can be prevented by allowing the machine to access only the websites whose certificates are installed on the machine.

It is recommended to enable [Site Certificate Check] especially when you send data using Extended JavaScript.

To enable [Site Certificate Check], it is necessary to enable the machine's SSL function and install site certificates.

For details about configuring SSL, see page 86 "Configuring SSL/TLS Settings".

For details about installing site certificates, see page 108 "Configuring IEEE 802.1X Authentication".

The machine's Site Certificate Check settings can be specified only via Web Image Monitor.

See the related articles in the Web Image Monitor Help.

If [Site Certificate Check] is disabled and the user accesses an untrusted Web site, a warning message may appear.

If this is the case, the connected website may have security problems. In such a case, the machine administrator must refer to page 149 "Troubleshooting", and then instruct the users to take appropriate measures accordingly.

Further, even if such a message does not appear, to minimize the risk of information leakage and data tampering, the administrator should instruct users to check the certificates and URLs of the connected websites so that access to unauthorized Web sites can be prevented.

Untrusted Web site

An "untrusted website" is as follows:

- It does not issue any certificate.
- An unknown source issues the site's certificate.
- The site's certificate has expired.

Troubleshooting

If the connected website has a security problem, a message may appear.

If this is the case, the machine administrator must check the message and instruct the users to take appropriate measures accordingly.

Messages

- "This site has a security problem. The certificate has expired."
- "This site has a security problem. The root certificate for verification does not exist."
- "This site has a security problem. Verification of the server to connect to cannot be performed."
- "This site has a security problem. The http subcontents are included in the https site."*1

*1 The connected website contains non-encrypted data.

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 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.

Also, managing device setting information file with the device management server, allows device setting information file to be imported periodically at a specified time or at device startup.

Data that can be imported and exported

- Web Image Monitor Setting
- Web Service Settings
- System Settings
- Browser Features

Data that cannot be imported or exported

- Some System Settings *1 *2

*1 The setting for the date, settings that require device certificates, 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
- Settings that can be specified via telnet
- @Remote-related data
- Counters
- External 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 and export is possible between machines only if their models, region of use, and the following device configurations 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
- 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.
- You can also use Web Image Monitor to configure the import, export, and server settings.

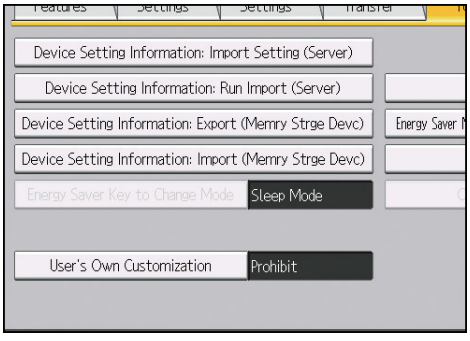
Exporting Device Information

When device information is exported from the control panel, the data is saved on an SD card.

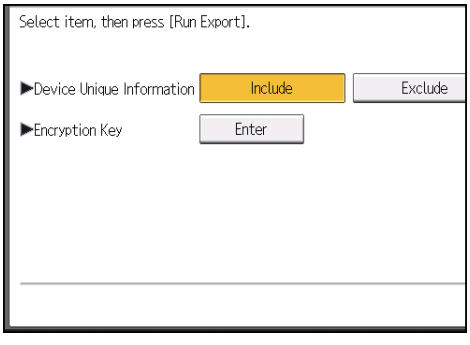
1. **Insert an SD card into the media slot on the side of the control panel.**

   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 user administrator, machine administrator, network administrator, and file administrator privileges.**
3. **Press [System Settings].**
4. **Press [Administrator Tools].**
5. **Press [▼Next] 3 times.**

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.

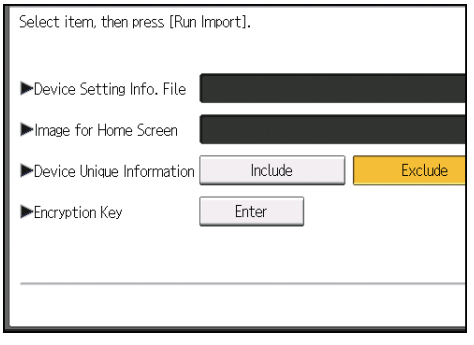
Importing Device Information

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 user administrator, machine administrator, network administrator, and file administrator privileges.**
3. **Press [System Settings].**
4. **Press [Administrator Tools].**
5. **Press [▼Next] 3 times.**
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

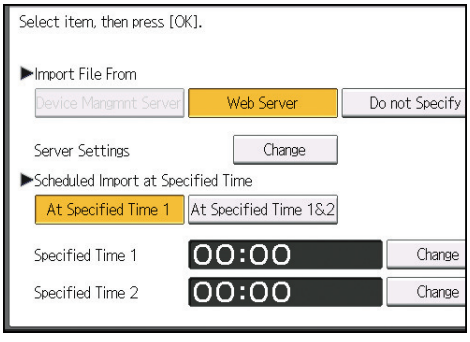
- If import or export fails, you can check the log for the error. The log is stored in the same location as the exported device setting information file.

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 user administrator, machine administrator, network administrator, and file administrator 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.**

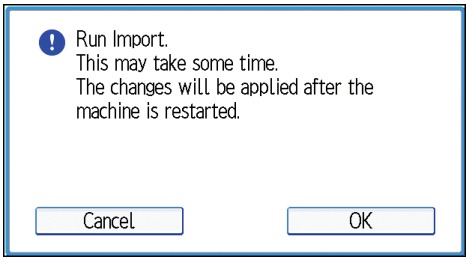
Note

- 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 user administrator, machine administrator, network administrator, and file administrator privileges.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼Next] 3 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 resolve the problem or do not know how to resolve 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 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.	Perform 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 unavailable.

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 recorded 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 unavailable. 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 indicates how often color, duplex and combine printing is used to the total number of printed sheets.

Also, the eco-friendly index indicates how much toner and paper are being saved. Higher eco-friendly index results in greater resource saving.

Note

- When Basic, Windows, or LDAP authentication is used for user authentication, the machine compiles 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 data and displays its overall eco-friendly counter.

Configuring 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. **Press [Eco-friendly Counter Period / Administrator Message].**
5. **Change the settings.**
6. **Press [OK].**
7. **Press [Exit].**
8. **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 1" or "Fixed Message 2", a default message is displayed.

If you select "User Message", the machine administrator can enter a message to be displayed.

Default: [**Fixed Message 1**]

Display Information Screen

Specify whether or not to display the information screen at user login.

Default: [**Off**]

Display Time

Specify when the information screen is displayed.

Default: [**Every Time Login**]

Resetting a Machine's Eco-friendly Counter

A machine's eco-friendly counter can be reset.

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.**

Resetting Users' Eco-friendly Counters

By resetting users' eco-friendly counter, all users' eco-friendly counters are reset.

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 for Address Book Data

Specify how the machine processes a request for auto registration after the registered data in the Address Book reaches 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 when the number of the registered data reaches its maximum.

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

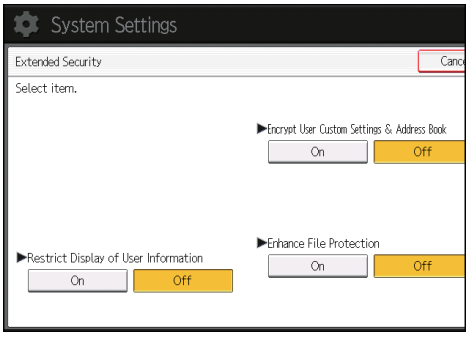
You can delete all data registered in the Address Book.

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.

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 differ depending on the setting.

Restrict Display of User Information

The machine administrator can specify this if user authentication is specified.

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

Default: [**Off**]

Encrypt User Custom Settings & Address Book

The user administrator can specify this.

Encrypt the individual settings of the machine users and the data in the Address Book.

Even if the machine's internal information is obtained illegally, encryption prevents the individual user settings or the Address Book data from being read.

For details, see page 51 "Protecting the Address Book".

Default: [Off]

Enhance File Protection

The file administrator can specify this.

By specifying "Enhance File Protection", files are locked and inaccessible if an invalid password is entered ten times. This can protect files from unauthorized access attempts using random passwords.

If the Enhance File Protection function is enabled, the  icon appears at the bottom right of the screen.

The locked files can only be unlocked by the file administrator.

When files are locked, it is not possible to select them even if the correct password is entered.

Default: [Off]

Settings by SNMPv1, v2

The network administrator can specify this.

If SNMPv1 or SNMPv2 protocols are used to access the machine, authentication cannot be performed, so that paper settings or other settings that the machine administrator specifies can be changed. If you select [Prohibit], the setting can be viewed but not specified with SNMPv1, v2.

Default: [Do not Prohibit]

Authenticate Current Job

This function is not available on this model.

Password Policy

The user administrator can specify this.

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

If you select [Level 1], specify a password using a combination of 2 types of characters selected from upper-case letters, lower-case letters, decimal numbers, and symbols such as #.

If you select [Level 2], specify a password using a combination of 3 types of characters selected from upper-case letters, lower-case letters, decimal numbers, and symbols such as #.

Default: [Off]. There are no restrictions on the number of characters, and the types of characters are not specified.

@Remote Service

The machine administrator can specify this.

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

The machine administrator can specify this.

This setting is to specify whether or not to allow firmware updates on the machine. A service representative updates the firmware, or firmware updates are performed via the network.

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

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

Default: [**Do not Prohibit**]

Change Firmware Structure

The machine administrator can specify this.

This setting is to specify whether or not to prevent changes in the machine's firmware structure. The Change Firmware Structure function detects the machine's status when the SD card is inserted, removed or replaced.

If you select [Prohibit], the machine stops during startup if 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 check 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

The machine administrator can specify this.

If the number of authentication requests exceeds the number specified by the setting, the system recognizes the access as a password attack. The access 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 specify the value between "0" and "100", and then press [#].

Default: [30]

- Measurement Time

  Specify the interval between repeated authentication attempts that result in authentication failures. When the measurement time elapses, the records of authentication attempts are cleared.

  Use the number keys to specify the value between "1" and "10", and then press [#].

  Default: [5]

Note

- Depending on the values specified for the settings for [Max. Allowed No. of Access] and [Measurement Time], you may receive violation detection e-mails frequently.
- If you receive violation detection e-mail s frequently, check the content and review the setting values.

Security Setting for Access Violation

The machine administrator.

When logging in to the machine via a network application, a user may be locked out by mistake because the number of authentication attempts by the user does not match the number of the attempts specified on the machine.

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 how many user accesses are allowed.

    Use the number keys to specify the value between "0" and "60", and then press [#].

    Default: [15]
  - Managed User Host Limit

    Specify how many user accounts can be managed under "Security Setting for Access Violation".

    Use the number keys to specify the value between "50" and "200", and then press [#].

    Default: [200]
  - Password Entry Host Limit

    Specify how many passwords can be managed under "Security Setting for Access Violation".

    Use the number keys to specify the value 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 specify the value between "1" and "10", and then press [#].

  Default: [3]

- Off

Default: [Off]

Device Access Violation

The machine administrator can specify this.

If the number of login requests exceeds the number specified by the setting, the system recognizes the access as an access violation. The access 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], access violations are not detected.

In "Authentication Delay Time", you can specify response delay time for login requests to prevent the system from becoming unresponsive when an access violation is detected.

In "Simultns. Access Host Limit", you can specify the maximum number of hosts that access the machine at one time. If the number of simultaneous accesses exceeds the number specified by the setting, monitoring becomes unavailable and the machine's monitoring status is recorded in the Log.

- Max. Allowed No. of Access

  Specify the maximum number of allowable access attempts.

  Use the number keys to specify the value between "0" and "500", and then press [#].

  Default: [100]

- Measurement Time

  Specify the interval between excessive accesses. When the measurement time elapses, the records of excessive accesses are cleared.

  Use the number keys to specify the value between "10" and "30", and then press [#].

  Default: [10]

- Authentication Delay Time

  Specify authentication delay time when an access violation is detected.

  Use the number keys to specify the value 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 specify the value between "50" and "200", and then press [#].

Default: [200]

Note

- Depending on the values specified for the settings for [Max. Allowed No. of Access] and [Measurement Time], you may receive violation detection e-mails frequently.
- If you receive violation detection e-mails frequently, check the content and review the setting values.

Other Security Functions

This section explains the settings for preventing information leakage.

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.

Checking Firmware Validity

When the machine starts up, this function is used to check that the firmware is valid.

If an error occurs while a verification process is performed, a verification error is displayed on the control panel.

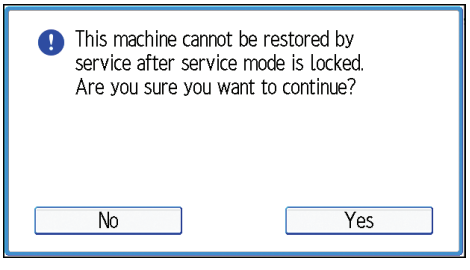
Note that this can also be checked on Web Image Monitor after the machine starts. If an error occurs in a verification process of Web Image Monitor, Web Image Monitor cannot be used. If this is the case, check the control panel.

Restricting a Customer Engineer Operation

You can restrict the customer engineer's access to the service mode.

A customer engineer uses service mode 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 inspection and repair can be performed 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.

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 47 "Auto Logout".
Administrator Tools	Administrator Authentication Management→User Management	Select [On], and then select [Administrator Tools] for "Available Settings". See page 11 "Configuring Administrator Authentication".
Administrator Tools	Administrator Authentication Management→Machine Management	Select [On], and then select each of "Available Settings". See page 11 "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 11 "Configuring Administrator Authentication".
Administrator Tools	Administrator Authentication Management→File Management	Select [On], and then select [Administrator Tools] for "Available Settings". See page 11 "Configuring Administrator Authentication".
Administrator Tools	Extended Security→ Settings by SNMPv1, v2	Prohibit See page 162 "Specifying the Extended Security Functions".

Tab	Item	Setting
Administrator Tools	Extended Security→ Password Policy	"Complexity Setting": Level 1 or higher, "Minimum Character No.": 8 or higher See page 162 "Specifying the Extended Security Functions".
Administrator Tools	Network Security Level	Level 2 To acquire the machine status through printer driver or Web Image Monitor, enable "SNMP" on Web Image Monitor. See page 77 "Specifying Network Security Levels".
Administrator Tools	Service Mode Lock	On See page 169 "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] has already been selected, further encryption settings are not necessary. See page 55 "Encrypting Data on the Machine".

6

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.

Device Management→Configuration

Category	Item	Setting
Device Settings→ Logs	Collect Job Logs	Active
Device Settings→ Logs	Collect Access Logs	Active

Category	Item	Setting
Security→User Lockout Policy	Lockout	Active For details, see page 45 "User Lockout Function".
Security→User Lockout Policy	Number of Attempts before Lockout	5 times or less. For details, see page 45 "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 45 "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 45 "User Lockout Function".
Network→ SNMPv3	SNMPv3 Function	Inactive To use SNMPv3 functions, set "SNMPv3 Function" to [Active], and set "Permit SNMPv3 Communication" to [Encryption Only]. Because SNMPv3 enforces authentication for each packet, Login log will be disabled as long as SNMPv3 is active.
Security→ Network Security	FTP	Inactive Before specifying this setting, set "Network Security Level" to [Level 2] on the control panel.

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

Device Management→Configuration

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.

7. 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 are not specified.

If this appears when you use a function:

- The function is not specified in the Address Book management setting.
- The user administrator must decide whether to additionally assign the privileges to use the function.

If this appears when you specify a machine setting:

- The administrator differs depending on the machine settings users want to specify.
- Using the list of settings, the administrator who is responsible for the machine settings users want to specify must decide whether to additionally assign the privileges to use the function.

"Authentication has failed."

Causes of authentication failures vary and they are indicated by error codes.

For details, see page 176 "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, or LDAP authentication, you must first enable user administrator privileges in [Administrator Authentication Management].

For details, see page 11 "Configuring Administrator Authentication".

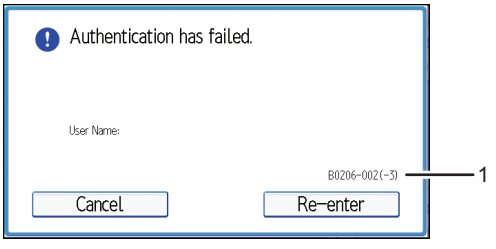
Note

- 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 an error code does not appear on the below lists, write down the error code and contact your service representative.

Error code display position



1. **Error code**

   An error code appears.

Basic Authentication

B0104-000

Failed to decrypt password.

- A password error occurred.

  Make sure the password is entered correctly.

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, while only the administrator has authentication privileges.

- 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 (").

- Create the account again if the account name contains any of these prohibited characters.
- If the account name was entered wrongly, 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 the number of allowed authentication attempts has its maximum.

- Ask the user administrator to unlock the account.

Windows Authentication

W0104-000

Failed to encrypt a password.

- A password error occurred.

  Make sure the password is entered correctly.

W0206-002

The user attempted authentication from an application on the "System Settings" screen, while only the administrator has authentication privileges.

- 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 (").

- Create the account again if the account name contains any of these prohibited characters.
- If the account name was entered wrongly, 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 the number of allowed authentication attempts has reached its limit.

- 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 significant numbers 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 (").

- Create the account again if the account name contains any of these prohibited characters.
- If the account name was entered wrongly, enter it correctly and log on again.

W0406-101

Authentication cannot be completed because of significant numbers of authentication attempts.

- Wait a few minutes, and then try again.
- If the situation does not improve, 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 authentication attack potentials.

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 are more than one DCs, make sure that a confidential relationship has been configured between DCs.

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 upper-case 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 / W0517-000

The authentication server login name is the same as a user name already registered on the machine. (Names are identified 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 words 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 its maximum.)

- 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.

W09XX-019

Automatic user registration on the server failed when an access from the client using the Central Address Book Management function was authenticated.

- Check the network connection between the client and the server.
- Users cannot be registered while the address book on the server is being edited.

LDAP Authentication

L0104-000

Failed to encrypt a password.

- A password error occurred.

  Make sure the password is entered correctly.

L0206-002

A user attempted authentication from an application on the "System Settings" screen, while only the administrator has authentication privileges.

- 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 (").

- Create the account again if the account name contains any of these prohibited characters.
- If the account name was entered wrongly, 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 the number of allowed authentication attempts has reached its maximum.

- 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 search conditions for the login attribute 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 (").

- Create the account again if the account name contains any of these prohibited characters.
- If the account name was entered wrongly, enter it correctly and log in again.

L0406-200

Authentication cannot be completed because of significant numbers of authentication attempts.

- Wait a few minutes, and then try again.
- If the situation does not improve, 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 authentication attack potentials.

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, an error in the network settings might have occurred.

  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 or 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 upper-case letters.

L0409-000

Authentication timed out because the server did not respond.

- Contact the server or network administrator.
- If the situation does not improve, 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 identified 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 words 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 its maximum.)

- 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.

L09XX-019

Automatic user registration on the server failed when an access from the client using the Central Address Book Management function was authenticated.

- Check the network connection between the client and the server.
- Users cannot be registered while the address book on the server is being edited.

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.

Problem	Cause	Solution
User authentication is disabled, yet users registered in the Address Book do not appear.	User authentication might have been disabled without "All Users" being selected for "Protect Destination".	Enable user authentication again, and select [All Users] as the access permission setting of the users you want to display. For details, see page 51 "Protecting the Address Book".
Cannot print when user authentication has been enabled.	User code authentication may not be specified in the printer driver.	Specify user code authentication in the printer driver. For details, see the printer driver Help.
After 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 55 "Encrypting Data on the Machine" has elapsed, contact your service representative.

8. 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].

Understanding the symbols

R/W: Executing, changing, and reading possible.

R: Reading is possible.

-: Executing, changing, and reading are not possible.

System Settings

When administrator authentication is specified, restrictions to user operations differ depending on the configurations in "Available Settings".

[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
[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
[Output: Printer]	R	R/W	R	R	R/W	R
[Output Tray Setting]	R	R/W	R	R	R/W	R
[Paper Tray Priority: Printer]	R	R/W	R	R	R/W	R
[Key Repeat]	R	R/W	R	R	R/W	R
[System Status Display Time]	R	R/W	R	R	R/W	R
[Status Indicator]	R	R/W	R	R	R/W	R
[Z-fold Position]	R	R/W	R	R	R/W	R
[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
[External Keyboard]	R	R/W	R	R	R/W	R
[Program/Change USB Device List]	R	R/W	R	R	R/W	R
[Perfect Binding Cut Fine Adjustment]	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
[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
[Fusing Unit Off Mode (Energy Saving) On/Off]	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

Settings	User	Mach	N/W	File	Unset	Set
[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
[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
[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 connection tests.

[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
[SMTP Server]	R	R	R/W	R	R/W	R
[SMTP Authentication]*3	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 Email Address]	R	R/W	R	R	R/W	R

Settings	User	Mach	N/W	File	Unset	Set
[Email Communication Port]	R	R	R/W	R	R/W	R
[Email Reception Interval]	R	R	R/W	R	R/W	R
[Email Storage in Server]	R	R	R/W	R	R/W	R
[Auto Email Notify]	–	R/W	–	–	R/W	–

*3 Passwords cannot be read.

[Administrator Tools]

Settings	User	Mach	N/W	File	Unset	Set
[Address Book Management]	R/W	R/W *4	R/W *4	R/W *4	R/W *5	R*5
[Address Book: Program / Change / Delete Group]	R/W	R/W *4	R/W *4	R/W *4	R/W *5	R*5
[Address Book: Change Order]	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	–
[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 *6	R/W *7	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
[User Authentication Management]	R	R/W	R	R	R/W	R

Settings	User	Mach	N/W	File	Unset	Set
[Enhanced Authentication Management]	R	R/W	R	R	R/W	R
[Administrator Authentication Management]	R/W *8*9	R/W *9	R/W *9	R/W *9	R/W	–
[Program / Change Administrator]	R/W *10	R/W *10	R/W *10	R/W *10	–	–
[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]						
• [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
• [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	–	–
• [Password Entry Violation]	–	R/W	–	–	–	–
• [Security Setting for Access Violation]	–	R/W	–	–	–	–
• [Device Access Violation]	–	R/W	–	–	–	–
[Program / Change / Delete LDAP Server]*3	–	R/W	–	–	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	–

Settings	User	Mach	N/W	File	Unset	Set
[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]*11	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)]*12	–	–	–	–	–	–
[Device Setting Information: Run Import (Server)]*12	–	–	–	–	–	–
[Device Setting Information: Export (Memry Strge Devc)]*12	–	–	–	–	–	–
[Device Setting Information: Import (Memry Strge Devc)]*12	–	–	–	–	–	–
[Energy Saver Key to Change Mode]	R	R/W	R	R	R/W	R
[User's Own Customization]	R	R/W	R	R	R/W	R
[Select Switchable Languages]	–	R/W	–	–	R/W	–
[Collect Logs]	R	R/W	R	R	R/W	R
[Central Address Book Management]						
• [Central Address Book Management]	R	R/W	R	R	R	R
• [Client Synchronization]*13	R/W	R/W	R	R	R	R

Settings	User	Mach	N/W	File	Unset	Set
• [Synchronize with Server]*14	R/W	R/W	R	R	R	R

*3 Passwords cannot be read.

*4 Only heading changes and user searches are possible.

*5 The items that can be executed, changed, and read differ depending on access privileges.

*6 Can only be cleared.

*7 Can only be printed.

*8 Cannot be changed when the individual authentication function is used.

*9 Only the administrator privilege settings can be changed.

*10 Administrators can only change their own accounts.

*11 Can only be changed to [Off].

*12 R/W can be performed by the administrator with all privileges that include user administrator, machine administrator, network administrator, and file administrator privileges.

*13 This appears if you use the machine as the server.

*14 This appears if you use the machine as a client.

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".

[Tray Paper Settings]

Settings	User	Mach	N/W	File	Unset	Set
[Paper Tray]	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	–	–	–	–

Browser Features

When administrator authentication is set, the restrictions to user operations differ depending on the configuration in "Available Settings".

Settings	User	Mach	N/W	File	Unset	Set
[Browser Default Settings]	R	R/W	R	R	R/W	R
[Settings per Users]	R	R/W	R	R	R/W	R
[View Logs]	R	R	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

Maintenance

When administrator authentication is set, the restrictions to user operations differ depending on the configuration in "Available Settings".

[Maintenance]

Settings	User	Mach	N/W	File	Unset	Set
[Color Registration]	–	R/W	–	–	R/W	–

Web Image Monitor: Display Eco-friendly Counter

These settings are in [Status/Information].

A user can only view their 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].

[Job List]

Settings	User	Mach	N/W	File	Unset	Set
[Current/Waiting Jobs]	–	R	–	–	–	R*1

*1 A user can only view their own job.

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 configuration in "Available Settings".

[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
[Energy Saver Key to Change Mode]	R	R/W	R	R	R/W	R
[Display IP Address on Device Display Panel]	R	R/W	R	R	–	–
[Output Tray]	R	R/W	R	R	R/W	R
[Paper Tray Priority]	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 1-8]	R	R/W	R	R	R/W	R
[Tray A]	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

Settings	User	Mach	N/W	File	Unset	Set
[Perfect Binder Interposer Lower Tray]	R	R/W	R	R	R/W	R
[Low Paper Detection]	R	R/W	R	R	R	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
[Auto Logout Timer]	R	R/W	R	R	R/W	R
[Fusing Unit Off Mode On/Off]	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]*2	R	R/W	R	R	R/W	R
[Classification Code]	R	R/W	R	R	R/W	R
[Delete All Logs]	–	R/W	–	–	R/W	–

*2 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
[Reception Protocol]	–	R/W	–	–	R/W	R
[Email Reception Interval]	–	–	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	–

Settings	User	Mach	N/W	File	Unset	Set
[SMTP Auth. Password]*3	–	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
[POP User Name]	–	R/W	–	–	R/W	–
[POP Password]*3	–	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]*3	–	R/W	–	–	R/W	–

*3 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
[Receivable Email Address/Domain Name Settings]	R	R/W	R	R	R/W	R

[User Authentication Management]

Settings	User	Mach	N/W	File	Unset	Set
[User Authentication Management]	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

[Administrator Authentication Management]

Settings	User	Mach	N/W	File	Unset	Set
[User Administrator Authentication]	R/W	R	R	R	R	R
[Machine Administrator Authentication]	R	R/W	R	R	R	R
[Network Administrator Authentication]	R	R	R/W	R	R	R
[File Administrator Authentication]	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	–	–

Settings	User	Mach	N/W	File	Unset	Set
[Network Administrator]	R	R	R/W	R	–	–
[File Administrator]	R	R	R	R/W	–	–
[Login User Name]*4	R/W	R/W	R/W	R/W	–	–
[Login Password]*4	R/W	R/W	R/W	R/W	–	–
[Encryption Password]*4	R/W	R/W	R/W	R/W	–	–

*4 Administrators can only change their own accounts.

[LDAP Server]

Settings	User	Mach	N/W	File	Unset	Set
[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	–	–	–	–	–	–

Settings	User	Mach	N/W	File	Unset	Set
[Email Failure Notification]*5	–	–	–	–	–	–
[Number of Retries]*5	–	–	–	–	–	–
[Retry Interval]*5	–	–	–	–	–	–
[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.

[Import/Export Device Setting Information]

Settings	User	Mach	N/W	File	Unset	Set
[Export Device Setting Information]*5	–	–	–	–	–	–
[Import Device Setting Information]*5	–	–	–	–	–	–
[Export Image File for Home Screen]*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

[Program/Change USB Device List]

Settings	User	Mach	N/W	File	Unset	Set
[Device 1]	R	R/W	R	R	R/W	R
[Device 2]	R	R/W	R	R	R/W	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 configuration in "Available Settings".

[Interface Settings]

Settings	User	Mach	N/W	File	Unset	Set
[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
[USB Host]	R	R/W	R	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 configuration 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 You cannot disable IPv4 when using Web Image Monitor through an IPv4 connection.

[IPv6]

Settings	User	Mach	N/W	File	Unset	Set
[IPv6]	R	R	R/W *2	R	R/W *2	R
[Host Name]	R	R	R/W	R	R/W	R

Settings	User	Mach	N/W	File	Unset	Set
[Domain Name]	R	R	R/W	R	R/W	R
[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

*2 You cannot disable IPv6 when using Web Image Monitor through an IPv6 connection.

[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	–	–	–

Settings	User	Mach	N/W	File	Unset	Set
[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

[System Log]

Settings	User	Mach	N/W	File	Unset	Set
[System Log]	R	R	R	R	R	–

Web Image Monitor: Security

These settings are in [Configuration] in [Device Management].

Settings	User	Mach	N/W	File	Unset	Set
[Network Security]	–	–	R/W	–	–	–
[Access Control]	–	–	R/W	–	–	–
[SSL/TLS]	–	–	R/W	–	–	–
[ssh]	–	–	R/W	–	R	R
[Site Certificate]	–	–	R/W	–	–	–
[Device Certificate]	–	–	R/W	–	–	–
[IPsec]	–	–	R/W	–	–	–
[User Lockout Policy]	–	R/W	–	–	–	–
[IEEE 802.1X]	–	–	R/W	–	–	–
[Extended Security]						
• [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
• [Authenticate Current Job]	R	R/W	R	R	R/W	R
• [@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	–	–
• [Password Policy]	R/W	–	–	–	–	–
• [Settings by SNMPv1, v2]	R	R	R/W	R	R/W	R
• [Security Setting for Access Violation]	–	R/W	–	–	–	–
• [Password Entry Violation]	–	R/W	–	–	–	–

Settings	User	Mach	N/W	File	Unset	Set
• [Device Access Violation]	–	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 configuration 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
[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

These settings are in [Device Management].

Settings	User	Mach	N/W	File	Unset	Set
[Add User]	R/W	–	–	–	R/W	R/W
[Change]	R/W	–	–	–	R/W	R/W
[Delete]	R/W	–	–	–	R/W	R/W
[Add Group]	R/W	–	–	–	R/W	R/W
[Maintenance]	R/W	–	–	–	–	–
[Central Address Book Management]	R/W	–	–	–	–	–

Web Image Monitor: Central Address Book Management

These settings are in [Device Management].

This does not appear if you have user administrator privilege. In this case, specify it by accessing [Device Management] > [Address Book].

Settings	User	Mach	N/W	File	Unset	Set
[Central Address Book Management]	–	R/W	–	–	–	–

Web Image Monitor: Main Power Off

These settings are in [Device Management].

Settings	User	Mach	N/W	File	Unset	Set
[Main Power Off Mode]	–	R/W	–	–	–	–
[OK]	–	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 configuration 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 configuration 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 only change 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

List of Operation Privileges for Address Books

Understanding headers

- Read

  Users assigned with read privileges.

- Edit

  Users assigned with editing privileges.

- E/D

  Users assigned with edit/delete privileges.

- Full

  Users assigned with full control privileges.

- Entry

  Indicates a user whose personal information is registered in the Address Book. Also, it indicates any user who knows his or her user login name and password.

- User

  Indicates the user administrator.

Understanding the symbols

R/W: Executing, changing, and reading are possible.

R: Reading is possible.

–: Executing, changing, 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
[Registration No.]	R	R/W	R/W	R/W	R/W	R/W
[Display Priority]	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

Settings	Read	Edit	E/D	Full	Entry	User
[Login User Name]	–	–	–	–	R	R/W
[Login Password]	–	–	–	–	R/W *1	R/W *1
[Other Functions]	–	–	–	–	R	R/W

*1 Passwords cannot be read.

[Protection]

Settings	Read	Edit	E/D	Full	Entry	User
[Protect Destination]: [Permissions for Users / Groups]	–	–	–	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

INDEX

U

W

EN GB EN US EN AU M238-1022