



User Guide

For RICOH IM 370/370F/460F

Author: RICOH COMPANY, LTD.

Date: 2023.08

Part Number: D0DM7314

For information not found in this manual, see the online manuals available on our web site (<https://www.ricoh.com/>) or via the control panel.

[Top Page](#)

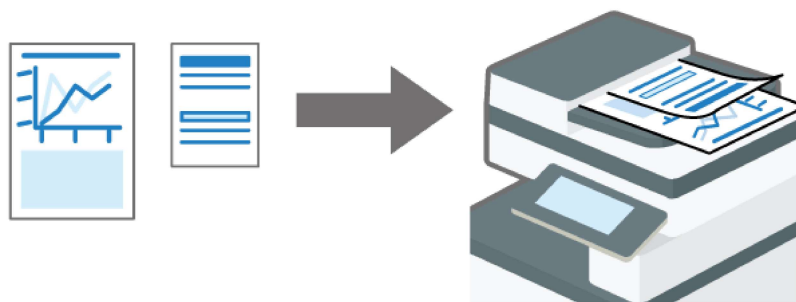
User Guide IM 370/370F/460F/460FTL

Recommended Functions

Frequently Read Pages



Copying in Page Order

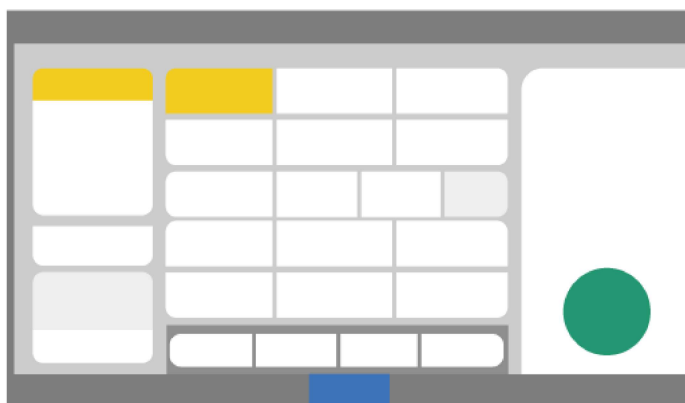


Copying Mixed-size Originals

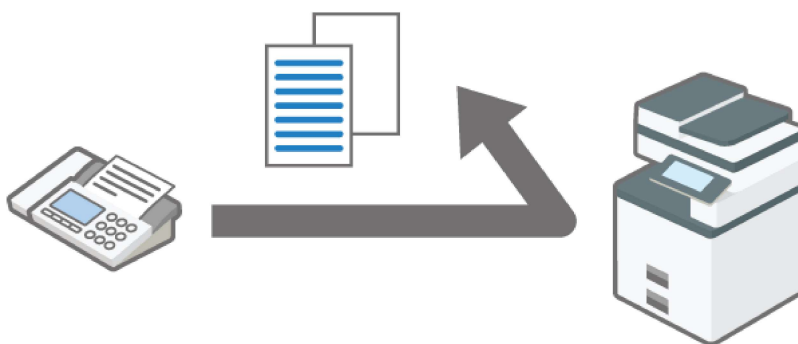




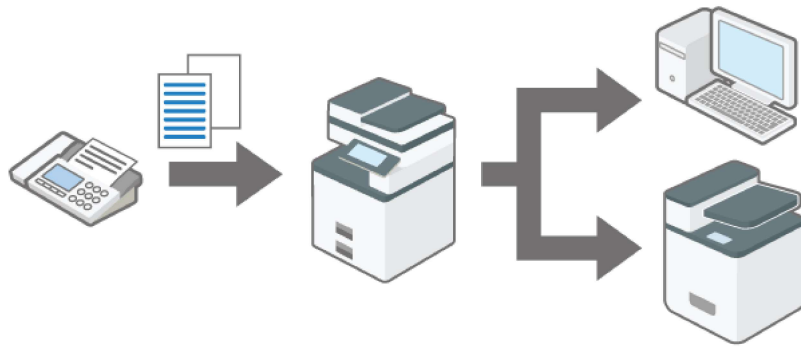
Changing the Default Value of Each Function



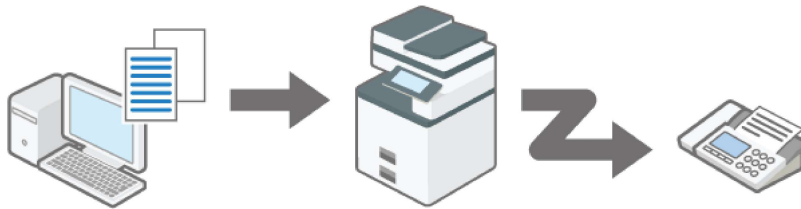
How to Use the Copy Screen



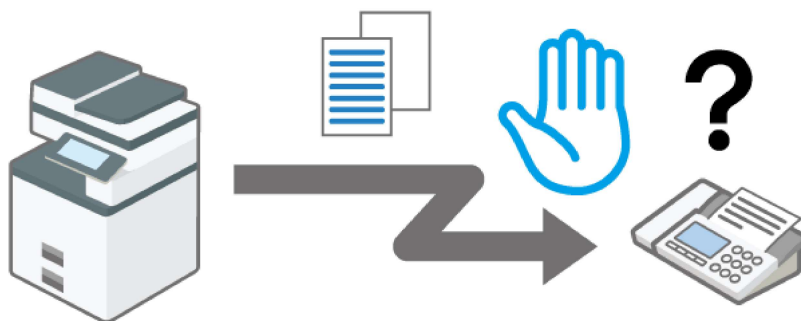
Preventing Unwanted Faxes



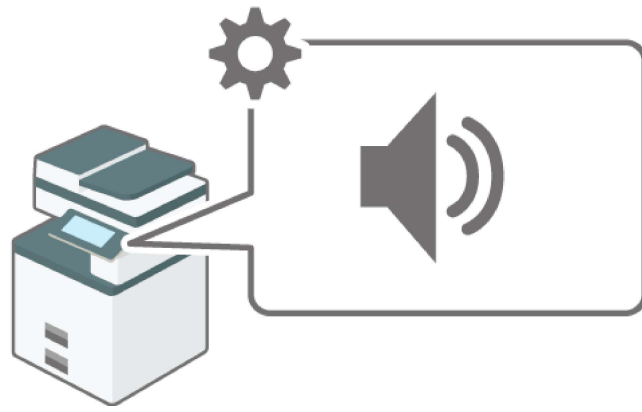
Transferring a Received Fax Document to E-mail Address or Folder



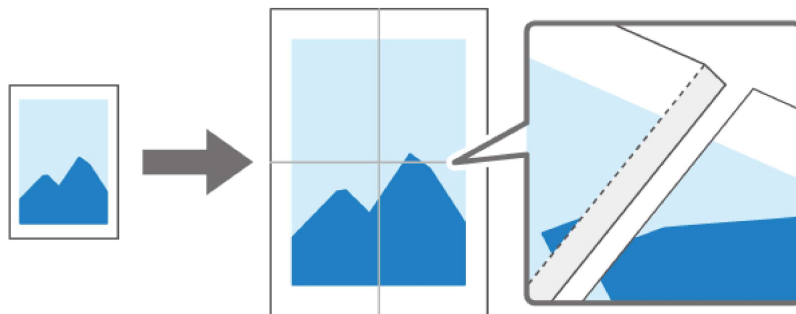
Sending Faxes from a Computer



Preventing a Fax Transmission to the Wrong Destination



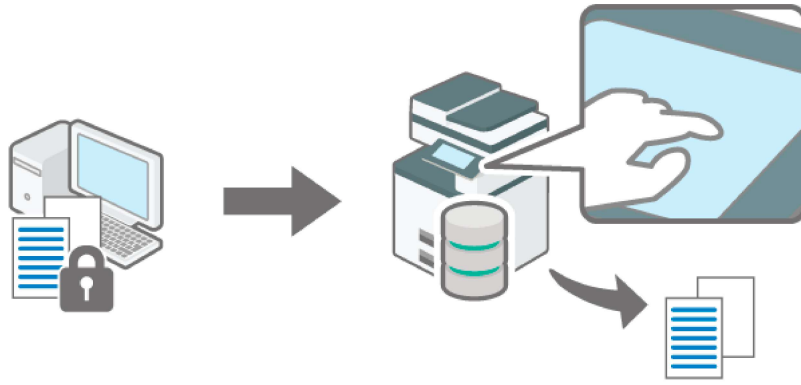
Setting the Sound Volume and Type



Printing a Poster by Dividing and Tiling a Single Page across Multiple Sheets



Printing on Custom-sized Paper Loaded on the Bypass Tray



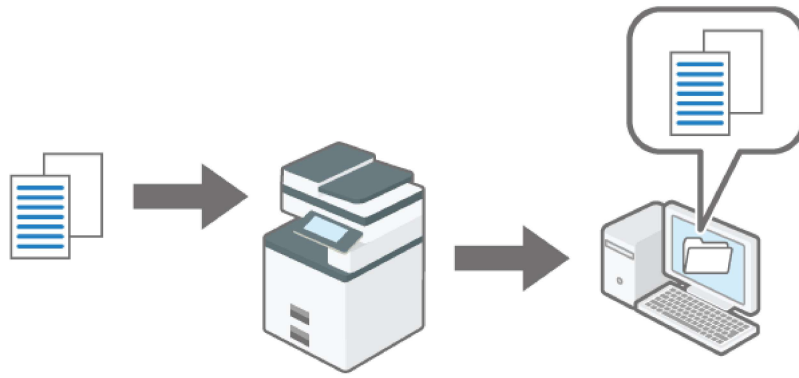
Storing Documents to Print in the Machine



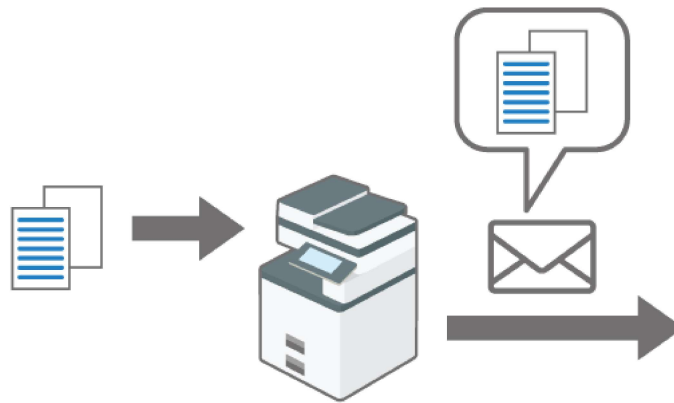
Registering Frequently Used Settings



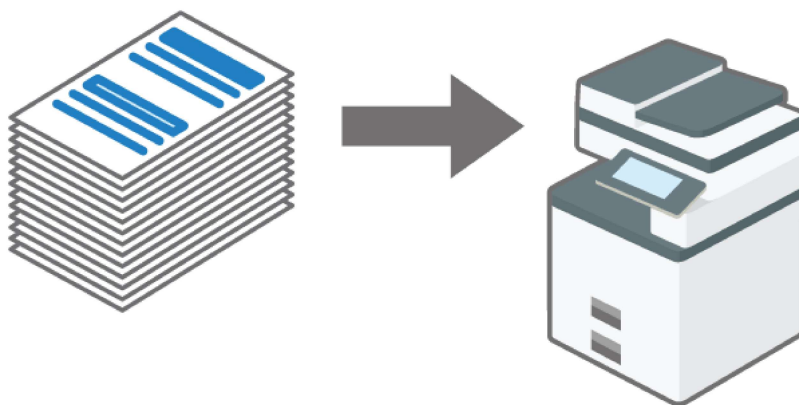
Applying Different Print Settings Depending on the Document Type



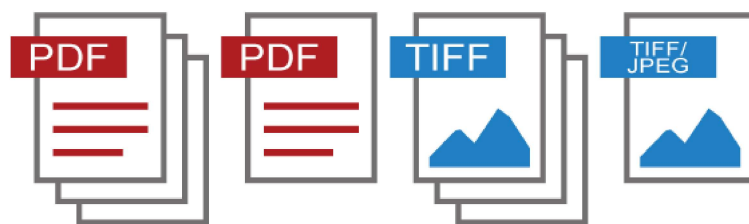
Scanning Documents and Sending the Scanned Data to a Folder



Scanning Documents and Sending the Scanned Data by E-mail



Combining the Data of Multiple Scans into a Single File

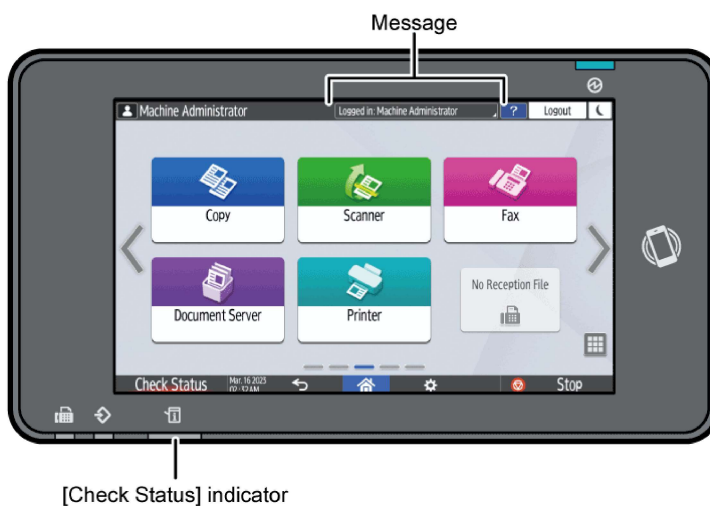


Specifying the File Type or File Name When Scanning a Document

[Page Top](#)

Checking the Indicators, Icons, and Messages on the Control Panel

The machine notifies you of the machine condition or status of an application with the [Check Status] indicator or a message displayed on the control panel. Check the status and resolve the problem accordingly.



- **Message**
Displays a message indicating the status of the machine or application. Press the message to display it in full text. You can also view more than one message as a list.
- **[Check Status] indicator**
If there is a problem such as a paper jam, the [Check Status] indicator lights up or flashes along with a message displayed on the screen. Press [Check Status] to check the status of the machine or application, and resolve the problem accordingly.

When an Icon is Displayed with a Message

When you need to resolve a problem such as a paper jam, an icon is displayed at the beginning of a message. See the table below for the meaning of each icon.

Icon	Condition	Solution and reference
	Maintenance or repair is required.	Prepare for maintenance or consider repairing the machine.

	Toner is almost depleted, or has run out.	Prepare a replacement toner. Replace the toner when it runs out. Replacing the Toner  Note If  appears when there is a lot of toner, pull out the print cartridge by following the toner replacement procedure that is displayed on the screen, and then set it back again.
	The waste toner bottle is full, or almost full.	Prepare a replacement waste toner bottle. Replace the bottle when it becomes full. Replacing the Waste Toner Bottle
	A cover is open.	Check that all covers of the machine and external devices are closed.



Section Top

When the [Check Status] Indicator is lit or flashing

The [Check Status] indicator notifies the user when the machine requires immediate attention.

Flashing in red

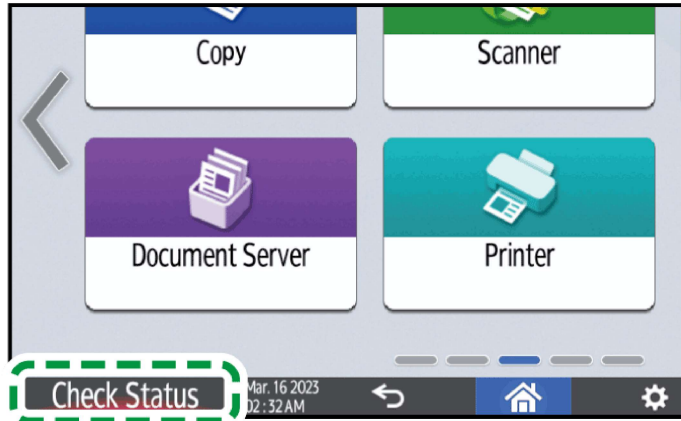
The machine is unavailable for use. Press [Check Status] and resolve the problem as soon as possible.

Flashing in yellow

Maintenance on the machine needs to be performed soon. Perform the required procedure accordingly.

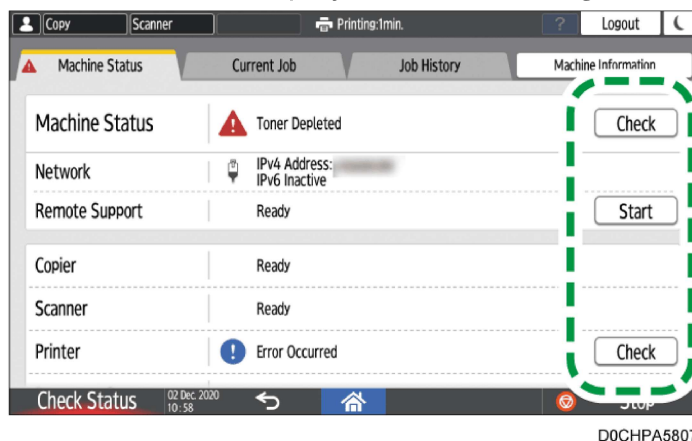
You can display the status confirmation screen with [Check Status]. On the screen, check the detailed status of the machine or application.

1. Press [Check Status].



2. Press [Check] to check the details, and perform the required procedure.

When an Icon is Displayed with a Message



: The machine cannot be used.

: Some of the functions cannot be used, or the toner is almost depleted.

Note

- Depending on the machine condition, such as a paper jam or open cover, the status confirmation screen may be displayed automatically without pressing [Check Status].

Section Top

Collecting Logs

You can collect logs stored in the machine to check the usage of the machine's various functions, error histories, and detailed access data to the machine.

- Download the collected logs from the internal storage on the machine converting into a CSV file.
- Use Web Image Monitor to download the collected logs. You can also use a log collect server instead of Web Image Monitor.

Note

- Contact your sales representative for details about a log collect server.

Log Types

The machine stores three types of logs as follows:

Job log

- User file-related operations such as copying, storing in the Document Server, printing, sending faxes, and sending scan files
- Printing reports such as the configuration list output from the control panel

Access log

- Authentications such as login and logout activities
- Stored file operations such as creating, editing, and deleting
- Customer engineer operations such as internal storage formatting
- System operations such as viewing log transfer results
- Security operations such as specifying settings for encryption, unprivileged access detection, user lockout, and firmware authentication

Eco-friendly Log

- Main power ON and OFF
- Transitions in power status
- Job run times or time interval between jobs
- Paper consumption per hour
- Power consumption of the machine

[Section Top](#)

Specifying Logs to Collect

Specify the types and items of logs to collect.

Specifying logs to collect using the control panel

1. **Log in to the machine as the machine administrator on the control panel.**

Logging in to the Machine as an Administrator

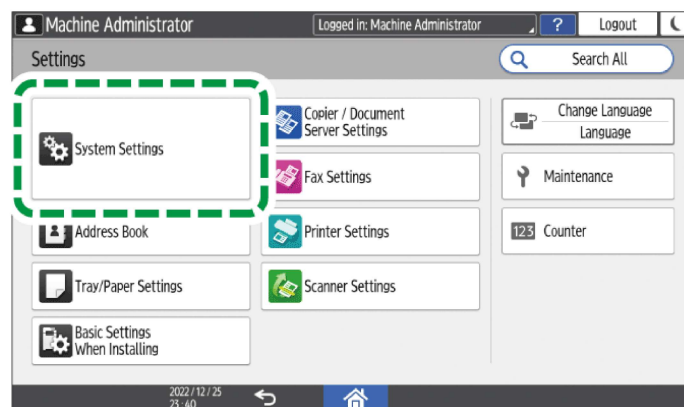
When custom-privileges administrators are registered, you can log in to the machine as a custom-privileges administrator with the Data Management privilege as well.

Logging in to the Machine as a Custom-Privileges Administrator

2. **On the Home screen, press [Settings].**

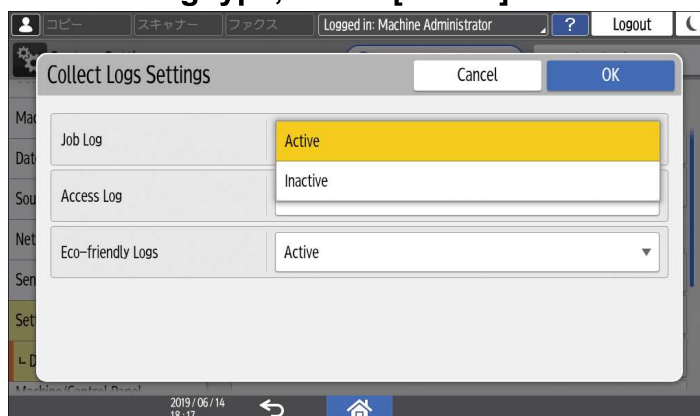


3. **Press [System Settings].**



4. **Press [Settings for Administrator] ► [Data Management] ► [Collect Logs Settings].**

5. **For each log type, select [Active] from the list.**



6. **Press [OK].**

7. **Press [Home] ().**

8. **When the confirmation dialog is displayed, press [Exit]**

The machine restarts automatically.

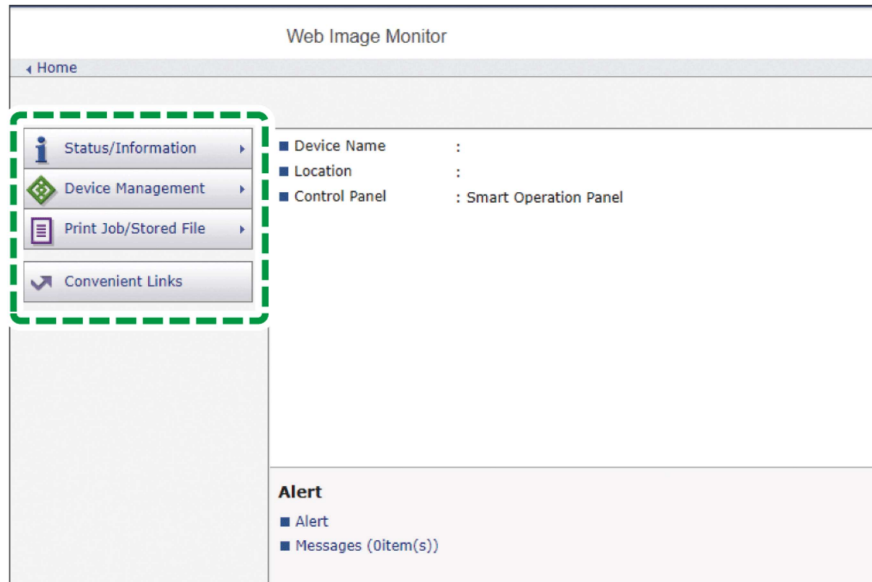
1. **Log in to the machine as the machine administrator from Web Image Monitor.**

Logging in to the Machine as an Administrator

When custom-privileges administrators are registered, you can log in to the machine as a custom-privileges administrator with the Data Management privilege as well.

Logging in to the Machine as a Custom-Privileges Administrator

2. **Click [Configuration] on the [Device Management] menu.**



3. **On the "Configuration" screen, click [Logs] in the "Device Settings" category.**

4. **Select [Active] of "Collect Job Logs", "Collect Access Logs", or "Collect Eco-friendly Logs" according to the log type to collect.**

5. **Specify the items to record in each log for "Job Log Collect Level", "Access Log Collect Level", or "Eco-friendly Log Collect Level".**

Job Log Collect Level

- Level 1: All job logs are collected.

Access Log Collect Level

- Level 1: The following items are recorded in the access log.
Internal Storage Format, All Logs Deletion, Log Setting Change, and Log Collection Item Change
- Level 2: All access logs are collected.

Eco-friendly Log Collect Level

- Level 1: Eco-friendly Logs are not collected.
- Level 2: All eco-friendly logs are collected.

When a level is changed, the selection status of log details changes according to the level. You can change the settings of some of the items whether to collect or not.

6. **Click [OK].**

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

If nothing appears on the screen after you click [OK], wait for a while, and then refresh the web browser screen.

8. **Log out of the machine, and then exit the Web browser.**

 Note

- When you changed Active/Inactive of Log Collect, delete all logs.

Deleting All Logs

[Section Top](#)

Job Log Information Items

Job Log Item	Log Type Attribute	Content
Copier: Copying	Copier: Copying	Details of normal and Sample Copy jobs.
Copier: Copying and Storing	Copier: Copying and Storing	Details of files stored in the Document Server that were also copied at the time of storage.
Document Server: Storing	Document Server: Storing	Details of files stored using the Document Server screen.
Document Server: Stored File Downloading	Document Server: Stored File Downloading	Details of files stored in the Document Server and downloaded using Web Image Monitor.
Stored File Printing	Stored File Printing	Details of files printed using the Document Server screen.
Scanner: Sending	Scanner: Sending	Details of sent scan files.
Scanner: Sending and Storing	Scanner: Sending and Storing	Details of scan files stored in the Document Server that were also sent at the time of storage.
Scanner: Storing	Scanner: Storing	Details of scan files stored in the Document Server.
Scanner: Stored File Downloading	Scanner: Stored File Downloading	Details of scan files stored in the Document Server and downloaded using Web Image Monitor.
Scanner: Stored File Sending	Scanner: Stored File Sending	Details of the stored scan files that were also sent.

Printer: Printing	Printer: Printing	Details of normal print jobs.
Printer: Locked Print (Incomplete)	Printer: Locked Print (Incomplete)	Log showing Locked Print documents temporarily stored on the machine.
Printer: Locked Print	Printer: Locked Print	Log showing Locked Print documents temporarily stored on the machine and printed from the control panel or through Web Image Monitor.
Printer: Sample Print (Incomplete)	Printer: Sample Print (Incomplete)	Log showing Sample Print documents temporarily stored on the machine.
Printer: Sample Print	Printer: Sample Print	Log showing Sample Print documents temporarily stored on the machine and printed from the control panel or through Web Image Monitor.
Printer: Hold Print (Incomplete)	Printer: Hold Print (Incomplete)	Log showing Hold Print documents temporarily stored on the machine.
Printer: Hold Print	Printer: Hold Print	Log showing Hold Print documents temporarily stored on the machine and printed from the control panel or through Web Image Monitor.
Printer: Stored Print	Printer: Stored Print	Details of Stored Print files stored on the machine.
Printer: Store and Normal Print	Printer: Store and Normal Print	Details of Stored Print files that were printed at the time of storage (when "Job Type:" was set to [Store and Print] in printer properties).
Printer: Stored File Printing	Printer: Stored File Printing	Details of Stored Print files printed from the control panel or Web Image Monitor.
Printer: Document Server Sending	Printer: Document Server Sending	Details of files stored in the Document Server when "Job Type:" was set to [Document Server] in printer properties.
Printer: Hold Print File Printing	Printer: Hold Print File Printing	When a document is held for printing and stored temporarily on the machine, this records the time a user specified for the document to be printed from the control panel or Web Image Monitor.
Report Printing	Report Printing	Details of reports printed from the control panel.

Result Report Printing/Emailing	Result Report Printing/Emailing	Details of job results printed or notified by e-mail.
Scanner: TWAIN Driver Scanning	Scanner: TWAIN Driver Scanning	Details of scan files that were scanned using TWAIN driver.
Fax: Sending	Fax: Sending	Details of faxes sent from the machine.
Fax: LAN-Fax Sending	Fax: LAN-Fax Sending	Details of fax files sent from computers.
Fax: Storing	Fax: Storing	Details of fax files stored on the machine using the Fax function.
Fax: Stored File Printing	Fax: Stored File Printing	Details of fax files stored on the machine and printed using the Fax function.
Fax: Stored File Downloading	Fax: Stored File Downloading	Details of fax files stored in the Document Server and downloaded using Web Image Monitor.
Fax: Receiving	Fax: Receiving	Details of received fax files.
Fax: Receiving and Delivering	Fax: Receiving and Delivering	Details of faxes that received and delivered by the machine.
Fax: Receiving and Storing	Fax: Receiving and Storing	Details of faxes that received and stored by the machine.

Section Top

Access Log Information Items

Access Log Item	Log Type Attribute	Content
Login ^{*1}	Login	Times of login.
Logout	Logout	Times of logout.
File Storing	File Storing	Details of files stored in the Document Server.
Stored File Deletion	Stored File Deletion	Details of files deleted from the Document Server.

All Stored Files Deletion	All Stored Files Deletion	Details of deletions of all Document Server files.
Internal Storage Format *2	Internal Storage Format	Details of internal storage formatting.
Unauthorized Copying	Unauthorized Copying	Details of documents scanned with "Data Security for Copying".
All Logs Deletion	All Logs Deletion	Details of deletions of all logs.
Log Setting Change	Log Setting Change	Details of changes made to log settings.
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 log items to collect.
Collect Encrypted Communication Logs	Collect Encrypted Communication Logs	Log of encrypted transmissions between the utility, Web Image Monitor or outside devices.
Access Violation*3	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*4	Firmware: Structure	Details of checks for changes to firmware module structure made at times such as when the machine was switched on.
Firmware: Invalid	Firmware: Invalid	Details of checks for firmware validity made at times such as when the machine was switched on.
Date/Time Change	Date/Time Change	Details of changes made to date and time settings.
File Access Privilege Change	File Access Privilege Change	Log for changing the access privilege to the stored files.

Password Change	Password Change	Details of changes made to the login password.
Administrator Change	Administrator Change	Details of changes of administrators.
Address Book Change	Address Book Change	Details of changes made to Address Book entries.
Capture Error	Capture Error	Details of file capture errors.
Machine Configuration	Machine Configuration	Log of changes to the machine's settings.
Back Up Address Book	Back Up Address Book	Log of when data in the Address Book is backed up.
Restore Address Book	Restore Address Book	Log of when data in the Address Book is restored.
Enhanced Print Volume Use Limitation: Tracking Permission Result	Enhanced Print Volume Use Limitation: Tracking Permission Result	Log of when a tracking error occurs.
Counter Clear Result: Selected User(s)	Counter Clear Result: Selected User(s)	Log of when the counter for an individual user is cleared.
Counter Clear Result: All Users	Counter Clear Result: All Users	Log of when the counters for all users are cleared.
Import Device Setting Information	Import Device Setting Information	Log of when a device setting information file is imported.
Export Device Setting Information	Export Device Setting Information	Log of when a device setting information file is exported.
Creating/Deleting Folders	Creating/Deleting Folders	Log of when folders are created and deleted.
Stored File Editing	Stored File Editing	Log of a file edited by being combined, inserted, or deleted.
Insertion into another File	Insertion into another File	Log of combining or inserting to another file.

*1 There is no "Login" log made for SNMPv3.

*2 If the internal storage 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.

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

*4 The first log created after the power is turned on is the "Firmware: Structure" log.

[Section Top](#)

Eco-friendly Log Information Items

Eco-friendly Log Items	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.

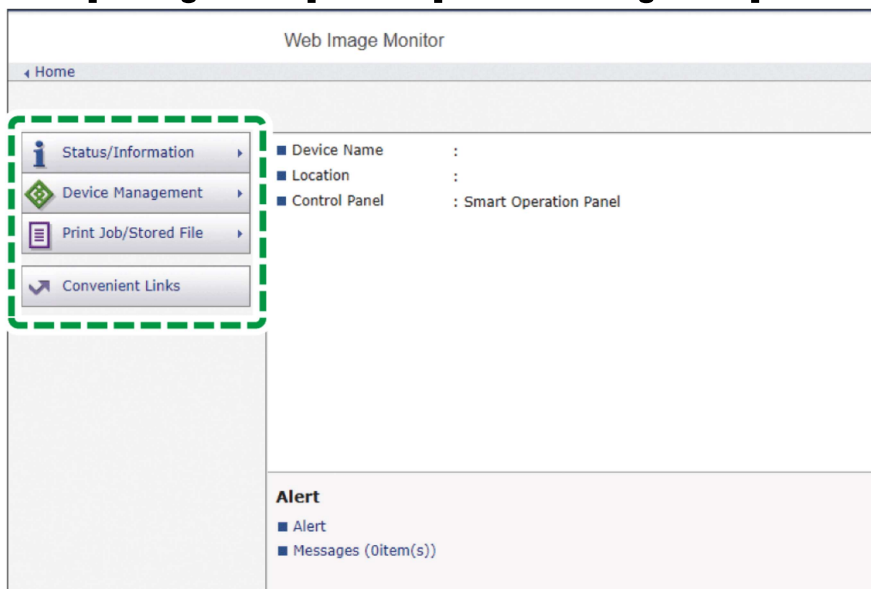
[Section Top](#)

Downloading the Logs

You can download the logs recorded on the machine as a CSV file.

- 1. Log in to the machine as the machine administrator from Web Image Monitor.**
Logging in to the Machine as an Administrator

2. Click [Configuration] on the [Device Management] menu.



3. On the "Configuration" screen, click [Download Logs] in the "Device Settings" category.

4. Select the log type on "Logs to Download", and then click [Download].

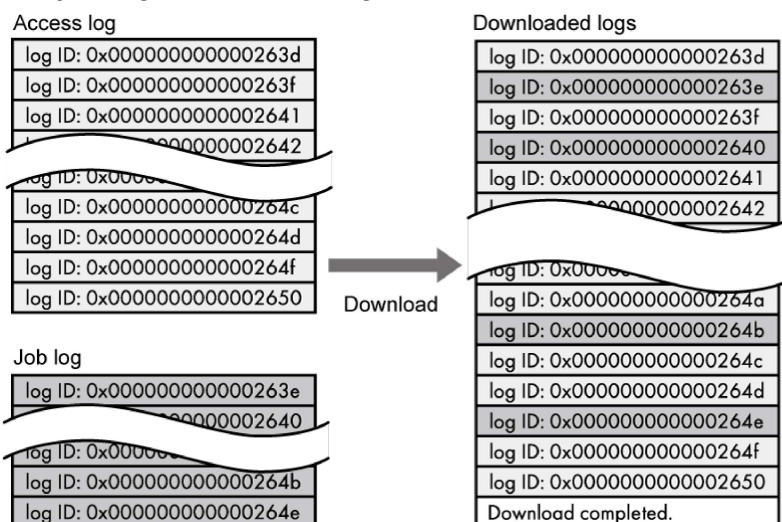
The downloaded log files are stored in the "Download" folder.

- Security Logs: Downloads both job logs and access logs into a single file.
- Security Logs (Job Log): Downloads job logs only.
- Security Logs (Access Log): Downloads access logs only.
- Eco-friendly Logs: Downloads eco-friendly logs only.

5. Log out of the machine, and then exit the Web browser.

Note

- When a log is downloaded successfully, "Download completed." will appear in the last line of the log file.
- The job log and access log are downloaded as one file aligned in the order of the log IDs.



DZX792

- After downloading logs, delete all logs.

- Downloaded logs contain data of completed jobs recorded up to the time you click [Download]. 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.
- Downloaded log files use UTF-8 character encoding. To view a log file, open it using an application that supports UTF-8.
- The machine administrator must manage downloaded log files appropriately.

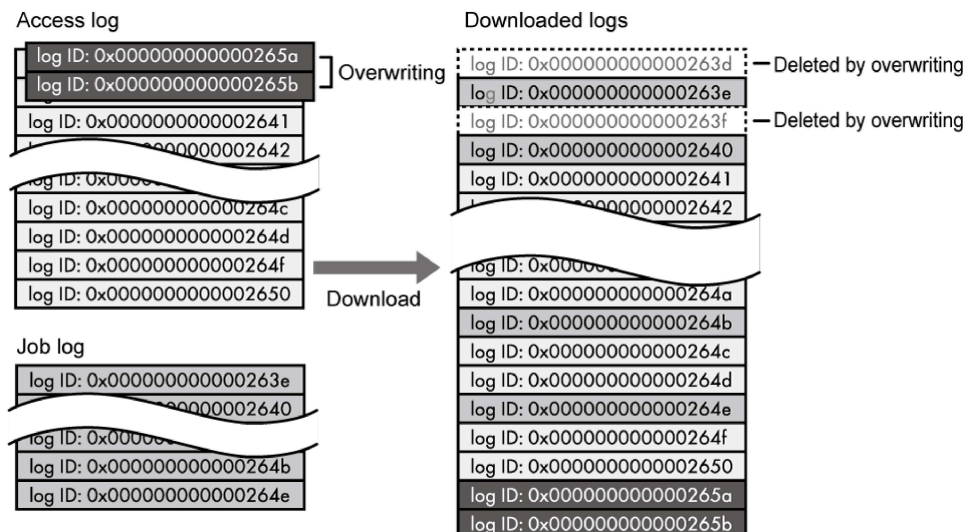
Number of logs that can be kept on the machine

Maximum numbers of logs that can be stored in the machine are as follows:

Log types	Maximum number of logs
Job logs	4,000
Access logs	12,000
Eco-friendly Logs	4,000

- If the number of logs that can be stored on the machine exceeds the limit 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.
- The example below shows when the number of stored logs exceeds the maximum and old logs are overwritten.

When the oldest two access logs are overwritten by the newest two access logs, the downloaded logs lack the log IDs.



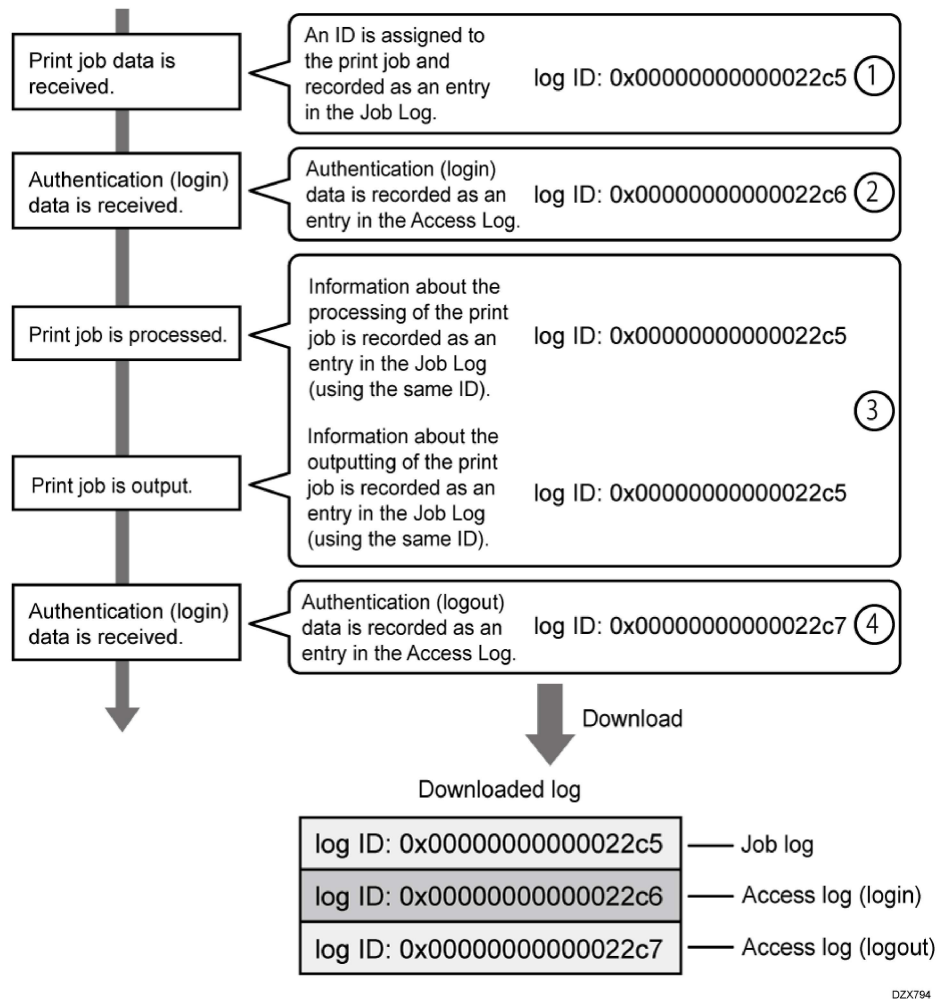
DZX793

- Check the message in the last line of the downloaded logs to determine whether overwriting occurs or not while the logs were downloading. The messages are shown below:
 - When overwriting did not occur:
Download completed.
 - When overwriting occurred:
Download completed.
A part of the logs before Log ID XXXX does not exist anymore.
(The logs before "Log ID XXXX" are deleted.)

Order of printer job log and access log

Print log entries are recorded before the login entry is recorded in the access log.

Details of jobs (reception, processing, output of the jobs' data, and so on) are recorded as single entries.



When the machine receives a print job, it creates a log ID for the job and records information about data reception in the job log. (1)

The machine then creates a log ID for the authentication information and records it in the access log of login. (2)

Log related to job data processing is added in the job log created first. (3)

In the end, it creates a log ID for logout entry and records it in the access log. (4)

In the result, when downloading job log, access log of login, and access log of logout, they are aligned in this order.

Section Top

Deleting All Logs

You can delete all logs recorded on the machine.

[Delete All Logs] appears when one of the job log, access log, or eco-friendly log is set to [Active].

Deleting all logs using the control panel

1. Log in to the machine as the machine administrator on the control panel.

Logging in to the Machine as an Administrator

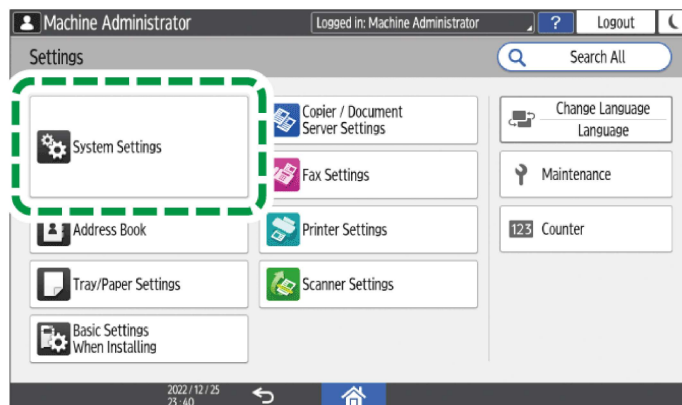
When custom-privileges administrators are registered, you can log in to the machine as a custom-privileges administrator with the Data Management privilege as well.

Logging in to the Machine as a Custom-Privileges Administrator

2. On the Home screen, press [Settings].



3. Press [System Settings].



4. Press [Settings for Administrator] ► [Data Management] ► [Delete All Logs].

5. When the confirmation dialog is displayed, press [Yes].

6. When the confirmation dialog is displayed, press [Exit].

7. Press [Home] (🏠), and then log out of the machine.

Deleting all logs using Web Image Monitor

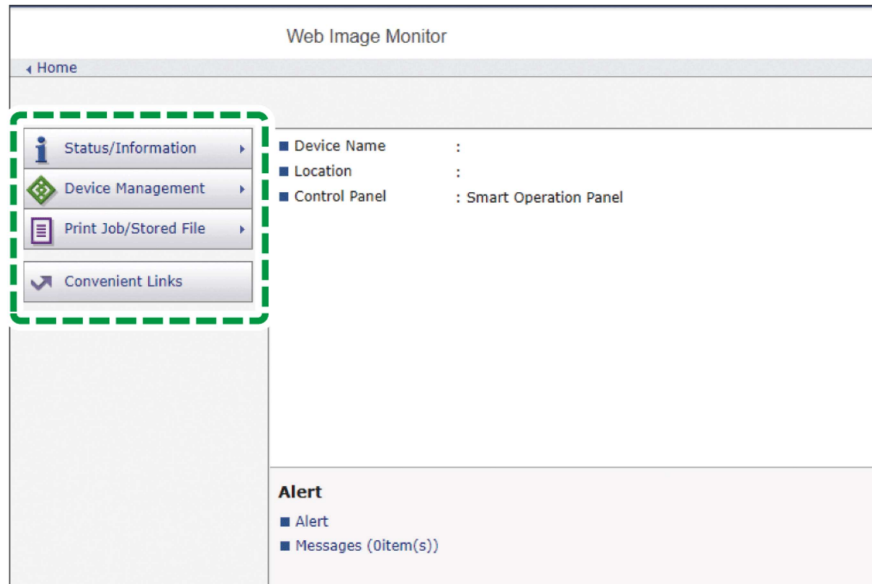
1. **Log in to the machine as the machine administrator from Web Image Monitor.**

Logging in to the Machine as an Administrator

When custom-privileges administrators are registered, you can log in to the machine as a custom-privileges administrator with the Data Management privilege as well.

Logging in to the Machine as a Custom-Privileges Administrator

2. **Click [Configuration] on the [Device Management] menu.**



3. **On the "Configuration" screen, click [Logs] in the "Device Settings" category.**

4. **Click [Delete] of "Delete All Logs", and then click [OK].**

5. **Log out of the machine, and then exit the Web browser.**

Section Top

Disabling Log Transfer to the Log Collection Server

Disabling log transfer to the log collection server using the control panel

1. **Log in to the machine as the machine administrator on the control panel.**

Logging in to the Machine as an Administrator

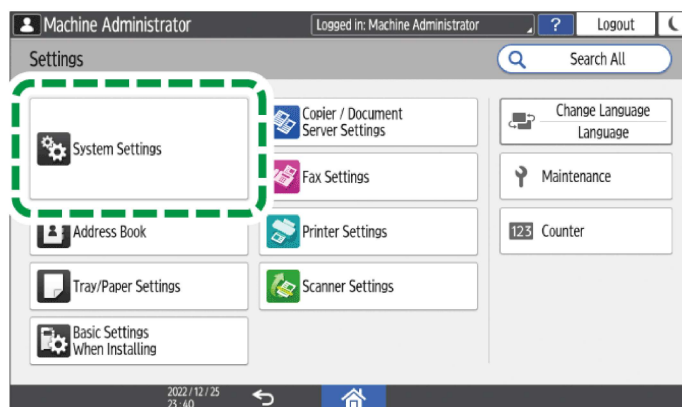
When custom-privileges administrators are registered, you can log in to the machine as a custom-privileges administrator with the Data Management privilege as well.

Logging in to the Machine as a Custom-Privileges Administrator

2. **On the Home screen, press [Settings].**

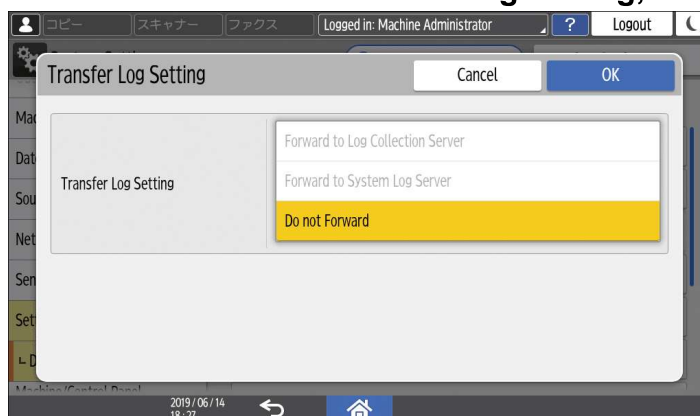


3. **Press [System Settings].**



4. **Press [Settings for Administrator] ► [Data Management] ► [Transfer Log Setting].**

5. **From the list next to Transfer Log Setting, select [Do not Forward].**



6. **Press [OK].**

7. **When the confirmation dialog is displayed, press [OK].**

8. **Press [Home] (🏠), and then log out of the machine.**

Disabling log transfer to the log collection server using Web Image Monitor

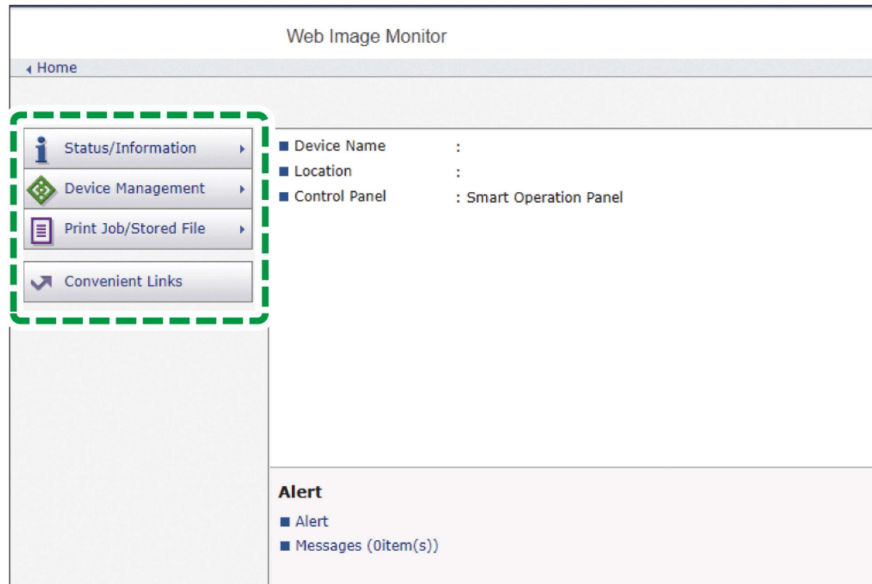
1. **Log in to the machine as the machine administrator from Web Image Monitor.**

Logging in to the Machine as an Administrator

When custom-privileges administrators are registered, you can log in to the machine as a custom-privileges administrator with the Data Management privilege as well.

Logging in to the Machine as a Custom-Privileges Administrator

2. **Click [Configuration] on the [Device Management] menu.**



3. **On the "Configuration" screen, click [Logs] in the "Device Settings" category.**

4. **Under "Common Settings for All Logs", select [Inactive] of "Transfer Logs", and then click [OK].**

5. **Log out of the machine, and then exit the Web browser.**

Section Top

Date/Time/Timer

This section describes the settings in [Date/Time/Timer] under [System Settings].

How to Use the "Settings"

Date/Time

Setting Items	Description
---------------	-------------

Daylight Saving Time

Specify the period and time for daylight saving.

 **Region A** (mainly Europe)

- Default: **[Active]**

 **Region A** (mainly Asia)/ **Region B** (Taiwan)

- Default: **[Inactive]**

 **Region B** (mainly North America)

- Default: **[Active]**

- Start Time/End Time

Specify Month, Week, Day of the Week, Time to start/end the daylight saving time.

- Default of Month

 **Region A** (mainly Europe)

- Start Time: **[March]**
- End Time: **[October]**

 **Region B** (mainly North America)

- Start Time: **[March]**
- End Time: **[November]**

- Default of Week

 **Region A** (mainly Europe)

- Start Time: (Final week)
- End Time: (Final week)

 **Region B** (mainly North America)

- Start Time: **[2nd]**
- End Time: **[1st]**

- Default of Day of the Week: **[Sunday]**

- Default of Time

 **Region A** (mainly Europe)

- Start Time: **[00]**
- End Time: **[01]**

 **Region B** (mainly North America)

- Start Time: **[02]**
- End Time: **[02]**

- Offset

Specify the amount of time to move the clock forward for the daylight saving time.

- Default: **[1] hour(s) [0] minute(s)**

Set Date	Set the date and time for the machine's internal clock.
Set Time	 Region A (mainly Europe and Asia)/  Region B (Taiwan) Enter the time using the 24-hour format.  Region B (mainly North America) Enter the time using the 12-hour format.
Time Zone	Specify the standard time in the region where the machine is used.  Region A (mainly Europe) • Default: [GMT+01:00]  Region A (mainly Asia) • Default: [GMT+08:00]  Region A (Korea) • Default: [GMT+09:00]  Region B (mainly North America) • Default: [GMT-05:00]  Region B (Taiwan) • Default: [GMT+08:00]

Section Top

Timer

Setting Items	Description
Sleep Mode Timer	Specify the time to wait before entering Sleep mode for power saving. • Default: [1] minute(s) When quick card authentication is enabled, the machine does not enter Sleep mode regardless of this setting. Preparation for Quick Card Authentication Setting

Fusing Unit Off Mode (Energy Saving) On/Off	Specify whether to enable Fusing Unit Off mode when no operations are in progress for a certain period. • Default: [On] When you select [On], specify the following items: • Exit Fusing Unit Off Mode Specify when to exit Fusing Unit Off mode • On Printing • On Operating Control Panel If the Copier function screen is displayed, the machine exits Fusing Unit Off mode regardless of this setting. • Fusing Unit Off Mode Timer Specify the time that the machine enters the Fusing Unit Off mode.
System Auto Reset Timer	Specify the time to automatically switch the screen to the Home screen when no operations are in progress for a certain period. You can specify the screen other than the Home screen by [Display/Input] ► [Display] ► [Function Priority (Default Displayed Application)]. • Default: [On], [60] second(s)
Copier/Document Server Auto Reset Timer Fax Auto Reset Timer Printer Auto Reset Timer Scanner Auto Reset Timer	Specify the time to elapse before the function is reset when no operations are in progress for a certain period. • Default • Copier/Document Server: [On], [60] second(s) • Fax: [30] second(s) • Printer: [On], [60] second(s) • Scanner: [On], [60] second(s)
Auto Logout Timer	Specify the time to automatically log out when no operations are in progress for certain period. • Default: [On], [180] second(s) Specifying the Period of Time Until the Machine Logs You Out Automatically
System Status/Job List Display Time	Specify whether to hide the screen displayed by pressing [Check Status] automatically. You can specify the display time. • Default: [On], [15] second(s)

Displayed Application Switchover Timer	Specify when to switch the screen if an event occurs in a different application because there have been no key inputs for a certain period of time on the application screen. • Default: [Set Time], [3] second(s)
Weekly Timer Detailed Settings	Specify whether to activate or inactivate the weekly timer. • Default: [Inactive] When you activate the timer, specify time when the machine switches to and from Off mode or Sleep mode daily or for Monday through Sunday. You can set up to six timer settings a day or for Monday through Sunday and specify the following items: • Weekly Timer Code Settings Specify whether to enable the weekly timer code. When you enable the code, specify a password (up to eight digits) for when the machine recovers from Off mode or Sleep mode. • Weekly Timer Schedule Specify event, such as Enter Sleep Mode, Cancel Weekly Timer Code, or Main Power Off or On, and the day or day of the week to perform it.  Region A (mainly Europe and Asia)/ Region B (Taiwan) Enter the time using the 24-hour format.  Region B (mainly North America) Enter the time using the 12-hour format. • Main Power On Timer Suspension Period Specify the period to disable the timer to turn the main power On (the year change period). To use the machine after this period, turn the main power switch On manually. To use this setting, activate Administrator Authentication. Activating Administrator Authentication

Weekly Timer Easy Settings

When you specify the schedule of the weekly timer only, you can use the timer only by specifying this setting. If a day of the week and time is set here, [Weekly Timer Schedule] under [Weekly Timer Detailed Settings] is activated and the setting overwrites the schedule of the selected day.

 **Region A** (mainly Europe and Asia)/ **Region B** (Taiwan)

Enter the time using the 24-hour format.

 **Region B** (mainly North America)

Enter the time using the 12-hour format.

To use this setting, activate Administrator Authentication.

Activating Administrator Authentication

Section Top

Logging in to Web Image Monitor

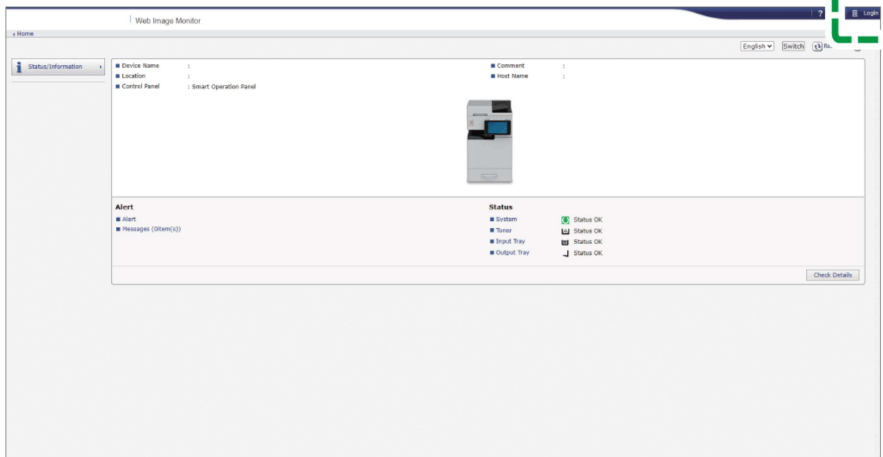
Access the management screen of the machine from the Web browser of the computer using the same authentication information as that used when logging in from the control panel.

You can change the login password in Web Image Monitor. Using the tool, not only can you monitor the machine status, but also manage the files stored in the machine.

Operating or Configuring the Machine from Computer (Web Image Monitor)

Logging in to the Web Image Monitor from the Computer

1. **Launch the Web browser.**
2. **Enter "http://(IP address of the machine or host name)/" on the address bar of the Web browser, and then press the Enter key.**
3. **Click [Login].**



4. **Enter the login user name and password, and then click [Login].**

When [User Code Authentication] is specified on the machine for user authentication, enter the user code in [Login User Name], and then click [Login].

Note

- Ask the administrator for the Login user name and Login password.

- When a time during which users can operate the machine is specified in [Time Settings Allowing Operating Machine by Logging in], you cannot login to the machine outside of that specified time.

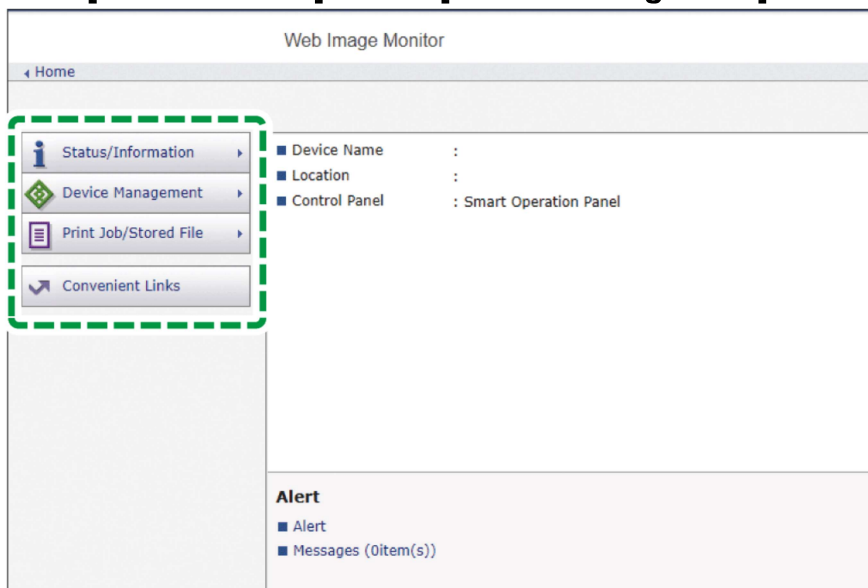
Section Top

Changing the Login Password by Using Web Image Monitor

★ Important

- Only the administrator can change the user code. To change the user code, log in to Web Image Monitor as an administrator.

1. **Launch the Web browser.**
2. **Enter "http://(IP address of the machine or host name)/" on the address bar of the Web browser, and then press the Enter key.**
3. **Click [Login].**
4. **Enter the login user name and password, and then click [Login].**
5. **Click [Address Book] on the [Device Management] menu.**



6. **Select the user for whom to change the login password.**
7. **Click [Change].**
8. **Click [Change] in "Login Password" of "Authentication Information".**
9. **Enter the new password in [New Password], and then re-enter the password in [Confirm Password].**
10. **Click [OK] three times.**

Methods for Sending a Fax

You can scan an original and send it to a fax device at the destination via the telephone line or Internet. The machine is capable of sending a fax using the following methods:

Communication methods

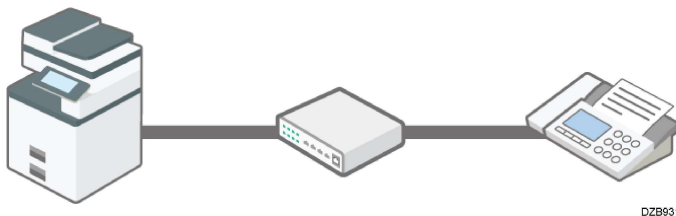
- G3 fax

The specifications for standard fax machines that use an analog telephone line. To send a fax, enter the fax number (telephone number) of the destination device such as an MFP or telephone with the fax function.



- IP-Fax

Specify the IP address or host name of the supporting device to send a fax over an IP network (intranet).



- Internet Fax

A fax is sent via the Internet relayed by an e-mail server. Specify an e-mail address to send the fax to a supporting device or computer.



↓ Note

- You can send a document to the machine directly and send it by fax without printing it.
Sending Faxes from a Computer
- By using an MFP with the fax function, you can send a fax from an MFP that does not have a fax function.

Overview of the Remote Fax Function

Scanning and sending a document

The machine scans the document to send on the exposure glass or in the auto document feeder (ADF). The machine stores the scanned data in the memory and then sends it (Memory Transmission). When using Memory Transmission, you can use various useful functions such as redialing and broadcast transmission.

Note

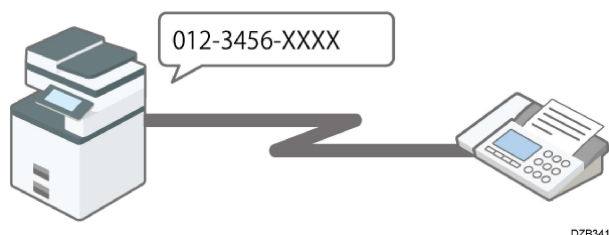
- Immediate Transmission is useful when you want to send a fax while confirming that it is received at the destination properly. You can use this feature when using G3 fax or IP-Fax.

Sending a Fax While Scanning the Original

- Use the machine's fax functions to reduce the communication time and cost and enhance security as needed.
- For details about the advantages of the transmission methods and Memory Transmission, see the following:

G3 fax

A fax is sent over a public telephone line to the destination. Specify the fax number (telephone number) of the destination. You can use this function to send and receive faxes between the machine and a device that does not support IP-Fax or Internet Fax.



Basic Procedure for Transmitting Faxes

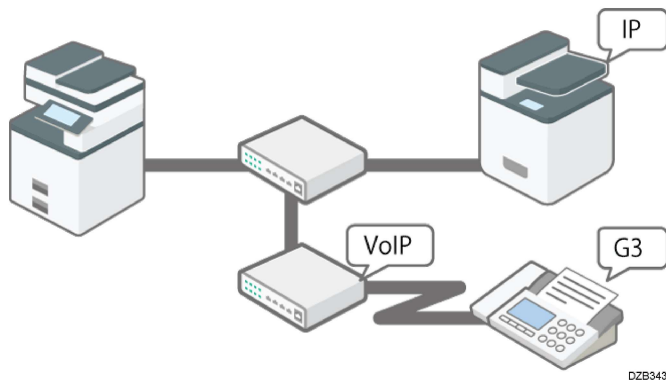
- Connect an external telephone to talk to a person at the destination.
- Call charges are incurred depending on the telephone service contract and the distance to the destination.

Note

[Section Top](#)

IP-Fax

Documents are sent and received between devices that support IP-Fax. Connect the devices via an IP network (a network that uses TCP/IP as the communication protocol) to send documents. Specify the destination by entering the IP address, host name or Own Fax No. according to the connection environment. You can use this function to send and receive faxes between the machine and an other manufacturer's device that supports IP-Fax.



Sending Documents by IP-Fax

- You can reduce communication costs because no call charges are incurred.
- You can communicate faster over an IP network compared to an analog phone line. Also, it does not require an e-mail server to relay the message, so you can send and receive documents without any delay.
- This function is suitable for communicating between devices in the same local area network such as your company intranet.
- You can send a fax to a G3 fax by relaying the communication from the machine through a VoIP gateway to a public telephone line.

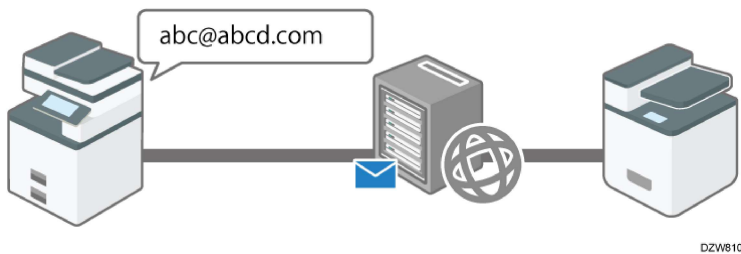
Note

- IP-Fax supported by this machine is ITU-T Recommendation T.38 compliant.
- To send to a G3 fax via a gateway connected to a public telephone line, you must specify it's the receiver's machine telephone number. For example, if the receiver's fax number is "0312345678", specify "5678". To send from an IP-Fax to G3 fax without using gatekeeper or SIP server, you must register the gateway also.
- An alias telephone number is a number that is registered in the gatekeeper, and is available only in the network to which the gatekeeper is connected.
- Pay attention to the number of telephone number digits set in the gateway/IP address conversion table to avoid transmission error.
- Although the machine can have multiple IP addresses in an IPv6 environment, only one address can receive IP-Faxes.

[Section Top](#)

Internet Fax

Documents are sent and received via an Internet connection between devices that support Internet Fax. When sending a fax, specify the destination by entering its e-mail address. The document is sent as an attachment in an e-mail. You can use this function to send and receive faxes between the machine and an other manufacturer's device that supports Internet Fax.

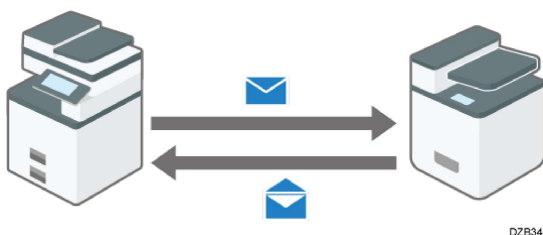


Preparing the Machine for Sending and Receiving Documents by Internet Fax

- Using this function, you can also send a fax to a computer.
- No call charges are incurred, and you can reduce communication costs especially when sending a fax to a destination in a remote location.
- You can apply encryption and attach a digital signature to send the e-mail more safely and securely.

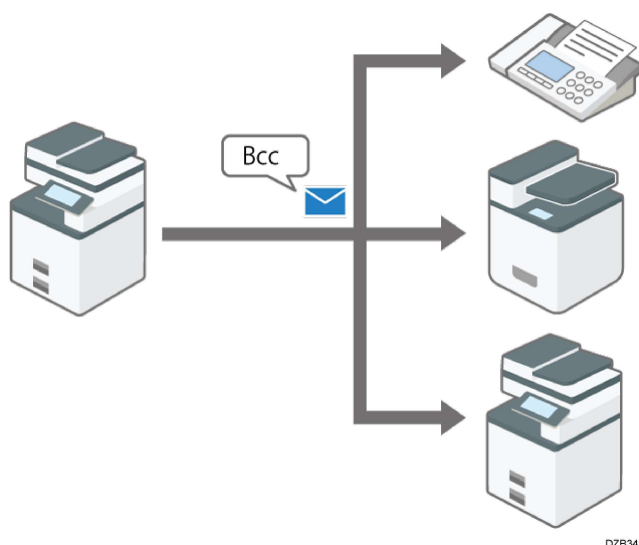
Applying Encryption and Using a Signature for Enhanced Security When Sending an Internet Fax

- The Internet Fax function of the machine allows you to:
 - Receive a reception confirmation from the destination of an Internet Fax. You can also obtain the performance details of the destination device and send a fax to the same destination using the send settings that are optimized for the destination device.



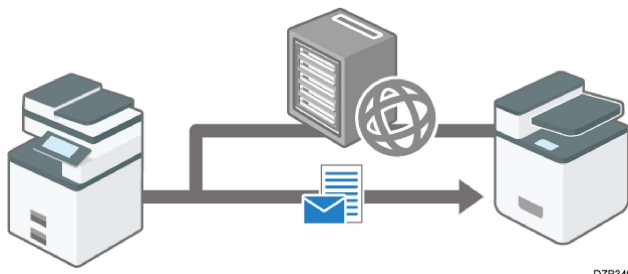
Confirming the Reception of an Internet Fax at the Destination

- You can send a broadcast transmission by Internet Fax to a destination specified in the Bcc field instead of the To field.



Sending a Document by Internet Fax to a Destination Specified in the Bcc Field

- You can specify the destination domain directly when sending an Internet Fax. This shortens the time required to go through the SMTP server and reduces the load on the server as well.



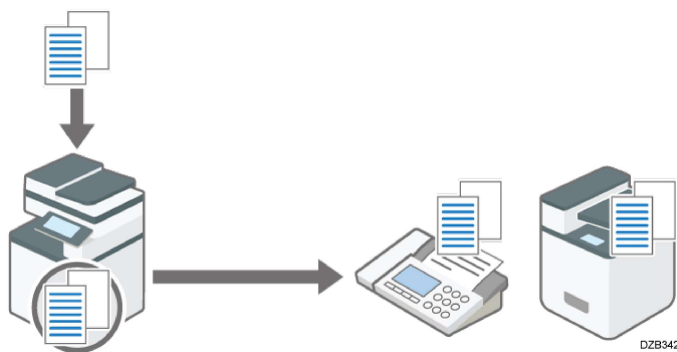
DZB346

Sending Internet Faxes without Using SMTP Server

[Section Top](#)

Advantages of Memory Transmission

The machine stores the scanned original in the memory temporarily and then sends it. This is convenient when sending a large number of originals, because you can start dialing and sending without waiting for all the originals to be scanned (Parallel Memory Transmission).



DZB342

Basic Procedure for Transmitting Faxes

You can use the following useful features when sending a fax:

- The machine automatically tries redialing at five-minute intervals when the line at the destination is busy or a transmission error occurs. You can change the number of times to redial in [Fax Settings] ► [Send Settings] ► [Number of Resends Settings].
Send Settings
- You can scan another original while the machine is sending or receiving a fax or printing a report, so that you can send the next fax immediately.
- You can send the same fax to more than one destination after scanning the original one time (Broadcast transmission).
- You can scan the original and then send it later at a specified time.
Sending a Fax at a Specified Time
- The machine displays a warning message when sending a fax to more than one destination.

Preventing a Fax Transmission to the Wrong Destination

Memory Transmission and Parallel Memory Transmission

In Parallel Memory Transmission, the machine dials the destination fax number while scanning the original and sends a fax.

- A fax is sent by Memory Transmission in the following cases:
 - The destination line was busy and could not be connected
 - The machine was communicating with another destination
 - An original was placed on the exposure glass when sending a fax
 - More than one destination was specified
 - The time for transmission was specified
 - [Preview] was specified
 - A fax may be sent in normal memory transmission if the remaining amount of memory is low. The remaining amount of memory at which the machine switches to normal memory transmission varies according to whether the optional fax memory unit is attached to the machine.
 - Transmission is terminated and the Communication Result Report is printed when you press [Stop], the original is jammed, or the remaining amount of memory becomes low. The stored document is deleted.
 - You can specify not to use Parallel Memory Transmission and to store all documents in the memory before sending.
- List of Parameter Settings

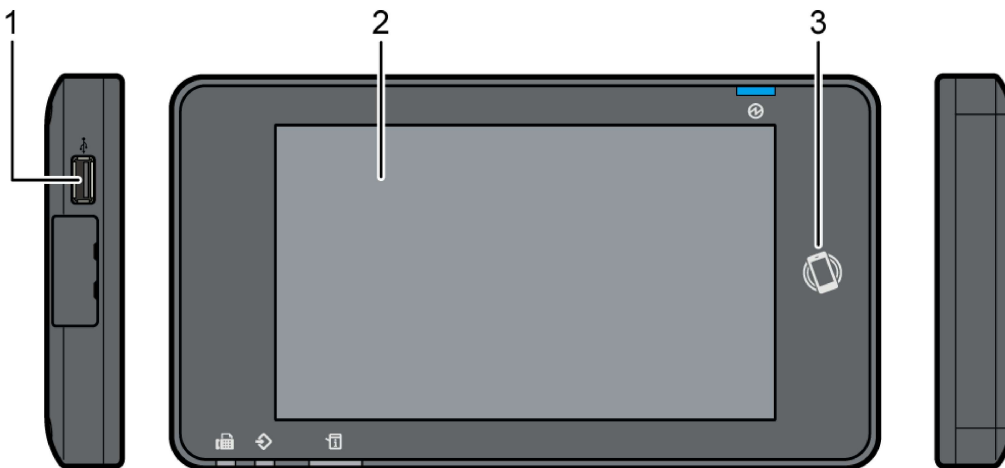
[Section Top](#)

Names and Functions of the Control Panel

The touch panel (Smart Operation Panel) that displays the operation screen of the machine is referred to as the "Control Panel".

- On both sides of the control panel, interfaces for connecting external devices and slots to insert a USB flash memory device are provided.
- Even when the screen is turned off, the LED indicators on the frame of the control panel show the status of the machine.

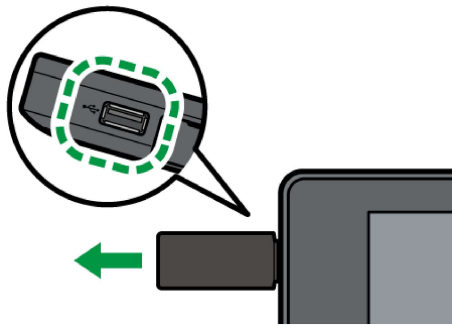
Touch Panel/Interface



1. Media slots

Insert a USB flash memory device. You can store the scanned data or print the file stored on the media.

- Use the media formatted in FAT16 or FAT32.
- Certain types of USB flash memory devices cannot be used in the machine.
- A USB extension cable, hub, or card reader cannot be used.
- If the power of the machine is turned off or the media is removed from the machine while the machine is reading the data in the media, check the data in the media.
- Before removing the media from the slot, press the icon displayed on the screen () to cancel the connection.



- Do not change the write protection switch of the USB flash memory device while the USB flash memory device is inserted.

2. Touch Panel

Displays the Home screen, operation screen of applications, and messages. Operate with the fingertips.

How to Use the Home Screen

Intuitive Screen Operation Using Fingertips

3. Touch mark

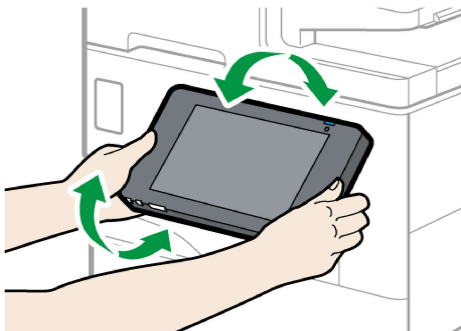
Used to connect the machine and a smart device with the RICOH Smart Device Connector.

Using the Machine Functions from a Mobile Device

Logging In Using a Mobile Device

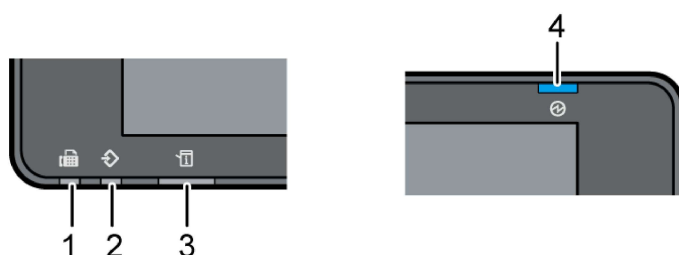
↓ Note

- You can adjust the angle of the control panel to improve visibility. When adjusting the angle of the control panel, be careful not to pinch your fingers.



Section Top

LED Indicators



1. Fax indicator

Indicates the status of the fax function.

- Flashing: transmitting and receiving data
- Lit: receiving data (Substitute RX File/Memory Lock Reception/Personal Box)

2. **Data In indicator**

Flashes when the machine is receiving data sent from the printer driver or LAN-Fax driver.

3. **Status indicator**

Indicates the status of the system. Stays lit when an error occurs or toner runs out.

Checking the Indicators, Icons, and Messages on the Control Panel

4. **Main power indicator**

The main power indicator lights up when you turn on the main power switch. In Sleep mode, it flickers slowly.

[Section Top](#)

Reception Settings

This section describes the settings in [Reception Settings] under [Fax Settings].

How to Use the "Settings"

Reception File Settings

Setting Items	Description
---------------	-------------

Action on Receiving File

Specify the output method of the received document.

- **Store:** Store documents on the machine
When [On] is selected, specify whether to notify that the document is stored and that memory is nearly full in [Store Notification Settings].
 - Default: **[Off]**
- **Forwarding:** Forward the document to a pre-registered destination
When [On] is selected, specify the forwarding destination, security, etc. in [Forwarding].
 - Default: **[Off]**
- **Print:** Print the document automatically
 - Default: **[On]**
- **Memory Lock Reception:** Perform Memory Lock Reception that requires entering the Memory Lock ID to print
 - Default: **[Off]**

Note

- When [On] is specified for Store, more memory space is used as the number of saved documents increases. After memory space becomes insufficient, no more documents are saved on the internal storage. Based on the bit number 7 setting of the switch number 10, the machine prints and deletes the stored documents starting from the one with the oldest stored date; or deletes them without printing and prints the Reception File Erased Report. When memory space becomes insufficient, delete the stored documents.
- When [On] is specified for Store, you can specify the parameter setting (the bit number 0 of the switch number 40) to stop the machine automatically receiving new faxes when available memory space runs too low.

Overview of Output Mode Switch Timer

Configuring the Machine to Store Received Documents

Transferring Received Fax Documents to Another Fax by Forwarding

List of Parameter Settings

Output Mode Switch Timer	Specify the output method of documents received during the specified time period from Print, ID Required Print, Forwarding, or Store. Default: [Do not Use] Configuring Output Mode Switch Timer
Prohibit Auto Print	Store the document as a standby to print document without printing it automatically. Default: [Do not Prohibit] Overview of Output Mode Switch Timer
Print Standby to Print Files	Select this to print a standby to print document designated by [Output Mode Switch Timer] and [Prohibit Auto Print]. Confirming the Output Mode that is Applied Automatically
Action on Receiving File when a Memory Is Full	Specify whether to delete the oldest received document or cancel receiving new documents when the internal storage of the machine is full. When you select [Delete Old File and Receive New File], also specify whether to print the old document or print a report without printing the document. - Default - Receiving When Memory Is Full: [Delete Old File and Receive New File] - When Deleting Old File: [Print Old File] Configuring the Machine Behavior When a Document Cannot Be Stored
Reception File Storage Location	This setting is available when [Store] is enabled in [Action on Receiving File]. Received documents are stored on the internal storage and in the fax memory of the machine as well. When [Reception File Storage Location] is set to [Internal Storage], the machine stores received documents on its internal storage even after the fax memory becomes full, thus enabling you to store more documents. Default: [Fax Memory]
Create / Change / Delete Reception File Store Folder	Register, modify or delete a folder to store received documents.

Store Reception File Per Line Setting	Specify a folder to store received documents according to a line type. Default: [Same as Action on Receiving File]
Download Stored Reception File (Permissions: File Administrator)	Press [Start Download] to download the stored reception files to the USB memory in PDF format. When downloading, you can specify a reception date(s) by specifying [Specify Period] for "Specify Download File".
Print/Store When All Memory Transmissions Complete	Specify whether to print or store the received document when memory forwarding is complete. - Default: [Same as Action on Receiving File]  Note - Select [Off] for this setting item if not printing or storing a document that has been transferred normally even when [On] is specified for Print or Store in [Reception File Settings] ► [Action on Receiving File].

Section Top

Reception Mode Settings

Setting Items	Description
Switch Reception Mode	Select whether to receive an incoming fax automatically or manually depending on the fax usage. Default: [Auto Reception]

Section Top

Register Special Sender

Setting Items	Description
Register/Change/Delete	Register senders to specify the reception setting. You can specify a different setting for each sender.
Register Special Sender: Print List	Select this to print the list of special senders.

Authorized Reception	Select this to limit the sender of the incoming fax to receive. Default: [Off]
Special Reception Function	Specify whether to use the Special Sender function. Default: [Off]
Print/Store when [Forwarding per Sender] is On	Specify whether to print or store the document received from a Special Sender and forwarded to the specified destination. Default: [Off]
Receive Fax (Caller ID Blocked)	Specify whether to receive faxes without caller ID. Default: [Accept]
Bypass Tray Paper Size	Specify the paper size when the bypass tray is specified to output the documents received from a special sender. Default: [Regular Size]

Specifying the Action to Perform When Receiving a Fax from Different Senders

Preventing Unwanted Faxes

[Section Top](#)

Box Setting

Setting Items	Description
Register/Change/Delete Box	Register, modify or delete Personal Box, Information Box and Transfer Box that use a SUB / SEP Code.
Box Setting: Print List	Select this to print the list of opened Personal Box, Information Box, and Transfer Box.

Receiving Faxes to Personal Boxes

Transferring Received Fax Documents to Another Fax Destination

[Section Top](#)

Stored Reception File User Setting

Setting Items	Description
---------------	-------------

Stored Reception File User Setting

Specify the user to manage the received documents stored on the internal storage (administrative user). When an administrative user is specified, you are asked to enter the user code or login information of the administrative user when viewing, printing, and deleting documents from Web Image Monitor. You can also restrict viewing, printing, and deleting of the stored reception files on the control panel.

- Default: **[Off]**

Note

- If the registered user code is deleted from the Address Book, you cannot view the received and saved documents using Web Image Monitor or the machine's control panel.

Section Top

SMTP Reception File Delivery Settings

Setting Items	Description
SMTP Reception File Delivery Settings	Select whether to deliver e-mails received by SMTP. • Default: [Off] Enabling the Delivery Setting

Section Top

Reception File Print Settings

Setting Items	Description
---------------	-------------

2 Sided Print Combine Two Originals	Configure the following functions: • Print the received document on both sides of paper or two pages on a sheet • Default • 2 Sided Print: [Off] • Combine Two Originals: [Off] Printing on Both Sides of Paper When Receiving a Document Comprising Multiple Pages Combining and Printing Pages on One Side of Paper When Receiving a Document Comprising Multiple Pages
Print Reception Time	Select whether to print the reception date and time in the bottom margin of the output sheet. • Default: [Off]
Reception File Print Quantity	Specify the number of copies of the received document to print. • Default: [1] set(s) Printing More than One Copy for a Received Document
Paper Tray	Specify the tray to feed paper on which received fax documents are printed. A paper tray is not specified when [Auto Select] is selected. • Default: [Auto Select]
Just Size Printing	Specify whether to print received documents only when paper of the same size and orientation as the document is available in any tray. • Default: [Off] Printing Only When Paper of the Same Size as the Received Document Is Available
Print with Margin	Specify whether to compress the received documents for printing. • Default: [Off] Printing the Received Document Slightly Smaller

Section Top

Setting Items	Description
Folder Transfer Result Report	Select whether to notify the specified destination of the result of transferring a document by e-mail when the destination of forwarding or Forwarding per Sender includes a folder. You can apply the security setting (encryption and signature) to the e-mail. • Default: [Do not Email]
Email address/Folder Path on Communication Log	Specify whether to display the e-mail address or folder path instead of the destination's name in the destination field of the transmission history when sending or forwarding a document to a destination registered in the address book. • Default: [Do not Display]
File Name Setting in Folder Transfer	Specify the settings related to the file name of the document transferred to folders, such as adding destination information and limiting characters that can be used. When limited, you can only use alphanumeric characters, "-", and "_" in the file name; however, the last two are not allowed to be used at the beginning of the file name. • Default • Add Sender Information to File Name: [No] • Limit File Name Character Type: [No]

Section Top

Remote Reception Setting per Line

This setting item is displayed when a fax connection unit is installed on the machine.

Setting Items	Description
G3	Select whether to print documents received on the main machine from a sub-machine when using the Remote Fax function.

Section Top

Maximum Reception Size

Setting Items	Description
Maximum Reception Size	Specify the maximum reception size. When a document of a size other than the specified one is sent, the machine receives it in the specified size by enlarging or reducing it automatically. • Default: [A4]

[Section Top](#)

Trays for Paper Tray Selection

Setting Items	Description
Trays for Paper Tray Selection	Specify whether to use the paper tray with the Fax function for each tray. • Default • Tray 1 - 4: [On]

[Section Top](#)

[Send Settings](#) | [Detailed Initial Settings](#)

[Page Top](#)

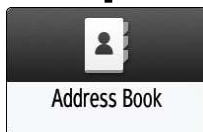
Registering a User in the Address Book and Specifying the Login Information

When "Basic Authentication" is specified on the machine as the User Authentication, specify the login user name and password for each user who uses the machine.

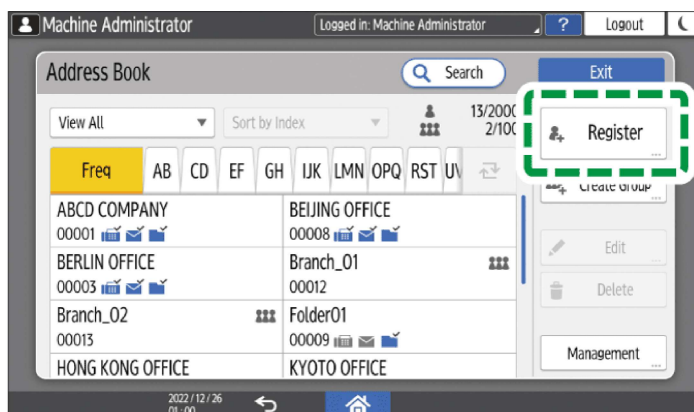
Note

- If you specify the authentication method that uses the LDAP Server (LDAP Authentication), you have to specify the user name and password only when the authentication screen to access the LDAP Server is displayed.

1. Press **[Address Book]** on the Home screen.



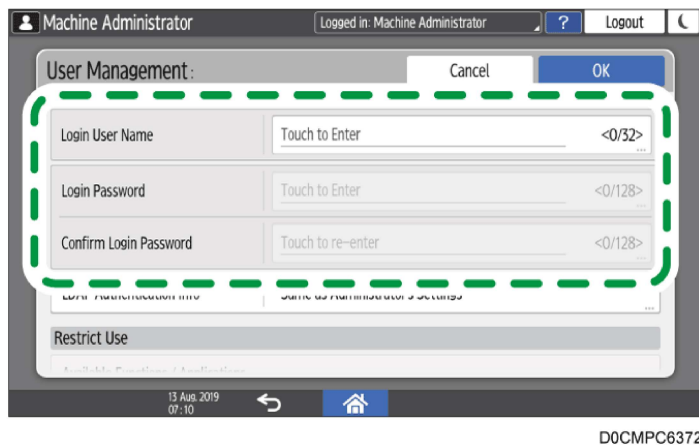
2. On the Address Book screen, press **[Register]** and enter the user name.



3. Press the **[User Management / Other]** tab ► **[User Management]**.
4. Enter the login information.

For Basic Authentication

1. Enter the Login User Name.

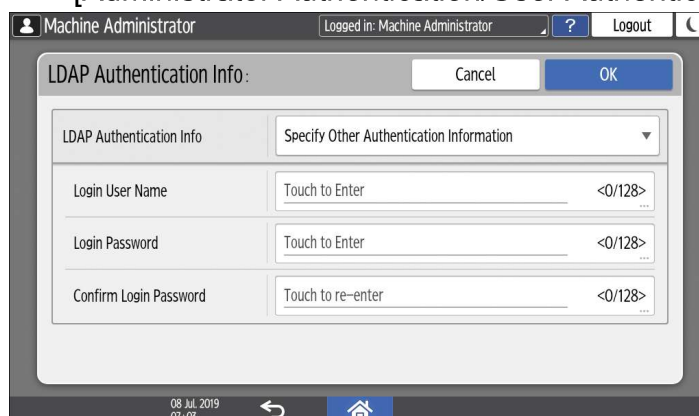


2. Enter the password in [Login Password], and then re-enter the password in [Confirm Login Password] for confirmation.
3. Press [OK].

For LDAP Authentication

1. Press [LDAP Authentication Info].
2. Select [Specify Other Authentication Information] in "LDAP Authentication Info", and then enter the Login User Name and Login Password to access the LDAP Server. Re-enter the password in [Confirm Login Password].
Ask the administrator of the LDAP server for the Login user name and Login password.
When you select an item other than [Specify Other Authentication Information] in "LDAP Authentication Info", the login user name and login password specified in [Register/Change/Delete LDAP Server] are enabled.

- [System Settings] ► [Settings for Administrator] ► [Authentication/Charge] ► [Administrator Authentication/User Authentication/App Auth.]



3. Press [OK].

5. Press [OK].

6. After completing the procedure, press [Home] (🏠).

7. When a message prompting you to back up the address book appears on the screen, press [Go to Backup] to back up the address book.

- If a message prompting you to contact the administrator to back up the address book appears on the screen, ask the administrator to back up the address book.
- If you select [Close], you can close the address book without backing up and go back to the Home screen.

Making a Backup or Restoring the Address Book

[Logging In from the Control Panel](#) | [Registering the User Code in the Address Book](#)

[Page Top](#)

Registering/Changing/Deleting Fax Numbers in the Address Book

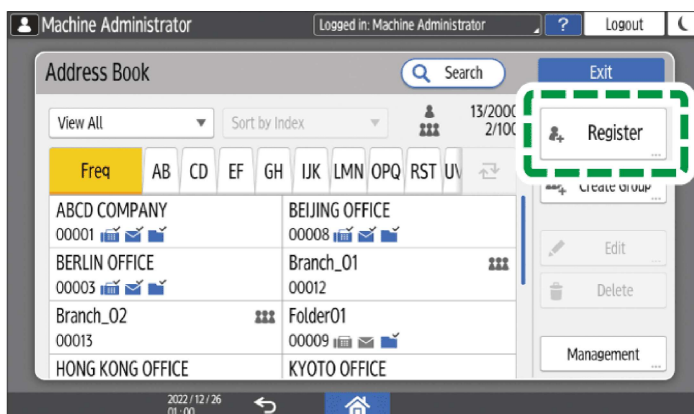
By registering the destinations to which you frequently send faxes together with the send conditions in the address book, you can easily send faxes.

Registering a Fax Number and Send Conditions

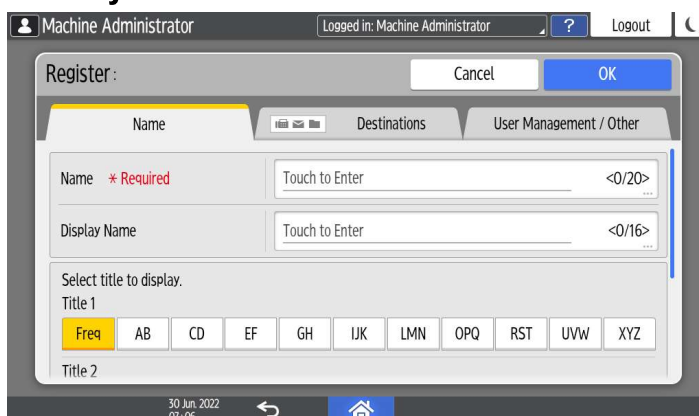
1. Press **[Address Book]** on the Home screen.



2. Press **[Register]** on the Address Book screen.

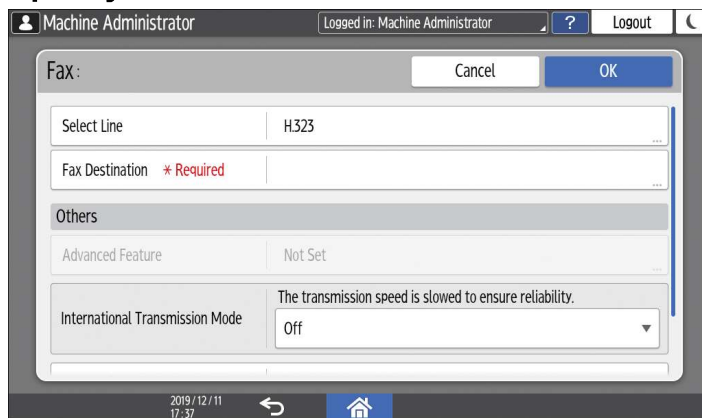


3. Enter the information of the destination on the **[Name]** tab, and then select a title to classify it.



4. Press **[Destinations]** tab ► **[Fax]**.

5. Specify the Fax Destinations and send conditions.



The screenshot shows a 'Fax' configuration window. At the top, it says 'Machine Administrator' and 'Logged in: Machine Administrator'. There are 'Cancel' and 'OK' buttons. The 'Select Line' dropdown is set to 'H323'. The 'Fax Destination' field is marked as '* Required'. Under the 'Others' section, 'Advanced Feature' is 'Not Set'. 'International Transmission Mode' is set to 'Off'. A note states 'The transmission speed is slowed to ensure reliability.' The bottom status bar shows the date '2019/12/11' and time '17:37'.

- Select Line: Select the line to use.
- Fax Destination: Register the fax destination.
- International Transmission Mode: Specify whether to reduce errors occurring when sending abroad.
- Fax Header: Select the name of the sender printed on the reception sheet of the destination. Register the fax header in advance.

Printing the Destination Name, Fax Header, and Standard Message on the Fax Received at the Destination

- Label Insertion: Specify the name (title + name) and fixed phrase printed on the reception sheet of the destination.

Printing the Destination Name, Fax Header, and Standard Message on the Fax Received at the Destination

- Advanced Feature: Register SUB code or SEP code.

6. Press the **[User Management / Other]** tab as necessary, and specify the settings.

- User Management: Enter the authentication information to login and use the machine.
- Add to Group: Select a group to which this destination belongs as necessary. Register the group in advance.

Registering/Changing/Deleting Groups in the Address Book

- Display Priority: When the destinations are sorted in the order of priority, a destination with higher priority is displayed prior to that with lower priority. The destinations with the same priority are displayed in the order of registration.
- Destination Protection: Select this check box to require entering of the protection code to select the destination.

Using the Protection Function to Prevent the Misuse of Addresses

7. Press **[OK]**.

8. After completing the procedure, press **[Home]** (.

9. When a message prompting you to back up the address book appears on the screen, press [Go to Backup] to back up the address book.

- If a message prompting you to contact the administrator to back up the address book appears on the screen, ask the administrator to back up the address book.
- If you select [Close], you can close the address book without backing up and go back to the Home screen.

Making a Backup or Restoring the Address Book

Section Top

Changing/Deleting the Registered Data Such as Fax Number

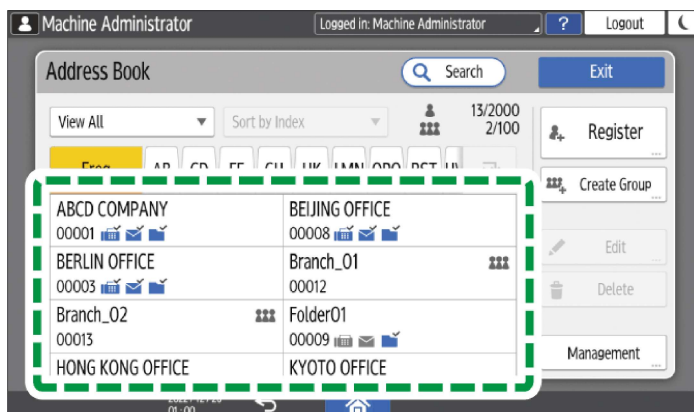
If you delete the destination used for the personal box, file transmission will fail. Exclude the destination from the personal box before deleting it.

Receiving Faxes to Personal Boxes

1. Press [Address Book] on the Home screen.



2. Select the destination to change or delete on the Address Book screen.



You can delete multiple destinations at one time.

3. Press [Edit] or [Delete] to change or delete the destination information.

4. When changing or deleting is complete, press [Home] ().

5. When a message prompting you to back up the address book appears on the screen, press [Go to Backup] to back up the address book.

- If a message prompting you to contact the administrator to back up the address book appears on the screen, ask the administrator to back up the address book.
- If you select [Close], you can close the address book without backing up and go back to the Home screen.

[Section Top](#)

[How to Use the Address Book](#) | [Registering Destinations in the Address Book from the Fax Screen](#)

[Page Top](#)

Settings for Administrator

This section describes the settings in [Settings for Administrator] under [System Settings].

How to Use the "Settings"

Security Pattern/Stamp

Setting Items	Description
Detect Data Security for Copying	Specify whether to gray out the contents of a document with the embedded text for Data Security for Copying when the document is scanned by the Copier or Scanner function or stored on the Document Server. • Default: [Off]
Unauthorized Copy Prevention Printing: Copier Unauthorized Copy Prevention Printing: Document Server Unauthorized Copy Prevention Printing: Printer	Specify whether to use the Data Security for Copying or Unauthorized Copy Prevention for Pattern for each function when printing on the machine. Specifying the Unauthorized Copy Prevention Function
Compulsory Security Stamp: Copier Compulsory Security Stamp: Document Server Compulsory Security Stamp: Fax Compulsory Security Stamp: Printer	Specify whether to print the user and device information for each function when a file is output using the Copier, Document Server, Fax, or Printer function. • Default: [Off] Specifying the Compulsory Security Stamp Function

[Section Top](#)

Data Management

Setting Items	Description
Auto Erase Memory Setting (This setting item is displayed only when the machine is equipped with the HDD option.)	Specify whether to erase files printed on the printer driver or image of the scanned original for each job automatically. • Default: [Off] Enabling the Auto Erase Memory Setting Function
Erase All Memory	Delete all data stored in the machine. Initializing the Machine with the Erase All Memory Function
Delete All Logs	Delete all logs stored in the machine. Deleting All Logs
Transfer Log Setting	This is a setting item to disable the log transfer settings that can be enabled on the Collect Logs server. To disable the log transfer settings, specify [Do not Forward]. Disabling Log Transfer to the Log Collection Server
Collect Logs Settings	Specify whether to activate the collection of Job Log, Access Log, and Eco-friendly Logs. • Default • Job Log: [Inactive] • Access Log: [Inactive] • Eco-friendly Logs: [Inactive] Specifying Logs to Collect
Device Setting Information: Export (Memory Storage Device) Device Setting Information: Import (Memory Storage Device) Device Setting Information: Import Setting (Server) Device Setting Information: Run Import (Server)	You can export the machine's device information to an external device as a device setting information file, or import the exported device setting information file to the machine to restore the previous settings. Importing or Exporting the Device Setting Information
Backing Up User Data Restoring User Data (These setting items are not displayed when the machine is equipped with the HDD option or with the SSD option.)	You can save the user data stored on the internal storage (eMMC) of the machine to a USB flash memory device or restore the data to the machine. Making a Backup Copy of or Restoring User Data

Restore Default Control Panel Settings

You can initialize the settings of the control panel, such as the settings, Home screen settings, and browser settings on the control panel.

Section Top

File Management

Setting Items	Description
Machine Data Encryption Settings	Specify whether to encrypt the Address Book, authentication information, and Stored Files stored in the machine. Encrypting Data on the Internal Storage
Auto Delete File in Document Server (This setting item is displayed only when the machine is equipped with the HDD option or with the SSD option.)	Specify whether to delete the files stored in the Document Server automatically. To delete the stored files automatically, specify a number of days and hours to delete after they are stored. By default, the documents stored on the Document Server are automatically deleted in 3 days. Default: [Specify Days], [3] day(s) Changing the Storage Period of Document Server or Specifying an Indefinite Period
Delete All Files in Document Server (This setting item is displayed only when the machine is equipped with the HDD option or with the SSD option.)	Delete all files stored in the Document Server. Files stored with passwords are also deleted.
Document Server Function	Specify whether to use the Document Server function. When you specify [Off], you cannot store files sent from the printer driver. Default: [On]
Default Privilege for Stored File	Specify the default access privilege for the stored files granted to the users who are automatically registered in the address book when logging in to the machine with active Windows or LDAP authentication. Default: [Read-only] Specifying the Default Privilege for Stored Files

PDF File Type: PDF/A Fixed

Specify the PDF file format to PDF/A only that can be stored for a long time.

- Default: **[Off]**

Section Top

Security

Setting Items	Description
Extended Security Settings	Specify to encrypt transmitted data of the machine and data in the Address Book. For details, see "Specifying the Extended Security Functions" in this section.
Access Control Function	Specify whether to enable the function to allow only the communication within the specified range of the IP addresses (access control). You can allow only access from/to the specified IP addresses by selecting [Active (Firewall)]. • Default: [Inactive] Limiting Machine Access
Register/Delete Device Certificate	Register or delete a device certificate. Installing a Self-signed Certificate/Certificate Issued by a Certificate Authority
Service Mode Lock	Specify whether to lock the machine changing to Service Mode when a customer engineer performs maintenance and repair. • Default: [Off] Restricting Operations of the Customer Engineer without the Supervision of the Machine Administrator
CCC: Save Standard Values CCC: Apply Standard Values (This setting item is displayed only when the machine is equipped with the HDD option or with the SSD option.)	Store or reflect the Device Settings (reference value) for the International Evaluation Regulations for Information Security (CC Authentication) in the internal storage of the machine. When you change the settings for maintenance of the machine, backup and restore the settings before and after maintenance, and the device settings to satisfy the CC Authentication standards can be kept.

Credential Storage	• System (certificate system installed) Displays the contents of certificates installed in the system. Specify whether to use these certificates. • User (certificate installed from memory storage device) Install certificates from a USB flash memory device. You can install up to 10 certificates. • Delete All Certificates Deletes all contents of the installed certificates.
Server Settings	Specify whether to enable the server function for operating the Web application. You can install a server certificate for SSL communication. • Default • Server Function: [Active] • Setting Server Certificate: [The setting has not been made.]
Install Settings	Specify whether to allow installation of the application with the SHA-1 signature. • Default: [ON]

Specifying the Extended Security Functions

This section describes settings displayed in [Extended Security Settings]. You can encrypt transmitted data and data in the Address Book. An administrator who can changes the settings depends on the setting item.

Setting Items	Description
Driver Encryption Key (Permissions: Network Administrator)	Specify a text string to decrypt login passwords or file passwords sent from each driver when user authentication is specified to ON. Register the encryption key specified using the machine in the driver.
Driver Encryption Key: Encryption Strength (Permissions: Network Administrator)	Specify encryption strength for sending jobs from the driver to the machine. The machine confirms the encryption strength of the password appended to a job and processes it. • Simple Encryption All jobs that are verified by user authentication are accepted. • DES Jobs encrypted with DES or AES are accepted. • AES Jobs encrypted with AES are accepted. When you select [AES] or [DES], specify the encryption settings using the printer driver. For details about the settings of the printer driver, see the printer driver Help. • Default: [Simple Encryption]
Restrict Display of User Information (Permissions: Machine Administrator)	Specify when user authentication is enabled. Specify whether to display all personal information hidden to confirm the job history using a network connection for which authentication is not provided. For example, the job history of Web Image Monitor is displayed as "*****". • Default: [Off]

Enhance File Protection (Permissions: File Administrator)	Specify whether to lock the files to be inaccessible if an invalid password is entered ten times. This can protect files from unauthorized access attempts to release the password using random passwords. If the Enhance File Protection function is specified, the icon () appears at the bottom left of the screen. When files are locked, it is not possible to select them even if the correct password is entered. Unlocking by the file administrator is required. • Default: [Off]
Restrict Use of Destinations (Fax) Restrict Use of Destinations (Scanner) (Permissions: User Administrator)	Specify whether to limit the available fax and scanner destinations to the destinations registered in the Address Book and searched with the LDAP Search function. When you specify the setting to receive e-mails via SMTP using the Fax function, you cannot use this function. • Default: [Off]
Restrict Adding of User Destinations (Fax) Restrict Adding of User Destinations (Scanner) (Permissions: User Administrator)	These are the settings when you do not use "Restrict Use of Destinations". Specify whether to restrict adding of user destinations entered directly in the Address Book. You can send e-mail to the destination entered directly. • Default: [Off]
Transfer to Fax Receiver (Permissions: Machine Administrator)	Specify whether to prohibit the use of forwarding or transferring function of the Fax function. • Default: [Do not Prohibit] Transferring Received Fax Documents to Another Fax Destination

Authenticate Current Job (Permissions: Machine Administrator)	This is a setting item to specify when Basic authentication, Windows authentication, or LDAP authentication is activated. Specify whether authentication is required for operations such as interrupting jobs under the Copier function or canceling jobs under the Printer function. When you specify [Login Privilege], authorized users who have the privilege to use the current function can operate the job. When you specify [Access Privilege], users who execute the job and the machine administrator can operate the job. • Default: [Off]
@Remote Service (Permissions: Machine Administrator)	Specify how to use the @Remote Service. If it is specified to [Prohibit Some Services], it becomes impossible to change settings via a remote connection from the center, providing optimally secure operation. • Default: [Do not Prohibit]
Update Firmware (Permissions: Machine Administrator)	Specify whether to prohibit firmware updates on the machine by a service representative or via the network. • Default: [Do not Prohibit]
Change Firmware Structure (Permissions: Machine Administrator)	Specify whether to prevent changes in the machine's firmware structure without confirmation by a machine administrator. When you specify [Prohibit] and the machine detects the structure change, the machine starts after authenticated by a machine administrator. As the new firmware version is displayed on the screen, the administrator can confirm whether the updated structure change is permissible or not. • Default: [Do not Prohibit]

Password Policy (Permissions: User Administrator)	Specify whether to limit the text and the number of characters for the user password when using Basic Authentication. Specify a password using a combination of 2 or more types of characters for [Level 1] and 3 or more types of characters for [Level 2] selected from the types described below. - Upper-case letters, lower-case letters, decimal numbers, and symbols such as # You can specify passwords that meet the conditions specified in complexity and minimum character number. - Default - Complexity Setting: [Off] - Minimum Number of Characters: [0] characters
Settings by SNMPv1, v2 (Permissions: Network Administrator)	Specify whether to prohibit setting change on the machine by SNMPv1/v2 protocol. You can change the machine configuration without Administrator Privileges because authentication cannot be performed by SNMPv1/v2 protocol, but if you specify [Prohibit], you can prevent the change that is not intended by the administrator. Default: [Do not Prohibit]
Password Entry Violation (Permissions: Machine Administrator)	Specify the standards that the system recognizes the access as a password attack. If the number of authentication requests exceeds the number specified by the setting, the access is recorded in the Access Log and the log data is sent to the machine administrator by e-mail. You can specify Maximum Allowed Number of Access up to 100 and Measurement Time up to 10 seconds. If the Maximum Allowed Number of Access is set to "0", password attacks are not detected. If you receive violation detection e-mails frequently, check the content and review the setting values. - Default - Maximum Allowed Number of Access: [30] time(s) - Measurement Time: [5] second(s)

Device Access Violation (Permissions: Machine Administrator)	Specify the standards that the system recognizes the access as an access violation. If the number of login requests exceeds the number specified by the setting, 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. You can specify Maximum Allowed Number of Access up to 500 and Measurement Time up to 10 to 30 seconds. If the Maximum Allowed Number of Access is set to "0", access violations are not detected. Also, you can specify response delay time for login requests when an access violation is detected (Authentication Delay Time) or the number of acceptable authentication attempts (Simultaneous Access Host Limit). If you receive violation detection e-mails frequently, check the content and review the setting values. • Default • Maximum Allowed Number of Access: [100] time(s) • Measurement Time: [10] second(s) • Authentication Delay Time: [3] second(s) • Simultaneous Access Host Limit: [200]
Security Setting for Access Violation (Permissions: Machine Administrator)	Specify whether to prevent the incorrect lockout caused by the network environment. When you log 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. In this case, specify the setting to On, and control the lockout by period but not by counts. When you specify [On], you can specify the period to deny the continuous accesses by a user (0 to 60 minutes). You can also specify how many user accounts or passwords can be managed (50 to 200) and the monitoring interval (1 to 10 seconds). • Default: [Off]

Section Top

Remote Panel Operation

Setting Items	Description
Remote Panel Operation	Specify whether to enable remote operation of the machine, the remote connection timeout period, and so on.

Section Top

Function Restriction

Setting Items	Description
Menu Protect	Specify the level of access privilege to allow changing the settings for the functions that can be changed by non-administrative users. Specifying Menu Protect
Restrict Functions of Each Application	You can specify not to use the copier, Document Server, scanner, and printer applications individually. You can also specify the following limitations. • Specifying the scan to Limit to Auto Color Selection • Specifying the destination of the Scanner function to e-mail or folder

Section Top

Authentication/Charge

Administrator Authentication/User Authentication/App Auth.

Setting Items	Description
Administrator Authentication Management Register/Change Administrator	Specify whether an Administrator manages the settings of the machine. Register the user name and password of the administrator to prevent the settings changed by the user other than the administrator. You can manage four categories; user management, machine management, network management, and file management. Activating Administrator Authentication Adding Built-in Administrators or Changing the Privileges
User Authentication Management	Specify the authentication method to authenticate the user. When you specify the authentication, you can limit the functions to use or the access to the Address Book or stored files. • Default: [Off] Verifying Users to Operate the Machine (User Authentication)
Setting for Entering Authentication Password	Specify whether to allow double-byte characters to be used for passwords. • Default: [Only 1 Byte Characters]
Application Authentication Management	This is a setting item to specify when the authentication is activated by [User Authentication Management]. Specify functions to allow users to use without logging in to the machine. Specifying Application Authentication Management
Application Authentication Settings	Specify privileges to use applications for all users or for each user. For example, you can specify to inhibit the use of all applications related to the Copier function or to use only a part of application related to the Copier function. Specifying Application Authentication Management
User's Own Customization	Specify whether to store the layout of Home screen or Application screen and the displayed language for each login user. • Default: [Prohibit]

Register/Change/Delete Realm	Register the realm to be used for Kerberos authentication. Be sure to specify both Realm Name and KDC Server Name when registering a realm. Registering the Realm
Register/Change/Delete LDAP Server	You can register up to five settings for the LDAP Server. Registering the LDAP Server
LDAP Search (This setting item is displayed only when the machine is equipped with the HDD option or with the SSD option.)	Specify whether to use the LDAP server for searching destinations or users. When [Active] is specified for Follow Referrals on LDAP Server, referrals are used for LDAP searches. - Default - LDAP Search: [Off] - Follow Referrals on LDAP Server: [Inactive]
Time Settings Allowing Operating Machine by Logging in	Specify the time period to allow users to log in to and use the machine. Default: [Inactive] Specifying the Time Period to Allow Users to Log In to and Use the Machine

Print Volume Use Limitation

Setting Items	Description
Machine Action When Limit is Reached	Specify whether to continue printing when Print Volume Use reaches the limit. • Default: [Allow Continue Use] Limiting Print Volume
Volume Use Counter: Scheduled/Specified Reset Settings (This setting item is displayed only when the machine is equipped with the HDD option or with the SSD option.)	Specify whether to reset the Volume Use Counter periodically. • Default: [Do not Specify] Resetting Print Volume Use Counter Regularly
Print Volume Use Limitation: Default Limit Value	Specify the limit value of the Print Volume Use. Limiting Print Volume
Print Volume Use Limitation: Unit Count Setting	Specify the function and count to limit the print volume use. Limiting Print Volume
Enhanced Print Volume Use Limitation	This is the setting item to limit the maximum print volume use using the SDK application. To limit the maximum print volume use, specify whether to notify the tracking information from the machine to the SDK application. When [On] is specified for Tracking Permission, also specify whether to stop printing using the SDK application for Stop Printing. • Default: [Off]

External Charge Unit Management

Setting Items	Description
Key Counter Management	Specify whether to limit the user with the key counter for each function.
External Charge Unit Management	Specify whether to limit the user for each function with the key card.

Auto Firmware Update

Setting Items	Description
Auto Firmware Update Settings	Specify whether to update the firmware automatically. • Default: [Active] When [Auto Firmware Update Settings] is set to [Active], you can set the timers to prohibit updates as well.
Last Update Information	Information about the previous auto firmware update is displayed.

Specifying Access Privileges for Documents Saved in Document Server

You can specify access privileges (authority to read or edit a document) for documents saved in the document server so as to prevent unauthorized use. Only the user who has access privileges can perform operations on the document within his/her privileges.

- Register the users to whom you want to grant access privileges in the address book in advance.

Registering a User in the Address Book and Specifying the Login Information

- The user who saved the document, the file administrator, or a custom-privileges administrator who has privileges equal to the file administrator can specify the access privileges. For details about the file administrator and custom-privileges administrator, see the following section:

Registering Standard-Privileges Administrators

Registering Custom-Privileges Administrators

- In advance, specify user authentication in the machine. To protect a document when user authentication is not specified, specify a password on the document when saving.

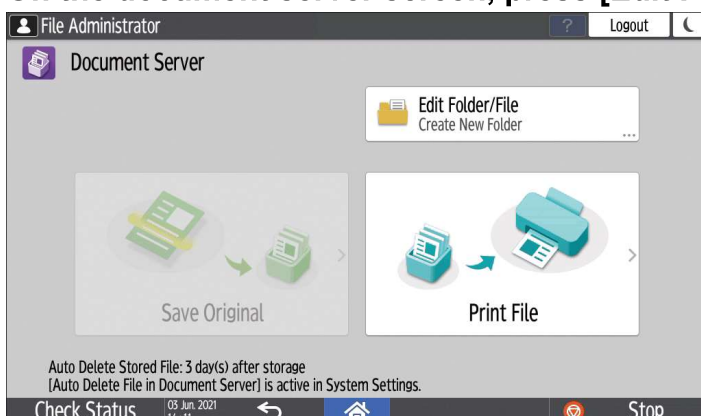
Editing the Information of Documents in Document Server

Verifying Users to Operate the Machine (User Authentication)

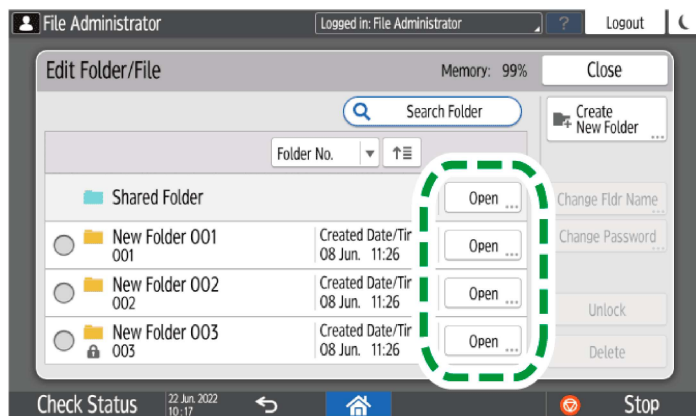
1. On the Home screen, press [Document Server].



2. On the document server screen, press [Edit Folder/File].



3. Press [Open].

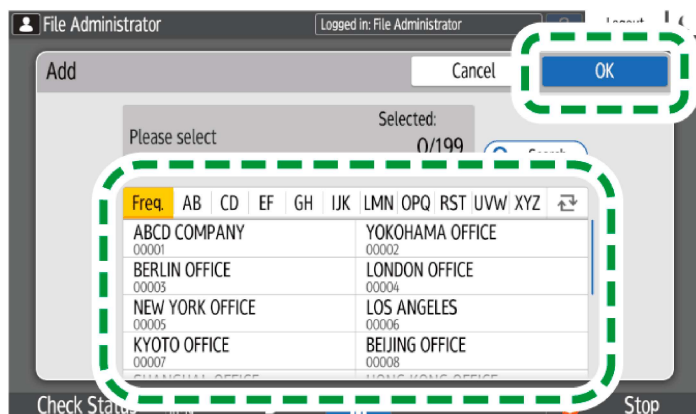


- Press [Search Folder] to search for a folder by folder name or number.
- If you select a password-protected folder, enter the password, and then press [OK].

4. Select the document to specify the access privileges, and then press [Access Privileges].

5. Press [Add].

6. Select the user to grant access privileges, and then press [OK].



7. Select the user to grant access privileges, and then press [Change Privilege].

- To grant access privileges to all users, check [All Users].
- To grant access privileges to individual users, make sure that [All Users] is unchecked, and then check the individual users. You can also check multiple users at the same time.

8. Select a level of access privileges for the user.

The contents of the access privileges are as follows:

- No Privilege: Not able to read or edit the document. You can select this when you check [All Users].
- Read-only: Authorized to read and print the document.
- Edit: The privileges of [Read-only], and authorized to change the printer settings.
- Edit/Delete: The privileges of [Edit], and authorized to delete the document.
- Full Control: The privileges of [Edit/Delete], and authorized to specify the access privileges.

9. Press [OK] ► [Close].

 Note

- To cancel access privileges, select a user and press [Delete] in [Access Privileges Administration] screen after Step 4, and then press [Delete].
- Access privileges to saved print documents sent from the printer driver and saved on the machine can only be specified in Web Image Monitor.
Specifying Access Privileges on Documents Stored in the Machine
- For the access privilege to saved documents, which is automatically granted to users who register in the address book when Windows or LDAP authentication is enabled, see the following section:
Specifying the Default Privilege for Stored Files
Specifying the Default Privilege for Stored Files per User

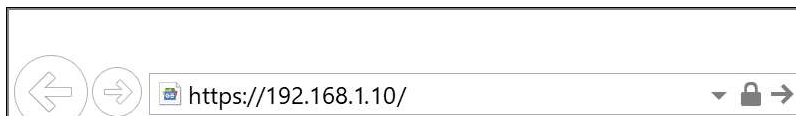
Changing the Storage Period of Document Server or Specifying an Indefinite Period |
Managing Folders as a File Administrator

[Page Top](#)

Accessing to Web Image Monitor

1. Enter the IP address of the machine in the address bar of the Web browser.

You can check the IP address of the machine in by accessing [Network] in Check Status.



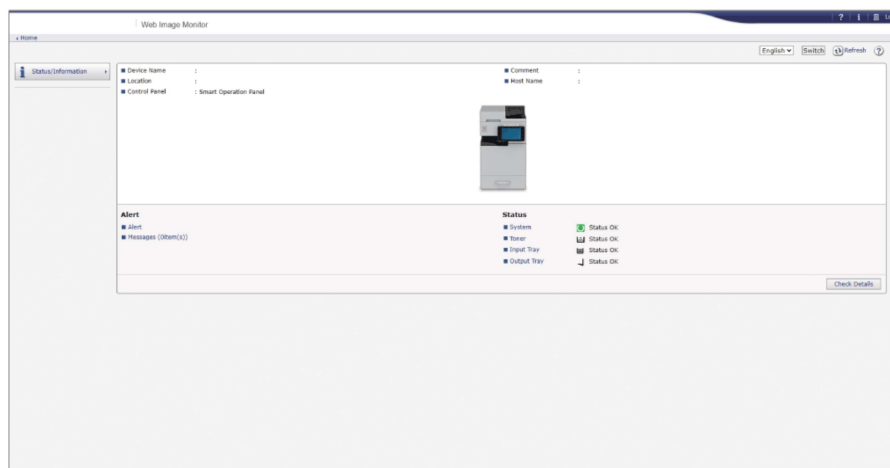
Example: when the IP address of the machine is "192.168.1.10"

- If SSL is specified
https://192.168.1.10/
- If SSL is not specified
http://192.168.1.10/

When you do not know whether SSL is specified on the machine, enter the address starting with https. When you fail the connection, enter the address starting with http.

When entering the IPv4 address, do not enter "0" for each segment. If "192.168.001.010" is entered, you cannot access the machine.

2. Confirming the machine status or settings on the top page of Web Image Monitor.



The machine status and remaining amount of consumables are displayed.

You can access Web Image Monitor more quickly by registering the machine's URL as a bookmark. Note that the URL you register must be the URL of the top page, which is the page that appears before login. If you register the URL of a page that appears after login, Web Image Monitor will not open properly from the bookmark.

To change the settings, click [Login] at the top right on the screen and enter the User Name and Password.

Operating or Configuring the Machine from Computer (Web Image Monitor)

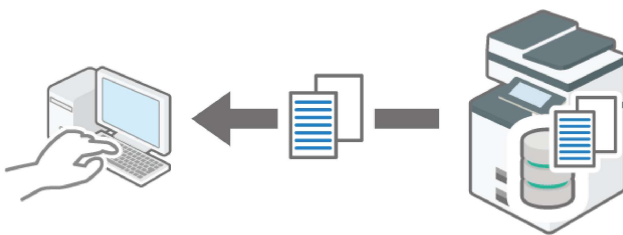
Web Image Monitor is a tool that can check the machine status and configure machine settings from your computer.

If the machine and your computer are ready to connect to the network, you can access Web Image Monitor just by entering the IP address or host name of the machine in the address bar of your web browser.

The settings that can be set by using the control panel can also be set by using the Web Image Monitor, except for some functions.

For example, you can also view documents on the document server by using your computer. As mentioned above, it is recommended that you use Web Image Monitor if you want to operate the machine from your own desk.

Also, downloading of documents on the document server can be performed only by using Web Image Monitor.



Useful functions available by using Web Image Monitor

To check the help of Web Image Monitor, see to the procedure below.

Specifying Web Image Monitor Help

Recommended functions for administrators

Function summary	Procedure and reference
------------------	-------------------------

Registration of the address book You can add login users or destinations to the address book. You can enter characters by using the keyboard of your computer, which is useful for registering a large amount of information. You can also import and export the information in a CSV format.	Registering User Information from Web Image Monitor
Displaying list/history of print jobs, and canceling print jobs You can check the printing status and print history of the machine from your computer. Also, you can cancel stored print jobs in batches from your computer.	• Job list Displayed by going to [Status/Information] in Web Image Monitor ► [Job] ► [Job List] ► [Current/Waiting Jobs]. • Job history Displayed by going to [Status/Information] in Web Image Monitor ► [Job] ► [Job List] ► [Job History]. • Canceling job Displayed by going to [Status/Information] in Web Image Monitor ► [Job] ► [Job List] ► [Current/Waiting Jobs].
Managing output quantity You can check and reset the total counter and counters per user from your computer.	See [Status/Information] in Web Image Monitor help ► [Counter per User] for details.
Settings for sending/receiving email You can configure the settings needed for sending emails and sending to folders from your computer.	See [Device Management] in Web Image Monitor help ► [Configuration] ► [Device Settings] ► [Email] for details.
Settings for receiving faxes You can configure the settings for receiving and rejecting faxes from your computer.	See [Device Management] in Web Image Monitor help ► [Configuration] ► [Fax] ► [Program Special Sender] for details.
Synchronize with time server You can synchronize with a time server when you want to adjust the clock in the machine.	See [Device Management] in Web Image Monitor help ► [Configuration] ► [Device Settings] ► [Date/Time] ► [SNTP Server Name] for details.

Setting the time to enter sleep mode You can configure the time settings for the "Sleep mode" function that automatically turns the display of the control panel off if there is no operation within a specified period of time.	See [Device Management] in Web Image Monitor help ► [Configuration] ► [Device Settings] ► [Timer] ► [Sleep Mode Timer] for details.
Setting auto email notification You can configure the machine to send emails to notify you about the machine's status, such as when paper has run out or a paper jam has occurred. This is useful when managing multiple printers.	Machine Status Notification by E-mail
Monitoring, viewing/operating the control panel screen You can monitor the control panel of the machine from your computer. An administrator can check errors, operate the machine as a user, and change settings, to smoothly perform support operations and manage the machine.	- Monitoring control panel screen See [Device Management] in Web Image Monitor help ► [Screen Monitoring] for details. - Viewing/Operating the control panel See [Device Management] in Web Image Monitor help ► [Remote Panel Operation] for details.
Configuring/changing security/network settings You can configure/change the IP address that can access the machine and configure the settings of the DNS server, and so on.	- Security settings Access Control - Network settings Configuring Network Settings from a Computer Using Web Image Monitor

Recommended functions for user

To use the functions below, users must be registered to the machine and logged in to Web Image Monitor.

Function summary	Procedure and reference
Document operations on the document server You can view, edit, and download documents on the document server.	Accessing Documents in Document Server from a Web Browser

Operation of received and stored faxes You can view or download received and stored faxes. The user must be given the privilege to manage stored documents by the administrator beforehand. See the procedure below. Restricting the Users Who Can Access the Stored Reception Files	Viewing/Operating the Stored Documents from Web Image Monitor
Registration of the address book You can add login users or destinations to the address book. You can enter characters by using the keyboard of your computer, which is useful when you register a large amount of information.	Registering User Information from Web Image Monitor

Recommended Web Browser

Windows	macOS
Firefox 52 or later	Safari 3.0 or later
Google Chrome version 50 or later	Firefox 52 or later
Microsoft Edge 79 or later	Google Chrome version 50 or later

- You can use the screen reader software JAWS 2018.0 or later on Windows 10 and JAWS 2021 or later on Windows 11.

Checking the Machine Status from the Control Panel | What You Can Do on the Web Image Monitor

[Page Top](#)

When a Message Appears and the Machine Cannot Be Operated

Message	Condition	Solution and reference
"Service Call" SCXXX-XX "Contact" "Serial No. of Machine"	The machine needs to be repaired.	Consider repairing the machine.
"Functional Problems" SCXXX-XX "Contact" "Serial No. of Machine"	A malfunction that requires maintenance or repair has occurred.	Prepare for maintenance or consider repairing the machine. If a message prompts you to turn the power of the machine off and then on, the problem may be resolved by turning off the power, waiting for 10 seconds or more after confirming that the main power indicator is turned off, and then turning on the power. Turning On and Off the Power When "Press [Cancel] to cancel functions." is displayed, you can continue using the machine except for the function in which the malfunction is occurring after pressing [Cancel].
"Please wait."	The machine is recovering from the sleep mode.	Wait a while. Turn off the power of the machine if the message persists after five minutes, wait for 10 seconds or more after confirming that the main power indicator is turned off, and then turn on the power. Turning On and Off the Power

"Please wait."	The machine is preparing to perform a function or executing the image stabilization process.	Wait a while and do not turn off the power of the machine.
	The ambient temperature is outside the temperature range specified for the machine operation.	Check the room temperature and whether it satisfies the operational requirements of the machine. If the machine has just been moved to the current location, leave it be for some time and allow it to adapt to the environment before use. Installation Requirements After Moving the Machine If the message persists after five minutes even when the room temperature is within the specifications, wait for 10 seconds or more after confirming that the main power indicator is turned off, and then turn on the power. Turning On and Off the Power
"Please wait."	A consumable or supply such as the toner has been replenished.	Wait a while and do not turn off the power of the machine. Turn off the power of the machine if the message persists after five minutes, wait for 10 seconds or more after confirming that the main power indicator is turned off, and then turn on the power. Turning On and Off the Power
"Shutting down... Please wait. Main power will be turned off automatically. Maximum waiting time: 4 minute(s)"	The power of the machine was turned off while the machine was starting up or in the standby mode.	Wait until the power is turned off.



Tap to see the table

 Note

- If the message persists even after you have performed the operations as instructed in the following message, a malfunction may temporarily occur on the machine. Turn off the power of the machine, wait for 10 seconds or more after confirming that the main power indicator is turned off, and then turn on the power.
 - "Cover Open"
 - "Add Toner"
 - "Waste Toner Bottle is full."
 - "Original(s) left on exposure glass."
 - "No paper."

Turning On and Off the Power

When Messages Appear | When a Message Appears While Using the Copy Function

Page Top

Access Control

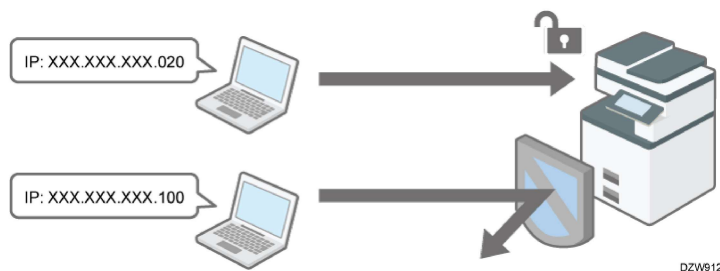
The administrator can limit devices or protocols that can be connected to the machine to avoid unintended access.

Also, the administrator can select a security level at which to enable or disable a protocol and to configure the port status.

Limiting machine access (access control)

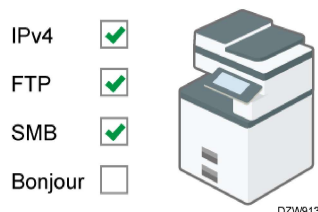
You can limit the IP addresses from which devices can access the machine or limit machine access with a firewall.

For example, when specifying the range of IP address from "192.168.15.1" to "192.168.15.99", the machine cannot be accessed from IP addresses in the range from 192.168.15.100 to 255.



Disabling unused protocols

The protocol setting can be changed on the control panel, in Web Image Monitor, or by using other setting methods. The protocols that can be configured vary depending on the method. Confirm the protocol to configure in Protocol Setting Method List and follow the instruction.



Limiting Machine Access

Limiting the IP addresses from which devices can access the machine

Specify the range of the IP address that can access the machine.

 Important

- You can limit access from the following protocols.
LPR, RCP/RSH, FTP, Bonjour, WSD (Device), WSD (Printer), IPP, DIPRINT, SNMP, telnet, NBT
 - The machine also limits access from Web Image Monitor.
1. **Log in to the machine as the network administrator from Web Image Monitor.**
Logging in to the Machine as an Administrator
 2. **Click [Configuration] on the [Device Management] menu.**
 3. **Click [Access Control] in the "Security" category.**
 4. **In "Access Control Range", click [Active] and specify the range of IP addresses that have access to the machine.**
 - To specify an IPv4 address, enter a range that has access to the machine in [Access Control Range].
 - To specify an IPv6 address, select [Range] or [Mask] in "Access Control Range", and then enter a range that has access to the machine.
 - To allow guest users to print directly via Wi-Fi using smart devices, select [Active] for "Access Control for Direct Connection (Group Owner Mode Only)".
 5. **Click [OK].**
 6. **Log out of the machine, and then exit the Web browser.**

Limiting machine access with a firewall

You can block machine access and then allow access only from/to the IP addresses specified in reception/transmission filters. Specify sets of an IP address, a port number, and a protocol as filters. You can configure up to five filters each for reception and transmission.

1. **Log in to the machine as the network administrator from Web Image Monitor.**
Logging in to the Machine as an Administrator

2. **Click [Configuration] on the [Device Management] menu.**

3. **Click [Access Control] in the "Security" category.**

4. **In Access Control Range, click [Active (Firewall)] and specify reception and transmission filters.**

Specify the following for each reception/transmission filter.

- IPv4/IPv6 reception filter
 - Remote IP Address: Enter source IP addresses from which to allow incoming communications. To allow incoming communications from all IP addresses, select [All].
 - Local Port Number: Enter a port number on the machine through which to allow incoming communications. To allow incoming communications to all ports, select [All].
 - Protocol: Select a protocol in which to allow communications.
- IPv4/IPv6 transmission filter
 - Remote IP Address: Enter destination IP addresses to which to allow outgoing communications. To allow outgoing access to all IP addresses, select [All].
 - Remote Port Number: Enter port numbers to which to allow outgoing communications. To allow outgoing communications to all ports, select [All].
 - Protocol: Select a protocol in which to allow communications.

5. **Click [OK].**

6. **Log out of the machine, and then exit the Web browser.**

 Note

- When filters are not configured properly, access to the machine is not possible. In such a case, specify [Inactive] for [System Settings] ► [Settings for Administrator] ► [Security] ► [Access Control Function] on the control panel.

Protocol Setting Method List

You can view the protocol setting methods in the following list:

- 1: Control Panel 2: Web Image Monitor 3: telnet 4: Device Manager NX 5: Remote Communication Gate S

Protocol/Port	Setting method	Function that cannot be used when Protocol/Port is disabled
IPv4 -	1, 2, 3	All applications that operate over IPv4 (IPv4 cannot be disabled from Web Image Monitor when using IPv4 transmission.)
IPv6 -	1, 2, 3	All applications that operate over IPv6
IPsec -	1, 2, 3	Encrypted transmission using IPsec
FTP TCP:21	2, 3, 4, 5	Transmissions that require FTP (You can restrict only the personal information from being displayed by settings on the control panel.)
telnet TCP:23	2, 4	Transmissions that require telnet
SMTP TCP:25 (variable)	1, 2, 4, 5	E-mail notification function that requires SMTP reception
HTTP TCP:80	2, 3	Transmissions that require HTTP Print using IPP on port 80
HTTPS TCP:443	2, 3	Transmissions that require HTTP (You can make settings to require SSL transmission only and to reject non-SSL transmission using the control panel or Web Image Monitor.)
NBT UDP:137/UDP:138	3	NetBIOS designated functions on the WINS server

SNMPv1-v2 UDP:161	2, 3, 4, 5	Transmissions that require SNMPv1/v2 (Using the control panel, Web Image Monitor, or telnet, you can specify SNMPv1/v2 to prohibit configuration and make it read-only.)
SNMPv3 UDP:161	2, 3, 4, 5	Transmissions that require SNMPv3 (You can make settings to require SNMPv3 encrypted transmission only and to reject non-SNMPv3 encrypted transmission using the control panel, Web Image Monitor, or telnet.)
RSH/RCP TCP:514	2, 3, 4, 5	Transmissions that require RSH Network TWAIN (You can prohibit only personal information from being displayed by the settings on the control panel.)
LPR TCP:515	2, 3, 4, 5	Transmissions that require LPR (You can restrict only personal information from being displayed by the settings on the control panel.)
IPP TCP:631	2, 3, 4, 5	Transmissions that require IPP
IP-Fax TCP:1720 (H.323) UDP:1719 (Gatekeeper) TCP/UDP:5060 (SIP) TCP:5000 (H.245) UPD:5004, 5005 (Voice) TCP/UDP:49152 (T.38)	1, 2, 4, 5	IP-Fax using H.323, SIP, or T.38
Bonjour UDP:5353	2, 3	Transmissions that require Bonjour
@Remote TCP:7443 TCP:7444	1, 2, 3	RICOH @Remote

DIPRINT TCP:9100	2, 3, 4, 5	Transmissions that require DIPRINT
RFU TCP:10021	1, 2, 3	Remote updating of firmware
WSD (Device) TCP:53000 (variable)	1, 2, 3	Transmissions that require WSD (Device)  Note WS-Discovery (TCP:3702, UDP:3702) also works.
WSD (Printer) TCP:53001 (variable)	1, 2, 3	Transmissions that require WSD (Printer)
LLMNR UDP:5355	2, 3	Name resolution requests using LLMNR

Note

- For details about the telnet command, see "Device Monitoring (TELNET)" on our website.
- For details about the settings in Device Manager NX or Remote Communication Gate S, see the user's manual of each tool.

Section Top

Disabling Unused Protocols Using the Control Panel

1. Log in to the machine as the machine administrator on the control panel.

Logging in to the Machine as an Administrator

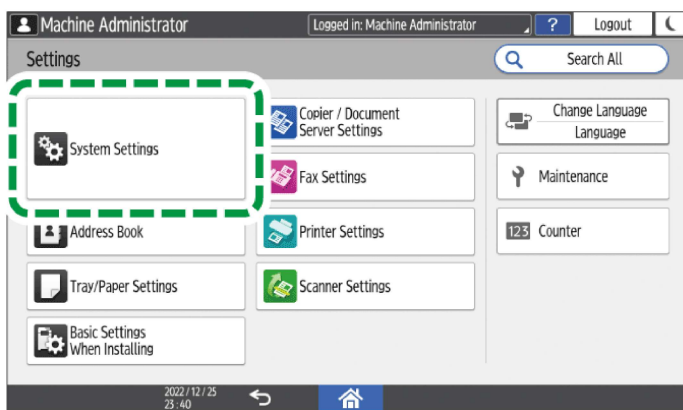
When custom-privileges administrators are registered, you can log in to the machine as a custom-privileges administrator with the Network/Interface privilege as well.

Logging in to the Machine as a Custom-Privileges Administrator

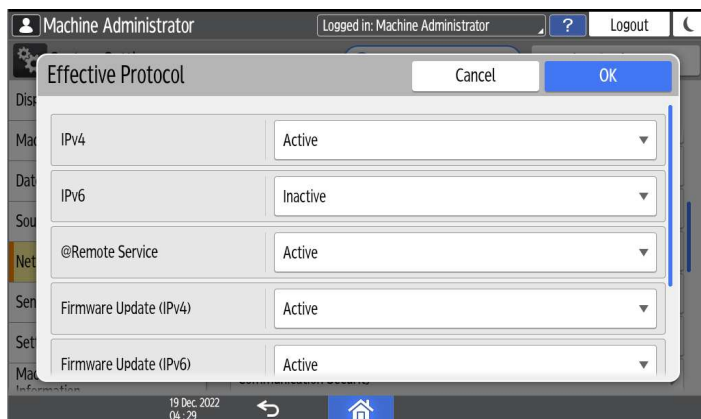
2. On the Home screen, press [Settings].



3. Press [System Settings].



4. Press **[Network/Interface]** ► **[Effective Protocol]**.
5. From the list next to each unused protocol, select **[Inactive]**.



6. Press **[OK]**.
7. Press **[Home]** () , and then log out of the machine.

Section Top

Disabling Unused Protocols Using Web Image Monitor

1. **Log in to the machine as the network administrator from Web Image Monitor.**
 Logging in to the Machine as an Administrator
 When custom-privileges administrators are registered, you can log in to the machine as a custom-privileges administrator with the Security privilege as well.
 Logging in to the Machine as a Custom-Privileges Administrator
2. Click **[Configuration]** on the **[Device Management]** menu.
3. Click **[Network Security]** in the "Security" category.
4. Specify protocols to disable or port numbers to close.
5. Click **[OK]**.

6. **Log out of the machine, and then exit the Web browser.**

[Section Top](#)

Encrypting Data to Prevent Data Leaks Caused by a Stolen or Disposed Machine

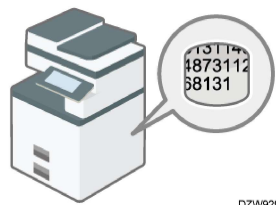
By encrypting data on the internal storage of the machine, you can prevent possible data leaks when you replace or dispose of the machine, or even if the machine were to be stolen.

Encrypting data on the internal storage



Encryption is an effective measure against data leaks. Be sure to keep the encryption key secure to use for decryption. Print it on a sheet or save it to a USB flash memory device.

Overwriting data to prevent restoration



You can delete data that you do not want to be restored. The Auto Erase Memory Setting function deletes the data temporarily stored on the machine for copying or printing, and the Erase All Memory function deletes all data and initializes the internal storage of the machine. The Auto Erase Memory Setting function is available only when the machine is equipped with the HDD option.

Encrypting Data on the Internal Storage

CAUTION

- Keep SD cards and 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.

You can encrypt data contained in the Address Book, authentication information, and stored documents to prevent data leaks in case the internal storage is removed from the machine.

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

The encryption algorithm used in the machine is AES-256.

★ Important

- The machine cannot be operated while encrypting data or canceling encryption.
- Do not turn off the power of the machine while encrypting data or canceling encryption. If you turn off the power, the internal storage may be damaged and all data may be unusable.
- After completing this procedure on the machine's control panel, turn off the main power and restart the machine to enable the new settings by turning it back on. Restarting can be slow when there is data to be carried over to the internal storage.
- The process for encrypting the standard internal storage takes several minutes.
- The encryption key is required for data recovery or migration to another machine. Be sure to keep the encryption key secure by printing it on a sheet or storing it in a USB flash memory device.
- To transfer data from the machine to another machine, you must decrypt the encrypted data. Contact your service representative for data migration.
- If you specify both the Erase All Memory function and the encryption function, the Erase All Memory function is performed first. Encryption starts after the Erase All Memory function has been completed and the machine has been rebooted.
- When you execute encryption/decryption function, the data in the internal storage will be initialized, so the device certificate will be deleted. After completing the encryption/decryption, install device certificate again and restart the machine as necessary.

Installing a Self-signed Certificate/Certificate Issued by a Certificate Authority

1. **Log in to the machine as the machine administrator on the control panel.**

Logging in to the Machine as an Administrator

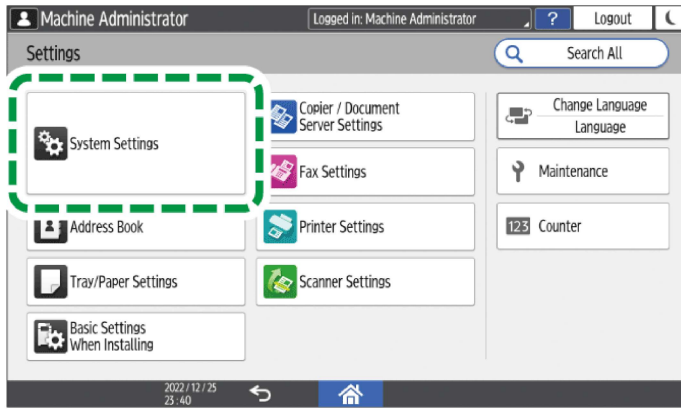
When custom-privileges administrators are registered, you can log in to the machine as a custom-privileges administrator with the File Management privilege as well.

Logging in to the Machine as a Custom-Privileges Administrator

2. **On the Home screen, press [Settings].**



3. Press [System Settings].



4. Press [Settings for Administrator] ► [File Management] ► [Machine Data Encryption Settings].

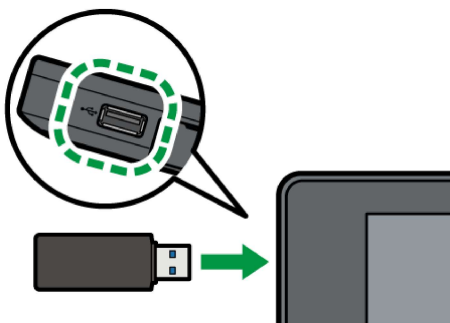
5. Press [Encrypt].



- If the data has been encrypted, you can decrypt the data or back up the data.
 - Cancel Encryption: Cancels encryption.
 - Back Up Encryption Key: Makes a backup of the encryption key. The encryption setting is not changed.

6. Select the location to store the encryption key.

- Save to Media: Saves the encryption key to a USB flash memory device. Insert a USB flash memory device into the media slot, and then press [Save to Media] ► [OK].



- Print on Paper: Prints the encryption key on a sheet of paper. Press [Print on Paper] ► [Print].

7. Press [OK].

8. When the confirmation dialog is displayed, press [Exit].

9. Press [Home] () , and then log out of the machine.

10. **Turn off the main power of the machine, and then turn it back on.**

When the main power is turned on, the machine starts to convert the data on the memory. Wait until the message "Memory conversion complete. Turn the main power switch off." appears. After that, turn off the main power again.

Section Top

Enabling the Auto Erase Memory Setting Function

When the machine is equipped with the HDD option, you can overwrite and erase job data that was temporarily stored on the machine when using certain functions.

★ Important

- When the Auto Erase Memory Setting function is set to [On], temporary data that remained on the hard disk while the Auto Erase Memory Setting function was set to [Off] might not be overwritten.
- If the main power switch is turned off before the Auto Erase Memory Setting process 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 the Auto Erase Memory Setting process is completed, overwriting will continue once the main power switch is turned back on.
- If an error occurs before the overwriting process is completed, turn off the main power. Turn it back on, and then repeat from Step 1.
- The machine will not enter Sleep mode until the overwriting process is completed.

1. **Log in to the machine as the machine administrator on the control panel.**

Logging in to the Machine as an Administrator

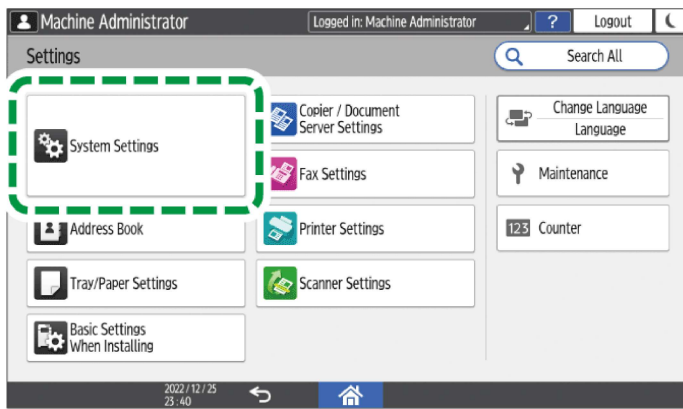
When custom-privileges administrators are registered, you can log in to the machine as a custom-privileges administrator with the Data Management privilege as well.

Logging in to the Machine as a Custom-Privileges Administrator

2. **On the Home screen, press [Settings].**



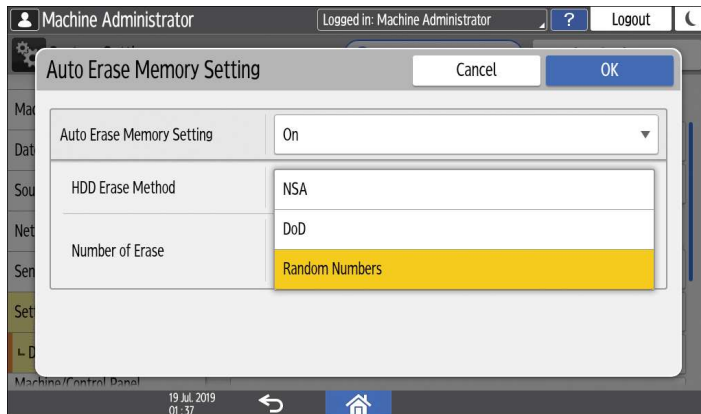
3. **Press [System Settings].**



4. Press [Settings for Administrator] ► [Data Management] ► [Auto Erase Memory Setting].

5. From the list next to Auto Erase Memory Setting, select [On], and then select an erase method.

The default erase method is [Random Numbers], and the default number of overwrites is [3].



- NSA^{*1}: Overwrites data twice with random numbers and once with zeros.
- DoD^{*2}: Overwrites data with a random number, then with its complement, then with another random number, and the data is verified.
- Random Numbers: Overwrites data multiple times with random numbers. Select the number of overwrites from one to nine.

^{*1} National Security Agency (U.S.A)

^{*2} Department of Defense (U.S.A)

6. Press [OK].

7. Press [Home] (🏠), and then log out of the machine.

⬇️ Note

- If you enable the Auto Erase Memory Setting function along with the data encryption function, the overwriting data will also be encrypted.

To check the overwriting process on the control panel

When the Auto Erase Memory Setting function is enabled, the data overwrite icon is displayed at the bottom right of the control panel screen to indicate the status of data that is not overwritten.

★ Important

- The machine will not enter Sleep mode while overwriting is in progress. When overwriting has been completed, the machine enters Sleep mode.
- Do not turn off the main power of the machine while overwriting is in progress. Be sure to check the data status with the data overwrite icon on the screen.
- Even though there is Hold Print/Stored Print/Locked Print/Sample Print data in the hard disk, the "No data remains" icon is displayed as the data overwrite icon.



There is data to be overwritten. 	This icon lights up when there is data to be overwritten, and flashes during overwriting. Overwriting starts automatically once the job is completed. The Copier, Fax, and Printer functions take priority over the Auto Erase Memory Setting function. Overwriting will start after the job is completed.
No data remains. 	The trash box of the icon is empty when there is no data to be overwritten. This icon is also displayed when there is Hold Print/Stored Print/Locked Print/Sample Print data in the hard disk.

↓ Note

- As data scanned enabling the read-ahead function of the TWAIN driver is stored on the HDD, it can be overwritten. Data scanned without enabling the read-ahead function is not overwritten.
- If the data overwrite icon indicates that there is data to be overwritten while there is no data to be overwritten, turn off the main power of the machine. Turn it on again and see if the icon changes to indicate that there is no data to be overwritten. If it does not change, contact your service representative.
- If the data overwrite icon is not displayed, first check if the Auto Erase Memory Setting function is set to [Off]. If the icon is not displayed even though the Auto Erase Memory Setting function is set to [On], contact your service representative

Initializing the Machine with the Erase All Memory Function

Overwrite and erase all data stored on the internal storage 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 service representative.

★ Important

- If the main power switch is turned off before the Erase All Memory process is completed, overwriting will be stopped and data will be left on the internal storage. Do not stop the overwrite mid-process. Doing so will damage the internal storage.
- Before you start the Erase All Memory process, we recommend that you back up the user codes, the counters for each user code, and the Address Book. You can back up the user codes and the counters for each user code using Device Manager NX. For details, see Device Manager NX Help. You can back up the Address Book using the control panel.

Backing Up/Restoring the Address Book Using Control Panel

- If the method of Random Numbers is selected and overwrite three times is set on the machine with the standard internal storage, the Erase All Memory process takes up to 2 hours and 15 minutes. You cannot operate the machine during overwriting.
- 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 the Erase All Memory process is completed.

1. **Log in to the machine as the machine administrator on the control panel.**

Logging in to the Machine as an Administrator

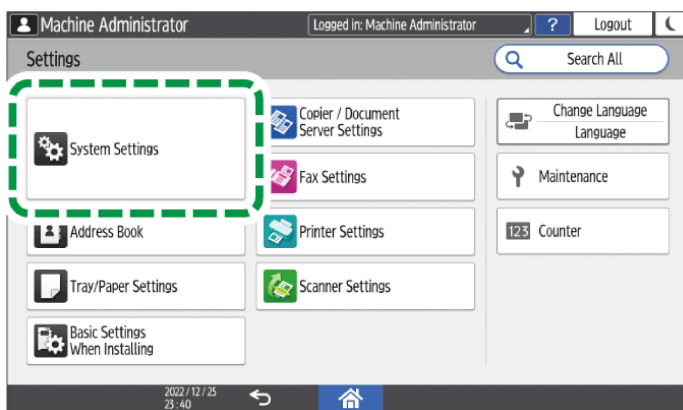
When custom-privileges administrators are registered, you can log in to the machine as a custom-privileges administrator with the Data Management privilege as well.

Logging in to the Machine as a Custom-Privileges Administrator

2. **On the Home screen, press [Settings].**



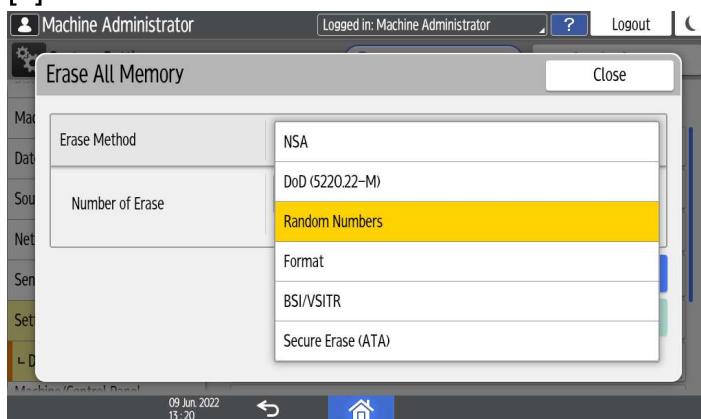
3. **Press [System Settings].**



4. Press [Settings for Administrator] ► [Data Management] ► [Erase All Memory].

5. From the list next to Erase Method, select an erase method.

The default erase method is [Random Numbers], and the default number of overwrites is [3].



- NSA^{*1}: Overwrites data twice with random numbers and once with zeros.
- DoD (5220.22-M)^{*2}: Overwrites data with a random number, then with its complement, then with another random number, and the data is verified.
- Random Numbers: Overwrites data multiple times with random numbers. Select the number of overwrites from one to nine.
- Format: Formats the internal storage. Data is not overwritten.
- BSI/VSITR: Overwrites data seven times with the fixed value (for example: 0x00).
- Secure Erase (ATA): Overwrites data using an algorithm that is built in to the internal storage.

*1 National Security Agency (U.S.A)

*2 Department of Defense (U.S.A)

6. Press [Erase].

7. Press [Yes].

8. When the Erase All Memory process is completed, press [Exit], and then turn off the main power of the machine.

- If the main power of the machine is turned off before the Erase All Memory process is completed, overwriting will start over when the main power is turned back on.
- If an error occurs before overwriting is completed, turn off the main power of the machine. Turn it back on, and then repeat from Step 1.
- To print the erase result, press [System Settings] ► [Settings for Administrator] ► [Data Management] ► [Erase All Memory], and then press [Print Report].
- Initialize the settings on the control panel as necessary. Press [System Settings] ► [Settings for Administrator] ► [Data Management] ► [Restore Default Control Panel Settings] to initialize the data, including the individual application settings and cache memory.

[Section Top](#)

Controlling Access to Untrusted Websites from the Control Panel | Restricting Operations of the Customer Engineer without the Supervision of the Machine Administrator

[Page Top](#)

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.

1. Log in to the machine as the user administrator on the control panel.

Logging in to the Machine as an Administrator

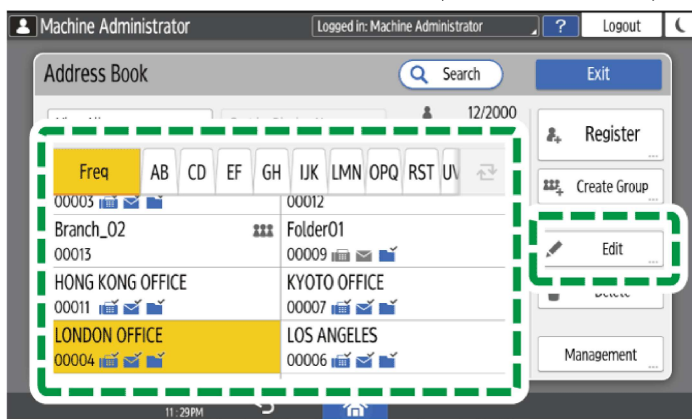
When custom-privileges administrators are registered, you can log in to the machine as a custom-privileges administrator with the Address Book privilege as well.

Logging in to the Machine as a Custom-Privileges Administrator

2. On the Home screen, press [Address Book].

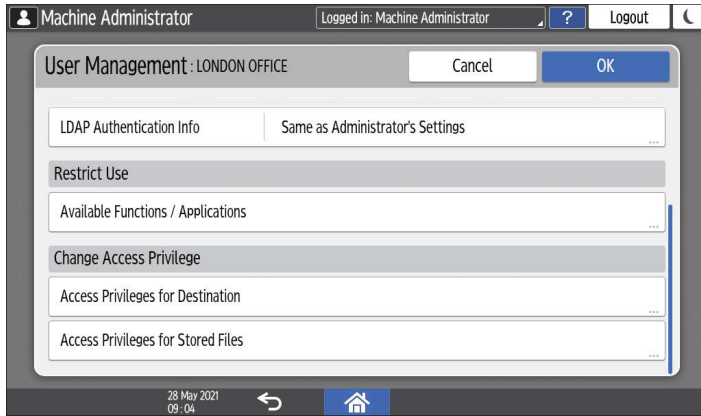


3. On the Address Book screen, select a user, and then press [Edit].



4. Press the [User Management / Other] tab ► [User Management].

5. Press **[Available Functions / Applications]** under **Restrict Use**, and then select available functions.



6. Press **[OK]** several times until the **Address Book** screen is displayed.

7. Press **[Exit]**.

8. When the confirmation dialog box is displayed, press **[Close]**, and then log out of the machine.

To back up the changed contents, press **[Go to Backup]**.

Backing Up/Restoring the Address Book Using Control Panel

Logging in to the Machine Using an IC Card or a Smart Device | Executing a Print Job with Authentication Information Only

[Page Top](#)

Preparing the Server to Use for User Authentication

When using Windows authentication or LDAP authentication as the user authentication method for the first time, check that your server environment meets the requirements for user authentication, and configure the required settings.

To use Windows authentication

Prepare the server as follows:

1. Check the requirements of Windows authentication.
2. Install the Web server (IIS) and the Active Directory Certificate Service in the server.
3. Create a server certificate.
You do not need to create a server certificate to transmit user information that is not encrypted.

To use LDAP authentication

Check the requirements of LDAP authentication, and configure the settings according to the server environment as necessary.

Requirements of Server Authentication Used for User Authentication

Windows authentication

Items	Explanation
Usable OS	Windows Server 2012/2012 R2/2016/2019/2022
Authentication method	Supports the following authentication methods: • NTLM authentication (NTLMv1/NTLMv2) • Kerberos authentication

Requirements for authentication	• Set up a domain controller in the domain you specify. • To obtain user information when Active Directory is running, use LDAP. It is recommended that communication be encrypted between the machine and the LDAP server by using SSL/TLS. The server must support the TLS 1.0/1.1/1.2/1.3 or SSL 3.0 encryption method. Register the server certificate of the domain controller in advance. Creating a Server Certificate • TLS 1.0, TLS 1.1, and SSL 3.0 are disabled by default. To use TLS 1.0/1.1 or SSL 3.0, enable it on Web Image Monitor. • Data transmission between the machine and the KDC (Key Distribution Center) server must be encrypted if Kerberos authentication is enabled. Encrypting Network Communication
---------------------------------	--

 Note

- The server can authenticate users managed in other domains, but cannot obtain information such as an e-mail address.
- When Kerberos authentication is enabled together with SSL/TLS, the e-mail address cannot be obtained.
- Even if you edit an authenticated user's information, such as an e-mail address, in the machine's Address Book, it may be overwritten by the information from the server when authentication is performed.
- If you created a new user in the domain controller and selected "User must change password at next login" at password configuration, first log on the computer and change the password.
- 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].

LDAP authentication

Items	Explanations
Usable version	LDAP Version 2.0/3.0

Authentication method	Supports the following authentication methods: • Kerberos authentication • Digest authentication • Cleartext authentication 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.
Requirements for authentication	• To use SSL/TLS, the server must support the TLS 1.0/1.1/1.2/1.3 or SSL 3.0 encryption method. • TLS 1.0, TLS 1.1, and SSL 3.0 are disabled by default. To use TLS 1.0/1.1 or SSL 3.0, enable it on Web Image Monitor. • To use Kerberos authentication, register the realm to distinguish the network area. Registering the Realm • Data transmission between the machine and the KDC (Key Distribution Center) server must be encrypted if Kerberos authentication is enabled. Encrypting Network Communication • When you use LDAP, only version 3.0 can use Digest authentication.

Notes when the LDAP server is configured using Active Directory

- When Kerberos authentication is enabled together with SSL/TLS, the e-mail address cannot be obtained.
- Anonymous authentication might be available. To improve security, set anonymous authentication to Disable.

Note

- Even if you edit an authenticated user's information, such as an e-mail address, in the machine's Address Book, it may be overwritten by the information from the server when authentication is performed.
- Under LDAP authentication, you cannot specify access limits for groups registered in the 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.
- When using the machine for the first time, the user can use Available Functions specified in [User Authentication Management].

- To specify Available Functions for each user, register the user together with Available Functions in the Address Book, or specify Available Functions in the user registered automatically in the address book.

[Section Top](#)

Installing the Web Server (IIS) and the "Active Directory Certificate Service"

Install the required service in the Windows server to obtain user information registered in Active Directory automatically.

1. **On the [Start] menu, 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 Service] and [Web Server (IIS)] check boxes, and then click [Next].**
If a confirmation message appears, click [Add Features].
7. **Check the features to install, and then click [Next].**
8. **Read the content information, 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, then click [Next].**
When using Windows Server 2016, proceed to Step 12 after reading the content information.
11. **Check the role services to install under Web server (IIS), and then click [Next].**
12. **Click [Install].**
13. **When using Windows Server 2019 or Windows Server 2022, click [Close].**
14. **After completing the installation, click the notification icon of the server manager, and then click [Configure Active Directory Certificate Service on the destination server].**
15. **Click [Next].**
16. **Check [Certification Authority] in the role service, and then click [Next].**
17. **Select [Enterprise CA], and then click [Next].**

18. **Select [Root CA], and then click [Next].**
19. **Select [Create a new private key], and then click [Next].**
20. **Select a cryptographic provider, key length, and hash algorithm to create a new private key, and then click [Next].**
21. **In [Common name for this CA:], enter the Certificate Authority name, and then click [Next].**
22. **Select the validity period, and then click [Next].**
23. **Leave [Certificate database location:] and [Certificate database log location:] without change, and then click [Next].**
24. **Click [Configure].**
25. **When the message "Configuration succeeded" appears, click [Close].**

[Section Top](#)

Creating a Server Certificate

To encrypt user information, create a server certificate in the Windows server. Windows Server 2016 is used as an example.

1. **On the [Start] menu, point to [All Applications], and then click [Internet Information Service (IIS) Manager] of [Administrative Tools].**
2. **In the left column, click [Server Name], and then double-click [Server Certificate].**
3. **In the right column, click [Create Certificate Request...].**
4. **Enter all the information, and 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. **Click [Finish].**

[Section Top](#)

Registering Standard-Privileges Administrators

There are four types of standard administrator privileges in accordance with the functional categories and they are assigned to Administrator 1 through Administrator 4 (built-in administrators). You can assign all four privileges to one person, or assign a specific privilege to a specific person. When Windows authentication or LDAP authentication is activated, you can assign administrator privileges to external authentication server accounts as well (external administrators).

Sharing the administrator tasks facilitates each administrator's tasks and at the same time prevents unauthorized operations by administrators.

Types of standard administrator privileges

	1	2	3	4
	☒	☒	☐	☐
	☒	☐	☒	☐
	☒	☐	☐	☒
	☒	☒	☐	☐

DZW903

- **User Management:** Manages information registered in the Address Book. You can add users to the Address Book and change the registered information.
- **Machine Management:** Mainly manages the settings of the devices. You can configure the settings so that the settings for each function can be changed only by the administrator.
- **Network Management:** Manages the settings for connecting to the network.
- **File Management:** Manages the permission to access the stored files. You can specify the settings so that only the registered users or permitted users can view or edit the files stored in the machine.

Workflow to register built-in administrators

1. Activate Administrator Authentication.

Activate the Administrator Authentication function of the machine from [Settings].

Activating Administrator Authentication

2. Log in to the machine as an administrator.

Enter the login user name and login password of a built-in administrator to log in to the machine.

Logging in to the Machine as an Administrator

3. Add built-in administrators or change the privileges.

Assign the privileges to each administrator. You can register up to four built-in administrators.

Adding Built-in Administrators or Changing the Privileges

Workflow to register external administrators

1. Activate Administrator Authentication.

Activate the Administrator Authentication function of the machine from [Settings].

Activating Administrator Authentication

2. Log in to the machine as an administrator.

Enter the login user name and login password of a built-in administrator to log in to the machine.

Logging in to the Machine as an Administrator

3. Register external administrator groups and assign the privileges.

Register external administrator groups and assign standard administrator privileges.

Registering External Administrator Groups and Assigning the Standard Administrator Privileges

Note

- The built-in administrators are distinguished from the users registered in the Address Book. The login user name registered in the Address Book cannot be used as the login user name of a built-in administrator.

Activating Administrator Authentication

An administrator can manage the machine by activating the management function. Select whether to activate the management function according to the range of information to manage, and then specify the allowable range of settings by users.

Important

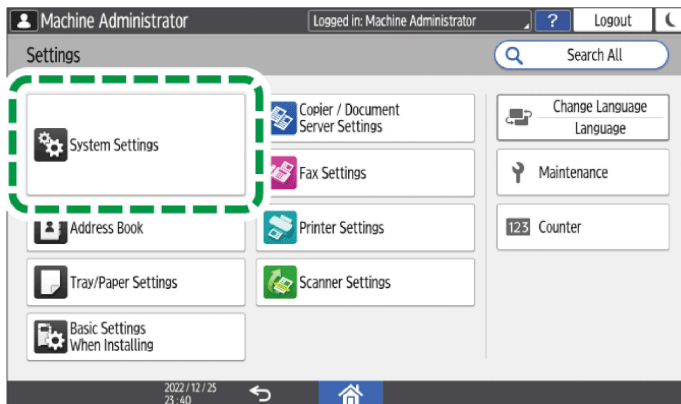
- If you have activated Administrator Authentication, make sure not to forget the login user names and login passwords of the built-in administrators. If you forget an administrator login user name or password, you must specify a new password using the supervisor's privilege.

Changing the Password of a Built-in Administrator

1. On the Home screen, press [Settings].



2. Press [System Settings].

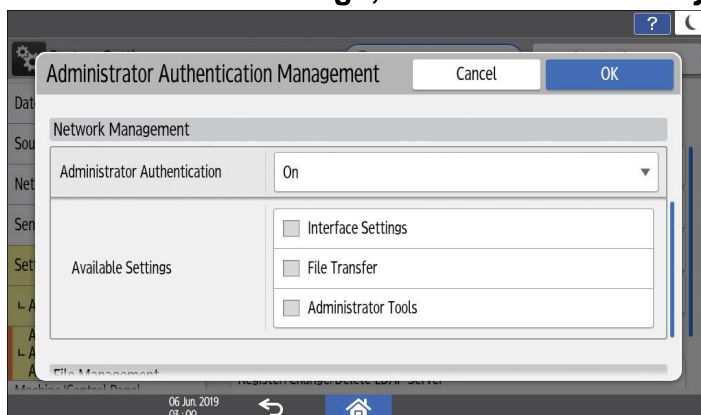


3. Press [Settings for Administrator] ► [Authentication/Charge] ► [Administrator Authentication/User Authentication/App Auth.] ► [Administrator Authentication Management].

4. For each standard administrator privilege to activate Administrator Authentication, select [On] from the list.

- User Management: To manage the information registered in the Address Book, select [On].
- Machine Management: To configure the settings so that the initial settings for each function can be changed only by the administrator, select [On]
- Network Management: To manage the network settings, select [On].
- File Management: To manage the files stored in the machine, select [On].

5. From Available Settings, select the items subject to management.



The selected items cannot be changed by users.

User Management

- Administrator Tools: Mainly restrict the settings for the Address Book.

Machine Management

Press [Not Selected] next to Available Settings, select the items subject to management on the Available Settings screen, and then press [OK].

- General Features: Restrict the settings for the control panel and paper output tray.
- Tray Paper Settings: Restrict the settings for the size and type of the paper set in the paper tray.
- Timer Settings: Restrict the settings for the time and processing hours.
- Interface Settings: Restrict the settings related to the network.
- File Transfer: Restrict the settings related to the e-mail send and receive functions.
- Administrator Tools: Mainly restrict the settings related to the machine.
- Maintenance: Restrict the settings for print correction.

Network Management

- Interface Settings: Restrict the settings related to the network.
- File Transfer: Restrict the settings related to the e-mail send and receive functions.
- Administrator Tools: Mainly restrict the settings related to the network and security.

File Management

- Administrator Tools: Restrict the settings for the File Protection and Document Server functions.

6. Press [OK].

7. Press [Home] ()

8. When the confirmation dialog is displayed, press [OK] to log out of the machine.

Note

- Administrator Authentication can also be activated via Web Image Monitor. For details, see Web Image Monitor Help.

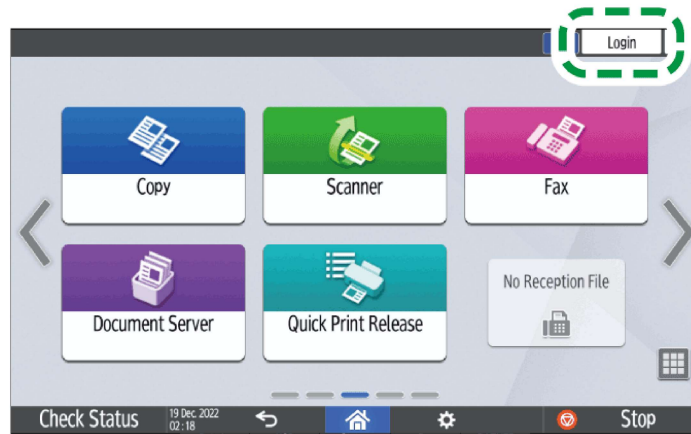
[Section Top](#)

Logging in to the Machine as an Administrator

To log in to the machine for the first time, log in as Administrator 1 of the built-in administrators. Refer to the provided guide for the login user name. Enter the login password that was set as the login password at the first startup.

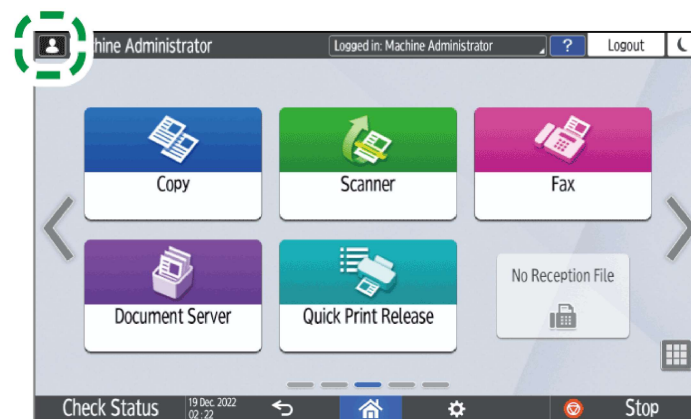
Logging in to the machine using the control panel

1. On the Home screen, press [Login].



2. Enter the login user name and login password of an administrator, and then press [Login].

When you log in, the user icon is displayed at the upper left on the screen.



To register or change a built-in administrator, follow the procedures described in Adding Built-in Administrators or Changing the Privileges.

3. After completing machine operations, press [Logout].

You can also log out of the machine by pressing the energy saver key ().

Note

- If you log in to the machine using one of the standard administrator privileges, the name of the built-in administrator logging in appears. When you log in with a user name that has multiple standard administrator privileges, one of the standard administrator privileges associated with that name is displayed.
- For the characters that can be used for login user names and passwords, see Usable Characters for User Names and Passwords.

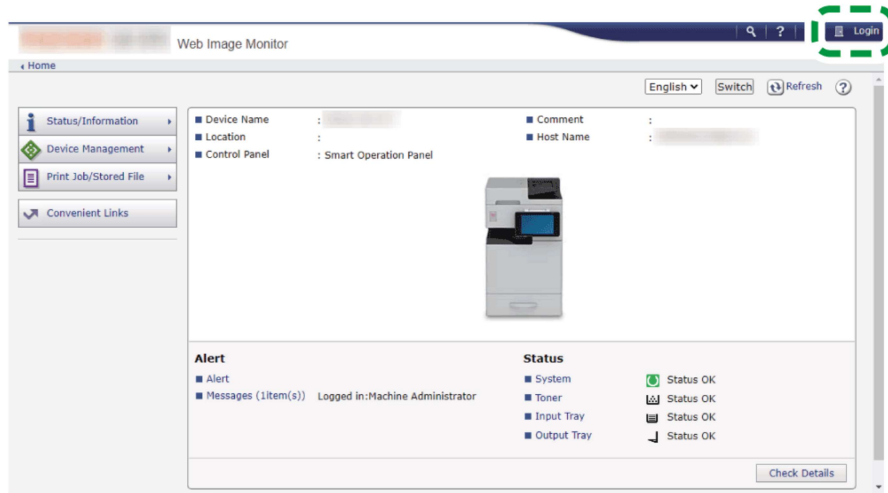
Logging in to the machine using Web Image Monitor

1. **Launch the Web browser.**

2. **Enter "http://(IP address of the machine or host name)/" on the address bar of the Web browser, and then press the Enter key.**

Accessing to Web Image Monitor

3. **Click [Login].**



4. **Enter the login user name and login password of the administrator, and then click [Login].**

5. **After completing machine operations, click [Logout].**

Delete the cache memory of a web browser after logging out.

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.

Section Top

Adding Built-in Administrators or Changing the Privileges

You can register up to four administrators. All four registered personnel can have all the standard administrator privileges. To reduce the administrator's load, each of the four registered personnel can have a specific one of the standard administrator privileges.

Discuss the number of users to add and privileges to give in advance, decide the login user name and login password for Administrator 2 to Administrator 4, and configure the settings.

Important

- Do not forget the login user names and login passwords of the added built-in administrators.

- A built-in administrator cannot change the login user names and passwords for other built-in administrators.

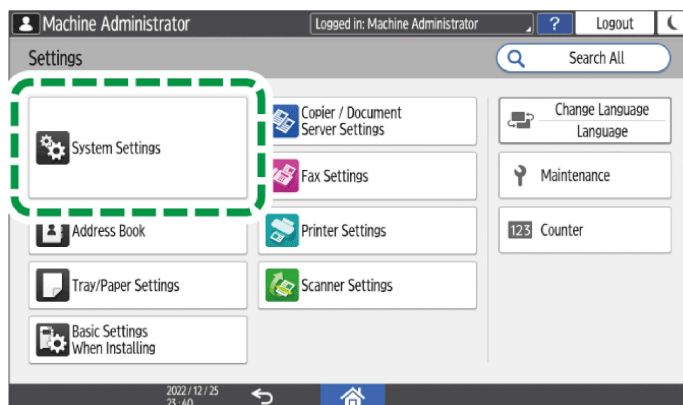
1. Log in to the machine as an administrator with all the standard administrator privileges on the control panel.

Logging in to the Machine as an Administrator

2. On the Home screen, press [Settings].



3. Press [System Settings].



4. Press [Settings for Administrator] ► [Authentication/Charge] ► [Administrator Authentication/User Authentication/App Auth.] ► [Register/Change Administrator] ► [Set Administrator Login User Name/Login Password].

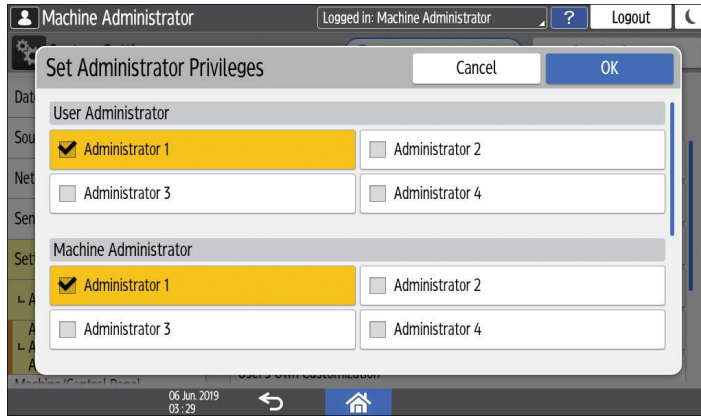
5. Press the desired built-in administrator ([Administrator 1] to [Administrator 4]).

6. Specify the login user name and login password, and then press [OK].

- For the characters that can be used for login user names and passwords, see Usable Characters for User Names and Passwords.
- When you manage the machine with software supporting SNMPv3 such as Device Manager NX, you have to specify the password to encrypt communication.

7. After completing the settings for each administrator, press [Close], and then press [Set Administrator Privileges].

8. **Select a built-in administrator to assign for each standard administrator privilege, and then press [OK].**



- Assign the privileges of User Administrator, Machine Administrator, Network Administrator, or File Administrator to [Administrator 1] to [Administrator 4].
- By default, all standard administrator privileges are assigned to the logged-in built-in administrator (Administrator 1).

9. **Press [OK].**

When settings are complete, the machine logs you out automatically.

Take note of the login user names and login passwords specified for other administrators and inform them of the specified ones.

Note

- An administrator with any one of the standard administrator privileges can add built-in administrators or change the privileges as well by logging in to the machine. The privilege(s) that the administrator can assign to other built-in administrators, however, is limited to the same privilege as the one that is assigned to the administrator himself.
- A custom-privileges administrator with the Authentication/Charge privilege can add built-in administrators as well by logging in to the machine. However, the administrator is not allowed to change the privileges.
- You can add built-in administrators or change the privileges by using Web Image Monitor as well. For details, see Web Image Monitor Help.

[Section Top](#)

Registering External Administrator Groups and Assigning the Standard Administrator Privileges

When Windows authentication or LDAP authentication is activated as the user authentication method, you can register external authentication server accounts as external administrators. Register external administrator groups and assign the same four types of standard administrator privileges as the ones that are assigned to the built-in administrators.

To register a Windows server account as an external administrator, register an external administrator group with the same name as the global account to which the target account belongs and for which it has administrative privileges. You first need to confirm the name of

the global group to which the target account belongs.

Specifying Windows Authentication

★ Important

- You cannot configure any Windows server account as an account for SNMPv3 access.
- When the central address book management is enabled, no external administrators can be registered.

Others (System Settings)

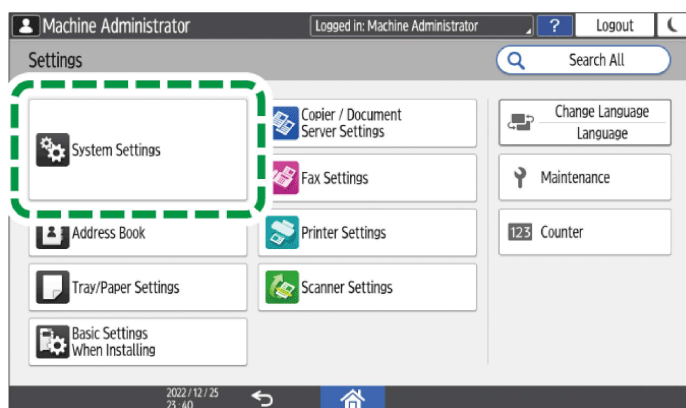
1. **Log in to the machine as an administrator with all the standard administrator privileges on the control panel.**

Logging in to the Machine as an Administrator

2. **On the Home screen, press [Settings].**



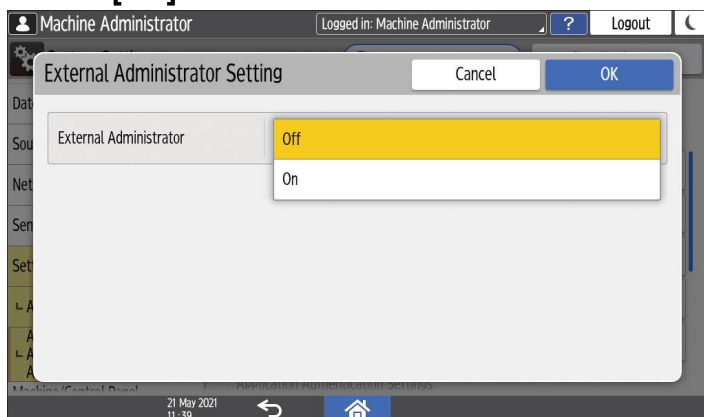
3. **Press [System Settings].**



4. **Press [Settings for Administrator] ► [Authentication/Charge] ► [Administrator Authentication/User Authentication/App Auth.] ► [Register/Change Administrator].**

5. **Press [External Administrator Setting] under External Administrator.**

6. **Select [On] from the list next to External Administrator, and then press [OK].**



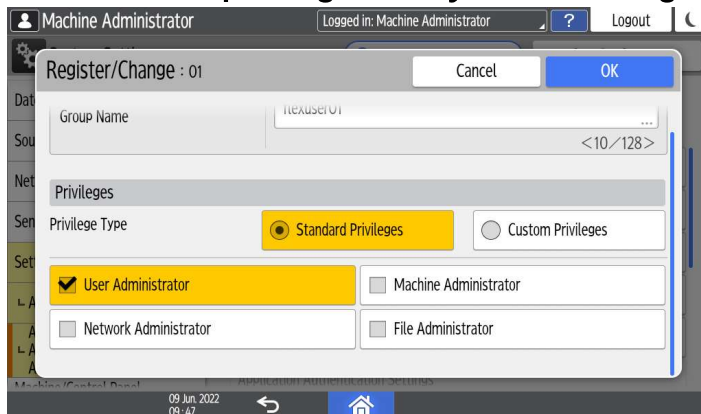
7. **Press [External Administrator Group Management] under External Administrator.**

8. **Select [* Not Registered], and then press [Register/Change].**

9. **Enter the name of an external administrator group for Group Name.**

To register Windows server accounts as external administrators, enter the same group name as the name of the global group to which the target account belongs.

10. **Select [Standard Privileges] next to Privilege Type, and then select the administrator privileges that you want assign to the external administrator.**



11. **Press [OK].**

12. **Press [Close].**

13. **Press [OK].**

When settings are complete, the machine logs you out automatically.

Note

- You can register up to 10 external administrator groups.
- To change the name or standard administrator privilege of the registered external administrator group, select a group name in step 8, and then press [Register/Change].
- To delete the registered external administrator group, select a group name in step 8, and then press [Delete].
- An administrator with any one of the standard administrator privileges can add external administrator groups or change the privileges as well by logging in to the machine. The privilege(s) that the administrator can assign to other external administrator groups, however, is limited to the same privilege as the one that is assigned to the administrator himself.
- In the event that a user account on the Windows server belongs both to a group with the administrator privileges and to an ordinary user group, the user is recognized as an ordinary user, not as an external administrator, when logging in to the machine. To let the user log in to the machine as an external administrator, make sure that the user is not a member of an ordinary user group on the Windows server.
- When a user registered in the Address Book of the machine logs in to the machine, user recognition by the machine varies depending on the group to which the user is registered on the Windows server.
 - When registered in a group with the administrator privileges: Recognized as an external administrator.

- When registered in an ordinary user group: Recognized as the same user as the one registered in the address book of the machine.
- You can register external administrator groups and assign the standard administrator privileges using Web Image Monitor as well. For details, see Web Image Monitor Help.

[Section Top](#)

[Taking Measures to Prevent Security Threats](#) | [Registering Custom-Privileges Administrators](#)

[Page Top](#)

Using the Supervisor Privilege

The supervisor has the privilege to manage the built-in administrators. When the built-in administrator is changed, the supervisor can reset the login password. There is only one supervisor.

Changing the Supervisor Settings

This section describes how to change the supervisor's login user name and password.

Refer to the provided guide for the default login user name and login password of the supervisor.

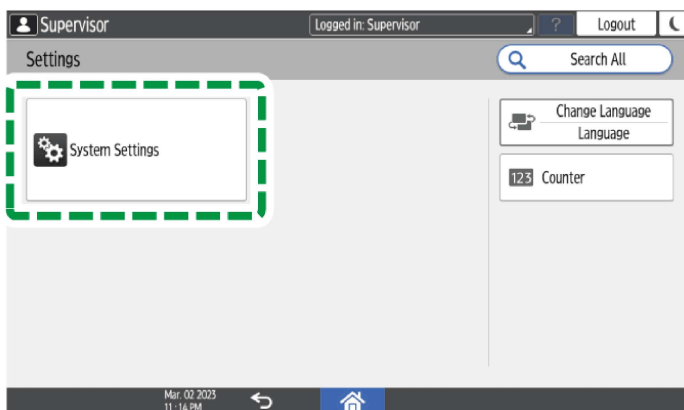
★ Important

- Do not forget the login user name and login password of the supervisor. If you forget these, you have to restore the factory default settings, which will result in loss of data.
1. **Log in to the machine as the supervisor on the control panel.**
Logging in to the Machine as an Administrator

2. **On the Home screen, press [Settings].**



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



4. **Press [Settings for Administrator] ► [Authentication/Charge] ► [Administrator Authentication/User Authentication/App Auth.] ► [Register/Change Administrator] ► [Set Administrator Login User Name/Login Password].**

5. Press [Supervisor].



6. Enter the login user name for Login User Name.

7. Press [Change] next to Login Password.

8. Enter the login password for New Password.

9. Enter the login password for Confirm New Password again.

10. Press [OK] twice.

11. Press [Close].

12. Press [OK].

When settings are complete, the machine logs you out automatically.

Note

- For the characters that can be used for login user names and passwords, see Usable Characters for User Names and Passwords.

[Section Top](#)

Changing the Password of a Built-in Administrator

Only the supervisor has the privilege to change the password of the built-in administrators. If a built-in administrator forgets the password or wants to change the password, the supervisor must reset the password.

Refer to the provided guide for the default login user name and login password of the supervisor.

Important

- Do not forget the login user name and login password of the supervisor. If you forget these, you have to restore the factory default settings, which will result in loss of data.

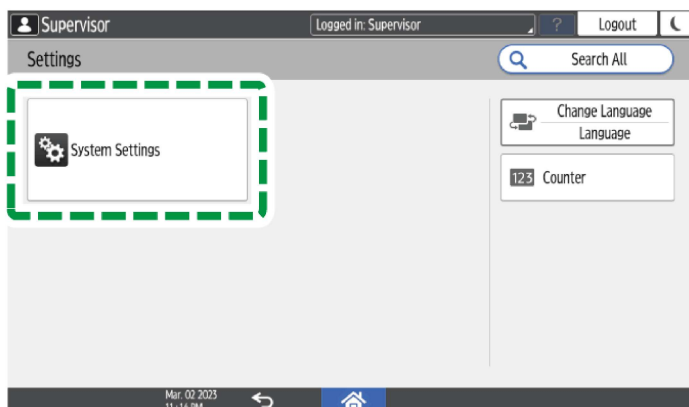
1. Log in to the machine as the supervisor on the control panel.

Logging in to the Machine as an Administrator

2. On the Home screen, press [Settings].



3. Press [System Settings].



4. Press [Settings for Administrator] ► [Authentication/Charge] ► [Administrator Authentication/User Authentication/App Auth.] ► [Register/Change Administrator] ► [Set Administrator Login User Name/Login Password].

5. Press the desired built-in administrator ([Administrator 1] to [Administrator 4]).



6. Press [Change] next to Login Password.

7. Enter the login password for New Password.

8. Enter the login password for Confirm New Password again.

9. Press [OK] twice.

10. Press [Close].

11. Press [OK].

When settings are complete, the machine logs you out automatically.

Note

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

Section Top

Changing the Administrator Login Setting

Only the supervisor has the privilege to allow/prohibit login to the machine by the built-in administrators.

In the event of a failure in communicating with an external authentication server while login by the built-in administrators is prohibited and only the external administrators are allowed to log in to the machine, no administrators can log in to the machine. In such a case, the supervisor must change the administrator login setting to allow the built-in administrators to log in to the machine.

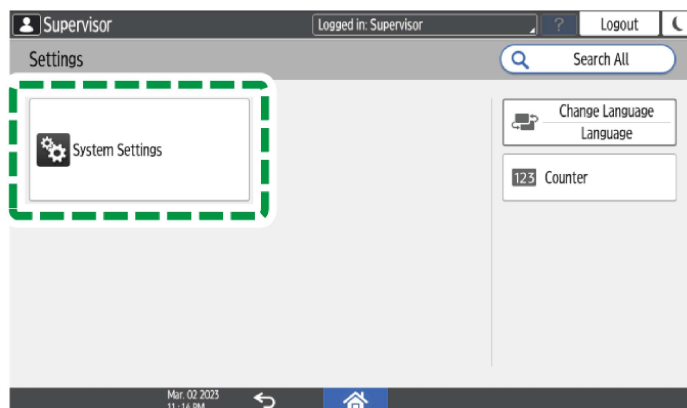
1. Log in to the machine as the supervisor on the control panel.

Logging in to the Machine as an Administrator

2. On the Home screen, press [Settings].

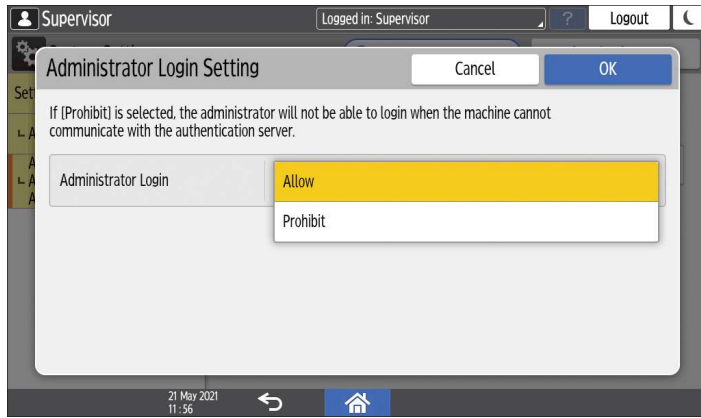


3. Press [System Settings].



4. Press [Settings for Administrator] ► [Authentication/Charge] ► [Administrator Authentication/User Authentication/App Auth.] ► [Register/Change Administrator] ► [Administrator Login Setting].

5. **Select [Allow] or [Prohibit] from the list next to Administrator Login.**



6. **Press [OK] twice.**

When settings are complete, the machine logs you out automatically.

[Section Top](#)

[Registering Custom-Privileges Administrators](#) | [Usable Characters for User Names and Passwords](#)

[Page Top](#)

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)

	Supervisor/Built-in Administrators/Users	External Administrators
Login user name	• Can be up to 32 characters long. • Cannot contain spaces, colons or quotation marks. • Cannot be left blank. • The login user name of the supervisor and administrators must contain characters other than numerical characters (numbers) if it is up to 8 characters. If it consists of only numbers, 9 or more must be used.	

Login password	• The maximum password length for the administrators and supervisor is 32 characters. • The maximum password length for users is 128 characters. • There are no restrictions on the types of characters that can be used for a password. For security, it is recommended to create passwords consisting of uppercase or lowercase characters, numbers, and symbols. A password consisting of a large number of characters is less easily guessed by others. • In [Password Policy] in [Extended Security Settings], 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. Security	• The maximum password length is 128 characters. *1 • For the other conditions, the password policy of the external authentication server is applied.
----------------	---	--

*1 Attempts to log in as an external administrator may fail from an application where a limitation is imposed on the password length.

Registering the LDAP Server

You can search user information stored in the LDAP Server. Use it for the following purposes:

- When you send files by e-mail under the Scanner or Fax function, you can search the Address Book stored in the server and specify the e-mail address.
- Log in the machine using the authentication information registered in the server.

Note

- A user logged into the LDAP server for the first time is automatically stored in the Address Book.

Managing the User Information Registered Automatically

1. Log in to the machine as the machine administrator on the control panel.

Logging in to the Machine as an Administrator

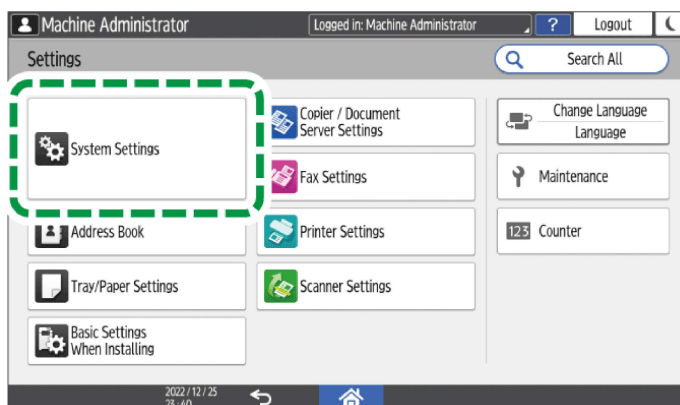
When custom-privileges administrators are registered, you can log in to the machine as a custom-privileges administrator with the Authentication/Charge privilege as well.

Logging in to the Machine as a Custom-Privileges Administrator

2. On the Home screen, press [Settings].



3. Press [System Settings].



4. Press [Settings for Administrator] ► [Authentication/Charge] ► [Administrator Authentication/User Authentication/App Auth.] ► [Register/Change/Delete LDAP Server].

5. Select a Not Registered item, and then press [Register/Change].

6. Enter the information for the LDAP Server.

- Name: Enter a registration name. The name is to distinguish the server from another LDAP server.
- Server Name: Enter the host name or IPv4 address of the LDAP server.
- Search Base: Select a root folder to start a search. E-mail addresses stored in this folder are search targets when files are sent using the Scanner or Fax function.
- Port Number: Enter the port number used for the communication with the LDAP server.
- Use Secure Connection (SSL): When set to [On], the port number is changed to 636. When set to [Off], security problems may occur.
Encrypting Network Communication
- Authentication: Select the authentication method according to the authentication settings of the LDAP server.
 - Kerberos Authentication: Authentication is performed on the KDC server. The password is protected with encryption and is then sent to the KDC server.
When you select [Kerberos Authentication], specify the following:
 - User Name, Password: Enter the user name and password of the account that requests Search to the LDAP server (administrator or representative). For the search request with the authentication information of the user, do not enter. You can browse the Address Book instead of entering the user name and password directly.
 - Realm Name: Select the Realm Name. Register the Realm in advance.
Registering the Realm
 - Digest Authentication: Authentication is performed on the LDAP server. This method is only available on a server supporting LDAP version 3.0. The password is protected with encryption and is then sent to the LDAP server.
 - Cleartext Authentication: The password is sent to the LDAP server without encryption.
 - Off: Select when server authentication is not required.
- Japanese Character Code: Select the Japanese character code used on the LDAP server (if applicable).

7. Press [Connection Test].

8. After checking the connection with the LDAP server, set the search conditions or key display name.



- Search Conditions: Specify the Name, Email Address, Fax Number, Company Name, Department Name, and Group attributes as keywords for search conditions. Enter the Name, Email Address, Fax Number, Company Name, and Department Name attributes using up to 64 characters; and the Group attribute using up to 128 characters. Confirm and specify the server environment to be used. Because attributes are used for searching in the Address Book of the LDAP Server, a search is disabled if attributes are left blank.
- Search Options: Specify [Attribute] and [Display Name] according to the server you are using.
 - Attribute: Enter the attribute for optional search conditions as necessary. For example, to search using the employee number, register "employeeNo" as an attribute. Once search options are stored, register the key display names.
 - Display Name: Enter the display name of the column in which search options are entered. For example, if the search option is the employee number, register "employeeNo".

9. Press [OK].

10. Press [Close].

11. Press [Home] () , and then log out of the machine.

 Note

- To change/delete the stored LDAP server, select the desired LDAP server name, and then press [Register/Change] or [Delete].

Introduction and Basic Operations

Copy

Document Server

Fax

Printer

Scan

Maintenance

Troubleshooting

Settings

Security

Introduction

Taking Measures to Prevent Security Threats

Registering Standard-Privileges
Administrators

Registering Custom-Privileges
Administrators

Using the Supervisor Privilege

Usable Characters for User Names and
Passwords

Preventing Unauthorized Accesses

Taking Measures to Prevent Unauthorized
Access

Verifying Users to Operate the Machine
(User Authentication)

Registering/Changing/Deleting User Codes

Preparing the Server to Use for User
Authentication

Logging in to the Machine Using an IC Card
or a Smart Device

Limiting Available Functions

Executing a Print Job with Authentication
Information Only

Specifying the Policy on Login/Logout

Access Control

Encrypting Network Communication

Preventing Information Leaks

Taking Measures to Prevent Information
Leaks

Security

[Usable Characters for User Names and Passwords](#)[Preventing Unauthorized Accesses](#)[Taking Measures to Prevent Unauthorized Access](#)[Verifying Users to Operate the Machine \(User Authentication\)](#)[Registering/Changing/Deleting User Codes](#)[Preparing the Server to Use for User Authentication](#)[Logging in to the Machine Using an IC Card or a Smart Device](#)[Limiting Available Functions](#)[Executing a Print Job with Authentication Information Only](#)[Specifying the Policy on Login/Logout](#)[Access Control](#)[Encrypting Network Communication](#)[Preventing Information Leaks](#)[Taking Measures to Prevent Information Leaks](#)[Preventing Information Leaks by Sending Data to a Wrong Destination](#)[Preventing Information Leaks from the Media Slot](#)[Preventing Data Leaks from Printed Sheets](#)[Preventing Printing Personal Information in Fax Reports](#)[Controlling Access to Untrusted Websites from the Control Panel](#)[Encrypting Data to Prevent Data Leaks Caused by a Stolen or Disposed Machine](#)[Restricting Operations of the Customer Engineer without the Supervision of the Machine Administrator](#)[Specifications](#)[Setup](#)[Driver Installation Guide](#)[How to use this manual](#)

Security

[Browser Settings](#)[Introduction](#)

Specifying the Policy on Login/Logout

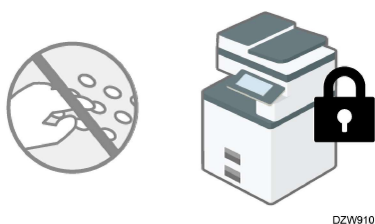
To protect the data in the machine, configure the machine so that login and logout are performed properly.

User authentication cannot prevent unauthorized use completely. For example, an unauthorized person can log in to the machine by guessing the password. If a user does not log out of the machine, another user can use the privileges of the previous user.

Specify the following functions to protect the machine against such risks.

User Lockout

If an incorrect login password is entered several times, the user lockout function prevents further login attempts under the same login user name (Lockout). The locked-out state can be automatically released in a specified period of time. It can be manually released by the administrator as well.



- The number of times that the locked-out state is automatically released can be limited to a maximum of four times. For each of the 1st to 4th lockout actions, you can specify whether to activate/deactivate the user lockout function, the number of login attempts before lockout, and the period of time before the locked-out state is automatically released.
- You can also specify whether to release the locked-out state by restarting the machine. Specifying User Lockout
- By default, an incorrect login password entry is permitted up to five times and the locked-out state is not released automatically.

Note

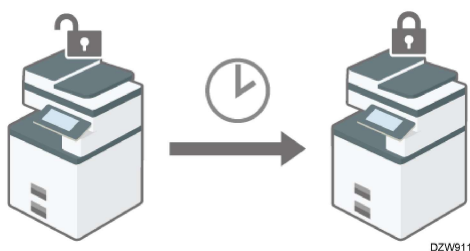
- The User lockout function is enabled on all users only when Basic authentication is specified. Under Windows authentication and LDAP authentication, only the supervisor and administrators are protected by User lockout. The policy of the certification server is applied to the other users.
- In the event that a user enters an incorrect login password, and the machine administrator changes the number of attempts before lockout afterwards, the state of the user concerning lockout may vary in accordance with the number of attempts before lockout that is changed by the administrator. Some examples are as follows:

Number of incorrect login password entries by user	Change to the number of attempts before lockout	State of user
3 entries	Twice -> 4 times	The locked-out state of the user is released.
3 entries	4 times -> Twice	The user is locked out.
3 entries	4 times -> 6 times	Remains unchanged (The user is not locked out.) ^{*1}

^{*1} After 3 entries of an incorrect login password, two more incorrect entries are permitted, and when an incorrect entry is performed for a third time, the user is locked out.

Auto Logout Timer

After you log in, the machine logs you out automatically if you do not use the control panel within a given time.



- By default, the machine logs you out automatically if you do not use the control panel for three minutes.

Timer

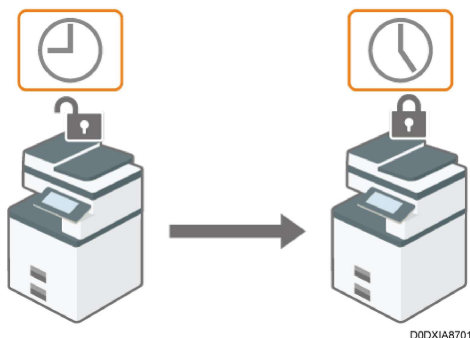
- When the time period to allow users to log in to and use the machine is specified, the machine logs you out upon completion of the time period even though the auto logout timer has not expired.

Specifying the Time Period to Allow Users to Log In to and Use the Machine

- For details about auto logout from Web Image Monitor, see Web Image Monitor Help.

Time Settings Allowing Operating Machine by Logging in

When the time period to allow users to log in to and use the machine is specified, the machine logs you out upon completion of the time period.



Specifying the Time Period to Allow Users to Log In to and Use the Machine

Specifying User Lockout

Specify the number of login password attempts to permit before locking out the user and the period of time until the lockout is released automatically.

1. **Log in to the machine as the machine administrator from Web Image Monitor.**
Logging in to the Machine as an Administrator
2. **Click [Configuration] on the [Device Management] menu.**
3. **Click [User Lockout Policy] in the "Security" category.**
4. **Specify the number of login password attempts to permit before locking out the user and the period of time until the lockout is automatically released.**

- **Lockout (nth Time)**
Select [Active], and then specify "Number of Attempts before Lockout" from 1 to 10.
- **Lockout Release Timer**
Select [Active] to release the locked-out state after a specified time elapses, and then enter the desired value in "Lock Out User for" up to 9999 minutes (about seven days).
- **Release Lockout When Restarting and Rebooting System**
Specify whether to activate the lockout release function by restarting the machine. The supervisor and administrators are subject to the lockout release function. It takes about 60 seconds for the locked-out state to be actually released after the machine restarts.

5. **Click [OK].**

6. **Log out of the machine, and then exit the Web browser.**

Section Top

Releasing the Locked-out State

When a general user is locked out, the user administrator must log in and release the locked-out state.

1. **Log in to the machine as the user administrator from Web Image Monitor.**
Logging in to the Machine as an Administrator
2. **Click [Address Book] on the [Device Management] menu.**
3. **Select the locked-out user's account, and then click [Change] on the [Detail Input] tab.**
4. **Select [Inactive] on "Lockout" of "Authentication Information".**
5. **Click [OK].**
6. **Log out of the machine, and then exit the Web browser.**

Note

- When an administrator is locked out, the supervisor must log in to the machine and release the locked-out state. When the supervisor is locked out, the machine administrator must log in to the machine and release the locked-out state. Click [Device Management] ► [Configuration] ► [Program/Change Administrator] to display the Program/Change Administrator screen, and then release the locked-out state.
- For the supervisor and administrators, you can specify whether to activate the lockout release function by restarting the machine as well.
Specifying User Lockout

Specifying the Period of Time Until the Machine Logs You Out Automatically

1. Log in to the machine as the machine administrator on the control panel.

Logging in to the Machine as an Administrator

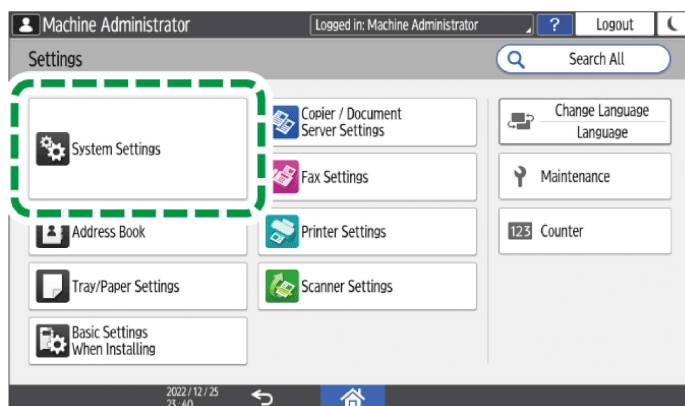
When custom-privileges administrators are registered, you can log in to the machine as a custom-privileges administrator with the Date/Time/Timer privilege as well.

Logging in to the Machine as a Custom-Privileges Administrator

2. On the Home screen, press [Settings].

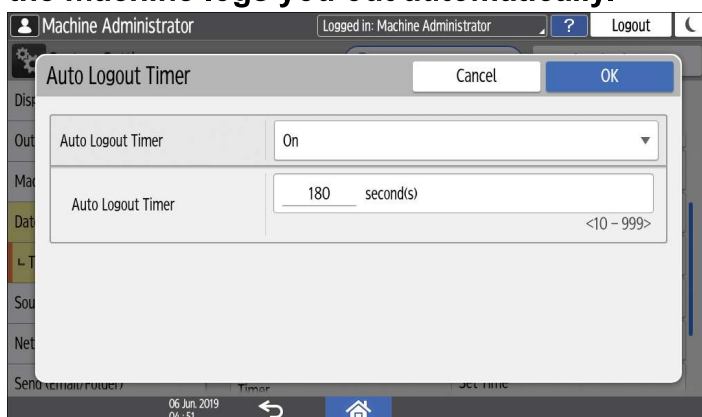


3. Press [System Settings].



4. Press [Date/Time/Timer] ► [Timer] ► [Auto Logout Timer].

5. From the list next to Auto Logout Timer, select [On], enter the period of time until the machine logs you out automatically.



You can enter from 10 to 999 seconds.

6. Press [OK].

7. Press [Home] ()

8. When the confirmation dialog is displayed, press [OK] to log out of the machine.

Note

- When the time period to allow users to log in to and use the machine is specified, the machine logs you out upon completion of this time period even though the auto logout timer has not expired.

Specifying the Time Period to Allow Users to Log In to and Use the Machine

Section Top

Specifying the Time Period to Allow Users to Log In to and Use the Machine

1. Log in to the machine as the machine administrator on the control panel.

Logging in to the Machine as an Administrator

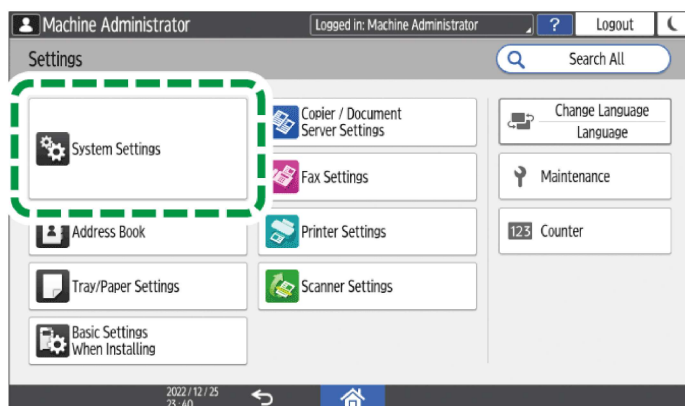
When custom-privileges administrators are registered, you can log in to the machine as a custom-privileges administrator with the Authentication/Charge privilege as well.

Logging in to the Machine as a Custom-Privileges Administrator

2. On the Home screen, press [Settings].

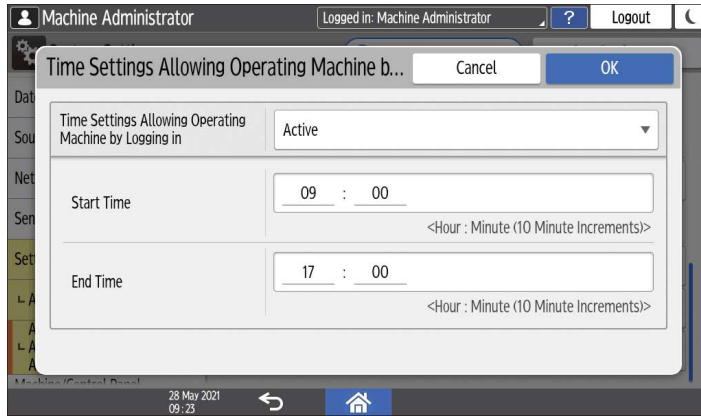


3. Press [System Settings].



4. Press [Settings for Administrator] ► [Authentication/Charge] ► [Administrator Authentication/User Authentication/App Auth.] ► [Time Settings Allowing Operating Machine by Logging in].

5. Select **[Active]** from the list next to **Time Settings Allowing Operating Machine by Logging in**, enter the time for **Start Time** and **End Time**.



6. Press **[OK]**.
7. When the confirmation dialog is displayed, press **[OK]**.
8. Press **[Home]** () , and then log out of the machine.

Note

- You can specify the time period to allow users to log in to and use the machine by using Web Image Monitor as well. For details, see Web Image Monitor Help.

Section Top

Taking Measures to Prevent Security Threats

Appropriate security measures are required to reduce the risk of information leaks and use by unauthorized persons.

The personal information stored in the Address Book and highly confidential files handled by the machine are important information assets. They should be protected from being stolen or abused.

To ensure secure use of the machine, specify the settings of the machine properly according to the specified environments, user level, administrator load, and the company's information security policy.

Administrators refer to special users who have the authority to manage various information and settings of the machine. To use the machine safely, important settings, such as user registration and security settings, must be configured only by administrators. Especially, security settings should be configured before the machine is placed in operation.

There are two types of administrators.

- Standard-privileges administrators
Registering Standard-Privileges Administrators
- Custom-privileges administrators
Registering Custom-Privileges Administrators

The security measures and their settings are described below. Take appropriate measures according to the operation environment of the machine.

1: Basic security measures

2: Strong security measures taken by the functions of the machine

3: Stronger security measures using the options of this machine or external security functions

Defining the administrator of the machine



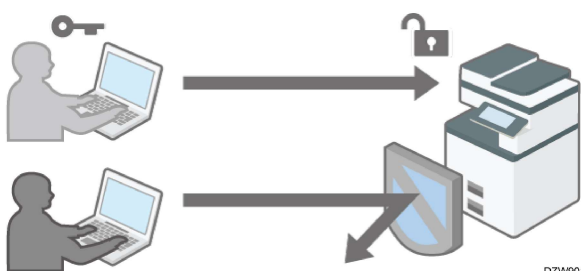
DZW900

1 Select an administrator who performs the maintenance and management of the machine. The administrator performs the important security settings.

Registering Standard-Privileges Administrators

Registering Custom-Privileges Administrators

Preventing unauthorized access by managing the users who can use the machine or the connected network



1 / **2** / **3** The administrator restricts the users who can use the machine to prevent the unauthorized access by unauthorized persons.

Verifying Users to Operate the Machine (User Authentication)

2 Prevent a brute-force attack on the password or unauthorized operation of the machine caused by user inattentiveness.

- When login is continuously fails due to an incorrect login password, login will be blocked.
- If the machine is not used for a specified period after logging in, the user is forcibly logged out.

Specifying the Policy on Login/Logout

2 Restrict the range of the IP addresses that are allowed to access the machine to block access to the machine from unauthorized computers. Also, specify the unused protocols to reduce the risk of intrusion.

Access Control

2 / **3** Prevent the leak or falsification of information by encrypting communication.

Encrypting Network Communication

Preventing the leak of information by handling files



DZW902

2 Restrict browsing of files stored in the machine or the Address Book to protect the leak of information by unauthorized persons.

Specifying Access Privileges for Documents Saved in Document Server

Specifying Access Privileges on Documents Stored in the Machine

Using the Protection Function to Prevent the Misuse of Addresses

2 Restrict the manual input of the destination to avoid wrong transmission by careless mistake.

Preventing Information Leaks by Sending Data to a Wrong Destination

2 Restrict the connection of external media to avoid the data being removed.

Preventing Information Leaks from the Media Slot

2 / **3** Prevent unauthorized copying or printed paper stolen by embedding a pattern on the printed surface or restricting normal printing.

Preventing Data Leaks from Printed Sheets

2 Prevent the leak of information when the machine is stolen or disposed by encrypting data.

Encrypting Data to Prevent Data Leaks Caused by a Stolen or Disposed Machine

2 Restrict the operation in Service Mode used for maintenance and repair by a customer engineer to prevent the leak of information.

Restricting Operations of the Customer Engineer without the Supervision of the Machine Administrator

Important

- To prevent this machine from being stolen or willfully damaged, install it in a secure location.
- If the security settings are not configured, the data in the machine may be vulnerable to attack.
- To avoid disrupting the work of users, select as administrators who can use the machine proficiently, and then have them supervise the operation of the machine.
- Before setting this machine's security features, the administrators must read the descriptions on security completely and thoroughly. Pay particular attention to the section entitled Registering Standard-Privileges Administrators.
- The 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 security measure.
- For protection of data during communication, 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.

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. For details, see Web Image Monitor Help.

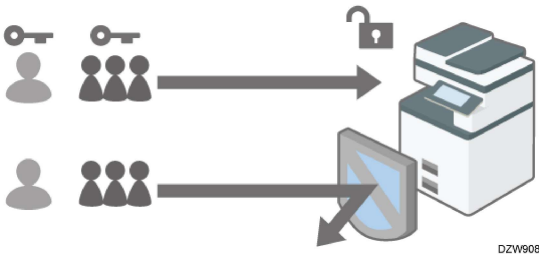
If an error occurs in a verification process of Web Image Monitor, Web Image Monitor cannot be accessed. If this is the case, check the control panel.

When an error occurs in a verification process, contact your service representative.

[Section Top](#)

Verifying Users to Operate the Machine (User Authentication)

"User authentication" is a system to authenticate users and grant them privileges to use the machine. The machine requires entering an arbitrary text, the login user name, or the login password to authenticate a user.



- User authentication prevents unauthorized users from operating the machine and is useful for managing and analyzing usage of the machine regarding the user, operation time, and frequency.

Confirming the Counter for Each User

- You can use the IC card or smart device instead of entering your authentication information on the control panel for user authentication.

Logging in to the Machine Using an IC Card or a Smart Device

User Authentication Method

There are four types of user authentication methods including Basic authentication that limits use of the machine and methods that use an authentication server in the network. Select a method depending on the usage condition or the number of users. You cannot use more than one authentication method at the same time.

User Authentication Method	Explanation
----------------------------	-------------

User Code authentication	Authentication is performed using an up to eight-digit user code registered in the Address Book of the machine. When specifying User Code authentication, the machine prompts you to enter the user code to use the machine. Multiple users can use the same user code. You can activate User Code authentication without activating Administrator Authentication.
Basic authentication	Authentication is performed using the login user name and login password registered in the Address Book on the machine. When specifying Basic authentication, the machine prompts you to enter the login information to use the machine.
Windows authentication	Authentication is performed using the account registered in the Active Directory of the Windows server. When specifying Windows authentication, the machine prompts you to enter the login information to use the machine.
LDAP authentication	Authentication is performed using the user information registered in the LDAP server. When specifying LDAP authentication, the machine prompts you to enter the login information to use the machine.

- In Windows or LDAP authentication, the machine can authenticate you without registering your user information in the machine's Address Book manually, as the user information in the server is registered in the machine automatically.
- In Windows or LDAP authentication, you can manage user information centrally in the server. You can also always use the address provided by the server as the sender (From) of e-mails sent from the machine. These features are useful to avoid data leakage by erroneous input of information or spoofing by an unauthorized user.
- When switching the authentication method from User Code authentication to another method, the user code will be used as the login user name. In this case, the login password is not specified. To avoid unauthorized use, delete unnecessary user information and set up a password for the continuing users.

Note

- If user authentication cannot be performed due to a problem with the machine or network, the machine administrator can disable user authentication temporarily in order to use the machine. Take this measure only during emergencies.
- User authentication can also be activated via Web Image Monitor. For details, see Web Image Monitor Help.

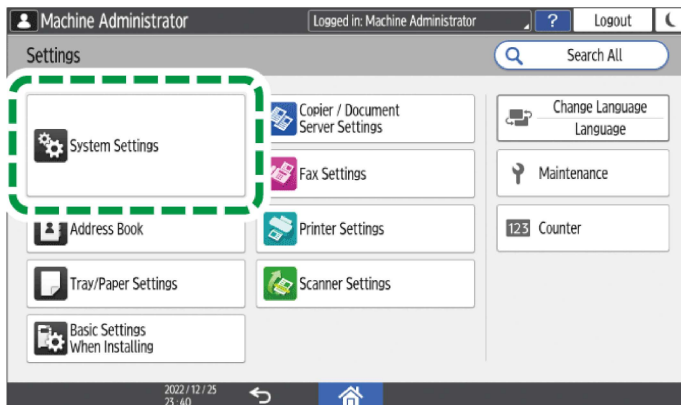
Specify the functions to restrict with User Code authentication.

1. **Log in to the machine as the machine administrator on the control panel.**
Logging in to the Machine as an Administrator

2. **On the Home screen, press [Settings].**

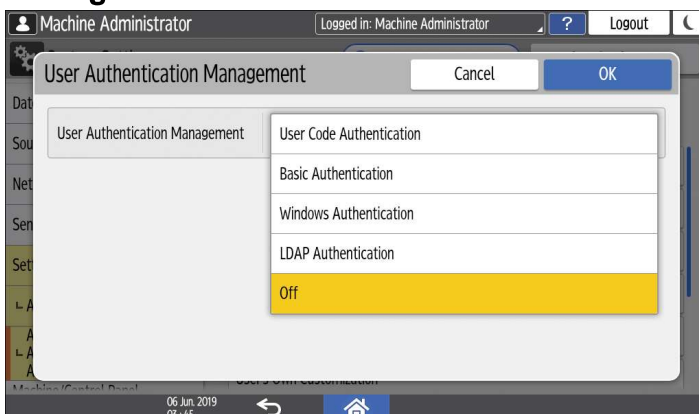


3. **Press [System Settings].**



4. **Press [Settings for Administrator] ► [Authentication/Charge] ► [Administrator Authentication/User Authentication/App Auth.] ► [User Authentication Management].**

5. **Select [User Code Authentication] from the list next to User Authentication Management.**



6. **From Functions to Restrict, select the functions to restrict against use.**

- Specify whether to perform User Code authentication for each function.
- When registering the user code of the printer driver automatically, select [PC Control] for Printer Function. Specify the user code registered in the Address Book to the printer driver.
- When [PC Control] is selected, the user code specified in the printer driver is registered in the Address Book automatically and is excluded from the print volume use limitation. To limit the print volume use, select other than [PC Control] for Print...

Function.

Specifying Maximum Print Volume Use of Each User

For Printer Job Authentication, specify the security level for print jobs using the printer driver.

Executing a Print Job with Authentication Information Only

7. Press [OK].

8. Press [Home] ()

9. **When the confirmation dialog is displayed, press [OK] to log out of the machine.**

If registration of the user information is not completed, register the user in the Address Book and specify the user code.

Registering the User Code in the Address Book

Section Top

Specifying Basic Authentication

Register the default values of the functions available to each user with Basic authentication.

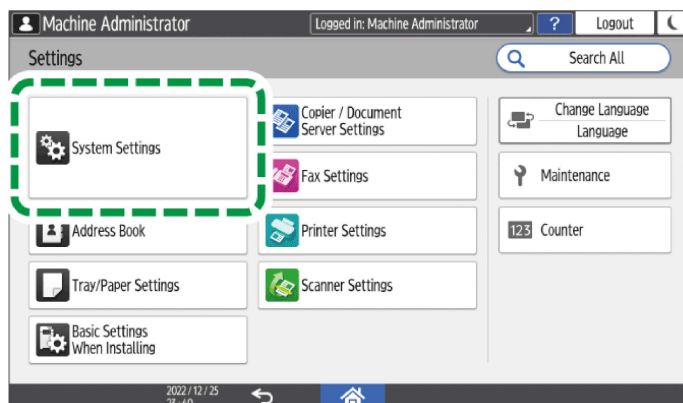
1. **Log in to the machine as the machine administrator on the control panel.**

Logging in to the Machine as an Administrator

2. **On the Home screen, press [Settings].**

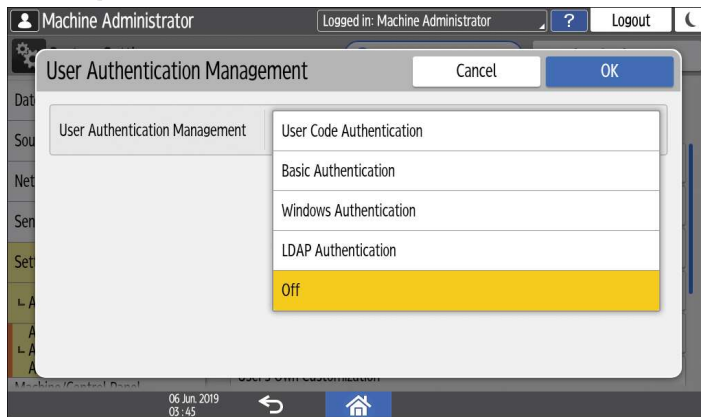


3. **Press [System Settings].**



4. **Press [Settings for Administrator] ► [Authentication/Charge] ► [Administrator Authentication/User Authentication/App Auth.] ► [User Authentication Management].**

5. **Select [Basic Authentication] from the list next to User Authentication Management.**



6. **From Available Functions, select the functions available to the user.**

- Specify the functions available to the user for each function.
- For Printer Job Authentication, specify the security level for print jobs using the printer driver.

Executing a Print Job with Authentication Information Only

7. **Press [OK].**

8. **Press [Home] ().**

9. **When the confirmation dialog is displayed, press [OK] to log out of the machine.**

If registration of the user information is not completed, register the user in the Address Book and specify the login information.

Registering a User in the Address Book and Specifying the Login Information

 Note

- The login user name and login password can be used to authenticate the user in the SMTP or LDAP server, or to authenticate shared folders. Use a login user name other than "other", "admin", "supervisor", or "HIDE****". (Enter an optional character string in "****".) You cannot use these user names for authentication because they are already in use in the machine.

Section Top

Specifying Windows Authentication

Register the Windows server information required for authentication with the Windows server.

 Important

- In advance, check the use conditions in the Windows server, and install the Web server (IIS) and the Active Directory Certificate Service in the Windows server.

Preparing the Server to Use for User Authentication

- To use Kerberos authentication in the server, register the realm in advance to determine the network area.

Registering the Realm

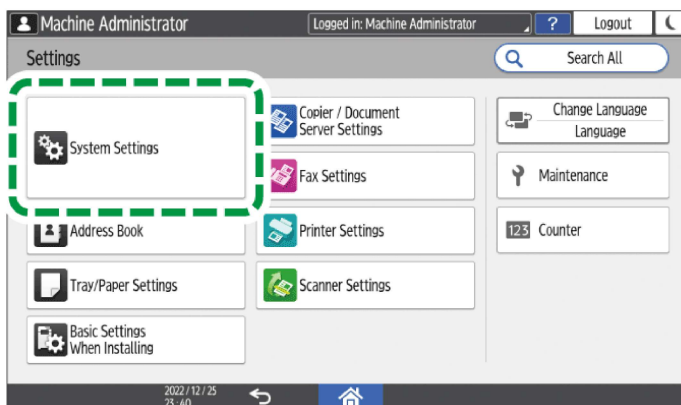
1. Log in to the machine as the machine administrator on the control panel.

Logging in to the Machine as an Administrator

2. On the Home screen, press [Settings].

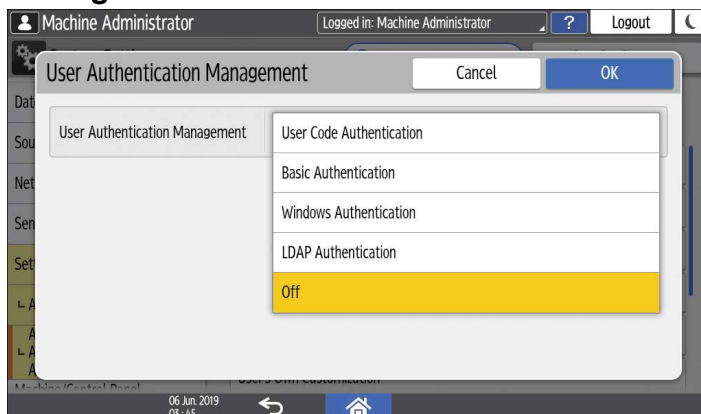


3. Press [System Settings].



4. Press [Settings for Administrator] ► [Authentication/Charge] ► [Administrator Authentication/User Authentication/App Auth.] ► [User Authentication Management].

5. Select [Windows Authentication] from the list next to User Authentication Management.



6. Register the server for authentication and specify the usable functions.

- Kerberos Authentication: To enable Kerberos authentication, select [On].
- Domain Name: To disable Kerberos authentication, enter the domain name to authenticate.
- Realm Name: To enable Kerberos authentication, select the realm name to authenticate.
- Use Secure Connection (SSL): To encrypt communication signals, select [On].

- **Printer Job Authentication:** Specify the security level for print jobs using the printer driver.

Executing a Print Job with Authentication Information Only

- **Group:** If global groups have been registered, you can specify usable functions for each global group. Press [* Not Registered], and then [Register/Change]. Enter the same name of the group as the one registered in the server to specify the available functions.

Users who are registered in multiple groups can use all functions available to those groups.

A user who is not registered in any group can use the authority specified in [* Default Group]. By default, all functions are available to the Default Group members.

For Available Functions, specify the functions available to each group.

7. Press [OK].

8. Press [Home] ().

9. When the confirmation dialog is displayed, press [OK] to log out of the machine.

Note

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

[Section Top](#)

Specifying LDAP Authentication

Register the LDAP server information required for authentication with the LDAP server.

Important

- In advance, check the use conditions in the LDAP server, and register the LDAP server in the machine.

Preparing the Server to Use for User Authentication

Registering the LDAP Server

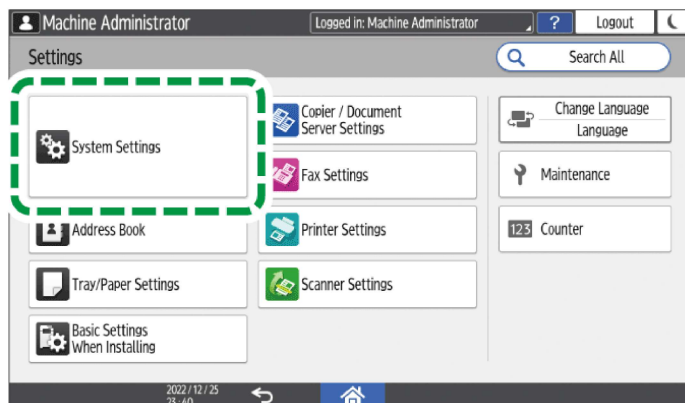
1. Log in to the machine as the machine administrator on the control panel.

Logging in to the Machine as an Administrator

2. On the Home screen, press [Settings].

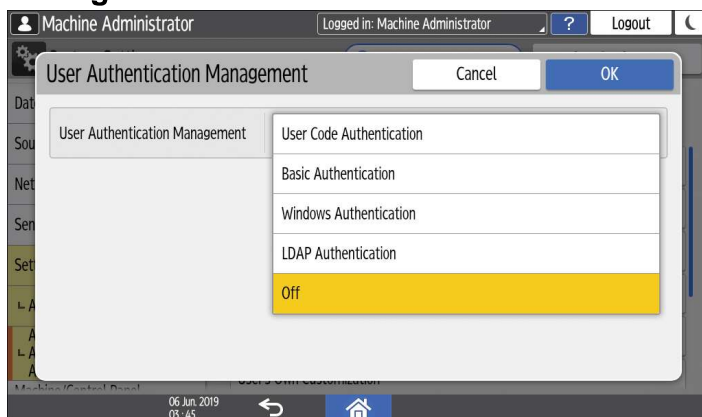


3. Press [System Settings].



4. Press [Settings for Administrator] ► [Authentication/Charge] ► [Administrator Authentication/User Authentication/App Auth.] ► [User Authentication Management].

5. Select [LDAP Authentication] from the list next to User Authentication Management.



6. Select the server for authentication and specify the available functions.

- LDAP Servers: Select the LDAP server to authenticate.
- Login Name Attribute: Use this as a search criterion to obtain user information. Create a search filter based on the login name attribute, select a user, and then retrieve the user information from the LDAP server to transfer to the machine's Address Book.
When separating multiple login attributes with a comma (,), the search will return hits by entering a login name for either or both attributes.
Also, by entering two login names separated by an equal sign (=) (for example: cn=abcde, uid=xyz), the search will return hits only for a match of the attributes of both login names.
This search function can be applied when "Cleartext Authentication" is specified.
- Unique Attribute: Specify this to match the user information in the LDAP server with that in the machine. A user whose unique attribute registered in the LDAP server matches that of a user registered in the machine is treated as the same user in the

machine. Specify the attribute that is used for unique information in the server as the Unique Attribute. You can enter "cn" or "employeeNumber" to use as "serialNumber" or "uid" as long as it is unique.

- Available Functions: Specify the functions available to the user for each function. For Printer Job Authentication, specify the security level for print jobs using the printer driver.

Executing a Print Job with Authentication Information Only

7. Press [OK].

8. Press [Home] ()

9. When the confirmation dialog is displayed, press [OK] to log out of the machine.

Note

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

Section Top

Taking Measures to Prevent Unauthorized Access | Registering/Changing/Deleting User Codes

Page Top