



User Guide - Security Guide

For RICOH IM 550/600/600SR Enhanced Security Firmware series



Author: RICOH COMPANY, LTD.

Date: 2022.07

Part Number: D0BW7263

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.

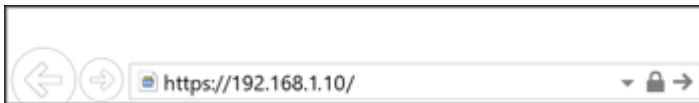
Using Web Image Monitor

Web Image Monitor is a screen to confirm the machine status and settings on the computer.

When the machine and a computer can be connected to a network, you can access to Web Image Monitor by entering the IP address of the machine on the address bar of the Web browser.

Accessing to Web Image Monitor

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



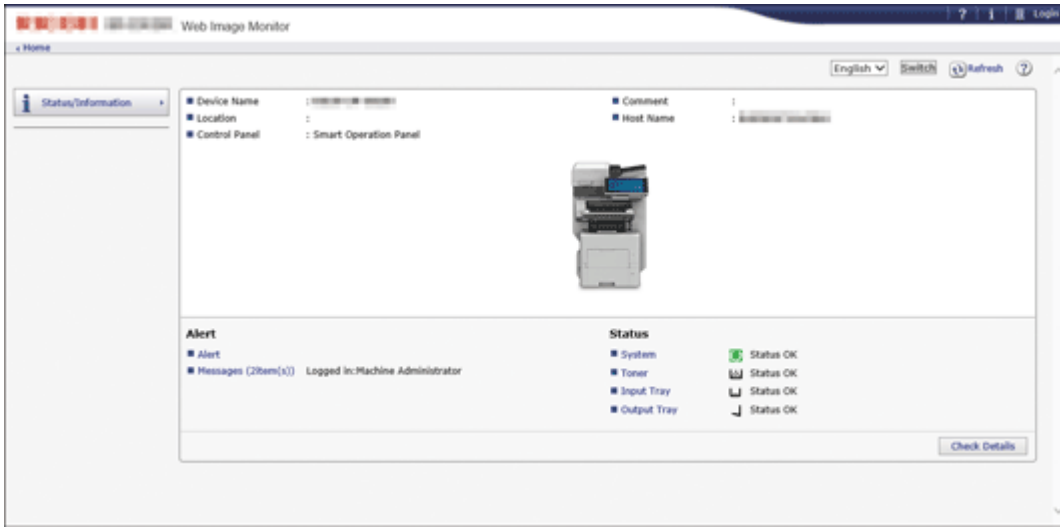
Example: when the IP address of the machine is "192.168.1.10"

- 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.

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

Recommended Web Browser

Windows	OS X/macOS
Internet Explorer 11 or later	Safari 3.0 or later
Firefox 52 or later	Firefox 52 or later
Google Chrome version 50 or later	Google Chrome version 50 or later
Microsoft Edge 20 or later	-

- You can use the screen reader software JAWS 7.0 or later on Internet Explorer.

Note

- When you use a DNS server or WINS server, you can use Host Name instead of IP address to connect the server.
- When the screen is distorted or the operation is unstable, confirm that "JavaScript" or "Use Cookies" is specified to Active on the computer.
- When using Host Name under Windows Server 2008 or later in the IPv6 environment, resolve Host Name in the external DNS server. You cannot use the host file.

- When specifying the settings from Web Image Monitor, do not log in to the machine from the control panel. The setting value may not be reflected.

What You Can Do on the Web Image Monitor

Items displayed on the Web Image Monitor and settings depend whether the machine is logged in.

- When not logged in

The machine status, settings, and job status are displayed. You can browse the settings of the machine but cannot change them.
- When logged in (as a user)

Log in as a user registered in the Address Book. The users can operate the jobs that they executed and change a part of settings of the machine.
- When logged in (as an Administrator)

The administrator can change all settings of the machine.

What you can do

Function	Not logged in	User	Administrator
Machine status	✓	✓	✓
Machine settings	✓ ^{*1}	✓ ^{*1}	✓
Machine setting change	-	✓ ^{*1}	✓
Job list	✓	✓	✓
Job history	✓	✓	✓
Access to Address Book	-	✓	✓
File operation in Document Server	-	✓	✓
Network settings	-	✓ ^{*1}	✓
Network settings change	-	✓ ^{*1}	✓
Cancel printing	-	-	✓

Security settings	-	-	✓
-------------------	---	---	---

✓: Available -: Not available

*1 Depending on the Administrator settings

Web Image Monitor Screen



1. Menu


Menu items described below are displayed.

- Status/Information: Displays the machine status, option configuration, counter, and job status.
- Device Management: Manages the machine settings and Address Book.
- Print Job/Stored File: Operates the files stored in the printer driver or document server.
- Convenient Links: Displays the link to the Favorite URL.

2. Header

An icon to link to the Login screen is placed at the top right on the screen. The Help, Version Information, and Keyword Search buttons are also displayed.

3. Refresh/Help

 (Refresh): Update the information in the work area.

 (Help): View or download Help file contents.

4. Main Area

The machine status and settings are displayed.



Specifying Web Image Monitor Help

Web Image Monitor has Help to describe the function of setting items. When you use Help for the first time, you can select to read online Help or to download Help File.

View Online Help Now

You can view the latest Web Image Monitor Help on the Internet.

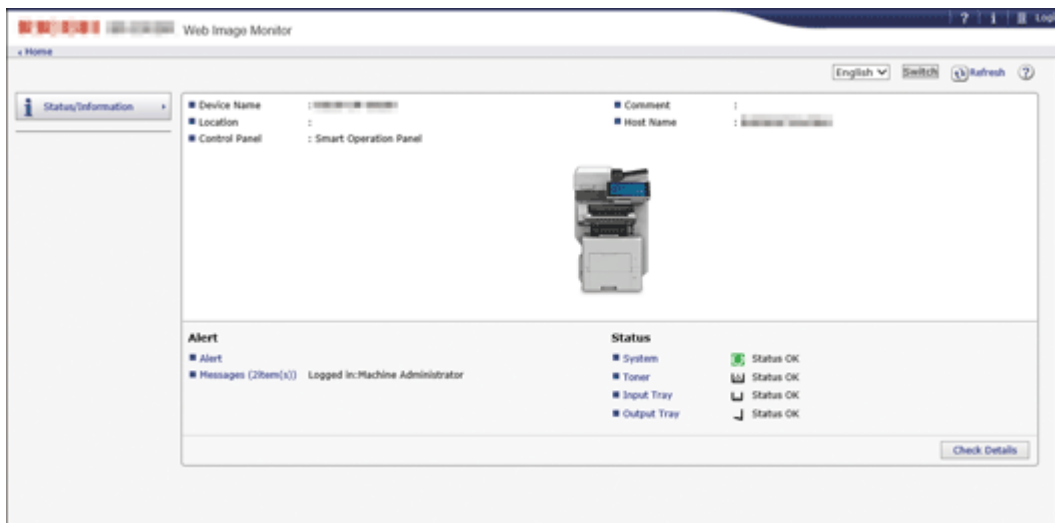
Download Help File

You can download Web Image Monitor Help to the computer and view it. When you store the downloaded Help file in the Web server and assign to the Help button ( ), you can view the Help without connecting to the Internet.

To assign the downloaded Help file to the Help button ( ), specify the path to the Help file following the procedure below.

1 Log in to Web Image Monitor as an Administrator.

2 Click the Help button ( ) at the top right on the screen.



- 3 Select the operating system and displayed language, and then click [Download].**
- 4 Unzip the downloaded zip file and store it in the Web server.**
- 5 Click [Configuration] on the "Device Management" menu on Web Image Monitor.**
- 6 Click [Webpage] under the "Webpage" category.**
- 7 Enter the path to the Help file stored in the Web server in "URL" under "Set Help URL Target".**
For example, when URL of the Help File is "http://a.b.c.d/HELP/JA/index.html", enter "http://a.b.c.d/HELP/".
- 8 Click [OK].**
- 9 After completing the procedure, log out and finish Web Image Monitor.**

[Page Top](#)

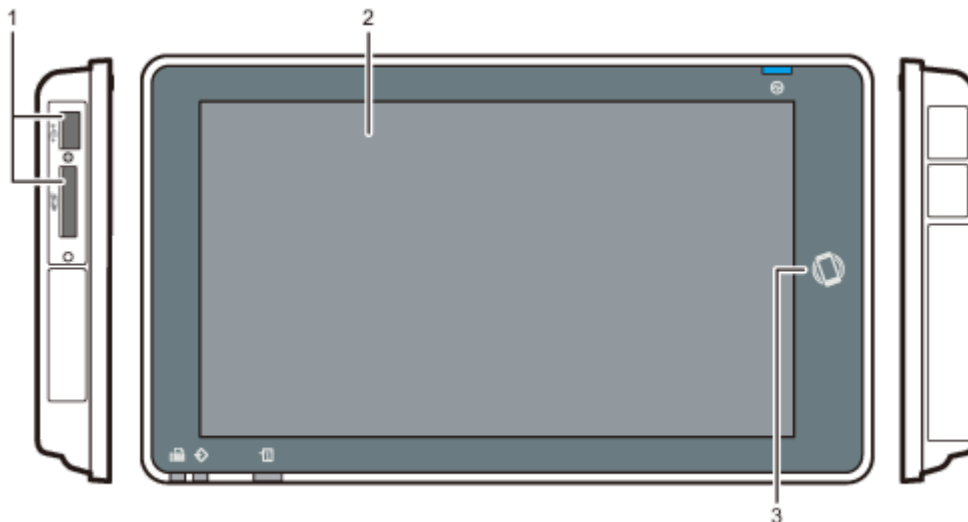
Copyright © 2019, 2020, 2022

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 the left side of the control panel, interfaces for connecting external devices and slots to insert an SD card/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





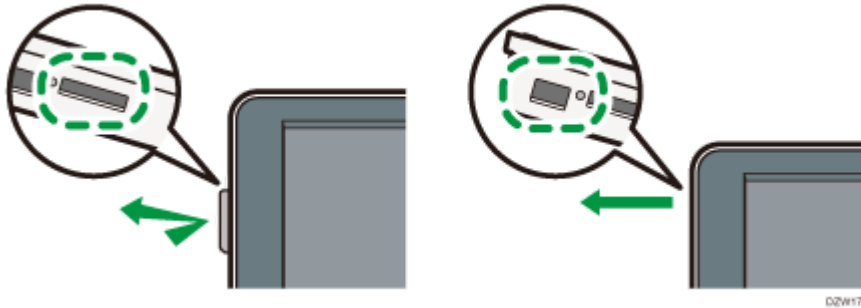
02B195

1. Media slots

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

- Use an SD memory card or SDHC memory card with a maximum capacity of 32 GB. You cannot use an SDXC memory card.
- 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.



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. NFC tag

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

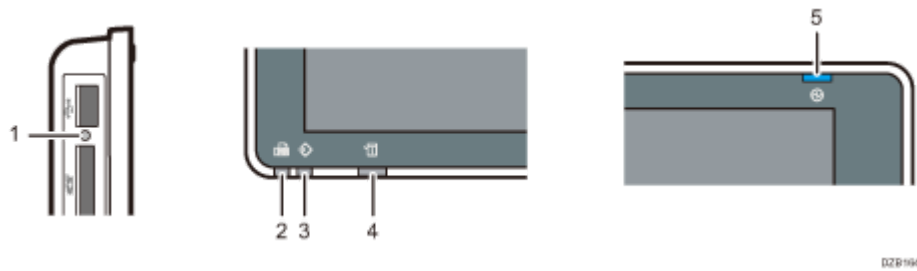
[Using the Machine Functions from a Mobile Device](#)

↓ Note

- You can adjust the angle of the control panel to improve visibility.



LED Indicators



1. Media access indicator

Flashes when data is being read from or written to an SD card

While the machine is accessing the SD card or USB flash memory device, do not turn the power off or remove the media.

2. 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)

3. Data In indicator

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

4. 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](#)

5. Main power indicator

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








[Page Top](#)







Copyright © 2019, 2020, 2022

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	<p>Specify the period and time for daylight saving.</p> <p> Region A (mainly Europe)</p> <ul style="list-style-type: none"> • Default: [Active] <p> Region A (mainly Asia)</p> <ul style="list-style-type: none"> • Default: [Inactive] <p> Region B (mainly North America)</p> <ul style="list-style-type: none"> • Default: [Active]
Daylight Saving Time (Continued)	<ul style="list-style-type: none"> • Start Time/End Time <p>Specify [Month], [Week], [Day of the Week], [Time] to start/end the daylight saving time.</p> <ul style="list-style-type: none"> • Default of [Month] <ul style="list-style-type: none">  Region A (mainly Europe) <ul style="list-style-type: none"> • Start Time: [March] • End Time: [October]  Region B (mainly North America) <ul style="list-style-type: none"> • Start Time: [March] • End Time: [November] • Default of [Week] <ul style="list-style-type: none">  Region A (mainly Europe) <ul style="list-style-type: none"> • Start Time: (Final week) • End Time: (Final week)  Region B (mainly North America)

	<ul style="list-style-type: none"> • Start Time: [2nd] • End Time: [1st] • Default of [Day of the Week]: [Sunday] • Default of [Time]  Region A (mainly Europe) <ul style="list-style-type: none"> • Start Time: [0] • End Time: [1]  Region B (mainly North America) <ul style="list-style-type: none"> • Start Time: [2] • End Time: [2] • Offset <p>Specify the amount of time to move the clock forward for the daylight saving time.</p> <ul style="list-style-type: none"> • Default: [1] hour(s) [0] minute(s)
<p>Set Date</p> <p>Set Time</p>	<p>Set the date and time for the machine's internal clock.</p> <p>  Region A (mainly Europe and Asia) Enter the time using the 24-hour format. </p> <p>  Region B (mainly North America) Enter the time using the 12-hour format. </p>
Time Zone	<p>Specify the standard time in the region where the machine is used.</p> <p>  Region A (mainly Europe and Asia) <ul style="list-style-type: none"> • Default: [GMT+01:00] </p> <p>  Region B (mainly North America) <ul style="list-style-type: none"> • Default: [GMT-05:00] </p>

Timer

Setting Items	Description
Sleep Mode Timer	<p>Specify the time to wait before entering Sleep mode for power saving.</p> <p>If the machine is left unused for a certain period of time, it first enters low-power mode and eventually enters Sleep</p>

	<p>mode.</p> <ul style="list-style-type: none"> • Default: [1] minute(s)
Low Power Mode Timer	<p>Specify the time to wait before entering low-power mode for power saving.</p> <p>If the machine is left unused for a certain period of time, it first enters low-power mode and eventually enters Sleep mode.</p> <ul style="list-style-type: none"> • Default: [Off]
System Auto Reset Timer	<p>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].</p> <ul style="list-style-type: none"> • Default: [On], [60] second(s)
<p>Copier/Document Server Auto Reset Timer</p> <p>Fax Auto Reset Timer</p> <p>Printer Auto Reset Timer</p> <p>Scanner Auto Reset Timer</p>	<p>Specify the time to elapse before the function is reset when no operations are in progress for a certain period.</p> <ul style="list-style-type: none"> • Default <ul style="list-style-type: none"> • Copier/Document Server, Printer, Scanner: [On], [60] second(s) • Fax: [30] second(s)
Auto Logout Timer	<p>Specify the time to automatically log out when no operations are in progress for certain period.</p> <ul style="list-style-type: none"> • Default: [On], [180] second(s)
System Status/Job List Display Time	<p>Specify whether to hide the screen displayed by pressing [Check Status] automatically. You can specify the display time.</p> <ul style="list-style-type: none"> • Default: [On], [15] second(s)
Weekly Timer Detailed Settings	<p>Specify whether to activate or inactivate the weekly timer.</p> <ul style="list-style-type: none"> • Default: [Inactive] <p>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.</p> <p>You can set up to six timer settings a day or for Monday through Sunday and specify the following items:</p> <ul style="list-style-type: none"> • Weekly Timer Code Settings <p>Specify whether to enable the weekly timer code. When you enable the code, specify a password (up to</p>

	<p>eight digits) for when the machine recovers from Off mode or Sleep mode.</p> <ul style="list-style-type: none"> Weekly Timer Schedule <p>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.</p> <p> Region A (mainly Europe and Asia)</p> <p>Enter the time using the 24-hour format.</p> <p> Region B (mainly North America)</p> <p>Enter the time using the 12-hour format.</p>
<p>Weekly Timer Detailed Settings (Continued)</p>	<ul style="list-style-type: none"> Main Power On Timer Suspension Period <p>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.</p> <p>To use this setting, activate the Administrator Authentication.</p> <p>Registering Administrators Before Using the Machine</p>
<p>Weekly Timer Easy Settings</p>	<p>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] changes to "Active" and the setting overwrites the schedule of the selected day.</p> <p> Region A (mainly Europe and Asia)</p> <p>Enter the time using the 24-hour format.</p> <p> Region B (mainly North America)</p> <p>Enter the time using the 12-hour format.</p> <p>To use this setting, activate the Administrator Authentication.</p> <p>Registering Administrators Before Using the Machine</p>

[Page Top](#)

Copyright © 2019, 2020, 2022

Specifying Access Privileges for Documents Stored in Document Server

RICOH Always Current Technology updates this function. For details, see [List of Newly Added Functions \(Release Notes\)](#).

You can specify access privileges (authority to read or edit a document) for documents stored 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.

- The user who stored the document or the document administrator can specify the access privileges. Access privileges can be granted to the users registered in the address book.
- You must specify user authentication on the machine in advance. To protect a document when user authentication is not specified, specify a password on the document when storing.

[Viewing and Editing the Information of Documents in Document Server](#)

Note

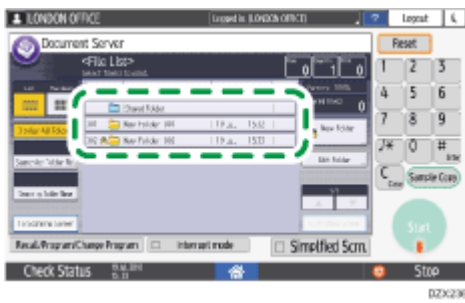
- Access privileges to stored print documents sent from the printer driver and stored on the machine can only be specified in Web Image Monitor.

[Specifying Access Privileges for Documents Stored in the Machine](#)

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



2 On the document server screen, select the desired folder.



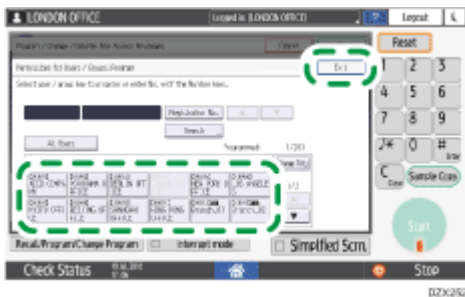
3 Select the document to specify the access privileges, and then press [Change File Info.].

4 Press [Change Access Priv.].

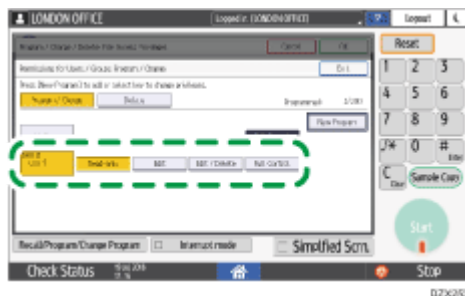
5 Press [Program/Change/Delete] of "Permissions for Users/Groups".

6 Press [New Program].

7 Select the user to receive access privileges, and then press [Exit].



8 Select the user and specify the access privileges.



The contents of the access privileges are as follows:

- 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 **[Exit]** ► **[OK]** ► **[OK]**.



- To cancel the Access Privileges, press [Delete] after performing Step 5 to select the user, and then press [Yes].

[Page Top](#)

Copyright © 2019, 2020, 2022

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	<p>Specify whether to display in gray tone when scanning the original with the data security for copying in the Copy or Scanner function or storing it in the document server.</p> <ul style="list-style-type: none"> • Default: [Off]
Unauthorized Copy Prevention Printing: Copier Unauthorized Copy Prevention Printing: Document Server Unauthorized Copy Prevention Printing: Printer	<p>Specify whether to use the Data Security for Copying or Unauthorized Copy Prevention for Pattern for each function when printing on the machine.</p> <p>[Data Security for Copying] is to cover images in the document with gray overprint when the printed document is scanned or stored in the document server using a Copier or MFP with the optional Data Security for Copying module installed.</p> <p>[Unauthorized Copy Prevention for Pattern] is to print a text pattern on the background of the document to prevent illegal copying. When you scan or store the printed document, the embedded text and pattern appear on the copied pages for preventing unauthorized copy. You can specify the text, font, size, angle, position, and pattern to embed.</p>

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. Available stamps are Date/Time, Printout User Name, Machine ID, and Machine IP Address. You can adjust the stamp position.

- Default: **[Off]**

Data Management

Setting Items	Description
Auto Erase Memory Setting	Specify whether to erase files printed on the printer driver or image of the scanned original for each job automatically. <ul style="list-style-type: none"> • Default: [Off] Encrypting Data to Prevent Data Leaks Caused by a Stolen or Disposed Machine
Erase All Memory	Delete all data stored in the machine.
Delete All Logs	Delete all logs stored in the machine.
Transfer Log Setting	This is a user tool 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].
Collect Logs Settings	Specify whether to activate the collection of Job Log, Access Log, and Eco-friendly Logs. <ul style="list-style-type: none"> • Default: [Inactive]
Job Execution Restrictions When Log Limit is Reached (This setting item is available on machines with RICOH Always Current Technology v1.2 or later installed.)	Specify whether to display a message on the control panel and send an e-mail to the administrator when the job log storage area is almost full. The machine will not accept any new jobs until the job log storage area has sufficient space. <ul style="list-style-type: none"> • Default: [Off]
Device Setting Information: Export (Memory Storage Device) Device Setting Information: Import (Memory Storage Device)	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.

Device Setting Information: Import Setting (Server) Device Setting Information: Run Import (Server)	
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.

File Management

Setting Items	Description
Machine Data Encryption Settings	Specify whether to encrypt the Address Book, Authentication Information, and Store Files stored in the machine. Encrypting Data to Prevent Data Leaks Caused by a Stolen or Disposed Machine
Auto Delete File in Document Server	Specify whether to delete the files stored the Document Server automatically. To delete the stored files automatically, specify a number of days and hours to delete after they are stored. <ul style="list-style-type: none"> Default: [Specify Days], [3] day(s) Changing the Storage Period of Document Server or Specifying an Indefinite Period
Delete All Files in Document Server	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. <ul style="list-style-type: none"> Default: [On]
Default Privilege for Stored File	Specify the default settings of the access privileges for the files stored in the document server. <ul style="list-style-type: none"> Default: [Read-only] Specifying Access Privileges for Documents Saved in Document Server

PDF File Type: PDF/A Fixed	<p>Specify the PDF file format to PDF/A only that can be stored for a long time.</p> <ul style="list-style-type: none"> • Default: [Off]
----------------------------	--

Security


Setting Items	Description
Extended Security Settings	<p>Specify to encrypt transmitted data of the machine and data in the Address Book.</p> <p>For details, see "Specifying the Extended Security Functions" in this section.</p>
Service Mode Lock	<p>Specify whether to lock the machine changing to Service Mode when a customer engineer performs maintenance and repair.</p> <ul style="list-style-type: none"> • Default: [Off] <p>Restricting Operations of the Customer Engineer without the Supervision of the Machine Administrator</p>
Network Security Level	<p>Specify the level of the Network Security and adjust the security level. You can select [Level 0], [Level 1], [Level 2], [FIPS140], or [Custom].</p> <p>Access Control</p>
Access Control Function	<p>Specify whether to enable the function to permit the communication within the specified range of the IP addresses (Access Control).</p> <ul style="list-style-type: none"> • Default: [Inactive] <p>Access Control</p>
Register/Delete Device Certificate	<p>Program or delete a device certificate.</p> <p>Encrypting Network Communication</p>
HDD Authentication Code	<p>Enter the Authentication code of the hard disk of the machine within the range of 8 to 32 characters.</p> <p>Changing the HDD Authentication Code (Settings Screen Type: Standard)</p>

<p>CCC: Save Standard Values</p> <p>CCC: Apply Standard Values</p>	<p>Store or reflect the Device Settings (reference value) for the International Evaluation Regulations for Information Security (CC Authentication) in the hard disk of the machine.</p> <p>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.</p>
Credential Storage	<ul style="list-style-type: none"> System (certificate system installed) Displays the contents of certificates installed in the system. Specify whether to use these certificates. User (certificate installed from SD card) Install certificates from an SD card. You can install up to 10 certificates. Delete All Certificates Deletes all contents of the installed certificates.
Server Settings	<p>Specify whether to enable the server function for operating the Web application. You can install a server certificate for SSL communication.</p> <ul style="list-style-type: none"> Default: [Active]
Install Settings	<p>Specify whether to allow installation of the application with the SHA-1 signature.</p>

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 user tool.

Setting Items	Description
<p>Driver Encryption Key (Permissions: Network Administrator)</p>	<p>Specify a text string to decrypt login passwords or file passwords sent from each driver when user authentication is specified to ON.</p> <p>Register the encryption key specified using the machine in the driver.</p>
<p>Driver Encryption Key: Encryption Strength</p>	<p>Specify encryption strength for sending jobs from the driver to the machine. The machine confirms the</p>

<p>(Permissions: Network Administrator)</p>	<p>encryption strength of the password appended to a job and processes it.</p> <ul style="list-style-type: none"> • All jobs that are verified by [Simple Encryption] or user authentication are accepted. • [DES] Jobs encrypted with DES or AES are accepted. • [AES] Jobs encrypted with AES are accepted. <p>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.</p> <ul style="list-style-type: none"> • Default: [Simple Encryption]
<p>Restrict Display of User Information (Permissions: Machine Administrator)</p>	<p>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 "*****".</p> <ul style="list-style-type: none"> • Default: [Off]
<p>Enhance File Protection (Permissions: File Administrator)</p>	<p>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.</p> <p>If the Enhance File Protection function is specified, the icon () appears at the bottom left of the screen.</p> <p>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.</p> <ul style="list-style-type: none"> • Default: [Off]
<p>Restrict Use of Destinations (Fax) Restrict Use of Destinations (Scanner) (Permissions: User Administrator)</p>	<p>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.</p> <p>When you specify the setting to receive e-mails via SMTP using the Fax function, you cannot use this function.</p> <ul style="list-style-type: none"> • Default: [Off]
<p>Restrict Adding of User Destinations (Fax) Restrict Adding of User Destinations (Scanner)</p>	<p>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.</p>

(Permissions: User Administrator)	<ul style="list-style-type: none"> • Default: [Off]
Transfer to Fax Receiver (Permissions: Machine Administrator)	<p>Specify whether to prohibit the use of forwarding or transferring function of the Fax function.</p> <ul style="list-style-type: none"> • Default: [Do not Prohibit] <p>Transferring Received Fax Documents to Another Fax Destination</p>
Authenticate Current Job (Permissions: Machine Administrator)	<p>This is a user tool when Basic Authentication, Windows Authentication, or LDAP Authentication is used. Specify whether authentication is required for operations such as interrupting jobs under the Copy function or canceling jobs under Printer functions.</p> <p>When you specify [Login Privilege], authorized users who have the privilege to use the current function can operate the job.</p> <p>When you specify [Access Privilege], users who execute the job and the machine administrator can operate the job.</p> <ul style="list-style-type: none"> • Default: [Off]
@Remote Service (Permissions: Machine Administrator)	<p>Specify how to use the @Remote Service.</p> <p>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.</p> <ul style="list-style-type: none"> • Default: [Do not Prohibit]
Update Firmware (Permissions: Machine Administrator)	<p>Specify whether to prohibit firmware updates on the machine by a service representative or via the network.</p> <ul style="list-style-type: none"> • Default: [Do not Prohibit]
Change Firmware Structure (Permissions: Machine Administrator)	<p>Specify whether to prevent changes in the machine's firmware structure without confirmation by a machine administrator.</p> <p>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.</p> <ul style="list-style-type: none"> • Default: [Do not Prohibit]
Password Policy (Permissions: User Administrator)	<p>When Basic authentication is used, specify whether to limit the text and the number of characters for users' passwords.</p>

	<p>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.</p> <ul style="list-style-type: none"> • Upper-case letters, lower-case letters, decimal numbers, and symbols such as # <p>You can specify passwords that meet the conditions specified in complexity and minimum character number.</p> <ul style="list-style-type: none"> • Default <ul style="list-style-type: none"> • Complexity Setting: [Off] • Minimum Number of Characters: [0] characters
<p>Settings by SNMPv1, v2 (Permissions: Network Administrator)</p>	<p>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.</p> <ul style="list-style-type: none"> • Default: [Do not Prohibit]
<p>Password Entry Violation (Permissions: Machine Administrator)</p>	<p>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.</p> <p>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.</p> <ul style="list-style-type: none"> • Default <ul style="list-style-type: none"> • Maximum Allowed Number of Access: [30] time(s) • Measurement Time: [5] second(s) <p>If you receive violation detection e-mails frequently, check the content and review the setting values.</p>
<p>Device Access Violation (Permissions: Machine Administrator)</p>	<p>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,</p>

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).

- 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]**

If you receive violation detection e-mails frequently, check the content and review the setting values.

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]**

Remote Panel Operation

Setting Items	Description
Remote Operation/Monitoring	Specify whether to activate the Remote Operation/Monitoring function. <ul style="list-style-type: none"> Default: [Inactive]
Remote Connection Timeout	Specify the remote connection timeout period. <ul style="list-style-type: none"> Default: [30] minute(s)

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.
Restrict Functions of Each Application	Specify whether to restrict the Copy, Document Server, Scanner, and Printer functions. For the Scanner function, you can also specify the following items: <ul style="list-style-type: none"> Color Scan Mode Limitation Sending Method

Authentication/Charge

Administrator Authentication/User Authentication/App Auth.

Setting Items	Description
Administrator Authentication Management Register/Change Administrator	<p>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.</p> <p>You can manage four categories; user management, machine management, network management, and file management.</p> <p>Registering Administrators Before Using the Machine</p>
User Authentication Management	<p>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.</p> <p>You can select [User Code Authentication], [Basic Authentication], [Windows Authentication], or [LDAP Authentication].</p> <ul style="list-style-type: none"> • Default: [Off] <p>Verifying Users to Operate the Machine (User Authentication)</p>
Setting for Entering Authentication Password	<p>Specify whether to allow double-byte characters to be used for passwords.</p> <ul style="list-style-type: none"> • Default: [Only 1 Byte Characters]
Application Authentication Management	<p>This is a user tool when the authentication is set to On under [User Authentication Management]. Specify the authentication for each application.</p> <ul style="list-style-type: none"> • Default: [On]
Application Authentication Settings	<p>Specify the available application for each user. You can specify to inhibit the use of all applications related to Copy or to use only a part of application related to Copy.</p>
User's Own Customization	<p>Specify whether to store the layout of Home screen or Application screen and the displayed language for each login user.</p> <ul style="list-style-type: none"> • Default: [Prohibit]
Register/Change/Delete Realm	<p>Program the realm to be used for Kerberos authentication. Be sure to specify both the "Realm</p>

	Name" and "KDC Server Name" when programming a realm.
Register/Change/Delete LDAP Server	You can register up to five settings for the LDAP Server.
LDAP Search	<ul style="list-style-type: none"> LDAP Search Specify whether to use the LDAP server for searching destinations or users. <ul style="list-style-type: none"> Default: [Off] Follow Referrals on LDAP Server Specify whether to conform to the referral of the connected LDAP server when performing a LDAP search. This setting item is available on machines with RICOH Always Current Technology v1.2 or later installed. <ul style="list-style-type: none"> Default: [Inactive]

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. <ul style="list-style-type: none"> Default: [Allow Continue Use]
Volume Use Counter: Scheduled/Specified Reset Settings	Specify whether to reset the Volume Use Counter periodically. <ul style="list-style-type: none"> Default: [Do not Specify]
Print Volume Use Limitation: Default Limit Value	Specify the limit value of the Print Volume Use.
Print Volume Use Limitation: Unit Count Setting	Specify the function and count to limit the print volume use.
Enhanced Print Volume Use Limitation	This is a user tool to limit the maximum print volume use using the SDK application. You can specify the following two items:

- Whether to notify the tracking information from the machine to the SDK application
- Whether to stop printing using the SDK application
- Default: **[Off]**

External Charge Unit Management

Setting Items	Description
External Charge Unit Management	Specify whether to limit the user for each function with the key card.
Enhanced External Charge Unit Management	Specify the external charge unit used with the SDK application.

Switch Screen Type

Setting Items	Description
Switch Screen Type	<p>Select the screen layout of the "Settings" screen from [Classic] or [Standard]. The same setting items can be specified on both screen types.</p> <ul style="list-style-type: none"> • Default: [Standard]


[Page Top](#)

Copyright © 2019, 2020, 2022

Reception Settings

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

[How to Use the "Settings"](#)

Setting Items	Description
Reception File Settings	<p>Specify the output method of the received document.</p> <ul style="list-style-type: none"> • Store: Store documents on the hard disk drive of the machine <ul style="list-style-type: none"> • Default: [Off] • Forwarding: Forward the document to a pre-registered destination <ul style="list-style-type: none"> • Default: [Off] • Print: Print the document automatically <ul style="list-style-type: none"> • Default: [On] • Output Mode Switch Timer: Specify the output method of documents received during the specified time period from Print, ID Required Print, Forwarding, or Store. • Prohibit Auto Print: Store the document as a standby to print document without printing it automatically • Print Standby to Print Files: Select this to print a standby to print document designated by [Output Mode Switch Timer] and [Prohibit Auto Print]. • Memory Lock Reception: Perform Memory Lock Reception that requires entering the Memory Lock ID to print <ul style="list-style-type: none"> • Default: [Off] <p> Note</p> <ul style="list-style-type: none"> • When [Standard] is selected as the setting screen type on a device installed with RICOH Always Current Technology v1.1 or later, you can also use the Reception File Storage Location function. <p style="text-align: center;">Reception Settings (Standard)</p>
Switch Reception Mode	<p>Select whether to receive an incoming fax automatically or manually depending on the fax usage.</p> <ul style="list-style-type: none"> • Default: [Auto Reception]
Program Special Sender	<p>Register senders to specify the reception setting. You can specify a different setting for each sender.</p>

	<ul style="list-style-type: none"> • Authorized Reception per Sender: Select this to limit the sender of the incoming fax to receive. • Reception File Print Quantity per Sender: Select this to specify the number of copies to print a received fax from the specified sender. • Forwarding per Sender: Select this to specify the forwarding destination for each specified sender. • Print 2 Sided per Sender: Select this to print a received fax from the specified sender on both sides of the output paper. • Memory Lock Reception per Sender: Select this to apply Memory Lock Reception on the document received from the specified sender. • Paper Tray per Sender: Select this to specify the paper tray to print the document received from the specified sender. • Remote Reception Setting per Sender: Select this to transfer the document received from the specified sender to a pre-registered destination when the Remote Fax function is enabled.
Program Special Sender: Print List	<p>Select this to print the list of special senders.</p> <p>Specifying the Action to Perform When Receiving a Fax from Different Senders</p>
Stored Reception File User Setting	<p>Specify the user to manage the received documents stored on the hard disk drive (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.</p> <ul style="list-style-type: none"> • Default: [Off]
SMTP RX File Delivery Settings	<p>Select whether to deliver e-mails received by SMTP.</p> <ul style="list-style-type: none"> • Default: [Off] <p>Delivering E-mails Received via SMTP to Another Fax Destination</p>
2 Sided Print Checkered Mark Center Mark	<p>Configure the following functions:</p> <ul style="list-style-type: none"> • Print the received document on both sides of paper • Print a checkered mark or center mark on the output sheets of the received document • Default <ul style="list-style-type: none"> • 2 Sided Print: [Off] • Checkered Mark, Center Mark: [On] <p>Printing a Mark or Information on the Received Fax</p>
Print Reception Time	<p>Select whether to print the reception date and time in the bottom margin of the output sheet.</p>

	<ul style="list-style-type: none"> • Default: [Off]
Reception File Print Quantity	<p>Specify the number of copies of the received document to print.</p> <ul style="list-style-type: none"> • Default: [1]
Paper Tray	<p>Specify the paper source for printing the received documents. A paper tray is not specified when [Auto Select] is selected.</p> <ul style="list-style-type: none"> • Default: [Auto Select]
Specify Tray for Lines	<p>Select whether to specify a tray to eject the printed sheets of the received document per line type and sender (telephone line, Internet Fax, or IP-Fax).</p> <ul style="list-style-type: none"> • Default: [Off]
Folder Transfer Result Report	<p>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.</p> <ul style="list-style-type: none"> • Default: [Do not Email]
Remote Reception Setting per Line	<p>Select whether to print documents received on the main machine from a sub-machine when using the Remote Fax function. You can specify the sub-machine per reception line.</p>
Maximum Reception Size	<p>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 reducing it automatically.</p> <ul style="list-style-type: none"> • Default: [A4]
Trays for Paper Tray Selection	<p>Specify the tray to be used with the Fax function.</p> <ul style="list-style-type: none"> • Default: [On]

[Page Top](#)

Copyright © 2019, 2020, 2022

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.

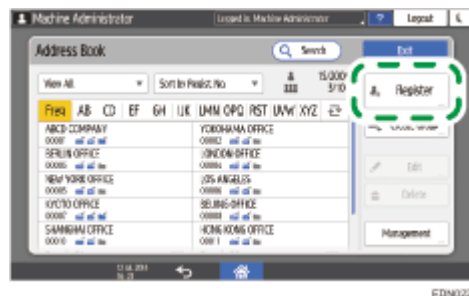
Note

- 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.

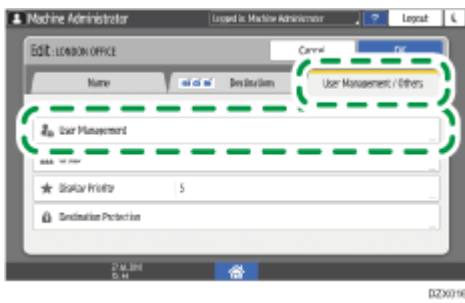


2 On the Address Book screen, press [Register] and enter the user name.



The items displayed on the screen vary depending on the version of RICOH Always Current Technology that is implemented on the machine.

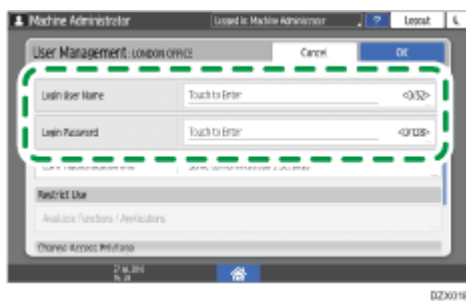
3 Press the [User Management / Others] tab ► [User Management].



4 Enter the login information.

For Basic Authentication

1. Enter the Login User Name and Login Password.



For LDAP Authentication

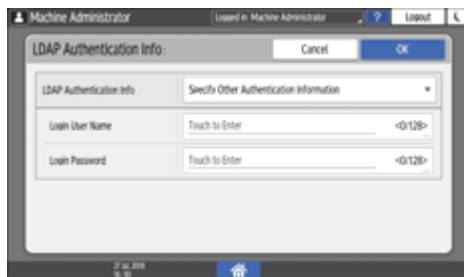
1. Press [LDAP Authentication Info].



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.

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

When you select [Specify Other Authentication Information] in "SMTP Authentication Info", the setting of [Program / Change / Delete LDAP Server] in the [System] tab ► [Administrator Tools] tab is enabled.



3. Press [OK].

5 Press [OK].

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

[Page Top](#)

Copyright © 2019, 2020, 2022

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.












D2C702

- **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.
	Paper is jammed.	See the animated illustration displayed on the control panel, and remove the jammed paper. When Paper or an Original Is Jammed
	An original has jammed.	See the animated illustration displayed on the control panel, and remove the jammed original. When Paper or an Original Is Jammed
	Paper has run out.	Load paper into the paper tray. Loading Paper into the Paper Tray
	Toner is almost depleted, or has run out.	Prepare a replacement toner. Replace the toner when it runs out. Replacing the Toner Note <ul style="list-style-type: none">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
	Staples have run out.	Prepare a cartridge for replacement, and load it when the staples run out. Replenishing the Staples (only for IM 600SRF)
	A cover is open.	Check that all covers of the machine and options are closed.

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.



- 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].

[Page Top](#)

Copyright © 2019, 2020, 2022

When a Message Appears and the Machine Cannot Be Operated

Message	Condition	Solution and reference
<p>“Service Call”</p> <p>SCxxx-xx</p> <p>Contact</p> <p>Serial No. of Machine</p>	<p>The machine needs to be repaired.</p>	<p>Consider repairing the machine.</p>
<p>“Functional Problems”</p> <p>SCxxx-xx</p> <p>Contact</p> <p>Serial No. of Machine</p>	<p>A malfunction that requires maintenance or repair has occurred.</p>	<p>Prepare for maintenance or consider repairing the machine.</p> <ul style="list-style-type: none"> 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. <p>Turning On and Off the Power</p> <ul style="list-style-type: none"> When “Press [Cancel] to cancel mode” is displayed, you can continue using the machine except for the function in which the malfunction is occurring after pressing [Cancel].
<p>“Please wait.”</p>	<p>The machine is recovering from the sleep mode.</p>	<p>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.</p> <p>Turning On and Off the Power</p>

“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.	<p>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.</p> <p>Installation Requirements After Moving the Machine</p> <p>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.</p> <p>Turning On and Off the Power</p>
“Please wait.”	A consumable or supply such as the toner has been replenished.	<p>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. If the message remains displayed for more than 5 minutes, consult your service representative.</p> <p>Turning On and Off the Power</p>
“Shutting down... Please wait. Main power will be turned off automatically. Maximum waiting time: four 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.

 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.

[Turning On and Off the Power](#)

- “Cover Open”
- “Add Toner”/“Add Staples”

- “Replace Waste Toner Bottle”
- “Original left on exposure glass.”
- “No paper”

[Page Top](#)

Copyright © 2019, 2020, 2022

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.

[Using 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].**



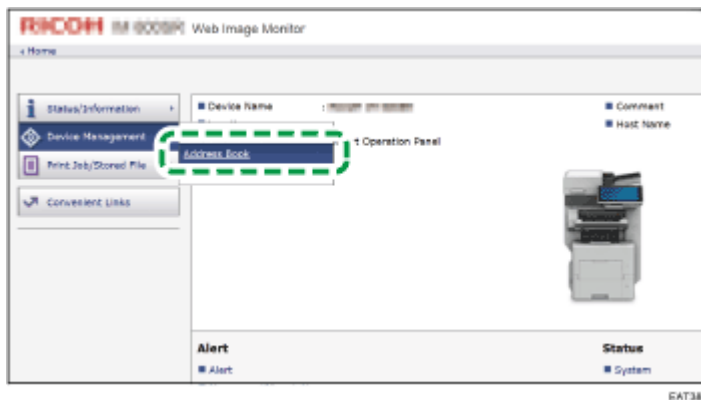
- 4 Enter the login user name and password, and then click [Login].**



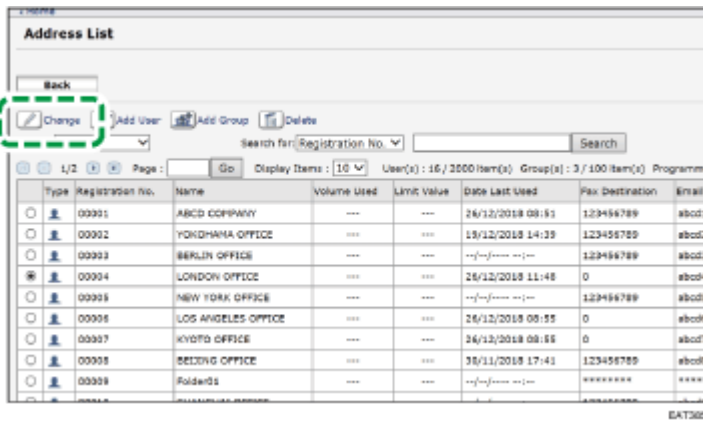
- Ask the administrator for the Login user name and Login password.

Changing the Login Password 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.**
- 3 Click [Login].**
- 4 Enter the login user name and password, and then click [Login].**
- 5 Click [Address Book] from the [Device Management] menu.**



- 6 Select the user for whom to change the login password.**
- 7 Click [Change].**



Address List

Back Change Add User Add Group Delete

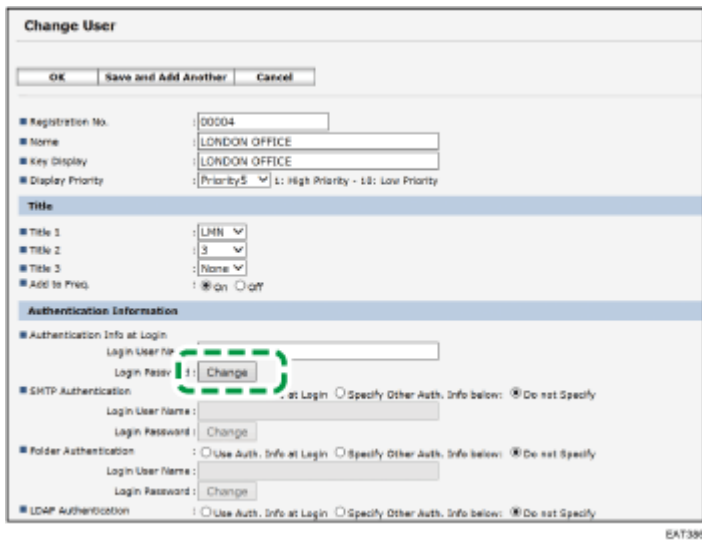
Search for: Registration No. Search

1/2 Page: Go Display Items: 10 User(s): 16 / 2000 Item(s) Group(s): 3 / 100 Item(s) Programs

Type	Registration No.	Name	Volume Used	Limit Value	Date Last Used	Fax Destination	Email
<input type="radio"/>	00001	ABCD COMPANY	---	---	26/12/2018 09:51	123456789	abcd1
<input type="radio"/>	00002	YOKOHAMA OFFICE	---	---	19/12/2018 14:39	123456789	abcd2
<input type="radio"/>	00003	BERLIN OFFICE	---	---	--/--/-- --:--	123456789	abcd3
<input checked="" type="radio"/>	00004	LONDON OFFICE	---	---	26/12/2018 11:48	0	abcd4
<input type="radio"/>	00005	NEW YORK OFFICE	---	---	--/--/-- --:--	123456789	abcd5
<input type="radio"/>	00006	LOS ANGELES OFFICE	---	---	26/12/2018 09:55	0	abcd6
<input type="radio"/>	00007	KYOTO OFFICE	---	---	26/12/2018 09:55	0	abcd7
<input type="radio"/>	00008	BEIJING OFFICE	---	---	30/11/2018 17:41	123456789	abcd8
<input type="radio"/>	00009	Folders	---	---	--/--/-- --:--	*****	****

EAT365

8 Click [Change] in "Login Password" of "Authentication Information".



Change User

OK Save and Add Another Cancel

Registration No.: 00004
 Name: LONDON OFFICE
 Key Display: LONDON OFFICE
 Display Priority: Priority 5 (High Priority - 10: Low Priority)

Title

Title 1: LHM
 Title 2: 3
 Title 3: None
 Add to Priv: on off

Authentication Information

Authentication Info at Login:
 Login User Name: [text box]
 Login Password: [Change]

SMTX Authentication:
 Login User Name: [text box]
 Login Password: [Change]

Folder Authentication:
 Login User Name: [text box]
 Login Password: [Change]

LDAP Authentication:
 Login User Name: [text box]
 Login Password: [Change]

EAT366

9 Enter the new password in the [New Password] box.

10 Enter the new password in the [Confirm Password] box.

11 Click [OK] three times.

[Page Top](#)

Copyright © 2019, 2020, 2022

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

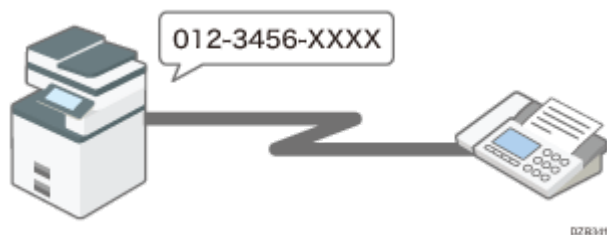
- Immediate Transmission is useful when you want to send a fax while confirming that it is received at the destination properly. You can use this feature when using G3 fax or IP-Fax.

[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.

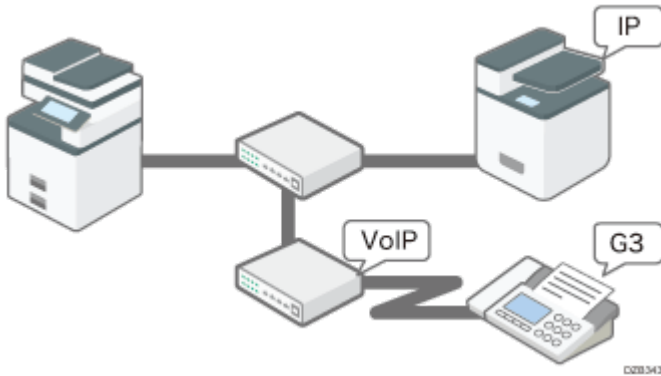


[Basic Procedure for Transmitting Faxes](#)

- 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.

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.

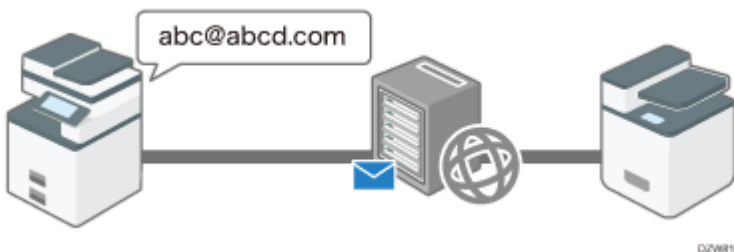


[Sending Documents by IP-Fax](#)

- 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.

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.

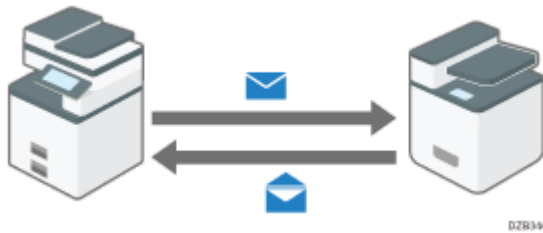


[Sending and Receiving Documents by Internet Fax](#)

- 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.

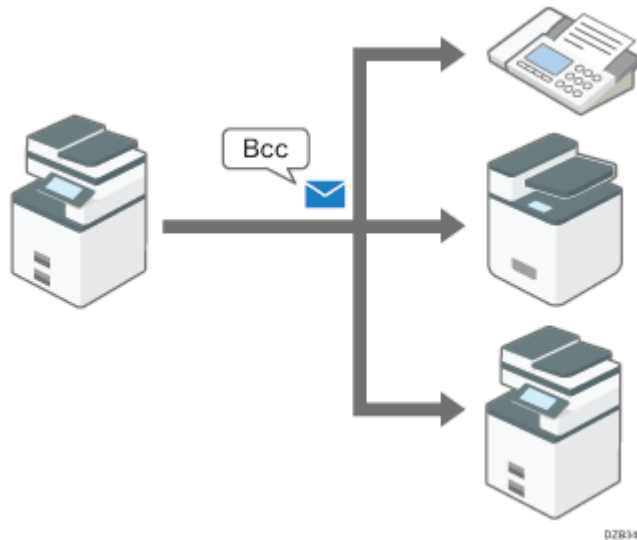
[Applying Encryption and Using a Signature for Enhanced Security When Sending an Internet Fax](#)

- 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.



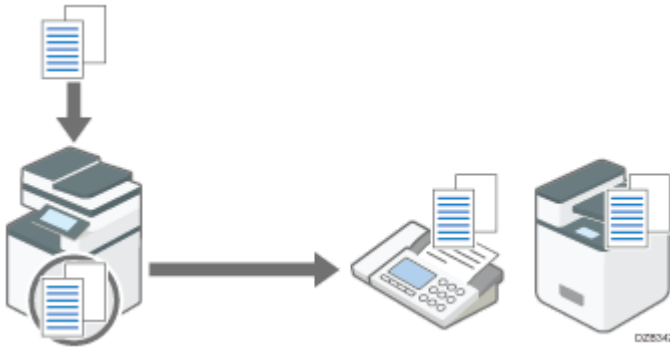
[Sending Internet Faxes without Using SMTP Server](#)

Note

- When using Internet Fax transmission, documents are sent at [Detail] resolution, even if you have specified [Super Fine]. To send a document at [Super Fine], configure the Full Mode when registering the destinations in the address book.
- For how e-mail is actually received by the computer, see [When Receiving Internet Fax on a Computer](#).

Advantages of Memory Transmission

The machine stores the scanned original in the memory temporarily and then sends it. When sending a document with many pages, the machine dials the destination number and starts transmission before scanning all pages of the original is completed (Parallel Memory Transmission).



[Basic Procedure for Transmitting Faxes](#)

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

- The machine tries redialing up to five times at five-minute intervals automatically when the line at the destination is busy or a transmission error occurs.
- 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 depending on the options 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.
 - Settings screen type: Standard
[List of Parameter Settings \(Standard\)](#)
 - Settings screen type: Classic
[List of Parameter Settings](#)

★ Important

- In case of a power outage, or if you leave the machine unplugged from the wall outlet for about one hour or more, all the documents stored in the memory of the fax will be erased. If a document has been erased, a "Power Off Report" listing the erased documents is printed.

[When an Error Is Reported in a Report or E-mail](#)

↓ Note

- If the machine redials while there are a large number of files stored in memory, documents might not be sent in the order they were scanned.

[Page Top](#)

Copyright © 2019, 2020, 2022

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 hard disk 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 hard disk 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

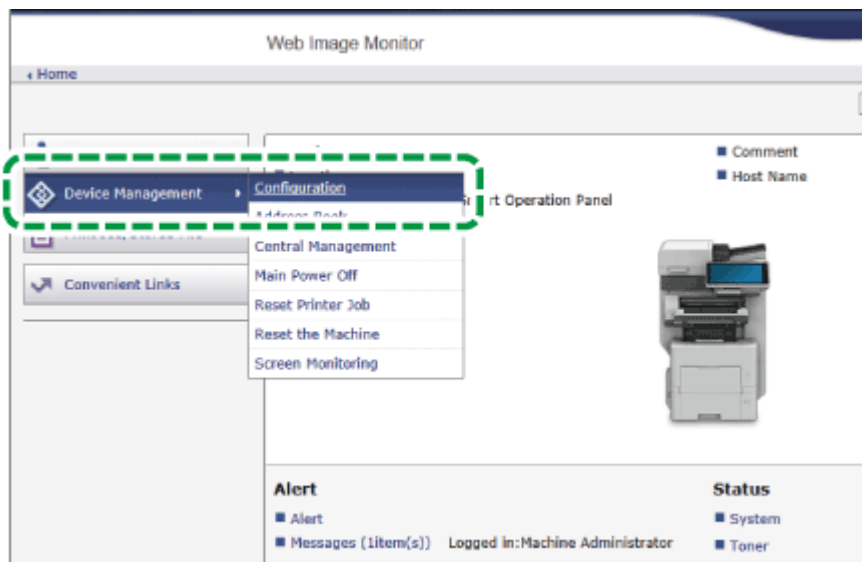
- Main power ON and OFF
- Transitions in power status
- Job run times or time interval between jobs
- Paper consumption per hour
- Power consumption of the machine

Selecting Logs to Collect

Select the types and items of logs to collect.

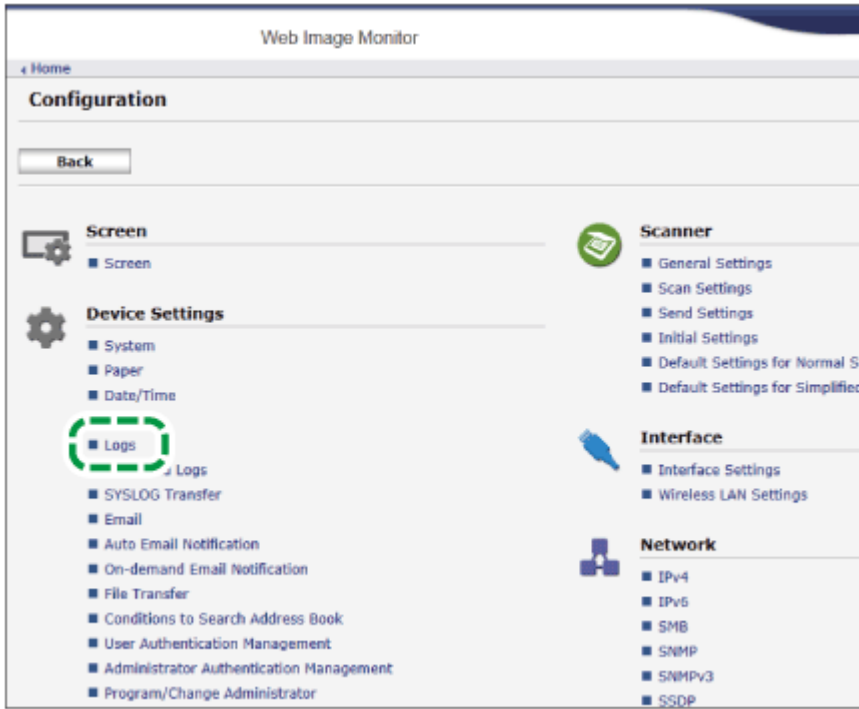
1 Log in to the machine as the machine administrator from Web Image Monitor.

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



EAT831

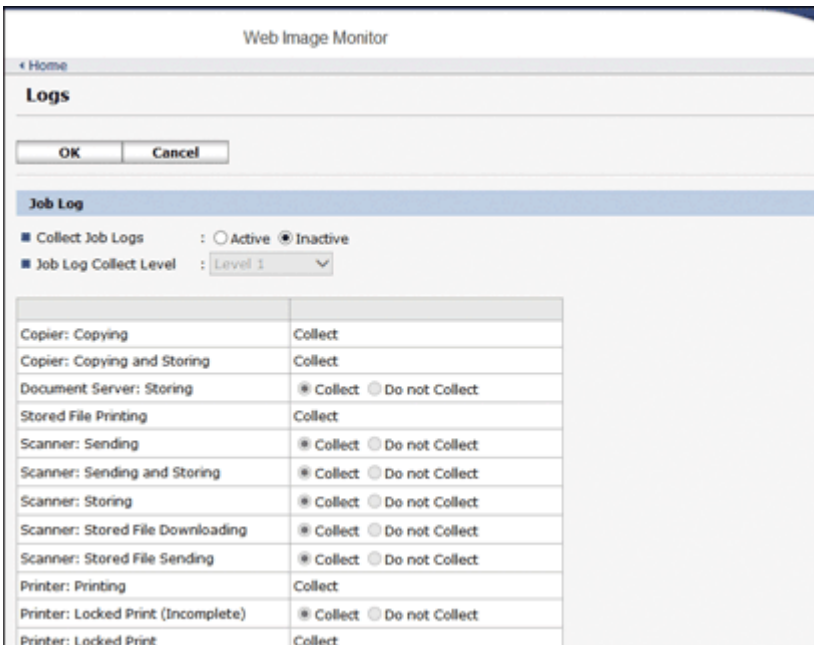
3 On the "Configuration" screen, click [Logs] of "Device Settings".



EAT832

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.
HDD 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 click the [Refresh] button on the web browser.

8 Click [Logout] and exit the Web browser.

Note

- When you changed Active/Inactive of Log Collect, perform "Delete All Logs".

Job Log Information Items

Job Log Item	Log Type Attribute	Content
Copier: Copying	Copier: Copying	Details of normal and Sample Copy jobs.
Copier: Copying and Storing	Copier: Copying and Storing	Details of files stored in Document Server that were also copied at the time of storage.
Document Server: Storing	Document Server: Storing	Details of files stored using the Document Server screen.
Document Server: Stored File Downloading	Document Server: Stored File Downloading	Details of files stored in Document Server and downloaded using Web Image Monitor.
Utility: Storing	Utility: Storing	Details of files stored using a utility.
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 Document Server that were also sent at the time of storage.
Scanner: Storing	Scanner: Storing	Details of scan files stored in Document Server.
Scanner: Stored File Downloading	Scanner: Stored File Downloading	Details of scan files stored in Document Server and downloaded using Web Image Monitor.
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 Document Server when "Job Type:" was set to [Document Server] in printer properties.
Report Printing	Report Printing	Details of reports printed from the control panel.
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.
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.
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 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.

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 Document Server.
Stored File Deletion	Stored File Deletion	Details of files deleted from Document Server.
All Stored Files Deletion	All Stored Files Deletion	Details of deletions of all Document Server files.
HDD Format ^{*2}	HDD Format	Details of hard disk formatting.
Unauthorized Copying	Unauthorized Copying	Details of documents scanned with "Data Security for Copying".
All Logs Deletion	All Logs Deletion	Details of deletions of all logs.
Log Setting Change	Log Setting Change	Details of changes made to log settings.
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.
Machine Data Encryption Key Change	Machine Data Encryption Key Change	Details of changes made to encryption keys using "Machine Data Encryption Key Change" setting.
Firmware: Invalid	Firmware: Invalid	Details of checks for firmware validity made at times such as when the machine was switched on.
Date/Time Change	Date/Time Change	Details of changes made to date and time settings.
Web Image Monitor Auto Logout	Web Image Monitor Auto Logout	Log of Auto Logout from Web Image Monitor.
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 hard disk is formatted, all the log entries up to the time of the format are deleted and a log entry indicating the completion of the format is made.

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

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

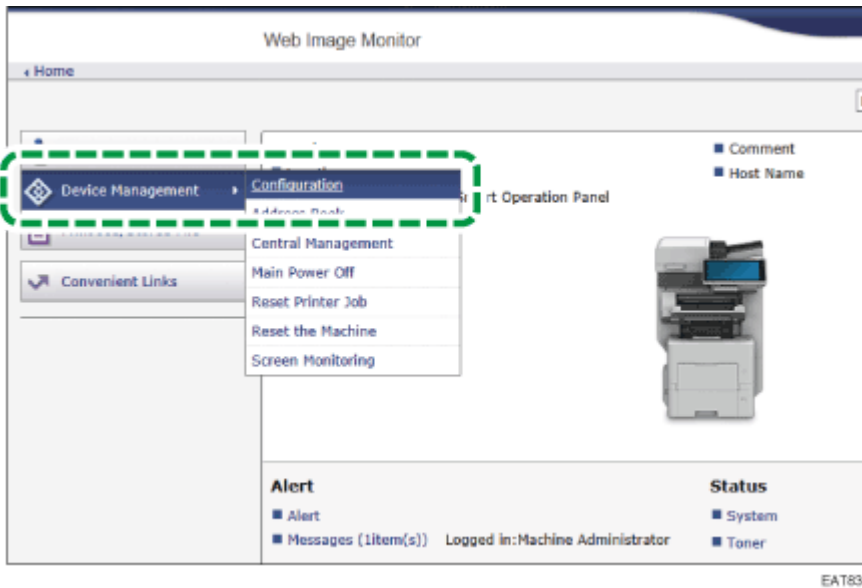
Eco-friendly Log Information Items

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.

Downloading the Logs

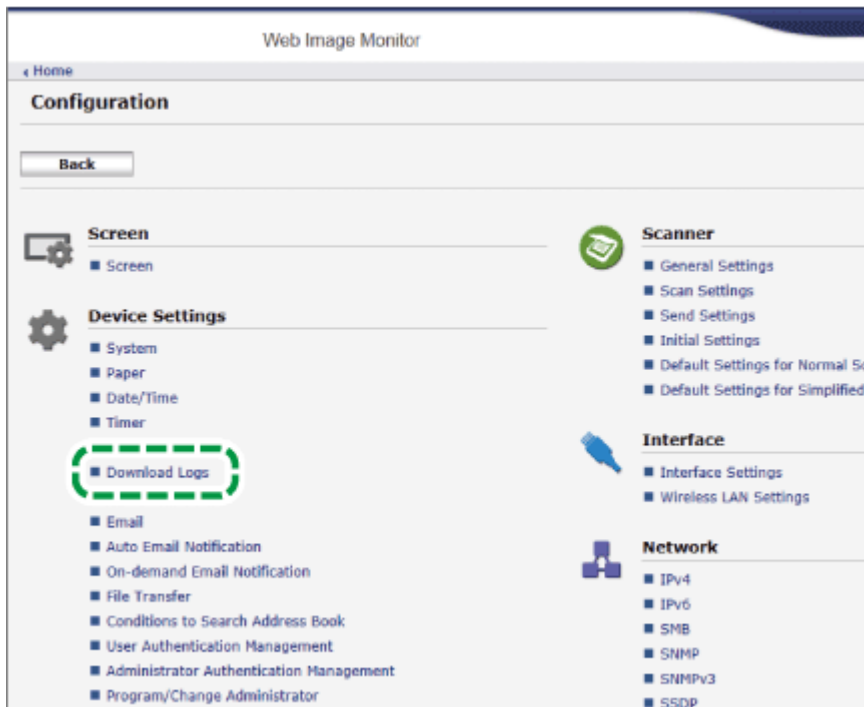
You can download the logs recorded on the machine as a CSV file.

- 1 Log in to the machine as the machine administrator from Web Image Monitor.**
- 2 Click [Configuration] from the [Device Management] menu.**



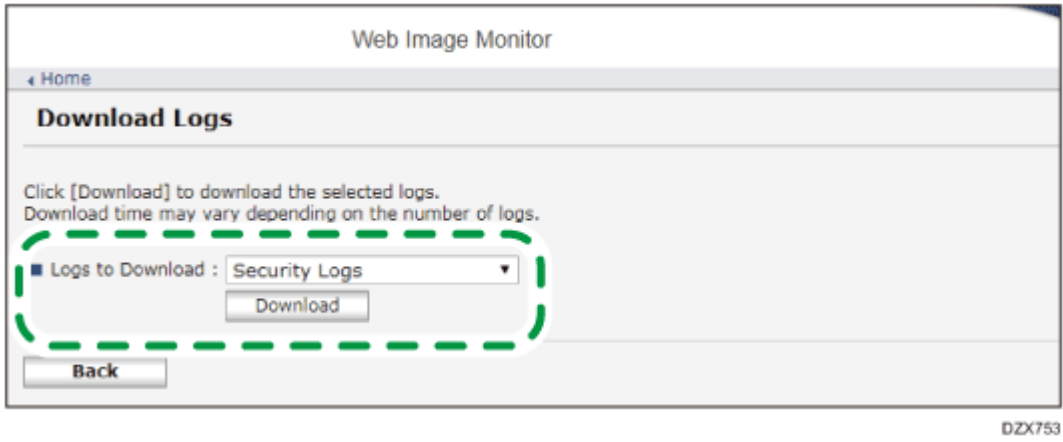
EAT831

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



EAT833

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



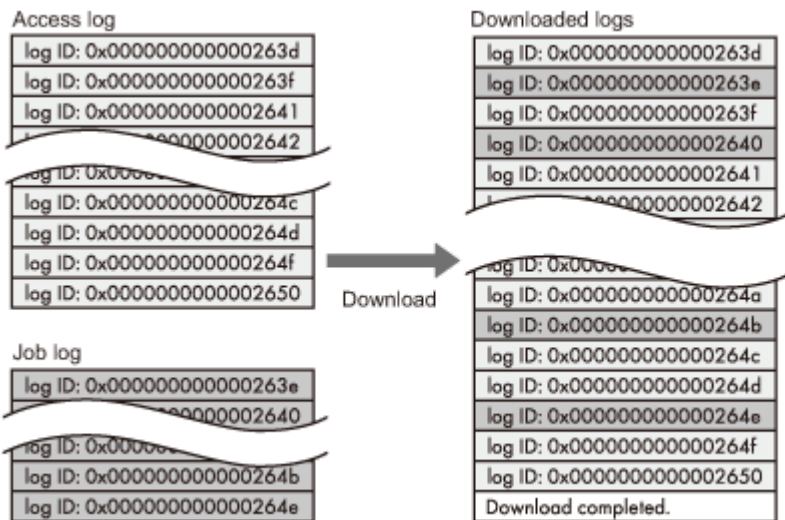
When you select [Security Logs], the downloaded file includes job log and access log.

5 Specify the location to store the file.

6 Click [Logout] and 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.



- The eco-friendly log is downloaded as an independent file.
- 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.

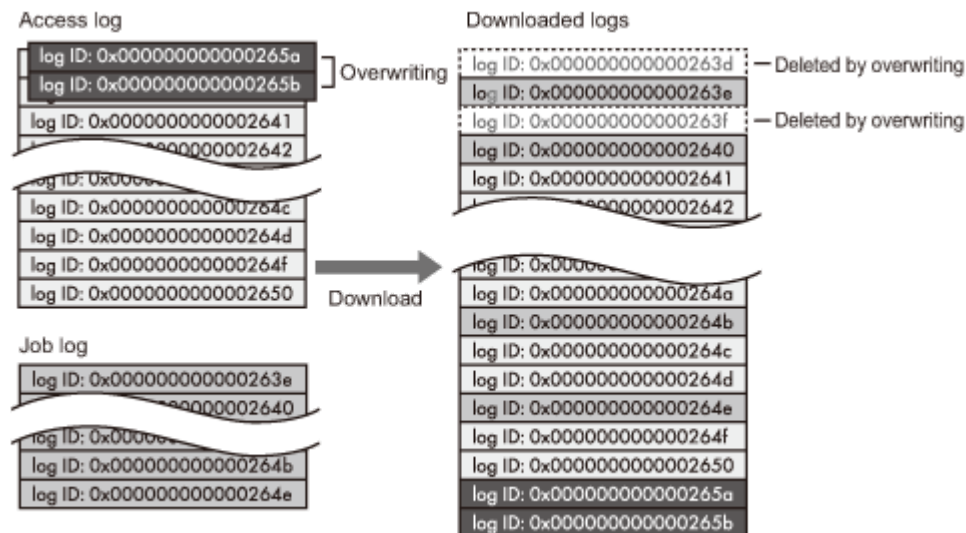
Number of logs that can be kept on the machine

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.



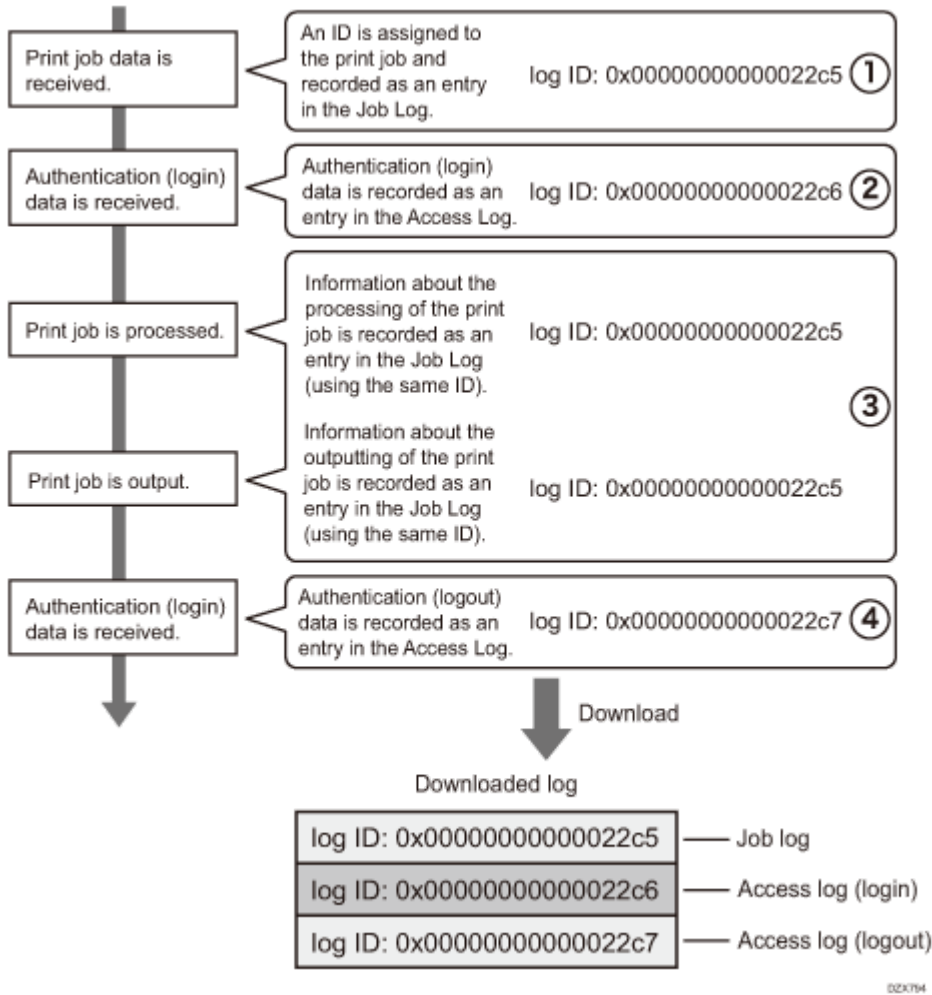
- Check the message in the last line of the downloaded logs to determine whether overwriting occurs or not while the logs were downloading. The messages are shown below:

- When overwriting did not occur:
Download completed.
- When overwriting occurred:
Download completed.
A part of the logs before Log ID xxxx does not exist any more.
(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.

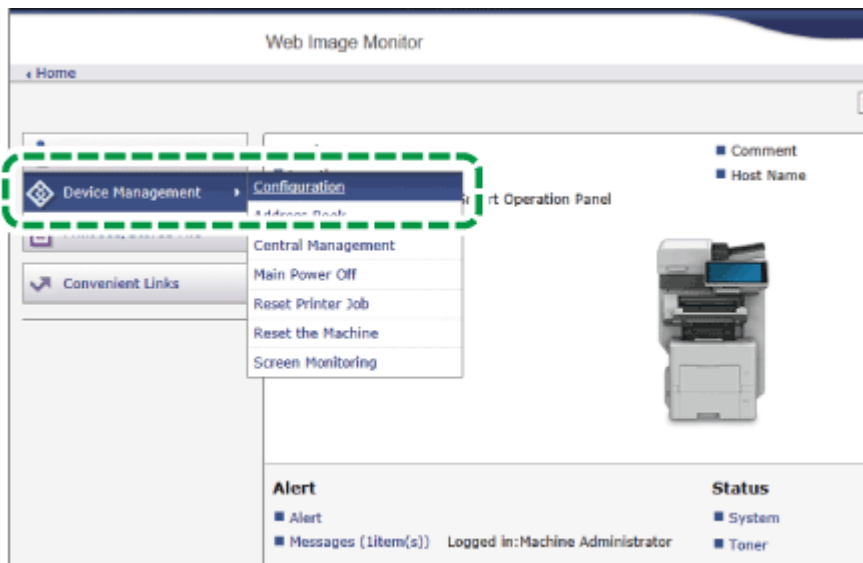
Deleting All Logs

You can delete all logs recorded on the machine.

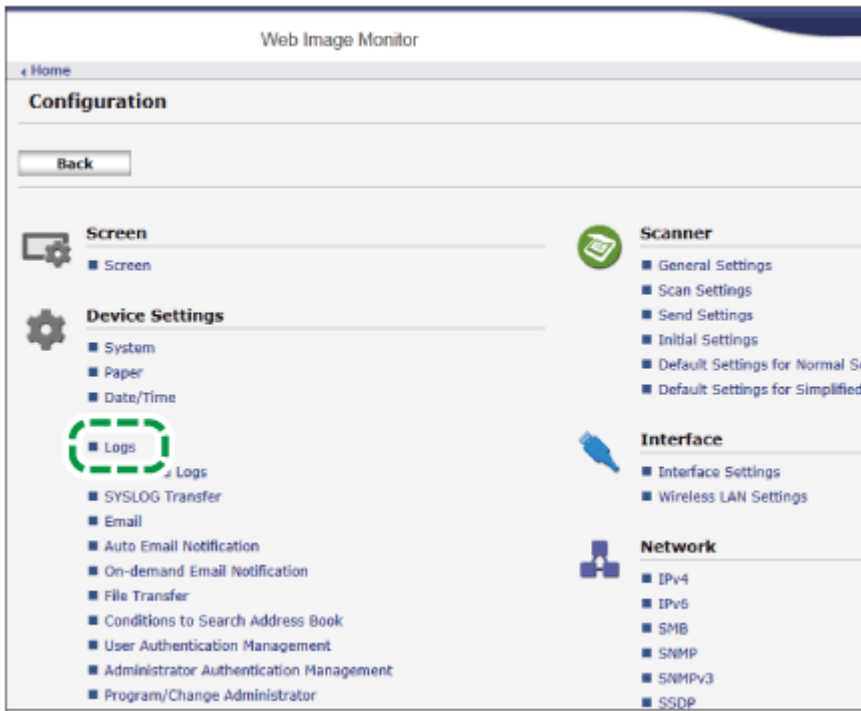
"Delete All Logs" appears when one of the job log, access log, or eco-friendly log is set to [Active].

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

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

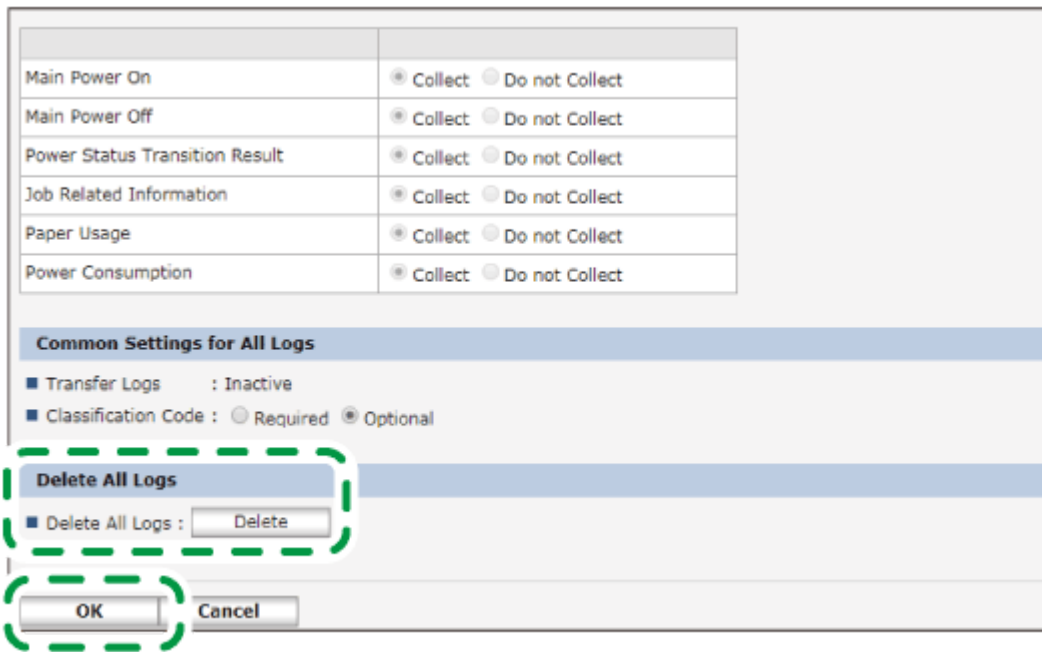


3 On the "Configuration" screen, click [Logs] of "Device Settings".



EAT832

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



DZX754

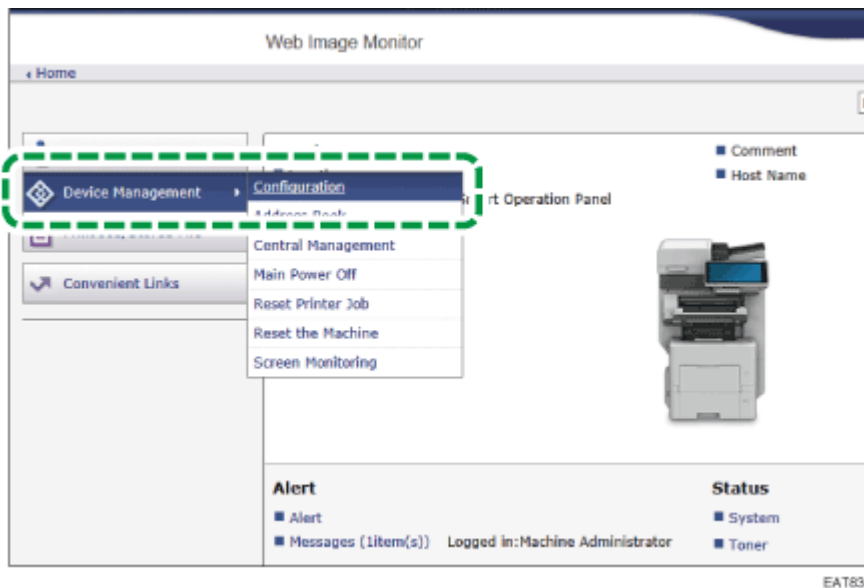
5 Click [Logout] and exit the Web browser.

Disabling Log Transfer to the Log Collection Server

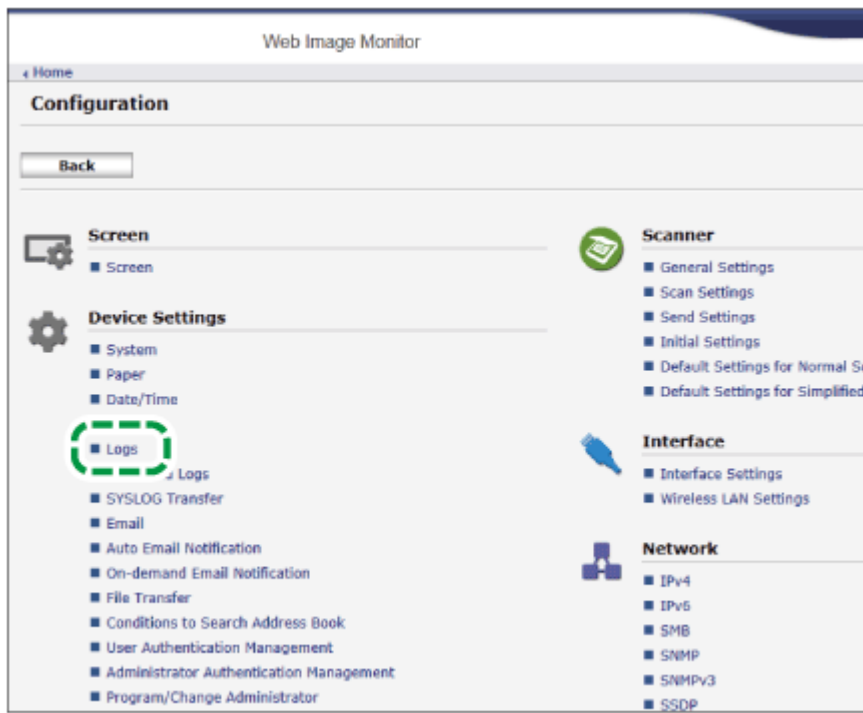
You can disable log transfer to the log collection server on Web Image Monitor.

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

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

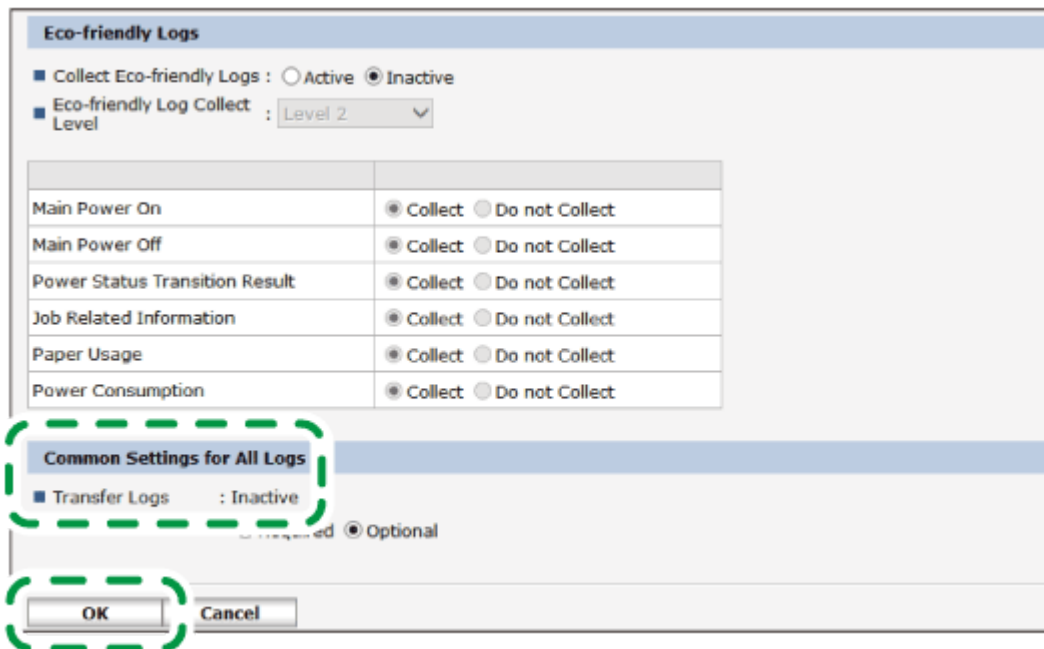


3 On the "Configuration" screen, click [Logs] of "Device Settings".



EAT832

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



DZX755

- 5** Click [Logout] and exit the Web browser.

Specifying Log Collection Setting or Deleting All Logs on the Control Panel

You can enable the settings about log collection on the control panel. You can also specify to transfer logs to the log collection server and delete all logs.

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

2 On the Home screen, press [Settings].



3 Press [Machine Features Settings].

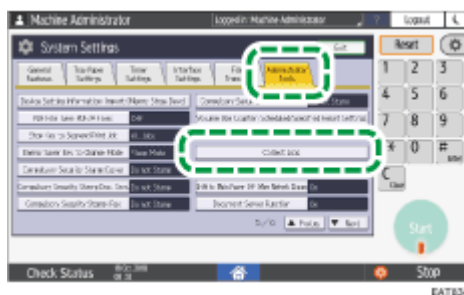


4 Press [System Settings] ► [Administrator Tools] tab.

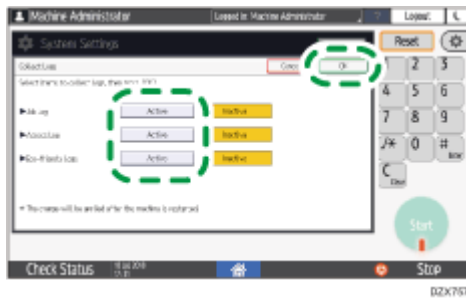
To specify log collection

Specify each type of log to be active.

1. Press [Collect Logs].



2. Select [Active] of "Job Log", "Access Log", and "Eco-friendly Logs", and then press [OK].



3. After completing the configuration, log out of the machine.
4. Turn off the main power of the machine, and then turn on the main power again.

To disable log transfer to the log collection server

You can disable log transfer to the log collection server. You can switch the log transfer setting to [Off] only when it is currently set to On.

1. Press [Transfer Log Setting].



2. Press [Do not Forward], and then press [OK].



3. After completing the configuration, log out of the machine.

5 After completing the management of log files, press [Home] (🏠).

Note

- To delete all logs, press [Yes] of [Delete All Logs].

[Page Top](#)

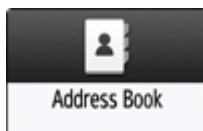
Copyright © 2019, 2020, 2022

Registering Fax Numbers in the Address Book

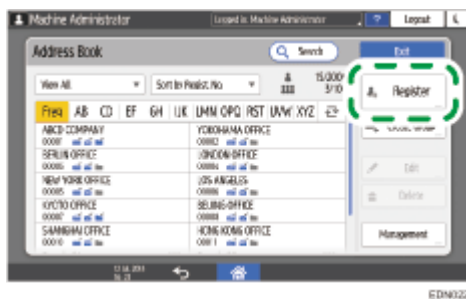
By registering the destinations to which you frequently send faxes together with the send conditions in the address book, you can easily send faxes.

Registering a Fax Number and Send Conditions

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

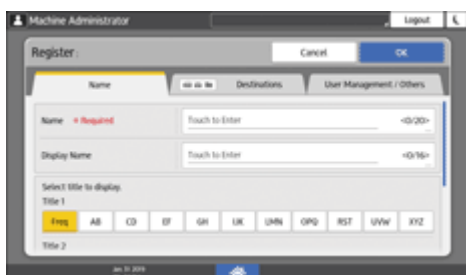


- 2 Press [Register] on the Address Book screen.



The items displayed on the screen vary depending on the version of RICOH Always Current Technology that is implemented on the machine.

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



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



5 Specify the Fax Destinations and send conditions.



- Select Line: Select the line to use.
- 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](#)

6 Press the [User Management / Others] tab, and specify the required settings.



- User Management: Enter the authentication information to login and use the machine.

- Registration Destination Group: Select a group to which this destination belongs as necessary. Register the group in advance.

[Registering 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] ().

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.

1 Press [Address Book] on the Home screen.




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



The items displayed on the screen vary depending on the version of RICOH Always Current Technology that is implemented on the machine.

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] ().

[Page Top](#)

Copyright © 2019, 2020, 2022



User Guide - Security Guide

For RICOH IM 550/600/600SR series



Author: RICOH COMPANY, LTD.

Date: 2022.07

Part Number: D0BW7276

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.

Registering Administrators Before Using the Machine


Administrators refers to special users who have the authority to manage various information and settings of the machine. To use the machine safely, register the administrators and allow only the administrators to configure the important settings such as registering users and the security settings.

Overview of the Administrator Privileges

For each function, there are four types of administrator privileges. You can assign all four privileges to one person, or assign a specific privilege to another person.

Types of the administrator privileges

	1	2	3	4
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



- **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.

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

Workflow to register the administrator

1. Activating the Administrator Authentication.

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

2. Logging in to the Machine as the Administrator

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

3. Registering or changing the administrator

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

 Note

- The administrators are distinguished from the users registered in the Address Book. A Login User Name registered in the Address Book cannot be used as an administrator.
- The supervisor has the privilege to manage the administrators. When the administrator is changed, the supervisor can reset the login password. There is only one supervisor.

Activating the Administrator Authentication (Settings Screen Type: Standard)

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.

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



- 2 On the Settings screen, press [System Settings].

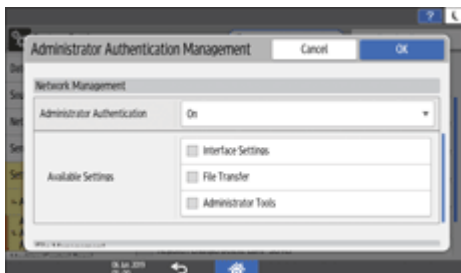


3 Press [Settings for Administrator] ► [Authentication/Charge] ► [Administrator Authentication/User Authentication/App Auth.] ► [Administrator Authentication Management].

4 For each 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] ().

Logging in to the Machine as the Administrator (Settings Screen Type: Standard)

Log in on the control panel as an administrator.

To log in to the machine for the first time, login as Administrator 1 using either of the following login user names and passwords.

- the default login user name and password (Refer to the provided guide for the Login User Name and Login Password.)

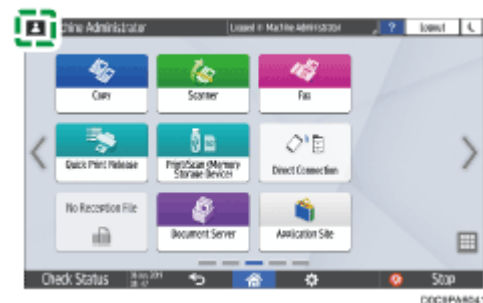
- the login user name and password that you changed in [Basic Settings When Installing] when you started the machine for the first time

1 On the Home screen, press [Login].



2 Enter the Login User Name and Login Password of the administrator.

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



To register or change an administrator other than yourself, follow the procedures described in [Adding Administrators or Changing the Privileges \(Settings Screen Type: Standard\)](#).

3 After completing machine operations, press [Logout].

Note

- If you log in using administrator privileges, the name of the administrator logging in appears. When you log in with a user name that has multiple administrator privileges, one of the administrator privileges associated with that name is displayed.
- If you try to log in from an operating screen, “You do not have the privileges to use this function. You can only change setting(s) as an administrator.” appears.

Adding Administrators or Changing the Privileges (Settings Screen Type: Standard)

You can register up to four administrators. All four registered personnel can have all administrator privileges. To reduce the administrator's load, the four registered personnel can share the administrator privileges.

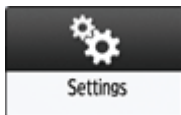
Discuss the number of users to add and privileges to give in advance, decide the Login User Name and Login Password for Administrator 2 to Administrator 4, and configure the settings.

★ Important

- Do not forget the Login User Name and Login Password of the administrators added.
- An administrator cannot change the login user names and passwords for other administrators.

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

2 On the Home screen, press [Settings].



3 On the Settings screen, 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].

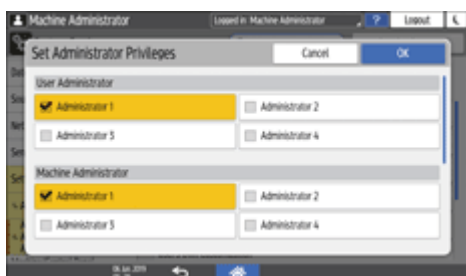
5 Press the desired administrator ([Administrator 1] to [Administrator 4]).

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

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 an administrator to assign for the administrator privileges, 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 privileges are assigned to the login administrator (Administrator 1).
- Administrator privileges assigned to a person can be shared with another person.

9 Press [OK].

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

Take note of the Login User Name and Login Password specified for the other administrators and inform them to the administrator.

Notes when specifying the login user name and password

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

- Upper case letters: A to Z (26 characters)
- Lower case letters: a to z (26 characters)
- Numbers: 0 to 9 (10 characters)

- Symbols: (space) ! " # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ` { | } ~ (33 characters)

Login user name/ password	Explanation
Login user name	<ul style="list-style-type: none"> • Cannot contain spaces, colons or quotation marks. • Cannot be left blank. • Can be up to 32 characters long. • The login user name of an administrator must contain characters other than numerical characters (numbers) if it is up to 8 characters. If it consists of only numbers, 9 or more must be used.
Login password	<ul style="list-style-type: none"> • The maximum password length for administrators and supervisors is 32 characters and 128 characters for users. • There are no restrictions on the types of characters that can be used for a password. For security, it is recommended to create passwords consisting of uppercase or lowercase characters, numbers, and symbols. A password consisting of a large number of characters is less easily guessed by others. • In [Password Policy] in [Extended Security 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. <p style="text-align: center;">Security</p>

Changing the Supervisor (Settings Screen Type: Standard)

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

To do this, you must enable the user administrator's privileges through the settings under "Administrator Authentication Management".

[Adding Administrators or Changing the Privileges \(Settings Screen Type: Standard\)](#)

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

2 On the Home screen, press [Settings].



3 On the Settings screen, press [System Settings].



4 Press [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, and then press [Done].

7 Press [Change] next to Login Password.

- 8 Enter the login password for New Password, and then press [Done].**
- 9 Enter the login password for Confirm New Password again, and then press [Done].**
- 10 Press [OK] twice.**
- 11 Press [Close].**
- 12 Press [OK].**

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

Changing the Password of an Administrator (Settings Screen Type: Standard)

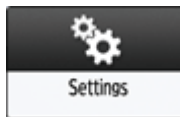
Only the supervisor has the privilege to change the password of the administrator. If an administrator forgets the password or wants to change the password, the supervisor must reset the password.

Refer to the provided guide for the 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.**
- 2 On the Home screen, press [Settings].**



3 On the Settings screen, press [System Settings].



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

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



6 Press [Change] next to Login Password.

7 Enter the login password for New Password, and then press [Done].

8 Enter the login password for Confirm New Password again, and then press [Done].

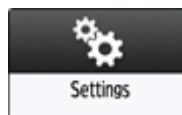
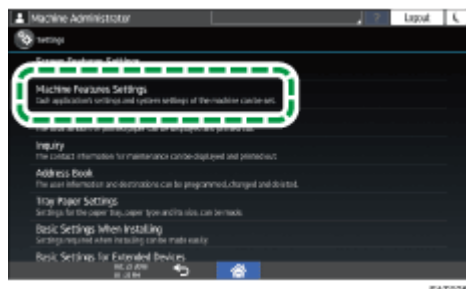
9 Press [OK] twice.

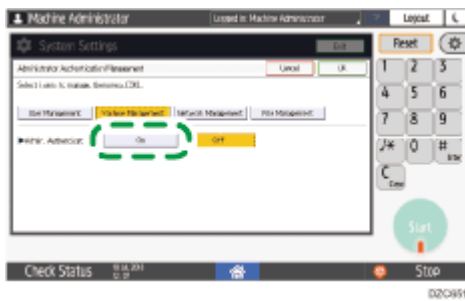
10 Press [Close].**11 Press [OK].**

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

Activating the Administrator Authentication (Settings Screen Type: Classic)

An administrator can manage the machine by activating the management function under [Administrator Authentication Management]. 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.

1 On the Home screen, press [Settings].**2 On the Settings screen, press [Machine Features Settings].****3 Press [System Settings] ► [Administrator Tools] tab ► [Administrator Authentication Management] to display the setting screen for the administrator privilege.****4 Select the Administrator Privilege to activate administrator authentication, and then press [On].**



- User Management: To manage the information registered in the Address Book, select [On].
- Machine Management: To configure the settings so that the 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 Select the items to manage for each administrator privilege from "Available Settings".



The selected items cannot be changed by users.

User Management

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

Machine Management

- 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] ().

Logging in to the Machine as the Administrator (Settings Screen Type: Classic)

Log in from [Machine Features Settings] on the control panel as an administrator.

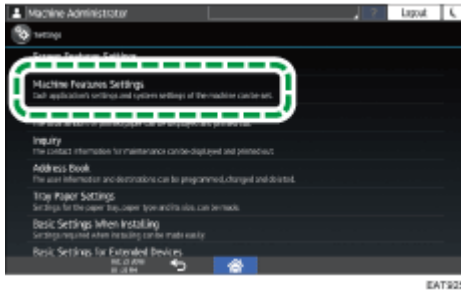
To log in to the machine for the first time, login as Administrator 1 using either of the following login user names and passwords.

- the default login user name and password (Refer to the provided guide for the Login User Name and Login Password.)
- the login user name and password that you changed in [Basic Settings When Installing] when you started the machine for the first time

1 On the Home screen, press [Settings].



2 On the Settings screen, press [Machine Features Settings].



EAT925

3 Press [Login].



EAT922

4 Enter the Login User Name and Login Password of the administrator.

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



EAT923

To register or change an administrator other than yourself, follow the procedures described in [Adding Administrators or Changing the Privileges \(Settings Screen Type: Classic\)](#).

5 After completing machine operations, press [Logout].

Note

- If you log in using administrator privileges, the name of the administrator logging in appears. When you log in with a user name that has multiple administrator privileges, one of the administrator privileges associated with that name is displayed.

- If you try to log in from an operating screen, “You do not have the privileges to use this function. You can only change setting(s) as an administrator.” appears.

Adding Administrators or Changing the Privileges (Settings Screen Type: Classic)

You can register up to four administrators. All four registered personnel can have all administrator privileges. To reduce the administrator's load, the four registered personnel can share the administrator privileges.

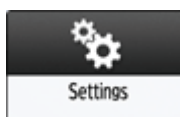
Discuss the number of users to add and privileges to give in advance, decide the Login User Name and Login Password for Administrator 2 to Administrator 4, and configure the settings.

★ Important

- Do not forget the Login User Name and Login Password of the administrators added.
- An administrator cannot change the login user names and passwords for other administrators.

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

2 On the Home screen, press [Settings].



3 On the Settings screen, press [Machine Features Settings].



4 Press [System Settings] ► [Administrator Tools] tab ► [Program / Change Administrator] to display the setting screen for the administrator.

5 Specify an administrator to assign for the administrator privileges.



- Assign the privileges of "User Administrator", "Machine Administrator", "Network Administrator", or "File Administrator" to [Administrator 1] to [Administrator 4].
- By default, all privileges are assigned to the login administrator (Administrator 1).
- Administrator privileges assigned to a person can be shared with another person.

6 Press [Change] of Administrator 1 to Administrator 4 to specify the Login User Name and Login Password.

When you manage the machine with software supporting SNMPv3 such as Device Manager NX, you have to specify the password to encrypt communication.

7 Press [OK].

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

Take note of the Login User Name and Login Password specified for the other administrators and inform them to the administrator.

Notes when specifying the login user name and password

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

- Upper case letters: A to Z (26 characters)
- Lower case letters: a to z (26 characters)
- Numbers: 0 to 9 (10 characters)
- Symbols: (space) ! " # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ` { | } ~ (33 characters)

Login user name/ password	Explanation
Login user name	<ul style="list-style-type: none"> • Cannot contain spaces, colons or quotation marks. • Cannot be left blank. • Can be up to 32 characters long. • The login user name of an administrator must contain characters other than numerical characters (numbers) if it is up to 8 characters. If it consists of only numbers, 9 or more must be used.
Login password	<ul style="list-style-type: none"> • The maximum password length for administrators and supervisors is 32 characters and 128 characters for users. • There are no restrictions on the types of characters that can be used for a password. For security, it is recommended to create passwords consisting of uppercase or lowercase characters, numbers, and symbols. A password consisting of a large number of characters is less easily guessed by others. • In [Password Policy] in [Extended Security], you can specify a password consisting of uppercase or lowercase characters, numbers, and symbols, as well as the minimum number of characters to be used for the password. <p style="text-align: center;">Specifying the Extended Security Functions</p>

Changing the Supervisor (Settings Screen Type: Classic)

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

To do this, you must enable the user administrator's privileges through the settings under "Administrator Authentication Management".

[Adding Administrators or Changing the Privileges \(Settings Screen Type: Classic\)](#)

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

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

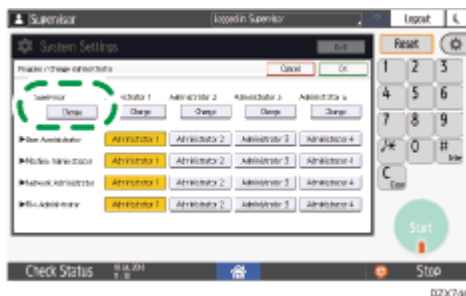


- 3 On the Settings screen, press [Machine Features Settings].**



- 4 Press [System Settings] ► [Administrator Tools] tab ► [Program / Change Administrator] to display the setting screen for the administrator.**

- 5 Under "Supervisor", press [Change].**



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

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

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

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

10 Enter the login password for confirmation again, and then press [OK].

11 Press [OK] twice.

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

Changing the Password of an Administrator (Settings Screen Type: Classic)

Only the supervisor has the privilege to change the password of the administrator. If an administrator forgets the password or wants to change the password, the supervisor must reset the password.

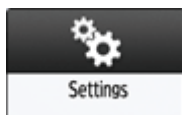
Refer to the provided guide for the Login User Name and Login Password of the supervisor.

★ 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.

2 On the Home screen, press [Settings].



3 On the Settings screen, press [Machine Features Settings].



EAT925

4 Press [System Settings] ► [Administrator Tools] tab ► [Program / Change Administrator] to display the setting screen for the administrator.

5 Press [Change] of the target administrator, and specify the Login Password.



[Adding Administrators or Changing the Privileges \(Settings Screen Type: Classic\)](#)

6 Press [OK].

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

[Page Top](#)

Copyright © 2019, 2020, 2022

Preparing the Server to Use for User Authentication



RICOH Always Current Technology updates this function. For details, see [List of Newly Added Functions \(Release Notes\)](#).

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 2008/2008 R2/2012/2012 R2/2016/2019

	<ul style="list-style-type: none"> To use Kerberos authentication under Windows Server 2008, install Service Pack 2 or later.
Authentication method	<p>Supports the following authentication methods:</p> <ul style="list-style-type: none"> NTLM authentication (NTLMv1/NTLMv2) Kerberos authentication <p>To specify Kerberos authentication, the server authenticating users must support Kerberos authentication. If the server does not support it, NTLM authentication is automatically selected.</p>
Requirements for authentication	<ul style="list-style-type: none"> 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 or SSL 3.0 encryption method. Register the server certificate of the domain controller in advance. <ul style="list-style-type: none"> Creating a Server Certificate TLS 1.0/SSL 3.0 is disabled in the factory default setting. To use TLS 1.0/SSL 3.0, specify TLS 1.0/SSL 3.0 to Enable on Web Image Monitor. Data transmission between the machine and the KDC (Key Distribution Center) server must be encrypted if Kerberos authentication is enabled. <ul style="list-style-type: none"> 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, the e-mail address cannot be obtained if SSL/TLS is specified.
- 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 logon" 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	<ul style="list-style-type: none"> • Kerberos authentication • Digest authentication • Cleartext authentication <p>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.</p>
Requirements for authentication	<ul style="list-style-type: none"> • To use SSL/TLS, the server must support the TLS 1.0/1.1/1.2 or SSL 3.0 encryption method. • TLS 1.0/SSL 3.0 is disabled in the factory default setting. To use TLS 1.0/SSL 3.0, specify TLS 1.0/SSL 3.0 to Enable on Web Image Monitor. • To use Kerberos Authentication, register the realm to distinguish the network area. <ul style="list-style-type: none"> • Settings screen type: Standard Registering the Realm • Settings screen type: Classic Programming 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 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.
- Under LDAP authentication, if "Anonymous Authentication" in the LDAP server's settings is not set to Prohibit, users who do not have an LDAP server account might be able to access the server.
- 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.

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.

Windows Server 2012/2016/2019

- 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 After completing the installation, click the notification icon of the server manager, and then click [Configure Active Directory Certificate Service on the destination server].**

- 14 Click [Next].**

- 15 Check [Certification Authority] in the role service, and then click [Next].**

- 16** Select **[Enterprise CA]**, and then click **[Next]**.

- 17** Select **[Root CA]**, and then click **[Next]**.

- 18** Select **[Create a new private key]**, and then click **[Next]**.

- 19** Select a cryptographic provider, key length, and hash algorithm to create a new private key, and then click **[Next]**.

- 20** In "Common name for this CA:" enter the Certificate Authority name, and then click **[Next]**.

- 21** Select the validity period, and then click **[Next]**.

- 22** Leave "Certificate database location:" and "Certificate database log location:" without change, and then click **[Next]**.

- 23** Click **[Configure]**.

- 24** When the message "Configuration succeeded" appears, click **[Close]**.

Windows Server 2008 R2

- 1** On the "Start" menu, point to "Administrative Tools", and then start the server manager.

2 Click **[Roles]** in the left column, click **[Add Roles]** from the "Action" menu.

3 Click **[Next]**.

4 Select the "Web Server (IIS)" and "Active Directory Certificate Services" check boxes, and then click **[Next]**.

If a confirmation message appears, click **[Add Features]**.

5 Read the content information, and then click **[Next]**.

6 Check "Certification Authority", and then click **[Next]**.

7 Select "Enterprise", and then click **[Next]**.

8 Select "Root CA", and then click **[Next]**.

9 Select "Create a new private key", and then click **[Next]**.

10 Select a cryptographic service provider, key length, and hash algorithm to create a new private key, and then click **[Next]**.

11 In "Common name for this CA:", enter the Certificate Authority name, and then click **[Next]**.

12 Select the validity period, and then click **[Next]**.

13 Leave "Certificate database location:" and "Certificate database log location:" without changing, and then click [Next].

14 Read the notes, and then click [Next].

15 Select the role services to install, and then click [Next].

16 Click [Install].

Installation of added features starts.

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, click [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].**

[Page Top](#)

Copyright © 2019, 2020, 2022

Programming 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.

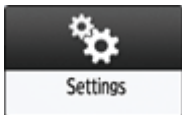
Note

- 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.

2 On the Home screen, press [Settings].

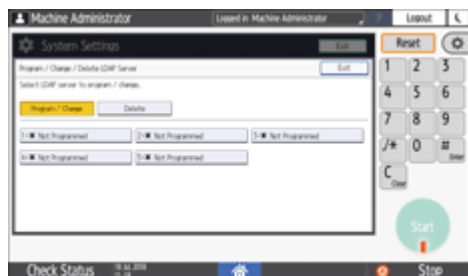


3 Press [Machine Features Settings].



4 Press [System Settings] ► [Administrator Tools] tab ► [Program / Change / Delete LDAP Server] to display the LDAP Server Program screen.

5 Press [Program / Change].



6 Press [*Not Programmed], and then enter the information for the LDAP Server.



- Name: Enter an optional program 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 No.: 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.
 - 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.
- 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: If [Kerberos Authentication] is selected, select the Realm Name.
Program the Realm in advance.

[Programming the Realm](#)

7 Press [Connection Test].

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



- Search Conditions: Enter the attributes as keywords for search conditions, [Name], [Email Address], [Fax Number], [Company Name], or [Department Name] using up to 64 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 [Key Display] 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.
 - Key Display: 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 After completing the procedure, press [Home] ().

Note

- To change/delete the stored LDAP server, display the [System Settings] ► [Administrator Tools] tab ► [Program / Change / Delete LDAP Server] screen, press [Program / Change] or [Delete], and then select the LDAP Server Name.

[Page Top](#)

Copyright © 2019, 2020, 2022

User Guide | IM 550/600 series

[Top Page](#) > [Security](#) > Specifying the Policy on Login/Logout

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 Policy

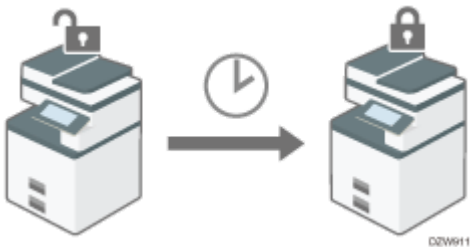
If an incorrect login password is entered several times, the User lockout function prevents further login attempts under the same login user name (Lockout).



- To enable a locked-out user to log in, the user administrator must disable the lockout or the user must wait until the lockout period elapses.
- You can specify the number of login password attempts to permit before locking out the user and the period of time until lockout is released automatically.
- By default, the login password can be entered up to five times and lockout is not released automatically.

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.
 - Settings screen type: Standard

[Timer](#)

- Settings screen type: Classic

[Timer Settings](#)

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

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.

Specifying User Lockout

Releasing Password Lockout

Specifying the Period of Time Until the Machine Logs You Out Automatically (Settings Screen Type: Standard)

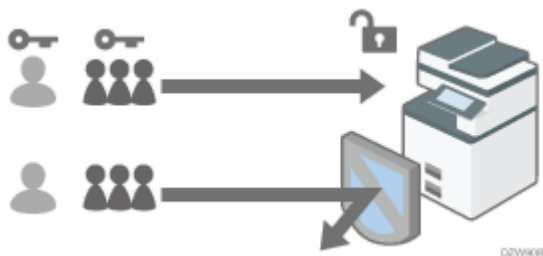
Specifying the Period of Time Until the Machine Logs You Out Automatically (Settings Screen Type: Classic)

[Page Top](#)

Copyright © 2019, 2020, 2022

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.
 - Settings screen type: Standard
 - [Confirming the Counter for Each User](#)
 - Settings screen type: Classic
 - [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.

User Authentication Method	Explanation
User Code authentication	Authentication is performed using an eight-digit user code. 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.
Basic authentication	<p>Authentication is performed using the login user name and login password registered in the address book on the machine.</p> <p>When specifying Basic authentication, the machine prompts you to enter the login information to use the machine.</p>
Windows authentication	<p>Authentication is performed using the account registered in the Active Directory of the Windows server.</p> <p>When specifying Windows authentication, the machine prompts you to enter the login information to use the machine.</p>
LDAP authentication	<p>Authentication is performed using the user information registered in the LDAP server.</p> <p>When specifying LDAP authentication, the machine prompts you to enter the login information to use the machine.</p>

- 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.

Specifying User Code Authentication (Settings Screen Type: Standard)

Specify the functions to restrict.

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

2 On the Home screen, press [Settings].

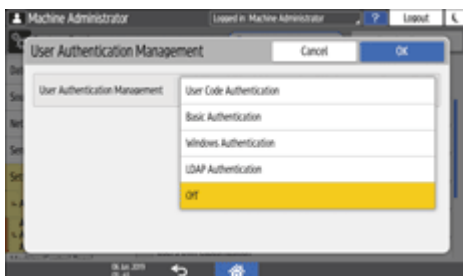


3 On the Settings screen, press [System Settings].



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 Printer 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], and then 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.

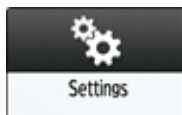
[Registering the User Code in the Address Book](#)

Specifying Basic Authentication (Settings Screen Type: Standard)

Register the default values of the functions available to each user.

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

2 On the Home screen, press [Settings].

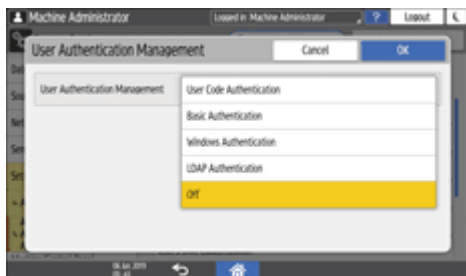


3 On the Settings screen, press [System Settings].



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], and then 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.

Specifying Windows Authentication (Settings Screen Type: Standard)

Register the information required for authentication in 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.

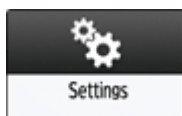
[Preparing the Server to Use for User Authentication](#)

- 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.

2 On the Home screen, press [Settings].

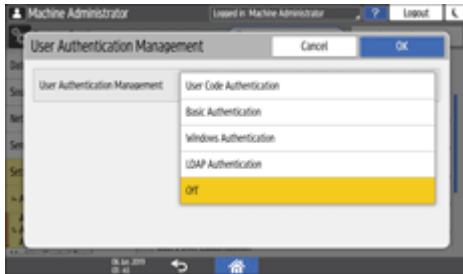


3 On the Settings screen, press [System Settings].



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 enter the same name 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], and then log out of the machine.

Note

- For the characters that can be used for login user names and passwords, see the section below:
[Adding Administrators or Changing the Privileges \(Settings Screen Type: Classic\)](#)
- When accessing the machine subsequently, you can use all the functions available to your group and to you as an individual user.
- Users who are registered in multiple groups can use all functions available to those groups.
- Under Windows Authentication, you do not need to create a server certificate unless you want to automatically register user information such as user names using SSL.

Specifying LDAP Authentication (Settings Screen Type: Standard)

Register the information required for authentication in the LDAP server.

Important

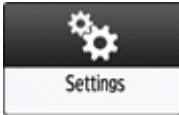
- In advance, check the use conditions in the LDAP server, and register the LDAP server in the machine.

[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.

2 On the Home screen, press [Settings].

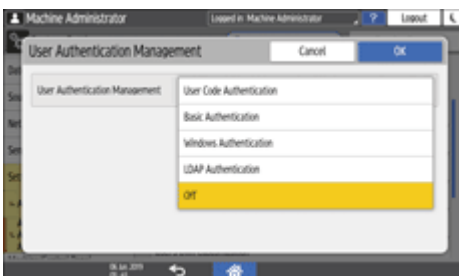


3 On the Settings screen, press [System Settings].



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], and then log out of the machine.

Note

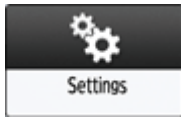
- For the characters that can be used for login user names and passwords, see the section below:
[Adding Administrators or Changing the Privileges \(Settings Screen Type: Standard\)](#)
- In LDAP simple authentication mode, authentication will fail if the password is left blank. To use blank passwords, contact your service representative.

Specifying User Code Authentication (Settings Screen Type: Classic)

Select [User Code Auth.] on [User Authentication Management], and specify the functions to restrict.

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

2 On the Home screen, press [Settings].



3 On the Settings screen, press [Machine Features Settings].



4 Press [System Settings] ► [Administrator Tools] tab ► [User Authentication Management] to display the User Authentication Management setting screen.

5 Press "User Code Auth.", and then select the functions to restrict.



- Functions to Restrict: Specify whether to perform User Code authentication for each function.

When registering the user code of the printer driver automatically, select [Printer: PC Control] in "Printer". Specify the user code registered in [System] to the printer driver.

When [Printer: 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 [Printer: PC Control] on "Printer".

[Specifying Maximum Print Volume Use of Each User](#)

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

[Executing a Print Job with Authentication Information Only](#)

6 Press [OK].

7 Press [Exit] to display the confirmation dialog, and then press [Yes] 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.

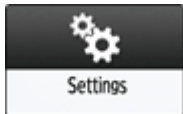
[Registering the User Code in the Address Book](#)

Specifying Basic Authentication (Settings Screen Type: Classic)

Select [Basic Auth.] on [User Authentication Management], and register the default values of the functions available to each user.

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

2 On the Home screen, press [Settings].



3 On the Settings screen, press [Machine Features Settings].



4 Press [System Settings] ► [Administrator Tools] tab ► [User Authentication Management] to display the User Authentication Management setting screen.

5 Press [Basic Auth.], and select the functions available to the user.



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

[Executing a Print Job with Authentication Information Only](#)

6 Press [OK].

7 Press [Exit] to display the confirmation dialog, and then press [Yes] 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.

Specifying Windows Authentication (Settings Screen Type: Classic)

On [User Authentication Management], select [Windows Auth.] to register the information required for authentication in the Windows server.



- 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.

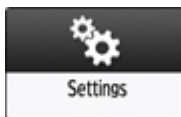
[Preparing the Server to Use for User Authentication](#)

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

[Programming the Realm](#)

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

2 On the Home screen, press [Settings].

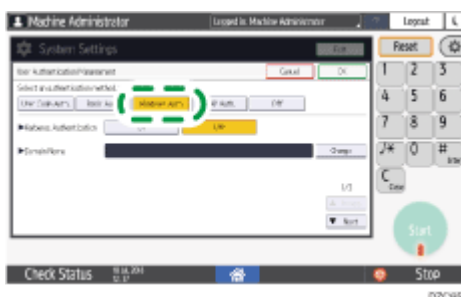


3 On the Settings screen, press [Machine Features Settings].



4 Press [System Settings] ► [Administrator Tools] tab ► [User Authentication Management] to display the User Authentication Management setting screen.

5 Select [Windows Auth.] to register the server for authentication and to specify the usable functions.



- Kerberos Authentication: To enable Kerberos Authentication, press [On].
- Realm Name: To enable Kerberos authentication, select the realm name to authenticate.
- Domain Name: To disable Kerberos authentication, press [Change] and enter the domain name to authenticate.
- Printer Job Authentication: Specify the security level for print jobs using the printer driver.

[Executing a Print Job with Authentication Information Only](#)

- Use Secure Connection (SSL): To encrypt communication signals, press [On].
- Group: If global groups have been registered, you can specify usable functions for each global group*. Press [Not Programmed], and then enter the same name 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.

- Available Functions: Specify the functions available to each group.

6 Press [OK].

7 Press [Exit] to display the confirmation dialog, and then press [Yes] to log out of the machine.

Note

- For the characters that can be used for login user names and passwords, see the section below:
[Adding Administrators or Changing the Privileges \(Settings Screen Type: Classic\)](#)
- When accessing the machine subsequently, you can use all the functions available to your group and to you as an individual user.
- Users who are registered in multiple groups can use all functions available to those groups.
- Under Windows Authentication, you do not need to create a server certificate unless you want to automatically register user information such as user names using SSL.

Specifying LDAP Authentication (Settings Screen Type: Classic)

On [User Authentication Management], select [LDAP Auth.] to register the information required for authentication in the LDAP server.

★ Important

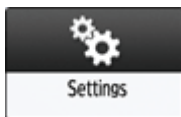
- In advance, check the use conditions in the LDAP server, and register the LDAP server in the machine.

[Preparing the Server to Use for User Authentication](#)

[Programming the LDAP Server](#)

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

2 On the Home screen, press [Settings].

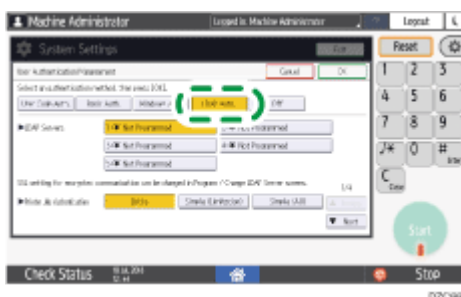


3 On the Settings screen, press [Machine Features Settings].



4 Press [System Settings] ► [Administrator Tools] tab ► [User Authentication Management] to display the User Authentication Management setting screen.

5 Select [LDAP Auth.] and select the server for authentication, and then specify the available functions.



- LDAP Servers: Select the LDAP server to authenticate.
- Printer Job Authentication: Specify the security level for print jobs using the printer driver.

[Executing a Print Job with Authentication Information Only](#)

- Available Functions: Specify the functions available to the user for each function.
- 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.

6 Press [OK].

7 Press [Exit] to display the confirmation dialog, and then press [Yes] to log out of the machine.

Note

- For the characters that can be used for login user names and passwords, see the section below:
[Adding Administrators or Changing the Privileges \(Settings Screen Type: Classic\)](#)
- In LDAP simple authentication mode, authentication will fail if the password is left blank. To use blank passwords, contact your service representative.

[Page Top](#)

Copyright © 2019, 2020, 2022

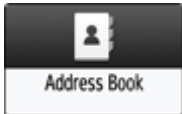
Limiting Available Functions

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

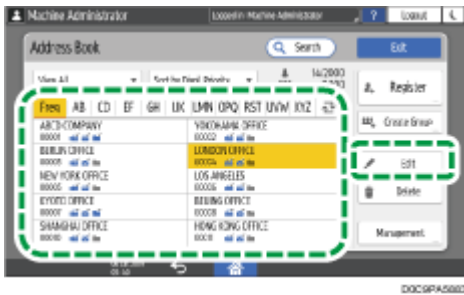
Specify the functions available to registered users. By configuring this setting, you can limit the functions available to users.

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

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



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

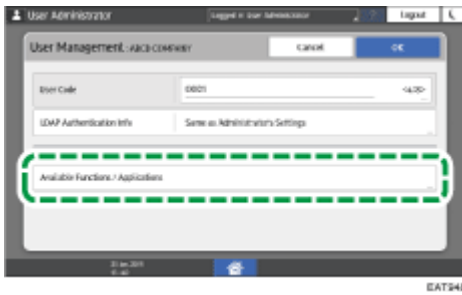


The items displayed on the screen vary depending on the version of RICOH Always Current Technology that is implemented on the machine.

4 Press [User Management / Others] tab ► [User Management].



5 Press [Available Functions / Applications].



6 Select available functions.



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

8 Press [Exit].

[Page Top](#)

Copyright © 2019, 2020, 2022

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

You can prevent data leaks by encrypting data on the hard disk of the machine even if the memory device is stolen, the machine is replaced with a new one, or the machine is disposed of.

Encrypting data on the hard disk



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 an SD card.

Overwriting data to prevent restoration



You can delete data that you do not want to be restored. The Auto Erase Memory 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 hard disk of the machine.

Changing the HDD Authentication Code

The Enhanced Security HDD Option attached to the machine protects the hard disk from tampering.

The self-encrypting function equipped with the Enhanced Security HDD Option encrypts all data stored in the machine. Also, the Enhanced Security HDD Option can authenticate the equipment connected to the HDD based on the Authentication Code. This function prevents the HDD data from being decrypted as long as the HDD Authentication Code is not known even if the hard disk were to be removed and connected to an analyzer.

[Changing the HDD Authentication Code \(Settings Screen Type: Standard\)](#)

[Changing the HDD Authentication Code \(Settings Screen Type: Classic\)](#)

Encrypting Data on the Hard Disk (Settings Screen Type: Standard)

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 hard disk 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

- This function is only available for the standard hard disk. If your machine is equipped with the Enhanced Security HDD Option, data on the hard disk is always encrypted. Therefore, this function can only encrypt the machine's NVRAM data.
- The machine cannot be operated while encrypting data, updating the encryption key, or canceling encryption.
- Do not turn off the power of the machine while encrypting data, updating the encryption key, or canceling encryption. If you turn off the power, the hard disk may be damaged and all data may be unusable.
- The encryption process takes several hours. Once the encryption process starts, it cannot be stopped.
- 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 an SD card.
- 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.
- If you use [Erase All Memory] and encryption simultaneously, and select overwrite 3 times for [Random Numbers], the process will take up to 9 hours 15 minutes. Re-encrypting from an already encrypted state takes the same amount of time.
- 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 has completed.
- Rebooting will be faster if there is no data to carry over to the hard disk and if encryption is set to [Format All Data], even if all data on the hard disk is formatted. Before you perform encryption, we

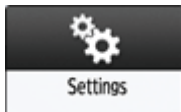
recommend you back up important data such as the Address Book and all data stored in Document Server.

- The encryption key is required for data recovery if the machine malfunctions. Be sure to store the encryption key safely for retrieving backup data.
- The machine cannot be used while the encryption key is being updated.
- The encryption key is required for recovery if the machine malfunctions. Be sure to store the encryption key safely for retrieving backup data.
- When the encryption key is updated, encryption is performed using the new key. After completing the procedure on the machine's control panel, turn off the main power and restart the machine to enable the new settings. Restarting can be slow when there is data to be carried over to the hard disk.
- Once the updating of the encryption key starts, it cannot be stopped. Make sure that the machine's main power is not turned off while the encryption process is in progress. If the machine's main power is turned off while the encryption process is in progress, the hard disk will be damaged and all data on it will be unusable.
- If the encryption key update was not completed, the created encryption key will not be valid.
- The machine cannot be used while data encryption is being cancelled.
- After completing the canceling on the machine's control panel, turn off the main power and restart the machine to enable the new settings. Restarting can be slow when there is data to be carried over to the hard disk.
- Once the canceling of data encryption starts, it cannot be stopped. Make sure that the machine's main power is not turned off while the encryption process is in progress. If the machine's main power is turned off while the encryption process is in progress, the hard disk will be damaged and all data on it will be unusable.
- When disposing of a machine, completely erase the memory. For details about erasing all the memory, see the section below:

[Initializing the Machine with the Erase All Memory Function \(Settings Screen Type: Standard\)](#)

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

2 On the Home screen, press [Settings].



3 On the Settings screen, 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, update the encryption Key, or back up the data.
 - Update Encryption Key: Encrypts data again and creates a new encryption Key.
 - Cancel Encryption: Cancels encryption.
 - Back Up Encryption Key: Makes a backup of the encryption key. The encryption setting is not changed. Proceed to Step 7.

6 Select one of the options from among [All Data], [File System Data Only], and [Format All Data] to encrypt the data.

The initial settings of the machine are not initialized regardless of the option you select.

When using the Embedded Software Architecture application, be sure to select [All Data] or [File System Data Only].

- All Data: Encrypts all data.
- File System Data Only: The following data are encrypted or initialized:
 - Data that are encrypted
 - Program/log of the Embedded Software Architecture application, Address Book, registered fonts, job logs, access logs, thumbnail images of stored documents, sent/received e-mail,

documents transferred to the document management server, files received by Mail to Print, spooled jobs

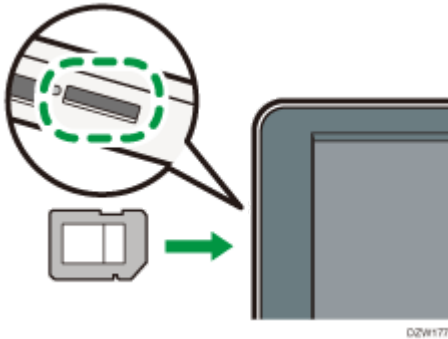
- Data that are initialized

Stored documents (documents in the Document Server, documents related to Locked Print/Sample Print/Stored Print/Hold Print, documents of fax stored reception), registered data (stamps/forms)

- Format All Data: Initializes all data without encryption. The NVRAM data (memory that remains even after the machine is turned off) will not be deleted (initialized).

7 Select the location to store the encryption key.

- Save to SD Card: Saves the encryption key to an SD card. Insert an SD card into the media slot, and then press [Save to SD Card] ► [OK].



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

8 Press [OK].

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

10 Press [Home] ().

11 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.

Specifying Auto Erase Memory (Settings Screen Type: Standard)

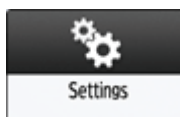
★ Important

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

You can overwrite and erase job data that was temporarily stored on the machine when using certain functions.

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

2 On the Home screen, press [Settings].



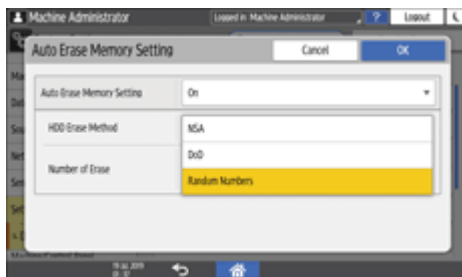
3 On the Settings screen, press [System Settings].



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] ().

Note

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



To check the overwriting process on the control panel

When Auto Erase Memory 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.
- The Data Overwrite icon will be "Clear" when there is a Sample Print/Locked Print/Hold Print/Stored Print job.



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

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

Initializing the Machine with the Erase All Memory Function (Settings Screen Type: Standard)

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

If your machine is equipped with the Enhanced Security HDD Option, the hard disk automatically discards the encryption key, making it impossible to decrypt the data on the hard disk before the data is erased using the selected overwriting method.

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 hard disk.
- Do not stop the overwrite mid-process. Doing so will damage the hard disk.
- We recommend that before you erase the hard disk, you use Device Manager NX to back up the user codes, the counters for each user code, and Address Book. For details, see Device Manager NX Help.
- If the method of Random Numbers is selected and overwrite three times is set, the Erase All Memory process takes up to 3 hours and 45 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 has completed.
- You must also format the data stored on the operation panel when deleting the data stored on the machine's hard disk. You can format the data stored on the panel by pressing [System Settings] ► [Settings for Administrator] ► [Data Management] ► [Restore Default Control Panel Settings]. You can format the screen features settings, individual application settings, and cache memory.
- When the extended features are installed on the machine, uninstall them before executing Erase All Memory. For details about uninstalling the extended features, see Extended Features Settings.

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

2 On the Home screen, press [Settings].



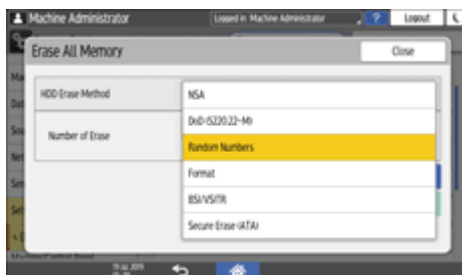
3 On the Settings screen, press [System Settings].



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

5 From the list next to HDD 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 hard disk. 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 hard disk drive.

*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.

Note

- 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.
- If the main power of the machine is turned off before the Auto Erase 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.

Changing the HDD Authentication Code (Settings Screen Type: Standard)

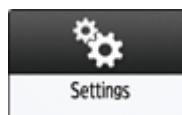
To securely protect confidential information stored on the attached Enhanced Security HDD Option, change the HDD Authentication Code when the machine is installed and at regular intervals (using 8 to 32 alphanumeric characters).

Important

- The HDD Authentication Code currently specified is not displayed on the screen of the machine to protect data.
- Prevent the HDD Authentication Code from being leaked so that the data remains secure.

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

2 On the Home screen, press [Settings].



3 On the Settings screen, press [System Settings].



4 Press [Settings for Administrator] ► [HDD Authentication Code].

5 Enter the authentication code, and then press [OK].

6 Press [OK].

7 Press [Home] ().

Encrypting Data on the Hard Disk (Settings Screen Type: Classic)

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 hard disk 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

- This function is only available for the standard hard disk. If your machine is equipped with the Enhanced Security HDD Option, data on the hard disk is always encrypted. Therefore, this function can only encrypt the machine's NVRAM data.

- The machine cannot be operated while encrypting data, updating the encryption key, or canceling encryption.
- Do not turn off the power of the machine while encrypting data, updating the encryption key, or canceling encryption. If you turn off the power, the hard disk may be damaged and all data may be unusable.
- The encryption process takes several hours. Once the encryption process starts, it cannot be stopped.
- 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 an SD card.
- 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.
- If you use [Erase All Memory] and encryption simultaneously, and select overwrite 3 times for [Random Numbers], the process will take up to 9 hours 15 minutes. Re-encrypting from an already encrypted state takes the same amount of time.
- 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 has completed.
- Rebooting will be faster if there is no data to carry over to the hard disk and if encryption is set to [Format All Data], even if all data on the hard disk is formatted. Before you perform encryption, we recommend you back up important data such as the Address Book and all data stored in Document Server.
- The encryption key is required for data recovery if the machine malfunctions. Be sure to store the encryption key safely for retrieving backup data.
- The machine cannot be used while the encryption key is being updated.
- The encryption key is required for recovery if the machine malfunctions. Be sure to store the encryption key safely for retrieving backup data.
- When the encryption key is updated, encryption is performed using the new key. After completing the procedure on the machine's control panel, turn off the main power and restart the machine to enable the new settings. Restarting can be slow when there is data to be carried over to the hard disk.
- Once the updating of the encryption key starts, it cannot be stopped. Make sure that the machine's main power is not turned off while the encryption process is in progress. If the machine's main power is turned off while the encryption process is in progress, the hard disk will be damaged and all data on it will be unusable.
- If the encryption key update was not completed, the created encryption key will not be valid.
- The machine cannot be used while data encryption is being cancelled.
- After completing the canceling on the machine's control panel, turn off the main power and restart the machine to enable the new settings. Restarting can be slow when there is data to be carried over to the hard disk.
- Once the canceling of data encryption starts, it cannot be stopped. Make sure that the machine's main power is not turned off while the encryption process is in progress. If the machine's main power is

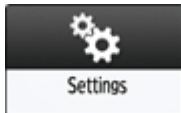
turned off while the encryption process is in progress, the hard disk will be damaged and all data on it will be unusable.

- When disposing of a machine, completely erase the memory. For details about erasing all the memory, see the section below:

[Initializing the Machine with the Erase All Memory Function \(Settings Screen Type: Classic\).](#)

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

2 On the Home screen, press [Settings].



3 On the Settings screen, press [Machine Features Settings].



4 Press [System Settings] ► [Administrator Tools] tab ► [Machine Data Encryption Settings] to display the setting screen.

5 Press [Encrypt].



- If the data has been encrypted, you can decrypt the data, update the encryption Key, or back up the data.



- Update Encryption Key: Encrypts data again and creates a new encryption Key.
- Cancel Encryption: Cancels encryption.
- Back Up Encryption Key: Makes a backup of the encryption key. The encryption setting is not changed. Proceed to Step 7.

6 Select one of the options from among [All Data], [File System Data Only], and [Format All Data] to encrypt the data.

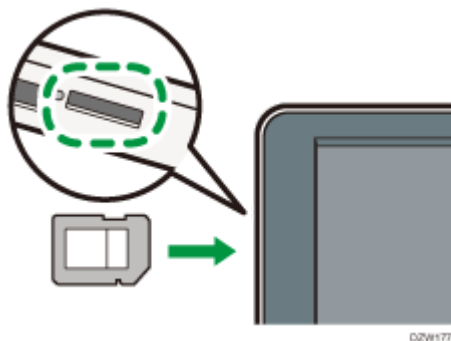
The settings of the machine are not initialized regardless of the option you select.

When using the Embedded Software Architecture application, be sure to select [All Data] or [File System Data Only].

- All Data: Encrypts all data.
- File System Data Only: The following data are encrypted or initialized:
 - Data that are encrypted
Program/log of the Embedded Software Architecture application, address book, registered fonts, job logs, access logs, thumbnail images of stored documents, sent/received e-mail, documents transferred to the document management server, files received by Mail to Print, spooled jobs
 - Data that are initialized
Stored documents (documents in the document server, documents related to locked print/sample print/stored print/hold print, documents of fax stored reception), registered data (stamps/forms)
- Format All Data: Initializes all data without encryption. The NVRAM data (memory that remains even after the machine is turned off) will not be deleted (initialized).

7 Select the location to store the encryption key.

- Save to SD Card: Saves the encryption key to an SD card. Insert an SD card into the media slot, and then press [Save to SD Card] ► [OK].



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

8 Press [OK].

The process of encryption or initialization starts.

9 Press [Home] ().

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.

Specifying Auto Erase Memory (Settings Screen Type: Classic)

★ Important

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

You can overwrite and erase job data that was temporarily stored on the machine when using certain functions.

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

2 On the Home screen, press [Settings].



3 On the Settings screen, press [Machine Features Settings].



4 Press [System Settings] ► [Administrator Tools] tab ► [Auto Erase Memory Setting] to display the setting screen.

5 Press [On] and select the overwriting method.

The default method for overwriting 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] ().

Note

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


To check the overwriting process on the control panel

When Auto Erase Memory 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.
- The Data Overwrite icon will be "Clear" when there is a Sample Print/Locked Print/Hold Print/Stored Print job.



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

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

Initializing the Machine with the Erase All Memory Function (Settings Screen Type: Classic)

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

If your machine is equipped with the Enhanced Security HDD Option, the hard disk automatically discards the encryption key, making it impossible to decrypt the data on the hard disk before the data is erased using the selected overwriting method.

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

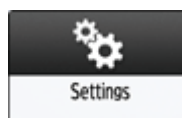
★ Important

- 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 hard disk.
- Do not stop the overwrite mid-process. Doing so will damage the hard disk.
- We recommend that before you erase the hard disk, you use Device Manager NX to back up the user codes, the counters for each user code, and Address Book. For details, see Device Manager NX Help.
- If the method of Random Numbers is selected and overwrite three times is set, the Erase All Memory process takes up to 3 hours and 45 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 has completed.
- You must also format the data stored on the operation panel when deleting the data stored on the machine's hard disk. You can format the data stored on the panel in [Initialize Screen Features Settings] in [Screen Device Settings] under [Screen Features Settings]. You can format the screen features settings, individual application settings, and cache memory.
- When the extended features are installed on the machine, uninstall them before executing Erase All Memory. For details about uninstalling the extended features, see Extended Features Settings.

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

2 On the Home screen, press [Settings].



3 On the Settings screen, press [Machine Features Settings].



4 Press [System Settings] ► [Administrator Tools] tab ► [Erase All Memory] to display the setting screen.

5 Select the overwriting method.

The default method for overwriting is "Random Numbers", and the default number of overwrites is 3.



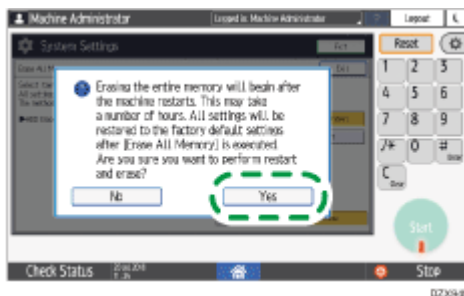
- NSA^{*1}: Overwrites data twice with random numbers and once with zeros.
- DoD (5220.22-M)^{*2}: Overwrites data with a random number, then with its complement, then with another random number, and the data is verified.
- Random Numbers: Overwrites data multiple times with random numbers. Select the number of overwrites from one to nine.
- 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 hard disk drive.
- Format: Formats the hard disk. Data is not overwritten.

*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.

Note

- To print the erase result, press [System Settings] ► [Administrator Tools] tab ► [Erase All Memory], and then press [Print Report].

- Initialize the settings on the control panel as necessary. Press [Screen Features Settings] ► [System] ► [Screen Device Settings] ► [Initialize Screen Features Settings] to initialize the settings of applications or bills.
- If the main power switch is turned off before the Auto Erase Memory process is completed, overwriting will start over when the main power switch is turned back on.
- If an error occurs before overwriting is completed, turn off the main power. Turn it on again, and then repeat from Step 1.

Changing the HDD Authentication Code (Settings Screen Type: Classic)

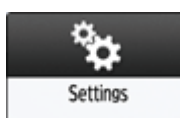
To securely protect confidential information stored on the attached Enhanced Security HDD Option, change the HDD Authentication Code when the machine is installed and at regular intervals (using 8 to 32 alphanumeric characters).

★ Important

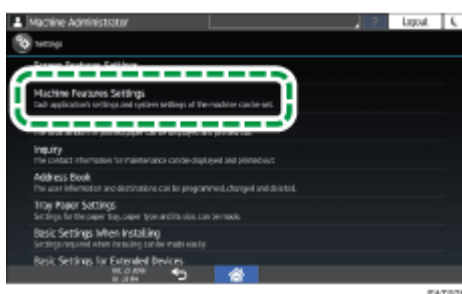
- The HDD Authentication Code currently specified is not displayed on the screen of the machine to protect data.
- Prevent the HDD Authentication Code from being leaked so that the data remains secure.


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

2 On the Home screen, press [Settings].



3 On the Settings screen, press [Machine Features Settings].



- 4 Press [System Settings] ► [Administrator Tools] tab ► [HDD Authentication Code] to display the setting screen.**
- 5 Enter the authentication code, and then press [OK].**
- 6 Press [OK].**
- 7 Press [Home] ().**

[Page Top](#)

Copyright © 2019, 2020, 2022

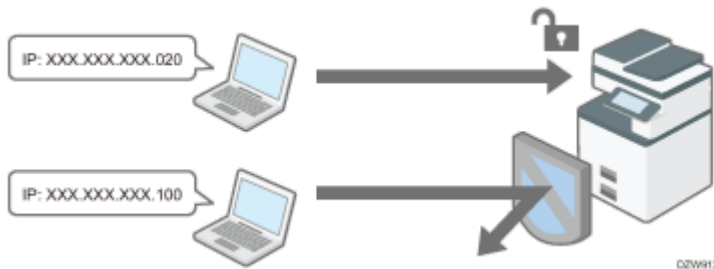
Access Control

RICOH Always Current Technology updates this function. For details, see [List of Newly Added Functions \(Release Notes\)](#).

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.

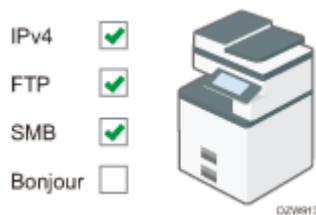
Limiting the IP addresses from which devices can access the machine (access control)

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.



Specifying the security level

You can select from among four security levels combining different protocols, ports, and encryption algorithms. Confirm the description of each level in [Security Level Setting List](#).

You can customize the security setting based on the selected level setting to suit your condition.

Limiting the IP Addresses from which Devices Can Access the Machine

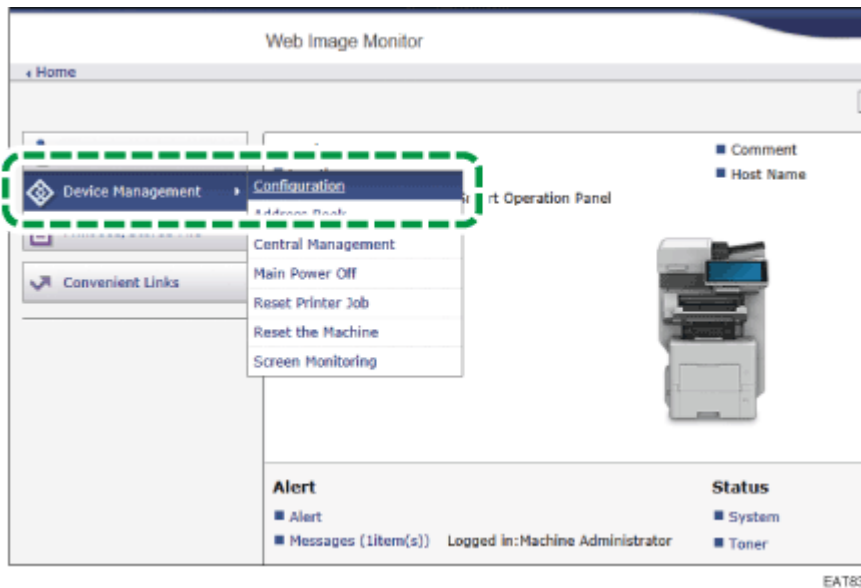
Specify the range of the IP address that can access the machine by using Web Image Monitor.

★ Important

- You can limit access from the following protocols.
 - LPR, RCP/RSH, FTP, Bonjour, SMB, WSD (Device), WSD (Printer), WSD (Scanner)/DSM, IPP, DIPRINT, RHPP, snmp, telnet, NBT
- The machine also limits access from Web Image Monitor.

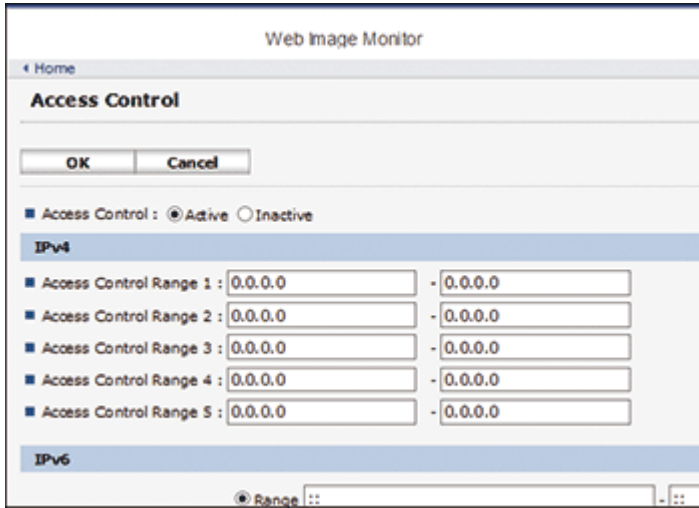
1 Log in to the machine as the network administrator from Web Image Monitor.

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



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

4 In "Access Control", 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.

5 Click [OK].

6 Click [OK] and exit the Web browser.


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.)
SMB TCP:139 TCP:445	1, 2, 3, 4, 5	Transmissions that require SMB
NBT UDP:137/UDP:138	3	SMB print via TCP/IP 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	<p>Transmissions that require RSH</p> <p>Network TWAIN</p> <p>(You can prohibit only personal information from being displayed by the settings on the control panel.)</p>
LPR TCP:515	2, 3, 4, 5	<p>Transmissions that require LPR</p> <p>(You can restrict only personal information from being displayed by the settings on the control panel.)</p>
IPP TCP:631	2, 3, 4, 5	Transmissions that require LPR
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
SSDP UDP:1900	2, 3	Device search using UPnP from Windows
Bonjour UDP:5353	2, 3	Transmissions that require Bonjour
@Remote TCP:7443 TCP:7444	1, 3	RICOH @Remote
DIPRINT TCP:9100	2, 3, 4, 5	Transmissions that require DIPRINT
RFU TCP:10021	1, 3	Remote updating of firmware
WSD (Device) TCP:53000 (variable)	2, 3	<p>Transmissions that require WSD (Device)</p> <p> Note</p>

		<ul style="list-style-type: none"> WS-Discovery (TCP:3702, UDP:3702) also works.
WSD (Printer) TCP:53001 (variable)	2, 3	Transmissions that require WSD (Printer)
WSD (Scanner)/DS M TCP:53002 (variable)	2, 3	Transmissions that require WSD (Scanner) Scanner management that requires DSM
RHPP TCP:59100	2, 3	Print with RHPP
LLMNR UDP:5355	2, 3	Name resolution requests using LLMNR

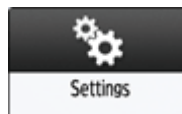
Note

- 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.

Disabling Unused Protocols from the Control Panel (Settings Screen Type: Standard)

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

2 On the Home screen, press [Settings].



3 On the Settings screen, press [System Settings].



4 Press [Network/Interface] ► [Effective Protocol].

5 From the list next to unused protocols, select [Inactive].



6 Press [OK].

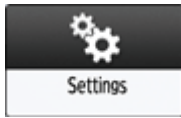
7 Press [Home] ().

Disabling Unused Protocols from the Control Panel (Settings Screen Type: Classic)

Configure protocols on [System Settings] ► [Interface Settings] tab.

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

2 On the Home screen, press [Settings].



3 On the Settings screen, press [Machine Features Settings].



4 Press [System Settings] ► [Interface Settings] tab ► [Effective Protocol] to display the setting screen of each protocol.

5 Disable unused protocols.



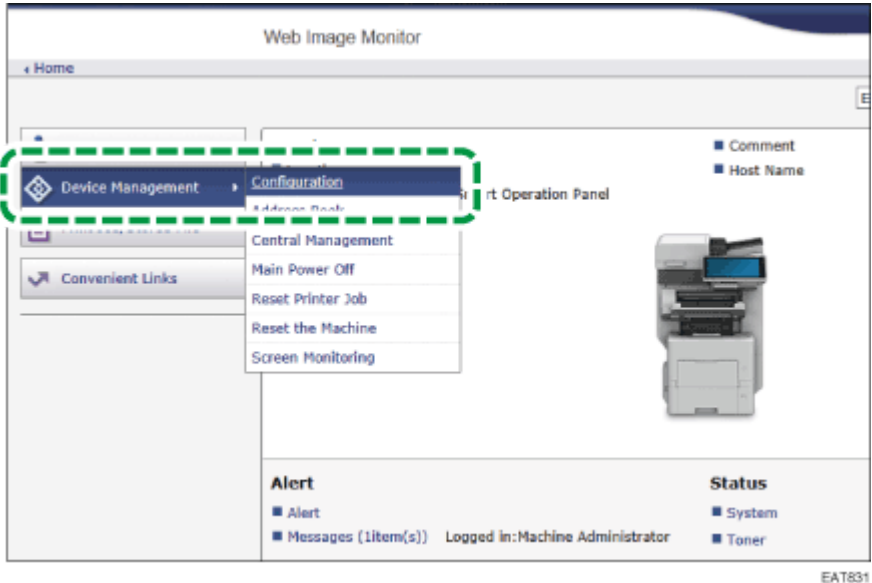
6 Press [OK].

7 Press [Home] ().

Disabling Unused Protocols from Web Image Monitor

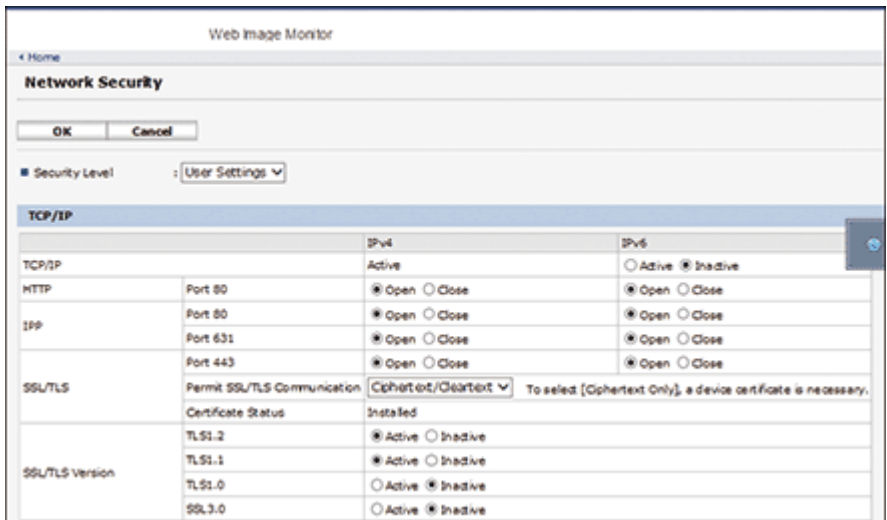
1 Log in to the machine as the machine administrator from Web Image Monitor.

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



3 Click [Network Security] in the "Security" category.

4 Specify protocols to disable or port numbers to close.



Select the security level from the pull-down menu of "Security Level". You can change the security level of multiple items at the same time. For details about the items changed by the setting of the security level, see either of the sections below:

[Specifying the Security Level Using the Control Panel \(Settings Screen Type: Standard\)](#)

[Specifying the Security Level Using the Control Panel \(Settings Screen Type: Classic\)](#)

[Specifying the Security Level Using Web Image Monitor](#)

5 Click [OK].

6 Click [OK] and exit the Web browser.

Security Level Setting List

You can configure security level settings using the control panel or Web Image Monitor. You can select the following security levels:

★ Important

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

- Level 0

Users can use all features without restriction. Select this when you have no information that needs to be protected from external threats.

- Level 1

Level 1 is suitable for a connection in an office.

- FIPS140

FIPS140 provides a security strength intermediate between "Level 1" and "Level 2".

You can only use codes recommended by the U.S. government as its coding/authentication algorithm. Settings other than the algorithm are the same as "Level 2".

- Level 2

Level 2 is the maximum security that is available in the machine. Select it to protect extremely important information.

For details about the security level settings, see the following list: You can change the setting for a particular function according to the use condition of the machine.

TCP/IP^{*1} (✓: Enabled. -: Function is disabled.)

Function	Level 0	Level 1	FIPS 140	Level 2
TCP/IP ^{*2}	✓	✓	✓	✓
HTTP > Port 80	Open	Open	Open	Open
IPP > Port 80	Open	Open	Open	Open
IPP > Port 631	Open	Open	Closed	Closed
SSL/TLS > Port 443	Open	Open ^{*3}	Open ^{*3}	Open ^{*3}
SSL/TLS > Permit SSL/TLS Communication	Ciphertext Priority	Ciphertext Priority	Ciphertext Only	Ciphertext Only
SSL/TLS Version > TLS1.2	✓	✓	✓	✓
SSL/TLS Version > TLS1.1	✓	✓	✓	✓
SSL/TLS Version > TLS1.0	✓	-	-	-
SSL/TLS Version > SSL3.0	✓	-	-	-
SSL/TLS > Encryption Strength Setting > AES	128bit/ 256bit	128bit/ 256bit	128bit/ 256bit	128bit/ 256bit
SSL/TLS > Encryption Strength Setting > 3DES	168bit	-	-	-
SSL/TLS > Encryption Strength Setting > RC4	-	-	-	-
SSL/TLS > Key Exchange	RSA	RSA	RSA	RSA
SSL/TLS > Digest	SHA1	SHA1	SHA1	SHA1
DIPRINT	✓	✓	-	-
LPR	✓	✓	-	-
FTP	✓	✓	✓	✓
RSH/RCP	✓	✓	-	-
TELNET	✓	-	-	-

Bonjour	✓	✓	-	-
SSDP	✓	✓	-	-
SMB	✓	✓	-	-
NetBIOS over TCP/IPv4	✓	✓	-	-
WSD (Device)	✓	✓	✓	✓
WSD (Printer)	✓	✓	✓	✓
WSD (Scanner)	✓	✓	✓	✓
WSD (Encrypted Communication of Device)	-	-	✓ ^{*4}	✓ ^{*4}
RHPP	✓	✓	-	-

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

*2 TCP/IP setting is not controlled by the security level. Specify manually whether to enable or disable this setting.

*3 IPP-SSL Communication is enabled under Windows 8.1 or later.

*4 This is enabled under Windows 8.1 or later.

SNMP (✓: Enabled -: Disabled)

Function	Level 0	Level 1	FIPS 140	Level 2
SNMP	✓	✓	✓	✓
Permit Settings by SNMPv1 and v2	✓	-	-	-
SNMPv1 and v2 functions	✓	✓	-	-
SNMPv3 function	✓	✓	✓	✓
Permit SNMPv3 Communication	Ciphertext/Cleartext	Ciphertext/Cleartext	Ciphertext Only	Ciphertext Only

TCP/IP Encryption Strength Setting

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

S/MIME > Encryption Algorithm	3DES-168bit	3DES-168bit	DES-168bit	AES-256bit
S/MIME > Digest Algorithm	SHA1	SHA1	SHA1	SHA-256bit
SNMPv3 > Authentication Algorithm	MD5	SHA1	SHA1	SHA1
SNMPv3 > Encryption Algorithm	DES	DES	AES-128	AES-128
Kerberos Authentication > Encryption Algorithm	AES256- CTSHMACSHA1- 96/AES128- CTSHMACSHA1- 96/DES3-CBC- SHA1/RC4- HMAC/DES- CBC-MD5	AES256- CTSHMACSHA1- 96/AES128-CTS- HMAC-SHA1- 96/DES3-CBC- SHA1/RC4- HMAC	AES256- CTSHMACSHA1- 96/AES128- CTSHMACSHA1- 96/DES3-CBC- SHA1	AES256- CTSHMACSHA1- 96/AES128- CTSHMAC- SHA1-96
Driver Encryption Key > Encryption Strength Setting	Simple Encryption	DES	AES	AES

Specifying the Security Level Using the Control Panel (Settings Screen Type: Standard)

- 1** Log in to the machine as the network administrator on the control panel.
- 2** On the Home screen, press [Settings].

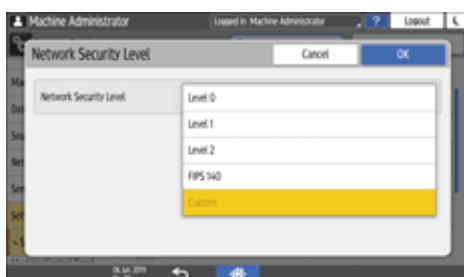


3 On the Settings screen, press [System Settings].



4 Press [Settings for Administrator] ► [Security] ► [Network Security Level].

5 From the list next to Network Security Level, select a security level.



- Select a security level from among Level 0, Level 1, Level 2, and FIPS140.

For the security levels, see the section below:

[Security Level Setting List](#)

- If you have customized the security level using Web Image Monitor, [Custom] is selected. You cannot enable [Custom] from the control panel. To customize the security level, use Web Image Monitor.

6 Press [OK].

7 Press [Home] ().

Specifying the Security Level Using the Control Panel (Settings Screen Type: Classic)

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

2 On the Home screen, press [Settings].



3 On the Settings screen, press [Machine Features Settings].



4 Press [System Settings] ► [Administrator Tools] tab ► [Network Security Level].

5 Specify the security level.



- Select a security level from among Level 0, Level 1, Level 2, and FIPS140, and Custom.

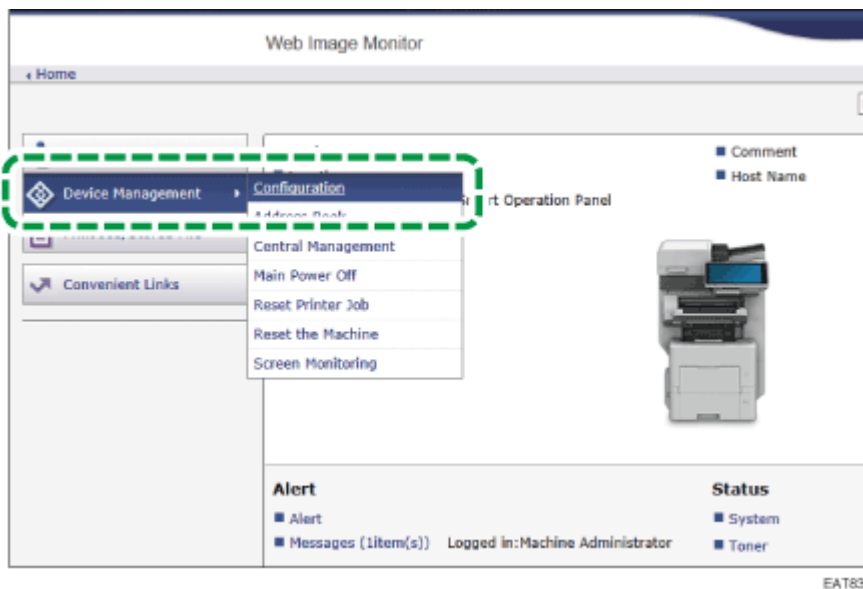
6 Press [OK].

7 Press [Home] ().

Specifying the Security Level Using Web Image Monitor

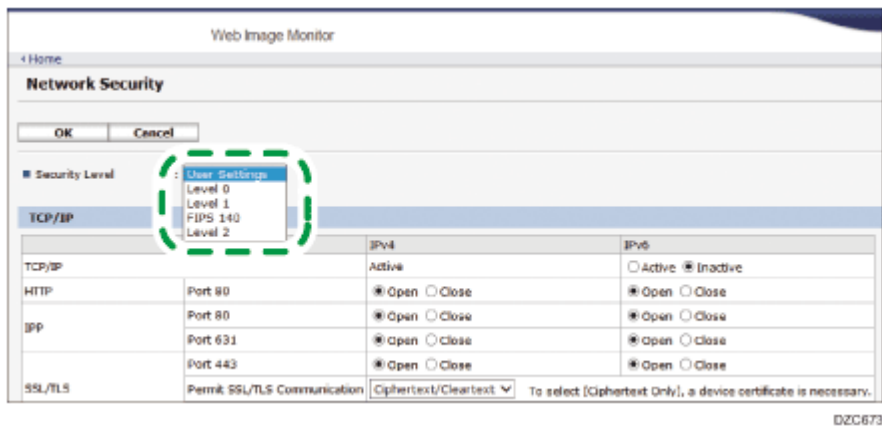
1 Log in to the machine as the network administrator from Web Image Monitor.

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



3 Click [Network Security] in the "Security" category.

4 Select a security level in "Security Level".



DZC673

5 Specify the settings as necessary.

- Specify each item according to the network condition or security policy.
- When the settings are changed, the security level is changed to [User Settings] automatically. [Custom] is displayed on the control panel.

6 Click [OK].

7 Click [OK] and exit the Web browser.

[Page Top](#)

Copyright © 2019, 2020, 2022

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.

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

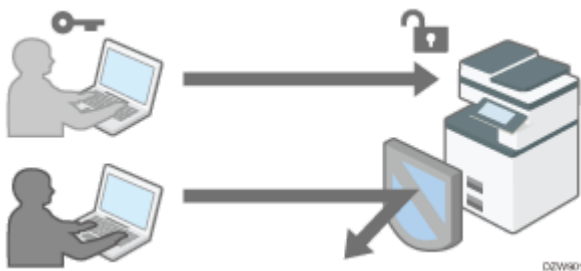
Defining the administrator of the machine



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

[Registering Administrators Before Using the Machine](#)

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



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

[Preventing Information Leaks by Sending Data to a Wrong Destination](#)

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.
- Select a person who can responsibly use the machine as the machine administrator, and use the machine appropriately.
- 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 Administrators Before Using the Machine](#).
- 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. If an error occurs in a verification process of Web Image Monitor, Web Image Monitor cannot be used. If this is the case, check the control panel.

[Page Top](#)

Copyright © 2019, 2020, 2022

Encrypting Network Communication

 Update Ver. 2.0

RICOH Always Current Technology updates this function. For details, see [List of Newly Added Functions \(Release Notes\)](#).

To protect communicated information, it is necessary to encrypt communication between computers and external equipment.

Data sent from and received by the machine can be intercepted, cracked, or tampered with during transmission. For example, the following data can be transmitted between the machine and external devices or the computer:

- Documents printed in the company using the printer driver
- Documents scanned and sent by e-mail to use in a meeting
- Login user name and login password

See the table below for the methods of encrypting data.

Data to encrypt	Encryption method	Process/Reference
Web Image Monitor IPP print Windows authentication LDAP authentication E-mail transmission	SSL/TLS	Install a device certificate. <ol style="list-style-type: none"> 1. Installing a Self-signed Certificate/Certificate Issued by a Certificate Authority 2. Encrypting Transmission Using SSL/TLS
E-mail	S/MIME	Install a user certificate. <ul style="list-style-type: none"> • Encrypting E-mail Sent from the Machine by S/MIME
Machine management data	SNMPv3	Specify an encryption password. <ul style="list-style-type: none"> • Encrypting Data Communicated with Machine Management Software Via SNMPv3
Authentication information of print jobs	Driver encryption key IPP authentication	Specifying a Driver Encryption Key Specify IPP authentication.

		<ul style="list-style-type: none"> • Encrypting the Login Password of Print Jobs
Kerberos authentication data	Varies depending on the KDC server	<p>Select an encryption method.</p> <ul style="list-style-type: none"> • Encrypting Communication Between KDC and the Machine

★ Important

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

Installing a Self-signed Certificate/Certificate Issued by a Certificate Authority (Settings Screen Type: Standard)

To encrypt communication with the machine, install a device certificate.

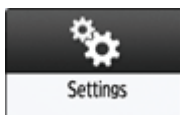
Two types of device certificates can be used: a self-signed certificate created by the machine and a certificate issued by a certificate authority. When you need higher reliability, use a certificate issued by a certificate authority.



- Install a device certificate from the control panel or Web Image Monitor.
- You can install only one self-signed certificate from the control panel. To install multiple certificates or a certificate issued by a certificate authority, specify the settings from Web Image Monitor.

Installing a self-signed certificate on the control panel

- 1** Log in to the machine as the network administrator on the control panel.
- 2** On the Home screen, press [Settings].



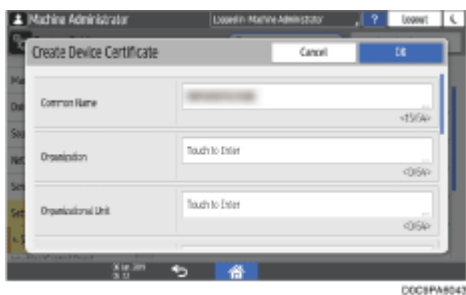
3 On the Settings screen, press [System Settings].



4 Press [Settings for Administrator] ► [Security] ► [Register/Delete Device Certificate].

5 Select [Certificate No. 1] and press [Register].

6 Specify the information to include in the certificate.



- Common Name: Enter the name of the device certificate to create. You must enter a name.
- Email Address: To use the device certificate for S/MIME, PDF Digital Signature, or PDF/A Digital Signature, enter the machine administrator's e-mail address.
- Specify Organization, Organizational Unit, and other items as necessary.

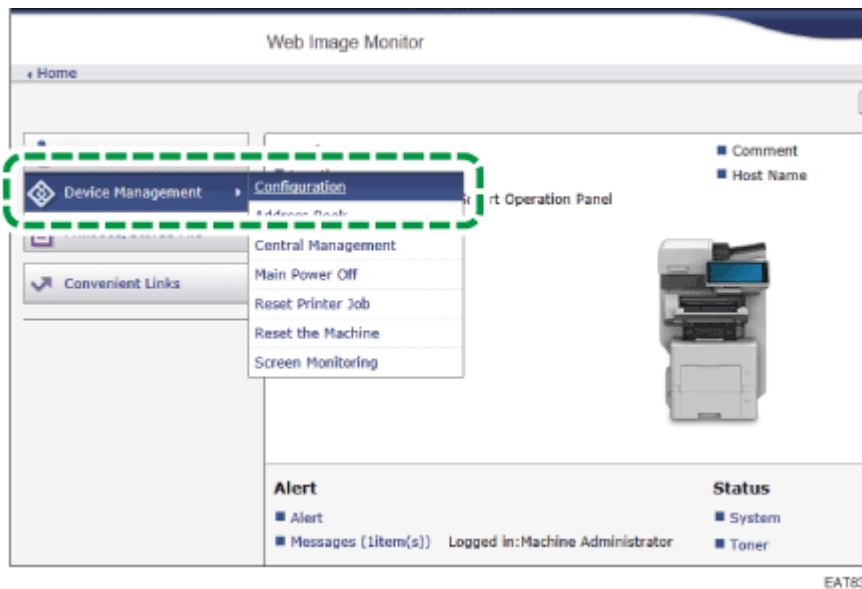
7 Press [OK].

8 Press [Exit].

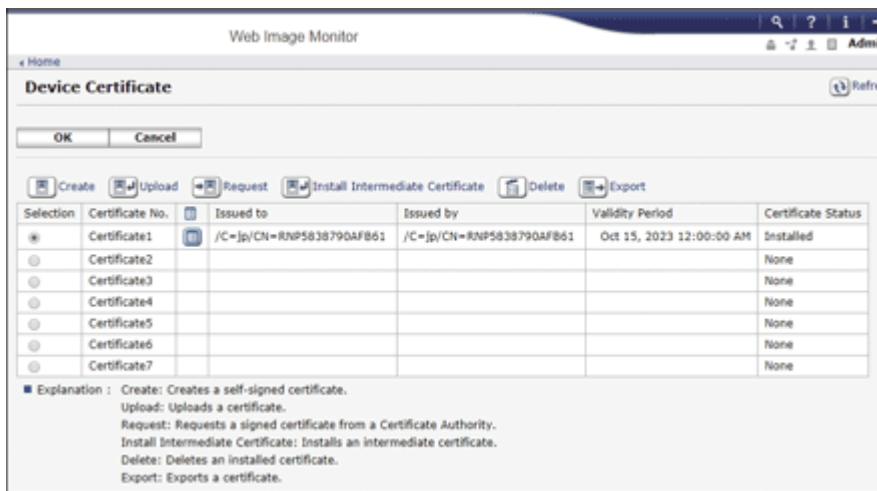
9 Press [Home] ().

Installing a self-signed certificate/certificate issued by a certificate authority from Web Image Monitor

- 1 Log in to the machine as the network administrator from Web Image Monitor.**
- 2 Click [Configuration] from the [Device Management] menu.**



- 3 Click [Device Certificate] in the "Security" category.**
- 4 On the "Device Certificate" screen, install a self-signed certificate or certificate issued by a certificate authority by following the instructions below:**



To install a self-signed certificate

Create and install a self-signed certificate.

1. Select the number from the list to create a self-signed certificate.
2. Click [Create] to specify the necessary settings.
 - Common Name: Enter the name of the device certificate to create. You must enter a name.
 - Email Address: To use the device certificate for S/MIME, PDF Digital Signature, or PDF/A Digital Signature, enter the machine administrator's e-mail address.
 - Enter "Organization", "Organizational Unit", and other items as necessary.
3. Click [OK].


"Installed" is displayed in "Certificate Status".

To install a certificate issued by a certificate authority

Request a device certificate from a certificate authority and install it. Follow the same steps to install an intermediate certificate.

1. Select the number from the list to create a device certificate.
2. Click [Request] to specify the necessary settings.
3. Click [OK].

"Requesting" is displayed in "Certificate Status".
4. Apply to the certificate authority for the device certificate.
 - You cannot apply to the certificate authority from Web Image Monitor. The application procedure varies depending on the certificate authority. For details, contact the certificate authority.

- For the application, click the Details icon  and use the information that appears in "Certificate Details".
- The issuing location may not be displayed if you request multiple certificates at the same time. When you install a certificate, be sure to check the certificate destination and installation procedure.

5. After the device certificate has been issued by the certificate authority, select the number of the issued certificate from the list on the "Device Certificate" screen, and then click [Install].

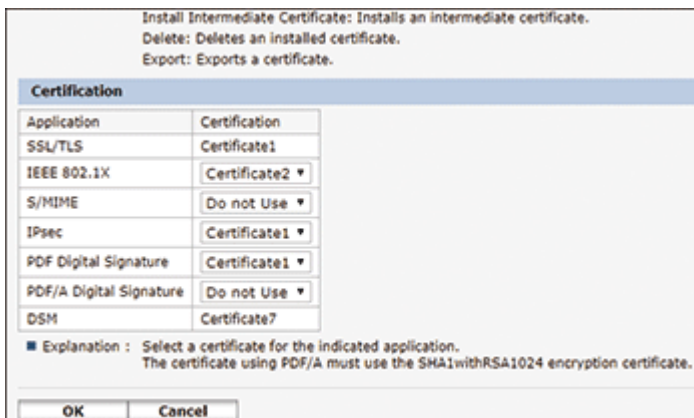
6. Enter the contents of the device certificate in the entry fields.

- To install the intermediate certificate at the same time, enter also the contents of the intermediate certificate.
- If an intermediate certificate issued by a certificate authority is not installed, an alert message is displayed during network communication. When an intermediate certificate has been issued by a certificate authority, you must install the intermediate certificate.

7. Click [OK].

"Installed" is displayed in "Certificate Status".

5 After completing the installation, select the certificate for each application on "Certification".



6 Click [OK].

7 Click [OK] and exit the Web browser.

↓ Note

- To print data in the machine using IPP-SSL, the user must install a certificate in the computer. Select "Trusted Root Certification Authorities" for the certificate store location when accessing the machine by IPP.
- To change "Common Name" of the device certificate when using the Windows standard IPP port, delete any previously configured PC printer beforehand and install the printer driver again. Also, to change the user authentication settings (login user name and password), delete any previously configured PC printer beforehand, change the user authentication settings, and then install the printer driver again.

Encrypting Transmission Using SSL/TLS (Settings Screen Type: Standard)

SSL (Secure Sockets Layer) /TLS (Transport Layer Security) is a method to encrypt network communications. SSL/TLS prevents data from being intercepted, cracked, or tampered.

↓ Note

- To check whether SSL/TLS configuration is enabled, enter "https://(the machine's IP address or host name)/" in your Web browser's address bar to access this machine. If the "The page cannot be displayed" message appears, check the configuration because the current SSL/TLS configuration is invalid.
- If you enable SSL/TLS for IPP (printer functions), sent data is encrypted, preventing it from being intercepted, analyzed, or tampered with.

Flow of SSL/TLS encrypted communications

1. The user's computer requests the SSL/TLS device certificate and public key when accessing the machine.
2. The device certificate and public key are sent from the machine to the user's computer.



3. The shared key created on the computer is encrypted using the public key, sent to the machine, and then decrypted using the private key in the machine.



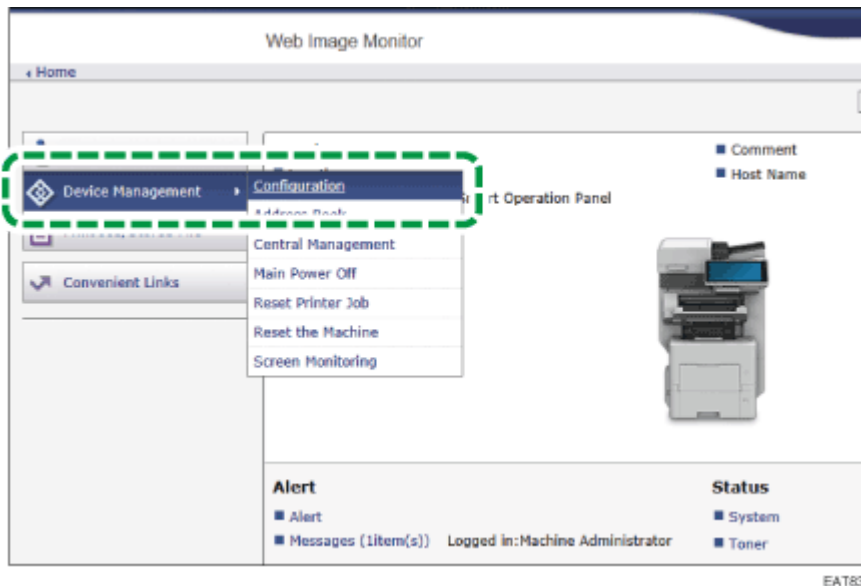
4. The shared key is used for data encryption and decryption, thus achieving secure transmission.



- To enable encrypted communication, install a device certificate in the machine in advance.
- To encrypt communication using SSL/TLS, enable SSL/TLS as follows:

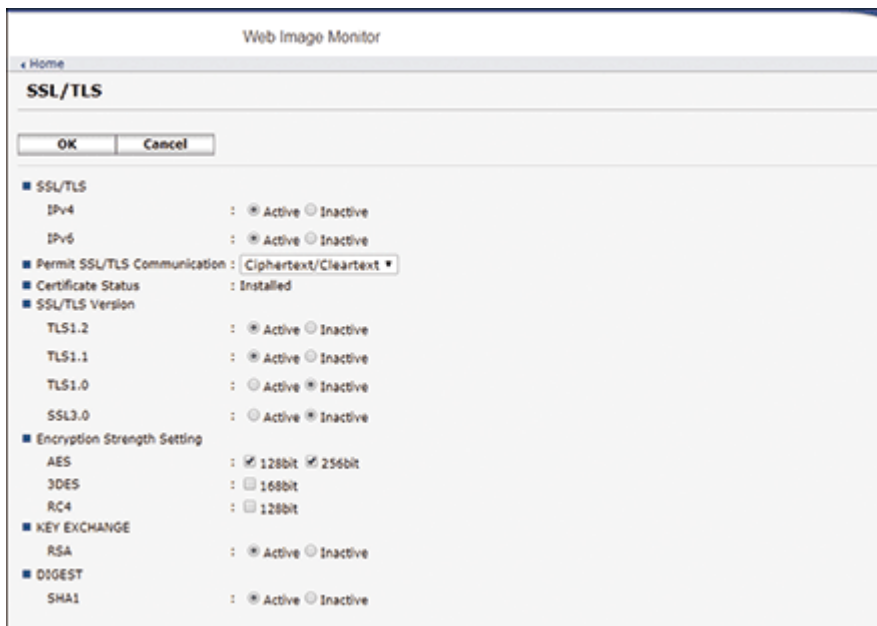
Enabling SSL/TLS

- 1 Log in to the machine as the network administrator from Web Image Monitor.
- 2 Click [Configuration] from the [Device Management] menu.



3 Click [SSL/TLS] in the "Security" category.

4 Select the protocol to enable encrypted communication on "SSL/TLS" to specify the details about the communication method.



- **Permit SSL/TLS Communication:** Select one of the encryption communication modes below:
 - **Ciphertext Priority:** Performs encrypted communication when a device certificate has been created. If encryption is not possible, the machine communicates data in clear text.
 - **Ciphertext/Cleartext:** Performs encrypted communication when connecting to the machine using an "https" address from a Web browser. Communicates in clear text when connecting to the machine using an "http" address.
 - **Ciphertext Only:** Allows encrypted communication only. If encryption is not possible for some reason, the machine cannot communicate. If this is the case, select [System Settings] ► [Network/Interface] ► [Communication Security] ► [Permit SSL/TLS Communication] on the control panel, change the communication mode to [Ciphertext/Cleartext] temporarily, and then check the settings.
- **SSL/TLS Version:** Specify TLS 1.2, TLS 1.1, TLS 1.0, and SSL 3.0 to enable or disable. At least one of these protocols must be enabled.
- **Encryption Strength Setting:** Specify the encryption algorithm to apply to AES, 3DES, and RC4. You must select at least one check box.
- **KEY EXCHANGE:** Specify whether to enable or disable exchanging of the RSA key.
- **DIGEST:** Specify whether to enable or disable SHA-1 DIGEST.

5 Click [OK] and exit the Web browser.

To encrypt communications with the SMTP server, use the following procedure to change "Use Secure Connection (SSL)" to [On].

↓ Note

- Depending on the states you specify for TLS 1.2, TLS 1.1, TLS 1.0, and SSL 3.0, the machine might not be able to connect to an external LDAP server.

Enabling SSL for SMTP connection

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

2 On the Home screen, press [Settings].

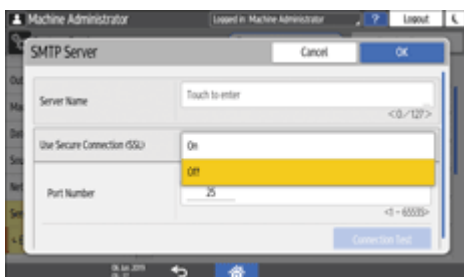


3 On the Settings screen, press [System Settings].



4 Press [Send (Email/Folder)] ► [Email] ► [SMTP Server].

5 From the list next to Use Secure Connection (SSL), select [On].



- After completing the configuration, the port number changes to 465 (SMTP over SSL). When using SMTP over TLS (STARTTLS) for encryption, change the port number to 587.
- When you specify the port number to a number other than 465 and 587, the communication is encrypted according to the setting in the SMTP server.

6 Press [OK].

7 Press [Home] ().

Note

- When SSL is enabled in the SMTP server, Internet fax is always sent via the SMTP server.

Installing a Self-signed Certificate/Certificate Issued by a Certificate Authority (Settings Screen Type: Classic)

To encrypt communication with the machine, install a device certificate.

Two types of device certificates can be used: a self-signed certificate created by the machine and a certificate issued by a certificate authority. When you need higher reliability, use a certificate issued by a certificate authority.



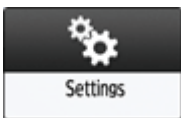
- Install a device certificate from the control panel or Web Image Monitor.

- You can install only one self-signed certificate from the control panel. To install multiple certificates or a certificate issued by a certificate authority, specify the settings from Web Image Monitor.

Installing a self-signed certificate on the control panel

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

2 On the Home screen, press [Settings].



3 On the Settings screen, press [Machine Features Settings].



4 Press [System Settings] ► [Administrator Tools] tab ► [Program / Delete Device Certificate] to display the setting screen.

5 Press [Certificate 1].



6 Specify the necessary settings.



- Common Name: Enter the name of the device certificate to create. You must enter a name.
- Email Address: To use the device certificate for S/MIME, PDF Digital Signature, or PDF/A Digital Signature, enter the machine administrator's e-mail address.
- Enter "Organization", "Organizational Unit", and other items as necessary.

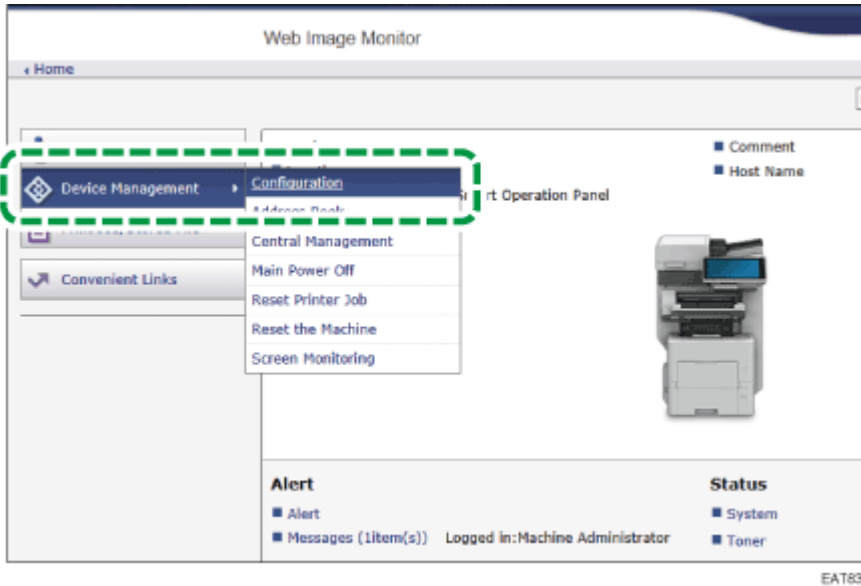
7 Press [OK].

8 Press [Exit].

9 Press [Home] ().

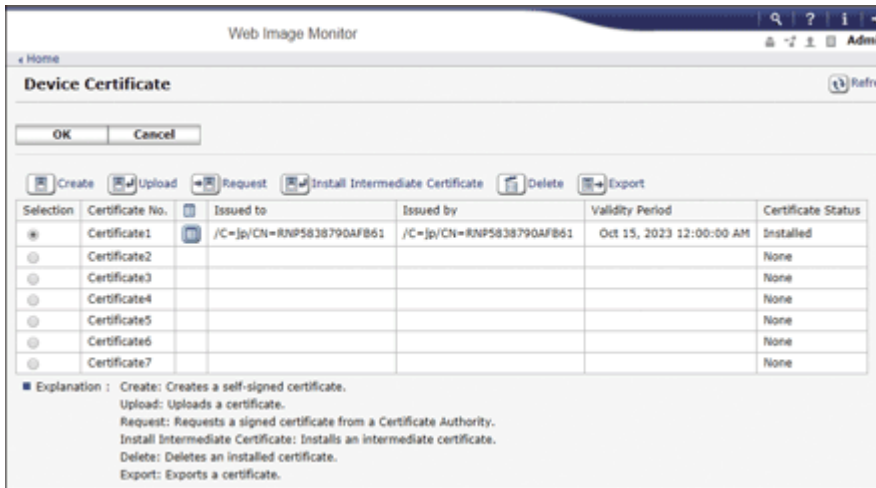
Installing a self-signed certificate/certificate issued by a certificate authority from Web Image Monitor

- 1 Log in to the machine as the network administrator from Web Image Monitor.**
- 2 Click [Configuration] from the [Device Management] menu.**



3 Click [Device Certificate] in the "Security" category.

4 On the "Device Certificate" screen, install a self-signed certificate or certificate issued by a certificate authority by following the instructions below:



To install a self-signed certificate

Create and install a self-signed certificate.

1. Select the number from the list to create a self-signed certificate.
2. Click [Create] to specify the necessary settings.

- Common Name: Enter the name of the device certificate to create. You must enter a name.

- Email Address: To use the device certificate for S/MIME, PDF Digital Signature, or PDF/A Digital Signature, enter the machine administrator's e-mail address.
- Enter "Organization", "Organizational Unit", and other items as necessary.

3. Click [OK].

"Installed" is displayed in "Certificate Status".

To install a certificate issued by a certificate authority

Request a device certificate from a certificate authority and install it. Follow the same steps to install an intermediate certificate.


1. Select the number from the list to create a device certificate.

2. Click [Request] to specify the necessary settings.

3. Click [OK].

"Requesting" is displayed in "Certificate Status".

4. Apply to the certificate authority for the device certificate.

- You cannot apply to the certificate authority from Web Image Monitor. The application procedure varies depending on the certificate authority. For details, contact the certificate authority.
- For the application, click the Details icon  and use the information that appears in "Certificate Details".
- The issuing location may not be displayed if you request multiple certificates at the same time. When you install a certificate, be sure to check the certificate destination and installation procedure.

5. After the device certificate has been issued by the certificate authority, select the number of the issued certificate from the list on the "Device Certificate" screen, and then click [Install].

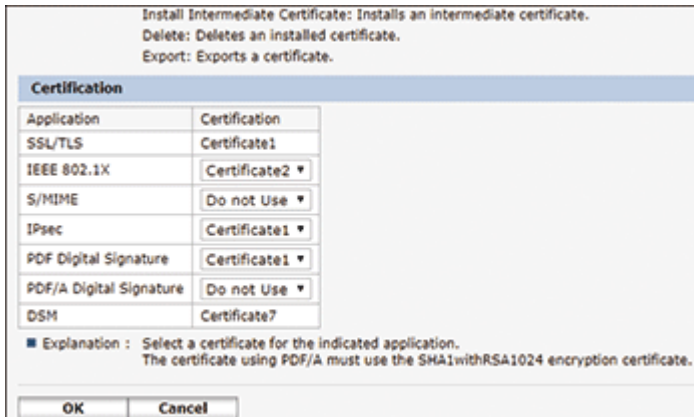
6. Enter the contents of the device certificate in the entry fields.

- To install the intermediate certificate at the same time, enter also the contents of the intermediate certificate.
- If an intermediate certificate issued by a certificate authority is not installed, an alert message is displayed during network communication. When an intermediate certificate has been issued by a certificate authority, you must install the intermediate certificate.

7. Click [OK].

"Installed" is displayed in "Certificate Status".

- 5 After completing the installation, select the certificate for each application on "Certification".**



- 6 Click [OK].**

- 7 Click [OK] and exit the Web browser.**

Note

- To print data in the machine using IPP-SSL, the user must install a certificate in the computer. Select "Trusted Root Certification Authorities" for the certificate store location when accessing the machine by IPP.
- To change "Common Name" of the device certificate when using the Windows standard IPP port, delete any previously configured PC printer beforehand and install the printer driver again. Also, to change the user authentication settings (login user name and password), delete any previously configured PC printer beforehand, change the user authentication settings, and then install the printer driver again.

Encrypting Transmission Using SSL/TLS (Settings Screen Type: Classic)

SSL (Secure Sockets Layer) /TLS (Transport Layer Security) is a method to encrypt network communications. SSL/TLS prevents data from being intercepted, cracked, or tampered.

Note

- To check whether SSL/TLS configuration is enabled, enter "https://(the machine's IP address or host name)/" in your Web browser's address bar to access this machine. If the "The page cannot be displayed" message appears, check the configuration because the current SSL/TLS configuration is invalid.
- If you enable SSL/TLS for IPP (printer functions), sent data is encrypted, preventing it from being intercepted, analyzed, or tampered with.

Flow of SSL/TLS encrypted communications

1. The user's computer requests the SSL/TLS device certificate and public key when accessing the machine.
2. The device certificate and public key are sent from the machine to the user's computer.



3. The shared key created on the computer is encrypted using the public key, sent to the machine, and then decrypted using the private key in the machine.



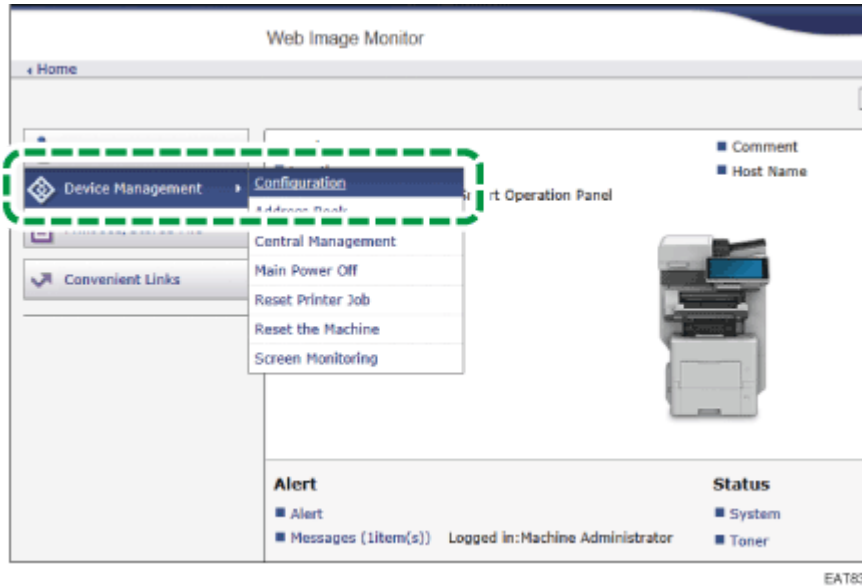
4. The shared key is used for data encryption and decryption, thus achieving secure transmission.



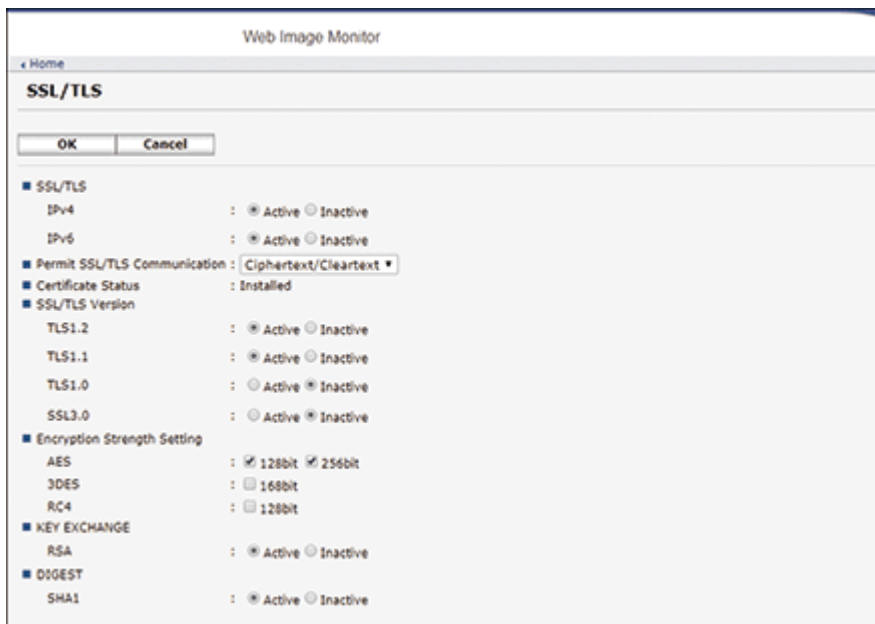
- To enable encrypted communication, install a device certificate in the machine in advance.
- To encrypt communication using SSL/TLS, enable SSL/TLS as follows:

Enabling SSL/TLS

- 1 Log in to the machine as the network administrator from Web Image Monitor.
- 2 Click [Configuration] from the [Device Management] menu.



- 3 Click [SSL/TLS] in the "Security" category.
- 4 Select the protocol to enable encrypted communication on "SSL/TLS" to specify the details about the communication method.



- **Permit SSL/TLS Communication:** Select one of the encryption communication modes below:
 - **Ciphertext Priority:** Performs encrypted communication when a device certificate has been created. If encryption is not possible, the machine communicates data in clear text.
 - **Ciphertext/Cleartext:** Performs encrypted communication when connecting to the machine using an "https" address from a Web browser. Communicates in clear text when connecting to the machine using an "http" address.
 - **Ciphertext Only:** Allows encrypted communication only. If encryption is not possible for some reason, the machine cannot communicate. If this is the case, select [System Settings] ► [Interface Settings] tab ► [Permit SSL/TLS Communication] on the control panel, change the communication mode to [Ciphertext/Cleartext] temporarily, and then check the settings.
- **SSL/TLS Version:** Specify TLS 1.2, TLS 1.1, TLS 1.0, and SSL 3.0 to enable or disable. At least one of these protocols must be enabled.
- **Encryption Strength Setting:** Specify the encryption algorithm to apply to AES, 3DES, and RC4. You must select at least one check box.
- **KEY EXCHANGE:** Specify whether to enable or disable exchanging of the RSA key.
- **DIGEST:** Specify whether to enable or disable SHA-1 DIGEST.

5 Click [OK].

6 Click [OK] and exit the Web browser.

To encrypt communications with the SMTP server, use the following procedure to change "Use Secure Connection (SSL)" to [On].

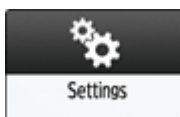
Note

- Depending on the states you specify for TLS 1.2, TLS 1.1, TLS 1.0, and SSL 3.0, the machine might not be able to connect to an external LDAP server.

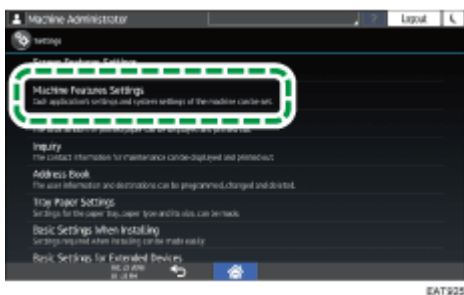
Enabling SSL for SMTP connection

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

2 On the Home screen, press [Settings].



3 On the Settings screen, press [Machine Features Settings].



4 Press [System Settings] ► [File Transfer] tab ► [SMTP Server] to display the setting screen.

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



- After completing the configuration, the port number changes to 465 (SMTP over SSL). When using SMTP over TLS (STARTTLS) for encryption, change the port number to 587.
- When you specify the port number to a number other than 465 and 587, the communication is encrypted according to the setting in the SMTP server.

6 Press [OK].

7 Press [Home] ().



- When SSL is enabled in the SMTP server, Internet fax is always sent via the SMTP server.

Encrypting E-mail Sent from the Machine by S/MIME

S/MIME (Secure/Multipurpose Internet Mail Extensions) is an encryption method to improve security of e-mail communications. By specifying S/MIME, you can send an encrypted e-mail attaching an encrypted file or electronic signature.

★ Important

- To install an S/MIME device certificate, you must first register the administrator's email address as the e-mail address for the device certificate. Note that even if you do not use S/MIME, you must specify an e-mail address for the S/MIME device certificate. You can specify the administrator's email address by pressing the settings shown below.
 - Settings Screen Type: Standard
[System Settings] ► [Send (Email/Folder)] ► [Email] ► [Administrator's Email Address]
 - Settings Screen Type: Classic
[System Settings] ► [File Transfer] tab ► [Administrator's Email Address]
- To create digitally signed PDFs, you must first specify the administrator's email address. You can specify the administrator's email address by pressing the settings shown below.
 - Settings Screen Type: Standard
[System Settings] ► [Send (Email/Folder)] ► [Email] ► [Administrator's Email Address]
 - Settings Screen Type: Classic
[System Settings] ► [File Transfer] tab ► [Administrator's Email Address]
- To use the device certificate for digitally signed PDFs, you must first specify the administrator's e-mail address so that it is the same as that registered as the registered one. You can specify the administrator's email address by pressing the settings shown below.
 - Settings Screen Type: Standard
[System Settings] ► [Send (Email/Folder)] ► [Email] ► [Administrator's Email Address]
 - Settings Screen Type: Classic
[System Settings] ► [File Transfer] tab ► [Administrator's Email Address]



- When you send e-mails to both users whose mail clients support S/MIME and users whose clients does not support it, only e-mails sent to clients supporting S/MIME are encrypted.
- The receiver must use software that supports S/MIME.
- You can apply either an e-mail encryption or electronic signature, or apply both functions together.
- When sending an e-mail attached with an electronic signature, you do not need the user certificate. Install a device certificate, and then specify the electronic signature to attach to the e-mail. For details about installing a device certificate, see the section below:

[Installing a Self-signed Certificate/Certificate Issued by a Certificate Authority \(Settings Screen Type: Standard\)](#)

[Installing a Self-signed Certificate/Certificate Issued by a Certificate Authority \(Settings Screen Type: Classic\)](#)

- For details about using S/MIME with the scanner function, see the section below:

[Applying Security Settings to an E-mail When Sending a Scanned Document](#)

- For details about using S/MIME with the fax function, see the section below:

[Applying Encryption and Using a Signature for Enhanced Security When Sending an Internet Fax](#)

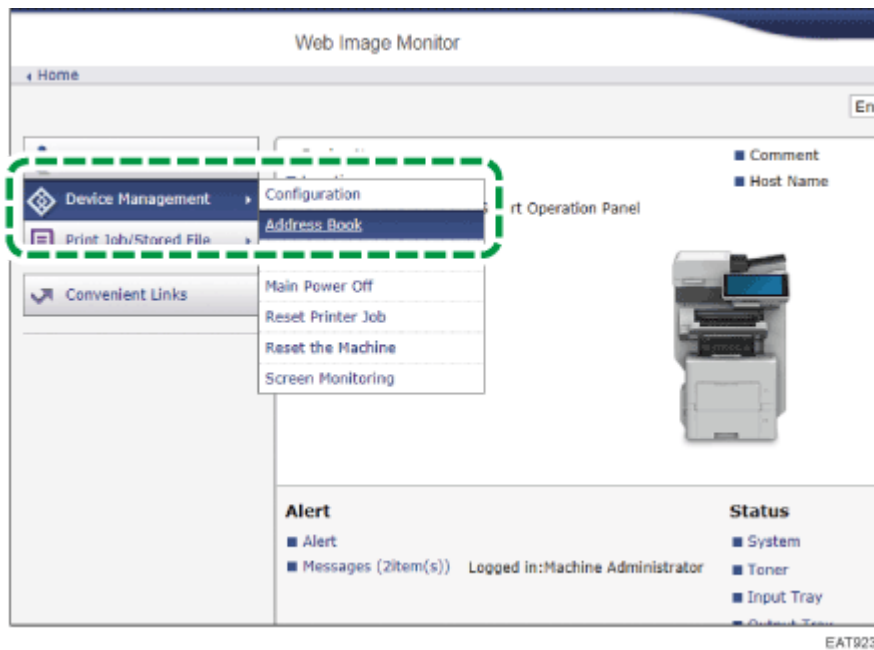
Registering a user certificate to the user that will receive e-mails

To send an encrypted e-mail, first register a user certificate to the user that will receive the e-mail.

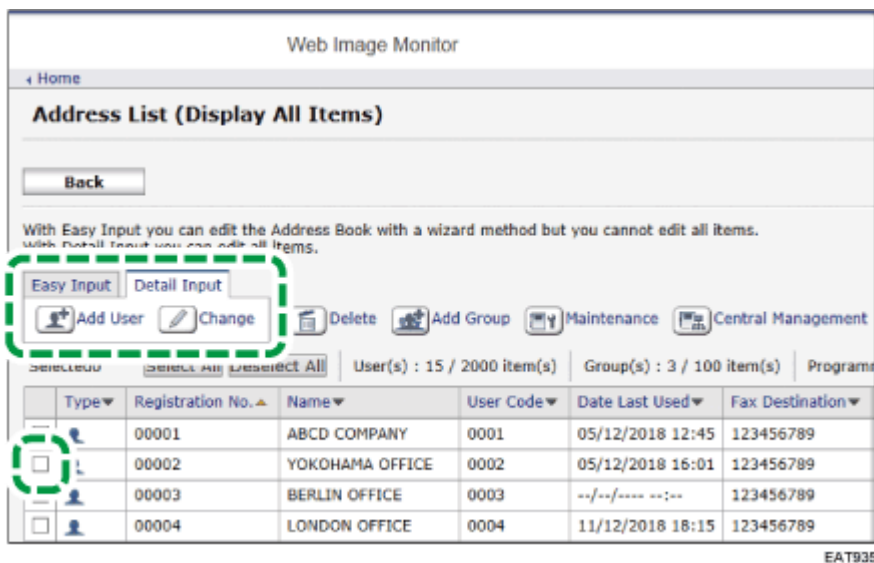
Prepare user certification in advance. You can register three types of user certificates to the machine: "DER Encoded Binary X.509", "Base 64 Encoded X.509", and "PKCS #7 certificate".

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

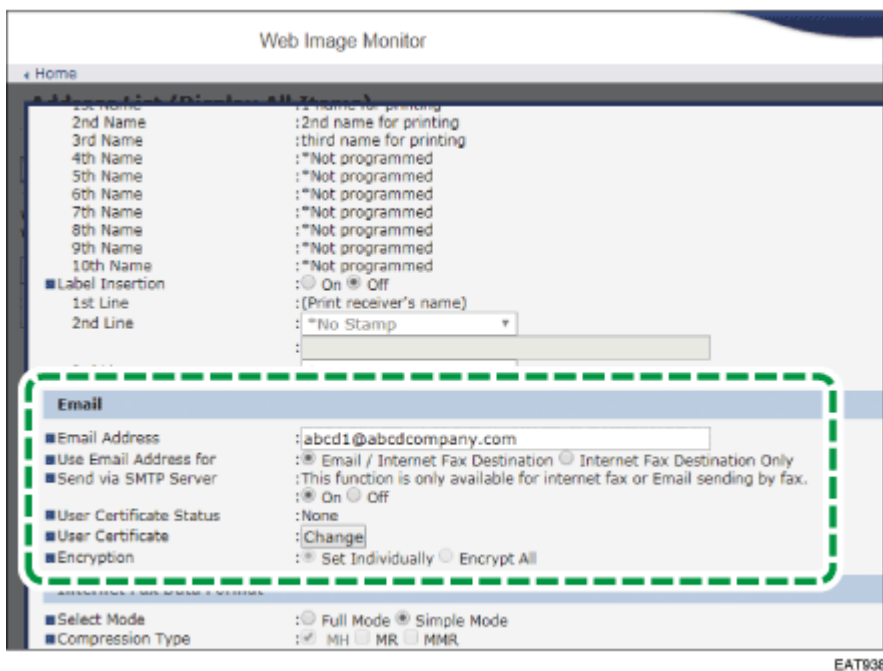
2 Click [Address Book] from the [Device Management] menu.



- 3** Select the user to install the certificate, and then click [Change] on the [Detail Input] tab.



- 4** In the "Email" category, specify the necessary settings.



- Email Address: Enter the e-mail address of the user.
- User Certificate: Click [Change] and specify the user certificate to use.

5 Click [OK].

6 Click [OK] and exit the Web browser.

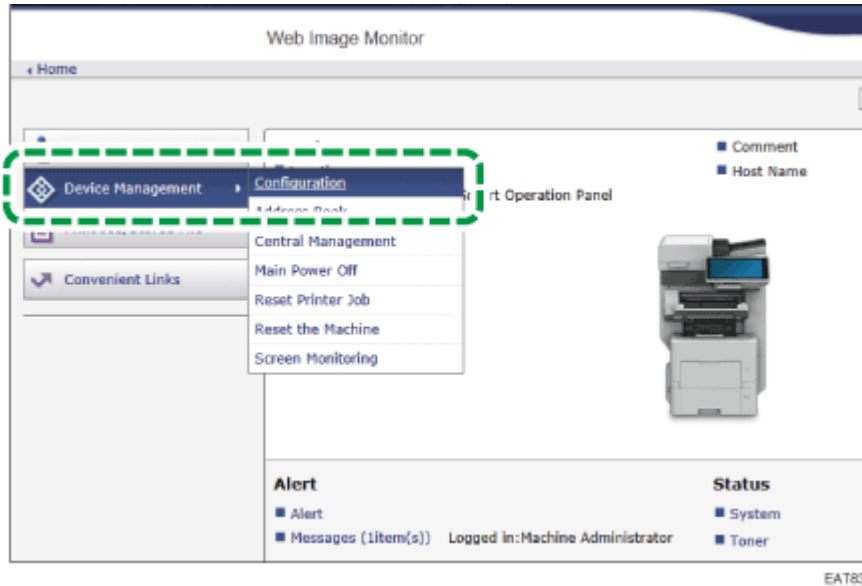
Use the following procedure to specify the details of encryption to be enabled.

Note

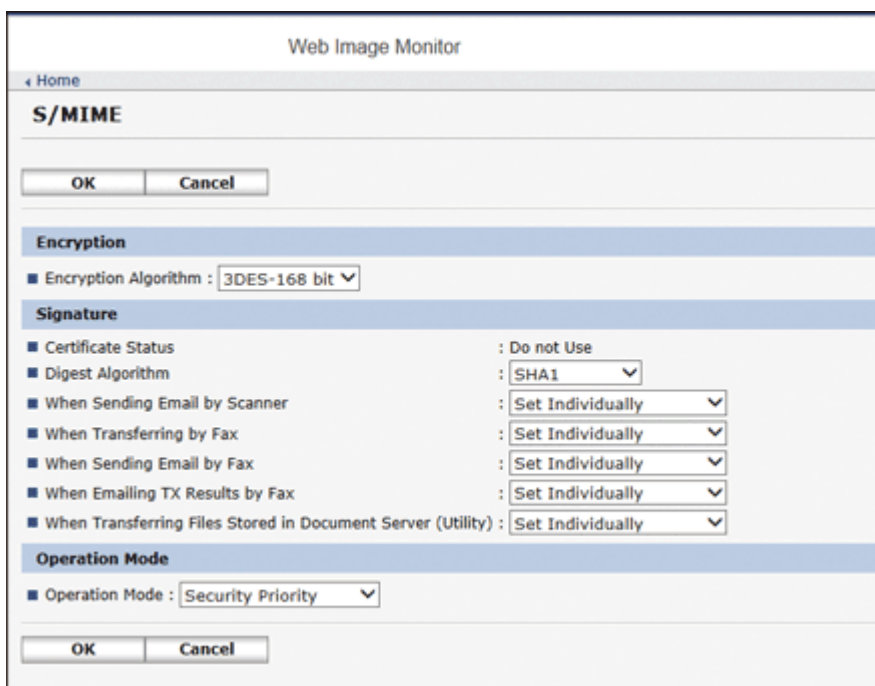
- When installing a user certificate to the Address Book using Web Image Monitor, an error message may appear if the certificate file contains more than one certificate. If this is the case, install the certificates one at a time.
- Once the valid period of the selected user certificate elapses, encrypted messages can no longer be sent. Select a certificate that is within its valid period.

Configuring the encryption algorithm and attachment of an electronic signature

- 1 Log in to the machine as the network administrator from Web Image Monitor.
- 2 Click [Configuration] from the [Device Management] menu.



- 3 Click [S/MIME] in the "Security" category.
- 4 Configure the e-mail encryption and electronic signature.



Encryption

- **Encryption Algorithm:** Select the encryption algorithm of the shared key used to encrypt e-mails with S/MIME. Select the encryption algorithm that is supported by the user's e-mail software.

Signature

- **Certificate Status:** The certificate specified for S/MIME is displayed.
- **Digest Algorithm:** Select the digest algorithm to use for the electronic signature.
- **When Sending Email by Scanner, When Transferring by Fax, When Sending Email by Fax, When Emailing TX Results by Fax, When Transferring Files Stored in Document Server (Utility):** Specify whether to select the method for attaching an electronic signature in each function when sending or transferring e-mails or documents.

Operation Mode

- **Operation Mode:** Select the timing at which the validity period of a certificate is checked.
 - **Performance Priority:** The validity period of a user certificate is checked when you select the address. The validity period of a device certificate is checked when you press [Start]. It does not meet the International Evaluation Regulations for Information Security (CC Authentication), but it responds to the user quicker than when [Security Priority] is selected.
 - **Security Priority:** The validity period is checked when you select the address and when you press [Start]. It takes some time to respond to the user and performs properly under the conditions that meet the International Evaluation Regulations for Information Security (CC Authentication).

5 Click [OK].

6 Click [OK] and exit the Web browser.

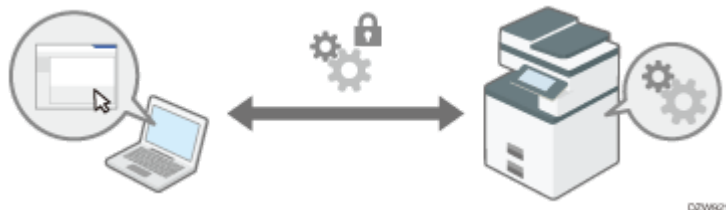
Note

- If a certificate was valid when transmitted but has expired before the e-mail is retrieved from the mail server to the client computer, the e-mail may not be retrieved.
- When attaching an electronic signature to an e-mail, the e-mail address of the administrator is used in "From", and the e-mail address of the user selected as "Sender" is used in "Reply-To".

- If an error occurs outside the validity period of the certificate when an e-mail is sent automatically using Memory Transmission or at a specified time, an error will be reported by clear text e-mail to the e-mail address of the sender or administrator. When the job log collection function is enabled, you can view the error details in the job log.
 - Settings screen type: Standard
[Collecting Logs](#)
 - Settings screen type: Classic
[Collecting Logs](#)
- If the selected device certificate expires, signatures cannot be attached to PDFs. Select a certificate that is within its valid period.
- The signature algorithm for the device certificate's digital signature that can be attached to PDF/A files is "sha1WithRSA-1024".

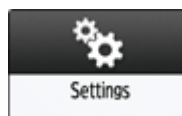
Encrypting Data Communicated with Machine Management Software Via SNMPv3 (Settings Screen Type: Standard)

When monitoring devices using Device Manager NX via a network, you can encrypt the transmitted data by using the SNMPv3 protocol.



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

2 On the Home screen, press [Settings].

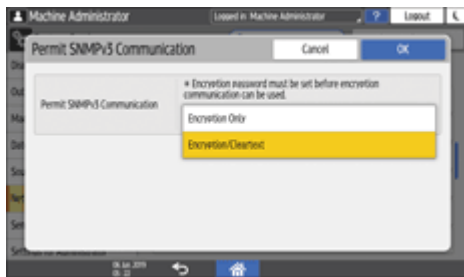


3 On the Settings screen, press [System Settings].



4 Press [Network/Interface] ► [Permit SNMPv3 Communication].

5 From the list next to Permit SNMPv3 Communication, select [Encryption Only].



6 Press [OK].

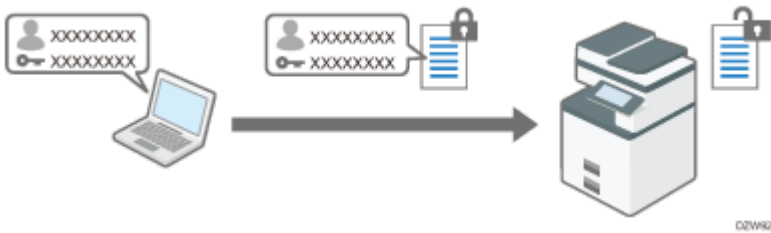
7 Press [Home] ().

Note

- To change the settings specified in the machine from Device Manager NX, specify an encryption password to the network administrator in [Register/Change Administrator], and then register the encryption password in the SNMP account of Device Manager NX.

Encrypting the Login Password of Print Jobs (Settings Screen Type: Standard)

You can encrypt the login password for the printer driver and the password for IPP printing to increase security against password cracking.



- To perform printing from a LAN inside the office, specify the driver encryption key.
- To perform IPP printing from an external network, encrypt the password of IPP printing.

Specifying a Driver Encryption Key to Encrypt Passwords

Specify the driver encryption key specified in the machine also to the printer driver to encrypt and decrypt passwords.

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

2 On the Home screen, press [Settings].



3 On the Settings screen, press [System Settings].



4 Press [Settings for Administrator] ► [Security] ► [Extended Security Settings].

5 Press [Change] next to Driver Encryption Key.



6 Enter the password to be used as the driver encryption key, and then press [Done].

7 Enter the password for Confirm Password again, and then press [Done].

8 Press [OK] twice.

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

10 The network administrator must give users the driver encryption key specified on the machine so they can register it on their computers.

- Make sure to enter the same driver encryption key as that specified on the machine.
- When using a PCL 6 printer driver, you can enter the driver encryption key on [Printer Properties] ► the [Advanced Options] tab.

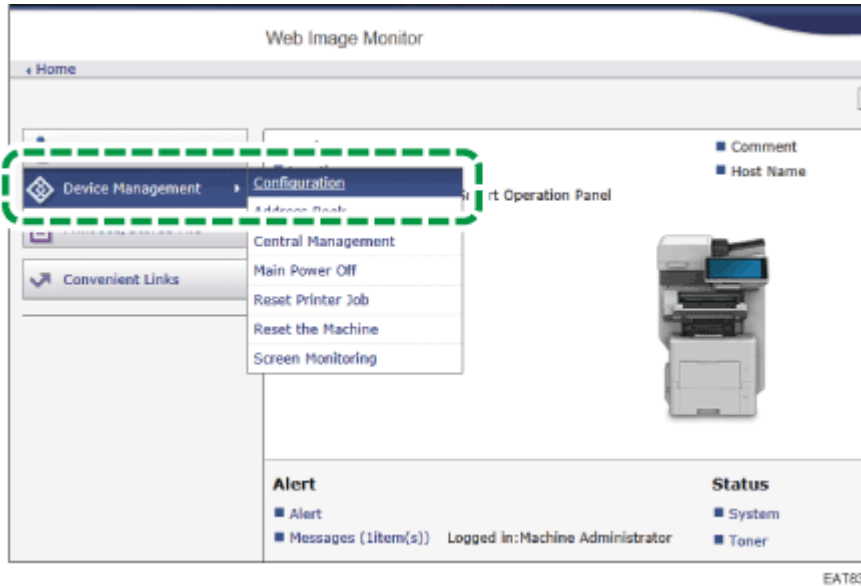
 **Note**

- You can also encrypt the print job itself. For details, see the section below:
Storing Documents to Print in the Machine

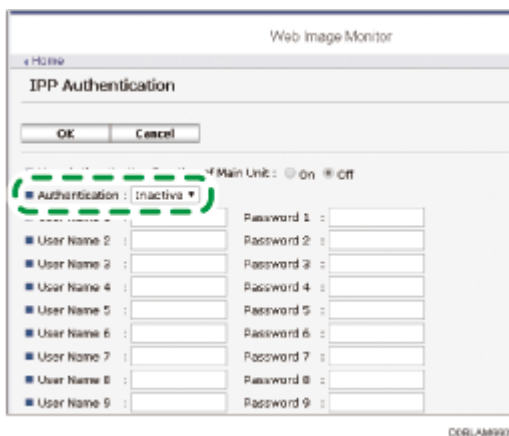
Encrypting the password of IPP printing

When printing using the IPP protocol, specify the authentication method to [DIGEST] to encrypt the IPP authentication password. Register the user name and password for IPP authentication separately from the user information in the address book.

- 1 Log in to the machine as the network administrator from Web Image Monitor.
- 2 Click [Configuration] from the [Device Management] menu.



- 3 Click [IPP Authentication] in the "Security" category.
- 4 Select "DIGEST" in "Authentication".



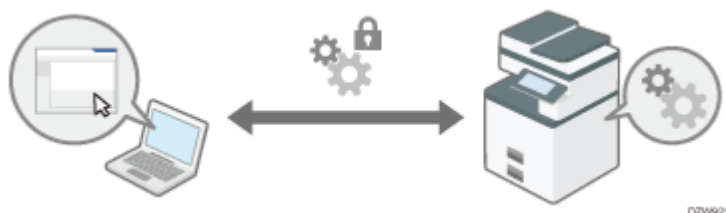
Click [On] of "User Authentication Function of Main Unit" to use the user authentication information specified on the machine instead of the user name and password for IPP authentication.

- 5 Enter User Name and Password.

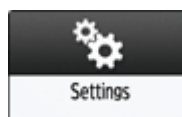
- 6 Click [OK] and exit the Web browser.

Encrypting Data Communicated with Machine Management Software Via SNMPv3 (Settings Screen Type: Classic)

When monitoring devices using Device Manager NX via a network, you can encrypt the transmitted data by using the SNMPv3 protocol.



- 1 Log in to the machine as the network administrator on the control panel.
- 2 On the Home screen, press [Settings].



- 3 On the Settings screen, press [Machine Features Settings].



- 4 Press [System Settings] ► [Interface Settings] tab ► [Permit SNMPv3 Communication] to display the setting screen.

5 Press [Encryption Only].



6 Press [OK].

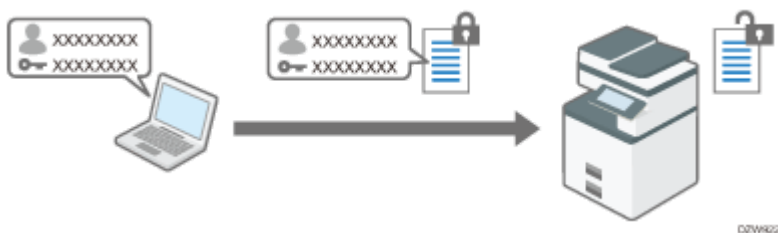
7 Press [Home] ().

Note

- To change the settings specified in the machine from Device Manager NX, specify an encryption password to the network administrator in [Program / Change Administrator], and then register the encryption password in the SNMP account of Device Manager NX.

Encrypting the Login Password of Print Jobs (Settings Screen Type: Classic)

You can encrypt the login password for the printer driver and the password for IPP printing to increase security against password cracking.



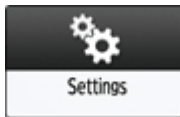
- To perform printing from a LAN inside the office, specify the driver encryption key.
- To perform IPP printing from an external network, encrypt the password of IPP printing.

Specifying a Driver Encryption Key to Encrypt Passwords

Specify the driver encryption key specified in the machine also to the printer driver to encrypt and decrypt passwords.

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

2 On the Home screen, press [Settings].



3 On the Settings screen, press [Machine Features Settings].



4 Press [System Settings] ► [Administrator Tools] tab ► [Extended Security] to display the setting screen.

5 Press [Change] for "Driver Encryption Key".



6 Enter a character string to use as the driver encryption key, and then press [OK].

7 Press [OK].

8 Press [Home] ().

9 The network administrator must give users the driver encryption key specified on the machine so they can register it on their computers.

- Make sure to enter the same driver encryption key as that specified on the machine.
- When using a PCL 6 printer driver, you can enter the driver encryption key on [Printer Properties] ► [Advanced Options] tab.

 **Note**

- You can also encrypt the print job itself. For details, see the section below:

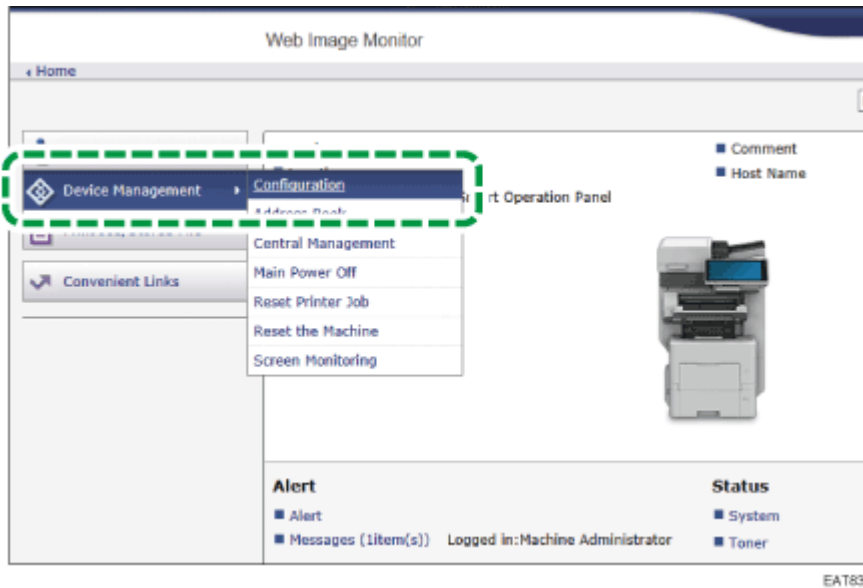
Storing Documents to Print in the Machine

Encrypting the password of IPP printing

When printing using the IPP protocol, specify the authentication method to [DIGEST] to encrypt the IPP authentication password. Register the user name and password for IPP authentication separately from the user information in the address book.

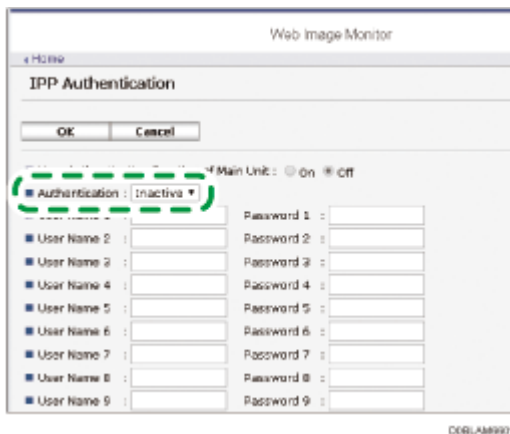
1 Log in to the machine as the network administrator from Web Image Monitor.

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



3 Click [IPP Authentication] in the "Security" category.

4 Select "DIGEST" in "Authentication".



Click [On] of "User Authentication Function of Main Unit" to use the user authentication information specified on the machine instead of the user name and password for IPP authentication.

5 Enter User Name and Password.

6 Click [OK] and exit the Web browser.

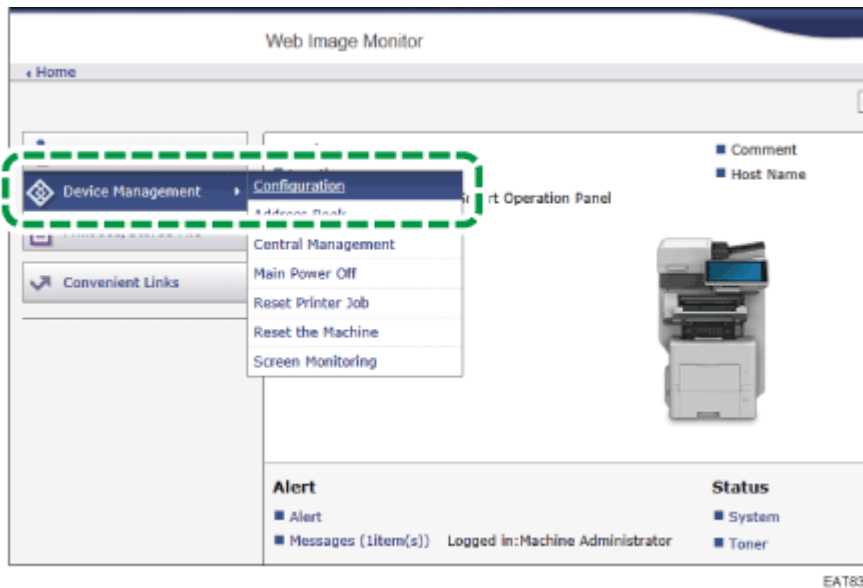
Encrypting Communication Between KDC and the Machine

You can encrypt communications between the machine and the Key Distribution Center (KDC) server when using Kerberos authentication with Windows or LDAP authentication to secure communication.

The supported encryption algorithm differs depending on the type of KDC server.

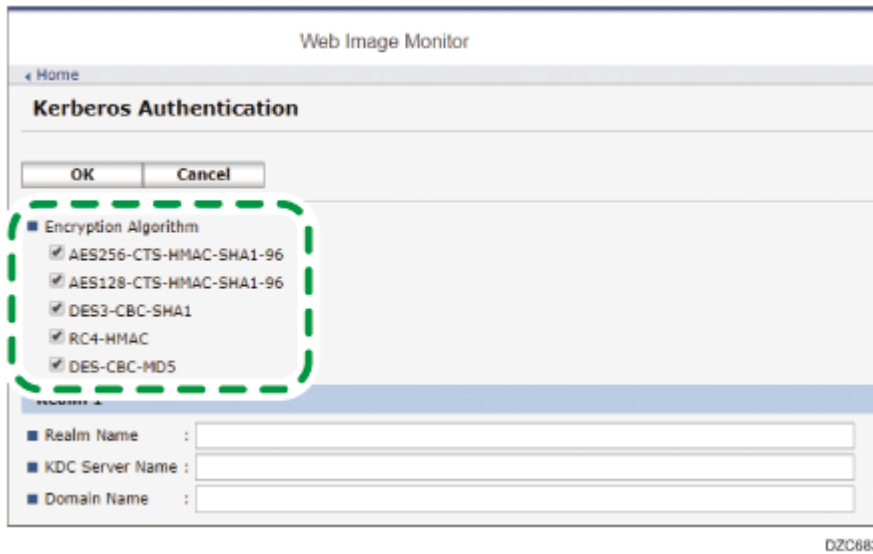
1 Log in to the machine as the machine administrator from Web Image Monitor.

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



3 Click [Kerberos Authentication] of the "Device Settings" category.

4 Select the encryption algorithm to enable.



- Only Heimdal supports DES3-CBC-SHA1.
- To use DES-CBC-MD5 in Windows Server 2008 R2 or later, enable it in the operating system settings.

5 Click [OK] and exit the Web browser.

[Page Top](#)

Copyright © 2019, 2020, 2022