Operating Instructions

Security Reference

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

Introduction

This manual contains detailed instructions and notes on the operation and use of this machine. For your safety and benefit, read this manual carefully before using the machine. Keep this manual in a handy place for quick reference.

Do not copy or print any item for which reproduction is prohibited by law.

Copying or printing the following items is generally prohibited by local law:

bank notes, revenue stamps, bonds, stock certificates, bank drafts, checks, passports, driver's licenses.

The preceding list is meant as a guide only and is not inclusive. We assume no responsibility for its completeness or accuracy. If you have any questions concerning the legality of copying or printing certain items, consult with your legal advisor.

Important

Contents of this manual are subject to change without prior notice. In no event will the company be liable for direct, indirect, special, incidental, or consequential damages as a result of handling or operating the machine.

Trademarks

Microsoft®, Windows® and Windows NT® are registered trademarks of Microsoft Corporation in the United States and/or other countries.

AppleTalk, EtherTalk, Rendezvous are registered trademarks of Apple Computer, Inc.

Other product names used herein are for identification purposes only and might be trademarks of their respective companies. We disclaim any and all rights to those marks.

The proper names of the Windows operating systems are as follows:

- The product name of Windows® 95 is Microsoft® Windows 95.
- The product name of Windows® 98 is Microsoft® Windows 98.
- The product name of Windows® Me is Microsoft® Windows Millennium Edition (Windows Me).
- The product names of Windows® 2000 are as follows:
  Microsoft® Windows® 2000 Advanced Server
  Microsoft® Windows® 2000 Server
  Microsoft® Windows® 2000 Professional
- The product names of Windows® XP are as follows:
  Microsoft® Windows® XP Professional
  Microsoft® Windows® XP Home Edition
- The product names of Windows Server™ 2003 are as follows:
  Microsoft® Windows Server™ 2003 Standard Edition
  Microsoft® Windows Server™ 2003 Enterprise Edition
  Microsoft® Windows Server™ 2003 Web Edition
- The product names of Windows NT® 4.0 are as follows:
  Microsoft® Windows NT® Server 4.0
  Microsoft® Windows NT® Workstation 4.0

Notes

Some illustrations in this manual might be slightly different from the machine.

Certain options might not be available in some countries. For details, please contact your local dealer.

Manuals for This Machine

The following manuals describe the operational procedures of this machine. For particular functions, see the relevant parts of the manual.

Note

❒ Manuals provided are specific to machine type.

❒ Adobe Acrobat Reader / Adobe Reader is necessary to view the manuals as a PDF file

❒ Two CD-ROMs are provided:

- CD-ROM 1 “Operating Instructions”
- CD-ROM 2 “Scanner Driver and Utilities”

❖ **General Settings Guide**

Provides an overview of the machine and describes System Settings (such as Tray Paper Settings), Document Server functions, and troubleshooting.
Refer to this manual for Address Book procedures such as registering e-mail addresses and user codes.

❖ **Security Reference (this manual)**

This manual is for administrators of this machine. It describes security functions that the administrators can use to protect data from being tampered, or prevent the machine from unauthorized use. Also refer to this manual for the procedures for registering administrators, as well as setting user and administrator authentication.

❖ **Network Guide (PDF file - CD-ROM1)**

Provides information about configuring and operating the scanner (Type 480) in a network environment.
For details about network settings of the scanner (RW480) and printer (RW480), see the manual that comes with the related option.

❖ **Copy Reference**

Describes operations, functions, and troubleshooting for the machine's copier function.

❖ **Scanner Reference (Scanner Unite Type 480) (PDF file - CD-ROM1)**

Describes operations, functions, and troubleshooting for the machine's scanner function.

❖ Manuals for DeskTopBinder Lite

DeskTopBinder Lite is a utility included on the CD-ROM labeled “Scanner Driver and Utilities”.

- DeskTopBinder Lite Setup Guide (PDF file - CD-ROM2)
  Describes installation of, and the operating environment for DeskTop-Binder Lite in detail. This guide can be displayed from the **[Setup]** display when DeskTopBinder Lite is installed.
- DeskTopBinder Lite Introduction Guide (PDF file - CD-ROM2)
  Describes operations of DeskTopBinder Lite and provides an overview of its functions. This guide is added to the **[Start]** menu when DeskTopBinder Lite is installed.
- Auto Document Link Guide (PDF file - CD-ROM2)
  Describes operations and functions of Auto Document Link installed with DeskTopBinder Lite. This guide is added to the **[Start]** menu when Desk-TopBinder Lite is installed.

❖ Other manuals

- Manuals for Printer (RW480) function
- Manuals for Scanner (RW480) function

TABLE OF CONTENTS

5. Management Based on Authentication and Access Control

6. Specifying the Administrator/Security Functions

7. Troubleshooting

8. Appendix

How to Read This Manual

Symbols

The following set of symbols is used in this manual.

⚠ ***WARNING:***
This symbol indicates a potentially hazardous situation that might result in death or serious injury when you misuse the machine without following the instructions under this symbol. Be sure to read the instructions, all of which are described in the Safety Information section.

⚠ ***CAUTION:***
This symbol indicates a potentially hazardous situation that might result in minor or moderate injury or property damage that does not involve personal injury when you misuse the machine without following the instructions under this symbol. Be sure to read the instructions, all of which are described in the Safety Information section.

* The statements above are notes for your safety.

Important
If this instruction is not followed, paper might be misfed, originals might be damaged, or data might be lost. Be sure to read this.

Preparation
This symbol indicates information or preparations required prior to operating.

Note
This symbol indicates precautions for operation, or actions to take after abnormal operation.

Limitation
This symbol indicates numerical limits, functions that cannot be used together, or conditions in which a particular function cannot be used.

Reference
This symbol indicates a reference.

[ ]
Keys that appear on the machine's display panel.

[ ]
Keys and buttons that appear on the computer's display.

【 】
Keys built into the machine's control panel.

【 】
Keys on the computer's keyboard.

Enhanced Security

This machine's security function can be enhanced through the management of the machine and its users using the improved authentication functions.

By specifying access limits on the machine's functions and the documents and data stored in the machine, you can prevent information leaks and unauthorized access.

Data encryption can prevent unauthorized data access and tampering via the network.

❖ **Authentication and Access Limits**

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

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

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

Reference

For details, see p.67 "The Roles of Administrators".

❖ **Encryption Technology**

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

Glossary

❖ **Administrator**
Administrators manage a specific area of machine usage, such as settings or user registration.
There are four types of administrator: user administrator, network administrator, machine administrator, and file administrator. One person can act as more than one type of administrator.
Basically, administrators make machine settings and manage the machine; they cannot perform normal operations, such as copying.

❖ **User**
A user performs normal operations on the machine, such as copying.

❖ **File Creator (Owner)**
This is a user who can store files in the machine and authorize other users to view, edit, or delete those files.

❖ **Registered User**
This is a user whose personal information is registered in the address book. The registered user is the user who knows the login user name and password.

❖ **Administrator Authentication**
Administrators are authenticated by means of the login user name and login password supplied by the administrator when specifying the machine's settings or accessing the machine over the network.

❖ **User Authentication**
Users are authenticated by means of the login user name and login password supplied by the user when specifying the machine's settings or accessing the machine over the network.

❖ **Login**
This action is required for administrator authentication and user authentication. Enter your login user name and login password on the machine's control panel.
A login user name and login password may also be supplied when accessing the machine over the network or using such utilities as Web Image Monitor and SmartDeviceMonitor for Admin.

❖ **Logout**
This action is required with administrator and user authentication. This action is required when you have finished using the machine or changing the settings.

Security Measures Provided by this Machine

Preventing Information Leaks

❖ **Protecting Stored Files from Unauthorized Access**

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

Reference

For details, see p.9 “Specifying Access Permission for Stored Files”.

❖ **Protecting Stored Files from Theft**

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

Reference

For details, see p.9 “Specifying Access Permission for Stored Files”.

❖ **Preventing Data Leaks Due to Unauthorized Transmission**

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

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

Reference

For details, see p.16 “Preventing Data Leaks Due to Unauthorized Transmission”.

❖ **Protecting Registered Information in the Address Book**

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

To protect the data from unauthorized reading, you can also encrypt the data in the address book.

Note

❒ To encrypt the data in the address book, the machine must have the scanner function.

Reference

For details, see p.18 “Protecting the Address Book”.

❖ **Overwriting the Data on the Hard Disk**

You can overwrite data on the hard disk.

Reference

For details, see p.22 “Overwriting the Data on the Hard Disk”.

1

Preventing Unauthorized Operation

❖ **Preventing Modification or Deletion of Stored Data**

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

You can permit selected users who are allowed to access stored files to modify or delete the files.

Reference

For details, see p.9 “Specifying Access Permission for Stored Files”.

❖ **Preventing Modification of Machine Settings**

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

Register the administrators so that users cannot change the administrator settings.

Reference

For details, see p.27 “Preventing Modification of Machine Settings”.

❖ **Limiting Available Functions**

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

Reference

For details, see p.28 “Limiting Available Functions”.

Enhanced Network Security

❖ **Preventing Unauthorized Access**

You can limit IP addresses or disable ports to prevent unauthorized access over the network and protect the address book, stored files, and default settings.

Reference

For details, see p.31 “Preventing Unauthorized Access”.

❖ **Encrypting Transmitted Passwords**

Prevent login passwords, group passwords for PDF files, and IPP authentication passwords being revealed by encrypting them for transmission.
Also, encrypt the login password for administrator authentication and user authentication.

Note

❒ To encrypt transmitted passwords, the machine must have the scanner function.

Reference

For details, see p.34 “Encrypting Transmitted Passwords”.

❖ **Safer Communication Using SSL**

When you access the machine using a Web browser or IPP, you can establish encrypted communication using SSL. When you access the machine using an application such as SmartDeviceMonitor for Admin, you can establish encrypted communication using SNMPv3 or SSL.
To protect data from interception, analysis, and tampering, you can install a server certificate in the machine, negotiate a secure connection, and encrypt transmitted data.

Note

❒ To establish encrypted communication using SSL, the machine must have the scanner function.

Reference

For details, see p.37 “Protection Using Encryption”.

2. Preventing Information Leaks

Specifying Access Permission for Stored Files

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

You can prevent activities such as the sending of stored files by unauthorized users.

❖ **Access Permission**

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

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

Note

❒ Files can be stored by any user who is allowed to use the Document Server or scanner function.

❒ Using Web Image Monitor, you can check the content of stored files. For details, see the Web Image Monitor Help.

❒ The default access permission for the file creator (owner) is "Read-only".

❖ **Password for Stored Files**

Passwords for stored files can be specified by the file creator (owner) or file administrator.

You can obtain greater protection against the unauthorized use of files.

Assigning Users and Access Permission for Stored Files

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

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

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

2

Preparation

For details about logging on with administrator authentication, see p.73 “Logging on Using Administrator Authentication”.

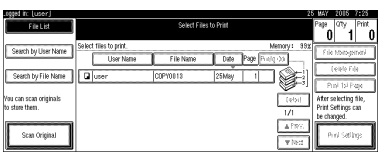
For details about logging off with administrator authentication, see p.74 “Logging off Using Administrator Authentication”.

Important

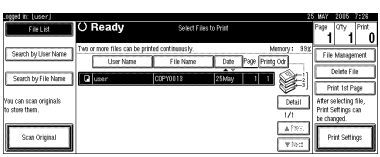
❒ If files become inaccessible, reset their access permission as the file creator (owner). This can also be done by the file administrator. If you want to access a file but do not have access permission, ask the file creator (owner).

1 **Press the [Document Server] key.**

2 **Select the file.**



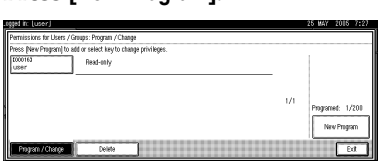
3 **Press [File Management].**



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

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

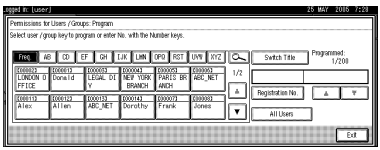
6 **Press [New Program].**



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

You can select more than one users.

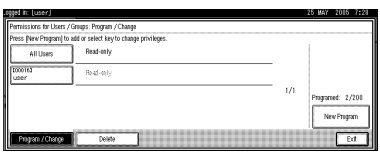
By pressing **[All Users]**, you can select all the users.



8 Press [Exit].

9 Select the user who you want to assign an access permission to, and then select the permission.

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



10 Press [Exit].

11 Press [OK].

12 Press [OK].

Assigning the User and the Access Permission for the User's Stored Files

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

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

Only those users granted access permission can access stored files.

This makes the management of access permission easier than it is when permission is specified for each stored file.

Preparation

For details about logging on with administrator authentication, see p.73 "Logging on Using Administrator Authentication".

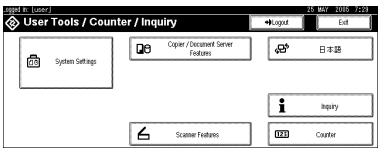
For details about logging off with administrator authentication, see p.74 "Logging off Using Administrator Authentication".

Important

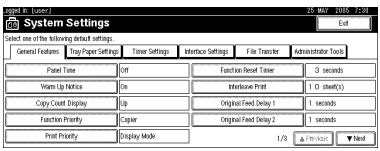
❒ If files become inaccessible, be sure to enable the user administrator, and then reset the access permission for the files in question.

1 **Press the 【User Tools/Counter】 key.**

2 **Press [System Settings].**



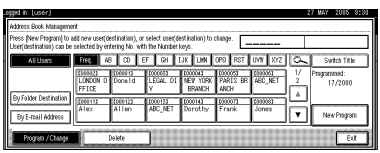
3 **Press [Administrator Tools].**



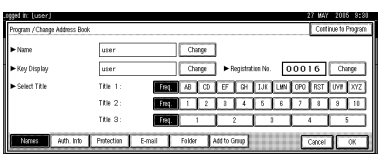
4 **Press [Address Book Management].**

If it does not appear, press **[▼Next]**.

5 **Select the user or group.**



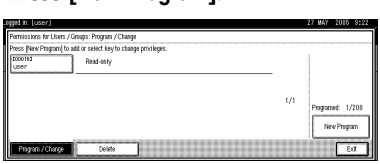
6 **Press [Protection].**



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

If it does not appear, press **[▼Next]**.

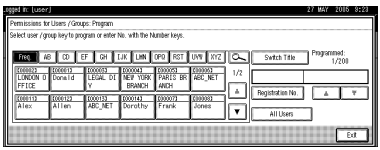
8 **Press [New Program].**



9 **Select the users or groups to register.**

You can select more than one users.

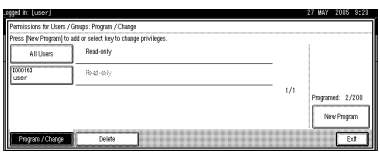
By pressing **[All Users]**, you can select all the users.



10 **Press [Exit].**

11 **Select the user who you want to assign an access permission to, and then select the permission.**

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



12 **Press [Exit].**

13 **Press [OK].**

14 **Press [Exit].**

15 **Press the 【User Tools/Counter】 key.**

Specifying Passwords for the Stored Files

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

Specify passwords for the stored files.

Provides increased protection against unauthorized use of files.

2

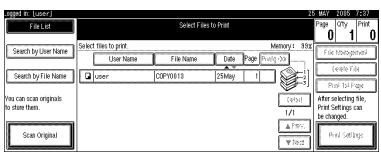
Preparation

For details about logging on with administrator authentication, see p.73 “Logging on Using Administrator Authentication”.

For details about logging off with administrator authentication, see p.74 “Logging off Using Administrator Authentication”.

1 **Press the 【Document Server】 key.**

2 **Select the file.**



3 **Press [File Management].**

4 **Press [Change Password].**

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

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

6 **Press [Change] at the bottom of the screen.**

7 **Confirm the password by re-entering it using the number keys.**

8 **Press [#].**

9 **Press [OK].**

10 **Press [OK].**

Unlocking Files

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

Only the file administrator can unlock files.

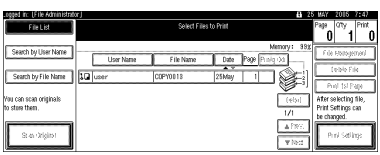
For details about “Enhance File Protection”, see p.76 “Specifying the Extended Security Functions”.

Preparation

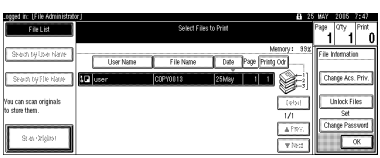
For details about logging on with administrator authentication, see p.73 “Logging on Using Administrator Authentication”.

For details about logging off with administrator authentication, see p.74 “Logging off Using Administrator Authentication”.

1. **Press the 【Document Server】 key.**
2. **Select the file.**



3. **Press [File Management].**
4. **Press [Unlock Files].**



5. **Press [Yes].**
6. **Press [OK].**

Preventing Data Leaks Due to Unauthorized Transmission

If user authentication is specified, the user who has logged on can be designated as the sender to prevent unauthorized access.

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

Restrictions on Destinations

This can be specified by the user administrator.

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

By making this setting, the destinations can be restricted to addresses registered in the address book.

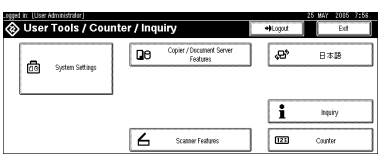
Preparation

For details about logging on with administrator authentication, see p.73 “Logging on Using Administrator Authentication”.

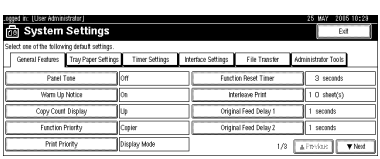
For details about logging off with administrator authentication, see p.74 “Logging off Using Administrator Authentication”.

1 **Press the 【User Tools/Counter】 key.**

2 **Press [System Settings].**

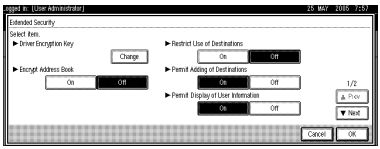


3 **Press [Administrator Tools].**



4 **Press [Extended Security].**

5 **Press [On] for "Restrict Use of Destinations".**



Note

- ❒ If you set "Restrict Use of Destinations" to **[Off]**, "Permit Adding of Destinations" appears.
- ❒ If you set "Permit Adding of Destinations" to **[On]**, the user can register destinations by entering them directly.
- ❒ If you set "Permit Adding of Destinations" to **[Off]**, the user cannot register destinations by entering them directly.
- ❒ If you set "Permit Adding of Destinations" to **[Off]**, you cannot make changes to the address book.

6 **Press [OK].**

7 **Press the 【User Tools/Counter】 key.**

Reference

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

Protecting the Address Book

You can specify who is allowed to access the data in the address book. By making this setting, you can prevent the data in the address book being used by unregistered users.

To protect the data from unauthorized reading, you can also encrypt the data in the address book.

Address Book Access Permission

This can be specified by the registered user. The access permission can also be specified by a user granted full control or the user administrator.

You can specify who is allowed to access the data in the address book.

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

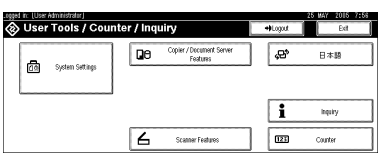
Preparation

For details about logging on with administrator authentication, see p.73 “Logging on Using Administrator Authentication”.

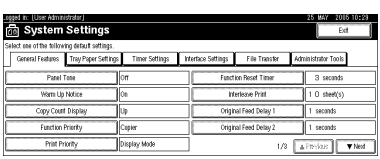
For details about logging off with administrator authentication, see p.74 “Logging off Using Administrator Authentication”.

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

2 **Press [System Settings].**



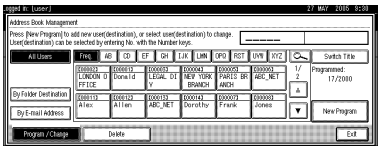
3 **Press [Administrator Tools].**



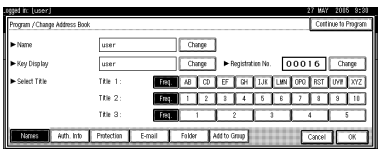
4 **Press [Address Book Management].**

If it does not appear, press **[▼Next]**.

5 **Select the user or group.**

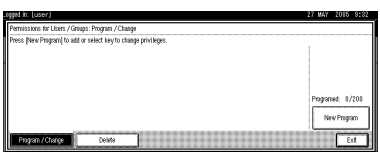


6 **Press [Protection].**



7 **Under "Protect Destination", press [Program/Change/Delete] for "Permissions for Users/Groups".**

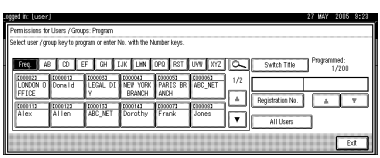
8 **Press [New Program].**



9 **Select the users or groups to register.**

You can select more than one users.

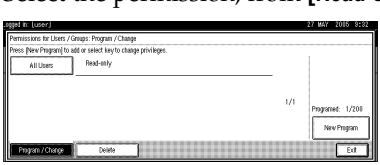
By pressing **[All Users]**, you can select all the users.



10 **Press [Exit].**

11 **Select the user who you want to assign an access permission to, and then select the permission.**

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



12 **Press [Exit].**

13 Press [OK].

14 Press [Exit].

15 Press the 【User Tools/Counter】 key.

Encrypting the Data in the Address Book

This can be specified by the user administrator.

Encrypt the data in the address book.

Preparation

For details about logging on with administrator authentication, see p.73 “Logging on Using Administrator Authentication”.

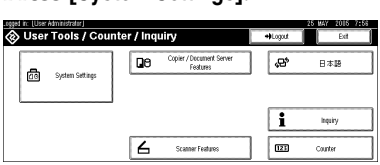
For details about logging off with administrator authentication, see p.74 “Logging off Using Administrator Authentication”.

Note

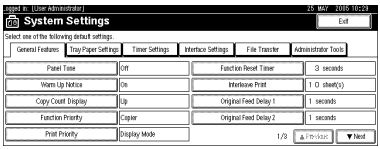
- To encrypt the data in the address book, the machine must have the scanner function.
- Encrypting the data in the address book may take a long time. (Up to three minutes)
- The time it takes to encrypt the data in the address book depends on the number of registered users.
- The machine cannot be used during encryption.
- If you press **[Stop]** during encryption, the data is not encrypted.
- Normally, once encryption is complete, **[Exit]** appears. If three minutes have passed and **[Exit]** has still not appeared, contact your service representative.
- If you press **[Stop]** during decryption, the data stays encrypted.
- Do not switch the main power off during encryption, as doing so may corrupt the data.

1 Press the 【User Tools/Counter】 key.

2 Press [System Settings].

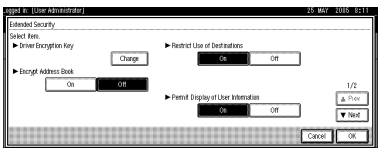


3 **Press [Administrator Tools].**



4 **Press [Extended Security].**

5 **Press [On] for "Encrypt Address Book".**



6 **Press [Change] for [Encryption Key].**

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

Enter the encryption key using up to 32 alphanumeric characters.

8 **Press [Encrypt / Decrypt].**

9 **Press [Yes].**

10 **Press [Exit].**

11 **Press [OK].**

12 **Press the 【User Tools/Counter】 key.**

Overwriting the Data on the Hard Disk

To use this function, the optional DataOverwriteSecurity unit must be installed.

You can overwrite data on the hard disk.

Note

❒ Depending on the hard disk capacity and the method of erasing the data, this action may take a few hours. The machine cannot be used during this time.

❖ **Auto Erase Memory Setting**

To erase selected data on the hard disk, specify **[Auto Erase Memory Setting]**.

❖ **Erase All Memory**

To erase all the data on the hard disk, using **[Erase All Memory]**.

❖ **Methods of Erasing the Data**

You can select the method of erasing the data from the following:
The default is "NSA".

NSA *1	Overwrites the data on the hard disk twice with random numbers and once with zeros.
DoD *2	Overwrites the data with a number, its complement, and random numbers, and then checks the result.
Random Numbers	Overwrites the data with random numbers the specified number of times. You can specify between 1 and 9 as the number of times the data is overwritten with random numbers. The default is 3 times.

*1 National Security Agency
*2 Department of Defense

Reference

For details, see the manual supplied with the DataOverwriteSecurity unit.

"Auto Erase Memory Setting"

This can be specified by the machine administrator.

A document scanned in Copier or Scanner mode is temporarily stored on the machine's hard disk.

Even after the job is completed, it remains in the hard disk as temporary data. Auto Erase Memory erases the temporary data on the hard disk by writing over it.

Overwriting starts automatically once the job is completed.

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

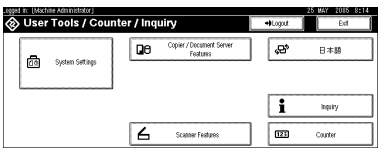
Preparation

For details about logging on with administrator authentication, see p.73 “Logging on Using Administrator Authentication”.

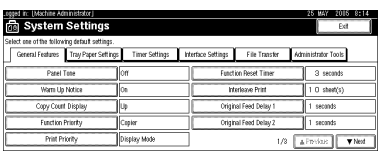
For details about logging off with administrator authentication, see p.74 “Logging off Using Administrator Authentication”.

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

2 **Press [System Settings].**



3 **Press [Administrator Tools].**



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

If it does not appear, press **[▼Next]**.

5 **Press [On], and then select the method of erasing the data.**

Select the method of erasing the data from **[NSA]**, **[DoD]**, or **[Random Numbers]**.

When you select “Random Numbers”

❶ **Press [Change].**

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

6 **Press [OK].**

Auto Erase Memory is set.

Important

❒ When Auto Erase Memory is set to "On", temporary data that remained on the hard disk when Auto Erase Memory was "Off" might not be overwritten.

Note

❒ Should the main power switch of the machine be turned off before overwriting is completed, the temporary data will remain on the hard disk until the main power switch is next turned on and overwriting is resumed.

❒ If the overwriting method is changed while overwriting is in progress, the remainder of the temporary data will be overwritten using the method set originally.

Canceling Auto Erase Memory

1 Follow steps 1 to 4 in "Auto Erase Memory Setting".

2 Press [Off].

3 Press [OK].

Auto Erase Memory is disabled.

Note

❒ To set Auto Erase Memory to "On" again, repeat the procedure in "Auto Erase Memory Setting".

Types of Data that Can or Cannot Be Overwritten

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

Data overwritten by Auto Erase Memory	Copier	• Copy jobs
	Scanner *1	• Scanned files sent by e-mail • Files sent by Scan to Folder • Documents sent using DeskTopBinder, the ScanRouter delivery software or a Web browser
Data not overwritten by Auto Erase Memory	Documents stored by the user in the Document Server using the Copier or Scanner functions *2	
	Information registered in the Address Book *3	
	Counters stored under each user code	

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

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

*3 Data stored in the Address Book can be encrypted for security. For details, see p.20 "Encrypting the Data in the Address Book".

“Erase All Memory”

This can be specified by the machine administrator.

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

Preparation

For details about logging on with administrator authentication, see p.73 “Logging on Using Administrator Authentication”.

For details about logging off with administrator authentication, see p.74 “Logging off Using Administrator Authentication”.

Important

❒ User codes and the counters under each user code, user stamps, data stored in the Address Book, network settings, and the SSL Certificate will be overwritten.

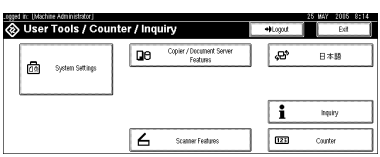
Note

❒ Before erasing the hard disk, you can back up user codes, counters for each user code, and Address Book data using SmartDeviceMonitor for Admin. For details, see SmartDeviceMonitor for Admin Help.

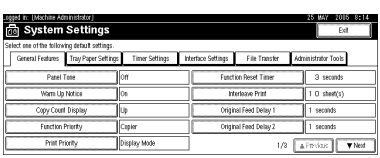
1 **Disconnect communication cables connected to the machine.**

2 **Press the 【User Tools/Counter】 key.**

3 **Press [System Settings].**



4 **Press [Administrator Tools].**



5 **Press [Erase All Memory].**

If it does not appear, press **[▼Next]**.

6 Select the method of erasing the data.

Select the method of erasing the data from **[NSA]**, **[DoD]**, or **[Random Numbers]**.

When you select "Random Numbers"

❶ **Press [Change].**

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

7 Press [OK].

8 Press [Yes].

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

Reference

Before turning the power off, see "Turning On the Power", *General Settings Guide*.

Important

❒ Should the main power switch of the machine be turned off before Erase All Memory is completed, overwriting is canceled.

❒ Make sure the main power switch is not turned off during overwriting.

Note

❒ If the main power is turned off when Erase All Memory is in progress, overwriting will start again when you next turn on the main power.

❒ If an error occurs before overwriting is completed, turn off the main power. Turn it on again, and then repeat from step **2**.

Canceling Erase All Memory

1 Press [Cancel] while Erase All Memory is in progress.

2 Press [Yes].

Erase All Memory is canceled.

Note

❒ If you stop this before completion, the data is not fully erased. Execute **[Erase All Memory]** again to erase the data.

3 Turn off the main power.

Note

❒ To resume overwriting after power off, turn on the main power of the machine, and then repeat the procedure in "Erase All Memory".

3. Preventing Unauthorized Use of Functions and Settings

Preventing Modification of Machine Settings

The machine settings that can be modified depend on the type of administrator. Users cannot change the administrator settings.

Register the administrators before using the machine.

❖ **Type of Administrator**

Register the administrator on the machine, and then authenticate the administrator using the administrator's login user name and login password. The machine settings that can be modified depend on the type of administrator. To manage the machine, the following types of administrator can be designated:

- User Administrator
- Network Administrator
- File Administrator
- Machine Administrator

Reference

For details, see p.67 "The Roles of Administrators".

For details, see p.69 "Administrator Authentication".

For details, see p.91 "Machine Administrator Settings".

For details, see p.96 "Network Administrator Settings".

For details, see p.100 "File Administrator Settings".

For details, see p.101 "User Administrator Settings".

❖ **Menu Protect**

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

You can specify Menu Protect for the following settings:

- Copier / Document Server
- Scanner Features

Reference

For details, see p.101 "User Administrator Settings".

Limiting Available Functions

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

❖ **Available Functions**
Specify the available functions from the copier, Document Server, and scanner functions.

3

Specifying Which Functions are Available

This can be specified by the user administrator. Specify the functions available to registered users. By making this setting, you can limit the functions available to users.

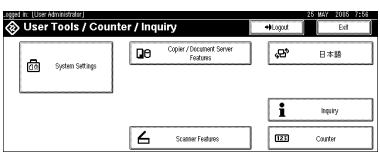
Preparation

For details about logging on with administrator authentication, see p.73 "Logging on Using Administrator Authentication".

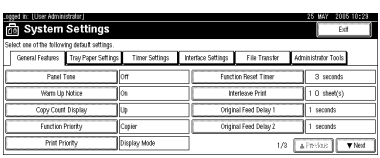
For details about logging off with administrator authentication, see p.74 "Logging off Using Administrator Authentication".

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

2 **Press [System Settings].**



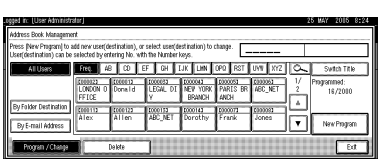
3 **Press [Administrator Tools].**



4 **Press [Address Book Management].**

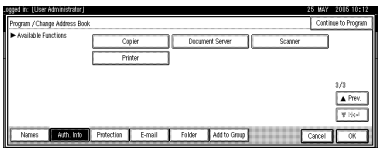
If it does not appear, press **[▼Next]**.

5 **Select the user.**



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

7 **In [Available Functions], select the functions you want to specify.**



If the setting to be specified does not appear, press **[▼Next]**.

8 **Press [OK].**

9 **Press [Exit].**

10 **Press the 【User Tools/Counter】 key.**

4. Enhanced Network Security

Preventing Unauthorized Access

You can limit IP addresses or disable ports to prevent unauthorized access over the network and protect the address book, stored files, and default settings.

Enabling/Disabling Protocols

This can be specified by the network administrator.

Specify whether to enable or disable the function for each protocol.

By making this setting, you can specify which protocols are available and so prevent unauthorized access over the network.

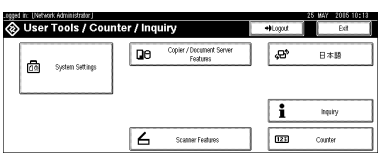
Preparation

For details about logging on with administrator authentication, see p.73 "Logging on Using Administrator Authentication".

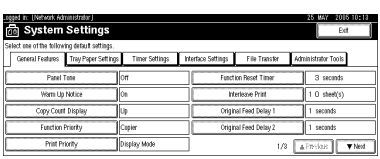
For details about logging off with administrator authentication, see p.74 "Logging off Using Administrator Authentication".

1 **Press the 【User Tools/Counter】 key.**

2 **Press [System Settings].**



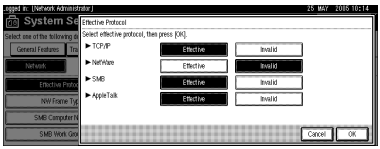
3 **Press [Interface Settings].**



4 **Press [Effective Protocol].**

If the setting to be specified does not appear, press **[▼Next]**.

5 **Press [Invalid] for the protocol you want to disable.**



6 **Press [OK].**

7 **Press the 【User Tools/Counter】 key.**

Reference

Advanced network settings can be specified using Web Image Monitor. For details, see the Web Image Monitor Help.

4

Access Control

This can be specified by the network administrator.

The machine can control TCP/IP access.

Limit the IP addresses from which access is possible by specifying the access control range.

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

Limitation

- ❒ Using access control, you can limit access involving lpd, rcp/rsh, ftp, diprint, ipp, Web Image Monitor, SmartDeviceMonitor for Client or DeskTopBinder. You cannot limit the Monitoring of SmartDeviceMonitor for Client.
- ❒ You cannot limit access involving telnet, or SmartDeviceMonitor for Admin.

1 **Open a Web browser.**

2 **Enter "http://(machine's-address)/" in the address bar to access the machine.**

3 **Log onto the machine.**

The network administrator can log on using the appropriate login user name and login password.

4 **Click [Configuration], click [Security], and then click [Access Control].**

The **[Access Control]** page appears.

5 **In [Access Control Range], enter the IP addresses from which access to the machine is permitted.**

6 **Click [Apply].**

Access control is set.

7 **Log off from the machine.**

Reference

For details, see the Web Image Monitor Help.

Encrypting Transmitted Passwords

Prevent login passwords, group passwords for PDF files, and IPP authentication passwords being revealed by encrypting them for transmission.

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

❖ **Driver Encryption Key**

To encrypt the login password, specify the driver encryption key for the driver used for the machine and the user's computer.

Limitation

❒ The driver encryption key cannot be used under Windows 95/98 SE/Me.

❖ **Password for IPP Authentication**

Using Web Image Monitor, you can encrypt the password for IPP authentication.

Note

❒ You can use Telnet or FTP to manage passwords for IPP authentication, although it is not recommended.

Note

❒ To encrypt transmitted passwords, the machine must have the scanner function.

Driver Encryption Key

This can be specified by the network administrator.

Specify the driver encryption key on the machine.

By making this setting, you can encrypt login passwords for transmission to prevent them from being analyzed.

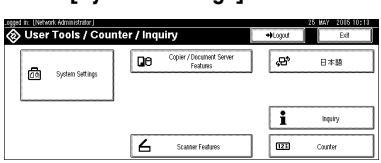
Preparation

For details about logging on with administrator authentication, see p.73 "Logging on Using Administrator Authentication".

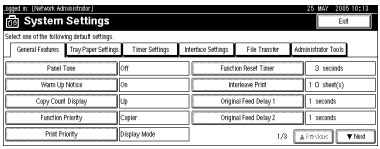
For details about logging off with administrator authentication, see p.74 "Logging off Using Administrator Authentication".

1 **Press the 【User Tools/Counter】 key.**

2 **Press [System Settings].**

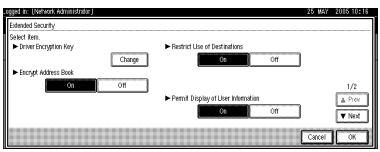


3 **Press [Administrator Tools].**



4 **Press [Extended Security].**

5 **For [Driver Encryption Key], press [Change].**



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

Enter the driver encryption key using up to 32 alphanumeric characters.

Note

❒ 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.

7 **Press [OK].**

8 **Press the 【User Tools/Counter】 key.**

Reference

See the TWAIN driver Help.

IPP Authentication Password

This can be specified by the network administrator.

Specify the IPP authentication passwords for the machine using Web Image Monitor.

By making this setting, you can encrypt IPP authentication passwords for transmission to prevent them from being analyzed.

1. **Open a Web browser.**
2. **Enter "http://(machine's-address)/" in the address bar to access the machine.**
3. **Log onto the machine.**

   The network administrator can log on. Enter the login user name and login password.
4. **Click [Configuration], click [Security], and then click [IPP Authentication].**

   The **[IPP Authentication]** page appears.
5. **Select [DIGEST] from the [Authentication] list.**

   Note

   ❒ When using the IPP port under Windows XP or Windows Server 2003, you can use the operating system's standard IPP port.
6. **Enter the user name in the [User Name] box.**
7. **Enter the password in the [Password] box.**
8. **Click [Apply].**

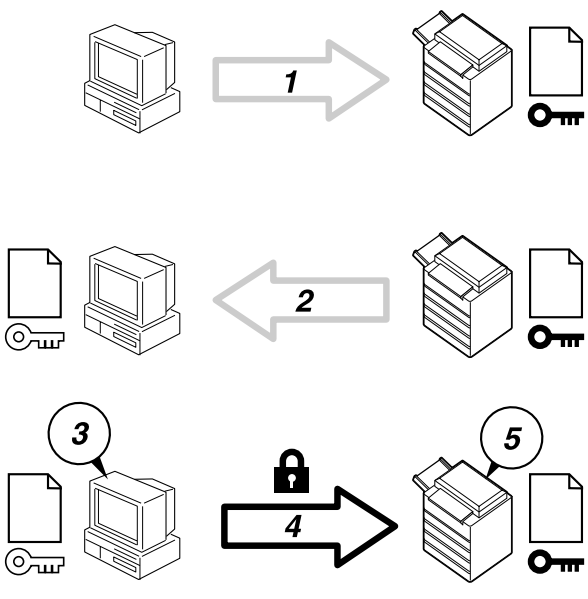
   IPP authentication is specified.
9. **Log off from the machine.**

Protection Using Encryption

When you access the machine using a Web browser or IPP, you can establish encrypted communication using SSL. When you access the machine using an application such as SmartDeviceMonitor for Admin, you can establish encrypted communication using SNMPv3 or SSL.

To protect data from interception, analysis, and tampering, you can install a server certificate in the machine, negotiate a secure connection, and encrypt transmitted data.

❖ SSL (Secure Sockets Layer)



① To access the machine from a user's computer, request for the SSL server certificate and public key.

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

③ Using the public key, encrypt the data for transmission.

④ The encrypted data is sent to the machine.

⑤ The encrypted data is decrypted using the private key.

Note

❒ To establish encrypted communication using SSL, the machine must have the scanner function.

SSL (Secure Sockets Layer) Encryption

This can be specified by the network administrator.

To protect the communication path and establish encrypted communication, create and install the server certificate.

There are two ways of installing a server certificate: create and install a self-certificate using the machine, or request a certificate from a certificate authority and install it.

❖ **Configuration flow (self-signed certificate)**

① Creating and installing the server certificate
Install the server certificate using Web Image Monitor.

② Enabling SSL
Enable the **[SSL/TLS]** setting using Web Image Monitor.

❖ **Configuration flow (certificate issued by a certificate authority)**

① Creating the server certificate
Create the server certificate using Web Image Monitor.
The application procedure after creating the certificate depends on the certificate authority. Follow the procedure specified by the certificate authority.

② Installing the server certificate
Install the server certificate using Web Image Monitor.

③ Enabling SSL
Enable the **[SSL/TLS]** setting using Web Image Monitor.
Creating and Installing the Server Certificate (Self-Signed Certificate)
Create and install the server certificate using Web Image Monitor.

Note

❒ To confirm whether SSL configuration is enabled, enter https://(machine's-address) in your Web browser's address bar to access this machine. If the "The page cannot be displayed" message appears, check the configuration as the SSL configuration is invalid.

Creating and Installing the Self-Signed Certificate

Create and install the server certificate using Web Image Monitor.

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

1 Open a Web browser.

2 Enter "http://(machine's-address)/" in the address bar to access the machine.

3 Log onto the machine.

The network administrator can log on.

Enter the login user name and login password.

4 **Click [Configuration], click [Security], and then click [Certificates].**

5 **Click [Create].**

6 **Make the necessary settings.**

Reference

For details about the displayed items and selectable items, see Web Image Monitor Help.

7 **Click [OK].**

The setting is changed.

8 **Click [OK].**

A security warning dialog box appears.

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

[Installed] appears under **[Certificate Status]** to show that a server certificate for the machine has been installed.

10 **Log off from the machine.**

Note

❒ Click **[Delete]** to delete the server certificate from the machine.

Creating the Server Certificate (Certificate Issued by a Certificate Authority)

Create the server certificate using Web Image Monitor.

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

1 **Open a Web browser.**

2 **Enter "http://(machine's-address)/" in the address bar to access the machine.**

3 **Log onto the machine.**

The network administrator can log on.

Enter the login user name and login password.

4 **Click [Configuration], click [Security], and then click [Certificates].**

The **[Certificates]** page appears.

5 **Click [Request].**

6 **Make the necessary settings.**

Reference

For details about the displayed items and selectable items, see Web Image Monitor Help.

7 **Click [OK].**

[Requesting] appears for **[Certificate Status]** in the **[Certificates]** area.

Use the data in the **[Certificate Request Contents:]** dialog box to apply to the certificate authority.

8 **Log off from the machine.**

9 **Apply to the certificate authority for the server certificate.**

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

When applying, use the data created with Web Image Monitor.

Note

❒ Using Web Image Monitor, you can create the contents of the server certificate but you cannot send the application.

❒ Click **[Cancel Request]** to cancel the request for the server certificate.

4

Installing the Server Certificate (Certificate Issued by a Certificate Authority)

Install the server certificate using Web Image Monitor.

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

Enter the server certificate contents issued by the certificate authority.

1 **Open a Web browser.**

2 **Enter "http://(machine's-address)/" in the address bar to access the machine.**

3 **Log onto the machine.**

The network administrator can log on.

Enter the login user name and login password.

4 **Click [Configuration], click [Security], and then click [Certificates].**

The **[Certificates]** page appears.

5 **Click [Install].**

6 **Enter the contents of the server certificate.**

In the **[Certificate Request]** box, enter the contents of the server certificate received from the certificate authority.

Reference

For details about the displayed items and selectable items, see Web Image Monitor Help.

7 **Click [OK].**

[Installed] appears under **[Certificate Status]** to show that a server certificate for the machine has been installed.

8 **Log off from the machine.**

Enabling SSL

After installing the server certificate in the machine, enable the SSL setting.

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

1 **Open a Web browser.**

2 **Enter "http://(machine's-address)/" in the address bar to access the machine.**

3 **Log onto the machine.**

The network administrator can log on.

Enter the login user name and login password.

4 **Click [Configuration], click [Security], and then click [SSL/TLS].**

The **[SSL/TLS]** page appears.

5 **Click [Enable] for [SSL/TLS].**

6 **Click [Apply].**

The SSL setting is enabled.

7 **Log off from the machine.**

Note

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

User Settings for SSL (Secure Sockets Layer)

If you have installed a server certificate and enabled SSL (Secure Sockets Layer), you need to install the certificate on the user's computer.

The network administrator must explain the procedure for installing the certificate to users.

If a warning dialog box appears while accessing the machine using the Web browser or IPP, start the Certificate Import Wizard and install a certificate.

1 When the [Security Alert] dialog box appears, click [View Certificate].

The **[Certificate]** dialog box appears.

To be able to respond to inquiries from users about such problems as expiry of the certificate, check the contents of the certificate.

2 On the [General] tab, click [Install Certificate...].

Certificate Import Wizard starts.

3 Install the certificate by following the Certificate Import Wizard instructions.

Note

❒ For details about how to install the certificate, see the Web browser Help.

❒ If a certificate issued by a certificate authority is installed in the machine, confirm the certificate store location with the certificate authority.

Reference

For details about where to store the certificate when accessing the machine using IPP, see the SmartDeviceMonitor for Client Help.

Setting the SSL / TLS Encryption Mode

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

❖ **Encrypted Communication Mode**

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

Ciphertext Only	Allows encrypted communication only. If encryption is not possible, the machine does not communicate.
Ciphertext Priority	Performs encrypted communication if encryption is possible. If encryption is not possible, the machine communicates without it.
Ciphertext / Clear Text	Communicates with or without encryption, according to the setting.

Setting the SSL / TLS Encryption Mode

This can be specified by the network administrator or machine administrator.

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

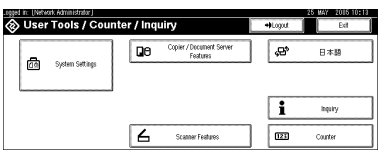
Preparation

For details about logging on with administrator authentication, see p.73 “Logging on Using Administrator Authentication”.

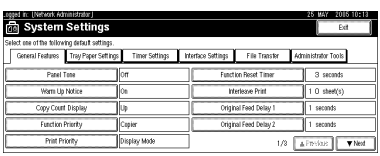
For details about logging off with administrator authentication, see p.74 “Logging off Using Administrator Authentication”.

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

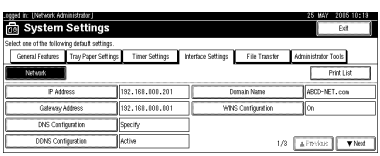
2 **Press [System Settings].**



3 **Press [Interface Settings].**



4 **Press [Permit SSL / TLS Communication]**



If it does not appear, press **[▼Next]**.

5 **Select the encrypted communication mode.**

Select **[Ciphertext Only]**, **[Ciphertext Priority]**, or **[Ciphertext / Clear Text]** as the encrypted communication mode.

6 **Press [OK].**

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

Note

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

SNMPv3 Encryption

This can be specified by the network administrator.

When using SmartDeviceMonitor for Admin or another application to make various settings, you can encrypt the data transmitted.

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

Preparation

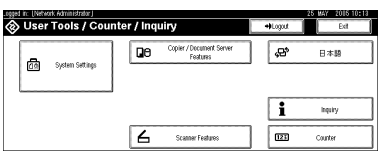
For details about logging on with administrator authentication, see p.73 “Logging on Using Administrator Authentication”.

For details about logging off with administrator authentication, see p.74 “Logging off Using Administrator Authentication”.

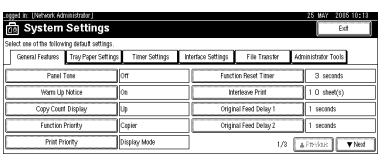
4

1. Press the 【User Tools/Counter】 key.

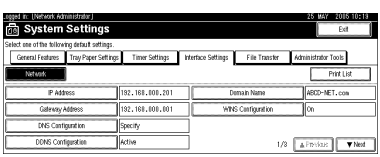
2. Press [System Settings].



3. Press [Interface Settings].



4. Press [Permit SNMP V3 Communication].



If it does not appear, press **[▼Next]**.

5. Press [Encryption Only].

6. Press [OK].

7. Press the 【User Tools/Counter】 key.

Note

❒ To use SmartDeviceMonitor for Admin for encrypting the data for specifying settings, you need to specify the network administrator's **[Encryption Password]** setting and **[Encryption Key]** in **[SNMP Authentication Information]** in SmartDeviceMonitor for Admin, in addition to specifying **[Permit SNMP V3 Communication]** on the machine.

❒ If the machine does not have the scanner function, or if network administrator's **[Encryption Password]** setting is not specified, the data for transmission may not be encrypted or sent.

Reference

For details about specifying the network administrator's **[Encryption Password]** setting, see p.72 "Registering the Administrator".

For details about specifying **[Encryption Key]** in SmartDeviceMonitor for Admin, see the SmartDeviceMonitor for Admin Help.

5. Management Based on Authentication and Access Control

The Management Function

The machine has an authentication function requiring a login user name and login password. By using the authentication function, you can specify access limits for individual users and groups of users. Using access limits, you can not only limit the machine's available functions but also protect the machine settings and files and data stored in the machine.

Important

- ❒ If you have enabled **[Administrator Authentication Management]**, make sure not to forget the administrator login user name and login password. If an administrator login user name or login password is forgotten, a new password must be specified using the supervisor's authority.
- ❒ Be sure not to forget the supervisor login user name and login password. If you do forget them, a service representative will to have to return the machine to its default state. This will result in all data in the machine being lost and the service call may not be free of charge.

Reference

For details, see p.87 "Operations by the Supervisor".

Administrators and Users

When controlling access using the authentication specified by an administrator, select the machine's administrator, enable the authentication function, and then use the machine.

The administrators manage access to the allocated functions, and users can use only the functions they are permitted to access. To enable the authentication function, the login user name and login password are required in order to use the machine.

When specifying user authentication, specify administrator authentication as well.

Important

❒ If user authentication is not possible because of a problem with the hard disk or network, you can use the machine by accessing it using administrator authentication and disabling user authentication. Do this if, for instance, you need to use the machine urgently. For details, see the Web Image Monitor Help.

Administrator

There are four types of administrator according to the administered function: machine administrator, network administrator, file administrator, and user administrator.

By sharing the administrative work among different administrators, you can spread the workload and limit unauthorized operation by a single administrator.

Administrators are limited to managing the machine's settings and access limits, so user authentication is required to use such function as copying.

Note

❒ One person can act as more than one type of administrator.

Reference

For details, see p.67 "The Roles of Administrators".

For details, see p.72 "Registering the Administrator".

User

Users are managed using the personal information registered in the machine's address book.

By enabling user authentication, you can allow only people registered in the address book to use the machine. Users can be registered in the address book by the user administrator or registered user. In addition to registering users with the machine's control panel, you can register them using SmartDeviceMonitor for Admin or Web Image Monitor.

Note

❒ Users can be registered only by a user administrator, using SmartDeviceMonitor for Admin or Web Image Monitor.

Reference

For details about registering users in the address book, see *General Settings Guide*, the SmartDeviceMonitor for Admin Help, or the Web Image Monitor Help.

Enabling Authentication

To control administrators' and users' access to the machine, perform administrator authentication and user authentication using login user names and login passwords. To perform authentication, the authentication function must be enabled.

Note

❒ To specify authentication, the administrator must be registered.

Reference

For details, see p.72 "Registering the Administrator".

Administrator Authentication

To use administrator authentication, enable **[Administrator Authentication Management]** on the control panel.

Important

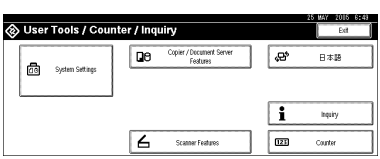
❒ If you have enabled **[Administrator Authentication Management]**, make sure not to forget the administrator login user name and login password. If an administrator login user name or login password is forgotten, a new password must be specified using the supervisor's authority.

Reference

For details, see p.87 "Operations by the Supervisor".

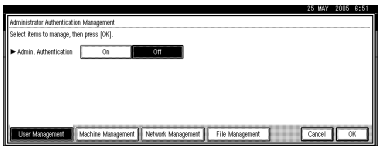
Specifying Administrator Authentication Management

1. **Press the 【User Tools/Counter】 key.**
2. **Press [System Settings].**



3. **Press [Administrator Tools].**
4. **Press [Administrator Authentication Management].**
5. **Press the [User Management], [Machine Management], [Network Management], or [File Management] key to select which settings to manage.**

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



[Available Settings] appears.

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

Note

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

8 **Press [OK].**

9 **Press the 【User Tools/Counter】 key.**

5

User Authentication

There are four types of user authentication method: user code authentication, basic authentication, Windows authentication, and LDAP authentication. To use user authentication, select an authentication method on the control panel, and then make the required settings for the authentication. The settings depend on the authentication method.

Important

❒ When using Windows authentication or LDAP authentication, keep in mind that if you edit an authenticated user's e-mail address or any of the other data that is automatically stored after successful authentication, the edited data may be overwritten when it is reacquired at the next authentication.

Note

❒ User code authentication is used for authenticating on the basis of the user code, and basic authentication, Windows authentication, and LDAP authentication are used for authenticating individual users.

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

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

User Code Authentication

This is an authentication method for limiting access to functions according to the user code. The same user code can be used by more than one user. For details about specifying user codes, see *General Settings Guide*.

Limitation

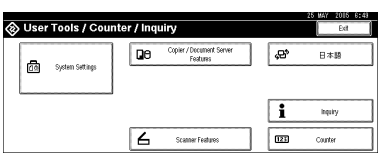
❒ If user code authentication is specified, files stored in the machine cannot be delivered using DeskTopBinder. To deliver stored files using DeskTopBinder, use basic authentication, Windows authentication, or LDAP authentication.

Reference

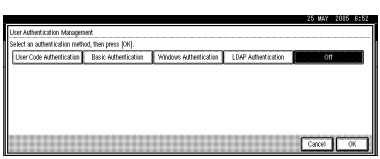
For details about specifying the TWAIN driver user code, see the TWAIN driver Help.

Specifying User Code Authentication

1. **Press the 【User Tools/Counter】 key.**
2. **Press [System Settings].**



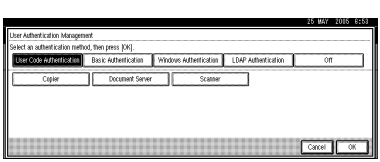
3. **Press [Administrator Tools].**
4. **Press [User Authentication Management].**
5. **Select [User Code Authentication].**



Note

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

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



7 **Press [OK].**

8 **Press the 【User Tools/Counter】 key.**

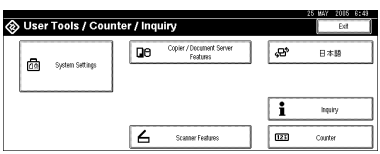
Basic Authentication

Specify this authentication when using the machine's address book to authenticate for each user. Using basic authentication, you can not only manage the machine's available functions but also limit access to stored files and to the personal data in the address book.

Specifying Basic Authentication

1 **Press the 【User Tools/Counter】 key.**

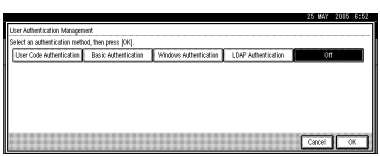
2 **Press [System Settings].**



3 **Press [Administrator Tools].**

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

5 **Select [Basic Authentication].**



Note

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

6 **Press [OK].**

7 **Press the 【User Tools/Counter】 key.**

Windows Authentication

Specify this authentication when using the Windows domain controller to authenticate users who have their accounts on the directory server. Users cannot be authenticated if they do not have their accounts in the directory server. Under Windows authentication, you can specify the access limit for each group registered in the directory server.

❖ Operational Requirements for Windows Authentication

- To specify Windows authentication, the following requirements must be met:
  - The machine has the scanner function.
  - A domain controller has been set up in a designated domain.
- This function is supported by the operating systems listed below. NTLM authentication is used for Windows authentication. To obtain user information when running Active Directory, use LDAP. For this to be possible, the version of Windows being used must support TLSv1.
  - Windows NT 4.0 Server
  - Windows 2000 Server
  - Windows Server 2003

Limitation

❒ Users managed outside the domain are subject to user authentication, but they cannot obtain items such as e-mail addresses.

❒ With Active Directory, you can authenticate users and obtain user information. Under Windows NT 4.0 domain controller, you can only authenticate users.

❒ If you can obtain user information, the sender's address (From:) is fixed to prevent unauthorized access when sending e-mails under the scanner function.

Note

❒ Enter the login password correctly, keeping in mind that it is case-sensitive.

❒ In a network environment with a WINS server, where other networks can be accessed via a router, you must specify WINS.

❒ If you want to use Windows Authentication, you need to register the user name that is registered in the Windows server.

❒ Users who are not registered in groups and whose available functions are not limited in the machine's address book can use the available functions specified in **[Default Group]**.

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

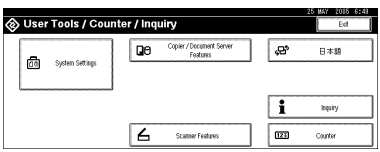
Specifying Windows Authentication

Note

❒ Under Windows authentication, the machine and domain controller communicate using SSL, so you need to create a server certificate for the domain controller. For details about creating the certificate, see p.56 “Creating the Server Certificate”.

1 **Press the 【User Tools/Counter】 key.**

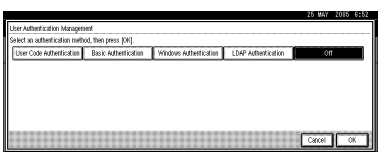
2 **Press [System Settings].**



3 **Press [Administrator Tools].**

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

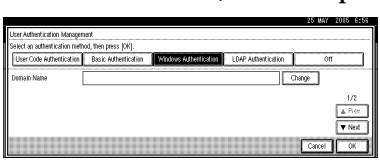
5 **Select [Windows Authentication].**



Note

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

6 **Press [Change] for “Domain Name”, enter the name of the domain controller to be authenticated, and then press [OK].**



If global groups have been registered:

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

You need to create global groups in the Windows server in advance and register in each group the users to be authenticated.

You also need to register in the machine the functions available to the global group members.

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

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

If the setting to be specified does not appear, press **[▼Next]**.

❷ **Press [Change], and then enter the group name.**

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

❹ **Press [OK].**

7 **Press [OK].**

8 **Press the 【User Tools/Counter】 key.**

5

Creating the Server Certificate

This section explains how to create a Windows certificate for authentication. The procedure given uses Windows 2000 as an example.

Note

❒ Before you can create a certificate, you need to install Internet Information Service (IIS).

① In **[Control Panel]**, click **[Add/Remove Programs]**.

② Click **[Add/Remove Windows Components]** and install **[Certificates Service]**.

③ On the **[Start]** menu, point to **[Programs]**, **[Administrative tools]**, and then click **[Internet Information Service]**.

④ Right-click **[Default Web Site]** and click **[Properties]**.

⑤ Click the **[Directory Security]** tab.

⑥ Click **[Server Certificate...]** in **[Secure Communication]** at the bottom of the dialog box.

⑦ Follow Web Server Certificates Wizards to create and install the server certificate.

LDAP Authentication

Specify this authentication when using the LDAP server to authenticate users who have their accounts on the LDAP server. Users cannot be authenticated if they do not have their accounts on the LDAP server. The address book stored in the LDAP server can be downloaded to the machine, enabling user authentication without first using the machine to register individual settings in the address book.

Limitation

- ❒ To use LDAP authentication, the network configuration must allow the machine to detect the presence of the LDAP server.
- ❒ SSL communication is used for LDAP authentication, so the machine must have the scanner function.
- ❒ To use LDAP authentication you need to register the LDAP server in the machine. For details about registration, see *Network Guide*.
- ❒ Enter the user's login user name using up to 32 characters and login password using up to 128 characters.
- ❒ Enter the administrator's login user name and login password using up to 32 characters for each.

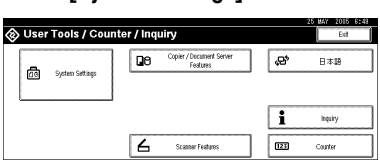
Note

- ❒ If the LDAP server is Active Directory, the login user name is specified as "username@domainname". However, you can omit the domain name by doing the following: On the Windows server's **[Start]** menu, select **[Programs]**, **[Administrative tools]**, **[Active Directory Domains and Trusts]**; then, on the **[Action]** menu, select **[Properties]**; and then, in **[Active Directory Domains and Trusts Properties]**, add the UPN suffix.
- ❒ If you want to use LDAP authentication, you need to register the user name that is registered in the LDAP server.

Specifying LDAP Authentication

1 **Press the 【User Tools/Counter】 key.**

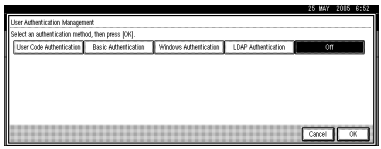
2 **Press [System Settings].**



3 **Press [Administrator Tools].**

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

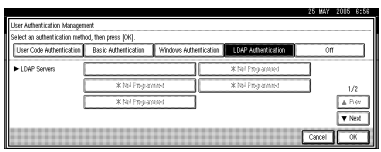
5 **Select [LDAP Authentication].**



Note

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

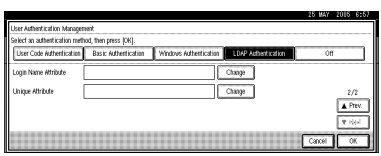
6 **Select the LDAP server to be used for LDAP authentication.**



5

7 **Enter the login name attribute in the [Login Name Attribute] box.**

If it does not appear, press **[▼Next]**.



Note

❒ The default login name attribute for Active Directory is “userPrincipalName”.

8 **Enter the unique attribute in the [Unique Attribute] box.**

Note

❒ The default unique attribute for Active Directory is “objectGUID”.

9 **Press [OK].**

10 **Press the 【User Tools/Counter】 key**

Authentication Information Stored in the Address Book

In **[User Authentication Management]**, specify the login user name and password. The login user name and password specified in **[User Authentication Management]** can be used as the login information for "SMTP Authentication", "Folder Authentication", and "LDAP Authentication".

If you do not want to use the login user name and password specified in **[User Authentication Management]** for "SMTP Authentication", "Folder Authentication", or "LDAP Authentication", see *General Settings Guide*.

Preparation

For details about logging on using administrator authentication, see p.73 "Logging on Using Administrator Authentication".

For details about logging off with administrator authentication, see p.74 "Logging off Using Administrator Authentication".

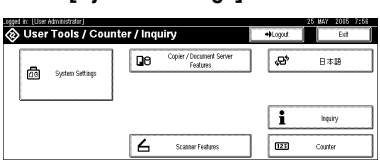
You need to register a user in the address book. For details about the address book, see *General Settings Guide*.

Specifying Authentication Information to Log on

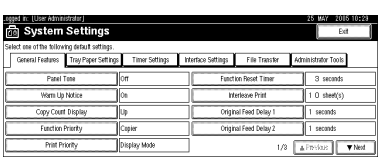
If you want to use **[Windows Authentication]** or **[LDAP Authentication]** in **[User Authentication Management]**, take the user name registered in the server and register it in the machine's address book.

1 **Press the 【User Tools/Counter】 key.**

2 **Press [System Settings].**



3 **Press [Administrator Tools].**



4 **Press [Address Book Management].**

If the setting to be specified does not appear, press **[▼Next]**.

5 **Select the user or group.**

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

7 **Specify the login user name and password.**

8 **In "Available Functions", select the functions available to the user.**

Reference

For details about limiting available functions, see p.28 "Limiting Available Functions".

9 **Select [Use Auth. Info at Login] in "SMTP Authentication".**

If the setting to be specified does not appear, press **[▼Next]**.

Limitation

- When using **[Use Auth. Info at Login]** for "SMTP Authentication", "Folder Authentication", or "LDAP Authentication", a user name other than "other" or "HIDE***" must be specified. The symbol "***" represents any character.
- To use **[Use Auth. Info at Login]** for SMTP authentication, a login password up to 64 characters in length must be specified.

Note

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

10 **Press [OK].**

11 **Press [Exit].**

12 **Press the 【User Tools/Counter】 key.**

If User Authentication Has Been Specified

When user authentication (User Code Authentication, Basic Authentication, Windows Authentication, or LDAP Authentication) is set, the authentication screen is displayed. Unless a valid user name and password are entered, operations are not possible with the machine. Log on to operate the machine, and log off when you are finished operations. Be sure to log off to prevent unauthorized users from using the machine.

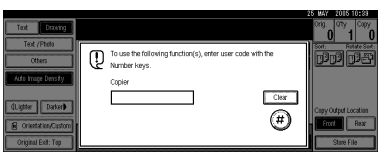
Note

❒ Consult the User Administrator about your login user name, password, and user code.

❒ For user code authentication, enter a number registered in the address book as **[User Code]**.

User Code Authentication (Using the Control Panel)

When user authentication is set, the following screen appears.

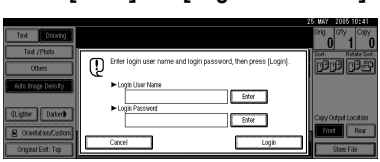


Enter a user code (eight digit), and then press **[#]**.

Login (Using the Control Panel)

Follow the procedure below to log on when Basic Authentication, Windows Authentication, or LDAP Authentication is set. Follow the procedure below to log on when basic authentication, Windows authentication, or LDAP authentication is set.

1 **Press [Enter] for [Login User Name].**



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

3 **Press [Enter] for [Login Password].**

4 **Enter a login password, and then press [OK].**

5 **Press [Login].**

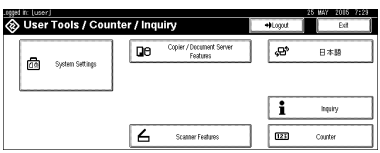
When the user is authenticated, the screen for the function you are using appears.

Log Off (Using the Control Panel)

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

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

2 **Press [Logout].**



3 **Press [Yes].**

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

Login (Using Web Image Monitor)

Follow the procedure below to log on when user authentication is set.

1 **Click [Login].**

2 **Enter a login user name and password, and then click [OK].**

Note

❒ For user code authentication, enter a user code in **[User Name]**, and then click **[OK]**.

❒ The procedure may differ depending on the Web browser used.

Log Off (Using Web Image Monitor)

1 **Click [Logout] to log off.**

Note

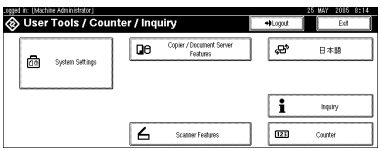
❒ Delete the cache memory in the Web browser after logging off.

Auto Logout

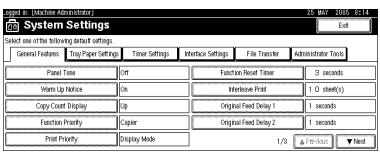
When using user authentication management, the machine automatically logs you off if you do not use the control panel within a given time. This feature is called "Auto Logout". Specify how long the machine is to wait before performing Auto Logout.

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

2. **Press [System Settings].**



3. **Press [Timer Settings].**



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

   If the setting to be specified does not appear, press **[▼Next]**.

5. **Select [On], and then enter "10" to "999" (seconds) using the number keys.**

   Note

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

6. **Press [OK].**

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

Menu Protect

The administrator can also limit users' access permission to the machine's settings. The machine's System Settings menu can be locked so they cannot be changed. This function is also effective when management is not based on user authentication.

Note

❒ To change the menu protect setting, you must first enable administrator authentication.

Reference

For details about the menu protect level for each function, see p.101 "User Administrator Settings".

Menu Protect

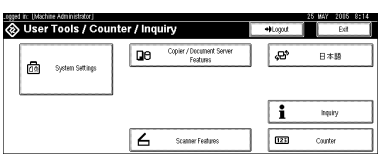
You can set menu protect to **[Off]**, **[Level 1]**, or **[Level 2]**. If you set it to **[Off]**, no menu protect limitation is applied. To limit access to the fullest extent, select **[Level 2]**.

Copying Functions

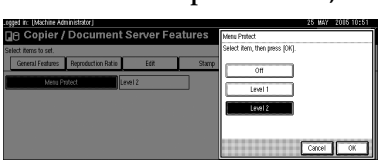
Note

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

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



3. **Press [Administrator Tools].**
4. **Press [Menu Protect].**
5. **Select the menu protect level, and then press [OK].**



6 Press the 【User Tools/Counter】 key.

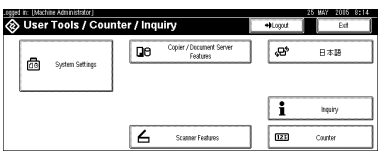
Scanner Functions

Note

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

1 Press the 【User Tools/Counter】 key.

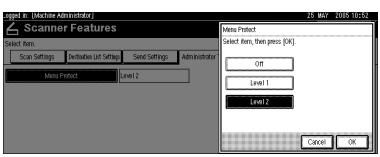
2 Press **[Scanner Features]**.



3 Press **[Administrator Tools]**.

4 Press **[Menu Protect]**.

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



6 Press the 【User Tools/Counter】 key.

6. Specifying the Administrator/Security Functions

The Roles of Administrators

By limiting the functions available to each user, you can protect the data in the machine from leaks and from being tampered with or deleted. The administrators each manage the access limits to the functions they are responsible for.

There are four types of administrator, as shown below. You can also specify a supervisor who can change each administrator's password.

- Machine Administrator
- Network Administrator
- File Administrator
- User Administrator
- Supervisor

Register the administrators and supervisor separately from the users registered in the address book. Users registered in the address book cannot be specified as administrators.

Reference

For details, see p.72 "Registering the Administrator".

❖ **Machine Administrator**

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

❖ **Network Administrator**

This is the administrator who manages the network settings. You can set the machine so that network settings such as the IP address and settings for sending and receiving e-mail can only be specified by the network administrator. By making this setting, you can prevent unauthorized users from changing the settings and disabling the machine, and thus ensure correct network operation.

❖ **File Administrator**

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

❖ **User Administrator**

This is the administrator who manages personal information in the address book.

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

Users registered in the address book can also change and delete their own information. If any of the users forget their password, the user administrator can delete it and create a new one, allowing the user to access the machine again.

❖ **Supervisor**

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

Reference

See p.87 "Operations by the Supervisor".

Administrator Authentication

Administrators are handled differently from the users registered in the address book. When registering an administrator, you cannot use a login user name and login password already registered in the address book. Windows Authentication and LDAP Authentication are not performed for an administrator, so an administrator can log on even if the server is unreachable because of a network problem.

Each administrator is identified by a login user name and login password. One person can act as more than one type of administrator if multiple administrator authority is granted to a single login user name and login password.

You can specify the login user name, login password, and encryption password for each administrator.

The encryption password is a password for performing encryption when specifying settings using Web Image Monitor or SmartDeviceMonitor for Admin.

The password registered in the machine must be entered when using applications such as SmartDeviceMonitor for Admin.

Note

- ❒ You can use up to 32 alphanumeric characters and symbols when registering login user names and login passwords. Keep in mind that passwords are case-sensitive.
- ❒ You should use at least eight characters for the login password so that other people will not be able to guess it easily.
- ❒ You cannot include spaces, semicolons (;) or quotes ("") in the user name, or leave the user name blank.
- ❒ You can register up to four sets of login user names and login passwords to which you can grant administrator authority.
- ❒ Administrator authentication can also be specified via Web Image Monitor. For details see the Web Image Monitor Help.

Administrator Authentication

To specify administrator authentication, set Administrator Authentication Management to **[On]**. You can also specify whether or not to manage the items in System Settings as an administrator.

If you have not registered any administrator, you can obtain each administrator's authority with the "Administrator 1" setting. To log on as an administrator, use the default login user name and login password.

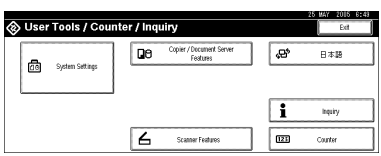
Preparation

For details about logging on with administrator authentication, see p.73 "Logging on Using Administrator Authentication".

For details about logging off with administrator authentication, see p.74 "Logging off Using Administrator Authentication".

The "Administrator 1" defaults are "admin" for the login name and blank for the password. If user authentication has been specified, a screen for authentication appears. To specify administrator authentication, log on as an administrator by entering "admin" as the login user name and leaving the login password blank.

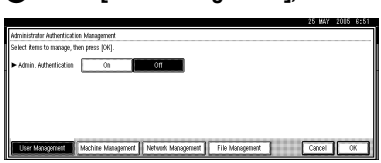
1. **Press the 【User Tools/Counter】 key.**
2. **Press [System Settings].**



3. **Press [Administrator Tools].**
4. **Press [Administrator Authentication Management].**
5. **Specify each administrator authentication.**

Specifying User Management Authentication

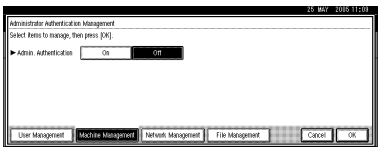
❶ **Press [User Management], and then press [On].**



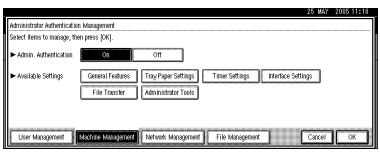
❷ **To specify address book management, press [Administrator Tools].**

Specifying Machine Management Authentication

❶ **Press [Machine Management], and then press [On].**

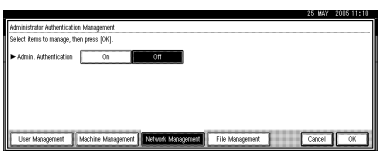


❷ **Press the item for which you want to specify management.**

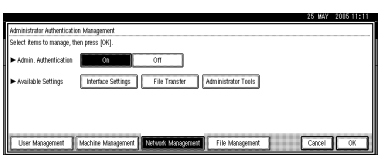


Specifying Network Management Authentication

❶ **Press [Network Management], and then press [On].**

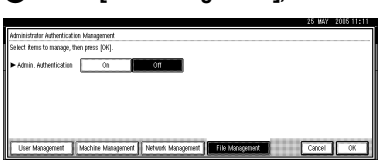


❷ **Press the item for which you want to specify management.**



Specifying File Management Authentication

❶ **Press [File Management], and then press [On].**



❷ **To specify file management, press [Administrator Tools].**

6 **Press [OK].**

7 **Press the 【User Tools/Counter】 key.**

Registering the Administrator

To specify the administrators separately when only "Administrator 1" has been specified, log on using the "Administrator 1" login user name and login password. To register an administrator, you need to specify the authority of one of the administrators. The data for each administrator can be changed using administrator authority.

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

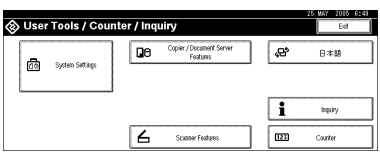
Preparation

If administrator authentication has already been specified, log on using a registered administrator name and password. For details about logging on using administrator authentication, see p.73 "Logging on Using Administrator Authentication".

For details about logging off with administrator authentication, see p.74 "Logging off Using Administrator Authentication".

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

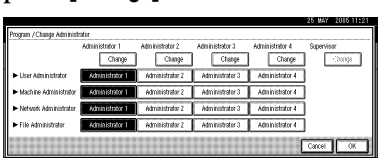
2. **Press [System Settings].**



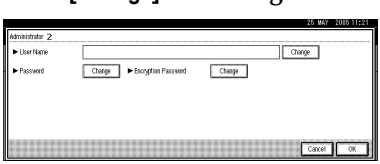
3. **Press [Administrator Tools].**

4. **Press [Program / Change Administrator].**

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

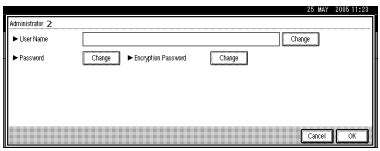


6. **Press [Change] for the login user name.**



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

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

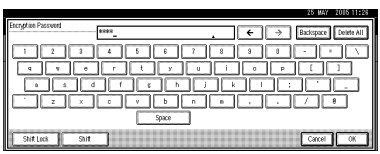


9 **Enter the login password, and then press [OK].**

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

11 **Press [Change] for the encryption password.**

12 **Enter the encryption password, and then press [OK].**



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

14 **Press [OK].**

15 **Press [OK].**

16 **Press the 【User Tools/Counter】 key.**

Logging on Using Administrator Authentication

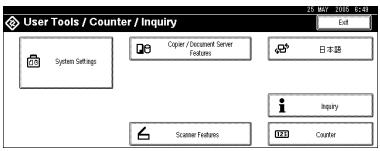
If administrator authentication has been specified, log on using an administrator's user name and password.This section describes how to log on.

Note

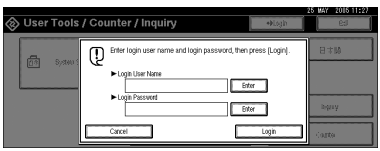
- ❒ If user authentication has already been specified, a screen for authentication appears.
- ❒ To log on as an administrator, enter the administrator's login user name and login password.
- ❒ If you log on using administrator authority, the name of the administrator logging on appears.
- ❒ If you log on using a login user name with the authority of more than one administrator, "Administrator" appears.
- ❒ If you try to log on from an operating screen, "Selected function cannot be used." appears. Press the 【User Tools/Counter】 key to change the default.

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

2 **Press [Login].**



3 **Press [Enter] next to "Login User Name".**

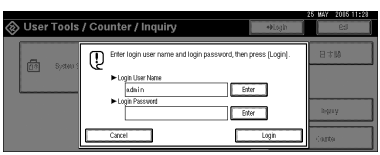


4 **Enter the login user name, and then press [OK].**

Note

❒ If assigning the administrator for the first time, enter "admin".

5 **Press [Enter] next to "Login Password".**



Note

❒ If assigning the administrator for the first time, proceed to step 7 without pressing **[Enter]**.

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

7 **Enter [Login].**

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

Logging off Using Administrator Authentication

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

1 **Press [Logout].**

2 **Press [Yes].**

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

Changing the Administrator

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

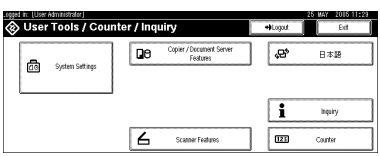
For example, to assign machine administrator authority and user administrator authority to **[Administrator 1]**, press **[Administrator 1]** in the lines for the machine administrator and the user administrator.

Preparation

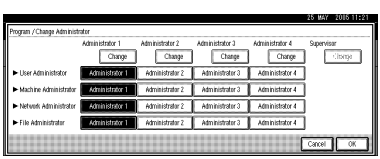
For details about logging on with administrator authentication, see p.73 "Logging on Using Administrator Authentication".

For details about logging off with administrator authentication, see p.74 "Logging off Using Administrator Authentication".

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



3. **Press [Administrator Tools].**
4. **Press [Program / Change Administrator].**
5. **In the line for the administrator you want to change, press [Administrator 1], [Administrator 2], [Administrator 3] or [Administrator 4], and then press [Change].**



6. **Press [Change] for the setting you want to change, and re-enter the setting.**
7. **Press [OK].**
8. **Press [OK].**
9. **Press the [User Tools/Counter] key.**

Specifying the Extended Security Functions

As well as providing basic security through user authentication and the machine access limits specified by the administrators, you can increase security by, for instance, encrypting transmitted data and data in the address book. If you need extended security, specify the machine's extended security functions before using the machine.

This section outlines the extended security functions and how to specify them. For details about when to use each function, see the corresponding chapters.

Changing the Extended Security Functions

To change the extended security functions, display the extended security screen as follows:

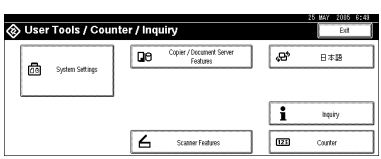
Preparation

For details about logging on with administrator authentication, see p.73 "Logging on Using Administrator Authentication".

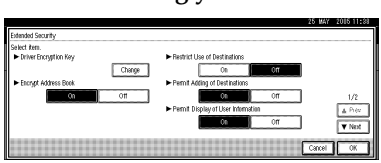
For details about logging off with administrator authentication, see p.74 "Logging off Using Administrator Authentication".

Procedure for Changing the Extended Security Functions

1. **Press the 【User Tools/Counter】 key.**
2. **Press [System Settings].**



3. **Press [Administrator Tools].**
4. **Press [Extended Security].**
5. **Press the setting you want to change, and change the setting.**



6 Press [OK].

7 Press the [User Tools/Counter] key.

Settings

❖ **Driver Encryption Key**

This can be specified by the network administrator. Encrypt the password transmitted when specifying user authentication. If you register the encryption key specified with the machine in the driver, passwords are encrypted.

- Driver Encryption Key

Reference

See the TWAIN driver Help.

❖ **Encrypt Address Book**

This can be specified by the user administrator. Encrypt the data in the machine's address book.

Even if one of the machine's internal parts is removed, the data in the address book is protected by encryption and cannot be read.

- On
- Off

Note

❒ Default: *Off*

❖ **Restrict Use of Destinations**

This can be specified by the user administrator.

The available scanner destinations are limited to the destinations registered in the address book.

A user cannot directly enter the destinations for transmission.

Note

❒ The destinations searched by "Search LDAP" can be used.

- On
- Off

Note

❒ Default: *On*

❖ **Permit Adding of Destinations**

This can be specified by the user administrator.

When "Restrict Use of Destinations" is set to **[Off]**. After directly entering a scanner destination, you can register it in the address book by pressing **[ProgDest]**. If this setting is set to **[Off]**, **[ProgDest]** does not appear. This prevents the registration of destinations not managed by the administrator.

- On
- Off

Note

❒ Default: *On*

❖ **Permit Display of User Information**

This can be specified if user authentication is specified. When the job history is checked using a network connection for which authentication is not available, all personal information can be displayed as "********". For example, when someone not authenticated as an administrator checks the job history using SNMP in SmartDeviceMonitor for Admin, personal information can be displayed as "********" so users cannot be identified. Because no information identifying registered users can be viewed, unauthorized users can be prevented from obtaining information about the registered files.

- On
- Off

Note

❒ Default: *On*

❖ **Enhance File Protection**

This can be specified by the file administrator. By specifying a password, you can limit operations such as deleting, and sending files, and can prevent unauthorized people from accessing the files. However, it is still possible for the password to be cracked.

By specifying "Enhance File Protection", files are locked and so become inaccessible if an invalid password is entered ten times. This can protect the files from unauthorized access attempts in which a password is repeatedly guessed.

The locked files can only be unlocked by the file administrator. When "Enhance File Protection" is specified, ( ) appears at the top right of the screen.

Note

❒ If files are locked, you cannot select them even if the correct password is entered.

- On
- Off

Note

❒ Default: *Off*

❖ **Permit Settings by SNMP V1 and V2**

This can be specified by the network administrator. When the machine is accessed using the SNMPv1, v2 protocol, authentication cannot be performed, allowing machine administrator settings such as the paper setting to be changed. If you select **[Off]**, the setting can be viewed but not specified with SNMPv1, v2.

- On
- Off

Note

❒ Default: *On*

❖ **Permit Simple Encryption**

This can be specified by the machine administrator.
Under Windows95/98/Me, advanced encryption is not possible with the printer driver, so simple encryption is used. If you select **[Off]**, printing with simple encryption is not allowed and you cannot connect using the printer driver under Windows95/98/Me. Specify this setting when using a driver that does not support advanced encryption.

Limitation

❒ When this setting is set to **[Off]** and you want to edit the address book in **[User Management Tool]** or **[Address Management Tool]** in SmartDeviceMonitor for Admin, or you want to access the machine using DeskTopBinder or the ScanRouter software, enable SSL/TLS for encrypted communication. For details about specifying SSL/TLS, see p.42 "Setting the SSL / TLS Encryption Mode".

- On
- Off

Note

❒ Default: *Off*

Limiting Machine Operation to Customers Only

The machine can be set so that operation is impossible without administrator authentication.

The machine can be set to prohibit operation without administrator authentication and also prohibit remote registration in the address book by a service representative.

We maintain strict security when handling customers' data. Also, by being authenticated by an administrator to use the machine, we operate the machine under the customer's control.

Use the following settings.

- Service Mode Lock

Settings

❖ **Service Mode Lock**

This can be specified by the machine administrator. Service mode is used by a customer engineer for inspection or repair. If you set the service mode lock to **[On]**, service mode cannot be used unless the machine administrator logs onto the machine and cancels the service mode lock to allow the customer engineer to operate the machine for inspection and repair. This ensures that the inspection and repair are done under the supervision of the machine administrator.

Specifying Service Mode Lock

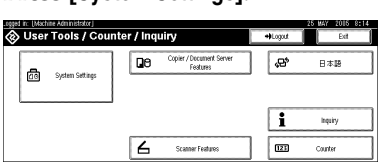
Preparation

For details about logging on with administrator authentication, see p.73 "Logging on Using Administrator Authentication".

For details about logging off with administrator authentication, see p.74 "Logging off Using Administrator Authentication".

1 **Press the 【User Tools/Counter】 key.**

2 **Press [System Settings].**



3 **Press [Administrator Tools].**

4 **Press [Service Mode Lock].**

5 **Press [On] and then [OK].**

A confirmation message appears.

6 **Press [Yes].**

7 **Press the 【User Tools/Counter】 key.**

Canceling Service Mode Lock

For a customer engineer to carry out inspection or repair in service mode, the machine administrator must log onto the machine and cancel the service mode lock.

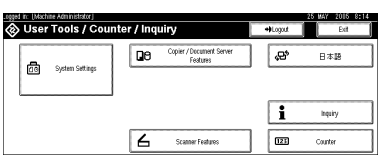
Preparation

For details about logging on with administrator authentication, see p.73 “Logging on Using Administrator Authentication”.

For details about logging off with administrator authentication, see p.74 “Logging off Using Administrator Authentication”.

1 **Press the 【User Tools/Counter】 key.**

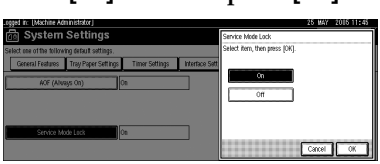
2 **Press [System Settings].**



3 **Press [Administrator Tools].**

4 **Press [Service Mode Lock].**

5 **Press [Off] and then press [OK].**



6 **Press the 【User Tools/Counter】 key.**

The customer engineer can switch to service mode.

Authentication Does Not Work Properly

This section explains what to do if a user cannot operate the machine because of a problem related to user authentication. Refer to this section if a user comes to you with such a problem.

A Message Appears

This section explains how to deal with problems if a message appears on the screen during user authentication.

The most common messages are explained. If some other message appears, deal with the problem according to the information contained in the message.

Messages	Causes	Solutions
`You do not have the privileges to use this function.`	The authority to use the function is not specified.	• If this appears when trying to use a function: The function is not specified in the address book management setting as being available. The user administrator must decide whether to authorize use of the function and then assign the authority. • If this appears when trying to specify a default setting: The administrator differs depending on the default settings you wish to specify. Using the list of settings, the administrator responsible must decide whether to authorize use of the function.

Messages	Causes	Solutions
Authentication has failed.	The entered login user name or login password is not correct	Inquire the user administrator for the correct login user name and login password.
	The number of users registered in the address book has reached the maximum limit allowed by Windows Authentication or LDAP Authentication, so you cannot register additional users.	Delete unnecessary user addresses.
	Cannot access the authentication server when using Windows authentication or LDAP authentication.	A network or server error may have occurred. Contact to the network administrator.
Selected files contain file(s) that the user does not have access privileges to. Please note that only the files with access privileges will be deleted.	You have tried to delete files without the authority to do so.	Files can be deleted by the file creator (owner) or file administrator. To delete a file which you are not authorized to delete, contact the file creator (owner).

Machine Cannot Be Operated

If the following conditions arise while users are operating the machine, provide instructions on how to deal with them.

Condition	Cause	Solution
Cannot connect using the TWAIN driver.	The encryption key specified in the driver does not match the machine's driver encryption key.	Specify the driver encryption key registered in the machine. See p.34 "Driver Encryption Key".
	If "Permit Simple Encryption" is set to **[Off]**, data sent by the driver uses simple encryption.	Under Windows NT 4.0, Windows 2000/XP, and Windows server 2003, enable driver encryption. Under Windows 95/98/Me, you can use only simple encryption, so you cannot print. Under Windows 95/98/Me, set "Permit Simple Encryption" to **[On]** in the machine's **[System Settings]**.
Cannot authenticate using the TWAIN driver.	Another user is logging on to the machine.	Wait for the user to log off.
	Authentication is taking time because of operating conditions.	Make sure the LDAP server setting is correct. Make sure the network settings are correct.
	Authentication is not possible while the machine is editing the address book data.	Wait until editing of the address book data is complete.
Cannot log on to the machine using **[Document Server: Authentication/Encryption:]** in DeskTopBinder. Cannot access the machine using ScanRouter EX Professional V3 / ScanRouter EX Enterprise V2.	"Permit Simple Encryption" is not set correctly. Alternatively, **[SSL/TLS]** has been enabled although the required certificate is not installed in the computer.	Set "Permit Simple Encryption" to **[On]**. Alternatively, enable **[SSL/TLS]**, install the server certificate in the machine, and then install the certificate in the computer. **Reference** See p.79 "Permit Simple Encryption". See p.42 "Setting the SSL / TLS Encryption Mode".
Cannot connect to the ScanRouter delivery software.	The ScanRouter delivery software may not be supported by the machine.	Update to the latest version of the ScanRouter delivery software.
Cannot log off when using the copying or scanner functions.	The original has not been scanned completely.	When the original has been scanned completely, press **[#]**, remove the original, and then log off.

Condition	Cause	Solution
Cannot access the machine using ScanRouter EX Professional V2.	ScanRouter EX Professional V2 does not support user authentication.	
[ProgDest] does not appear on the scanner's screen for specifying destinations.	**[Permit Adding of Destinations]** is set to **[Off]** in **[Restrict Use of Destinations]** in **[Extended Security]**, so only the user administrator can register destinations in the address book.	Registration must be done by the user administrator.
Stored files do not appear.	User authentication may have been disabled while **[All Users]** is not specified.	Re-enable user authentication, and then enable **[All Users]** for the files that did not appear. For details about enabling **[All Users]**, see p.9 "Specifying Access Permission for Stored Files".
Destinations specified using the machine do not appear.	User authentication may have been disabled while **[All Users]** is not specified.	Re-enable user authentication, and then enable **[All Users]** for the destinations that did not appear. For details about enabling **[All Users]**, see p.18 "Protecting the Address Book".
If you try to interrupt a job while copying or scanning, an authentication screen appears.	With this machine, you can log off while copying or scanning. If you try to interrupt copying or scanning after logging off, an authentication screen appears.	Only the user who executed a copying or scanning job can interrupt it.Wait until the job has completed or consult an administrator or the user who executed the job.
Cannot register entries in **[Program No.10]** for program registration in the copier function.	If "Change Initial Mode" is set to **[Program No.10]** in **[General Features]** in **[Copier / Document Server Features]**, entries can be registered in **[Program No.10]** only by the machine administrator.	The machine administrator must carry out the registration.

Operations by the Supervisor

The supervisor can delete an administrator's password and specify a new one. If any of the administrators forget their passwords or if any of the administrators change, the supervisor can assign a new password. If logged on using the supervisor's user name and password, you cannot use normal functions or specify defaults. Log on as the supervisor only to change an administrator's password.

Important

- ❒ The default login user name is "supervisor" and the login password is blank. We recommend changing the login user name and login password.
- ❒ When registering login user names and login passwords, you can specify up to 32 alphanumeric characters and symbols. Keep in mind that user names and passwords are case-sensitive.
- ❒ Be sure not to forget the supervisor login user name and login password. If you do forget them, a service representative will to have to return the machine to its default state. This will result in all data in the machine being lost and the service call may not be free of charge.

Note

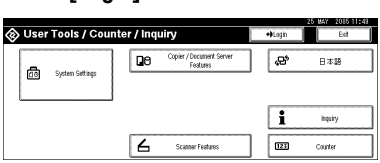
- ❒ You cannot specify the same login user name for the supervisor and the administrators.
- ❒ Using Web Image Monitor, you can log on as the supervisor and delete an administrator's password.

Logging on as the Supervisor

If administrator authentication has been specified, log on using the supervisor login user name and login password. This section describes how to log on.

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

2 **Press [Login].**



3 **Press [Enter] for [Login User Name].**

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

Note

❒ When you assign the administrator for the first time, enter "supervisor".

5 **Press [Enter] for [Login Password].**

6 **Enter a login password, and then press [OK].**

Note

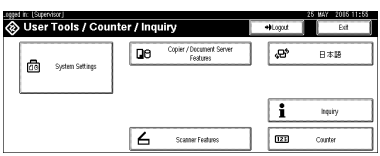
❒ When you assign the administrator for the first time, proceed to step 7 without pressing **[Enter]**.

7 **Press [Login].**

Logging off as the Supervisor

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

1 **Press [Logout].**



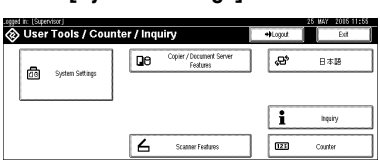
2 **Press [Yes].**

3 **Press the 【User Tools/Counter】 key.**

Changing the Supervisor

1 **Press the 【User Tools/Counter】 key.**

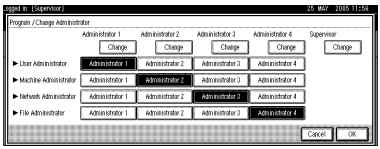
2 **Press [System Settings].**



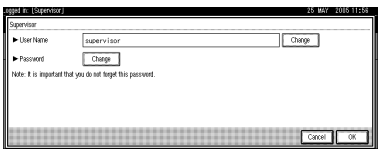
3 **Press [Administrator Tools].**

4 **Press [Program / Change Administrator].**

5 **Under "Supervisor", click [Change].**



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



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

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

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

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

11 **Press [OK].**

12 **Press [OK].**

13 **Press the 【User Tools/Counter】 key.**

Resetting an Administrator's Password

1 **Press the 【User Tools/Counter】 key.**

2 **Press [Login].**

3 **Log on as the supervisor.**

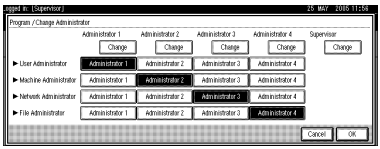
You can log on in the same way as an administrator.

4 **Press [System Settings].**

5 **Press [Administrator Tools].**

6 **Press [Program / Change Administrator].**

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



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

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

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

11 **Press [OK].**

12 **Press [OK].**

13 **Press the 【User Tools/Counter】 key.**

Machine Administrator Settings

The machine administrator settings that can be specified are as follows:

System Settings

The following settings can be specified.

❖ **General Features**
All the settings can be specified.

❖ **Tray Paper Settings**
All the settings can be specified.

❖ **Timer Settings**
All the settings can be specified.

❖ **Interface Settings**

- Machine Name
- Panel Off Timer

❖ **File Transfer**
The following settings can be specified.

- Delivery Option
- SMTP Authentication
  SMTP Authentication
  User Name
  E-mail Address
  Encryption
  Reception Protocol
- POP before SMTP
- POP3 Setting
  Server Name
  Encryption
- Administrator's E-mail Address
- Default User Name / Password (Send)
  SMB User Name
  FTP User Name
- Program / Change / Delete E-mail Message
- Program / Change / Delete Subject

❖ Administrator Tools

- User Authentication Management
  You can specify which authentication to use.
  You can also edit the settings for each function.
- Administrator Authentication Management
  Machine Management
- Program / Change Administrator
  Machine Administrator
  You can change the user name and the full-control user's authority.
- Key Counter Management
- External Charge Unit Management
- Enhanced External Charge Unit Management
- Extended Security
  Permit Display of User Information
- Display / Print Counter
  Display / Print Counter
- Display / Clear / Print Counter per User
  Display / Print Counter
- AOF (Always On)
- Program / Change / Delete LDAP Server
  Server Name
  Search Base
  Port No.
  Authentication
  User Name
  Password
  Japanese Chara. Code
  Search Conditions
  Search Options
- Use LDAP Server
- Service Mode Lock
- Auto Erase Memory Setting [*1]
- Erase All Memory [*1]

[*1] The DataOverwriteSecurity unit option must be installed.

Copier/Document Server Features

The following settings can be specified.

❖ **General Features**
All the settings can be specified.

❖ **Reproduction Ratio**
All the settings can be specified.

❖ **Edit**
All the settings can be specified.

❖ **Stamp**
All the settings can be specified.

❖ **Input / Output**
All the settings can be specified.

❖ **Administrator Tools**
All the settings can be specified.

Scanner Features

The following settings can be specified.

❖ **Scan Settings**
All the settings can be specified.

❖ **Destination List Settings**
All the settings can be specified.

❖ **Send Settings**
The following settings can be specified.

- TWAIN Standby Time
- File Type Priority
- Compression (Black & White)
- Print & Delete Scanner Journal
- E-mail Information Language
- Store File Priority
- Delete Scanner Journal
- Print Scanner Journal

❖ **Administrator Tools**
All the settings can be specified.

Settings via Web Image Monitor

The following settings can be specified.

❖ Top Page

- Reset Device

❖ Device Settings

- System
  Device Name
  Output Tray
  Paper Tray Priority
- Paper
  All the settings can be specified.
- Timer Settings
  All the settings can be specified.
- E-mail
  All the settings can be specified.
- File Transfer
  All the settings can be specified.
- User Authentication Management
  All the settings can be specified.
- Program/Change Administrator
  You can specify the following administrator settings as the machine administrator.
  Login User Name
  Login Password
  Change Encryption Password
- Administrator Authentication Management
  Machine Administrator Authentication
  Available Settings for Machine Administrator

❖ Network

- SNMPv3
- Access Type (Machine Administrator)

Settings via SmartDeviceMonitor for Admin

The following settings can be specified.

❖ **Device Information**

- Reset Device
- Reset Current Job
- Reset All Jobs

❖ **User Management Tool**

The following settings can be specified.

- User Counter Information
- Access Control List
- Reset User Counters
- Automatically add user codes

Network Administrator Settings

The network administrator settings that can be specified are as follows:

System Settings

The following settings can be specified.

❖ Interface Settings

- Network
  All the settings can be specified.
- IEEE 1394 *1
  All the settings can be specified.
- IEEE 802.11b *2
  All the settings can be specified.

Note

❒ If **[DHCP]** is set to **[On]**, the settings that are automatically obtained via DHCP cannot be specified.

*1 The IEEE1394 interface board option must be installed.
*2 The IEEE802.11b interface unit option must be installed.

❖ File Transfer

- SMTP Server
  SMTP Server Name
  Port No.
- E-mail Communication Port
- Scanner Recall Interval Time
- Number of Scanner Recalls
- Auto Specify Sender Name

❖ Administrator Tools

- Administrator Authentication Management
  Network Management
- Program / Change Administrator
  Network Administrator
  You can specify the user name and change the full-control user's authority.
- Extended Security
  Driver Encryption Key
  Permit Simple Encryption
  Permit Settings by SNMP V1 and V2

Scanner Features

The following settings can be specified.

❖ Send Settings

- Max. E-mail Size
- Divide & Send E-mail

Settings via Web Image Monitor

The following settings can be specified.

❖ Device Settings

- System
  Comment
  Location
- E-mail
  SMTP Server Name
  SMTP Port No.
  POP Port No.
- Program/Change Administrator
  You can specify the following administrator settings for the machine administrator.
  Login User Name
  Login Password
  Change Encryption Password
- Administrator Authentication Management
  Network Administrator Authentication
  Available Settings for Network Administrator

❖ Interface Settings

- Change Interface
- IEEE 802.11b *1
  Communication Mode
  SSID
  Channel
  WEP Setting
  Authentication Type
  WEP Key Status
  Key
  Confirm Key
- IEEE 1394 *2
  IP over 1394
  SCSI print (SBP-2)
  Bidirectional SCSI print

*1 The IEEE802.11b interface unit option must be installed.
*2 The IEEE1394 interface board option must be installed.

❖ Network

- Protocol
  All the settings can be specified.
- TCP/IP
  All the settings can be specified.
- NetWare
  All the settings can be specified.
- AppleTalk
  All the settings can be specified.
- SMB
  All the settings can be specified.
- SNMP
  All the settings can be specified.
- SNMPv3
  SNMPv3
  Protocol
  SNMP v3 Function
  SNMPv3 Trap Communication
  Authentication Algorithm
  Permit SNMP v3 Communication
  SNMPv3 Trap Communication Setting
  Account Name (User)
  Authentication Password (User)
  Encryption Password (User)
  Access Type (User)
  Access Type (Network Administrator)
- Rendezvous
  All the settings can be specified.

❖ Webpage

All the settings can be specified.

❖ Security

- Access Control
  All the settings can be specified.
- IPP Authentication
  All the settings can be specified.
- SSL/TLS
  All the settings can be specified.
- Certificates
  All the settings can be specified.

Settings via SmartDeviceMonitor for Admin

The following settings can be specified.

❖ **NIB Setup Tool**
All the settings can be specified.

File Administrator Settings

The file administrator settings that can be specified are as follows:

System Settings

The following settings can be specified.

❖ **Administrator Tools**

- Administrator Authentication Management
  File Management
- Program / Change Administrator
  File Administrator
- Extended Security
  Enhance File Protection

Settings via Web Image Monitor

The following settings can be specified.

❖ **Document Server**

All the settings can be specified.

❖ **Device Settings**

- Program/Change Administrator
  You can specify the following administrator settings for the file administrator.
  Login User Name
  Login Password
  Change Encryption Password
- Administrator Authentication Management
  File Administrator Authentication
  Available Settings for File Administrator

User Administrator Settings

The user administrator settings that can be specified are as follows:

System Settings

The following settings can be specified.

❖ **Administrator Tools**

- Administrator Authentication Management
  User Management
- Program / Change Administrator
  User Administrator
- Extended Security
  Restrict Use of Destinations
  Permit Adding of Destinations
  Encrypt Address Book
- Print Address Book: Destination List
- Address Book Management
- Address Book: Program / Change / Delete Group
- Address Book: Change Order
- Address Book: Edit Title
- Address Book: Select Title

Settings via Web Image Monitor

The following settings can be specified.

❖ **Address Book**

All the settings can be specified.

❖ **Device Settings**

- Program/Change Administrator
  The user administrator settings that can be specified are as follows:
  Login User Name
  Login Password
  Change Encryption Password
- Administrator Authentication Management
  File Administrator Authentication
  Available Settings for File Administrator

Settings via SmartDeviceMonitor for Admin

The following settings can be specified.

❖ **Address Management Tool**
All the settings can be specified.

❖ **User Management Tool**

- Restrict Access To Device
- Add New User
- Delete User
- User Properties

The Available Functions for Using the Files Stored in Document Server

The authorities for using the files stored in Document Server are as follows:

The authority designations in the list indicate users with the following authorities.

- Read-only
  This is a user assigned "Read-only" authority.
- Edit
  This is a user assigned "Edit" authority.
- Edit / Delete
  This is a user assigned "Edit / Delete" authority.
- Full Control
  This is a user granted full control.
- Owner
  This is a user who can store files in the machine and authorize other users to view, edit, or delete those files.
- File Administrator
  This is the file administrator.

❍ =Granted authority to operate.

- =Not granted authority to operate.

User	Viewing Details about Stored Files	Viewing Thumbnails	Print/Transmission	Changing Information about Stored Files	Deleting Files	Specifying File Password	Specifying Permissions for Users/Groups	Unlocking Files
Read-only	❍	❍	❍	-	-	-	-	-
Edit	❍	❍	❍	❍	-	-	-	-
Edit / Delete	❍	❍	❍	❍	❍	-	-	-
Full Control	❍	❍	❍	❍	❍	-	❍	-
Owner	❍	❍	❍	❍	❍	❍	❍	-
File Administrator	❍	❍	-	-	❍	❍	❍	❍

Settings That Can Be Specified In the Address Book

The authorities for using the address book are as follows:

The authority designations in the list indicate users with the following authorities.

- Read-only
  This is a user assigned “Read-only” authority.
- Edit
  This is a user assigned “Edit” authority.
- Edit / Delete
  This is a user assigned “Edit / Delete” authority.
- Full Control
  This is a user granted full control.
- Registered User
  This is a user whose personal information is registered in the address book. The registered user is the user who knows the login user name and password.
- User Administrator
  This is the user administrator.

❍ =You can view and change the setting.

▲ =You can view the setting.

- =You cannot view or specify the setting.

Settings		User			User Administrator	Registered User	Full Control
		Read-only	Edit	Edit / Delete			
Registration No.		▲	❍	❍	❍	❍	❍
Key Display		▲	❍	❍	❍	❍	❍
Name		▲	❍	❍	❍	❍	❍
Select Title		▲	❍	❍	❍	❍	❍
Auth. Info	User Code	-	-	-	❍	-	-
	Login User Name	-	-	-	❍	❍	-
	Login Password	-	-	-	❍ *1	❍ *1	-
	SMTP Authentication	-	-	-	❍ *1	❍ *1	-
	Folder Authentication	▲	❍	❍	❍	❍	-
	LDAP Authentication	-	-	-	❍ *1	❍ *1	-
	Available Functions	-	-	-	❍	▲	-
Protection	Use Name as	▲	▲	▲	❍	❍	▲
	Protection Code	-	-	-	❍ *1	❍ *1	❍ *1
	Protection Object	▲	▲	▲	❍	❍	▲
	Protect Dest.: Permissions for Users/Groups	-	-	-	❍	❍	❍
	Protect File(s): Permissions for Users/Groups	-	-	-	❍	❍	❍
E-mail Address	E-mail Address	▲	❍	❍	❍	❍	-

Settings		User			User Administrator	Registered User	Full Control
		Read-only	Edit	Edit / Delete			
Folder Destination	SMB/FTP	▲	❍	❍	❍	❍	-
	SMB: Path	▲	❍	❍	❍	❍	-
	FTP: Server Name	▲	❍	❍	❍	❍	-
	FTP: Path	▲	❍	❍	❍	❍	-
	Japanese Chara. Code	▲	❍	❍	❍	❍	-

*1 You can only enter the password.

User Settings

If you have specified administrator authentication, the available functions and settings depend on the menu protect setting.

The following settings can be specified by someone who is not an administrator.

❍ =You can view and change the setting.

▲ =You can view the setting.

- =You cannot view or specify the setting.

Note

❒ Settings that are not in the list can only be viewed, regardless of the menu protect level setting.

Copier/Document Server Features

The default for **[Menu Protect]** is **[Level 2]**.

Tab Names	Settings	Menu Protect		
		Off	Level 1	Level 2
General Features	Copy Quality	❍	❍	▲
	Image Density	❍	❍	▲
Edit	Erase Original Shadow in Combine	❍	❍	▲
	Copy Order in Combine	❍	❍	▲
	Image Repeat Separation Line	❍	❍	▲
	Double Copies Separation Line	❍	❍	▲
	Separation Line in Combine	❍	❍	▲
	Program / Delete Format	❍	❍	▲
	Partial Copy Priority	❍	❍	▲

Tab Names		Settings	Menu Protect		
			Off	Level 1	Level 2
Stamp	Background Numbering	Size	❍	❍	▲
		Density	❍	❍	▲
	Preset Stamp	Stamp Position: COPY *1	❍	❍	▲
		Stamp Position: URGENT *1	❍	❍	▲
		Stamp Position: PRIORITY *1	❍	❍	▲
		Stamp Position: For Your Info. *1	❍	❍	▲
		Stamp Position: Preliminary *1	❍	❍	▲
		Stamp Position: For internal use *1	❍	❍	▲
		Stamp Position: CONFIDENTIAL *1	❍	❍	▲
		Stamp Position: DRAFT *1	❍	❍	▲
		Stamp Language	❍	❍	▲
	User Stamp	Program / Delete Stamp	❍	❍	▲
		Stamp Position: 1	❍	❍	▲
		Stamp Format: 1	❍	❍	▲
		Stamp Position: 2	❍	❍	▲
		Stamp Format: 2	❍	❍	▲
		Stamp Position: 3	❍	❍	▲
		Stamp Format: 3	❍	❍	▲
		Stamp Position: 4	❍	❍	▲
		Stamp Format: 4	❍	❍	▲
	Date Stamp	Format	❍	❍	▲
		Font	❍	❍	▲
		Stamp Position: *1	❍	❍	▲
		Size	❍	❍	▲
		Superimpose	❍	❍	▲

Tab Names		Settings	Menu Protect		
			Off	Level 1	Level 2
Stamp	Page Numbering	Stamp Format	❍	❍	▲
		Font	❍	❍	▲
		Size	❍	❍	▲
		Page Numbering in Combine	❍	❍	▲
		Stamp Position: P1, P2… *1	❍	❍	▲
		Stamp Position: 1/5, 2/5… *1	❍	❍	▲
		Stamp Position: 1, 2… *1	❍	❍	▲
		Stamp Position: -1-, -2-… *1	❍	❍	▲
		Stamp Position: P.1, P.2… *1	❍	❍	▲
		Stamp Position: 1-1, 1-2… *1	❍	❍	▲
		Superimpose	❍	❍	▲

*1 You can adjust the print position but not specify it.

Scanner Features

The default for **[Menu Protect]** is **[Level 2]**.

Tab Names	Settings	Menu Protect		
		Off	Level 1	Level 2
Destination List Settings	Update Delivery Server Destination List	❍	❍	▲
Send Settings	Compression (Black & White)	❍	❍	▲
	E-mail Information Language	❍	❍	▲

System Settings

The settings available to the user depend on whether or not administrator authentication has been specified.

If administrator authentication has been specified, the settings available to the user depend on whether or not "Available Settings" has been specified.

Tab Names	Settings	Administrator authentication has not been specified.	Administrator authentication has been specified.	
			"Available Settings" has been specified.	"Available Settings" has not been specified.
General Features	Panel Tone	❍	❍	▲
	Warm Up Notice	❍	❍	▲
	Copy Count Display	❍	❍	▲
	Function Priority	❍	❍	▲
	Print Priority	❍	❍	▲
	Function Reset Timer	❍	❍	▲
	Interleave Print	❍	❍	▲
	Output: Copier	❍	❍	▲
	Output: Document Server	❍	❍	▲
Tray Paper Settings	Paper Tray Priority: Copier	❍	❍	▲
	Tray Paper Size: Tray 1-4	❍	❍	▲
	Paper Type: Bypass Tray	❍	❍	▲
	Paper Type: Tray 1-4	❍	❍	▲
Timer Settings	Auto Off Timer	❍	❍	▲
	Panel Off Timer	❍	❍	▲
	Energy Saver Timer	❍	❍	▲
	System Auto Reset Timer	❍	❍	▲
	Copier/ Document Server Auto Reset Timer	❍	❍	▲
	Scanner Auto Reset Timer	❍	❍	▲
	Auto Logout Timer	❍	❍	▲
	Set Date	❍	❍	▲
	Set Time	❍	❍	▲
	Auto Logout Timer	❍	❍	▲

Tab Names		Settings	Administrator authentication has not been specified.	Administrator authentication has been specified.	
				"Available Settings" has been specified.	"Available Settings" has not been specified.
Interface Settings	Network	IP Address *1	❍	❍	▲
		Sub-net Mask	❍	❍	▲
		Gateway Address	❍	❍	▲
		DNS Configuration *1	❍	❍	▲
		Domain Name *1	❍	❍	▲
		WINS Configuration *1	❍	❍	▲
		DDNS Configuration	❍	❍	▲
		Effective Protocol	❍	❍	▲
		NW Frame Type	❍	❍	▲
		SMB Computer Name	❍	❍	▲
		SMB Work Group	❍	❍	▲
		Ethernet Speed	❍	❍	▲
		LAN Type	❍	❍	▲
		Ping Command	❍	❍	▲
		Permit SNMP V3 Communication	❍	❍	▲
		Permit SSL / TLS Communication	❍	❍	▲
		Host Name	❍	❍	▲
	IEEE 1394 *5	IP Address *1	❍	❍	▲
		DDNS Configuration	❍	❍	▲
		Host Name	❍	❍	▲
		Domain Name *1	❍	❍	▲
		WINS Configuration *1	❍	❍	▲
		IP over 1394	❍	❍	▲
		SCSI print (SBP-2)	❍	❍	▲
		Bidirectional SCSI print	❍	❍	▲

Tab Names		Settings	Administrator authentication has not been specified.	Administrator authentication has been specified.	
				"Available Settings" has been specified.	"Available Settings" has not been specified.
Interface Settings	IEEE 802.11b *6	Communication Mode	❍	❍	▲
		Transmission Speed	❍	❍	▲
		SSID Setting	❍	❍	▲
		Channel	❍	❍	▲
	WEP (Encryption) Setting	WEP (Encryption) Setting *2	❍	❍	▲
		Transmission Speed	❍	❍	▲
		Return to Defaults	❍	❍	▲
	Print List		❍	❍	▲
File Transfer		Delivery Option *3	❍	❍	▲
		Capture Server IP Address	❍	❍	▲
		SMTP Server	❍	❍	▲
		SMTP Authentication *4	❍	❍	▲
		POP before SMTP	❍	❍	▲
		POP3 Setting	❍	❍	▲
		Administrator's E-mail Address	❍	❍	▲
		E-mail Communication Port	❍	❍	▲
		Default User Name / Password (Send) *4	❍	❍	▲
		Program / Change / Delete E-mail Message	▲	▲	▲
		Program / Change / Delete Subject	▲	▲	▲
		Scanner Recall Interval Time	❍	❍	▲
		Number of Scanner Recalls	❍	❍	▲
		Auto Specify Sender Name	❍	❍	▲

Tab Names	Settings	Administrator authentication has not been specified.	Administrator authentication has been specified.	
			"Available Settings" has been specified.	"Available Settings" has not been specified.
Administrator Tools	User Authentication Management	❍	❍	▲
	Administrator Authentication Management	❍	❍	▲
	Key Counter Management	❍	❍	▲
	External Charge Unit Management	❍	❍	▲
	Enhanced External Charge Unit Management	❍	❍	▲
	Display / Print Counter	❍	❍	▲
	Display / Clear / Print Counter per User	❍	❍	▲
	Print Address Book: Destination List	▲	▲	▲
	Address Book Management	▲	▲	▲
	Address Book: Program / Change / Delete Group	▲	▲	▲
	Address Book: Change Order	❍	❍	▲
	Address Book: Edit Title	❍	❍	▲
	Address Book: Select Title	❍	❍	▲
	Auto Delete File	❍	❍	▲
	Delete All Files	❍	❍	▲
	AOF (Always On)	❍	❍	▲
	Program / Change / Delete LDAP Server *4	❍	❍	▲
	Use LDAP Server	❍	❍	▲
	Service Mode Lock	❍	❍	▲
	Firmware Version	❍	❍	▲
	Auto Erase Memory Setting *7	❍	❍	▲
	Erase All Memory *7	❍	❍	▲

*1 If you select **[Auto-Obtain (DHCP)]**, you can only view the setting.
*2 You can only view the encryption setting.
*3 You can only view Main Delivery Server IP Address and Sub Delivery Server IP Address.
*4 You can only specify the password.
*5 The IEEE1394 interface board option must be installed.
*6 The IEEE802.11b interface unit option must be installed.
*7 The data overwrite security unit option must be installed.

Web Image Monitor Setting

❖ Device Settings

The settings available to the user depend on whether or not administrator authentication has been specified.
If administrator authentication has been specified, the settings available to the user depend on whether or not "Available Settings" has been specified.

Category	Settings	Administrator authentication has not been specified.	Administrator authentication has been specified.	
			"Available Settings" has been specified.	"Available Settings" has not been specified.
System	Comment	❍	❍	▲
	Location	❍	❍	▲
	Output Tray	❍	❍	▲
	Paper Tray Priority	❍	❍	▲
Paper	Paper Size	❍	❍	▲
	Paper Type	❍	❍	▲
	Apply Auto Paper Select	❍	❍	▲
Timer Settings	Auto Off Timer	❍	❍	▲
	Energy Saver Timer	❍	❍	▲
	Panel Off Timer	❍	❍	▲
	System Auto Reset Timer	❍	❍	▲
	Copier/Document Server Auto Reset Timer	❍	❍	▲
	Scanner Auto Reset Timer	❍	❍	▲
	Set Date	❍	❍	▲
	Set Time	❍	❍	▲
	SNTP Server Address	❍	❍	▲
	SNTP Polling Interval	❍	❍	▲
	Time Zone	❍	❍	▲

Category	Settings	Administrator authentication has not been specified.	Administrator authentication has been specified.	
			"Available Settings" has been specified.	"Available Settings" has not been specified.
E-mail	Administrator E-mail Address	❍	❍	▲
	SMTP Server Name	❍	❍	▲
	SMTP Port No.	❍	❍	▲
	SMTP Authentication	❍	❍	▲
	SMTP Auth. E-mail Address	❍	❍	▲
	SMTP Auth. Encryption	❍	❍	▲
	POP before SMTP	❍	❍	▲
	POP E-mail Address	❍	❍	▲
	Timeout setting after POP Auth.	❍	❍	▲
	POP Server Name	❍	❍	▲
	POP Auth. Encryption	❍	❍	▲
	POP Port No.	❍	❍	▲
	E-mail Notification E-mail Address	❍	❍	▲
File Transfer	SMB User Name	❍	❍	▲
	SMB Password *1	❍	❍	▲
	FTP User Name	❍	❍	▲
	FTP Password *1	❍	❍	▲
User Authentication Management	User Authentication Management	❍	❍	▲
	User Code - Available Function	❍	❍	▲
	Windows Authentication - Domain Name	❍	❍	▲
	Windows Authentication - Group Settings for Windows Authentication	❍	❍	▲
	LDAP Authentication - LDAP Authentication	❍	❍	▲
	LDAP Authentication - Login Name Attribute	❍	❍	▲
	LDAP Authentication - Unique Attribute	❍	❍	▲

*1 You can only specify the password.

❖ Interface

The settings available to the user depend on whether or not administrator authentication has been specified.
If administrator authentication has been specified, the settings available to the user depend on whether or not "Available Settings" has been specified.

Category	Settings	Administrator authentication has not been specified.	Administrator authentication has been specified.	
			"Available Settings" has been specified.	"Available Settings" has not been specified.
	Change Interface	❍	❍	▲
IEEE 802.11b *1	Communication Mode	❍	❍	▲
	Channel	❍	❍	▲
	WEP Setting	❍	❍	▲
	WEP Key Status	❍	❍	▲
	Authentication Type	❍	❍	▲
	Key	❍	❍	▲
	Confirm Key	❍	❍	▲
IEEE 1394 *2	IP over 1394	❍	❍	▲
	SCSI print (SBP-2)	❍	❍	▲
	Bidirectional SCSI print	❍	❍	▲

*1 The IEEE802.11b interface unit option must be installed.
*2 The IEEE1394 interface board option must be installed.

❖ Network

The settings available to the user depend on whether or not administrator authentication has been specified.
If administrator authentication has been specified, the settings available to the user depend on whether or not "Available Settings" has been specified.

Category	Settings	Administrator authentication has not been specified.	Administrator authentication has been specified.	
			"Available Settings" has been specified.	"Available Settings" has not been specified.
Protocol	LPR	❍	❍	▲
	RSH/RCP	❍	❍	▲
	DIPRINT	❍	❍	▲
	FTP	❍	❍	▲
	IPP	❍	❍	▲
	Rendezvous	❍	❍	▲
	NetWare	❍	❍	▲
	AppleTalk	❍	❍	▲
	SMB	❍	❍	▲
	SNMP	❍	❍	▲

Category	Settings	Administrator authentication has not been specified.	Administrator authentication has been specified.	
			"Available Settings" has been specified.	"Available Settings" has not been specified.
TCP/IP	Host Name	❍	❍	▲
	DHCP	❍	❍	▲
	Domain Name	❍	❍	▲
	IP Address	❍	❍	▲
	Subnet Mask	❍	❍	▲
	DDNS	❍	❍	▲
	WINS	❍	❍	▲
	Primary WINS Server	❍	❍	▲
	Secondary WINS Server	❍	❍	▲
	Scope ID	❍	❍	▲
	Default Gateway Address	❍	❍	▲
	DNS Server	❍	❍	▲
	LPR	❍	❍	▲
	RSH/RCP	❍	❍	▲
	DIPRINT	❍	❍	▲
	FTP	❍	❍	▲
	IPP	❍	❍	▲
	IPP Timeout	❍	❍	▲
	Rendezvous	❍	❍	▲

Category	Settings	Administrator authentication has not been specified.	Administrator authentication has been specified.	
			"Available Settings" has been specified.	"Available Settings" has not been specified.
NetWare	NetWare	❍	❍	▲
	Print Server Name	❍	❍	▲
	Logon Mode	❍	❍	▲
	File Server Name	❍	❍	▲
	NDS Tree	❍	❍	▲
	NDS Context Name	❍	❍	▲
	Operation Mode	❍	❍	▲
	Remote Printer No.	❍	❍	▲
	Frame Type	❍	❍	▲
	Print Server Protocol	❍	❍	▲
AppleTalk	AppleTalk	❍	❍	▲
	Printer Name	❍	❍	▲
	Zone Name	❍	❍	▲
SMB	SMB	❍	❍	▲
	Protocol	❍	❍	▲
	Workgroup Name	❍	❍	▲
	Computer Name	❍	❍	▲
	Comment	❍	❍	▲
	Notify Print Completion	❍	❍	▲
Rendezvous	Rendezvous	❍	❍	▲
	Computer Name	❍	❍	▲
	Location	❍	❍	▲
	PRIORITY (DIPRINT)	❍	❍	▲
	PRIORITY (LPR)	❍	❍	▲
	PRIORITY (IPP)	❍	❍	▲

Functions That Require Options

The following functions require certain options and additional functions.

- Hard Disk overwrite erases function
  DataOverwriteSecurity unit
- Data Encryption
  Scanner option

INDEX

S

T

U

W

Operating Instructions Security Reference

Printed in Japan
EN (USA)
AE (AE) B188-7571