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, are registered trademarks of Apple Computer, Inc.

Rendezvous is a trademark of Apple Computer Inc.

PostScript® and Acrobat® are registered trademarks of Adobe Systems, Incorporated.

PCL is a registered trademark of Hewlett-Packard Company.

NetWare is a registered trademarks of Novell, Inc.

Bluetooth is a Trademark of the Bluetooth SIG, Inc. (Special Interest Group) and licensed to Ricoh Company Limited.

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 Document Management Utility”

❖ **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 fax numbers, 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 printer in a network environment or using software.
This manual covers all models, and therefore contains functions and settings that may not be available for your model.
Images, illustrations, functions, and supported operating systems may differ from those of your model.

❖ **Copy Reference**

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

❖ **Facsimile Reference <Basic Features>**

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

❖ **Facsimile Reference <Advanced Features>**

Describes advanced facsimile functions such as line settings and procedures for registering IDs.

❖ **Printer Reference**

Describes system settings, operations, functions, and troubleshooting for the machine's printer function.

❖ Scanner Reference (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 Document Management Utility”.

- DeskTopBinder Lite Setup Guide (PDF file - CD-ROM2)
  Describes installation of, and the operating environment for DeskTopBinder 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 DeskTopBinder Lite is installed.

❖ Other manuals

- PostScript3 Supplement (PDF file-CD-ROM1)
- UNIX Supplement (available from an authorized dealer, or as a PDF file on our Web site)

TABLE OF CONTENTS

1. Getting Started

2. Preventing Information Leaks

3. Preventing Unauthorized Use of Functions and Settings

4. Enhanced Network Security

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.

1. Getting Started

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.99 “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 and printing.

❖ User

A user performs normal operations on the machine, such as copying and printing.

❖ 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.

Setting Up the Machine

If you want higher security, make the following setting before using the machine:

1. **Turn the machine on.**
2. **Press the 【User Tools/Counter】 key.**
3. **Press 【System Settings】.**
4. **Press 【Interface Settings】.**
5. **Specify IP Address.**
6. **Connect the machine to the network.**
7. **Start the Web browser, and then log on to the machine as the administrator.**
8. **Install the server certificate.**
9. **Enable secure sockets layer (SSL).**
10. **Enter the administrator's user name and password.**
11. **During steps 6 to 9, the administrator's default account (user name: admin, password: blank) in unencrypted form will be vulnerable to network interception, and this account may be used for breaking into the machine over the network.**

    If you consider this risky, we recommend that you specify a temporary administrator password between steps 1 and 6.

Security Measures Provided by this Machine

Preventing Information Leaks

❖ **Printing confidential files**

Using the printer's Locked Print, you can store files in the machine as confidential files and then print them. You can print a file using the machine's control panel and collect it on the spot to prevent others from seeing it.

Reference

For details, see p.16 "Printing a Confidential Document".

❖ **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.20 "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.20 "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 or fax 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.27 "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.

Reference

For details, see p.29 "Protecting the Address Book".

❖ Managing Log Files

You can improve data security by deleting log files stored in the machine. By transferring the log files, you can check the history data and identify unauthorized access.

Reference

For details, see p.33 "Log Information and Deleting Data on the Hard Disk".

❖ Overwriting the Data on the Hard Disk

Before disposing of the machine, make sure all data on the hard disk is deleted. Prevent data leakage by automatically deleting transmitted printer jobs from memory.

Reference

For details, see p.35 "Overwriting the Data on the Hard Disk".

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.20 "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.41 "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.42 "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.45 “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.

Reference

For details, see p.50 “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.

Reference

For details, see p.54 “Protection Using Encryption”.

2. Preventing Information Leaks

Guarding Against Unauthorized Copying

Using the printer driver, you can embed a pattern in the printed copy to discourage or prevent unauthorized copying.

If you enable data security for copying on the machine, printed copies of a document with data security for copying are grayed out to prevent unauthorized copying.

Make the setting as follows:

❖ Unauthorized Copy Prevention

① Using the printer driver, specify the printer settings for unauthorized copy prevention.
See p.13 “Specifying Printer Settings for Unauthorized Copy Prevention (Printer Driver Setting)”.

❖ Data Security for Copying

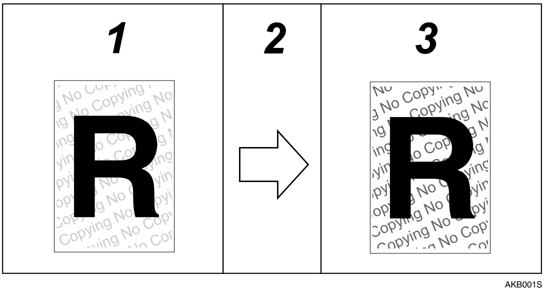
① Using the printer driver, specify the printer settings for data security for copying.
See p.14 “Specifying Printer Settings for Data Security for Copying (Printer Driver Setting)”.

② Specifying data security for copying on the machine. Printed copies of a document with data security for copying are grayed out.
See p.15 “Specifying Data Security for Copying (Machine Setting)”.

Unauthorized Copy Prevention

Using the printer driver, you can embed mask and pattern (for instance, a warning such as "No Copying") in the printed document.

If the document is copied, scanned, or stored in a Document Server by a copier or multifunction printer, the embedded pattern appears clearly on the copy, discouraging unauthorized copying.



***1.* Printed Documents**

Using the printer driver, you can embed background images and pattern in a printed document for Unauthorized Copy Prevention.

***2.* The document is copied, scanned, or stored in the Document Server.**

***3.* Printed Copies**

Embedded pattern (for instance, a warning such as “No Copying”) in a printed document appears conspicuously in printed copies.

Important

❒ Unauthorized copy prevention discourages unauthorized copying, and will not necessarily stop information leaks.

❒ The embedded pattern is not assured to be copied, scanned, or stored properly in the Document Server.

Limitation

❒ Depending on the machine and scanner settings, the embedded pattern may not be copied ,scanned, or stored in the Document Server.

Note

❒ To make the embedded pattern clear, set the character size to at least 50 pt (preferably 70 to 80 pt) and character angle to between 30 and 40 degrees.

Reference

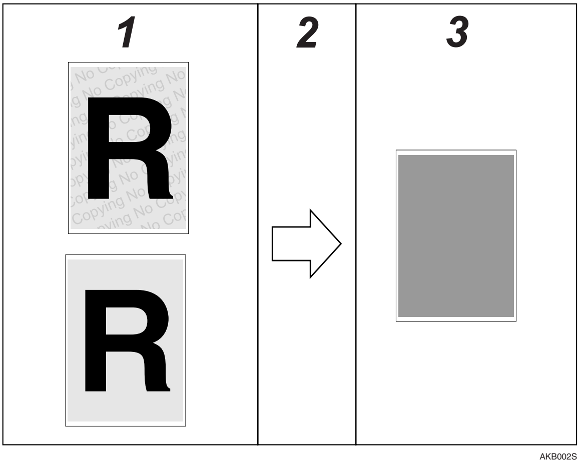
To use the printer function under the User Authentication, you must enter the login user name and password for the printer driver.

For details see the printer driver Help.

Data Security for Copying

Using the printer driver to enable data security for the copying function, you can print a document with an embedded pattern of hidden text. Such a document is called a data security for copying document.

If a data security for copying document is copied or stored in the Document Server using a copier or multi-function printer with the Copy Data Security Unit, protected pages are grayed out in the copy, preventing confidential information being copied. Also if a document with embedded pattern is detected, the machine beeps.



***1.* Documents with data security for copying**

***2.* The document is copied or stored in the Document Server.**

***3.* Printed Copies**

Text and images in the document are grayed out in printed copies.

Limitation

- ❒ To gray out copies of data security for copying documents when they are copied or stored in the Document Server, the optional Copy Data Security Unit must be installed in the machine.
- ❒ If the Copy Data Security Unit is installed in the machine, you cannot use the scanner and fax functions.
- ❒ If the Copy Data Security Unit is installed, you cannot specify a scaling factor less than 50% using the Control Panel under the Copier and Document Server functions.
- ❒ If a document with embedded pattern for data security for copying is copied, or stored in the Document Server by a copier or multi-function printer without Copy Data Security Unit, the embedded pattern appears conspicuously in the copy. However, how conspicuously the text appears depends on the model of the copier or multi-function printer being used and its scanning setting.

Note

❒ You can also embed pattern in a document protected by data security for copying. However, if such a document is copied or stored in the Document Server using a copier or multi-function printer with the Copy Data Security Unit, the copy is grayed out, so the embedded pattern does not appear on the copy.

❒ If misdetection occurs, contact your service representative.

❒ If a document with embedded pattern for data security for copying is copied, scanned, or stored in the Document Server using a copier or multi-function printer without the Copy Data Security Unit, the embedded pattern appears clearly on the copy.

❒ If a data security for copying document is detected, the machine beeps.

❒ If the scanned data security for copying document is registered as a user stamp, the machine does not beep, the file registered as a user stamp is grayed out, and no entry is added to the unauthorized copying log.

Printing Limitations

The following is a list of limitations on printing with unauthorized copy prevention and data security for copying.

❖ Unauthorized copy prevention / Data security for copying

Limitation

❒ You can print using the only RPCS printer driver.

❒ You cannot print at 200 dpi resolution.

❒ You cannot partially embed pattern in the printed document.

❒ You can only embed pattern that is entered in the **[Text]** box of the printer driver.

❒ Printing with embedding takes longer than normal printing.

❖ Data security for copying Only

Limitation

❒ Select 182 × 257 mm / 7.2 × 10.1 inches or larger as the paper size.

❒ Select Plain or Recycled with a brightness of 70% or more as the paper type.

❒ If you select Duplex, the data security for copying function may not work properly due to printing on the back of sheets.

Notice

1.The supplier does not guarantee that unauthorized copy prevention and data security for copying will always work. Depending on the paper, the model of copier or multi-function printer, and the copier or printer settings, unauthorized copy prevention and data security for copying may not work properly.

2.The supplier is not liable for any damage caused by using or not being able to use unauthorized copy prevention and data security for copying.

Printing with Unauthorized Copy Prevention and Data Security for Copying

Specifying Printer Settings for Unauthorized Copy Prevention (Printer Driver Setting)

Using the printer driver, specify the printer settings for unauthorized copy prevention.

Reference

To use the printer function under the User Authentication, you must enter the login user name and password for the printer driver.

For details see the printer driver Help.

For details about specifying data security for copying using the printer driver, see the printer driver Help.

1. **Open the printer driver dialog box.**
2. **On the [Edit] tab, select the [Unauthorized copy...] check box.**
3. **Click [Control Settings...].**
4. **In the [Text] box in the [Unauthorized copy prevention: Text] group, enter the text to be embedded in the printed document.**

   Also, specify **[Font]**, **[Font style:]**, and **[Size]**.
5. **Click [OK].**

   Reference

   For details, see the printer driver Help.

Specifying Printer Settings for Data Security for Copying (Printer Driver Setting)

If a document printed using this function is copied or stored in the Document Server by a copier or multi-function printer, the copy is grayed out.

Using the printer driver, specify the printer settings for data security for copying.

For details about data security for copying, see p.11 "Data Security for Copying".

Reference

To use the printer function under the User Authentication, you must enter the login user name and password for the printer driver.

For details see the printer driver Help.

For details about specifying data security for copying using the printer driver, see the printer driver Help.

1. **Open the printer driver dialog box.**
2. **On the [Edit] tab, select the [Unauthorized copy...] check box.**
3. **Click [Control Settings...].**
4. **In the [Unauthorized copy prevention: Pattern] group, check the [Data security for copying].**
5. **Click [OK].**

   Reference

   For details, see the printer driver Help.

Specifying Data Security for Copying (Machine Setting)

This can be specified by the machine administrator.

To use this function, the Copy Data Security Unit must be installed.

If a document printed is copied or stored in the Document Server, the copy is grayed out.

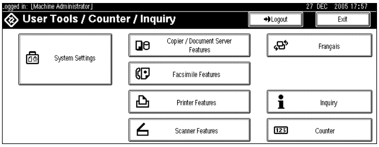
For details about data security for copying, see p.11 "Data Security for Copying".

Preparation

For details about logging on and logging off with administrator authentication, see p.106 "Logging on Using Administrator Authentication", p.107 "Logging off Using Administrator Authentication".

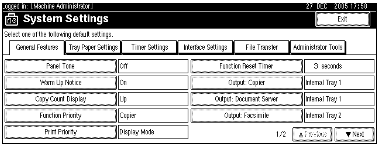
1 Press the 【User Tools/Counter】key.

2 Press [System Settings].



ogged in: [Machine Administrator] 27 DEC 2005 17:57

3 Press [Administrator Tools].



ogged in: [Machine Administrator] 27 DEC 2005 17:58

Select one of the following default settings.

Panel Tone: Off
Warm Up Notice: On
Copy Count Display: Up
Function Priority: Copier
Print Priority: Display Mode
Function Reset Timer: 3 seconds
Output: Copier: Internal Tray 1
Output: Document Server: Internal Tray 1
Output: Facsimile: Internal Tray 2

4 Press [Data security for copying].

If the setting you want to specify does not appear, press **[▼Next]** to scroll down to other settings.

5 Press[On].

If you do not want to specify **[Data security for copying]**, select **[Off]**.

6 Press[OK].

7 Press [Exit].

8 Press the 【User Tools/Counter】 key.

Printing a Confidential Document

Depending on the location of the machine, it is difficult to prevent unauthorized persons from viewing prints lying in the machine's output trays. When printing confidential documents, use the Locked Print function.

❖ **Locked Print**

Using the printer's Locked Print function, store files in the machine as Locked Print files and then print them from the control panel and retrieve them immediately, preventing others from viewing them.

Note

❒ To store files temporarily, select **[Stored Print]** under the printer function. If you select **[Share stored print files]**, also, you can share these files.

Choosing a Locked Print file

Using the printer driver, specify a Locked Print file.

Reference

If user authentication has been enabled, you must enter the login user name and login password using the printer driver. For details see the printer driver Help.

You can perform Locked Print even if user authentication is not enabled. For details see *Printer Reference*.

1 Open the printer driver dialog box.

2 Set [Job type:] to [Locked Print].

3 Click [Details...].

4 Enter the user ID and password.

Note

❒ The password entered here let you use the Locked Print function.

❒ To print a Locked Print file, enter the same password on the control panel.

Limitation

❒ Enter the user ID using up to 8 alphanumeric characters.

❒ Enter the password using 4 to 8 numbers.

5 Click [OK].

A confirmation message appears.

6 Confirm the password by re-entering it.

7 Click [OK].

8 Perform Locked Print.

Reference

For details, see the printer driver Help.

Printing a Locked Print File

To print a Locked Print file, face the machine and print the file using the control panel.

To print Locked Print files, the password is required. If you do not enter the correct password, you cannot print the files.

This can also be specified via Web Image Monitor.

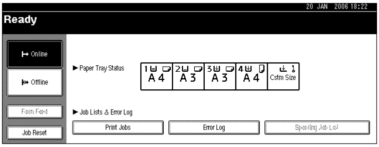
For details see the Web Image Monitor Help.

Preparation

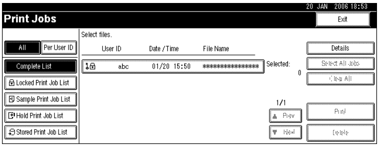
For details about logging on and logging off with user authentication, see p.92 "Login (Using the Control Panel)", p.92 "Log Off (Using the Control Panel)".

1 Press the 【Printer】 key.

2 Press [Print Jobs].



3 Press [Locked Print Job List].



Select files.

User ID	Date / Time	File Name
abc	01/20 15:50	****************

Selected: 0

Only Locked Print files belonging to the user who has logged on appear.

4 Select the Locked Print file to print.

5 Press [Print].

6 Enter the password for the stored file, and then press [OK].

Note

- ❒ Enter the password specified in step 4 on p.16 "Choosing a Locked Print file".

7 Press [Yes].

Deleting Locked Print Files

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

To delete Locked Print files, you must enter the password for the files. If the password has been forgotten, ask the file administrator to delete the password.

This can also be specified via Web Image Monitor.

For details see the Web Image Monitor Help.

Note

❒ Locked Print files can also be deleted by the file administrator.

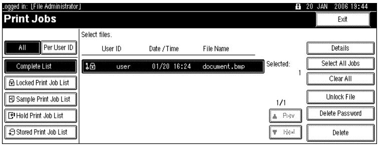
1 Press the 【Printer】 key.

2 Press [Print Jobs].

3 Press [Locked Print Job List].

4 Select the file.

5 Press [Delete].



Logged in: [File Administrator] 20 JAN 2006 19:44

Print Jobs

Select files.

	User ID	Date / Time	File Name
	user	01/20 16:24	document.bmp

Selected: 1

1/1

6 Enter the password of the Locked Print file, and then press [OK].

7 Press [Yes].

Deleting Passwords of Locked Print Files

If the file creator (owner) forgets the password for deleting Locked Print files, the file administrator must delete the password.

If the password is deleted, the files can be deleted but not printed.

This can also be specified via Web Image Monitor.

For details see the Web Image Monitor Help.

Note

❒ If you delete a password, and then turn the machine off and then back on, the deleted password is restored.

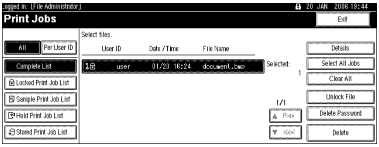
1 Press the 【Printer】key.

2 Press [Print Jobs].

3 Press [Locked Print Job List].

4 Select the file.

5 Press [Delete Password].



User ID	Date / Time	File Name
user	01/20 16:24	document.bmp

6 Press [Yes].

Unlocking Locked Print 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.109 “Specifying the Extended Security Functions”.

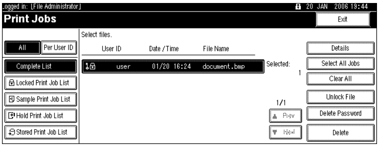
1 Press the 【Printer】 key.

2 Press [Print Jobs].

3 Press [Locked Print Job List].

4 Select the file.

5 Press [Unlock File].



User ID	Date / Time	File Name
user	01/20 16:24	document.bmp

6 Press [Yes].

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 printing or 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 print and send the files.
Edit	You can change the print settings for stored files. This includes permission to view files.
Edit / Delete	You can delete stored files. This includes permission to view and edit files.
Full Control	You can specify the user and access permission.This includes permission to view, edit, and edit / delete files.

Note

- ❒ Files can be stored by any user who is allowed to use the Document Server, scanner function, or fax 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”. You can also specify the access permission.

❖ 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.

Preparation

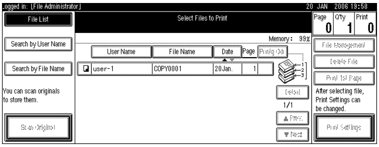
For details about logging on and logging off with administrator authentication, see p.106 "Logging on Using Administrator Authentication", p.107 "Logging off Using Administrator Authentication".

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.



Logged in: [File Administrator] 20 JAN 2006 19:58

Select Files to Print

Page 0 Q'ty 1 Print 0

Memory: 99%

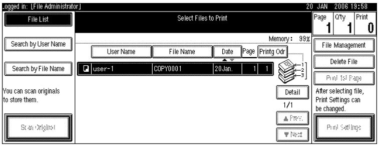
User Name	File Name	Date	Page	Printg Odr
user-1	COPY0001	20Jan.	1	

You can scan originals to store them.

After selecting file, Print Settings can be changed.

1/1

3 Press [File Management].



Logged in: [File Administrator] 20 JAN 2006 19:58

Select Files to Print

Page 1 Q'ty 1 Print 0

Memory: 99%

User Name	File Name	Date	Page	Printg Odr
user-1	COPY0001	20Jan.	1	1

You can scan originals to store them.

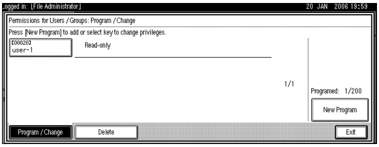
After selecting file, Print Settings can be changed.

1/1

4 Press [Change Acs. Priv.].

5 Press [Program/Change/Delete].

6 Press [New Program].



Logged in: [File Administrator] 20 JAN 2006 19:59

Permissions for Users / Groups: Program / Change

Press [New Program] to add or select key to change privileges.

[00020] user-1 Read-only

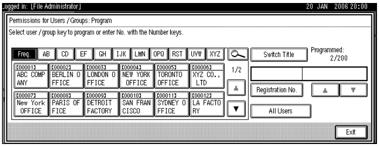
1/1

Programed: 1/200

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.



Logged in: [File Administrator] 20 JAN 2006 20:00

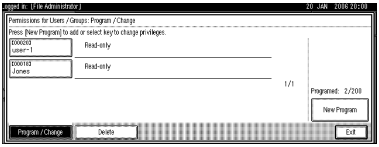
Permissions for Users / Groups: Program

Select user / group key to program or enter No. with the Number keys.

Programmed: 2/200

8 Press [Exit].

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



Logged in: [File Administrator] 20 JAN 2006 20:00

Permissions for Users / Groups: Program / Change

Press [New Program] to add or select key to change privileges.

[00020] user-1 Read-only

[00018] Jones Read-only

Programed: 2/200

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

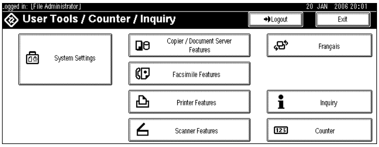
For details about logging on and logging off with administrator authentication, see p.106 “Logging on Using Administrator Authentication”, p.107 “Logging off Using Administrator Authentication”.

Important

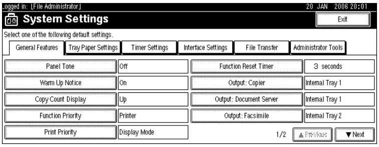
❒ If files become inaccessible, be sure to enable the user administrator, and then reset the access permission for the files in question.

1 Press the 【User Tools/Counter】 key.

2 Press [System Settings].



3 Press [Administrator Tools].



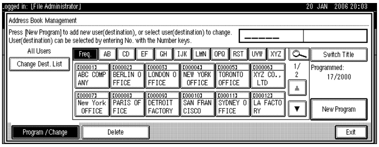
Select one of the following default settings.

Panel Tone	Off	Function Reset Timer	3 seconds
Warm Up Notice	On	Output: Copier	Internal Tray 1
Copy Count Display	Up	Output: Document Server	Internal Tray 1
Function Priority	Printer	Output: Facsimile	Internal Tray 2
Print Priority	Display Mode		

4 Press [Address Book Management].

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

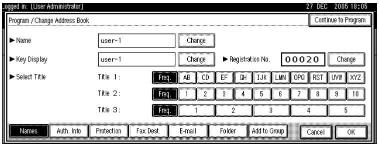
5 Select the user or group.



Press [New Program] to add new user(destination), or select user(destination) to change.
User(destination) can be selected by entering No. with the Number keys.

Programmed: 17/2000

6 Press [Protection].



▶Name: user-1

▶Key Display: user-1

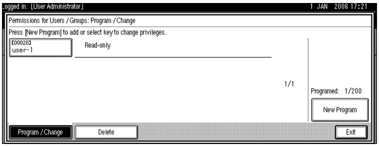
▶Registration No.: 00020

▶Select Title: Title 1 : / Title 2 : / Title 3 :

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

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

8 Press [New Program].


Logged in: [User Administrator]
1 JAN 2006 17:21
Permissions for Users / Groups: Program / Change
1/1
New Program
Program / Change
Delete
Exit

Press [New Program] to add or select key to change privileges.

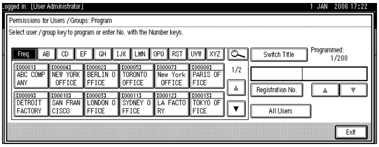
[00020] user-1 Read-only

Programed: 1/200

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.



Logged in: [User Administrator] 1 JAN 2006 17:22

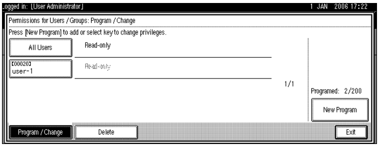
Permissions for Users / Groups: Program

Select user / group key to program or enter No. with the Number keys.

Programmed: 1/200

10 Press [Exit].

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



Logged in: [User Administrator] 1 JAN 2006 17:22

Permissions for Users / Groups: Program / Change

Press [New Program] to add or select key to change privileges.

All Users: Read-only

【00020】 user-1: Read-only

1/1

Programed: 2/200

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.

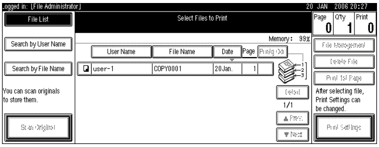
Provides increased protection against unauthorized use of files.

Preparation

For details about logging on and logging off with administrator authentication, see p.106 “Logging on Using Administrator Authentication”, p.107 “Logging off Using Administrator Authentication”.

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

2. **Select the file.**



Logged in: [File Administrator]　20 JAN 2006 20:27

Select Files to Print

Page 0　Q'ty 1　Print 0

Memory: 99%

User Name	File Name	Date	Page
user-1	COPY0001	20Jan.	1

1/1

You can scan originals to store them.

After selecting file, Print Settings can be changed.

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.

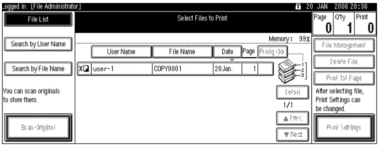
For details about “Enhance File Protection”, see p.109 “Specifying the Extended Security Functions”.

Preparation

For details about logging on and logging off with administrator authentication, see p.106 “Logging on Using Administrator Authentication”, p.107 “Logging off Using Administrator Authentication”.

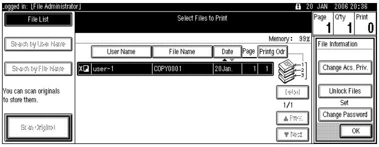
1 **Press the 【Document Server】 key.**

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 will be designated as the sender to prevent data from being sent by an unauthorized person masquerading as the user.

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 and phone numbers under the scanner and fax functions.

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

If you set **[Restrict Use of Destinations]** to **[On]**, you can prohibit users from directly entering telephone numbers, e-mail addresses, or Folder Path in order to send files. If you set **[Restrict Use of Destinations]** to **[Off]**, **[Restrict Adding of User Destinations]** appears. In **[Restrict Adding of User Destinations]**, you can restrict users from registering data in the address book.

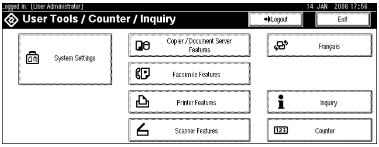
If you set **[Restrict Adding of User Destinations]** to **[Off]**, users can directly enter destination telephone numbers, e-mail addresses, and Folder Path in **[ProgDest]** on the fax and scanner screens. If you set **[Restrict Adding of User Destinations]** to **[On]**, users can specify destinations directly, but cannot use **[ProgDest]** to register data in the address book. When this setting is made, only the user administrator can change the address book.

Preparation

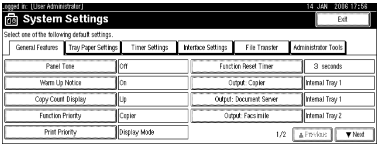
For details about logging on and logging off with administrator authentication, see p.106 “Logging on Using Administrator Authentication”, p.107 “Logging off Using Administrator Authentication”.

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

2 **Press [System Settings].**



3 Press **[Administrator Tools]**.



Logged in: [User Administrator] 14 JAN 2006 17:56

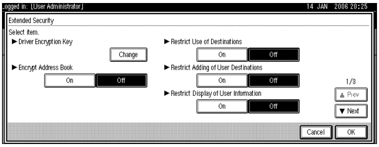
System Settings

Select one of the following default settings.

Panel Tone	Off	Function Reset Timer	3 seconds
Warm Up Notice	On	Output: Copier	Internal Tray 1
Copy Count Display	Up	Output: Document Server	Internal Tray 1
Function Priority	Copier	Output: Facsimile	Internal Tray 2
Print Priority	Display Mode		

4 Press **[Extended Security]**.

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



Logged in: [User Administrator] 14 JAN 2006 20:25

Extended Security

Select item.

- ► Driver Encryption Key: Change
- ► Encrypt Address Book: On [✓ Off]
- ► Restrict Use of Destinations: On [✓ Off]
- ► Restrict Adding of User Destinations: On [✓ Off]
- ► Restrict Display of User Information: On [✓ Off]

6 Press **[OK]**.

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

Reference

This can also be specified using Web Image Monitor or SmartDeviceMonitor for Admin. For details, see the Help for each application.

Protecting the Address Book

If user authentication is specified, the user who has logged on will be designated as the sender to prevent data from being sent by an unauthorized person masquerading as the user.

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.

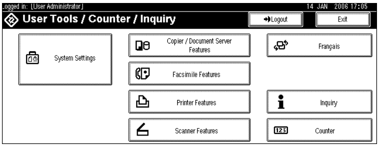
By making this setting, you can prevent the data in the address book being used by unregistered users.

Preparation

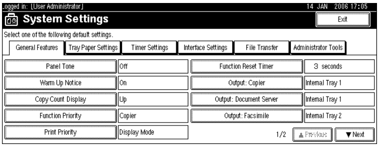
For details about logging on and logging off with administrator authentication, see p.106 "Logging on Using Administrator Authentication", p.107 "Logging off Using Administrator Authentication".

1 Press the 【User Tools/Counter】 key.

2 Press [System Settings].



3 Press [Administrator Tools].



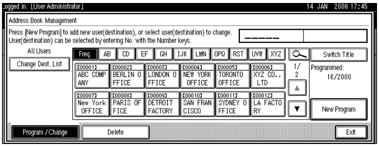
Select one of the following default settings.

Panel Tone: Off
Warm Up Notice: On
Copy Count Display: Up
Function Priority: Copier
Print Priority: Display Mode
Function Reset Timer: 3 seconds
Output: Copier: Internal Tray 1
Output: Document Server: Internal Tray 1
Output: Facsimile: Internal Tray 2

4 Press [Address Book Management].

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

5 Select the user or group.



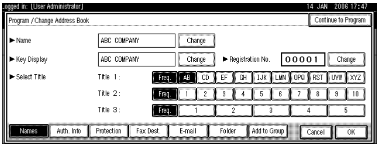
Logged in: [User Administrator] 14 JAN 2006 17:45

Address Book Management

Press [New Program] to add new user(destination), or select user(destination) to change. User(destination) can be selected by entering No. with the Number keys.

Programmed: 16/2000

6 Press [Protection].



Logged in: [User Administrator] 14 JAN 2006 17:47

Program / Change Address Book

▶Name: ABC COMPANY

▶Key Display: ABC COMPANY

▶Registration No.: 00001

▶Select Title

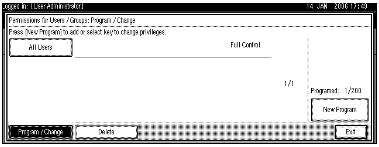
Title 1:

Title 2:

Title 3:

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

8 Press [New Program].



Logged in: [User Administrator] 14 JAN 2006 17:49

Permissions for Users / Groups: Program / Change

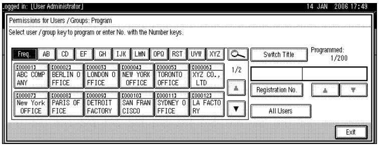
Press [New Program] to add or select key to change privileges.

All Users: Full Control

1/1

Programed: 1/200

9 Select the users or groups to register.



Logged in: [User Administrator] 14 JAN 2006 17:49

Permissions for Users / Groups: Program

Select user / group key to program or enter No. with the Number keys.

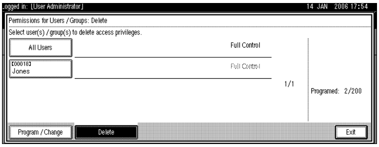
Programmed: 1/200

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.



Logged in: [User Administrator] 14 JAN 2006 17:54

Permissions for Users / Groups: Delete

Select user(s) / group(s) to delete access privileges.

All Users: Full Control

[00018] Jones: Full Control

1/1

Programed: 2/200

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.

Reference

See p.109 “Changing the Extended Security Functions”.

Preparation

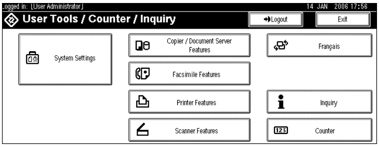
For details about logging on and logging off with administrator authentication, see p.106 “Logging on Using Administrator Authentication”, p.107 “Logging off Using Administrator Authentication”.

Note

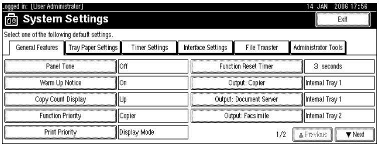
- ❒ Encrypting the data in the address book may take a long time. (Up to three minutes)
- ❒ The time it takes to encrypt the data in the address book depends on the number of registered users.
- ❒ The machine cannot be used during encryption.
- ❒ If you press **[Stop]** during encryption, the data is 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.
- ❒ If you register additional users after encrypting the data in the address book, those users are also encrypted.

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

2 **Press [System Settings].**



3 Press [Administrator Tools].



Logged in: [User Administrator] 14 JAN 2006 17:56

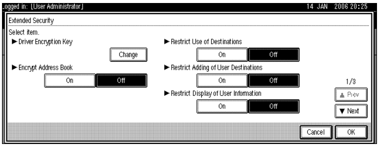
System Settings

Select one of the following default settings.

Panel Tone	Off	Function Reset Timer	3 seconds
Warm Up Notice	On	Output: Copier	Internal Tray 1
Copy Count Display	Up	Output: Document Server	Internal Tray 1
Function Priority	Copier	Output: Facsimile	Internal Tray 2
Print Priority	Display Mode		

4 Press [Extended Security].

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



Logged in: [User Administrator] 14 JAN 2006 20:25

Extended Security

Select item.

► Driver Encryption Key: Change

► Encrypt Address Book: On ● Off

► Restrict Use of Destinations: On ● Off

► Restrict Adding of User Destinations: On ● Off

► Restrict Display of User Information: On ● Off

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.

Log Information and Deleting Data on the Hard Disk

① Hard Disk
The machine's optional hard disk lets you store data under the copy, printer, fax, scanner, and document server functions, as well as the address book and counters stored under each user code.
For details about deleting data on the hard disk, see p.35 "Overwriting the Data on the Hard Disk".

② Data Not Overwritten in the Hard Disk
The machine's memory lets you store fax numbers and data transmitted using the fax function, and network TWAIN scanner. Even if you delete the data on the hard disk, this data remains intact.

③ Log information
The following log information is stored in the machine's memory and on its hard disk:

- Job log
  Stores information about workflow related to user files, such as copying, printing, and scan file delivery
- Access log
  Stores information about access, such as logging on and off, creating and deleting files, scanning invalid images, administrator procedures [*1], and customer engineer procedures. [*2]

  [*1] Deleting all log information

  [*2] Formatting the hard disk and specifying whether or not to store job logs and access logs

  Limitation

  ❒ Fax job logs are not stored.

④ Deleting log information
By deleting the log files stored in the machine, you can prevent information leaks.

⑤ Transferring log information
You can transfer the log information, which indicates who tried to gain access and at what time.
By transferring the log files, you can check the history data and identify unauthorized access.

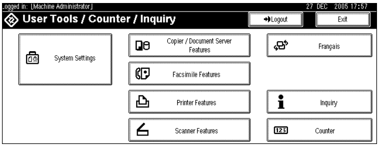
Specifying Delete All Logs

This can be specified by the machine administrator.

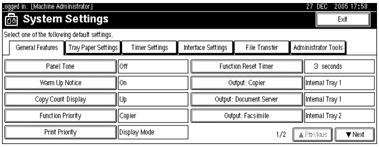
By deleting log files stored in the machine, you can prevent information leakage.

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

2 **Press [System Settings].**



3 **Press [Administrator Tools].**


.ogged in: [Machine Administrator] 27 DEC 2005 17:58

System Settings — Exit

Select one of the following default settings.

General Features | Tray Paper Settings | Timer Settings | Interface Settings | File Transfer | Administrator Tools

Panel Tone	Off	Function Reset Timer	3 seconds
Warm Up Notice	On	Output: Copier	Internal Tray 1
Copy Count Display	Up	Output: Document Server	Internal Tray 1
Function Priority	Copier	Output: Facsimile	Internal Tray 2
Print Priority	Display Mode	1/2 ▲Previous	▼Next

4 **Press [Delete All Logs].**

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

A confirmation message appears.

5 **Press [Yes].**

6 **Press [Exit].**

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

Transfer Log Setting

The machine administrator can select **[On]** from the log server only.

When using the machine's control panel, you can change the setting to **[Off]** only if it is set to **[On]**.

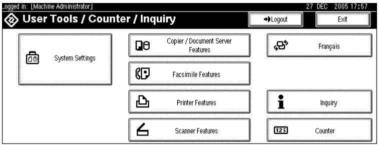
You can check and change the transfer log setting. This setting lets you transfer log files to the log server to check the history data and identify unauthorized access.

For details about log collection server, contact your local dealer.

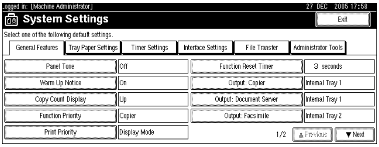
For details about the transfer log setting, see log collection server help.

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

2 Press **[System Settings]**.



3 Press **[Administrator Tools]**.



Panel Tone	Off	Function Reset Timer	3 seconds
Warm Up Notice	On	Output: Copier	Internal Tray 1
Copy Count Display	Up	Output: Document Server	Internal Tray 1
Function Priority	Copier	Output: Facsimile	Internal Tray 2
Print Priority	Display Mode		

4 Press **[Transfer Log Setting]**.

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

5 Press **[OK]**.

6 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, Fax, or Scanner mode, or print data sent from a printer driver is temporarily stored on the machine's hard disk.

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

Overwriting starts automatically once the job is completed.

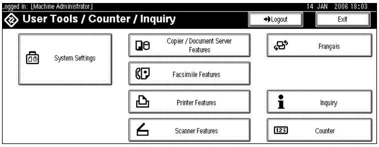
The Copier, Fax, and Printer functions take priority over the Auto Erase Memory function. If a copy, fax or print job is in progress, overwriting will only be done after the job is completed.

Preparation

For details about logging on and logging off with administrator authentication, see p.106 “Logging on Using Administrator Authentication”, p.107 “Logging off Using Administrator Authentication”.

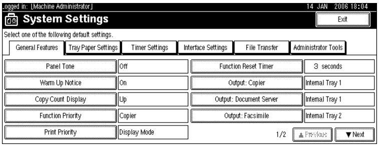
1 **Press the 【User Tools/Counter】 key.**

2 **Press [System Settings].**



Logged in: [Machine Administrator] 14 JAN 2006 18:03

3 **Press [Administrator Tools].**



Logged in: [Machine Administrator] 14 JAN 2006 18:04

System Settings

Select one of the following default settings.

Panel Tone	Off	Function Reset Timer	3 seconds
Warm Up Notice	On	Output: Copier	Internal Tray 1
Copy Count Display	Up	Output: Document Server	Internal Tray 1
Function Priority	Copier	Output: Facsimile	Internal Tray 2
Print Priority	Display Mode		

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

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

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
	Printer	• Print Jobs • Sample Print/Locked Print/Stored Print Jobs [*1] • Spool Printing jobs • PDF Direct Print data
	Fax [*2]	• PC fax print jobs • Internet fax transmitted data
	Scanner [*3]	• Scanned files sent by e-mail • Files sent by Scan to Folder • Documents sent using DeskTopBinder, the Scan-Router 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, Printer or Scanner functions [*4]	
	Information registered in the Address Book [*5]	
	Counters stored under each user code	
	Image overlay data [*6]	

[*1] A Sample Print, Locked Print, or Stored Print job can only be overwritten after it has been executed.Stored print jobs can be overwritten by Auto Erase Memory only if they have been deleted in advance.

[*2] The data for fax transmission and the registered fax numbers are stored in the memory. This data is not stored on the hard disk, so it will not be overwritten by Auto Erase Memory.

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

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

[*5] Data stored in the Address Book can be encrypted for security. For details, see p.31 “Encrypting the Data in the Address Book”.

[*6] Image overlay data can be overwritten by Auto Erase Memory only if it is deleted in advance.

“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 and logging off with administrator authentication, see p.106 “Logging on Using Administrator Authentication”, p.107 “Logging off Using Administrator Authentication”.

Important

❒ If you select Erase All Memory, the following are also deleted: user codes, counters under each user code, user stamps, data stored in the Address Book, printer fonts downloaded by users, applications using Embedded Software Architecture, SSL server certificates, and the machine’s network settings.

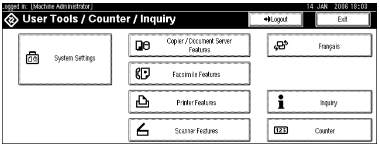
Note

❒ 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.**

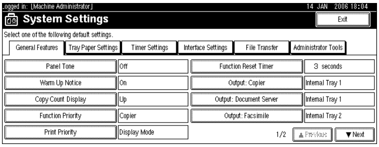
3 **Press [System Settings].**



.ogged in: [Machine Administrator]　14 JAN 2006 18:03

User Tools / Counter / Inquiry

4 **Press [Administrator Tools].**



.ogged in: [Machine Administrator]　14 JAN 2006 18:04

System Settings

Select one of the following default settings.

Panel Tone	Off	Function Reset Timer	3 seconds
Warm Up Notice	On	Output: Copier	Internal Tray 1
Copy Count Display	Up	Output: Document Server	Internal Tray 1
Function Priority	Copier	Output: Facsimile	Internal Tray 2
Print Priority	Display Mode		

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

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

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
- File Administrator
- Network Administrator
- Machine Administrator

Reference

For details, see p.99 "The Roles of Administrators".

For details, see p.101 "Administrator Authentication".

For details, see p.125 "Machine Administrator Settings".

For details, see p.132 "Network Administrator Settings".

For details, see p.136 "File Administrator Settings".

For details, see p.138 "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:

- Copy / Document Server Features
- Facsimile Features
- Printer Features
- Scanner Features

Reference

For details, see p.138 "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, fax, scanner, and printer functions.

Specifying Which Functions are Available

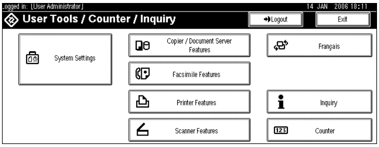
This can be specified by the user administrator. Specify the functions available to registered users. By making this setting, you can limit the functions available to users.

Preparation

For details about logging on and logging off with administrator authentication, see p.106 “Logging on Using Administrator Authentication”, p.107 “Logging off Using Administrator Authentication”.

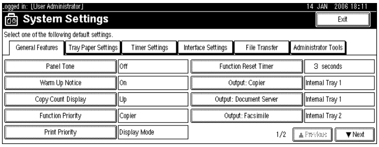
1 Press the 【User Tools/Counter】 key.

2 Press [System Settings].



Logged in: [User Administrator] 14 JAN 2006 18:11

3 Press [Administrator Tools].



Logged in: [User Administrator] 14 JAN 2006 18:11

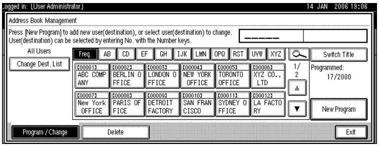
Select one of the following default settings.

Panel Tone	Off	Function Reset Timer	3 seconds
Warm Up Notice	On	Output: Copier	Internal Tray 1
Copy Count Display	Up	Output: Document Server	Internal Tray 1
Function Priority	Copier	Output: Facsimile	Internal Tray 2
Print Priority	Display Mode		

4 Press [Address Book Management].

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

5 Select the user.



Logged in: [User Administrator] 14 JAN 2006 19:06

Address Book Management

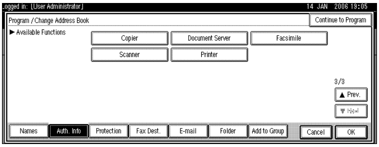
Press [New Program] to add new user(destination), or select user(destination) to change.
User(destination) can be selected by entering No. with the Number keys.

Programmed: 17/2000

[00001] ABC COMPANY	[00002] BERLIN OFFICE	[00003] LONDON OFFICE	[00004] NEW YORK OFFICE	[00005] TORONTO OFFICE	[00006] XYZ CO., LTD
[00007] New York OFFICE	[00008] PARIS OFFICE	[00009] DETROIT FACTORY	[00010] SAN FRANCISCO	[00011] SYDNEY OFFICE	[00012] LA FACTORY

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]** to scroll down to other settings.

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, disable ports and protocols, or use Web Image Monitor to specify the network security level 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.

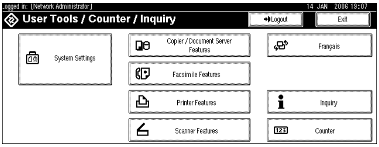
By making this setting, you can specify which protocols are available and so prevent unauthorized access over the network.

Preparation

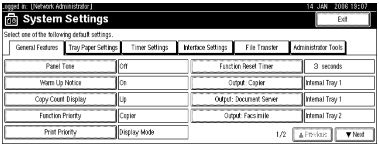
For details about logging on and logging off with administrator authentication, see p.106 "Logging on Using Administrator Authentication", p.107 "Logging off Using Administrator Authentication".

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

2 **Press [System Settings].**



3 **Press [Interface Settings].**



Logged in: [Network Administrator] 14 JAN 2006 19:07

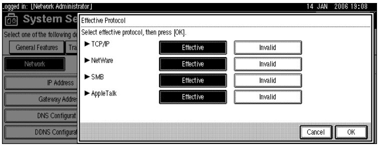
Select one of the following default settings.

Panel Tone	Off	Function Reset Timer	3 seconds
Warm Up Notice	On	Output: Copier	Internal Tray 1
Copy Count Display	Up	Output: Document Server	Internal Tray 1
Function Priority	Copier	Output: Facsimile	Internal Tray 2
Print Priority	Display Mode		

4 **Press [Effective Protocol].**

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

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



Logged in: [Network Administrator] 14 JAN 2006 19:08

Effective Protocol

Select effective protocol, then press [OK].

- TCP/IP: Effective
- NetWare: Effective
- SMB: Effective
- AppleTalk: Effective

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.

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, IPP, DIPRINT, 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.

Specifying Network Security Level

This can be specified by the network administrator.

This setting lets you change the security level to limit unauthorized access.

Set the security level to **[Level 0]**, **[Level 1]**, or **[Level 2]**.

Select **[Level 2]** for maximum security to protect confidential information.

Select **[Level 1]** for moderate security. Use this setting if the machine is connected to the office local area network (LAN).

Select **[Level 0]** to use this setting if no information needs to be protected.

You can specify the entire network security level setting the machine's control panel.

If you change this setting using Web Image Monitor, the network security level settings other than the specified one will be reset to the default.

Reference

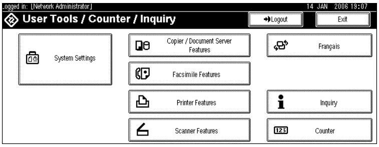
For details about logging on and logging off with user authentication, see p.106 "Logging on Using Administrator Authentication", p.107 "Logging off Using Administrator Authentication".

Note

- ❒ If you change this setting using Web Image Monitor, the network security level settings other than the specified one will be reset to the default.

1 Press the 【User Tools/Counter】key.

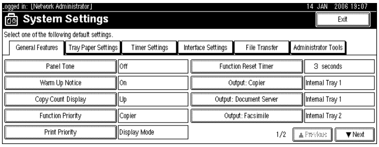
2 Press [System Settings].



Logged in: [Network Administrator]

14 JAN 2006 19:07

3 **Press [Administrator Tools].**



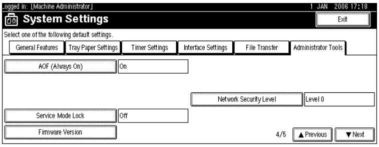
Logged in: [Network Administrator] 14 JAN 2006 19:07

System Settings

Select one of the following default settings.

Panel Tone: Off
Warm Up Notice: On
Copy Count Display: Up
Function Priority: Copier
Print Priority: Display Mode
Function Reset Timer: 3 seconds
Output: Copier: Internal Tray 1
Output: Document Server: Internal Tray 1
Output: Facsimile: Internal Tray 2

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



Logged in: [Machine Administrator] 1 JAN 2006 17:18

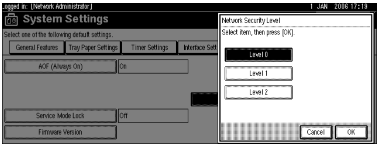
System Settings

Select one of the following default settings.

AOF (Always On): On
Network Security Level: Level 0
Service Mode Lock: Off
Firmware Version

If the setting you want to specify does not appear, press **[▼Next]** to scroll down to other settings.

5 **Select the network security level.**



Logged in: [Network Administrator] 1 JAN 2006 17:19

System Settings

Select one of the following default settings.

AOF (Always On): On
Service Mode Lock: Off
Firmware Version

Network Security Level

Select item, then press [OK].

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

6 **Press [OK].**

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

Status of Functions under each Network Security Level

○= Available

— = Unavailable

▲ = Port is open.

△ = Port is closed.

☆ = Automatic

★ = Ciphertext Only

× = Ciphertext Priority

	Function		Network Security Level		
			Level 0	Level 1	Level 2
Interface	IEEE1394 SBP-2		❍	❍	—
	Bluetooth		❍	❍	—
	IP over 1394		❍	❍	❍
TCP/IP	TCP/IP		❍	❍	❍
	HTTP	Port 80	▲	▲	▲
		Port 443	▲	▲	▲
		Port 631	▲	▲	△
		Port 7443/7444	▲	▲	▲
	IPP	Port 80	▲	▲	▲
		Port 631	▲	▲	△
		Port 443	▲	▲	▲
	DIPRINT		❍	❍	—
	LPR		❍	❍	—
	FTP	Port 21	▲	▲	▲
	RFU	Port 10021	▲	▲	▲
	RSH/RCP		❍	❍	—
	SNMP		❍	❍	❍
	SNMP v1v2	Setting	❍	—	—
		Browse	❍	❍	—
	SNMP v3		❍	❍	❍
		SNMP Encryption	☆	☆	★
	TELNET		❍	—	—
	SSDP	Port 1900	▲	▲	△
	NBT	Port 137/138	▲	▲	△
	SSL		❍	❍	❍
		SSL / TLS Encryption Mode	×	×	★
	mDNS		❍	❍	—
	SMB		❍	❍	—
NetWare	NetWare		❍	❍	—
AppleTalk	AppleTalk		❍	❍	—

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.

Reference

See p.109 "Changing the Extended Security Functions".

❖ Group Passwords for PDF Files

DeskTopBinder Lite's PDF Direct Print function allows a PDF group password to be specified to enhance security.

Note

❒ To use PDF direct print, the optional PostScript3 unit must be installed.

❖ 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.

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.

Reference

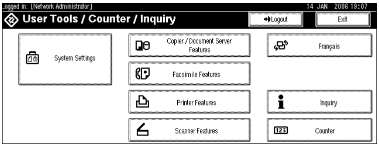
See p.109 "Changing the Extended Security Functions".

Preparation

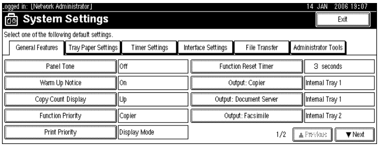
For details about logging on and logging off with administrator authentication, see p.106 "Logging on Using Administrator Authentication", p.107 "Logging off Using Administrator Authentication".

1 Press the 【User Tools/Counter】 key.

2 Press [System Settings].



3 Press [Administrator Tools].

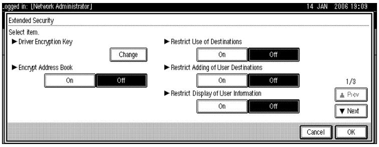


Select one of the following default settings.

Panel Tone	Off	Function Reset Timer	3 seconds
Warm Up Notice	On	Output: Copier	Internal Tray 1
Copy Count Display	Up	Output: Document Server	Internal Tray 1
Function Priority	Copier	Output: Facsimile	Internal Tray 2
Print Priority	Display Mode		

4 Press [Extended Security].

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



Extended Security

Select item.

- Driver Encryption Key
- Encrypt Address Book: On [✓ Off]
- Restrict Use of Destinations: On [✓ Off]
- Restrict Adding of User Destinations: On [✓ Off]
- Restrict Display of User Information: On [✓ Off]

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 printer driver Help.

See the TWAIN driver Help.

Group Password for PDF files

This can be specified by the network administrator.

On the machine, specify the group password for PDF files.

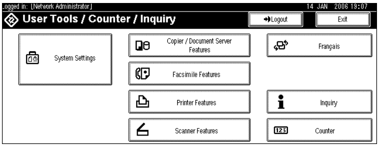
By using a PDF group password, you can enhance security and so protect passwords from being analyzed.

Preparation

For details about logging on and logging off with administrator authentication, see p.106 "Logging on Using Administrator Authentication", p.107 "Logging off Using Administrator Authentication".

1 Press the 【User Tools/Counter】 key.

2 Press [Printer Features].



3 Press [PDF Menu], and then press [PDF Group Password].

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

4 For [Current Password], press [Change].

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

Enter the group password for PDF files using up to 32 alphanumeric characters.

6 Press [OK].

7 For [New Password], press [Change].

8 Enter the password, and then press [OK].

9 For [Confirm New Password], press [Change].

10 Enter the password and press [OK].

11 Press [OK].

12 Press the 【User Tools/Counter】 key.

Note

- ❒ The network administrator must give users the group password for PDF files that is already registered on the machine. The users can then register it in DeskTopBinder on their computers.For details, see the DeskTopBinder Help
- ❒ Make sure to enter the same character string as that specified on the machine for the group password for PDF files.
- ❒ The group password for PDF files can also be specified using Web Image Monitor. For details, see the Web Image Monitor 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.

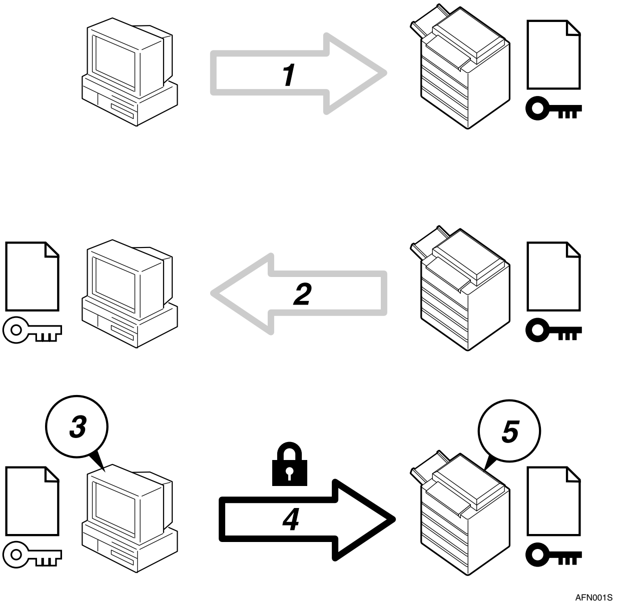
9 **Log off from the machine.**

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 printer and scanner functions.

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 printer.

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 printer 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 printer.

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.

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 printer.

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 printer.

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 printer, 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.

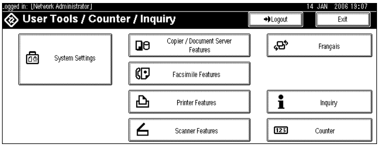
After installing the server certificate, specify the SSL/TLS encrypted communication mode. By making this setting, you can change the security level.

Preparation

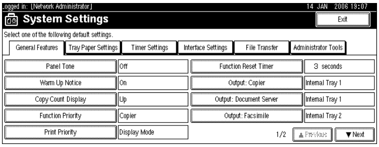
For details about logging on and logging off with administrator authentication, see p.106 “Logging on Using Administrator Authentication”, p.107 “Logging off Using Administrator Authentication”.

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

2 **Press [System Settings].**

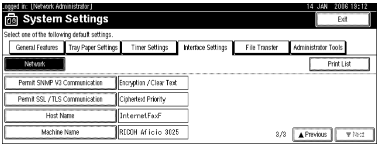


3 **Press [Interface Settings].**



Panel Tone	Off	Function Reset Timer	3 seconds
Warm Up Notice	On	Output: Copier	Internal Tray 1
Copy Count Display	Up	Output: Document Server	Internal Tray 1
Function Priority	Copier	Output: Facsimile	Internal Tray 2
Print Priority	Display Mode		

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



Permit SNMP V3 Communication	Encryption / Clear Text
Permit SSL / TLS Communication	Ciphertext Priority
Host Name	InternetFaxF
Machine Name	RICOH Aficio 3025

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

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.

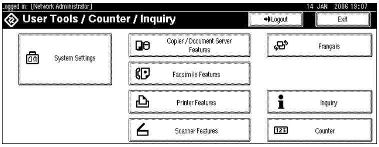
By making this setting, you can protect data from being tampered with.

Preparation

For details about logging on and logging off with administrator authentication, see p.106 "Logging on Using Administrator Authentication", p.107 "Logging off Using Administrator Authentication".

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

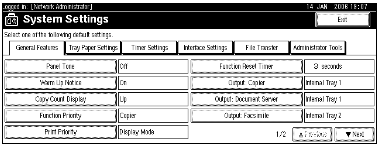
2. **Press [System Settings].**



.ogged in: [Network Administrator] 14 JAN 2006 19:07

User Tools / Counter / Inquiry

3. **Press [Interface Settings].**



.ogged in: [Network Administrator] 14 JAN 2006 19:07

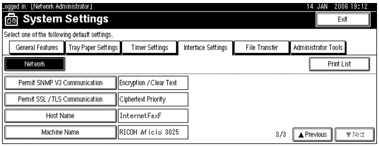
System Settings

Select one of the following default settings.

Panel Tone	Off	Function Reset Timer	3 seconds
Warm Up Notice	On	Output: Copier	Internal Tray 1
Copy Count Display	Up	Output: Document Server	Internal Tray 1
Function Priority	Copier	Output: Facsimile	Internal Tray 2
Print Priority	Display Mode		

1/2

4. **Press [Permit SNMP V3 Communication].**



.ogged in: [Network Administrator] 14 JAN 2006 19:12

System Settings

Select one of the following default settings.

Permit SNMP V3 Communication	Encryption / Clear Text
Permit SSL / TLS Communication	Ciphertext Priority
Host Name	InternetFaxF
Machine Name	RICOH Aficio 3025

3/3

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

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 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.104 "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

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.

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.

Specify administrator authentication and user authentication according to the following flowchart:

Administrator Authentication See p.68 "Administrator Authentication".	Specifying Administrator Authentication See p.68 "Administrator Authentication". Registering the Administrator See p.104 "Registering the Administrator".
User Authentication See p.68 "Enabling Authentication".	Specifying User Authentication Authentication that requires only the machine: • User Code Authentication See p.70 "User Code Authentication". • Basic Authentication See p.71 "Basic Authentication". Authentication that requires external devices: • Windows Authentication See p.73 "Windows Authentication". • LDAP Authentication See p.79 "LDAP Authentication". • Integration Server Authentication See p.82 "Integration Server Authentication".

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.

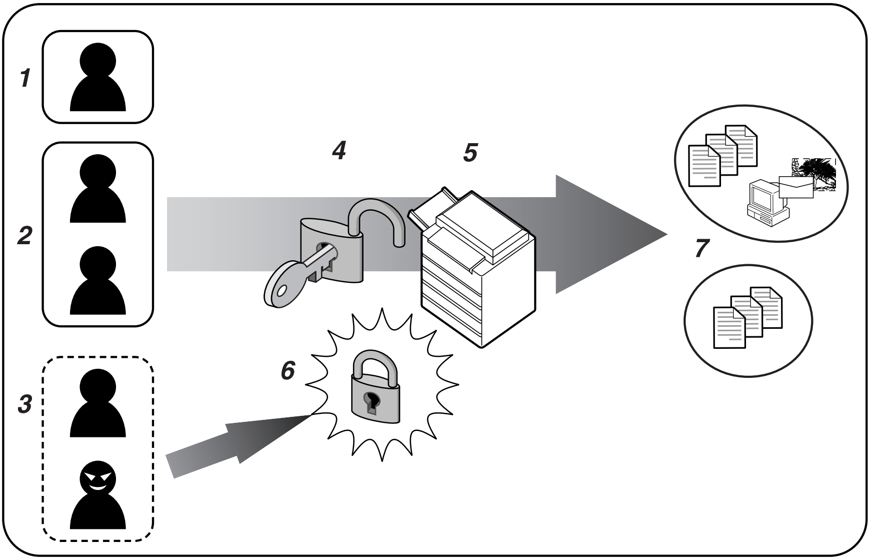
Reference

For details, see p.121 "Operations by the Supervisor".

About User Authentication

This machine has an authentication function to prevent unauthorized access.

By using login user name and login password, you can specify access limits for individual users and groups of users.



1. User

A user performs normal operations on the machine, such as copying and printing.

2. Group

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

3. Unauthorized User

4. Authentication

Using a login user name and password, user authentication is performed.

5. This Machine

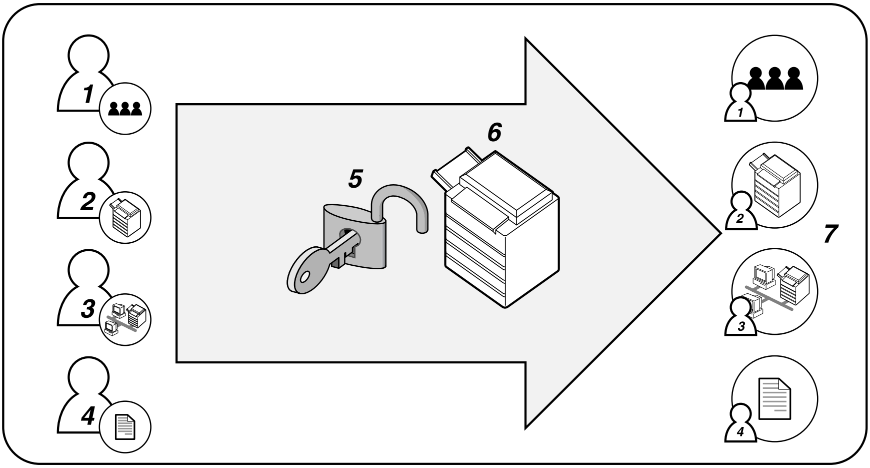
6. Access Limit

Using authentication, unauthorized users are prevented from accessing the machine.

7. Authorized users and groups can use only those functions permitted by the administrator.

About Administrator Authentication

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



1. User Administrator

This administrator manages personal information in the address book. You can register/delete users in the address book or change users' personal information.

2. Machine Administrator

This administrator manages the machine's default settings. You can set the machine so that the default such as data security for copying function and delete all logs can only be specified by the machine administrator.

3. Network Administrator

This administrator manages the network settings. You can set the machine so that network settings such as the IP address and settings for sending and receiving e-mail can only be specified by the network administrator only.

4. File Administrator

This administrator manages permission to access stored files. You can specify passwords for Locked Print files stored in the Document Server so only authorized users can view and change them.

5. Authentication

Administrators must enter their login user name and password to be authenticated.

6. This machine

7. Administrators manage the machine's settings and access limits. For details about each administrator, see p.99 "The Roles of Administrators".

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.

Reference

For details, see p.88 "Specifying Login User Name and Login Password".

For details, see p.121 "Operations by the Supervisor".

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 controlling user access. so they cannot use functions such as copying and printing. To use such functions, you need to register a user in the address book and then be authenticated as the user.

Note

- ❒ By sharing the administrative work among different administrators, you can spread the workload and limit unauthorized operation by a single administrator. We recommend only one person take each administrator role.

Reference

For details, see p.99 "The Roles of Administrators".

For details, see p.104 "Registering the Administrator".

User

Users are managed using the personal information managed 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 managed in the address book by the user administrator. In addition to registering users with the machine's control panel, you can register them using SmartDeviceMonitor for Admin or Web Image Monitor.

Note

❒ Only the user administrator can register users in the address book with Ridoc IO Admin and 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.

To perform Basic Authentication, the hard disk must be installed.

To perform Windows Authentication, LDAP Authentication, or Integration Server Authentication, the hard disk and Printer/Scanner unit must be installed.

To specify authentication, you need to register administrators.

Reference

For details, see p.104 "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.

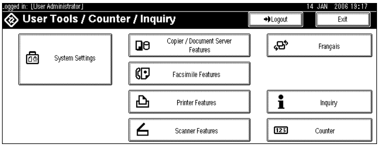
Reference

For details, see p.121 "Operations by the Supervisor".

Specifying Administrator Authentication Management

1 Press the 【User Tools/Counter】 key.

2 Press [System Settings].

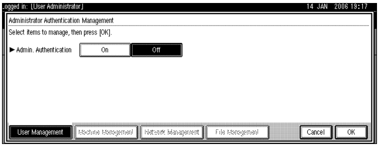


3 Press [Administrator Tools].

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].



Logged in: [User Administrator] 14 JAN 2006 19:17

Administrator Authentication Management

Select items to manage, then press [OK].

▶ Admin. Authentication On [Off]

[Available Settings] appears.

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

The selected settings will be unavailable to users.

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.

User Authentication

There are five types of user authentication method: user code authentication, basic authentication, Windows authentication, Integration Server 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

- ❒ To control the use of RidocDesk2000/Lt for the delivery of files stored in the machine, select Basic Authentication, Windows Authentication, LDAP Authentication, or Integration Server Authentication.

Reference

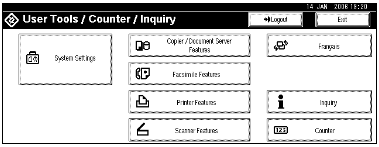
For details about specifying the user code for the printer driver, see *Printer Reference* or the printer driver Help.

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.

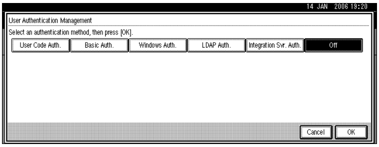
2 Press [System Settings].



3 Press [Administrator Tools].

4 Press [User Authentication Management].

5 Select [User Code Authentication].



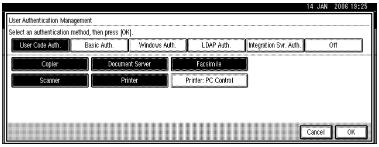
User Authentication Management

Select an authentication method, then press [OK].

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.



14 JAN 2006 19:25

User Authentication Management

Select an authentication method, then press [OK].

The selected settings will be available to users.

7 Press [OK].

8 Press the 【User Tools/Counter】 key.

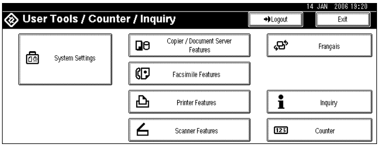
Basic Authentication

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. Under basic authentication, the administrator must specify the functions available to each user registered in the address book.

Specifying Basic Authentication

1 Press the 【User Tools/Counter】 key.

2 Press [System Settings].

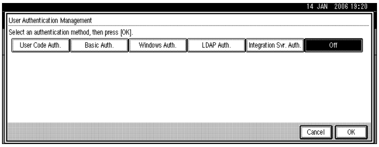


14 JAN 2006 19:20

3 Press [Administrator Tools].

4 Press [User Authentication Management].

5 Select [Basic Authentication].



14 JAN 2006 19:20

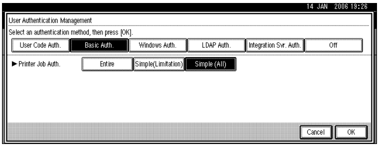
User Authentication Management

Select an authentication method, then press [OK].

Note

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

6 Select the "Printer Job Auth." level.



User Authentication Management

Select an authentication method, then press [OK].

Note

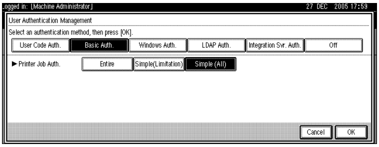
- ❒ If you select **[Entire]**, you cannot print using a printer driver or a device that does not support authentication. To print under an environment that does not support authentication, select **[Simple (All)]**. By making this setting, only registered users will be able to print.
- ❒ If you select **[Simple(Limitation)]**, you can specify clients for which printer job authentication is not required. Specify **[Parallel Interface: Simple]**, **[USB: Simple]** and the clients' IP address range in which printer job authentication is not required. Specify this setting if you want to print using unauthenticated printer drivers or without any printer driver. Authentication is required for printing with non-specified devices.
- ❒ If you select **[Simple (All)]** or **[Simple(Limitation)]**, you can print even with unauthenticated printer drivers or devices. Specify this setting if you want to print with a printer driver or device that cannot be identified by the machine or if you do not require authentication for printing.However, note that, because the machine does not require authentication in this case, it may be used by unauthorized users.

Reference

For details, see p.86 "Printer Job Authentication Levels and Printer Job Types".

Specifying **[Simple(Limitation)]**

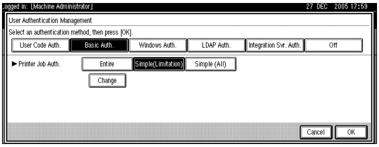
❶ **Press [Simple(Limitation)]**



User Authentication Management

Select an authentication method, then press [OK].

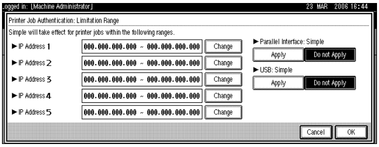
❷ **Press [Change].**



User Authentication Management

Select an authentication method, then press [OK].

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



Logged in: [Machine Administrator] 23 MAR 2006 16:44

Printer Job Authentication: Limitation Range

Simple will take effect for printer jobs within the following ranges.

- IP Address 1: 000.000.000.000 ~ 000.000.000.000
- IP Address 2: 000.000.000.000 ~ 000.000.000.000
- IP Address 3: 000.000.000.000 ~ 000.000.000.000
- IP Address 4: 000.000.000.000 ~ 000.000.000.000
- IP Address 5: 000.000.000.000 ~ 000.000.000.000

Parallel Interface: Simple — Do not Apply

USB: Simple — Do not Apply

❹ **Press [OK].**

7 Press [OK].

8 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. The address book stored in the directory server can be registered to the machine, enabling user authentication without first using the machine to register individual settings in the address book.

Important

❒ If user information on the server is changed, information registered in the machine may be overwritten when authentication is performed.

❖ Operational Requirements for Windows Authentication

- To specify Windows authentication, the following requirements must be met:
- 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. This requires a version of Windows that supports TLSv1, SSLv2, or SSLv3.
  - Windows NT 4.0 Server
  - Windows 2000 Server
  - Windows Server 2003

Limitation

❒ Users managed in other domains are subject to user authentication, but they cannot obtain items such as e-mail addresses.

❒ 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.

❒ If you have created a new user in the domain controller and selected **[User must change password at next logon]**, log on to the machine from the computer to change the password before logging on from the machine’s control panel.

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.
- ❒ 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.
- ❒ If you specify in the address book which functions are available to global group members, those settings have priority.
- ❒ A user registered in two or more global groups can use all the functions available to members of those groups.
- ❒ If the "Guest" account on the Windows server is enabled, even users not registered in the domain controller can be authenticated. When this account is enabled, users are registered in the address book and can use all functions.

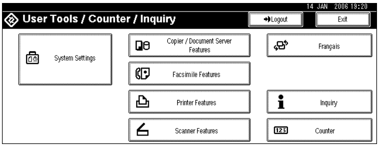
Specifying Windows Authentication

Note

- ❒ To automatically register fax numbers and e-mail addresses under Windows authentication, the machine and domain controller must communicate using SSL. To allow this, you must create a server certificate for the domain controller.
- ❒ You must create a server certificate only if you want to automatically register user information such as fax numbers and e-mail addresses under Windows authentication.

1 Press the 【User Tools/Counter】 key.

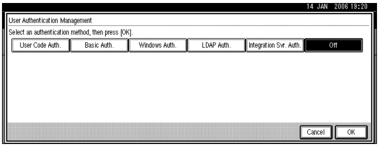
2 Press [System Settings].



3 Press [Administrator Tools].

4 Press [User Authentication Management].

5 Select [Windows Authentication].



14 JAN 2006 19:20

User Authentication Management

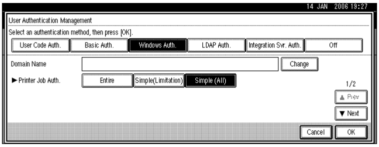
Select an authentication method, then press [OK].

Off

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].



14 JAN 2006 19:27

User Authentication Management

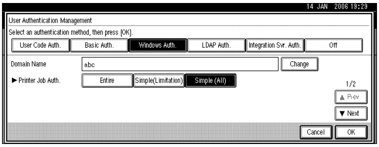
Select an authentication method, then press [OK].

Windows Auth.

Domain Name

Printer Job Auth.: Simple (All)

7 Select the "Printer Job Auth." level.



14 JAN 2006 19:29

User Authentication Management

Select an authentication method, then press [OK].

Windows Auth.

Domain Name: abc

Printer Job Auth.: Simple (All)

Note

❒ If you select **[Entire]**, you cannot print using a printer driver or a device that does not support authentication. To print under an environment that does not support authentication, select **[Simple (All)]**. By making this setting, only registered users will be able to print.

❒ If you select **[Simple(Limitation)]**, you can specify clients for which printer job authentication is not required. Specify **[Parallel Interface: Simple]**, **[USB: Simple]** and the clients' IP address range in which printer job authentication is not required. Specify this setting if you want to print using unauthenticated printer drivers or without any printer driver. Authentication is required for printing with non-specified devices.

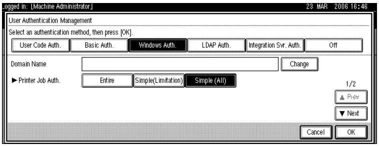
❒ If you select **[Simple (All)]**, you can print even with unauthenticated printer drivers or devices. Specify this setting if you want to print with a printer driver or device that cannot be identified by the machine or if you do not require authentication for printing.However, note that, because the machine does not require authentication in this case, it may be used by unauthorized users.

Reference

For details, see p.86 "Printer Job Authentication Levels and Printer Job Types".

Specifying **[Simple(Limitation)]**

❶ **Press [Simple(Limitation)]**



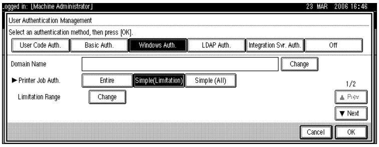
Logged in: [Machine Administrator] 23 MAR 2006 16:46

User Authentication Management

Select an authentication method, then press [OK].

Domain Name

❷ **Press [Change].**



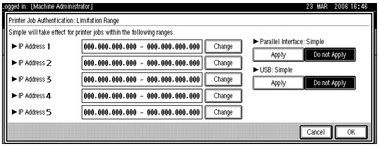
Logged in: [Machine Administrator] 23 MAR 2006 16:46

User Authentication Management

Select an authentication method, then press [OK].

Domain Name

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



Logged in: [Machine Administrator] 23 MAR 2006 16:46

Printer Job Authentication: Limitation Range

Simple will take effect for printer jobs within the following ranges.

► IP Address 1 000.000.000.000 ~ 000.000.000.000

► IP Address 2 000.000.000.000 ~ 000.000.000.000

► IP Address 3 000.000.000.000 ~ 000.000.000.000

► IP Address 4 000.000.000.000 ~ 000.000.000.000

► IP Address 5 000.000.000.000 ~ 000.000.000.000

► Parallel Interface: Simple

► USB: Simple

❹ **Press [OK].**

If global groups have been registered:

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

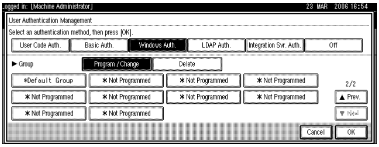
You need to create global groups in the Windows server in advance and register in each group the users to be authenticated.

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

Create global groups in the machine by entering the names of the global groups registered in the Windows Server. (Keep in mind that group names are case sensitive.) Then specify the machine functions available to each group.

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

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



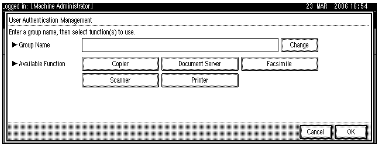
Logged in: [Machine Administrator] 23 MAR 2006 16:54

User Authentication Management

Select an authentication method, then press [OK].

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

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



Logged in: [Machine Administrator] 23 MAR 2006 16:54

User Authentication Management

Enter a group name, then select function(s) to use.

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

❹ Press [OK].

8 Press [OK].

9 Press the 【User Tools/Counter】 key.

Installing Internet Information Services (IIS) and Certificate services

Specify this setting if you want the machine to automatically obtain e-mail addresses registered in Active Directory.

We recommend you install Internet Information Services (IIS) and Certificate services as the Windows components.

Install the components, and then create the server certificate.

If they are not installed, install them as follows:

① Select **[Add/Remove Programs]** on the **[Control Panel]**.

② Select **[Add/Remove Windows Components]**.

③ Select the **[Internet Information Services (IIS)]** check box.

④ Select the **[Certificate Services]** check box, and then click **[Next]**.

⑤ Installation of the selected Windows components starts, and a warning message appears.

⑥ Click **[Yes]**.

⑦ Click **[Next]**.

⑧ Select the Certificate Authority, and then click **[Next]**.
On the displayed screen, **[Enterprise root CA]** is selected.

⑨ Enter the Certificate Authority name (optional) in **[CA Identifying Information]**, and then click **[Next]**.

⑩ Leave **[Data Storage Location]** at its default, and then click **[Next]**.

Creating the Server Certificate

After installing Internet Information Services (IIS) and Certificate services Windows components, create the Server Certificate as follows:

① Start **[Internet Services Manager]**.

② Right-click **[Default Web Site]**, and then click **[Properties]**.

③ On the **[Directory Security]** tab, click **[Server Certificate]**.
Web Server Certificate Wizard starts.

④ Click **[Next]**.

⑤ Select **[Create a new certificate]**, and then click **[Next]**.

⑥ Select **[Prepare the request now, but send it later]**, and then click **[Next]**.

⑦ Enter the required information according to the instructions given by Web Server Certificate Wizard.

⑧ Check the specified data, which appears as Request File Summary, and then click **[Next]**.
The server certificate is created.

If the fax number cannot be obtained

If the fax number cannot be obtained during authentication, specify the setting as follows:

① Start **[C:\WINNT\SYSTEM32\adminpak]**.
Start Setup Wizard.

② Select **[Install all of the Administrator Tools]**, and then click **[Next]**.

③ On the **[Start]** menu, select **[Run]**.

④ Enter **[mmc]**, and then click **[OK]**.

⑤ On the **[Console]**, select **[Add/Remove Snap-in]**.

⑥ Click **[Add]**.

⑦ Select **[ActiveDirectory Schema]**, and then click **[Add]**.

⑧ Select **[facsimile Telephone Number]**.

⑨ Right-click, and then click **[Properties]**.

⑩ Select **[Replicate this attribute]**, and then click **[Apply]**.

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 registered to the machine, enabling user authentication without first using the machine to register individual settings in the address book.

Important

- ❒ If user information on the server is changed, information registered in the machine may be overwritten when authentication is performed.

Limitation

- ❒ When using LDAP Authentication, to prevent the password information being sent over the network unencrypted, the machine and LDAP server must communicate via SSL. To enable this, you must create a server certificate for the LDAP server.
- ❒ To use LDAP authentication, the network configuration must allow the machine to detect the presence of the LDAP server.
- ❒ To use LDAP authentication you need to register the LDAP server in the machine. For details about registration, see *Network Guide*.
- ❒ Under LDAP authentication, you cannot specify access limits for groups registered in the LDAP Server.
- ❒ When using LDAP Authentication, you cannot use LDAP search.
- ❒ 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.
- ❒ Do not use Japanese, Traditional Chinese, Simplified Chinese or Hangul multi-byte characters when entering the login user name or password. If you use multi-byte characters , you cannot authenticate using Web Image Monitor.

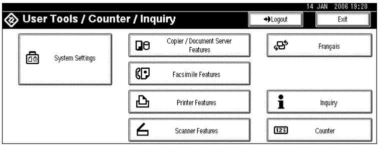
Note

- ❒ If you want to use LDAP authentication, you need to register the user name that is registered in the LDAP server.
- ❒ By default, the user can use all of the machine's functions. If you want to limit the available functions, specify the available functions for each user.

Specifying LDAP Authentication

1 Press the 【User Tools/Counter】 key.

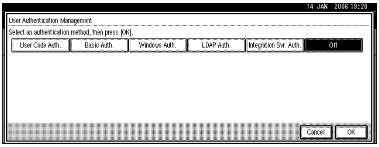
2 Press [System Settings].



3 Press [Administrator Tools].

4 Press [User Authentication Management].

5 Select [LDAP Authentication].


14 JAN 2006 19:20

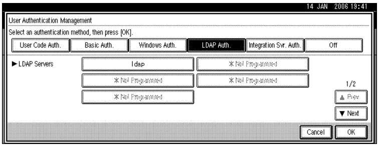
User Authentication Management

Select an authentication method, then press [OK].

Note

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

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


14 JAN 2006 19:41

User Authentication Management

Select an authentication method, then press [OK].

LDAP Auth.

► LDAP Servers: ldap

7 Select the "Printer Job Auth." level.

Note

- ❒ If you select **[Entire]**, you cannot print using a printer driver or a device that does not support authentication. To also print under an environment that does not support authentication, select **[Simple (All)]**. By making this setting, only registered users will be able to print.
- ❒ By selecting **[Simple(Limitation)]**, you can specify clients for which printer job authentication is not required. Specify **[Parallel Interface: Simple]**, **[USB: Simple]** and the clients' IP address range in which printer job authentication is not required. Specify this setting if you want to print using unauthenticated printer drivers or without any printer driver. Authentication is required for printing with non-specified devices.

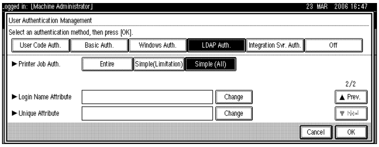
❒ If you select **[Simple (All)]** or **[Simple(Limitation)]**, you can print even with unauthenticated printer drivers or devices. Specify this setting if you want to print with a printer driver or device that cannot be identified by the machine or if you do not require authentication for printing.However, note that, because the machine does not require authentication in this case, it may be used by unauthorized users.

Reference

For details, see p.86 “Printer Job Authentication Levels and Printer Job Types”.

Specifying **[Simple(Limitation)]**

❶ Press [Simple(Limitation)]



ogged in: [Machine Administrator] 23 MAR 2006 16:47

User Authentication Management

Select an authentication method, then press [OK].

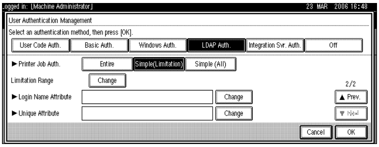
User Code Auth. | Basic Auth. | Windows Auth. | [✓ LDAP Auth.] | Integration Svr. Auth. | Off

► Printer Job Auth. Entire | Simple(Limitation) | [✓ Simple (All)]

► Login Name Attribute

► Unique Attribute

❷ Press [Change].



ogged in: [Machine Administrator] 23 MAR 2006 16:48

User Authentication Management

Select an authentication method, then press [OK].

User Code Auth. | Basic Auth. | Windows Auth. | [✓ LDAP Auth.] | Integration Svr. Auth. | Off

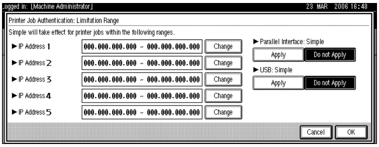
► Printer Job Auth. Entire | [✓ Simple(Limitation)] | Simple (All)

Limitation Range

► Login Name Attribute

► Unique Attribute

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



ogged in: [Machine Administrator] 23 MAR 2006 16:48

Printer Job Authentication: Limitation Range

Simple will take effect for printer jobs within the following ranges.

► IP Address 1 000.000.000.000 ~ 000.000.000.000

► IP Address 2 000.000.000.000 ~ 000.000.000.000

► IP Address 3 000.000.000.000 ~ 000.000.000.000

► IP Address 4 000.000.000.000 ~ 000.000.000.000

► IP Address 5 000.000.000.000 ~ 000.000.000.000

► Parallel Interface: Simple Apply [✓ Do not Apply]

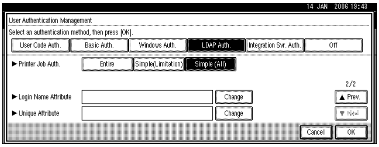
► USB: Simple Apply [✓ Do not Apply]

❹ Press [OK].

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

Note

- ❒ When using OpenLDAP, register the login name attribute using an attribute name such as "uid". However, you do not need to register this if you want to authenticate using the DN.



14 JAN 2006 19:43

User Authentication Management

Select an authentication method, then press [OK].

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

9 **Enter the unique attribute in [Unique Attribute], and then press [OK].**

Note

- ❒ In **[Unique Attribute]**, enter the attribute for managing unique information on the server. You can enter an attribute such as "serialNumber" or "uid". Additionally, you can enter "cn" or "employeeNumber", provided it is unique.

10 **Press [OK].**

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

Integration Server Authentication

To use Integration Server Authentication, you need a server on which ScanRouter software that supports authentication is installed.

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

For example, if the delivery server and the machine share the same Integration Server Authentication, single sign-on is possible using DeskTopBinder.

Important

- ❒ If user information on the server is changed, information registered in the machine may be overwritten when authentication is performed.

Limitation

- ❒ To use Integration Server Authentication, which depends on communication via the secure sockets layer (SSL), the machine must have the printer and scanner functions.

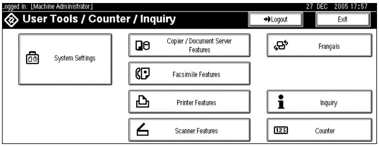
Note

- ❒ The built-in default administrator name is "Admin" on the Server and "admin" on the machine.

Specifying Integration Server Authentication

1 Press the 【User Tools/Counter】 key.

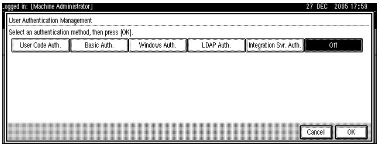
2 Press [System Settings].



3 Press [Administrator Tools].

4 Press [User Authentication Management].

5 Select [Integration Svr. Auth.].


Logged in: [Machine Administrator] 27 DEC 2005 17:59

User Authentication Management

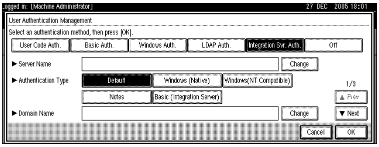
Select an authentication method, then press [OK].

Note

- ❒ If you do not wish to use User Authentication Management, select **[Off]**.

6 Press [Change] for "Server Name".

Specify the name of the server for external authentication.


Logged in: [Machine Administrator] 27 DEC 2005 18:01

User Authentication Management

Select an authentication method, then press [OK].

Authentication Type: Default

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

Enter the IP address or host name.

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

Select an available authentication system.

9 Press [Change] for "Domain Name".

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

Note

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

If global groups have been registered:

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

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

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

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]** to scroll down to other settings.

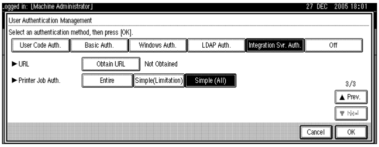
❷ Press [Change], and then enter the group name.

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

❹ Press [OK].

11 Press [OK]

12 Select the "Printer Job Auth." level.



Logged in: [Machine Administrator] 27 DEC 2005 18:01

User Authentication Management

Select an authentication method, then press [OK].

Integration Svr. Auth.

URL: Not Obtained

Printer Job Auth.: Simple (All)

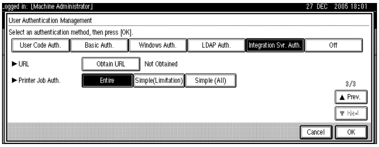
Note

- ❒ If you select **[Entire]**, you cannot print using a printer driver or a device that does not support authentication. To print under an environment that does not support authentication, select **[Simple (All)]**. By making this setting, only registered users will be able to print.
- ❒ If you select **[Simple(Limitation)]**, you can specify clients for which printer job authentication is not required. Specify **[Parallel Interface: Simple]**, **[USB: Simple]** and the clients' IP address range in which printer job authentication is not required. Specify this setting if you want to print using unauthenticated printer drivers or without any printer driver. Authentication is required for printing with non-specified devices.

❒ If you select **[Simple (All)]** or **[Simple(Limitation)]**, you can print even with unauthenticated printer drivers or devices. Specify this setting if you want to print with a printer driver or device that cannot be identified by the machine or if you do not require authentication for printing.However, note that, because the machine does not require authentication in this case, it may be used by unauthorized users.

Specifying **[Simple(Limitation)]**

❶ **Press [Simple(Limitation)]**



Logged in: [Machine Administrator] 27 DEC 2005 18:01

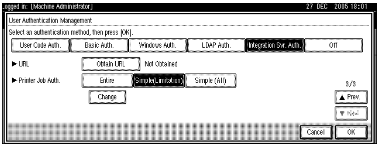
User Authentication Management

Select an authentication method, then press [OK].

▶URL Not Obtained

▶Printer Job Auth. Entire

❷ **Press [Change].**



Logged in: [Machine Administrator] 27 DEC 2005 18:01

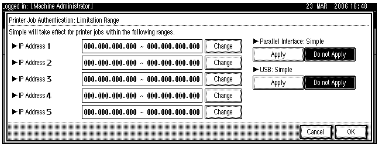
User Authentication Management

Select an authentication method, then press [OK].

▶URL Not Obtained

▶Printer Job Auth. Simple(Limitation)

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



Logged in: [Machine Administrator] 23 MAR 2006 16:48

Printer Job Authentication: Limitation Range

Simple will take effect for printer jobs within the following ranges.

▶IP Address 1 000.000.000.000 ~ 000.000.000.000

▶IP Address 2 000.000.000.000 ~ 000.000.000.000

▶IP Address 3 000.000.000.000 ~ 000.000.000.000

▶IP Address 4 000.000.000.000 ~ 000.000.000.000

▶IP Address 5 000.000.000.000 ~ 000.000.000.000

▶Parallel Interface: Simple Do not Apply

▶USB: Simple Do not Apply

❹ **Press [OK].**

Printer Job Authentication Levels and Printer Job Types

This section explains the relationship between printer job authentication levels and printer job types.

Depending on the combination of printer job authentication level and printer job type, the machine may not print properly. Set an appropriate combination according to the operating environment.

User authentication is supported by the RPCS and PCL printer drivers.

Machine Settings (displayed on the control panel)			Printer Job Types						
[User Authentication Management]	**[Printer Job Auth.]**	**[Restrict Use of Simple Encryption]**	①	②	③	④	⑤	⑥	⑦
[Off]	—	—	☆	☆	☆	☆	☆	☆	☆
[User Code Authentication]	—	—	❍	❍	❍	❍	❍	×	×
[Basic Authentication], [Windows Authentication], [LDAP Authentication], [Integration Svr. Auth.]	**[Simple (All)]**	**[Off]**	●	❍	×	☆	☆	☆	❍
		[On]		×					
	[Entire]	**[Off]**	●	❍	×	❍	×	×	❍
		[On]		×					

☆: Printing is possible regardless of user authentication.

❍: Printing is possible if user authentication is successful. If user authentication fails, the print job is reset.

●: Printing is possible if user authentication is successful and **[Driver Encryption Key]** for the printer driver and machine match.

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

Reference

For details about **[Restrict Use of Simple Encryption]**, see p.109 "Specifying the Extended Security Functions".

❖ [Printer Job Auth.]

- **[Entire]**
  The machine authenticates all printer jobs and remote settings, and cancels jobs and settings that fail authentication.
  Printer Jobs: Job Reset
  Settings: Disabled
- **[Simple (All)]**
  The machine authenticates printer jobs and remote settings that have authentication information, and cancels the jobs and settings that fail authentication. Printer jobs and settings without authentication information are performed without being authenticated.
- **[Simple(Limitation)]**.
  You can specify the range to apply **[Simple(Limitation)]** to by specifying **[Parallel Interface: Simple]**, **[USB: Simple]**, and the client's IP address.

❖ Printer Job Types

① In the RPCS printer driver dialog box, the **[Confirm authentication information when printing]** and **[Encrypt]** check boxes are selected.
In the PCL printer driver dialog box, the **[User Authentication]** and **[With Encryption]** check boxes are selected.
Personal authentication information is added to the printer job.
The printer driver applies advanced encryption to the login passwords.
The printer driver encryption key, enables the driver encryption to prevent the login password being stolen.

② In the RPCS printer driver dialog box, the **[Confirm authentication information when printing]** check box is selected.
In the PCL printer driver dialog box, the **[User Authentication]** and **[With Encryption]** check boxes are selected.
Personal authentication information is added to the printer job.
The printer driver applies simple encryption to login passwords.

③ In the RPCS printer driver dialog box, the **[Confirm authentication information when printing]** check box is not selected.
In the PCL printer driver dialog box, the **[User Authentication]** check box is not selected.
Personal authentication information is added to the printer job and is disabled.

④ When using the PostScript 3 printer driver, the printer job contains user code information.
Personal authentication information is not added to the printer job but the user code information is.

Note

❒ This type also applies to recovery/parallel printing using an RPCS/PCL printer driver that does not support authentication.

⑤ When using the PostScript 3 printer driver, the printer job does not contain user code information.
Neither personal authentication information nor user code information is added to the printer job.

Note

❒ Type 5 also applies to recovery/parallel printing using an RPCS/PCL printer driver that does not support authentication.

⑥ A printer job or PDF file is sent from a host computer without a printer driver and is printed via LPR.
Personal authentication information is not added to the printer job.

⑦ A PDF file is printed via ftp.
Personal authentication is performed using the user ID and password used for logging on via ftp. However, the user ID and password are not encrypted.

Authentication Information Stored in the Address Book

Preparation

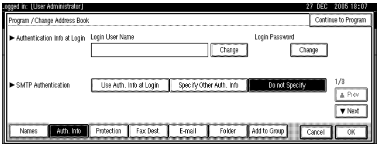
For details about logging on and logging off with administrator authentication, see p.106 “Logging on Using Administrator Authentication”, p.107 “Logging off Using Administrator Authentication”.

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

Specifying Login User Name and Login Password

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]** to scroll down to other settings.
5. **Select the user or group.**
6. **Press [Auth. Info].**
7. **Press [Change] for [Login User Name].**



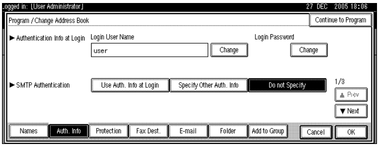
.ogged in: [User Administrator] 27 DEC 2005 18:07

Program / Change Address Book

▶ Authentication Info at Login Login User Name Login Password

▶ SMTP Authentication

8. **Enter a login user name, and then press [OK].**
9. **Press [Enter] for [Login Password].**



.ogged in: [User Administrator] 27 DEC 2005 18:06

Program / Change Address Book

▶ Authentication Info at Login Login User Name: user Login Password

▶ SMTP Authentication

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

12 Press [OK].

13 Press [Exit].

14 Press the 【User Tools/Counter】 key.

Specifying Authentication Information to Log on

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", "Integration Server 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", "Integration Server Authentication" or "LDAP Authentication", see *General Settings Guide*.

Note

❒ If you want to use **[Windows Authentication]**, **[LDAP Authentication]**, or **[Integration Svr. Auth.]** 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]** to scroll down to other settings.

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.42 "Limiting Available Functions".

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

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

Limitation

- ❒ When using **[Use Auth. Info at Login]** for “SMTP Authentication”, “Folder Authentication”, or “LDAP Authentication”, a user name other than “other” , “admin” , “supervisor” or “HIDE***” must be specified. The symbol “***” represents any character.
- ❒ 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

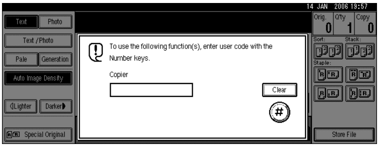
When user authentication (User Code Authentication, Basic Authentication, Windows Authentication, LDAP Authentication, or Integration Server Authentication) is set, the authentication screen is displayed. Unless a valid user name and password are entered, operations are not possible with the machine. 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.When auto logout timer is specified, the machine automatically logs you off if you do not use the control panel within a given time.

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.



To use the following function(s), enter user code with the Number keys.

Copier

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

Note

- ❒ To log off, do one of the following:
  - Press the Operation switch.
  - Press the **【User Tools/Counter】** key.
  - Press the **【Energy Saver】** key after jobs are completed.

User Code Authentication (Using a Printer Driver)

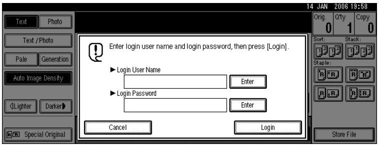
When user authentication is set, specify the user code in the printer properties of a printer driver. For details, see the printer driver Help.

Login (Using the Control Panel)

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

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

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



Enter login user name and login password, then press [Login].

▶ Login User Name

▶ Login Password

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].

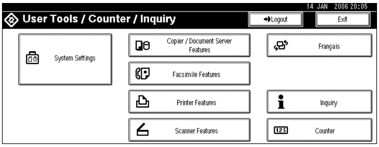
When the user is authenticated, the screen for the function you are using appears.

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 a Printer Driver)

When Basic Authentication, Windows Authentication, or LDAP Authentication is set, make encryption settings in the printer properties of a printer driver, and then specify a login user name and password. For details, see the printer driver Help.

Note

❒ When logged on using a printer driver, logging off is not required.

Login (Using Web Image Monitor)

This section explains how to log onto the machine via Web Image Monitor.

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

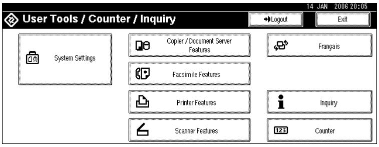
❒ Delete the cache memory in the Web browser after logging off.

Auto Logout

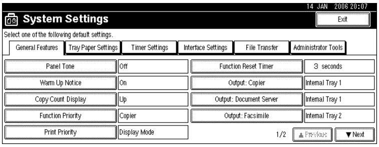
When using user authentication management, the machine automatically logs you off if you do not use the control panel within a given time. This feature is called "Auto Logout". Specify how long the machine is to wait before performing Auto Logout.

1 Press the 【User Tools/Counter】 key.

2 Press [System Settings].



3 Press [Timer Settings].



Select one of the following default settings.

Panel Tone	Off	Function Reset Timer	3 seconds
Warm Up Notice	On	Output: Copier	Internal Tray 1
Copy Count Display	Up	Output: Document Server	Internal Tray 1
Function Priority	Copier	Output: Facsimile	Internal Tray 2
Print Priority	Display Mode		

4 Press [Auto Logout Timer].

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

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 and the printer's regular menus 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.138 "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]**. For details about the menu protect level for each function, see p.138 "User Administrator Settings".

Note

❒ The functions that can be used and specified depend on which administrators (machine administrator, network administrator, or file administrator) are set to **[On]** in **[Menu Protect]** in **[Facsimile Features]**. If an administrator is set to **[Off]**, menu protect limitation is not effective for that administrator.

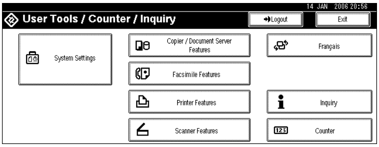
Copying Functions

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.**

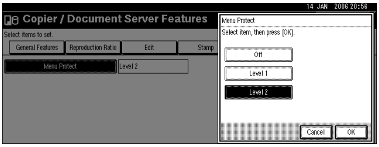
2 **Press [Copier / Document Server Features].**



3 **Press [Administrator Tools].**

4 **Press [Menu Protect].**

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



Copier / Document Server Features

Select items to set.

Menu Protect Level 2

Menu Protect

Select item, then press [OK].

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

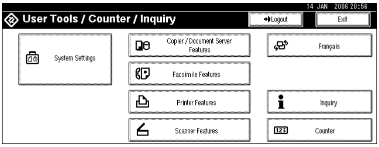
Fax Functions

Note

- ❒ To specify **[Menu Protect]** in **[Facsimile Features]**: Under **[System Settings]**, **[Administrator Tools]**, **[Administrator Authentication Management]**, set **[Machine Management]**, **[File Management]**, and **[Network Management]** to **[On]**.

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

2 **Press [Facsimile Features].**



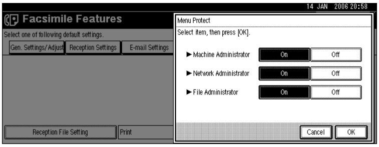
User Tools / Counter / Inquiry

3 **Press [Administrator Tools].**

4 **Press [Menu Protect].**

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

5 **Select the administrator setting, and then click [OK].**



Facsimile Features

Select one of following default settings.

Menu Protect

Select item, then press [OK].

► Machine Administrator On

► Network Administrator On

► File Administrator On

Note

- ❒ Only settings of the administrator who is logged on can be specified. If there is more than one administrator, make settings individually for each.

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

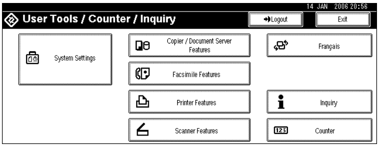
Printer Functions

Note

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

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

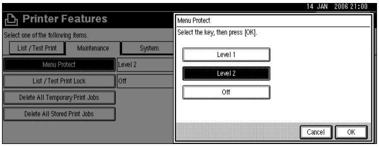
2 **Press [Printer Features].**



3 **Press [Maintenance].**

4 **Press [Menu Protect].**

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


14 JAN 2006 21:00
Printer Features
Select one of the following items.
List / Test Print
Maintenance
System

Menu Protect: Level 2

List / Test Print Lock: Off

Delete All Temporary Print Jobs
Delete All Stored Print Jobs
Menu Protect
Select the key, then press [OK].
Level 1
Level 2
Off
Cancel
OK

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

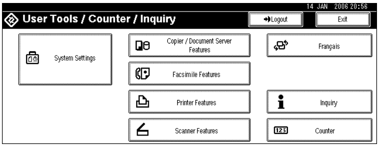
Scanner Functions

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.**

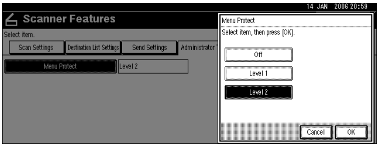
2 **Press [Scanner Features].**



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.

- User Administrator
- Machine Administrator
- Network Administrator
- File 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.104 "Registering the Administrator".

❖ **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.

❖ **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.

❖ 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.121 “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.

Administrators are limited to managing the machine's settings and controlling user access. so they cannot use functions such as copying and printing. To use such functions, you need to register a user in the address book and then be authenticated as the user.

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.

❒ To prevent the password from being guessed, we strongly recommend that you specify the login password according to the Password Policy.

❒ Do not use Japanese, Traditional Chinese, Simplified Chinese or Hangul multi-byte characters when entering the login user name or password.If you use multi-byte characters when entering the login user name or password, you cannot authenticate using Web Image Monitor.

❒ 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.

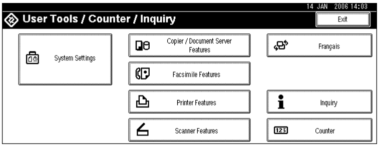
Preparation

For details about logging on and logging off with administrator authentication, see p.106 "Logging on Using Administrator Authentication", p.107 "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].



14 JAN 2006 14:03

User Tools / Counter / Inquiry

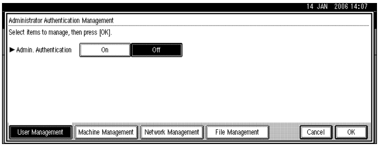
3 Press [Administrator Tools].

4 Press [Administrator Authentication Management].

5 Specify each administrator authentication.

Specifying User Management Authentication

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



14 JAN 2006 14:07

Administrator Authentication Management

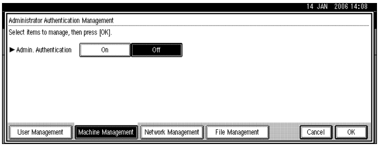
Select items to manage, then press [OK].

► Admin. Authentication

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

Specifying Machine Management Authentication

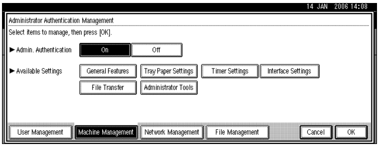
❶ **Press [Machine Management], and then press [On].**


14 JAN 2006 14:08

Administrator Authentication Management

Select items to manage, then press [OK].

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


14 JAN 2006 14:08

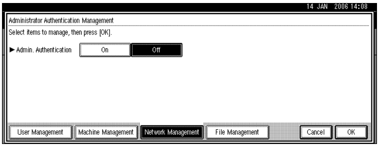
Administrator Authentication Management

Select items to manage, then press [OK].

The selected settings will be unavailable to users.

Specifying Network Management Authentication

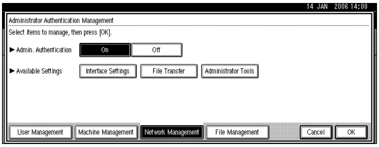
❶ **Press [Network Management], and then press [On].**


14 JAN 2006 14:08

Administrator Authentication Management

Select items to manage, then press [OK].

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


14 JAN 2006 14:08

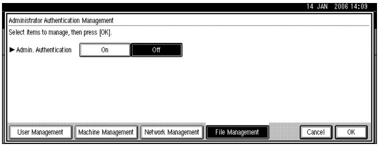
Administrator Authentication Management

Select items to manage, then press [OK].

The selected settings will be unavailable to users.

Specifying File Management Authentication

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

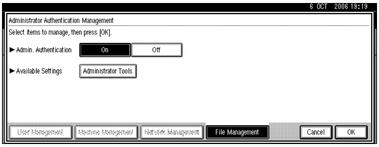


14 JAN 2006 14:09

Administrator Authentication Management

Select items to manage, then press [OK].

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



6 OCT 2006 19:19

Administrator Authentication Management

Select items to manage, then press [OK].

6 Press [OK].

7 Press the 【User Tools/Counter】 key.

Registering the Administrator

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

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

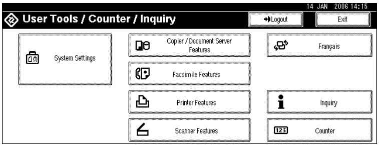
Administrator authentication can also be specified via Web Image Monitor. For details see the Web Image Monitor Help.

Preparation

If administrator authentication has already been specified, log on using a registered administrator name and password. For details about logging on and logging off with administrator authentication, see p.106 "Logging on Using Administrator Authentication", p.107 "Logging off Using Administrator Authentication".

1 Press the 【User Tools/Counter】 key.

2 Press [System Settings].

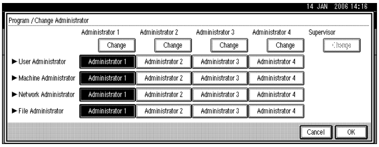


14 JAN 2006 14:15

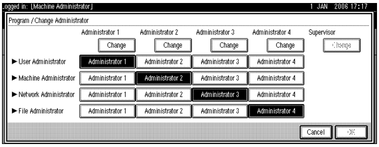
3 Press [Administrator Tools].

4 Press [Program / Change Administrator].

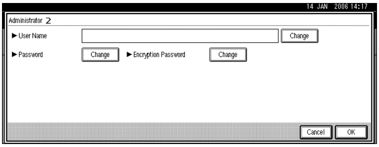
5 In the line for the administrator whose authority you want to specify, press [Administrator 1], [Administrator 2], [Administrator 3] or [Administrator 4], and then press [Change].



If you allocate each administrator's authority to a different person, the screen appears as follows:

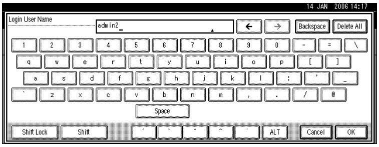


6 Press [Change] for the login user name.



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

8 Press [Change] for the login password.

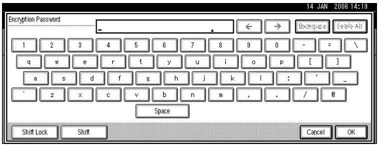


9 Enter the login password, and then press [OK].

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

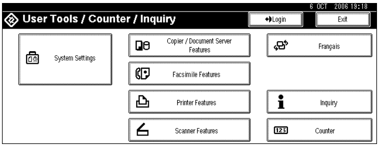
If administrator authentication has been specified, log on using an administrator's user name and password.This section describes how to log on.

Note

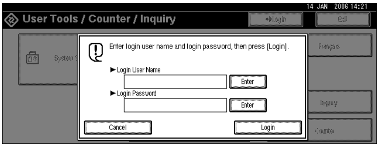
- ❒ If user authentication has already been specified, a screen for authentication appears.
- ❒ To log on as an administrator, enter the administrator's login user name and login password.
- ❒ If you log on using administrator authority, the name of the administrator logging on appears.
- ❒ If you log 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".



Enter login user name and login password, then press [Login].

▶Login User Name

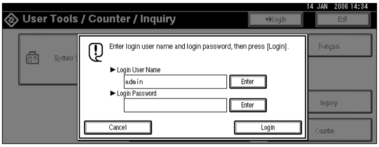
▶Login Password

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".



Enter login user name and login password, then press [Login].

▶Login User Name

admin

▶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.

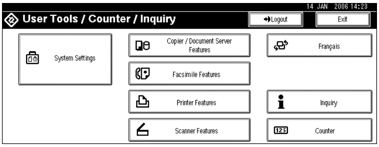
For example, to assign machine administrator authority and user administrator authority to **[Administrator 1]**, press **[Administrator 1]** in the lines for the machine administrator and the user administrator.

Preparation

For details about logging on and logging off with administrator authentication, see p.106 "Logging on Using Administrator Authentication", p.107 "Logging off Using Administrator Authentication".

1 Press the 【User Tools/Counter】 key.

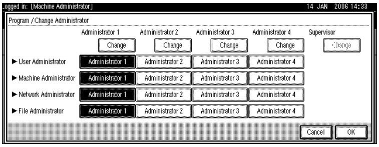
2 Press [System Settings].



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:

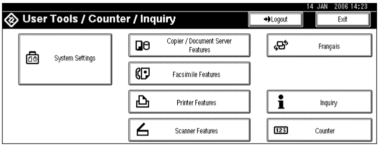
Preparation

For details about logging on and logging off with administrator authentication, see p.106 "Logging on Using Administrator Authentication", p.107 "Logging off Using Administrator Authentication".

Procedure for Changing the Extended Security Functions

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

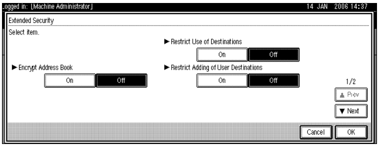
2. **Press [System Settings].**



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

4. **Press [Extended Security].**

5. **Press the setting you want to change, and change the setting.**


Logged in: [Machine Administrator]   14 JAN 2006 14:37

Extended Security

Select item.

▶Restrict Use of Destinations: On [✓ Off]

▶Encrypt Address Book: On [✓ Off]

▶Restrict Adding of User Destinations: On [✓ Off]

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 printer driver Help.

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.

Reference

See p.31 "Encrypting the Data in the Address Book".

- On
- Off

Note

❒ Default: *Off*

❖ Restrict Use of Destinations

This can be specified by the user administrator.
The available fax and scanner destinations are limited to the destinations registered in the address book.

Reference

See p.27 "Restrictions on Destinations".
A user cannot directly enter the destinations for transmission.

Limitation

❒ If you specify the setting to receive e-mails via SMTP, you cannot use **[Restrict Use of Destinations]**.

Note

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

- On
- Off

Note

❒ Default: *Off*

❖ Restrict Adding of User Destinations

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

- On
- Off

Note

❒ Default: *Off*

❖ Restrict Display of User Information

This can be specified by the machine administrator.
This can be specified if user authentication is specified. When the job history is checked using a network connection for which authentication is not available, all personal information can be displayed as "********". For example, when someone not authenticated as an administrator checks the job history using SNMP in 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: *Off*

❖ Enhance File Protection

This can be specified by the file administrator. By specifying a password, you can limit operations such as printing, deleting, and sending files, and can prevent unauthorized people from accessing the files. However, it is still possible for the password to be cracked.
By specifying "Enhance File Protection", files are locked and so become inaccessible if an invalid password is entered ten times. This can protect the files from unauthorized access attempts in which a password is repeatedly guessed.
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*

❖ **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 **[Prohibit]**, the setting can be viewed but not specified with SNMPv1, v2.

- Prohibit
- Do not Prohibit

Note

❒ Default: *Do not Prohibit*

❖ **Restrict Use of Simple Encryption**

This can be specified by the network administrator.
For example, this setting is set to **[On]** 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 delivery software, enable SSL/TLS for encrypted communication. For details about specifying SSL/TLS, see p.59 "Setting the SSL / TLS Encryption Mode".

- On
- Off

Note

❒ Default: *Off*

❖ **Transfer to Fax Receiver**

This can be specified by the machine administrator.
If you use **[Forwarding]** or **[Forwarding]** under the fax function, files stored in the machine can be transferred or delivered.
If you select **[Prohibit]** for this setting, stored files cannot be transferred by **[Forwarding]** and **[Transfer Request]**.
Use this setting, to prevent the stored files being transferred by mistake.

- Prohibit
- Do not Prohibit

Note

❒ Default: *Do not Prohibit*

❒ If you select **[Prohibit]** for this setting, the following functions are disabled:

- Polling Transmission
- Transfer Request
- Forwarding
- Transfer Box
- Delivery from Personal Box
- Information Box
- Delivery of Mail Received via SMTP

Reference

For details, see *Facsimile Reference <Advanced Features>*.

❖ **Authenticate Current Job**

This can be specified by the machine administrator.

This setting lets you specify whether or not authentication is required for operations such as canceling jobs under the copier and printer functions.

If you select **[Login Privilege]**, authorized users and the machine administrator can operate the machine. When this is selected, authentication is not required for users who logged on to the machine before **[Login Privilege]** was selected.

If you select **[Access Privilege]**, users who canceled a copy or print job in progress and the machine administrator can operate the machine.

Limitation

❒ Even if you select **[Login Privilege]** and log onto the machine, you cannot cancel a copy or print job in progress if you are not authorized to use the copy and printer functions.

❒ You can specify **[Authenticate Current Job]** only if **[User Authentication Management]** was specified.

- Login Privilege
- Access Privilege
- Off

Note

❒ Default: *Off*

❖ **Password Policy**

This can be specified by the user administrator.

This setting lets you specify **[Complexity Setting]** and **[Minimum Character No.]** for the password. By making this setting, you can limit the available passwords to only those that meet the conditions specified in **[Complexity Setting]** and **[Minimum Character No.]**.

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

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

Limitation

❒ This setting will only be effective if **[User Authentication]** or **[Basic Authentication]** has been specified.

Other Security Functions

Fax Function

❖ **Not Displaying Destinations and Senders in Reports and Lists**

You can specify whether or not to display destinations and senders by clicking **[Facsimile Features]**, **[Administrator Tools]**, **[Parameter Setting]** and specifying “Bit No. 04” and “Bit No. 05” under “Switch 04”. Not displaying destinations and senders helps prevent information leaks.

Reference

For details, see “User Parameters”, *Facsimile Reference <Advanced Features>*.

❖ **Stored RX File User Setting**

You can specify which users can manage fax files stored on the hard disk by setting **[Facsimile Features]**, **[Administrator Tools]**, **[Stored RX File User Setting]** to **[On]**.
To access the machine over the network, specified users must enter their user codes or login user names and passwords.
By allowing only authorized users to manage files, you can prevent others seeing the faxes you sent.

Reference

For details, see “Stored RX File User Setting”, *Facsimile Reference <Advanced Features>*.

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.

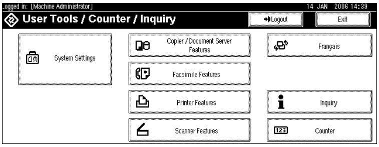
Specifying Service Mode Lock

Preparation

For details about logging on and logging off with administrator authentication, see p.106 "Logging on Using Administrator Authentication", p.107 "Logging off Using Administrator Authentication".

1 Press the 【User Tools/Counter】 key.

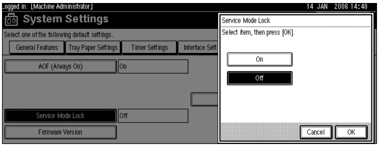
2 Press [System Settings].



3 Press [Administrator Tools].

4 Press [Service Mode Lock].

5 Press [On] and then [OK].


Logged in: [Machine Administrator] 14 JAN 2006 14:48

System Settings

Select one of the following default settings.

AOF (Always On): On

Service Mode Lock: Off

Service Mode Lock

Select item, then press [OK].

A confirmation message appears.

6 Press [Yes].

7 Press the 【User Tools/Counter】 key.

Canceling Service Mode Lock

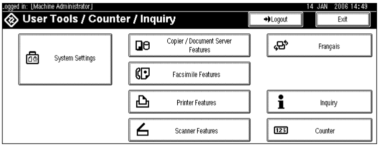
For a customer engineer to carry out inspection or repair in service mode, the machine administrator must log onto the machine and cancel the service mode lock.

Preparation

For details about logging on and logging off with administrator authentication, see p.106 "Logging on Using Administrator Authentication", p.107 "Logging off Using Administrator Authentication".

1 Press the 【User Tools/Counter】 key.

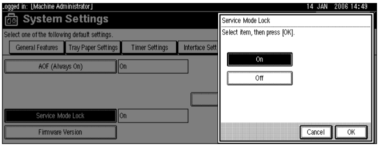
2 Press [System Settings].


Logged in: [Machine Administrator] 14 JAN 2006 14:49

3 Press [Administrator Tools].

4 Press [Service Mode Lock].

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


Logged in: [Machine Administrator] 14 JAN 2006 14:49

System Settings

Select one of the following default settings.

AOF (Always On): On

Service Mode Lock: On

Service Mode Lock

Select item, then press [OK].

6 Press the 【User Tools/Counter】 key.

The customer engineer can switch to service mode.

7. Troubleshooting

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
Failed to obtain URL.	The machine cannot connect to the server or cannot establish communication.	Make sure the server's settings, such as the IP Address and host name, are specified correctly on the machine. Make sure the host name of the UA Server is specified correctly.
	The machine is connected to the server, but the UA service is not responding properly.	Make sure the UA service is specified correctly.
	SSL is not specified correctly on the server.	Specify SSL using Authentication Management tool.
	Server authentication failed.	Make sure server authentication is specified correctly on the machine.
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, or Integration Server Authentication, so you cannot register additional users.	Delete unnecessary user addresses.
	Cannot access the authentication server when using Windows authentication , LDAP Authentication, or Integration Server Authentication.	A network or server error may have occurred. Contact to the network administrator.
The selected file(s) which you do not have access privileges to could not 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 print using the printer driver or connect using the TWAIN driver.	User authentication has been rejected.	Enter the login user name and login password in the printer driver. If using Windows authentication or , LDAP Authentication, or Integration Server Authentication, inquire the network administrator for the user name and login name. If using basic authentication, inquire the user administrator.
	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.50 "Driver Encryption Key".
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.
After starting **[User Management Tool]** or **[Address Management Tool]** in SmartDeviceMonitor for Admin and entering the correct login user name and password, a message appears to notify that an incorrect password has been entered.	"Restrict Simple Encryption" is not set correctly. Alternatively, **[SSL/TLS]** has been enabled although the required certificate is not installed in the computer.	Set "Restrict 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.112 "Restrict Use of Simple Encryption". See p.59 "Setting the SSL / TLS Encryption Mode".
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.		

Condition	Cause	Solution
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 access the machine using ScanRouter EX Professional V2.	ScanRouter EX Professional V2 does not support user authentication.	
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.
[ProgDest] does not appear on the fax or scanner screen for specifying destinations.	**[Restrict Adding of User 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.20 "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.29 "Protecting the Address Book".
Cannot print when user authentication has been specified.	User authentication may not be specified in the printer driver.	Specify user authentication in the printer driver. For details, see the printer driver Help.
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 or printer 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.

8. Appendix

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.

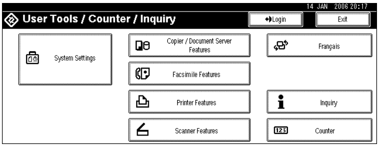
❒ Using Web Image Monitor, you can log on as the supervisor and delete an administrator's password.

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

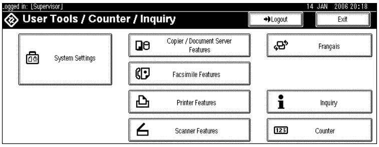
- ❒ When you assign the administrator for the first time, proceed to step 7 without pressing **[Enter]**.

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].

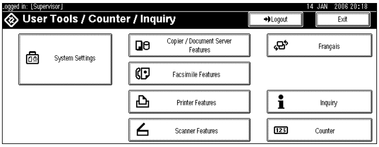


2 Press [Yes].

3 Press the 【User Tools/Counter】 key.

Changing the Supervisor

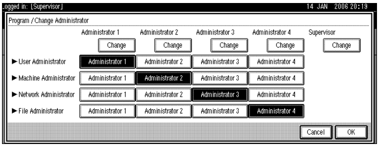
1. Press the 【User Tools/Counter】 key.
2. Press [System Settings].



.ogged in: [Supervisor] 14 JAN 2006 20:18

User Tools / Counter / Inquiry

3. Press [Administrator Tools].
4. Press [Program / Change Administrator].
5. Under “Supervisor”, click [Change].

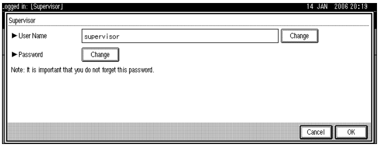


.ogged in: [Supervisor] 14 JAN 2006 20:19

Program / Change Administrator

	Administrator 1	Administrator 2	Administrator 3	Administrator 4	Supervisor
	Change	Change	Change	Change	Change
▶User Administrator	Administrator 1	Administrator 2	Administrator 3	Administrator 4	
▶Machine Administrator	Administrator 1	Administrator 2	Administrator 3	Administrator 4	
▶Network Administrator	Administrator 1	Administrator 2	Administrator 3	Administrator 4	
▶File Administrator	Administrator 1	Administrator 2	Administrator 3	Administrator 4	

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



.ogged in: [Supervisor] 14 JAN 2006 20:19

Supervisor

▶User Name supervisor Change

▶Password Change

Note: It is important that you do not forget this password.

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.**

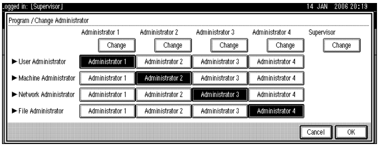
You can log on in the same way as an administrator.

4 **Press [System Settings].**

5 **Press [Administrator Tools].**

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

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



Logged in: [Supervisor] 14 JAN 2006 20:19

Program / Change Administrator

	Administrator 1	Administrator 2	Administrator 3	Administrator 4	Supervisor
	Change	Change	Change	Change	Change
▶ User Administrator	[✓ Administrator 1]	Administrator 2	Administrator 3	Administrator 4	
▶ Machine Administrator	Administrator 1	[✓ Administrator 2]	Administrator 3	Administrator 4	
▶ Network Administrator	Administrator 1	Administrator 2	[✓ Administrator 3]	Administrator 4	
▶ File Administrator	Administrator 1	Administrator 2	Administrator 3	[✓ Administrator 4]	

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

- Parallel Interface

❖ File Transfer

The following settings can be specified.

- Delivery Option
- Capture Server IP Address
- Fax RX File Transmission
  Line 1-3, E-mail Address, IP-Fax / RX File Delivery Settings
  Line 1-3, E-mail Address, IP-Fax / Print at Delivery
  Line 1-3, E-mail Address, IP-Fax / File to Deliver
- SMTP Authentication
  SMTP Authentication
  User Name
  E-mail Address
  Password
  Encryption
- POP before SMTP
  Wait Time after Auth.
  User Name
  E-mail Address
  Password
- Reception Protocol
- POP3 / IMAP4 Settings
  Server Name
  Encryption
- Administrator's E-mail Address

- Default User Name / Password (Send)
  SMB User Name / SMB Password
  FTP User Name / FTP Password
  NCP User Name / NCP Password
  Password
- Program / Change / Delete E-mail Message
- Program / Change / Delete Subject
- Fax E-mail Account

❖ 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
- Extended Security
  Restrict Display of user Information
  Transfer to Fax Receiver
  Authenticate Current Job
- Display / Print Counter
  Print Counter List
- Display / Clear / Print Counter per User
  All the settings can be specified.
- Capture Priority *1
  Capture: Ownership
  Capture: Public Priority
  Capture: Owner Defaults
- Extended Features
- AOF (Always On)
- Program / Change / Delete LDAP Server
  Identification Name
  Server Name
  Search Base
  Port No.
  Use Secure Connection (SSL)
  Authentication
  Search Conditions
  Search Options
- Use LDAP Server
- Service Mode Lock

- Auto Erase Memory Setting [*2]
- Erase All Memory [*2]
- Transfer Log Setting
- Data Security for Copying

[*1] File Format Converter option must be installed.

[*2] 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.

Facsimile Features

The following settings can be specified.

❖ Gen. Settings/ Adjust

All the settings can be specified

❖ Reception Settings

All the settings can be specified

❖ E-mail Settings

The following settings can be specified

- Internet Fax Settings
- SMTP RX File Delivery Settings

❖ Administrator Tools

The following settings can be specified.

- Program / Change / Delete Standard Message
- Store / Change / Delete Auto Document
- Program / Change / Delete Scan Size
- Print Journal
- Forwarding
- Memory Lock RX
- ECM
- Parameter Setting
- Program Special Sender
- Box Setting
- Transfer Report
- Program Confidential ID
- Program Polling ID
- Program Memory Lock ID
- Select Dial / Push Phone
- Program ISDN-G3 Line
- Program ISDN-G4 Line
- Memory File Transfer
- Reception File Setting
- Folder Transfer Result Report

Printer Features

The following settings can be specified.

❖ List / Test Print

All the settings can be specified.

❖ Maintenance

- Menu Protect
- List / Test Print Lock

❖ System

All the settings can be specified.

❖ Host Interface

All the settings can be specified.

❖ PCL Menu

All the settings can be specified.

❖ PS Menu [*1]

All the settings can be specified.

❖ PDF Menu [*1]

All the settings can be specified.

[*1] The PostScript 3 unit option must be installed.

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)
- Compression (Gray Scale)
- Print & Delete Scanner Journal
- E-mail Information Language
- Store File Priority
- Delete Scanner Journal
- Print Scanner Journal
- Stored file E-mail Method

❖ Administrator Tools

All the settings can be specified.

Settings via Web Image Monitor

The following settings can be specified.

❖ Top Page

- Reset Printer Job
- Reset Device

❖ Device Settings

- System
  Spool Printing
  Protect Printer Operation Panel
  Output Tray
  Paper Tray Priority
  Cover Sheet Tray
  Slip Sheet Tray
- Paper
  All the settings can be specified.
- Timer
  All the settings can be specified.
- Date/Time
  All the settings can be specified.
- E-mail
  All the settings can be specified.
- Auto E-mail Notification
  All the settings can be specified.
- On demand E-mail Notification
  All the settings can be specified.
- File Transfer
  All the settings can be specified.
- User Authentication Management
  All the settings can be specified.
- Administrator Authentication Management
  Machine Administrator Authentication
  Available Settings for Machine Administrator
- Program/Change Administrator
  You can specify the following administrator settings as the machine administrator.
  Login User Name
  Login Password
  Change Encryption Password
- LDAP Server
  All the settings can be specified.

❖ Printer

- System
  All the settings can be specified.
- Host Interface
  All the settings can be specified.
- PCL Settings
  All the settings can be specified.
- PS Settings [*1]
  All the settings can be specified.

- PDF Settings [*1]
  The following settings can be specified.
  Duplex
  Blank Page Print
  PDF Group Password
  Resolution
- PDF Group Password

[*1] The PostScript 3 unit option must be installed.

❖ Fax

- General
  All the settings can be specified.
- Administrator Tools
  All the settings can be specified.
- E-mail Settings
  All the settings can be specified.
- Parameter Settings
  All the settings can be specified.

❖ Interface Settings

- Parallel Interface
- USB

❖ Network

- SNMPv3

❖ RC Gate

All the settings can be specified.

❖ Webpage

All the settings can be specified.

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 Page Count
- Access Control List
- Reset User Counters

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
  Server Name
  Port No.
- E-mail Communication Port
- E-mail Reception Interval
- Scanner Recall Interval Time
- Number of Scanner Recalls
- Auto Specify Sender Name
- Max. Reception E-mail size
- E-mail Storage in Server

❖ 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
  Settings by SNMP V1 and V2
  Restrict Use of Simple Encryption

Facsimile Features

The following settings can be specified.

❖ E-mail Settings

- Max. E-mail Size

❖ IP-Fax Settings

All the settings can be specified.

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
  Device Name
  Comment
  Location
- E-mail
  Reception
  SMTP
  E-mail Communication Port
- Auto E-mail Notification
- 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

❖ Fax

- E-mail Settings
  Maximum E-mail Size
- IP-Fax Settings
  All the settings can be specified.
- Gateway Settings
  All the settings can be specified.

❖ Interface

- 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
- Bluetooth [*3]
  Operation Mode

[*1] The IEEE802.11b interface unit option must be installed.
[*2] The IEEE1394 interface board option must be installed.
[*3] The Bluetooth interface unit 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
  All the settings can be specified.

- SSDP
  All the settings can be specified.
- Rendezvous
  All the settings can be specified.

❖ Webpage

All the settings can be specified.

❖ Security

- Network Security
  All the settings can be specified.
- 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
- Auto Delete File in Document Server
- Delete All Files in Document Server

Facsimile Features

The following settings can be specified.

❖ Administrator Tools

- Stored RX File User Setting

Settings via Web Image Monitor

The following settings can be specified.

❖ Top Page

Reset Printer Job

❖ Document Server

All the settings can be specified.

❖ Job

- Printer
  Print Jobs [*1]

[*1] The file administrator can select **[Delete]**, **[Delete Password]**, and **[Unlock Job]**. The file administrator cannot print files.

❖ Device Settings

- Auto E-mail Notification
  All the settings can be specified.
- Administrator Authentication Management
  File Administrator Authentication
  Available Settings for File Administrator
- 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

❖ Printer

- Auto Delete Temporary Print Jobs
- Auto Delete Stored Print Jobs

❖ Webpage

- Download Help File

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
  Restrict Adding of User Destinations
  Encrypt Address Book
  Password Policy
- Print Address Book: Destination List
- Address Book Management
- Address Book: Program / Change / Delete Group
- Address Book: Program / Change / Delete Transfer Request
- 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

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

❖ Webpage

- Download Help File

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

Document Server File Permissions

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	❍[*1]	❍[*1]	❍[*1]	❍[*1]	❍[*1]	❍	❍	-
File Administrator	❍	❍	-	-	❍	❍	❍	❍

[*1] This setting can be specified by the owner.

The Privilege for User Account Settings 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]	-
	Protection Object	▲	▲	▲	❍	❍	▲
	Protect Dest.: Permissions for Users/ Groups	-	-	-	❍	❍	❍
	Protect File(s): Permissions for Users/ Groups	-	-	-	❍	❍	❍

Settings		**User**			**User Administrator**	**Registered User**	**Full Control**
		Read-only	**Edit**	**Edit / Delete**			
FaxDest.	Transmission Format	▲	❍	❍	❍	❍	▲
	Facsimile Number	▲	❍	❍	❍	❍	❍
	International TX Mode	▲	❍	❍	❍	❍	❍
	Fax Header	▲	❍	❍	❍	❍	❍
	Label Insertion	▲	❍	❍	❍	❍	❍
E-mail Address	E-mail Address	▲	❍	❍	❍	❍	❍
Folder Destination	SMB/FTP/NCP	▲	❍	❍	❍	❍	❍
	SMB: Path	▲	❍	❍	❍	❍	❍
	FTP: Port No.	▲	❍	❍	❍	❍	❍
	FTP: Server Name	▲	❍	❍	❍	❍	❍
	FTP: Path	▲	❍	❍	❍	❍	❍
	NCP: Path	▲	❍	❍	❍	❍	❍
	NCP: Connection type	▲	❍	❍	❍	❍	❍

*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 Function Key: F 1-5	❍	❍	▲
	Document Server Storage Key: F 1-5	❍	❍	▲
	Copy Quality	❍	❍	▲
	Image Density	❍	❍	▲
Edit	Erase Original Shadow in Combine	❍	❍	▲
	Image Repeat Separation Line	❍	❍	▲
	Double Copies Separation Line	❍	❍	▲
	Separation Line in Combine	❍	❍	▲
	Front Cover Copy in Combine	❍	❍	▲
	Copy on Designating Page in Combine	❍	❍	▲
	Orientation: Booklet, Magazine	❍	❍	▲
	Copy Order in Combine	❍	❍	▲

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 Only *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	Font	❍	❍	▲
		Stamp Position: *1	❍	❍	▲
		Size	❍	❍	▲
		Superimpose	❍	❍	▲

Tab Names		Settings	Menu Protect		
			Off	Level 1	Level 2
Stamp	Page Numbering	Font	❍	❍	▲
		Size	❍	❍	▲
		Duplex Back Page Stamping Position	❍	❍	▲
		Page Numbering in Combine	❍	❍	▲
		Stamp on Designating Slip Sheet	❍	❍	▲
		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]	❍	❍	▲
		Super Impose	❍	❍	▲
		Page Numbering Initial Letter	❍	❍	▲
Input / Output		Switch to Batch	❍	❍	▲
		Select Stack Function	❍	❍	▲

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

Printer Functions

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

❖ Normal Printer Screen

Functions	Menu Protect		
	Off	Level 1	Level 2
Print Jobs	❍	❍	❍

❖ Printer Features

Tab Names	Settings	Menu Protect		
		Off	Level 1	Level 2
System	Print Error Report	❍	▲	▲
	Auto Continue	❍	▲	▲
	Memory Overflow	❍	▲	▲
	Job Separation	❍	▲	▲
	Auto Delete Temporary Print Jobs	❍	▲	▲
	Auto Delete Stored Print Jobs	❍	▲	▲
	Initial Print Job List	❍	▲	▲
	Memory Usage	❍	▲	▲
	Duplex	❍	▲	▲
	Copies	❍	▲	▲
	Blank Page Print	❍	▲	▲
	Edge Smoothing	❍	▲	▲
	Toner Saving	❍	▲	▲
	Printer Language	❍	▲	▲
	Sub Paper Size	❍	▲	▲
	Page Size	❍	❍	▲
	Letterhead Setting	❍	▲	▲
	Bypass Tray Setting Priority	❍	▲	▲
	Edge to Edge Print	❍	▲	▲
	Default Printer Language	❍	▲	▲
	Tray Switching	❍	▲	▲
Host Interface	I/O Buffer	❍	▲	▲
	I/O Timeout	❍	▲	▲

Tab Names	Settings	Menu Protect		
		Off	Level 1	Level 2
PCL Menu	Orientation	❍	▲	▲
	Form Lines	❍	▲	▲
	Font Source	❍	▲	▲
	Font Number	❍	▲	▲
	Point Size	❍	▲	▲
	Font Pitch	❍	▲	▲
	Symbol Set	❍	▲	▲
	Courier Font	❍	▲	▲
	Extend A4 Width	❍	▲	▲
	Append CR to LF	❍	▲	▲
	Resolution	❍	▲	▲
PS Menu [*1]	Data Format	❍	▲	▲
	Resolution	❍	▲	▲
PDF Menu [*1]	Change PDF Password	❍	▲	▲
	PDF Group Password	❍	▲	▲
	Resolution	❍	▲	▲

[*1] The PostScript 3 unit option must be installed.

Scanner Features

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

Tab Names	Settings	Menu Protect		
		Off	**Level 1**	**Level 2**
Destination List Settings	Destination List Priority 1	❍	❍	▲
	Destination List Priority 2	❍	❍	▲
	Select Title	❍	❍	▲
	Update Delivery Server Destination List	❍	❍	▲
Send Settings	TWAIN Standby Time	❍	❍	▲
	File Type Priority	❍	❍	▲
	Compression (Black & White)	❍	❍	▲
	Compression (Gray Scale)	❍	❍	▲
	Print & Delete Scanner Journal	❍	❍	▲
	Print Scanner Journal	❍	❍	▲
	Delete Scanner Journal	❍	❍	▲
	E-mail Information Language	❍	❍	▲
	Store File Priority	❍	❍	▲
	Stored File E-mail Method	❍	❍	▲

Facsimile Features

Which functions can be used and specified depend on which administrators are set to **[On]** in **[Menu Protect]** in **[Facsimile Features]**. The default for **[Menu Protect]** is **[Off]**.

Tab	Names Settings	Menu Protect		
		Machine Administrator	Network Administrator	File Administrator
Gen. Settings / Adjust	Memory / Immed. Transmission Switch	▲	❍	❍
	Text Size Priority	▲	❍	❍
	Original Type Priority	▲	❍	❍
	Auto Image Density	▲	❍	❍
	Adjust Scan Density	▲	❍	❍
	Select Title	▲	❍	❍
	Change Initial Mode	▲	❍	❍
	Adjust Sound Volume	▲	❍	❍
	Program Fax Information	▲	❍	❍
	Scan End Reset	▲	❍	❍
	TX Stamp Priority	▲	❍	❍
	Line Priority Setting	▲	❍	❍
	Program Economy Time	▲	❍	❍
	On Hook Mode Release Time	▲	❍	❍
	Quick Operation Key	▲	❍	❍
Reception Settings	Authorized RX	▲	❍	❍
	Forwarding	▲	❍	❍
	RX File Print Qty	▲	❍	❍
	2 Sided Print	▲	❍	❍
	RX Reverse Printing	▲	❍	❍
	Paper Tray	▲	❍	❍
	Specify Tray for Lines	▲	❍	❍
	Checkered Mark	▲	❍	❍
	Center Mark	▲	❍	❍
	Print Reception Time	▲	❍	❍
	Switch Reception Mode	▲	❍	❍

Tab	Names Settings	Menu Protect		
		Machine Administrator	Network Administrator	File Administrator
E-mail Settings	Internet Fax Settings	▲	❍	❍
	Max. E-mail Size	❍	▲	❍
	SMTP RX File Delivery Settings	▲	❍	❍
IP-Fax Settings	Enable H.323	❍	▲	❍
	Enable SIP	❍	▲	❍
	H.323 Settings	❍	▲	❍
	SIP Settings	❍	▲	❍
	Program / Change / Delete Gateway	❍	▲	❍
Administrator Tools	Program / Change / Delete Standard Message	▲	❍	❍
	Store / Change / Delete Auto Document	▲	❍	❍
	Program / Change / Delete Scan Size	▲	❍	❍
	Print Journal	▲	❍	❍
	Transmission Page Count	▲	❍	❍
	Forwarding	▲	❍	❍
	Memory Lock RX	▲	❍	❍
	ECM	▲	❍	❍
	Parameter Setting	▲	❍	❍
	Program Special Sender	-	❍	❍
	Box Setting	-	❍	❍
	Transfer Report	▲	❍	❍
	Program Confidential ID	▲	❍	❍
	Program Polling ID	-	❍	❍
	Program Memory Lock ID	-	❍	❍
	Select Dial / Push Phone	-	❍	❍
	Folder Transfer Result Report	❍	▲	▲
	Reception File Setting	-	❍	❍
	Stored RX File User Setting	❍	❍	▲

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	❍	❍	▲
	Output: Copier	❍	❍	▲
	Output: Document Server	❍	❍	▲
	Output: Facsimile	❍	❍	▲
	Output: Printer	❍	❍	▲
Tray Paper Settings	Paper Tray Priority: Copier	❍	❍	▲
	Paper Tray Priority: Facsimile	❍	❍	▲
	Paper Tray Priority: Printer	❍	❍	▲
	Tray Paper Size: Tray 1-4	❍	❍	▲
	Paper Type: Bypass Tray	❍	❍	▲
	Paper Type: Tray 1-4	❍	❍	▲
	Cover Sheet Tray	❍	❍	▲
	Slip Sheet Tray	❍	❍	▲
	Printer Bypass Paper Size	❍	❍	▲

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.
Timer Settings		Auto Off Timer	❍	❍	▲
		Panel Off Timer	❍	❍	▲
		System Auto Reset Timer	❍	❍	▲
		Copier/ Document Server Auto Reset Timer	❍	❍	▲
		Facsimile Auto Reset Timer	❍	❍	▲
		Printer Auto Reset Timer	❍	❍	▲
		Scanner Auto Reset Timer	❍	❍	▲
		Set Date	❍	❍	▲
		Set Time	❍	❍	▲
		Auto Logout Timer	❍	❍	▲
Interface Settings	Network	IP Address [*1]	❍	❍	▲
		Gateway Address	❍	❍	▲
		DNS Configuration [*1]	❍	❍	▲
		DDNS Configuration	❍	❍	▲
		Domain Name [*1]	❍	❍	▲
		WINS Configuration [*1]	❍	❍	▲
		Effective Protocol	❍	❍	▲
		NCP Delivery Protocol	❍	❍	▲
		NW Frame Type	❍	❍	▲
		SMB Computer Name	❍	❍	▲
		SMB Work Group	❍	❍	▲
		Ethernet Speed	❍	❍	▲
		Ping Command	❍	❍	▲
		Permit SNMP V3 Communication	❍	❍	▲
		Permit SSL / TLS Communication	❍	❍	▲
		Host Name	❍	❍	▲
		Machine 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.
Interface Settings	Parallel Interface *8	Parallel Timing	○	○	▲
		Parallel Communication Speed	○	○	▲
		Selection Signal Status	○	○	▲
		Input Prime	○	○	▲
		Bidirectional Communication	○	○	▲
		Signal Control	○	○	▲
	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	○	○	▲
	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		○	○	▲

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.
File Transfer	Delivery Option *3	❍	❍	▲
	FAX RX File Transmission	❍	❍	▲
	SMTP Server	❍	❍	▲
	SMTP Authentication *4	❍	❍	▲
	POP before SMTP	❍	❍	▲
	Reception Protocol	❍	❍	▲
	POP3 / IMAP4 Settings	❍	❍	▲
	Administrator's E-mail Address	❍	❍	▲
	E-mail Communication Port	❍	❍	▲
	E-mail Reception Interval	❍	❍	▲
	Max. Reception E-mail Size	❍	❍	▲
	E-mail Storage in Server	❍	❍	▲
	Default User Name / Password (Send) *4	❍	❍	▲
	Program / Change / Delete E-mail Message	❍	▲	▲
	Program / Change / Delete Subject	❍	▲	▲
	Scanner Recall Interval Time	❍	❍	▲
	Number of Scanner Recalls	❍	❍	▲
	Fax E-mail Account	❍	❍	▲
	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	❍	❍	▲
	Extended Security	❍	❍	▲
	External Charge Unit Management	❍	❍	▲
	Display / Clear / Print Counter per User	❍	❍	▲
	Print Address Book: Destination List	▲	▲	▲
	Address Book Management	▲	▲	▲
	Address Book: Program / Change / Delete Group	▲	▲	▲
	Address Book: Program / Change / Delete Transfer Request	▲	▲	▲
	Address Book: Change Order	❍	❍	▲
	Address Book: Edit Title	❍	❍	▲
	Address Book: Select Title	❍	❍	▲
	Auto Delete File in Document Server	❍	❍	▲
	Delete All Files in Document Server	❍	❍	▲
	Capture Priority [*7]	❍	❍	▲
	Capture: Delete All Unsent Files [*7]	❍	❍	▲
	AOF (Always On)	❍	❍	▲
	Program / Change / Delete LDAP Server [*4]	❍	❍	▲
	Use LDAP Server	❍	❍	▲
	Firmware Version	❍	❍	▲
	Data Security for Copying	▲	▲	▲
	Transfer Log Setting	▲	▲	▲
	Auto Erase Memory Setting [*9]	❍	❍	▲
	Erase All Memory [*9]	❍	❍	▲

[*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 File Format Converter option must be installed.
*8 The IEEE 1284 interface board option must be installed.
*9 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	Device Name	❍	❍	▲
	Comment	❍	❍	▲
	Location	❍	❍	▲
	Spool Printing	❍	❍	▲
	Output Tray	❍	❍	▲
	Paper Tray Priority	❍	❍	▲
	Cover Sheet Tray	❍	❍	▲
	Slip Sheet Tray	❍	❍	▲
Paper	Paper Size	❍	❍	▲
	Paper Type	❍	❍	▲
	Apply Auto Paper Select	❍	❍	▲
	Copying Method in Duplex	❍	❍	▲
	Bypass Tray - Paper Size	❍	❍	▲
	Bypass Tray - Custom Paper Size	❍	❍	▲
	Bypass Tray - Paper Type	❍	❍	▲

Category	**Settings**	**Administrator authentication has not been specified.**	**Administrator authentication has been specified.**	
			"Available Settings" has been specified.	**"Available Settings" has not been specified.**
Date/Time	Set Date	❍	❍	▲
	Set Time	❍	❍	▲
	SNTP Server Address	❍	❍	▲
	SNTP Polling Interval	❍	❍	▲
	Time Zone	❍	❍	▲
Timer	Auto Off Timer	❍	❍	▲
	Panel Off Timer	❍	❍	▲
	System Auto Reset Timer	❍	❍	▲
	Copier/ Document Server Auto Reset Timer	❍	❍	▲
	Facsimile Auto Reset Timer	❍	❍	▲
	Scanner Auto Reset Timer	❍	❍	▲
	Printer Auto Reset Timer	❍	❍	▲
	Auto Logout Timer	❍	❍	▲
E-mail	Administrator E-mail Address	❍	❍	▲
	Reception Protocol	❍	❍	▲
	E-mail Reception Interval	❍	❍	▲
	Max. Reception E-mail Size	❍	❍	▲
	E-mail Storage in Server	❍	❍	▲
	SMTP Server Name	❍	❍	▲
	SMTP Port No.	❍	❍	▲
	SMTP Authentication	❍	❍	▲
	SMTP Auth. E-mail Address	❍	❍	▲
	SMTP Auth. User Name	❍	❍	-
	SMTP Auth. Password [*1]	❍	❍	-
	SMTP Auth. Encryption	❍	❍	▲
	POP before SMTP	❍	❍	▲
	POP E-mail Address	❍	❍	▲
	POP User Name	❍	❍	-

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	POP Password *1	❍	❍	-
	Timeout setting after POP Auth.	❍	❍	▲
	POP3/IMAP4 Server Name	❍	❍	▲
	POP3/IMAP4 Encryption	❍	❍	▲
	POP3 Reception Port No.	❍	❍	▲
	IMAP4 Reception Port No.	❍	❍	▲
	SMTP Reception Port No.	❍	❍	▲
	Fax E-mail Address	❍	❍	▲
	Receive FAX E-mail	❍	❍	-
	Fax E-mail User Name	❍	❍	-
	Fax E-mail Password *1	❍	❍	-
	E-mail Notification E-mail Address	❍	❍	▲
	Receive E-mail Notification	❍	❍	-
	E-mail Notification User Name	❍	❍	-
	E-mail Notification Password	❍	❍	-

Category	Settings	Administrator authentication has not been specified.	Administrator authentication has been specified.	
			“Available Settings” has been specified.	“Available Settings” has not been specified.
Auto E-mail Notification	Notification Message	❍	❍	▲
	Address List	❍	❍	▲
	Call Service	❍	❍	▲
	Out of Toner	❍	❍	▲
	Toner Almost Empty	❍	❍	▲
	Waste Toner Bottle is Full	❍	❍	▲
	Add Staple	❍	❍	▲
	Paper Misfeed	❍	❍	▲
	Cover Open	❍	❍	▲
	Out of Paper	❍	❍	▲
	Paper Tray Error	❍	❍	▲
	Output Tray Full	❍	❍	▲
	Unit Connection Error	❍	❍	▲
	Duplex Unit Error	❍	❍	▲
	Document Server Memory Full	❍	❍	▲
	Detailed Settings of Each Item	❍	❍	▲
On-demand E-mail Notification	Notification Subject	❍	❍	▲
	Notification Message	❍	❍	▲
	Restriction to System Config. Info.	❍	❍	▲
	Restriction to Network Config. Info.	❍	❍	▲
	Restriction to Printer Config. Info.	❍	❍	▲
	Restriction to Supply Info.	❍	❍	▲
	Restriction to Device Status Info.	❍	❍	▲
	Receivable E-mail Address/Domain Name	❍	❍	▲
	E-mail Language	❍	❍	▲

Category	Settings	Administrator authentication has not been specified.	Administrator authentication has been specified.	
			"Available Settings" has been specified.	"Available Settings" has not been specified.
File Transfer	SMB User Name	❍	❍	-
	SMB Password [*1]	❍	❍	-
	FTP User Name	❍	❍	-
	FTP Password [*1]	❍	❍	-
	NCP User Name	❍	❍	-
	NCP Password [*1]	❍	❍	-
User Authentication Management	User Authentication Management	❍	❍	▲
	User Code - Available Function	❍	❍	▲
	Basic Authentication - Printer Job Authentication	❍	❍	▲
	Windows Authentication - Printer Job Authentication	❍	❍	▲
	Windows Authentication - Domain Name	❍	❍	▲
	Windows Authentication - Group Settings for Windows Authentication	❍	❍	▲
	LDAP Authentication - Printer Job Authentication	❍	❍	▲
	LDAP Authentication - LDAP Authentication	❍	❍	▲
	LDAP Authentication - Login Name Attribute	❍	❍	▲
	LDAP Authentication - Unique Attribute	❍	❍	▲
	Integration Server Authentication - Printer Job Authentication	❍	❍	▲
	Integration Server Authentication - Integration Server Name	❍	❍	▲
	Integration Server Authentication - Authentication Type	❍	❍	▲
	Integration Server Authentication - Obtain URL	❍	❍	▲
	Integration Server Authentication - Domain Name	❍	❍	▲
	Integration Server Authentication - Group Settings for Integration Server Authentication	❍	❍	▲

[*1] You can only specify the password.

❖ Printer

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

Category	Settings	Menu Protect		
		Off	Level 1	Level 2
System	Print Error Report	❍	▲	▲
	Auto Continue	❍	▲	▲
	Memory Overflow	❍	▲	▲
	Job Separation	❍	▲	▲
	Auto Delete Temporary Print Jobs	❍	❍	▲
	Auto Delete Stored Print Jobs	❍	❍	▲
	Initial Print Job List	❍	❍	▲
	Memory Usage	❍	▲	▲
	Duplex	❍	▲	▲
	Copies	❍	▲	▲
	Blank Page Print	❍	▲	▲
	Printer Language	❍	▲	▲
	Edge Smoothing	❍	❍	▲
	Toner Saving	❍	❍	▲
	Sub Paper Size	❍	▲	▲
	Page Size	❍	❍	▲
	Letterhead Setting	❍	▲	▲
	Bypass Tray Setting Priority	❍	▲	▲
	Edge to Edge Print	❍	❍	▲
	Default Printer Language	❍	❍	▲
	Tray Switching	❍	❍	▲
Host Interface	I/O Buffer	❍	▲	▲
	I/O Timeout	❍	▲	▲

Category	Settings	Menu Protect		
		Off	Level 1	Level 2
PCL Settings	Orientation	❍	▲	▲
	Form Lines	❍	▲	▲
	Font Source	❍	▲	▲
	Font Number	❍	▲	▲
	Point Size	❍	▲	▲
	Font Pitch	❍	▲	▲
	Symbol Set	❍	▲	▲
	Courier Font	❍	▲	▲
	Extend A4 Width	❍	▲	▲
	Append CR to LF	❍	▲	▲
	Resolution	❍	▲	▲
PS Settings [*1]	Duplex	❍	▲	▲
	Blank Page Print	❍	▲	▲
	Data Format	❍	▲	▲
	Resolution	❍	▲	▲
PDF Settings [*1]	Resolution	❍	-	-
	PDF Temporary Password	❍	-	-
	PDF Fixed Password	❍	-	-
	PDF Group Password	❍	-	-

[*1] The PostScript 3 unit option must be installed.

❖ Fax

Functions that can be used and specified via Web Image Monitor depend on which administrators are set to **[On]** in **[Menu Protect]**, **[Facsimile Features]**.

Tab	Names Settings	Menu Protect		
		Machine Administrator	Network Administrator	File Administrator
General	Fax Information	-	❍	❍
	Reception Settings	-	❍	❍
	Transmission Settings	-	❍	❍
Administrator Tools	Program Confidential ID	-	❍	❍
	Program Polling ID	-	❍	❍
	ECM	-	❍	❍
	Memory Lock Reception	-	❍	❍
	Program Memory Lock ID	-	❍	❍
	Transfer Report	-	❍	❍
	Select Dial/Push Phone	-	❍	❍
E-mail Settings	Internet Fax Settings	-	❍	❍
	Maximum E-mail Size	❍	-	❍
	SMTP RX File Delivery Settings	-	❍	❍
IP-Fax Settings	Enable H.323	❍	-	❍
	Enable IP-Fax Gatekeeper	❍	-	❍
	Gatekeeper Address(Main)	❍	-	❍
	Gatekeeper Address(Sub)	❍	-	❍
	Own Fax No.	❍	-	❍
	Enable SIP	❍	-	❍
	Enable SIP Server	❍	-	❍
	SIP Server IP Address	❍	-	❍
	Proxy Server Addr. (Main)	❍	-	❍
	Proxy Server Address (Sub)	❍	-	❍
	Redirect Svr. Addr. (Main)	❍	-	❍
	Redirect Svr. Addr. (Sub)	❍	-	❍
	Registrar Address (Main)	❍	-	❍
	Registrar Address (Sub)	❍	-	❍
	SIP User Name	❍	-	❍

Tab	Names Settings	Menu Protect		
		Machine Administrator	Network Administrator	File Administrator
Gateway Settings	Prefix 1-5	❍	-	❍
	Select Protocol 1-5	❍	-	❍
	Gateway Address 1-5	❍	-	❍
Parameter Settings	Just Size Printing	-	❍	❍
	Combine 2 originals	-	❍	❍
	Indial	-	❍	❍
	Convert to PDF When Transferring to Folder	-	❍	❍
	Journal	-	❍	❍
	Immediate Transmission Result Report	-	❍	❍
	Communication Result Report	-	❍	❍
	Memory Storage Report	-	❍	❍
	Polling TX Clear Report	-	❍	❍
	Polling RX Result Report	-	❍	❍
	Polling RX Reserve Report	-	❍	❍
	Confidential File Report	-	❍	❍
	LAN-Fax Result Report	-	❍	❍
	Inclusion of part of image	-	❍	❍
	Error E-mail Notification	-	❍	❍
	Display Network Errors	-	❍	❍
	Journal Notification by E-mail	-	❍	❍
	Response to RX Notice Request	-	❍	❍
	Select Destination Type Priority	-	❍	❍

❖ 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	❍	❍	▲
Bluetooth [*3]	Operation Mode	❍	❍	▲
Parallel Interface [*4]	Parallel Timing	❍	❍	▲
	Parallel Communication Speed	❍	❍	▲
	Selection Signal Status	❍	❍	▲
	Input Prime	❍	❍	▲
	Bidirectional Communication	❍	❍	▲
USB	USB	❍	❍	▲

[*1] The IEEE802.11b interface unit option must be installed.
[*2] The IEEE1394 interface board option must be installed.
[*3] The Bluetooth interface unit option must be installed.
[*4] The IEEE 1284 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	❍	❍	▲

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.	❍	❍	▲
	Job Timeout	❍	❍	▲
	Frame Type	❍	❍	▲
	Print Server Protocol	❍	❍	▲
	NCP Delivery Protocol	❍	❍	▲
AppleTalk	AppleTalk	❍	❍	▲
	Printer Name	❍	❍	▲
	Zone Name	❍	❍	▲
SMB	SMB	❍	❍	▲
	Workgroup Name	❍	❍	▲
	Computer Name	❍	❍	▲
	Comment	❍	❍	▲
	Notify Print Completion	❍	❍	▲
Rendezvous	Rendezvous	❍	❍	▲
	Computer Name	❍	❍	▲
	Location	❍	❍	▲
	DIPRINT	❍	❍	▲
	LPR	❍	❍	▲
	IPP	❍	❍	▲

Functions That Require Options

The following functions require certain options and additional functions.

- Hard Disk overwrite erases function
  DataOverwriteSecurity unit
- Data security for copying function
  Copy Data Security Unit
- PDF Direct Print function
  PostScript unit

INDEX

MEMO

MEMO

Operating Instructions Security Reference

Printed in China
EN (USA)
AE (AE) B209-6707

B2096707

Notes for Security Administrators

This manual is intended to provide the security administrator with additional information about the security functions of this machine. Read this manual as well as Security Reference and Facsimile Reference<Advanced Features>.

Only the security administrator should have access to this manual and perform the operations it explains.

♦ Printing the Journal

When making authentication settings for users, to prevent personal information in transmission history being printed, set the Journal to not be printed.

Also, if more than 200 transmissions are made, transmissions shown in the Journal are overwritten each time a further transmission is made.

To prevent the Transmission History being overwritten, perform the following procedures:

- In the default settings for Fax, under "Administrator Settings", "Parameter Settings" (Switch 03, Bit 7), change the setting for automatically printing the Journal.
- In the default settings for Fax, under "Administrator Settings", "Parameter Settings" (Switch 21, Bit 4), set "Transmit Journal by E-mail" to "ON".

Reference:

Facsimile Reference<Advanced Features>

Printed in the Netherlands
GB ⒼⒷ B198-8554

B1988554