Notes for Administrator:

Using this Machine in a Network Environment Compliant with IEEE Std.2600.1™-2009

For safe and correct use, be sure to read the Safety Information in "About This Machine" 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.

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.

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.

TABLE OF CONTENTS

About This Booklet

This booklet describes operating environment compliance with the requirements of the Common Criteria for Information Technology Security Evaluation ("CC certification") and the configuration of the multifunction peripheral ("MFP") settings to meet the requirements. Be sure to read the booklet carefully and to understand its contents thoroughly. Note that regarding display and manual languages, CC certification has been obtained for English only in a network environment compliant with IEEE Std. 2600.1™-2009. The official name of IEEE Std. 2600.1™-2009 is 2600.1, Protection Profile for Hardcopy Devices, Operational Environment A(Version: 1.0, dated June 2009).

Administrator Manuals and User Manuals

The following manuals are intended for use by administrators (including the supervisor): "Network and System Settings Reference", "Security Reference", "About This Machine", and "Notes for Administrators: Using this Machine in a Network Environment Compliant with IEEE Std. 2600.1™-2009". To securely operate the machine, administrators must keep these manuals handy. All other manuals are for general users.

The person responsible for acquiring this machine must appoint competent personnel as the administrators, and instruct them to read the administrator manuals listed above.

Before Applying the Security Functions

Before applying any security functions, administrators must read and fully understand "Before Using the Security Functions" in Security Reference.

Checking Versions for CC Conformance

Administrators must use the following procedure to check the firmware, hardware, and manuals versions for CC conformance.

CC-conformant firmware and hardware versions are as follows:

Primary Classification	Secondary Classification	Version
Firmware	System/Copy	2.05
	Network Support	10.57
	Fax	02.00.00
	RemoteFax	01.00.00
	NetworkDocBox	1.04
	Web Support	1.02
	Web Uapl	1.01
	animation	1.00
	Scanner	01.04
	Printer	1.01
	PCL	1.07
	OptionPCL Font	1.02
	Data Erase Std	1.01x
	GWFCU3-23 (WW)	03.00.00
	Engine	1.02:02
	OpePanel	1.03
	LANG0	1.03
	LANG1	1.03
Hardware	Ic Key	01020700
	Ic Ctlr	03

You can check the firmware and hardware versions as follows:

1. **Press the [User Tools/Counter] key.**
2. **Log on as the administrator ("admin").**
3. **Press [System Settings].**
4. **Press [Administrator Tools].**

5. **Press [Firmware Version].**

The reference numbers of the CC-certified manuals and the model numbers of the machines covered by the manuals are as follows:

Identifying the model

- Mainly Europe

  "-67"

- Mainly North America

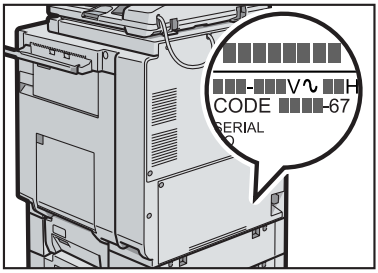
  "-57"

- Mainly Asia

  "-29"

In the following example, the machine's model number ends with "-67".

1. Check the label on the rear of the machine to identify the model.



2. Check whether the model number on the label ends with "-67".

Manual reference numbers for "-67" models

Paper Manuals

Manual Name	Reference Number
Safety Information for MP C300/MP C300SR/MP C400/MP C400SR/Aficio MP C300/ Aficio MP C300SR/Aficio MP C400/ Aficio MP C400SR	M026-7399
Note for Users	M026-7437
Quick Reference Copy Guide	M026-7411
Quick Reference Fax Guide	D483-8503
Quick Reference Printer Guide	M026-7428
Quick Reference Scanner Guide	M026-7433

Manual Name	Reference Number
CE Marking Traceability Information (For EU Countries Only)	AA00-0253A
Notes for Users	M026-7510
About the Software on the CD-ROM	M080-8547
Manuals for This Machine	D081-7602
Safety Information	A232-8561A
Notes for Users	D081-7676
SOFTWARE LICENSE AGREEMENT	D376-7905
Fax Option Type C400 (Machine Code: D483) Installation Procedure For Machine Code: M022/ M024/ M026/ M028 Copiers	D483-8610A
Operating Instructions Notes on Security Functions	M026-7441
Notes for Administrators: Using this Machine in a Network Environment Compliant with IEEE Std. 2600.1™-2009	M026-7440

Manual CD-ROMs

Manual Name	Reference Number
Manuals for Users Aficio MP C300/MP C300SR/MP C400/MP C400SR MP C300/MP C300SR/MP C400/MP C400SR A	M026-6906
Manuals for Administrators Security Reference Aficio MP C300/MP C300SR/MP C400/MP C400SR MP C300/MP C300SR/MP C400/MP C400SR	M026-6910

Manual reference numbers for "-57" models

Paper Manuals

Manual Name	Reference Number
C230/C230SR/C240/C240SR LD130C/LD130CSR/LD140C/LD140CSR Aficio MP C300/C300SR/C400/C400SR Operating Instructions About This Machine	M026-7401
Note for Users	M026-7438
Quick Reference Copy Guide	M026-7412
Quick Reference Printer Guide	M026-7429
Quick Reference Scanner Guide	M026-7434
C230/C230SR/C240/C240SR LD130C/LD130CSR/LD140C/LD140CSR Aficio MP C300/C300SR/C400/C400SR Operating Instructions Troubleshooting	M026-7415
Notes for Users	M026-7439
Notes for Users	D081-7678
Notes to users in the United States of America	D566-7091
About the Software on the CD-ROM	M080-8547
SOFTWARE LICENSE AGREEMENT	D376-7905
Quick Reference Fax Guide	D483-8504
Fax Option Type C400 (Machine Code: D483) Installation Procedure For Machine Code: M022/ M024/ M026/ M028 Copiers	D483-8610A
Operating Instructions Notes on Security Functions	M026-7443

Manual Name	Reference Number
Notes for Administrators: Using this Machine in a Network Environment Compliant with IEEE Std. 2600.1™-2009	M026-7442

Manual CD-ROMs

Manual Name	Reference Number
Manuals for Users Aficio MP C300/MP C300SR/MP C400/MP C400SR C230/C230SR/C240/C240SR LD130C/LD130CSR/LD140C/LD140CSR	M026-6908
Manuals for Administrators Aficio MP C300/MP C300SR/MP C400/MP C400SR C230/C230SR/C240/C240SR LD130C/LD130CSR/LD140C/LD140CSR	M026-6909

Manual reference numbers for "-29" models

Paper Manuals

Manual Name	Reference Number
MP C300/C300SR/C400/C400SR MP C300/C300SR/C400/C400SR Aficio MP C300/C300SR/C400/C400SR Operating Instructions About This Machine	M026-7403
Note for Users	M026-7438
Quick Reference Copy Guide	M026-7413
Quick Reference Printer Guide	M026-7429
Quick Reference Scanner Guide	M026-7435

Manual Name	Reference Number
MP C300/C300SR/C400/C400SR MP C300/C300SR/C400/C400SR Aficio MP C300/C300SR/C400/C400SR Operating Instructions Troubleshooting	M026-7417
Notes for Users	M026-7439
Notes for Users	D081-7678
User Information on Electrical & Electronic Equipment	D127-6601
About the Software on the CD-ROM	M080-8547
SOFTWARE LICENSE AGREEMENT	D376-7905
Quick Reference Fax Guide	D483-8505
Fax Option Type C400 (Machine Code: D483) Installation Procedure For Machine Code: M022/ M024/ M026/ M028 Copiers	D483-8610A
Operating Instructions Notes on Security Functions	M026-7443
Notes for Administrators: Using this Machine in a Network Environment Compliant with IEEE Std. 2600.1™-2009	M026-7442

Manual CD-ROMs

Manual Name	Reference Number
Manuals for Users Aficio MP C300/MP C300SR/MP C400/MP C400SR MP C300/MP C300SR/MP C400/MP C400SR	M026-6904
Manuals for Administrators Aficio MP C300/MP C300SR/MP C400/MP C400SR MP C300/MP C300SR/MP C400/MP C400SR	M026-6905

Note

- Because of modifications made after obtaining CC certification, the versions of the MFP firmware and hardware, and hence the reference number of the manuals, may differ from those of the CC-certified products.

After specifying the settings listed in "Settings" in this manual, the administrator must use the following procedure to check the log files and ROM version.

You can check that the FCU in use is a genuine product by checking that the entries in the log files and the ROM version match the following:

1. **Check that the machine is off.**
2. **Turn the machine on.**
3. **Check the details of the log files that were stored in this machine.**

   Check that the details for "Log Type", "Result", and "Module Name" in the recorded access log are as follows:

   Log Type: Firmware: Structure

   Result: Succeeded

   Module Name: G3

   For details about logs, see "Managing Log Files", Security Reference.
4. **Log on as the administrator ("admin").**
5. **Use the following procedure to check the fax parameter settings from the machine's control panel.**
   1. Press the [User Tools/Counter] key.
   2. Press [Facsimile Features].
   3. Press [Initial Settings].
   4. Press [Parameter Setting: Print List].
   5. Press the [Start] key.
   6. Check that the following ROM version matches the one shown in the printed list:

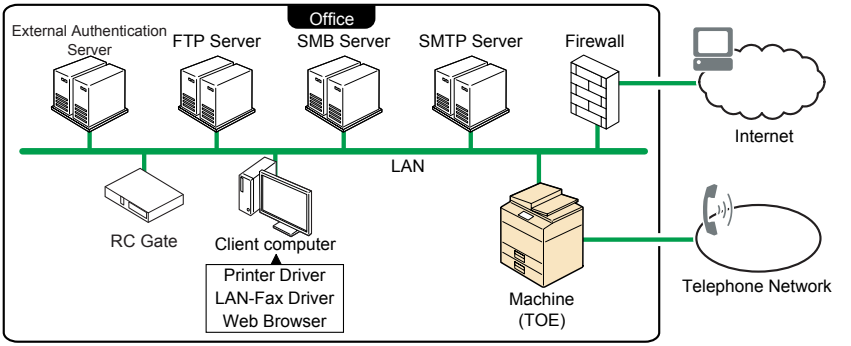
      [ROM Version]

      G3: 03.00.00(Validation Data: EB32)
6. **Log off.**

Example CC Conformant Environment

The following diagram outlines the CC evaluation test environment. This machine can be connected to other devices through a network, over a telephone line.

If this machine's LAN (local area network) is connected to an external network, be sure to use a firewall or some other means to block any unused ports. Check which ports are required and block any that are not.



Important

- The CC conformance standard stipulates that you request an authorized service representative to set up a CC-conformant environment.
- For faxing, use the public switched telephone network. IP-Fax and Internet Fax are not CC conformant. Do not use them.
- For print jobs and fax transmissions from the client computer, use IPP-SSL authentication.
- Windows Server 2008 and 2008 R2 are CC-certified external authentication servers.
- Use Windows Internet Explorer 6.0, 7.0, 8.0 or 9.0 as the Web browser.
- Use PCL6 Driver Ver. 1.0.0.0 or later and LAN-Fax Driver Ver. 1.64 or later. The version evaluated according to the CC certificate is: Ver. 1.0.0.0 for PCL6 Driver, and Ver. 1.64 for LAN-Fax Driver. You can download the drivers from the manufacturer's web site. Check the revision history to make sure there have been no security-related revisions to the CC conformant version of the driver.
- In the passwords of login users and administrators, use only the characters listed in "Characters You Can Use in Passwords in a CC Conformant Environment" in this manual.
- App2Me is not CC conformant. Do not use it.
- Embedded Software Architecture applications are not CC conformant. Do not use them.
- RC Gate is a device for @Remote Service. As the RC Gate, you can use any of the following products:

- Remote Communication Gate A
- Remote Communication Gate Type BN1
- Remote Communication Gate Type BM1

Settings

To maintain your environment's CC conformance, make changes to the machine's settings in accordance with the following conditions (Some settings may be factory-configured or pre-configured by the customer engineer.):

(Do not connect to a network in a normal operating environment until each item has been configured and a secure operating environment can be established.)

1. Changes to settings cannot be applied while the machine is in use, so before changing any settings, be sure to temporarily stop using the machine (procedure described below).
2. Before changing any settings, suspend the machine. To ensure CC conformance, be sure to specify the following settings according to this manual.

- Settings marked with an asterisk among the settings listed in "Settings to Specify Using the Control Panel" and "Specifying the group of users who can access stored received faxes"
- Settings marked with an asterisk in "Settings to Specify Using Web Image Monitor (1)" and "Settings to Specify Using Web Image Monitor (2)"
- Settings listed in "Settings to Specify Using telnet"

Note

- You do not have to stop using the machine to change passwords.
- Use the following procedure to temporarily stop the machine, change its settings, and then resume machine usage.
    1. Stop the machine's normal operations.
    2. Disconnect the machine from the normal network and connect it to the one accessible by administrators only.
    3. Change the settings.
    4. Make sure the system settings have been configured according to the instructions in this manual.
    5. Reconnect to the normal use network.
    6. Resume normal operations.

Settings to Specify Using the Control Panel

1. **Turn the machine on.**
2. **Press the [User Tools/Counter] key.**
3. **Log on as the administrator ("admin").**
4. **Press [System Settings].**
    1. Specify the following settings:

Tab	Item	Procedure
Interface Settings	Machine IPv4 Address	To specify the machine's static IPv4 address, press [Specify], and then enter the IPv4 address and subnet mask. To automatically obtain the IPv4 address from the DHCP server, press [Auto-Obtain (DHCP)].
Interface Settings	IPv4 Gateway Address	Enter the IPv4 gateway address. If you obtain the IPv4 address from the DHCP server, this setting does not have to be specified.
Interface Settings(*)	Effective Protocol	Set IPv4 to [Active]. Check that IPv6 is set to [Inactive].
Interface Settings	DNS Configuration	Specify this only if you are using a static DNS server. To specify a static DNS server, press [Specify], and then enter the server's IPv4 address in "DNS Server 1". If necessary, you can specify two more static DNS servers by entering their IPv4 addresses in "DNS Server 2" and "DNS Server 3". To obtain the DNS server's address automatically from the DHCP server, press [Auto-Obtain (DHCP)].
Interface Settings(*)	IEEE 802.1X Authentication for Ethernet	Set this to [Inactive].

Reference

- For details about specifying "Interface Settings", see "Interface Settings" in "System Settings", Network and System Settings Reference.

2. Specify the following settings:

Tab	Item	Procedure
Administrator Tools(*)	Administrator Authentication Management / User Management	Select [On], and then select [Administrator Tools] for "Available Settings".
Administrator Tools(*)	Administrator Authentication Management / Machine Management	Select [On], and then select [General Features], [Tray Paper Settings], [Timer Settings], [Interface Settings], [File Transfer], [Administrator Tools], and [Maintenance] for "Available Settings".
Administrator Tools(*)	Administrator Authentication Management / Network Management	Select [On], and then select [Interface Settings], [File Transfer], and [Administrator Tools] for "Available Settings".
Administrator Tools(*)	Administrator Authentication Management / File Management	Select [On], and then select [Administrator Tools] for "Available Settings".

Reference

- For details about specifying "Administrator Authentication Management", see "Enabling Administrator Authentication", Security Reference.

3. Specify the following settings:

Tab	Item	Procedure
Administrator Tools(*)	User Authentication Management	Select [Basic Auth.] or [Windows Auth.].

Reference

- For details about specifying "User Authentication Management", see "Enabling User Authentication", Security Reference.

4. Specify the following settings:

Tab	Item	Procedure
Administrator Tools(*)	Extended Security / Restrict Adding of User Destinations (Fax)	Set this to [On].
Administrator Tools(*)	Extended Security / Restrict Adding of User Destinations (Scanner)	Set this to [On].
Administrator Tools(*)	Extended Security / Restrict Use of Destinations (Fax)	Set this to [On].
Administrator Tools(*)	Extended Security / Restrict Use of Destinations (Scanner)	Set this to [On].
Administrator Tools(*)	Extended Security / Restrict Display of User Information	Set this to [On].
Administrator Tools(*)	Extended Security / Restrict Use of Simple Encryption	Set this to [Off].
Administrator Tools(*)	Extended Security / Transfer to Fax Receiver	Set this to [Prohibit].
Administrator Tools(*)	Extended Security / Authenticate Current Job	Set this to [Access Privilege].
Administrator Tools(*)	Extended Security / Password Policy	Press [Change], set "Complexity Setting" to [Level 1] or [Level 2], press [Change] on the right of "Minimum Character No.", and then set the number of characters to 8 or more. For example, to set the number of characters to 8, press the number key "8", and then "#".

Tab	Item	Procedure
Administrator Tools(*)	Extended Security / @Remote Service	Select [DoNotProh. (Optml)] if you use @Remote Service. Select [Prohibit] if you do not use. By selecting [DoNotProh. (Optml)], you can prevent @Remote Service from changing the machine settings. By selecting [Prohibit], you can stop @Remote Service.
Administrator Tools(*)	Extended Security / Update Firmware	Set this to [Prohibit].
Administrator Tools(*)	Extended Security / Change Firmware Structure	Set this to [Prohibit].

Reference

- For details about specifying "Extended Security", see "Specifying the Extended Security Functions", Security Reference.

5. Specify the following settings:

Tab	Item	Procedure
Administrator Tools(*)	Service Mode Lock	Set this to [On].
Administrator Tools(*)	Auto Delete File in Document Server	Set this to [On] or [Off].

Reference

- For details about specifying "Service Mode Lock", see "Limiting Machine Operations to Customers Only", Security Reference.
- For details about "Auto Delete File in Document Server", see "Administrator Tools" in "System Settings", Network and System Settings Reference.

6. Specify the following settings:

Tab	Item	Procedure
Administrator Tools(*)	Auto Erase Memory Setting	Select [On], and then select [NSA], [DoD], or [Random Numbers].

Reference

- For details about specifying "Auto Erase Memory Setting", see "Deleting Data on the Hard Disk", Security Reference.

7. Specify the following settings:

Tab	Item	Procedure
Administrator Tools(*)	Machine Data Encryption Settings	Ensure that the current data has been encrypted. If the data has been encrypted, the following message will appear: "The current data in the machine has been encrypted."

Reference

- For details about specifying "Machine Data Encryption Settings", see "Encrypting Data on the Hard Disk", Security Reference.

8. Specify the following settings:

Tab	Item	Procedure
Administrator Tools(*)	LDAP Search	Set this to [Off].
Administrator Tools(*)	Transfer Log Setting	Set this to [Off].

Reference

- For details about specifying "LDAP Search" and "Transfer Log Setting", see "Administrator Tools" in "System Settings", Network and System Settings Reference.

9. Specify the following settings:

Tab	Item	Procedure
File Transfer(*)	Delivery Option	Set this to [Off].

Reference

- For details about "Delivery Option", see "File Transfer" in "System Settings", Network and System Settings Reference.

5. Press [Exit].

A message confirming whether you want to log off may appear. If it does, press [Yes] to log off.

6. Log on again as the administrator.

7. **Press the [User Tools/Counter] key.**
8. **Press [Copier / Document Server Features].**

   Specify the following settings:

Tab	Item	Procedure
Administrator Tools(*)	Menu Protect	Set this to [Level 2].

Reference

- For details about specifying "Menu Protect", see "Menu Protect", Security Reference.

9. **Press [Exit].**
10. **Press [Printer Features].**

    Specify the following settings:

Tab	Item	Procedure
Maintenance(*)	Menu Protect	Set this to [Level 2].
System(*)	Auto Delete Temporary Print Jobs	Set this to [On] or [Off].
System(*)	Auto Delete Stored Print Jobs	Set this to [On] or [Off].

Reference

- For details about "Menu Protect", see "Maintenance" in "Printer Features", Printer Reference.
- For details about "Auto Delete Temporary Print Jobs" and "Auto Delete Stored Print Jobs", see "System" in "Printer Features", Printer Reference.

11. **Press [Exit].**
12. **Press [Scanner Features].**
    1. Specify the following settings:

Tab	Item	Procedure
General Settings(*)	Print & Delete Scanner Journal	Set this to [Do not Print: Delete Oldest] or [Do not Print: Disable Send].

Reference

- For details about specifying "Print & Delete Scanner Journal", see "General Settings" in "Scanner Features", Scanner Reference.

2. Specify the following settings:

Tab	Item	Procedure
Send Settings(*)	Stored File E-mail Method	Set this to [Send File].

Reference

- For details about specifying "Stored File E-mail Method", see "Send Settings" in "Scanner Features", Scanner Reference.

3. Specify the following settings:

Tab	Item	Procedure
Initial Settings(*)	Menu Protect	Set this to [Level 2].

Reference

- For details about specifying "Menu Protect", see "Initial Settings" in "Scanner Features", Scanner Reference.

13. Press [Exit].

14. Press [Facsimile Features].

1. Specify the following settings:

Tab	Item	Procedure
General Settings(*)	Box Setting	Set all items to [* Not Programmed].

Reference

- For details about specifying "Box Setting", see "General Settings" in "Facsimile Features", Facsimile Reference.

2. Specify the following settings:

Tab	Item	Procedure
Send Settings(*)	Backup File TX Setting	Set this to [Off]

Reference

- For details about specifying "Backup File TX Setting", see "Send Settings" in "Facsimile Features", Facsimile Reference.

3. Specify the following settings:

Tab	Item	Procedure
Reception Settings(*)	Forwarding	Set this to [Off].
Reception Settings(*)	Reception File Setting	Set this to [Store].
Reception Settings(*)	Memory Lock Reception	Set this to [Off].

Reference

- For details about specifying "Forwarding", see "Forwarding" in "Facsimile Features", Facsimile Reference.
- For details about specifying "Reception File Setting", see "Reception File Setting" in "Facsimile Features", Facsimile Reference.
- For details about specifying "Memory Lock Reception", see "Reception Settings" in "Facsimile Features", Facsimile Reference.

4. Specify the following settings:

Tab	Item	Procedure
Initial Settings(*)	Parameter Setting	Set "switch 10, bit 5" to [0]. This will prevent the printing of received faxes that are programmed to be stored.
Initial Settings(*)	Parameter Setting	Set "switch 40, bit 0" to [1]. If the machine's file storage device reaches its maximum capacity, the machine prints or deletes the stored fax document data. If this setting is enabled, the machine will not accept new fax document data. This setting keeps the received fax document data stored on the storage device, and those data will not be printed nor deleted.

Tab	Item	Procedure
Initial Settings(*)	Parameter Setting	Set "switch 10, bit 0" to [1]. Only users who are authorized by the administrator can access, from the control panel, received faxes that are stored.
Initial Settings(*)	Parameter Setting	Set "switch 03, bit 0" to [0]. This will prevent the automatic printing of the communication result report.
Initial Settings(*)	Parameter Setting	Set "switch 03, bit 2" to [0]. This will prevent automatic printing of the memory storage report.
Initial Settings(*)	Parameter Setting	Set "switch 04, bit 7" to [0]. If this is enabled, previews will not be included in the reports.

Reference

- For details about specifying "Parameter Settings", see "Parameter Settings" in "Facsimile Features", Facsimile Reference.

5. Specify the following settings:

Tab	Item	Procedure
Initial Settings(*)	Internet Fax Setting	Set this to [Off].
Initial Settings(*)	Menu Protect	Set this to [Level 2].
Initial Settings(*)	Folder Setting	Set this to [On].
Initial Settings(*)	E-mail Setting	Set this to [Off].

Reference

- For details about specifying "Internet Fax Setting", "Menu Protect", "Folder Setting", and "E-mail Setting", see "Initial Settings" in "Facsimile Features", Facsimile Reference.

15. Press [Exit] twice.

If the following message appears, press [Exit]:

"You do not have the privileges to use this function."

16. **Log off.**
17. **Turn off the main power.**

Settings to Specify Using Web Image Monitor (1)

1. **Connect the machine and a computer supporting the machine's Web browser to the network that can be accessed by the administrator only.**
2. **Turn the machine on.**
3. **Launch the Web browser on the computer, and then access "http://(machine's IP address)/".**
4. **Log on as the administrator ("admin").**
5. **Click [Configuration].**
6. **Use the following procedure to configure the administrator's login password.**
    1. Click [Program/Change Administrator] in "Device Settings", and then click [Change] in the "Login Password" field in "Administrator 1".
    2. Enter the changed password in "New Password" and "Confirm Password", and then click [OK].
    3. Click [OK].

       An Authentication Error message appears.
    4. Click [OK].
7. **Log on as the supervisor ("supervisor").**
8. **Click [Configuration].**
9. **Use the following procedure to configure the supervisor's login password.**
    1. Click [Program/Change Administrator] in "Device Settings", and then click [Change] in the "Login Password" field in "Supervisor".
    2. Enter the changed password in "New Password" and "Confirm Password", and then click [OK].
    3. Click [OK].

       An Authentication Error message appears.
    4. Click [OK].
10. **Log on as the administrator ("admin").**
11. **Click [Configuration].**
12. **Use the following procedure to specify the user authentication. (*)**

    Basic Authentication

        1. Click [User Authentication Management] in "Device Settings".

2. Make sure [User Authentication Management] is set to "Basic Authentication".
3. Set "Printer Job Authentication" to [Entire].
4. Configure [Available Functions] to match the operating environment.
5. Click [OK].

Windows Authentication

1. Click [Program/Change Realm] in "Device Settings".
2. Enter the [Realm Name], [KDC Server Name], and [Domain Name] in [Realm 1].
3. Click [OK].
4. Click [User Authentication Management] in "Device Settings".
5. Make sure [User Authentication Management] is set to [Windows Authentication].
6. Set "Printer Job Authentication" to [Entire].
7. Set "SSL" in "Windows Authentication Settings" to [On].
8. Set "Kerberos Authentication" in "Windows Authentication Settings" to [On].
9. Set [Realm Name] in "Windows Authentication Settings" that is specified in step 2.
10. Uncheck all [Available Functions] in [*Default Group] in [Group Settings for Windows Authentication]. Do not use global groups.

    You can specify which functions are available to users only after completing the user registration.
11. Click [OK].

Reference

- For details about specifying the Realm, see "Programming the Realm" in "System Settings", Network and System Settings Reference.
- For details about specifying which functions are available to users, see "Specifying Which Functions are Available", Security Reference.

13. Use the following procedure to specify the date and time.

1. Click [Date/Time] in "Device Settings".
2. Specify "Set Date", and then check "Apply".
3. Specify "Set Time", and then check "Apply".
4. Specify "Time Zone". (*)
5. Click [OK].

   A confirmation message appears.
6. Click [OK].

   Wait a while for the machine to reset itself.
7. Click [OK].

8. Log on as the administrator ("admin").
9. Click [Configuration].

14. Use the following procedure to specify the timer settings.

1. Click [Timer] in "Device Settings".
2. Specify "Auto Logout Timer". (*)

   Select [On].

   Set the range for the timer between 60-999 seconds.
3. Click [OK].

15. Use the following procedure to configure the settings for job and access log collection. (*)

1. Click [Logs] in "Device Settings".
2. Set "Collect Job Logs" in "Job Log" to [Active].
3. Set "Job Log Collect Level" to [Level 1].
4. Set "Collect Access Logs" in "Access Log" to [Active].
5. Set "Access Log Collect Level" to [Level 2].
6. Click [OK].

   Wait a while for the machine to reset itself.
7. Click [OK].

   An Authentication Error message appears.
8. Click [OK].
9. Log on as the administrator ("admin").
10. Click [Configuration].

16. Use the following procedure to configure the settings for sending and receiving e-mails.

1. Click [E-mail] in "Device Settings".
2. Enter the administrator's e-mail address in "Administrator E-mail Address".
3. Enter the SMTP server name (or IP address) in "SMTP Server Name".
4. Click [OK].

17. Use the following procedure to install the device certificate.

There are three types of device certificates: certificates issued by the certificate authority, self-signed certificates, and intermediate certificates issued by the certificate authority. The procedure is different according to the type of the certificate.

Installing the Certificate Issued by the Certificate Authority

1) Request the device certificate from the certificate authority according to the following procedure:

1. Click [Device Certificate] in "Security".

2. Select the certificate you want to install from the certificate list.

   As the certificate for "SSL/TLS", you can select [Certificate1] only.

   The certificate for "S/MIME" or "IPsec" can be selected. However, if the certificate is also used for "SSL/TLS", select [Certificate1].

3. Click [Request] at the top of the list.

   To select a certificate other than "Certificate1" (Certificate 2, 3, or 4) in "S/MIME" and "IPsec", you need to specify [Request] for the selected certificate.

4. For the certificate required for "S/MIME", enter the administrator's e-mail address in "E-mail Address".

5. Select "sha1WithRSA-1024" or "sha1WithRSA-2048" in "Algorithm Signature".

   If required, change or specify other settings.

6. Click [OK].

   Wait a while for the machine to reset itself.

7. Click [OK].

   The machine requests for the certificate. Wait a while for the machine to become usable.

8. Click [Details]( ) next to the number of requested certificate.

9. Using the text displayed in the "Text for Requested Certificate" field, request the certificate authority to issue the certificate.

   (The text displayed in the "Text for Requested Certificate" field includes the public key and the text entered on the "Request" page.)

   For details about the certificate issuance, ask the certificate authority.

10. Click [Back].

2) Install the certificate issued by the certificate authority in accordance with the following procedure:

1. Select the certificate you want to install from the certificate list, and then click [Install].
2. In the "Enter Device Certificate" box, enter the text of the device certificate issued by the certificate authority.
3. Click [OK].

   Wait a while for the machine to reset itself.

4. Click [OK].

3) Select the installed certificate in accordance with the following procedure:

1. In "S/MIME", select the certificate you selected in step 1). 2. in "Installing the Certificate Issued by the Certificate Authority"
2. In "IPsec", select the certificate you selected in step 1). 2. in "Installing the Certificate Issued by the Certificate Authority"

3. Click [OK].

   Wait a while for the machine to reset itself.

4. Click [OK].

Creating the Self-Signed Certificate

1) Create the self-signed certificate according to the following procedure:

1. Click [Device Certificate] in "Security".
2. Select the certificate you want to install from certificate list.

   As the certificate for "SSL/TLS", you can select [Certificate1] only.

   The certificate for "S/MIME" can be selected. However, if the certificate is also used for "SSL/TLS", select [Certificate1].

3. Click [Create] at the top of the list.

   To select a certificate other than "Certificate1" (Certificate 2, 3, or 4), you need to specify [Create] for the selected certificate.

4. For the certificate required for "S/MIME", enter the administrator's email address in "E-mail Address".
5. Select "sha1WithRSA-1024" or "sha1WithRSA-2048" in "Algorithm Signature".

   If required, change or specify other settings.

6. Click [OK].

   The machine creates the certificate. Wait a while for the machine to become usable.

2) Select the installed certificate in accordance with the following procedure:

1. In "S/MIME", select the certificate you selected in step 1). 2. of "Creating the Self-Signed Certificate".
2. Select [Certificate1] for "IPsec".
3. Click [OK].

   Wait a while for the machine to reset itself.

4. Click [OK].

Installing the Intermediate Certificate Issued by the Intermediate Certificate Authority

1) Request the intermediate certificate and device certificate from the root certificate authority and intermediate certificate authority according to the following procedure:

1. Click [Device Certificate] in "Security".
2. Select the certificate you want to install from the certificate list.

   As the certificate for "SSL/TLS", you can select [Certificate1] only.

   The certificate for "S/MIME" can be selected. However, if the certificate is also used for "SSL/TLS", select [Certificate1].

3. Click [Request] at the top of the list.

To select a certificate other than "Certificate1" (Certificate 2, 3, or 4) in "S/MIME", you need to specify [Request] for the selected certificate.

4. For the certificate required for "S/MIME", enter the administrator's email address in "E-mail Address".
5. Select "sha1WithRSA-1024" or "sha1WithRSA-2048" in "Algorithm Signature".

   If required, change or specify other settings.
6. Click [OK].

   Wait a while for the machine to reset itself.
7. Click [OK].

   The machine requests for the certificate. Wait a while for the machine to become usable.
8. Click [Details]( ) next to the number of requested certificate.
9. Using the text displayed in the "Text for Requested Certificate" field, request the intermediate certificate authority to issue the certificate.

   The intermediate certificate requires the root certificate authority's signature.

   (The text displayed in the "Text for Requested Certificate" field includes the public key and the text entered on the "Request" page.)

   For details about the certificate issuance, ask the certificate authority.
10. Click [Back].

2) Install the device certificate issued by the intermediate certificate authority in accordance with the following procedure:

1. Select the certificate you want to install from the certificate list, and then click [Install].
2. In the "Enter Device Certificate" box, enter the text of the device certificate issued by the intermediate certificate authority.
3. Click [OK].

   Wait a while for the machine to reset itself.
4. Click [OK].
5. Select the intermediate certificate you want to install from the certificate list, and then click [Install Intermediate Certificate].
6. In the "Enter Intermediate Certificate" box, enter the text of the intermediate certificate issued by the root certificate authority.
7. Click [OK].

   Wait a while for the machine to reset itself.
8. Click [OK].

3) Select the installed certificate in accordance with the following procedure:

1. In "S/MIME", select the certificate you selected in step 1). 2. in "Installing the Intermediate Certificate issued by the Intermediate Certificate Authority"
2. Click [OK].

   Wait a while for the machine to reset itself.
3. Click [OK].

18. Use the following procedure to specify the network security level. (*)

1. Click [Network Security] in "Security".
2. Set "Security Level" to [Level 2].
3. Click [OK].

   Wait a while for the machine to reset itself.

   Click [OK].
4. Click [Network Security] in "Security".
5. Select all check boxes in [AES] and [3DES] in [Encryption Strength Setting], select the [128bit] check box in [RC4], and uncheck all other boxes.
6. Set "IPv6" in "TCP/IP" to [Inactive].
7. Set "IPv4" in "Port 80" in "HTTP" to [Close].

   If you do this, "IPv4" in "Port 80" in "IPP" is also automatically set to [Close].
8. Set "IPv4" in "FTP" to [Inactive].
9. Set "IPv4" in "sftp" to [Inactive].
10. Set "IPv4" in "ssh" to [Inactive].
11. Set "IPv4" in "TELNET" to [Active].
12. Set "SNMP" in "SNMP" to [Inactive].
13. Click [OK].

    If "Security Level" is set to [Level 2], some functions become unavailable.

    For details about the available functions under each security level, see "Status of Functions under Each Network Security Level" described under "Specifying Network Security Level" and "Enabling and Disabling Protocols" in Security Reference.

    For details about the functions that become unavailable when "FTP" and "SNMP Function" are set to [Inactive] under each security level, see "Enabling and Disabling Protocols" in Security Reference.

    Wait a while for the machine to reset itself.
14. Click [OK].
15. Click [Network Security] in "Security".
16. For the SSL/TLS version settings, set "SSL2.0" to [Inactive], and set "SSL3.0" and "TLS" to [Active] respectively.

17. Click [OK].

    Wait a while for the machine to reset itself.

18. Click [OK].

19. Use the following procedure to configure the user lockout setting. (*)

1. Click [User Lockout Policy] in "Security".
2. Set "Lockout" to [Active].
3. Set "Number of Attempts before Lockout" to "5" or less.
4. Set "Lockout Release Timer" to [Active].
5. Enter a range of 1-9999 minutes in [Lock Out User for].
6. Click [OK].

20. Use the following procedure to configure the settings for IPsec communication. (*)

1. Click [IPsec] in "Security".
2. Select [Inactive] from "Encryption Key Manual Settings:" in the "IPsec" area.
3. Click [Edit] in "Encryption Key Auto Exchange Settings".
4. In "Encryption Key Auto Exchange Settings" in "Settings 1", specify the following settings:
   - Set "Address Type" to "IPv4".
   - Enter the machine's IP address in the "Local Address" field.
   - Enter the connected server's IP address in the "Remote Address" field.
   - Set "Security Level" to [Authentication and High Level Encryption].
   - Set "Authentication Method" in "Security Details" to [PSK] or [Certificate].

     (If you set "Authentication Method" to "Certificate", "Security Level" is automatically set to [User Settings].)

   If you selected [PSK] in [Authentication Method] in [Security Details].

   - Click [Change] next to "PSK Text".
   - Enter the PSK in the "PSK Text" field.
   - Enter the PSK again in the "Confirm PSK Text" field.

     (Do not forget the PSK; you will need it to configure the server settings when using Scan to Folder.)

   - Click [OK].
   - Click [OK].

   If you selected [Certificate] in [Authentication Method] in [Security Details].

   - Click [OK].

   To specify this setting differently according to conditions, specify the setting under each of the settings.

5. Set "IPsec:" in "IPsec" to [Active].
6. Select [Active] or [Inactive] in "Exclude HTTPS Communication:".
7. Click [OK].

   Wait a while for the machine to reset itself.
8. Click [OK].

21. Use the following procedure to configure the settings for S/MIME. (*)

1. Click [S/MIME] in "Security".
2. Set "Encryption Algorithm:" in "Encryption" to [3DES-168 bit].
3. Set "Digest Algorithm" in "Signature" to [SHA1].
4. Set "When Sending E-mail by Scanner" in "Signature" to [Use Signatures].
5. Set "When Transferring by Fax" in "Signature" to [Use Signatures].
6. Set "When Transferring Files Stored in Document Server (Utility)" in "Signature" to [Use Signatures].
7. Click [OK].

22. Use the following procedure to specify the IP-Fax settings. (*)

1. Click [IP-Fax Settings] in "Fax".
2. Set "Enable H.323" in "H.323" to [Off].
3. Set "Enable SIP" in "SIP" to [Off].
4. Click [OK].
5. Click [Parameter Settings] in "Fax".
6. Set "LAN-Fax Result Report" in "Automatic Printing Report" to [Off].
7. Click [OK].

23. Use the following procedure to specify the virtual printer settings. (*)

1. Click [Basic Settings] in "Printer".
2. Set "Virtual Printer" in "System" to [Inactive].
3. Click [OK].

24. Use the following procedure to specify the machine interface settings. (*)

1. Click [Interface Settings] in "Interface".
2. Set "USB" in "USB" to [Inactive].
3. Set "PictBridge" in "PictBridge" to [Inactive].
4. Click [OK].

   Wait a while for the machine to reset itself.
5. Click [OK].

25. **Log off, and then quit Web Image Monitor.**
26. **Turn off the main power.**

Settings to Specify Using telnet

1. **Turn the machine on.**
2. **Use the IP address or the host name of the machine to start telnet.**

   ```
   % telnet IP_address
   ```
3. **Log on as the administrator ("admin").**
4. **Enter the following command, and then press the [Enter] key.**

   ```
   msh> set rfu down
   ```
5. **Enter the following command, and then press the [Enter] key.**

   ```
   msh> logout
   ```

   A message asking whether or not to store the changed settings appears.
6. **Enter "yes", and then press the [Enter] key.**

   Reference

   - For details about specifying settings via telnet, see "Remote Maintenance Using telnet" in " Monitoring and Configuring the Machine", Network and System Settings Reference.
7. **Turn off the main power.**

Settings to Specify Using Web Image Monitor (2)

1. **Turn the machine on.**
2. **Launch the Web browser on the computer, and then access "https://(machine's IP address)/".**

   The message "There is a problem with this website's security certificate." may appear. If this happens, click "Continue to this website (not recommended).".
3. **Log on as the administrator ("admin").**
4. **Use the following procedure to specify the telnet setting. (*)**
   1. Click [Configuration].
   2. Click [Network Security] in "Security".
   3. Set "IPv4" in "TELNET" to [Inactive].
   4. Click [OK].

      Wait a while for the machine to reset itself.

5. Click [OK].

5. Log off, and then quit Web Image Monitor.

6. Turn off the main power.

Specifying the group of users who can access stored received faxes

The administrator must first register the user group that can manage received faxes that will be stored in the address book.

For details about registering user groups in the address book, see "Registering Names to a Group" in "Registering Addresses and Users for Facsimile/Scanner Functions", Network and System Settings Reference.

For details about specifying the group of users who can access received faxes that are stored, see "Stored Reception File User Setting" in "Facsimile Features", Facsimile Reference. The steps the administrator needs to take are as follows:

1. Turn the machine on.
2. Press the [User Tools/Counter] key.
3. Log on as the administrator ("admin").
4. Press [Facsimile Features].
5. Press [Reception Settings].
6. Press [Stored Reception File User Setting].
7. Press [On]. (*)
8. Press the Destination key of the group you wish to specify, and then press [OK].
9. Check the selected group, and then press [OK].
10. Press [Exit].
11. Log off.
12. Turn off the main power.
13. Disconnect the machine from the network only the administrators can access, and then connect it to the network that general users can access.

Notes for Setting Up and Operation

- To reconfigure the network encryption methods (SSL, IPsec, S/MIME), you must temporarily stop using the machine. You can make encryption settings only when the machine is idle.
- Before reconfiguring the device certificate or changing the e-mail address for the device certificate, temporarily stop the machine. If the device certificate is reconfigured, connect to the machine via Web Image Monitor and check that a lock icon appears in the Web browser's status field and that no error messages related to the device certificate appear.
- Do not register a user name for the MFP administrator if it is identical with the one that is registered in the Windows authentication server.
- When using Scan to Folder, make sure IPsec is enabled.

  As for the machine's IPsec specifications, self-signed certificates from the machine and intermediate certificates from the certificate authority cannot be used. Therefore, if you are using certificates, be sure to use certificates issued by the certificate authority.

  The Scan to Folder destination (FTP or SMB server) must be registered in the Address Book by the administrator. To register destinations in the address book, click [Change] in "Access Privileges" in "Protect Destination" in "Protection", and then select [Read-only] for users who are allowed to send files by Scan to Folder to those destinations.

  Specify IPsec for the relevant server.
- When registering, changing, or deleting Scan to Folder destinations, you must temporarily stop using the machine.

  Reference

  - For details about Scan to Folder, see "Sending Scan Files to Folders", Scanner Reference.
- Before using the machine, either create a new encryption key for encrypting the stored data or obtain one from your service representative.
- When sending scan files by e-mail, enable the S/MIME encryption setting to prevent data leakage.

  The administrator must register the e-mail destinations in the address book.

  When you register an e-mail destination in the address book, be sure to install the user certificate and set the encryption setting to [Encrypt All]. When you display addresses to send an e-mail, a icon appears next to destinations for which [Encrypt All] has been set.

  "Encryption", "User Certificate", and "E-mail Address" must be specified by the administrator using Web Image Monitor.

  Reference

  - For details about installing the user certificate, see "E-mail Encryption", Security Reference.
- The administrator is required to manage the expiration of certificates and renew the certificates before they expire.

- The administrator is required to check that the issuer of the certificate is valid.
- To manage the users who can access received fax documents, register the users to a group or delete them from a group using the "Stored Reception File User Setting". To create a new group, or register or delete users, use the Address Book. Do not modify groups if they were created using the Address Book and registered using the "Stored Reception File User Setting".
- When you configure "Program Special Sender" in the fax mode, do not specify "Forwarding per Sender" or "Memory Lock RX per Sender" before registering or changing special senders.
- The file creator (owner) has the authority to grant [Full Control] privileges to other users for stored documents in the Document Server. However, administrators should tell users that [Full Control] privileges are meant only for the file creator (owner).
- A third party may steal or read paper documents printed by this machine. Instruct users to collect printed copies immediately.
- If you use Windows authentication in an environment that has CC conformance, configure a password that has eight or more characters. Two or more types of characters (from among lower and upper case characters, numbers, and symbols) must be used for the password. Also, you need to apply a lockout setting so that a user will be locked out after five or less failed login attempts.
- When using Windows authentication, the user login is case sensitive. You will not be able to use the machine if you make a mistake.
- When using Windows authentication, the login name is case sensitive. If you make a mistake, the user's login name will be added to the address book. You should delete the added user.
- To install the LAN-Fax driver, enter the IP address as follows (also described in "Using the SmartDeviceMonitor for Client port" in "Installing Individual Applications" in "Fax via Computer", Facsimile Reference):

  https://(machine’s IP address)/printer
- To install the printer driver, enter the IP address as follows (also described in "Using the IPP Port" in "Installing the Printer Driver for the Selected Port" in " Preparing the Machine", Printer Reference):

  https://(machine's IP address)/printer
- Do not unlock the setting in [Service Mode Lock].
- Do not access other Web sites when using Web Image Monitor. Also, be sure to logout after you have finished using Web Image Monitor. Instruct users not to access other Web sites when they are using Web Image Monitor, and to be sure to logout when they have finished.
- To prevent incorrect timestamps from being recorded in the audit log, ensure that the External Authentication Server or File Server that connects to the MFP is synchronized with the MFP.
- Address Book restoration is not CC conformant. Do not use it.
- Use of the media slot is not CC-certified, so the customer engineer has configured settings to prevent the slot from being used.

Security Functions Covered by CC Certification

Conformance with CC certification requires enforcement of the following security functions:

For details about 1 to 4, see "Security Measures Provided by this Machine" in Security Reference.

1. Using Authentication and Managing Users
    - Enabling Authentication

      Use basic authentication or Windows Kerberos authentication.
    - Specifying Which Functions are Available

      "Auto Logout Timer" is effective only for a user who logs in from the machine's control panel. Users who log in via Web Image Monitor are automatically logged out after 30 minutes of inactivity.
2. Ensuring Information Security
    - Protecting Stored Files from Unauthorized Access
    - Protecting Stored Files from Theft
    - Preventing Data Leaks Due to Unauthorized Transmission
    - Using S/MIME to Protect E-mail Transmission
    - Managing Log Files

      This function is for detecting unauthorized use of the machine and checking that stored data has been encrypted and the transmission route protected.

      Obtain log files by downloading them via Web Image Monitor.
    - Encrypting Data on the Hard Disk
    - Overwriting the Data on the Hard Disk
3. Limiting and Controlling Access
    - Preventing Modification or Deletion of Stored Data

      Modification of stored data has not been rated for CC conformance.
    - Preventing Modification of Machine Settings

    You can register up to four administrators. When registering an administrator, assign all administrator roles (user administrator, machine administrator, network administrator, and file administrator) to each administrator.
    - Limiting Available Functions
4. Enhanced Network Security
    - Safer Communication Using SSL and IPsec

      Use SSL and IPsec for encrypted data communication.

      Using IPsec for Scan to Folder with FTP or SMB is CC conformant.

5. Other Security Functions
    - Service Mode Lock

      Use the machine with [Service Mode Lock] set to [On].
6. Telephone Access Authorization

   Prevention of unauthorized access via fax telephone line. If a protocol error occurs after a fax access is confirmed, the line will be disconnected in order to prevent external interference or malicious access attempts.
7. Firmware Verification at Power On

   To ensure the firmware is authentic, a verification check is automatically performed whenever the machine's main power is turned on. The machine becomes usable only if the verification check finds the firmware to be authentic.

   If the verification check does not find the firmware to be authentic, a service call message will appear on the control panel display.

   Also at power on, a check is automatically performed to verify the HDD encryption function is operating properly and the HDD encryption key is correct. If the HDD encryption function is not operating properly or the key is incorrect, a service call message will appear on the control panel display. If a service call message is displayed, contact your service representative.

   The function "Firmware Verification at Power On" does not include checking that the FCU in use is a genuine product. To check that the FCU in use is a genuine product, perform the procedure in "Checking Versions for CC Conformance".

Note

- The following message might also be displayed: "SD Card authentication has failed.". If it is, contact your service representative.
- To maintain usability even in the event of hard disk error, this machine is designed to automatically recover from errors whenever possible. Note however that following recovery, user authentication might fail, even if the correct password is entered. If this happens, contact your service representative.

Characters You Can Use in Passwords in a CC Conformant Environment

In a CC conformant environment, passwords can contain the following characters:

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

Log File Management

For details about logs, see "Managing Log Files", Security Reference.

Note

- The administrator is required to properly manage the log information downloaded on the computer, so that unauthorized users may not view, delete, or modify the downloaded log information.

Auditable events specified in the Security Target (ST) for CC certification correspond as follows to items in "Logs that can be collected" in "Logs That Can Be Managed Using Web Image Monitor" in Security Reference:

ST Auditable Events	Log Item	Log Type Attribute
Start-up of the Audit Function (TOE start-up event)	Firmware: Structure	Firmware: Structure
Success and failure of login operations (Login attempts from RC Gate are excluded)	Login	Login If an attempt to log in succeeds, "Succeeded" appears as the "Result" attribute of the log data. If an attempt to log in fails, "Failed" appears as the "Result" attribute of the log data.
Success and failure of login operations from RC Gate communication interface	Collect Encrypted Communication Logs	Collect Encrypted Communication Logs If an attempt to log in succeeds, "Succeeded" appears as the "Result" attribute of the log data. If an attempt to log in fails, "Failed" appears as the "Result" attribute of the log data.
New creation, modification, and deletion of the login user name of normal user by MFP administrator when the Basic Authentication is used	Address Book Change	Address Book Change
Modification of login user name of supervisor by supervisor	Administrator Change	Administrator Change

ST Auditable Events	Log Item	Log Type Attribute
New creation of login user name of MFP administrator by MFP administrator	Administrator Change	Administrator Change
Modification of own login user name by MFP administrator	Administrator Change	Administrator Change
New creation and modification of login password of normal user by MFP administrator when the Basic Authentication is used	Password Change	Password Change
Modification of own login password by normal user when the Basic Authentication is used	Password Change	Password Change
Modification of login password of supervisor by supervisor	Password Change	Password Change
Modification of login password of MFP administrator by supervisor	Password Change	Password Change
New creation of login password of MFP administrator by MFP administrator	Password Change	Password Change
Modification of own login password by MFP administrator	Password Change	Password Change
Modification of document user list by MFP administrator	File Access Privilege Change	File Access Privilege Change
Modification of document user list by the normal user who stored the document	File Access Privilege Change	File Access Privilege Change
Modification of available function list by MFP administrator	Address Book Change	Address Book Change
Modification of date and time by MFP administrator	Date/Time Change	Date/Time Change

ST Auditable Events	Log Item	Log Type Attribute
Deletion of audit logs by MFP administrator	All Logs Deletion	All Logs Deletion
New creation of HDD encryption key by MFP administrator	Machine Data Encryption Key Change	Machine Data Encryption Key Change This appears together with "Finish Updating Machine Data Encryption Key" appearing as the "Machine Data Encryption Key Operation" attribute and "Encryption Key for Hard Disk" appearing as the "Machine Data Encryption Key Type" attribute of the log data.
New creation, modification, and deletion of S/MIME user information by MFP administrator	Address Book Change	Address Book Change
New creation, modification and deletion of destination information for folder transmission by MFP administrator	Address Book Change	Address Book Change
Modification of users for stored and received documents by MFP administrator	Address Book Change	Address Book Change
Date settings (year/month/day), time settings (hour/minute)	Date/Time Change	Date/Time Change
Termination of session by auto logout	Logout	Logout "By Auto Logout" appears as the "Logout Mode" attribute of the log data.
Web Function communication	Collect Encrypted Communication Logs	Collect Encrypted Communication Logs
Folder transmission	Scanner: Sending	Scanner: Sending

ST Auditable Events	Log Item	Log Type Attribute
E-mail transmission of attachments	Scanner: Sending	Scanner: Sending
Printing via networks	Printer: Printing	Printer: Printing
LAN Fax via networks	Fax: LAN-Fax Sending	Fax: LAN-Fax Sending
Storing document data	File Storing	File Storing
Reading document data (print)	Stored File Printing	Stored File Printing
	Fax: Stored File Printing	Fax: Stored File Printing
	Printer: Stored File Printing	Printer: Stored File Printing
Reading document data (download)	Document Server: Stored File Downloading	Document Server:Stored File Downloading
	Scanner: Stored File Downloading	Scanner: Stored File Downloading
	Fax: Stored File Downloading	Fax: Stored File Downloading
Reading document data (fax transmission)	Fax: Sending	Fax: Sending
Reading document data (e-mail transmission)	Scanner: Stored File Sending	Scanner: Stored File Sending
Reading document data (folder transmission)	Scanner: Stored File Sending	Scanner: Stored File Sending
Deleting document data	Stored File Deletion	Stored File Deletion
	All Stored Files Deletion	All Stored Files Deletion
Success and failure of creation, modification, and deletion of S/MIME user information	Address Book Change	Address Book Change If an attempt to log in succeeds, "Succeeded" appears as the "Result" attribute of the log data. If an attempt to log in fails, "Failed" appears as the "Result" attribute of the log data.

ST Auditable Events	Log Item	Log Type Attribute
Success and failure of creation, modification, and deletion of destination folders	Address Book Change	Address Book Change If an attempt to log in succeeds, "Succeeded" appears as the "Result" attribute of the log data. If an attempt to log in fails, "Failed" appears as the "Result" attribute of the log data.
Communication with RC Gate	Collect Encrypted Communication Logs	Collect Encrypted Communication Logs

Audit Log Items specified in the Security Target (ST) for CC certification correspond as follows to items in "Attributes of logs you can download" in "Logs That Can Be Managed Using Web Image Monitor" in Security Reference:

ST Audit Log Items	Log Item
Date/time of the events	End Date/Time
Types of the events	Log Type
Subject identity	User Entry ID
Outcome	Result
Communication direction	Communication Direction
Communication IP address	IP Address
Communicating e-mail address	Destination Address

About Options

CC certification has been obtained for the machine with the following option attached.

- Fax Option Type C400

The following options are not CC-certified, but can still be used with the machine.

- Copy Data Security Unit Type F
- Paper Feed Unit PB1010
- Paper Feed Unit PB1000
- 1 Bin Tray BN1000
- Side Tray Type C400

Trademarks

Microsoft, Windows, Windows Server, Windows Vista, and Internet Explorer are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

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

- The product names of Windows XP are as follows:

  Microsoft® Windows® XP Professional

  Microsoft® Windows® XP Home Edition

  Microsoft® Windows® XP Media Center Edition

  Microsoft® Windows® XP Tablet PC Edition

- The product names of Windows Vista are as follows:

  Microsoft® Windows Vista® Ultimate

  Microsoft® Windows Vista® Business

  Microsoft® Windows Vista® Home Premium

  Microsoft® Windows Vista® Home Basic

  Microsoft® Windows Vista® Enterprise

- The product names of Windows 7 are as follows:

  Microsoft® Windows® 7 Home Premium

  Microsoft® Windows® 7 Professional

  Microsoft® Windows® 7 Ultimate

  Microsoft® Windows® 7 Enterprise

- The product names of Windows Server 2003 are as follows:

  Microsoft® Windows Server® 2003 Standard Edition

  Microsoft® Windows Server® 2003 Enterprise Edition

- The product names of Windows Server 2003 R2 are as follows:

  Microsoft® Windows Server® 2003 R2 Standard Edition

  Microsoft® Windows Server® 2003 R2 Enterprise Edition

- The product names of Windows Server 2008 are as follows:

  Microsoft® Windows Server® 2008 Standard

  Microsoft® Windows Server® 2008 Enterprise

- The product names of Windows Server 2008 R2 are as follows:

  Microsoft® Windows Server® 2008 R2 Standard

  Microsoft® Windows Server® 2008 R2 Enterprise

- The proper names of Internet Explorer 6, 7, 8, and 9 are as follows:

  Microsoft® Internet Explorer® 6

  Windows® Internet Explorer® 7

  Windows® Internet Explorer® 8

  Windows® Internet Explorer® 9

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.

Notes for Administrator: Using this Machine in a Network Environment Compliant with IEEE Std.2600.1™-2009

Printed in France
EN GB
EN US
EN AU
M026-7440