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

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): "Connecting the Machine/ System Settings", "Security Guide", "Getting Started", 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 Guide.

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:

❖ **Aficio MP C3002/C3502**

Primary Classification	Secondary Classification	Version
Firmware	System/Copy	1.05.4
	Network Support	11.77
	Fax	02.00.00
	RemoteFax	02.00.00
	NetworkDocBox	1.04
	Web Support	1.07
	Web Uapl	1.03
	animation	1.00
	Scanner	01.09
	Printer	1.05.1
	PCL	1.07
	PCL Font	1.06
	Data Erase Onb	1.01x
	GWFCU3.5-4(WW)	01.00.04
	Engine	0.16:04
	OpePanel	1.04
	LANG0	1.03
	LANG1	1.03
Hardware	Ic Key	01020700
	Ic Ctlr	03

2

❖ Aficio MP C4502/C5502

Primary Classification	Secondary Classification	Version
Firmware	System/Copy	1.05.4
	Network Support	11.77
	Fax	02.00.00
	RemoteFax	02.00.00
	NetworkDocBox	1.04
	Web Support	1.07
	Web Uapl	1.03
	animation	1.00
	Scanner	01.09
	Printer	1.05.1
	PCL	1.07
	PCL Font	1.06
	Data Erase Onb	1.01x
	GWFCU3.5-4(WW)	01.00.04
	Engine	0.16:04
	OpePanel	1.04
	LANG0	1.03
	LANG1	1.03
Hardware	Ic Key	01020700
	Ic Ctlr	03

❖ **Aficio MP C4502A/5502A**

Primary Classification	Secondary Classification	Version
Firmware	System/Copy	1.05.4
	Network Support	11.77
	Fax	02.00.00
	RemoteFax	02.00.00
	NetworkDocBox	1.04
	Web Support	1.07
	Web Uapl	1.03
	animation	1.00
	Scanner	01.09
	Printer	1.05.1
	PCL	1.07
	PCL Font	1.06
	Data Erase Onb	1.01x
	GWFCU3.5-4(WW)	01.00.04
	Engine	0.16:02
	OpePanel	1.04
	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].**

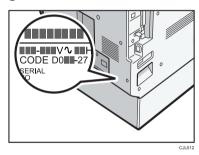**4** **Press [Administrator Tools].**

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
  "-27" or "-67"

- Mainly North America (Type A)
  "-17" or "-57"

- Mainly North America (Type B)
  "-51"

- Mainly Asia
  "-29" or "-69"

In the following example, the machine's model number ends with "-27".

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 "-27".

❖ **Aficio MP C3002/C3502**

❖ **Manual reference numbers for "-27" models**

❖ **Paper Manuals**

Manual Name	Reference Number
MP C3002/C3502/C4502/C4502A/C5502/C5502A Aficio MP C3002/C3502/C4502/C4502A/C5502/C5502A Read This First	D143-7007
Notes for Security Guide	D143-7347
FAX OPTION TYPE C5502 (Machine Code: D643) INSTALLATION PROCEDURE For Machine Code: D111/D142/D143/D144 Copiers	D643-8610
SOFTWARE LICENSE AGREEMENT	D645-7901
Safety Information	A232-8561A
Operating Instructions Notes on Security Functions	D143-7064
Notes for Administrators: Using this Machine in a Network Environment Compliant with IEEE Std. 2600.1^{TM}-2009	D143-7063

❖ **Manual CD-ROMs**

Manual Name	Reference Number
Manuals MP C3002/MP C3502/MP C4502/MP C4502A/MP C5502/MP C5502A Aficio MP C3002/MP C3502/MP C4502/MP C4502A/MP C5502/MP C5502A A	D143-7447
Printer/Scanner Drivers and Utilities RICOH Aficio MP C3002/MP C3502 MP C3002/MP C3502 infotec MP C3002/MP C3502	D143-7435

❖ **Manual reference numbers for "-17" models**

❖ **Paper Manuals**

Manual Name	Reference Number
MP C3002/C3502/C4502/C4502A/C5502/C5502A Aficio MP C3002/C3502/C4502/C4502A/C5502/C5502A User Guide	D143-7004
MP C3002/C3502/C4502/C4502A/C5502/C5502A Aficio MP C3002/C3502/C4502/C4502A/C5502/C5502A Read This First	D143-7008
Notes for Security Guide	D143-7348
Errata	D143-7046
FAX OPTION TYPE C5502 (Machine Code: D643) INSTALLATION PROCEDURE For Machine Code: D111/D142/D143/D144 Copiers	D643-8610
SOFTWARE LICENSE AGREEMENT	D645-7901
Operating Instructions Notes on Security Functions	D143-7066
Notes for Administrators: Using this Machine in a Network Environment Compliant with IEEE Std. 2600.1^{TM}-2009	D143-7065

❖ **Manual CD-ROMs**

Manual Name	Reference Number
Manuals MP C3002/MP C3502/MP C4502/MP C4502A/MP C5502/MP C5502A Aficio MP C3002/MP C3502/MP C4502/MP C4502A/MP C5502/MP C5502A	D143-7444
Printer/Scanner Drivers and Utilities RICOH Aficio MP C3002/MP C3002G/MP C3502/MP C3502G LANIER MP C3002/MP C3002G/MP C3502/MP C3502G SAVIN MP C3002/MP C3002G/MP C3502/MP C3502G	D143-7429

❖ **Manual reference numbers for "-51" models**

❖ **Paper Manuals**

Manual Name	Reference Number
MP C3002G/C3502G/C4502G/C5502G Aficio MP C3002G/C3502G/C4502G/C5502G User Guide	D143-7043
MP C3002G/C3502G/C4502G/C5502G Aficio MP C3002G/C3502G/C4502G/C5502G Read This First	D143-7044
Notes for Security Guide	D143-7350
Errata	D143-7047
FAX OPTION TYPE C5502 (Machine Code: D643) INSTALLATION PROCEDURE For Machine Code: D111/D142/D143/D144 Copiers	D643-8610
SOFTWARE LICENSE AGREEMENT	D645-7900
Operating Instructions Notes on Security Functions	D143-7068
Notes for Administrators: Using this Machine in a Network Environment Compliant with IEEE Std. 2600.1^{TM}-2009	D143-7067

❖ **Manual CD-ROMs**

Manual Name	Reference Number
Manuals MP C3002G/MP C3502G/MP C4502G/MP C4502AG/MP C5502G/MP C5502AG Aficio MP C3002G/MP C3502G/MP C4502G/MP C4502AG/MP C5502G/MP C5502AG	D143-7453
Printer/Scanner Drivers and Utilities RICOH Aficio MP C3002/MP C3002G/MP C3502/MP C3502G LANIER MP C3002/MP C3002G/MP C3502/MP C3502G SAVIN MP C3002/MP C3002G/MP C3502/MP C3502G	D143-7429

8

❖ **Manual reference numbers for "-29" models**

❖ **Paper Manuals**

Manual Name	Reference Number
MP C3002/C3502/C4502/C4502A/C5502/C5502A Aficio MP C3002/C3502/C4502/C4502A/C5502/C5502A User Guide	D143-7004
MP C3002/C3502/C4502/C4502A/C5502/C5502A Aficio MP C3002/C3502/C4502/C4502A/C5502/C5502A Read This First	D143-7009
Notes for Security Guide	D143-7348
Errata	D143-7046
FAX OPTION TYPE C5502 (Machine Code: D643) INSTALLATION PROCEDURE For Machine Code: D111/D142/D143/D144 Copiers	D643-8610
SOFTWARE LICENSE AGREEMENT	D645-7901
Operating Instructions Notes on Security Functions	D143-7066
Notes for Administrators: Using this Machine in a Network Environment Compliant with IEEE Std. 2600.1^{TM}-2009	D143-7065

❖ **Manual CD-ROMs**

Manual Name	Reference Number
Manuals MP C3002/MP C3502/MP C4502/MP C4502A/MP C5502/MP C5502A Aficio MP C3002/MP C3502/MP C4502/MP C4502A/MP C5502/MP C5502A	D143-7444
Printer/Scanner Drivers and Utilities RICOH Aficio MP C3002/MP C3502 Gestetner MP C3002/MP C3502 LANIER MP C3002/MP C3502	D143-7441

❖ **Aficio MP C4502/C4502A/C5502/5502A**

❖ **Manual reference numbers for "-27" and "-67" models**

❖ **Paper Manuals**

Manual Name	Reference Number
MP C3002/C3502/C4502/C4502A/C5502/C5502A Aficio MP C3002/C3502/C4502/C4502A/C5502/C5502A Read This First	D143-7007
Notes for Security Guide	D143-7347
FAX OPTION TYPE C5502 (Machine Code: D643) INSTALLATION PROCEDURE For Machine Code: D111/D142/D143/D144 Copiers	D643-8610
SOFTWARE LICENSE AGREEMENT	D645-7901
Safety Information	A232-8561A
Operating Instructions Notes on Security Functions	D143-7064
Notes for Administrators: Using this Machine in a Network Environment Compliant with IEEE Std. 2600.1^{TM}-2009	D143-7063

❖ **Manual CD-ROMs**

Manual Name	Reference Number
Manuals MP C3002/MP C3502/MP C4502/MP C4502A/MP C5502/MP C5502A Aficio MP C3002/MP C3502/MP C4502/MP C4502A/MP C5502/MP C5502A A	D143-7447
Printer/Scanner Drivers and Utilities RICOH Aficio MP C4502/MP C4502A/MP C5502/MP C5502A MP C4502/MP C4502A/MP C5502/MP C5502A infotec MP C4502/MP C4502A/MP C5502/MP C5502A	D143-7432

❖ **Manual reference numbers for "-17" and "-57" models**

❖ **Paper Manuals**

Manual Name	Reference Number
MP C3002/C3502/C4502/C4502A/C5502/C5502A Aficio MP C3002/C3502/C4502/C4502A/C5502/C5502A User Guide	D143-7004
MP C3002/C3502/C4502/C4502A/C5502/C5502A Aficio MP C3002/C3502/C4502/C4502A/C5502/C5502A Read This First	D143-7008
Notes for Security Guide	D143-7348
Errata	D143-7046
FAX OPTION TYPE C5502 (Machine Code: D643) INSTALLATION PROCEDURE For Machine Code: D111/D142/D143/D144 Copiers	D643-8610
SOFTWARE LICENSE AGREEMENT	D645-7901
Operating Instructions Notes on Security Functions	D143-7066
Notes for Administrators: Using this Machine in a Network Environment Compliant with IEEE Std. 2600.1™-2009	D143-7065

❖ **Manual CD-ROMs**

Manual Name	Reference Number
Manuals MP C3002/MP C3502/MP C4502/MP C4502A/MP C5502/MP C5502A Aficio MP C3002/MP C3502/MP C4502/MP C4502A/MP C5502/MP C5502A	D143-7444
Printer/Scanner Drivers and Utilities RICOH Aficio MP C4502/MP C4502A/MP C4502G/MP C4502AG/MP C5502/MP C5502A/MP C5502G/MP C5502AG LANIER MP C4502/MP C4502A/MP C4502G/MP C4502AG/MP C5502/MP C5502A/MP C5502G/MP C5502AG SAVIN MP C4502/MP C4502A/MP C4502G/MP C4502AG/MP C5502/MP C5502A/MP C5502G/MP C5502AG	D143-7426

❖ **Manual reference numbers for "-51" models**

❖ **Paper Manuals**

Manual Name	Reference Number
MP C3002G/C3502G/C4502G/C5502G Aficio MP C3002G/C3502G/C4502G/C5502G User Guide	D143-7043
MP C3002G/C3502G/C4502G/C5502G Aficio MP C3002G/C3502G/C4502G/C5502G Read This First	D143-7044
Notes for Security Guide	D143-7350
Errata	D143-7047
FAX OPTION TYPE C5502 (Machine Code: D643) INSTALLATION PROCEDURE For Machine Code: D111/D142/D143/D144 Copiers	D643-8610
SOFTWARE LICENSE AGREEMENT	D645-7900
Operating Instructions Notes on Security Functions	D143-7068
Notes for Administrators: Using this Machine in a Network Environment Compliant with IEEE Std. 2600.1^{TM}-2009	D143-7067

❖ **Manual CD-ROMs**

Manual Name	Reference Number
Manuals MP C3002G/MP C3502G/MP C4502G/MP C4502AG/MP C5502G/MP C5502AG Aficio MP C3002G/MP C3502G/MP C4502G/MP C4502AG/MP C5502G/MP C5502AG	D143-7453
Printer/Scanner Drivers and Utilities RICOH Aficio MP C4502/MP C4502A/MP C4502G/MP C4502AG/MP C5502/MP C5502A/MP C5502G/MP C5502AG LANIER MP C4502/MP C4502A/MP C4502G/MP C4502AG/MP C5502/MP C5502A/MP C5502G/MP C5502AG SAVIN MP C4502/MP C4502A/MP C4502G/MP C4502AG/MP C5502/MP C5502A/MP C5502G/MP C5502AG	D143-7426

❖ **Manual reference numbers for "-29" and "-69" models**

❖ **Paper Manuals**

Manual Name	Reference Number
MP C3002/C3502/C4502/C4502A/C5502/C5502A Aficio MP C3002/C3502/C4502/C4502A/C5502/C5502A User Guide	D143-7004
MP C3002/C3502/C4502/C4502A/C5502/C5502A Aficio MP C3002/C3502/C4502/C4502A/C5502/C5502A Read This First	D143-7009
Notes for Security Guide	D143-7348
Errata	D143-7046
FAX OPTION TYPE C5502 (Machine Code: D643) INSTALLATION PROCEDURE For Machine Code: D111/D142/D143/D144 Copiers	D643-8610
SOFTWARE LICENSE AGREEMENT	D645-7901
Operating Instructions Notes on Security Functions	D143-7066
Notes for Administrators: Using this Machine in a Network Environment Compliant with IEEE Std. 2600.1^{TM}-2009	D143-7065

❖ **Manual CD-ROMs**

Manual Name	Reference Number
Manuals MP C3002/MP C3502/MP C4502/MP C4502A/MP C5502/MP C5502A Aficio MP C3002/MP C3502/MP C4502/MP C4502A/MP C5502/MP C5502A	D143-7444
Printer/Scanner Drivers and Utilities RICOH Aficio MP C4502/MP C4502A/MP C5502/MP C5502A Gestetner MP C4502/MP C4502A/MP C5502/MP C5502A LANIER MP C4502/MP C4502A/MP C5502/MP C5502A	D143-7438

📝 **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:

A Check that the machine is off.

B Turn the machine on.

C 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 Guide.

D Log on as the administrator ("admin").

E 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:
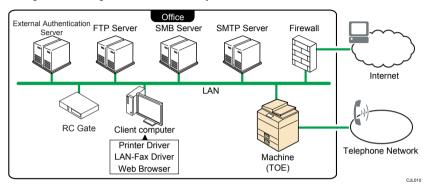**[ROM Version]**
G3: 01.00.04(Validation Data: 33DA)

F 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.

❐ The following versions of the PCL6 and LAN-Fax drivers are CC-conformant:

- Aficio MP C3002/C3502: PCL6 Driver Ver. 1.0.0.0, LAN-Fax Driver Ver. 1.68

- Aficio MP C4502/C5502: PCL6 Driver Ver. 1.0.0.0, LAN-Fax Driver Ver. 1.68

- Aficio MP C4502A/5502A: PCL6 Driver Ver. 1.0.0.0, LAN-Fax Driver Ver. 1.68

❐ Use only CC-conformant or later (post-CC-conformant) versions of the PCL6 and LAN-Fax drivers. If you use a post-CC-conformant driver version, check the revision history to make sure there has been no security-related revision to the CC-conformant version. You can download the drivers from the manufacturer's web site.

❒ 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.

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

📝 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 machine operations.

Settings to Specify Using the Control Panel (1)

A **Turn the machine on.**

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

C **Log on as the administrator ("admin").**

D **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", Connecting the Machine/ System Settings.

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]**, and **[Administrator Tools]** 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 "Configuring Administrator Authentication", Security Guide.

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 "Configuring User Authentication", Security Guide.

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]**.

Tab	Item	Procedure
Administrator Tools(*)	Extended Security / Restrict Display of User Information	Set this to **[On]**.
Administrator Tools(*)	Extended Security / Driver Encryption Key:Encryption Strength	Set this to **[Simple Encryption]**.
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 "#". Even if you change the password policy, passwords that have already been registered can still be used. The changed password policy will be applied only to passwords specified or changed subsequently.
Administrator Tools(*)	Extended Security / @Remote Service	Select **[Proh. Some Services]** if you use @Remote Service. Otherwise, select **[Prohibit]**. Do not set this to **[Do not Prohibit]**.
Administrator Tools(*)	Extended Security / Update Firmware	Set this to **[Prohibit]**.
Administrator Tools(*)	Extended Security /Change Firmware Structure	Set this to **[Prohibit]**.
Administrator Tools(*)	Extended Security / Security Setting for Access Violation	Set this to **[Off]**.

⚲ Reference

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

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]**.

$\mathcal{P}$ Reference

For details about specifying "Service Mode Lock", see "Limiting Machine Operations to Customers Only", Security Guide.

For details about "Auto Delete File in Document Server", see "Administrator Tools" in "System Settings", Connecting the Machine/ System Settings.

⑥ Specify the following settings:

Tab	Item	Procedure
Administrator Tools	Auto Erase Memory Setting	Select **[On]**, and then select **[NSA]**, [**DoD]**, or **[Random Numbers]**. Do not set this to **[Off]**.

$\mathcal{P}$ Reference

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

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."

$\mathcal{P}$ Reference

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

⑧ Specify the following settings:

Tab	Item	Procedure
Administrator Tools(*)	Media Slot Use / Store to Memory Device	Set this to **[Prohibit]**.
Administrator Tools(*)	Media Slot Use / Print from Memory Storage Device	Set this to **[Prohibit]**.

$\mathcal{P}$Reference

For details about specifying "Media Slot Use", see "Restricting Media Slot Access ", Security Guide.

⑨ Specify the following settings:

Tab	Item	Procedure
Administrator Tools(*)	LDAP Search	Set this to **[Off]**.
Administrator Tools(*)	Transfer Log Setting	Set this to **[Off]**.
Administrator Tools(*)	Stop Key to Suspend Print Job	Set this to **[Only Job Being Operated]**.

$\mathcal{P}$Reference

For details about specifying "Administrator Tools", see "Administrator Tools", Connecting the Machine/ System Settings.

⑩ Specify the following settings:

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

$\mathcal{P}$Reference

For details about "Delivery Option", see "File Transfer", Connecting the Machine/ System Settings.

E **Press [Exit].**

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

G **Log on again as the administrator.**

H **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 Guide.

[9] Press [Exit].

[10] Press [Printer Features].

Specify the following settings:

Tab	Item	Procedure
Maintenance(*)	Menu Protect	Set this to **[Level 2]**.
Maintenance(*)	Auto Delete Temporary Print Jobs	Select **[On]** if you use "Auto Delete Temporary Print Jobs". Otherwise, select **[Off]**.
Maintenance(*)	Auto Delete Stored Print Jobs	Select **[On]** if you use "Auto Delete Stored Print Jobs". Otherwise, select **[Off]**.
System(*)	Jobs Not Printed As Machn. Was Off	Set this to **[Do not Print]**.

Reference

For details about "Auto Delete Temporary Print Jobs" and "Auto Delete Stored Print Jobs", see "Maintenance" in "Printer Features", Print.

For details about "Jobs Not Printed As Machn. Was Off", see "System" in "Printer Features", Print.

[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", Scan.

② Specify the following settings:

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

M Press **[Exit].**

N Press **[Facsimile Features].**

① Specify the following settings:

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

$\mathcal{P}$ Reference

For details about specifying "Box Setting", see "Box Settings", Fax.

② Specify the following settings:

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

$\mathcal{P}$ Reference

For details about specifying "Backup File TX Setting", see "Send Settings", Fax.

③ Specify the following settings:

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

$\mathcal{P}$ Reference

For details about specifying "Reception File Setting", see "Reception File Settings", Fax.

④ Specify the following settings:

Tab	Item	Procedure
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.
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 04, bit 7" to **[0]**. If this is enabled, previews will not be included in the reports.

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 **[On]**.

$\mathcal{P}$ Reference

For details about specifying "Internet Fax Setting", "Folder Setting", and "E-mail Setting", see "Initial Settings", Fax.

⓯ Press [Exit] twice.

⓰ Log off.

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

The procedure is different for "Installing the Certificate Issued by the Certificate Authority", "Creating the Self-Signed Certificate", and "Installing the Intermediate Certificate Issued by the Intermediate Certificate Authority".

In the case of "Installing the Certificate Issued by the Certificate Authority" or "Installing the Intermediate Certificate Issued by the Intermediate Certificate Authority", skip to Step **18** since the device certificate will be installed in Step **16** of " Settings to Specify Using Web Image Monitor".

In the case of "Creating the Self-Signed Certificate", do the following:

① Log in as the administrator ("admin").

② Press **[System Settings]**.

③ Press **[Administrator Tools]**.

④ Press **[Next]** three times.

⑤ Press **[Program / Delete Device Certificate]**.

⑥ Check that **[Program]** is selected.

⑦ Select the certificate you want to install from the certificate list.
As the certificate for "SSL/TLS", you can select **[Certificate 1]** only.

⑧ If required, change or specify other settings.
For the certificate required for "S/MIME", enter the administrator's email address in "E-mail Address".
In "Algorithm Signature", select one of the following:

- sha512WithRSA-4096
- sha512WithRSA-2048
- sha256WithRSA-4096
- sha256WithRSA-2048
- sha1WithRSA-2048
- sha1WithRSA-1024

If required, change or specify other settings.

⑨ Press **[OK]**.
"Installed" appears under "Certificate Status" to show that a device certificate for the machine has been installed.

⑩ Logout.

18 **Turn off the main power.**

Connect the machine and a computer with a Web browser for accessing the machine to a network that only administrators can access.

A **Turn the machine on.**

B **Launch the Web browser on the computer, and then access "http://(machine's IP address or host name)/".**

The message "There is a problem with this website's security certificate." might appear. If this happens, click "Continue to this website (not recommended).".

C **Log on as the administrator ("admin").**

D **Point to [Device Management], and then click [Configuration].**

E **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]**.
After the password has been changed, an Authentication Error message appears.

④ Click **[OK]**.

F **Log on as the supervisor ("supervisor").**

G **Point to [Device Management], and then click [Configuration].**

H **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]**.
After the password has been changed, an Authentication Error message appears.

④ Click **[OK]**.

I **Log on as the administrator ("admin").**

J **Point to [Device Management], and then click [Configuration].**

⓫ **Use the following procedure to specify the user authentication. (*)**

❖ **If you have selected [Basic Authentication] in Step ❹-③ in "Settings to Specify Using the Control Panel (1)"**

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. However, do not specify **[Other Functions: Browser]**.

⑤ Click **[OK]**.

❖ **If you have selected [Windows Authentication] in Step ❹-③ in "Settings to Specify Using the Control Panel (1)"**

① Click **[Kerberos Authentication]** in "Device Settings".

② In "Encryption Algorithm", check "AES256-CTS-HMAC-SHA1-96", "AES128-CTS-HMAC-SHA1-96", "DES3-CBC-SHA1", and "RC4-HMAC", and uncheck "DES-CBC-MD5".

③ Enter the **[Realm Name]**, **[KDC Server Name]**, and **[Domain Name]** in **[Realm 1]**.

④ Click **[OK]**.

⑤ Click **[User Authentication Management]** in "Device Settings".

⑥ Make sure **[User Authentication Management]** is set to **[Windows Authentication]**.

⑦ Set "Printer Job Authentication" to **[Entire]**.

⑧ Set "SSL" in "Windows Authentication Settings" to **[On]**.

⑨ Set "Kerberos Authentication" in "Windows Authentication Settings" to **[On]**.

⑩ In **[Windows Authentication Settings]**, select the realm name specified in step ③.

⑪ 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.
However, do not specify **[Other Functions: Browser]**.

⑫ Click **[OK]**.

🔎**Reference**

For details about specifying the Realm, see "Programming the Realm" in "System Settings", Connecting the Machine/ System Settings.

For details about specifying which functions are available to users, see "Specifying Which Functions are Available", Security Guide.

⓬ 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]**.
An Authentication Error message appears.

⑧ Click **[OK]**.

⑨ Log on as the administrator ("admin").

⑩ Point to **[Device Management]**, and then click **[Configuration]**.

⓭ Use the following procedure to specify the timer settings.

① Click **[Timer]** in "Device Settings".

② Set "Auto Logout Timer" to **[On]**. (*)

③ Set the range for the timer between 60-999 seconds.
You can change the time without suspending the machine.

④ Click **[OK]**.

⓮ 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 Point to **[Device Management]**, and then click **[Configuration]**.

⓯ 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]**.

⓰ 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, 4, 5 or 6) 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 In "Algorithm Signature", select one of the following:
  - sha512WithRSA-4096
  - sha512WithRSA-2048
  - sha256WithRSA-4096
  - sha256WithRSA-2048
  - sha1WithRSA-2048
  - sha1WithRSA-1024

  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]**.
The message "There is a problem with this website's security certificate." might appear. If this happens, click "Continue to this website (not recommended).".

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]**.

❖ **If you have created a self-signed certificate**
1) Select the certificate for S/MIME signing according to the following procedure:

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

② In "S/MIME" in "Certification", select the certificate you want to use.

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, 4, 5 or 6) 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 In "Algorithm Signature", select one of the following:

- sha512WithRSA-4096
- sha512WithRSA-2048
- sha256WithRSA-4096
- sha256WithRSA-2048
- sha1WithRSA-2048
- sha1WithRSA-1024

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]**.
The message "There is a problem with this website's security certificate." might appear. If this happens, click "Continue to this website (not recommended).".

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]**.

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

① Click **[Network Security]** in "Security".

② Set "Security Level" to **[FIPS 140]**.

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]**, **[3DES]**, and **[RC4]** in **[Encryption Strength Setting]**.

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 "WSD (Device)" to **[Inactive]**.

⑫ Set "IPv4" in "WSD (Printer)" to **[Inactive]**.

⑬ Set "IPv4" in "WSD (Scanner)" to **[Inactive]**.

⑭ Set "SNMP" in "SNMP" to **[Inactive]**.

○15 Click **[OK]**.

Wait a while for the machine to reset itself.

If "Security Level" is set to **[FIPS 140]**, some functions become unavailable. For details about the available functions under each security level, see "Status of Functions under Each Network Security Level" and "Enabling and Disabling Protocols" in Security Guide.

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 Guide.

○16 Click **[OK]**.

○17 Click **[Network Security]** in "Security".

○18 In "SSL/TLS Version", set "TLS1.2", "TLS1.1", "TLS1.0", and "SSL3.0" to **[Active]**.

○19 Click **[OK]**.

Wait a while for the machine to reset itself.

○20 Click **[OK]**.

18 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.

You can change "Number of Attempts before Lockout" without suspending the machine. Set it to "5" or lower.

④ Set "Lockout Release Timer" to **[Active]**. (*)

⑤ Enter a range of 1-9999 minutes in **[Lock Out User for]**.

You can change "Lock Out User for" without suspending the machine.

⑥ Click **[OK]**.

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

① Click **[IPsec]** in "Security".

② In "IPsec:" in "IPsec", select **[Active]** or **[Inactive]**.

If you have set "IPsec:" to **[Inactive]**, do not use Scan to Folder. Also, delete the Scan to Folder destinations registered in the address book.

If you have set "IPsec:" to **[Inactive]**, skip to Step ⑦.

③ Select **[Inactive]** from "Encryption Key Manual Settings:" in the "IPsec" area.

④ Click **[Edit]** in "Encryption Key Auto Exchange Settings".

⑤ 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]**.

- In "Hash Algorithm" in "Security Details", select **[SHA1]**, **[SHA256]**, [**SHA384**], or **[SHA512]**.
- In "Encryption Algorithm" in "Security Details", select **[3DES]**, **[AES-128-CBC]**, **[AES-192-CBC]**, or **[AES-256-CBC]**.
- In "Diffie-Hellman Group" in "Security Details", select **[2]** or **[14]**.
- In "Authentication Algorithm" in "Security Details", check **[HMAC-SHA1-96]**, **[HMAC-SHA256-128]**, **[HMAC-SHA384-192]**, and **[HMAC-SHA512-256]**, and uncheck "HMAC-MD5-96".
- In "Encryption Algorithm Permissions" in "Security Details", check **[3DES]**, **[AES-128]**, **[AES-192]**, and **[AES-256]**, and uncheck **[Cleartext]** and **[DES]**.
- In "PFS" in "Security Details", select **[2]** or **[14]**.
- In "Authentication Method" in "Security Details", select **[PSK]** or **[Certificate]**.

❖ **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.

⑥ Select **[Active]** or **[Inactive]** in "Exclude HTTPS Communication:".
⑦ Click **[OK]**.
Wait a while for the machine to reset itself.
⑧ Click **[OK]**.

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

① Click **[S/MIME]** in "Security".
② In "Encryption Algorithm" in "Encryption", select **[AES-256 bit]**, **[AES-128 bit]**, or **[3DES-168 bit]**.
③ In "Digest Algorithm" in "Signature", select **[SHA-512 bit]**, **[SHA-384 bit]**, **[SHA-256 bit]**, or **[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 Sending E-mail by Fax" in "Signature" to **[Use Signatures]**.
⑦ Set "When E-mailing TX Results by Fax" in "Signature" to **[Use Signatures]**.

34

⑧ Set "When Transferring Files Stored in Document Server (Utility)" in "Signature" to **[Use Signatures]**.

⑨ Click **[OK]**.

㉑ Use the following procedure to specify the IPv4 settings. (*)

① Click **[IPv4]** in "Network".

② Set **[Inactive]** in "LLMNR".

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

④ Click **[OK]**.

㉕ Log off, and then quit Web Image Monitor.

㉖ Turn off the main power.

Settings to Specify Using the Control Panel (2)

A Turn the machine on.

B Press the [User Tools/Counter] key.

C Log in as the administrator ("admin").

4 Press **[System Settings].**

Specify the following settings:

Tab	Item	Procedure
Interface Settings(*)	Effective Protocol	Check that IPv4 is set to **[Active]**.
		Check that IPv6 is set to **[Inactive]**.
		Set Firmware Update (IPv4) to **[Inactive]**.
		Set Firmware Update (IPv6) to **[Inactive]**.

5 Press **[Exit]** twice.

6 Log out.

7 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", Connecting the Machine/ System Settings.

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", Fax. 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 log in from the machine's control panel while changing settings via Web Image Monitor. Doing so might invalidate the settings specified via Web Image Monitor.

- 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 Scanned Documents to a Client Computer", Scan.

- Before using the machine, either create a new encryption key for encrypting the stored data or obtain one from your service representative. Back up the encryption key only when you specify the settings listed on p.16 "Settings".

- 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.

  #### $\mathcal{P}$ Reference

  For details about installing the user certificate, see "E-mail Encryption", Security Guide.

- The administrator is required to check that the certificate was issued by a trusted certificate authority.

- 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).

- 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.

- A third party may steal or read paper documents printed by this machine. Instruct users to collect printed copies immediately.

- To install the LAN-Fax driver, enter the machine's IP address or host name in the **[Printer URL]** box as follows (also described in "Using the SmartDevice-Monitor for Client port" in "Specifying the Port When Installing the LAN-FAX Driver" in "Installing the LAN-Fax Driver", Driver Installation Guide):
  https://(machine's IP address or host name)/printer

- To install the printer driver, enter the machine's IP address or host name in the **[URL:]** box as follows (also described in "Using the IPP Port" in "Installing the Printer Driver for the Selected Port", Driver Installation Guide): https://(machine's IP address or host name)/printer
- 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.
- Do not use exported or imported device setting information since it is not CC-conformant.
- Do not perform address book restoration since it is not CC-conformant.
- Set **[Service Mode Lock]** to **[On]**.

Security Functions Covered by CC Certification

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

For details about ① to ⑦, see the chapters with corresponding titles in the Security Guide.

① Getting Started
- Configuring Administrator Authentication
  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.

② Configuring User Authentication
- Configuring User Authentication
  Use basic authentication or Windows Kerberos authentication.
- User Lockout Function
- Auto Logout
  "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.

③ Restricting Machine Usage
- Restricting Usage of the Destination List
- Preventing Changes to Administrator Settings
- Limiting Available Functions

④ Preventing Leakage of Information from Machines
- Encrypting Data on the Hard Disk
- Deleting Data on the Hard Disk

39

⑤ Enhanced Network Security

- Protecting the Communication Path via a Device Certificate
  Use SSL and IPsec for encrypted data communication.
  Using IPsec for Scan to Folder with FTP or SMB is CC conformant.
- Configuring SSL/TLS
- Configuring S/MIME
- Configuring IPsec

⑥ Preventing the Leaking of Documents

- Configuring Access Permissions for Stored Files
  Modification of stored data has not been rated for CC conformance.

⑦ Managing the Machine

- 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.

- Confirming Firmware Validity
  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".

⑧ 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.

Note

❒ The following message might also be displayed: "SD Card authentication has failed.". If it is, contact your service representative.

❒ In the event of a hard disk error, the machine displays a message asking whether or not to initialize the disk and initializes it upon receiving approval. Note however that following the hard disk initialization, user authentication might fail even though the correct password has been 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 Guide.

📝 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 Guide:

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.
Starting Lockout	Lockout	If the log type is "Lockout" and the log type attribute for "Lockout/Release" is "Lockout"
Releasing Lockout	Lockout	If the log type is "Lockout" and the log type attribute for "Lockout/Release" is "Release"
New creation, modification, and deletion of the login user name of normal user by MFP Administrator when Basic Authentication is used	Address Book Change	Address Book Change
Modification of login user name of supervisor by supervisor	Administrator Change	Administrator Change
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

ST Auditable Events	Log Item	Log Type Attribute
New creation and modification of login password of normal user by MFP Administrator when Basic Authentication is used	Password Change	Password Change
Modification of own login password by normal user when 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 Auto Logout Timer of the Operation Panel by MFP Administrator	Machine Configuration	Machine Configuration
Modification of Number of Attempts before Lockout by MFP Administrator when Basic Authentication is used	Machine Configuration	Machine Configuration
Modification of Lockout Release Timer Setting by MFP Administrator when Basic Authentication is used	Machine Configuration	Machine Configuration
Modification of lockout time by MFP Administrator when Basic Authentication is used	Machine Configuration	Machine Configuration
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
Deletion of audit logs by MFP Administrator	All Logs Deletion	All Logs Deletion

ST Auditable Events	Log Item	Log Type Attribute
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
Modification of IPsec setting information by MFP Administrator	Machine Configuration	Machine Configuration
Modification of Device Certificate by MFP Administrator	Machine Configuration	Machine Configuration
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 This will be recorded only if an attempt to log in fails (if "Failed" appears as the Result attribute of the log data).
Folder transmission	Scanner: Sending	Scanner: Sending
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

ST Auditable Events	Log Item	Log Type Attribute
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 of attachments)	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
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 Security Guide:

ST Audit Log Items	Log Item
Starting date/time of an event	Start Date/Time
Ending date/time of an event	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
Lockout operation type	Lockout/Release
Locked out User	Target User Entry ID
Locked out User who is to be released(user)	Target User Entry ID
Locked out User who is to be released(supervisor and MFP Administrator)	Lockout Administrators [1]

[1] "Unknown" in the "Lockout Administrators" log entry indicates that the lockout of the supervisor and all administrators has been released.

About Options

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

- Fax Option Type C5502

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

❖ **Aficio MP C3002/C3502**

- Copy Data Security Unit Type G
- Platen Cover Type 3352
- ARDF DF3060
- Paper Feed Unit PB3130
- LCIT PB3140
- Envelope Feeder EF3020
- LCIT RT3020
- Paper Feed Unit PB3120
- Caster Table Type D
- 1 Bin Tray BN3100
- Internal Shift Tray SH3060
- Bridge Unit BU3060
- Booklet Finisher SR3100
- Punch Kit PU3000 NA
- Punch Kit PU3000 EU
- Punch Kit PU3000 SC
- Finisher SR3070
- Finisher SR3090
- Side Tray Type C5502
- Hand Set Type C5502
- ADF Handle Type C
- Unicode Font Package for SAP® 1 License
- Unicode Font Package for SAP® 10 License
- Unicode Font Package for SAP® 100 License

❖ **Aficio MP C4502/C5502**

- Copy Data Security Unit Type G
- Platen Cover Type 3352
- ARDF DF3070
- Paper Feed Unit PB3130
- LCIT PB3140
- Envelope Feeder EF3020
- LCIT RT3020
- 1 Bin Tray BN3100
- Internal Shift Tray SH3060
- Bridge Unit BU3060
- Booklet Finisher SR3110
- Punch Unit PU3030 NA
- Punch Unit PU3030 EU
- Punch Unit PU3030 SC
- Finisher SR3120
- Finisher SR3090
- Side Tray Type C5502
- Hand Set Type C5502
- ADF Handle Type C
- Scanner Accessibility Option Type C5502
- Unicode Font Package for SAP® 1 License
- Unicode Font Package for SAP® 10 License
- Unicode Font Package for SAP® 100 License

❖ **Aficio MP C4502A/5502A**

- Copy Data Security Unit Type G
- Paper Feed Unit PB3130
- LCIT PB3140
- Envelope Feeder EF3020
- LCIT RT3020
- 1 Bin Tray BN3100
- Internal Shift Tray SH3060
- Bridge Unit BU3060
- Booklet Finisher SR3110
- Punch Unit PU3030 NA
- Punch Unit PU3030 EU
- Punch Unit PU3030 SC
- Finisher SR3120
- Finisher SR3090
- Side Tray Type C5502
- Hand Set Type C5502
- ADF Handle Type C
- Unicode Font Package for SAP® 1 License
- Unicode Font Package for SAP® 10 License
- Unicode Font Package for SAP® 100 License

Security Guide Errata

This section corrects errors in the supplied Security Guide. Please refer to it when reading the Security Guide.

Topic	Additional Description
8. Troubleshooting > If Authentication Fails > If an Error Code is Displayed > Windows authentication	【Error】 W0406-104 【Corrections】 W0406-107
8. Troubleshooting > If Authentication Fails > If an Error Code is Displayed > Windows authentication	【Error】 W0400-105 【Corrections】 W0400-107
8. Troubleshooting > If Authentication Fails > If an Error Code is Displayed > Windows authentication	【Error】 W0400-106 【Corrections】 W0400-107

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.

D1437067