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

"CC certification" refers to the "Common Criteria for Information Technology Security Evaluation" standard. Administrators wishing to use this machine in a CC-certified environment must read this booklet carefully and understand its content. To establish a CC-conformant environment, you must specify settings according to the instructions in this manual. 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

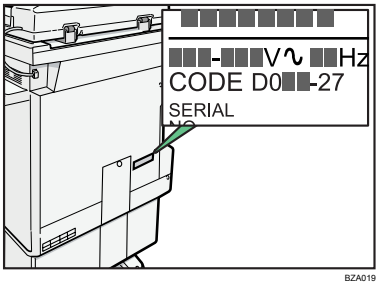
The following manuals are intended for use by administrators (including the supervisor): "General Settings Guide", "Security Reference", "Notes for Security Functions", "About This Machine", and "Notes for Administrators: Using this Machine in a Network Environment Compliant with IEEE Std. 2600.1™-2009". 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.

Check the machine's model number. If it ends with "-27", make sure the manual reference numbers are correct.

❖ Identifying the model

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".

❖ Manual reference numbers for "-27" models

❖ Paper Manuals

Manual Name	Reference Number
Quick Reference Copy Guide	D092-7714
Quick Reference FAX Guide	D509-8534
Quick Reference Printer Guide	D381-7303
Quick Reference Scanner Guide	D381-7309
Manuals for This Machine	D085-7538
Safety Information for Aficio MP 2851/Aficio MP 3351 (or Safety Information for MP 2851/MP 3351)	D085-7500 (or D085-7501)
Notes for Users	D085-7896A
App2Me Start Guide	D085-7904B
Notes for Users	D377-7250
Notes for Users	D060-7781
Notes for Users	G189-6786
Notes for Users	D092-7906
To Users of This Machine	D029-7904
Operating Instructions Notes on Security Functions	D085-7809

❖ Manuals on CD-ROM

Manual Name	Reference Number
Manuals for Users MP 2851/3351 Aficio MP 2851/3351 A	D085-7510
Manuals for Administrators Security Reference MP 2851/3351 Aficio MP 2851/3351	D085-7512
Manuals for Administrators Security Reference Supplement 9228/9233 MP 2851/3351 LD528/LD533 Aficio MP 2851/3351	D085-7522
VM Card Manuals	D377-7500
Manuals DataOverwriteSecurity Unit Type H/I	D377-7900A

Before Applying the Security Functions

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

Also, administrators must use the following procedure to check the firmware and hardware versions for CC conformance. If they are not, contact your service representative.

The administrator can confirm the version of the firmware and hardware.

How to Confirm the Version of the Firmware and Hardware

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].**

CC Conformant Firmware Versions

Software	System/Copy	1.02
	Network Support	7.34
	Scanner	01.12
	Printer	1.02
	Fax	02.00.00
	RemoteFax	02.00.00
	Web Support	1.05
	Web Uapl	1.03
	Network DocBox	1.00
	animation	1.1
	Option PCL	1.03
	OpitonPCLFont	1.01
	Engine	1.00:01
	OpePanel	1.10
	LANG0	1.09
	LANG1	1.09
Hardware	Ic Key	1100
	Ic Hdd	01
Option	GWFCU3-20(WW)	02.00.00
	Data Erase Opt	1.01m

After specifying the settings listed in "Settings" in this manual, the administrator must use the following procedure to check that the FCU in use is a genuine product.

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

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.

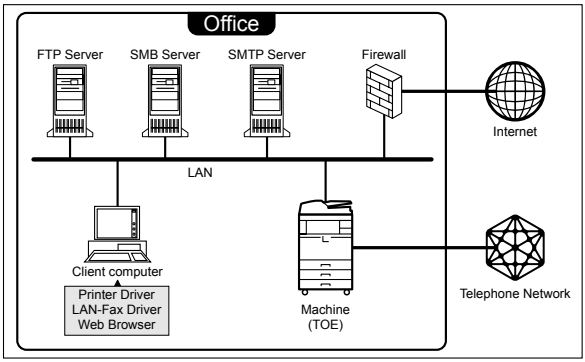
⑥ Check that the following ROM version matches the one shown in the printed list:
[ROM Version]
G3: 02.00.00 (Validation Data: 2450)

6 Log off.

Example CC Conformant Environment

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

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. Unused ports that remain unblocked can be used to gain unauthorized access to the LAN and the devices and data on it.



Important

- ❒ The CC conformance standard stipulates that installation be performed by an authorized service representative.
- ❒ 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 IP-SSL authentication.
- ❒ Use Windows Internet Explorer 6.0, 7.0, or 8.0 as the Web browser.
- ❒ Use PCL Driver Ver. 1.0.0.0 or later and LAN-Fax Driver Ver. 1.62 or later. 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.
- ❒ @Remote is not CC conformant. Do not use it.
- ❒ App2Me is not CC conformant. Do not use it.
- ❒ Embedded Software Architecture applications are not CC conformant. Do not use them.

Settings

To maintain your environment's CC conformance, make changes to the machine's settings in accordance with the following conditions:

(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. Changing certain settings will negate CC conformance. These settings are listed below. Do not change these settings:

- Settings on the tabs marked with an asterisk among the settings listed in "Settings to Specify Using the Control Panel"
- Settings listed in "Settings to Specify Using telnet"
- 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 Reconnect to the network that can be accessed by administrators only.

③ Change the settings.

④ Check that the settings that must not be changed are unchanged.

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)]**.

Reference

For details about specifying "Interface Settings", see "Interface Settings", General Settings Guide.

② Be sure to specify the following settings also:

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 "Administrator Authentication", Security Reference.

③ Be sure to specify the following settings also:

Tab	Item	Procedure
Administrator Tools(*)	User Authentication Management	Select **[Basic Auth.]**, and then set "Printer Job Authentication" to **[Entire]**. In "Available Functions", select all functions.

Reference

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

④ Be sure to specify the following settings also:

Tab	Item	Procedure
Administrator Tools(*)	Extended Security / Restrict Adding of User Destinations	Set this to **[On]**.
Administrator Tools(*)	Extended Security / Restrict Use of Destinations	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]**.

Tab	Item	Procedure
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 "#".
Administrator Tools(*)	Extended Security / @Remote Service	Set this to **[Prohibit]**.
Administrator Tools(*)	Extended Security / Update Firmware	Set this to **[Prohibit]**.
Administrator Tools(*)	Change Firmware Structure	Set this to **[Prohibit]**.

Reference

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

⑤ Be sure to specify the following settings also:

Tab	Item	Procedure
Administrator Tools(*)	Service Mode Lock	Set this to **[On]**.

Reference

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

⑥ Be sure to specify the following settings also:

Tab	Item	Procedure
Administrator Tools(*)	Auto Erase Memory Setting	Set this to **[On]**. You may select any of the displayed encryption systems.

Reference

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

⑦ Be sure to specify the following settings also:

Tab	Item	Procedure
Administrator Tools(*)	Machine Data Encryption Settings	Ensure 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.

5 Press [Exit].

A message confirming whether you want to log off appears. Press **[Yes]** to log off.

6 Log on again as the administrator.

7 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.

8 Press [Exit].

9 Press [Printer Features].

Specify the following settings:

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

10 Press [Exit].

11 Press [Scanner Features].

① Specify the following settings:

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

Reference

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

② Be sure to specify the following settings also:

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", General Settings Guide.

③ Be sure to specify the following settings also:

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

12 Press [Exit].

13 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 "Box Setting", General Settings Guide.

② Be sure to specify the following settings also:

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", General Settings Guide.

③ Be sure to specify the following settings also:

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", General Settings Guide.

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

For details about specifying "Memory Lock Reception", see "Reception Settings", General Settings Guide.

④ Be sure to specify the following settings also:

Tab	Item	Procedure
Initial Settings(*)	Parameter Setting	Set "switch 10, bit 5" to "0". This will prevent the printing of received fax documents that are 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, which 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 the received fax document 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". Does not load the image for the report.

⑤ Be sure to specify the following settings also:

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]**.

Reference

For details about specifying "Internet Fax Setting" and "Folder Setting", see "Initial Settings", General Settings Guide.

14 Press [Exit] twice.

If the following message appears, press **[OK]**:

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

15 Log off.

16 Turn off the main power.

For details about turning off the main power, see "Turning On/Off the Power", About This Machine.

Settings to Specify Using telnet

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 Use the IP address or the host name of the machine to start telnet.

```
% telnet IP_address
```

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

5 Enter the following command, and then press the【Enter】key.

```
msh> set rfu down
```

6 Enter the following command, and then press the【Enter】key.

```
msh> set nrs down
```

7 Enter the following command, and then press the【Enter】key.

```
msh> logout
```

A message asking whether or not to store the changed settings appears.

8 Enter "yes", and then press the【Enter】key.

Reference

For details about specifying settings via telnet, see "Remote Maintenance by telnet", Network Guide.

Settings to Specify Using Web Image Monitor

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

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

3 Click [Configuration].

4 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]**.

5 Log on as the supervisor ("supervisor").

6 Click [Configuration].

7 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]**.

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

9 Click [Configuration].

10 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]**.
Wait a while for the machine to reset itself.

⑥ Click **[OK]**.

⑦ Log on as the administrator ("admin").

⑧ Click **[Configuration]**.

11 Use the following procedure to specify the timer settings.

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

② Specify "Auto Logout Timer". (*)
Select **[On]**.
Set the timer to "180 seconds".

③ Click **[OK]**.

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

⑧ Click **[Configuration]**.

⑨ Click **[OK]**.

13 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]**.

⑤ Click **[On-demand E-mail Notification]** in "Device Settings".

⑥ Set the following three items in **[Access Restriction to Information]** to **[Inactive]**.

- Restriction to System Config. Info.
- Restriction to Network Config. Info.
- Restriction to Printer Config. Info.

⑦ Click **[OK]**.

14 Use the following procedure to install the device certificate.

There are two types of device certificates: certificates issued by the certificate authority and self-signed certificates. 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" can be selected. However, if the certificate is also used for "SSL/TLS", select **[Certificate1]**.

③ Click **[Request]**.
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 e-mail address in "E-mail Address".
If required, change or specify other settings.

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

⑥ Click **[OK]**.
The machine requests the certificate. Wait a while for the machine to become usable.

⑦ Click **[Details]**( ) next to the number of requested certificate.

⑧ 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.

⑨ 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 "Certificate Request" 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 Select **[Certificate1]** for "IPsec".

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

③ For the certificate required for "S/MIME", enter the administrator's e-mail address in "E-mail Address".
If required, change or specify other settings.

④ 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]**.

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

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

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

③ Set "IPv6" in "TCP/IP" to **[Inactive]**.

④ For the SSL/TLS version settings, set "SSL2.0" to **[Inactive]**, and set "SSL3.0" and "TLS" to **[Active]** respectively.

⑤ In "Port 80" in "HTTP" in the "TCP/IP" list, set "IPv4" to **[Close]**.
If you do this, "IPv4" in "Port 80" in "IPP" are also automatically set to **[Close]**.

⑥ Set "IPv4" in "FTP" to **[Inactive]**.

⑦ Set "IPv4" in "sftp" to **[Inactive]**.

⑧ Set "IPv4" in "ssh" to **[Inactive]**.

⑨ Set "SNMP" in "SNMP" to **[Inactive]**.

⑩ 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" and "Enabling/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/Disabling Protocols" in Security Reference.
Wait a while for the machine to reset itself.

⑪ Click **[OK]**.

16 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 Set "Lock Out User for" to "60 minute(s)".

⑥ Click **[OK]**.

17 Use the following procedure to configure the settings for IPsec communication.

① Click **[IPsec]** in "Security".

② Set "Encryption Key Manual Settings" to **[Inactive]**.

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]**.
  If you set "Address Type" to "IPv4", "Authentication Method" in "Security Details" is automatically set to **[PSK]**.
- Click **[Change]** next to "PSK Text".
- Enter the PSK in the "PSK Text" field.
- Enter the PSK again in the "Confirm PSK Text" field, and then click **[OK]**.
  Do not forget the PSK; you will need it to configure the server settings when using Scan to Folder.
  To specify this setting differently according to conditions, specify the setting under each of the settings.
- Click **[OK]**.

⑤ Set "IPsec:" in "IPsec" to **[Active]**.

⑥ Select **[Active]** in "Exclude HTTPS Communication:".

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

⑧ Click **[OK]**.

18 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]**.

19 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 Click **[OK]**.

20 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]**.

21 Log off, and then quit Web Image Monitor.

22 Turn off the main power.

For details about turning off the main power, see "Turning On/Off the Power", About This Machine.

❖ **Settings to Be Specified Using the Control Panel**

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", General Settings Guide.
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", General Settings Guide. 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 **[Specify User]**.

⑨ Press the Destination key of the group you wish to specify, and then press **[OK]**.

⑩ Check the selected group, and then press **[OK]**.

⑪ Press **[Exit]**.

⑫ Log off.

⑬ Turn off the main power.
For details about turning off the main power, see "Turning On/Off the Power", About This Machine.

⑭ 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.
- If the administrator intends to reconfigure the device certificate or change the e-mail address specified for the device certificate, first the machine should be temporarily stopped. 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.
- When using Scan to Folder, make sure IPsec is enabled.
- The Scan to Folder destination (FTP or SMB server) must be registered in the Address Book by the administrator. To register a Scan to Folder destination in the Address Book, do the following via Web Image Monitor: in "Protection", "Protect Destination" in the Address Book, click **[Change]** next to "Access Privilege", and then, in "Public", set "All Users" to **[Read-only]**.
- 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. If you want to change the encryption key, you must temporarily stop using the machine. When changing the encryption key, select **[All Data]**, so you can transfer all data to the HDD.

  Reference

  For details about updating the encryption key, see "Updating the Encryption Key", Security Reference.
- To prevent data leakage when sending files by e-mail, only use the machine in an environment that supports encryption.
- 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.

- Only users whose login user names are registered in the Address Book are CC conformant destinations when sending scan files by e-mail.
  "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.
- Specify the group of users who can access the received faxes that are stored. Do not change the group of users specified in step ⑨ of "Settings to Be Specified Using the Control Panel" in "Settings" in this manual.
- 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 remove or review paper documents printed by this machine. Instruct users to collect prints immediately.
- To install the LAN-Fax driver, enter the IP address as follows (also described in "Using the IPP Port" in "Installing Individual Applications", 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", 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.

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 only.
- 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
  Do not send by e-mail documents other than those saved on the machine using the scanner function.
- Protecting Registered Information in the Address Book
  Address Book restoration is not CC conformant. Do not use it.
- 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
  The printer's Locked Print, Sample Print, Stored Print, and Hold Print functions have not been rated for CC conformance.
- 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 has been 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.

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 Security Reference:

ST Auditable Events	Log Item	Log Type Attribute	Supplementary Explanation
Starting Audit Function	Firmware: Structure	Firmware: Structure	None
Login	Login	Login	None
Starting Lockout	Lockout	"Lockout" appears under both "Log Type" and "Lockout/Release".	None
Releasing Lockout	Lockout	"Lockout" appears under "Log Type", and "Release" appears under "Lockout/Release".	"Auto", which appears under "Lockout/Release Method", refers to auto lockout release; "Manual", which appears under "Lockout/Release Method", refers to manual lockout release.
	Firmware: Structure	Firmware: Structure	Lockout can be released by launching TOE.
HDD encryption key generation	Machine Data Encryption Key Change	"Machine Data Encryption Key Change" appears under "Log Type", "Finish Updating Machine Data Encryption Key" under "Machine Data Encryption Key Operation"; and "Encryption Key for Hard Disk" appears under "Machine Data Encryption Key Type".	None
Successful storage of Document Data	File Storing	"File Storing" appears under "Log Type", and "Succeeded" appears under "Result".	None

ST Auditable Events	Log Item	Log Type Attribute	Supplementary Explanation
Successful reading of Document Data	Stored File Printing	"Stored File Printing" appears under "Log Type", and "Succeeded" appears under "Result".	None
	Fax: Sending	"Fax: Sending" appears under "Log Type", and "Succeeded" appears under "Result".	None
	Fax: Stored File Downloading	"Fax: Stored File Downloading" appears under "Log Type", and "Succeeded" appears under "Result".	None
	Scanner: Stored File Downloading	"Scanner: Stored File Downloading" appears under "Log Type", and "Succeeded" appears under "Result".	None
	Scanner: Stored File Sending	"Scanner: Stored File Sending" appears under "Log Type", and "Succeeded" appears under "Result".	None
Successful deletion of Document Data	Stored File Deletion	"Stored File Printing" appears under "Log Type", and "Succeeded" appears under "Result".	None
	All Stored Files Deletion	"All Stored Files Deletion" appears under "Log Type", and "Succeeded" under "Result".	None
Receiving fax	Fax: Receiving	Fax:Receiving	None
Changing user password (include newly creating and deleting password)	Password Change	Password Change	None
Deleting Administrator Role	Administrator Change	Administrator Change	None
Adding Administrator Role	Administrator Change	Administrator Change	None
Changing Document Data ACL	File Access Privilege Change	File Access Privilege Change	None
Changing date and time of system clock	Date/Time Change	Date/Time Change	None
Communication with trusted IT product	Collect Encrypted Communication Logs	Collect Encrypted Communication Logs	None
Communication with remote user	Collect Encrypted Communication Logs	Collect Encrypted Communication Logs	None
Deleting the entire audit log	All Logs Deletion	All Logs Deletion	None

Basic Audit Information specified in the Security Target (ST) for CC certification corresponds as follows to items in "Attributes of Logs you can Download" in Security Reference:

ST Basic Audit Information	**Log Item**
Date/time of the events	End Date/Time
Types of the events	Log Type
Subject identity	User Entry ID
Outcome	Result
Locked out User	Target User Entry ID
Locked out User who is to be released	Target User Entry ID
Release methods (Auto Lockout Release/Manual Lockout Release)	Lockout/Release Method
In the case of newly creating/changing/deleting the user authentication information of others, the ID of the person making the change	Target User Entry ID
Communication IP address	IP Address
ID of object Document Data	Stored File ID

About Options

This CC-certified device is equipped with a printer/scanner unit. The following options are required for CC conformance:

- Fax Option Type 3351
- DataOverwriteSecurity Unit Type I
- HDD Encryption Unit Type A

Attaching any of the following options does not compromise CC conformance.

- Copy Data Security Unit Type F
- ARDF DF3030
- Platen Cover Type 3800C
- Finisher SR790
- Finisher SR3050
- Paper Feed Unit PB3030
- PS500
- Duplex Unit AD3000
- Bypass Tray BY3000
- Bridge Unit BU3020
- 1 Bin Tray BN3030
- Internal Shift Tray SH3010
- Hand Set Type1018

Printed in France
EN (GB) EN (US) EN (AU) D085-7806
D0857806