Notes for Administrators: Using this Machine in a CC-Certified Environment

"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 and Japanese only.

Administrator Manuals and User Manuals

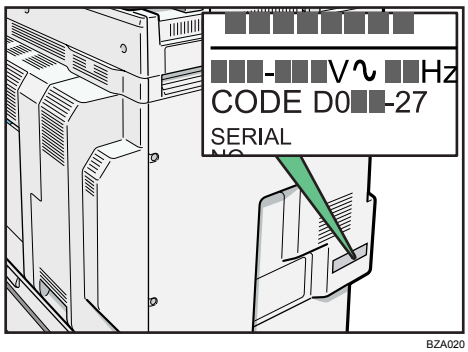
The following manuals are intended for usage by administrators: "General Settings Guide", "Security Reference", "Notes for Security Functions", "About This Machine", and "Notes for Administrators: Using this Machine in a CC-Certified Environment". All other manuals are for general users.

The person responsible for acquiring this machine must appoint competent personnel as the machine supervisor and 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.



BZA020

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	D092-7704
Safety Information for Aficio MP 4001/Aficio MP 5001 (or Safety Information for MP 4001/MP 5001)	D092-7700 (or D092-7701)
Notes for Users	D092-7726
App2Me Start Guide	D085-7904B

❖ Manuals on CD-ROM

Manual Name	Reference Number
Manuals for Users MP 4001/5001 Aficio MP 4001/5001 A	D092-7510
Manuals for Administrators Security Reference MP 4001/5001 Aficio MP 4001/5001	D092-7512
Manuals for Administrators Security Reference Supplement 9240/9250 MP 4001/5001 LD140/LD150 Aficio MP 4001/5001	D092-7790
VM Card Manuals	D377-7500

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 machine 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 Press [System Settings].

3 Press [Administrator Tools].

4 Press [Firmware Version].

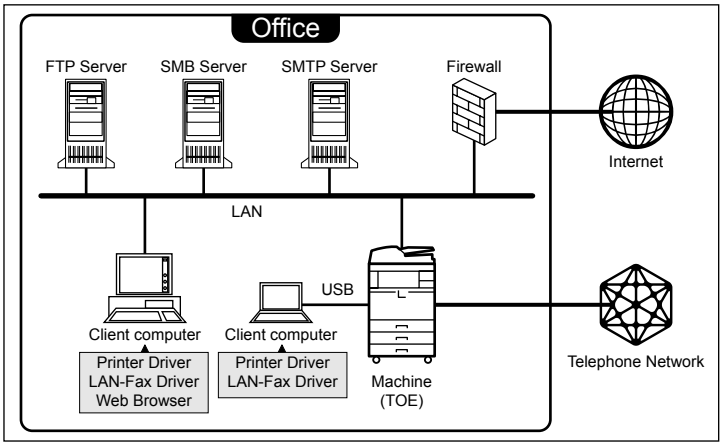
CC Conformant Firmware Versions

Software	System/Copy	1.00
	Network Support	7.29.3
	Scanner	01.24
	Printer	1.00
	Fax	01.00.00
	Web Support	1.00.1
	Web Uapl	1.02
	Network DocBox	1.00
Hardware	Ic Key	1100
	Ic Hdd	01
Option	GWFCU3-19(WW)	01.00.00

Example CC Conformant Environment

This machine can be connected to other devices through a network, over a telephone line, or directly via USB. 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.
- ❒ For print jobs and fax transmissions from the client computer, use IP-SSL authentication.
- ❒ IP-Fax and Internet Fax are not CC conformant. Do not use them.
- ❒ Use Windows Internet Explorer 6.0 or 7.0 as the Web browser.
- ❒ Use PCL Driver Ver. 1.0.0.0 or later and LAN-Fax Driver Ver. 1.61 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:

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 accessed in steps ⓭, ⓮, ⓯, ⓰, and ⓳ of "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]**. To send data to the shared folder, set SMB to **[Active]**.
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 SettingsTray 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 **[Off]**. If you set this to **[On]**, the addresses of users other than the user administrator cannot be registered. However, in this case, the password can only be changed by the user administrator.

Reference

For details about specifying "Restrict Adding of User Destinations", see "Preventing Data Leaks Due to Unauthorized Transmission", Security Reference.

⑤ Be sure to specify the following settings also:

Tab	Item	Procedure
Administrator Tools (*)	Extended Security / Settings by SNMPv1 and v2	Set this to **[Prohibit]**.
Administrator Tools (*)	Extended Security / Restrict Use of Simple Encryption	Set this to **[Off]**.
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]**.

Reference

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

⑥ 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.

⑦ Be sure to specify the following settings also:

Tab	Item	Procedure
Timer Settings	Set Date / Set Time	Set this to the current date and time.

Reference

For details about specifying "Set Date / Set Time", see "Timer Settings", General Settings Guide.

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 [Scanner Features].**

   Specify the following settings:

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

   Reference

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

8. **Press [Exit] twice.**

9. **Log off.**

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

   ```
   % telnet IP_address
   ```

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

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

   ```
   msh> set rfu down
   ```

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

   ```
   msh> set nrs down
   ```

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

   ```
   msh> logout
   ```

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

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

8. **Disconnect the machine from the administrators-only network, and then connect it to the general use network.**

   Reference

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

Settings to Specify Using Web Image Monitor

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

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

4 Click [Configuration].

5 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]**.

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

7 Click [Configuration].

8 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]**.

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

10 Click [Configuration].

11 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]**.

⓬ Use the following procedure to install the device certificate.

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 ⓬.1.3.

② Select **[Certificate1]** for "IPsec".

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

④ Click **[OK]**.

13 Use the following procedure to enable SSL.

① Click **[SSL/TLS]** in "Security".

② In "SSL/TLS", set "IPv4" to **[Active]**.

③ Set "Permit SSL/TLS Communication" to **[Ciphertext Only]**.

④ Click **[OK]**.
Wait a while for the machine to reset itself.

⑤ Click **[OK]**.

14 Use the following procedure to specify the network security level.

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

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

③ In "Port 80" in "HTTP" in the "TCP/IP" list, set "IPv4" and "IPv6" to **[Close]**.
If you do this, "IPv4" and "IPv6" in "Port 80" in "IPP" are also automatically set to **[Close]**.

④ Set "IPv4" and "IPv6" in "FTP" to **[Inactive]**.

⑤ Set "IPv4" in "sftp" to **[Inactive]**.

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

⑦ Set "SNMPv3 Function" in "SNMP" to **[Inactive]**.

⑧ 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 "SNMPv3 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.

⑨ Click **[OK]**.

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

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

② Set "Collect Job Logs" in "Job Log" to **[Active]**.

③ Set "Job Log Collect Level" to **[Level 1]**.

④ Set "Collect Access Logs" in "Access Log" to **[Active]**.

⑤ Set "Access Log Collect Level" to **[Level 2]**.

⑥ Click **[OK]**.
Wait a while for the machine to reset itself.

⑦ Click **[OK]**.

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 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 In "Digest Algorithm" in "Signature", select the digest algorithm to be used for the signature.

④ Set "When Sending E-mail by Scanner" in "Signature" to **[Use Signatures]**.

⑤ Set "When Transferring Files Stored in Document Server (Utility)" in "Signature" to **[Use Signatures]**.

⑥ Click **[OK]**.

19 Use the following procedure to disable JavaVM.

① In "Extended Feature Settings", click **[Startup Setting]**.

② If "Stop" does not appear in the "Status" column for "JavaVM", click the corresponding radio button in the "Selection" column, and then click **[Start Up/Stop]**.
"Stop" will appear in the "Status" column.

③ Click **[Back]**.

20 Log off, and then quit Web Image Monitor.

21 Turn off the main power.

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

22 Disconnect the machine from the administrators-only network, and then connect it to the general use network.

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 machine administrator intends to reconfigure the device certificate or change the e-mail address specified for the device certificate, machine operation must first be suspended.
- 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 user 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.
- Be sure to instruct users to select only registered folders as Scan to Folder destinations.
- 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 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, the administrator must instruct users to encrypt their files when sending them by Scan to Folder.
- When configuring a device certificate, be sure to specify **[Encrypt All]** as its encryption setting. In the Address Book, a symbol identifies destinations for which **[Encrypt All]** has been specified. Be sure to send e-mail only to destinations for which **[Encrypt All]** has been specified (identifiable by the symbol). Do not send e-mails to users not registered in the Address Book.
- 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 user administrator using Web Image Monitor.

  Reference

  For details about installing the user certificate, see "E-mail Encryption", Security Reference.
- To install the LAN-Fax driver, enter the IP address as follows (also described in "Installing Individual Applications", Facsimile Reference)
  https://(machine's IP address)/printer
- Use the LAN-Fax driver under Windows XP only.
- Service Mode operations have not been rated for CC conformance.
- 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.

② Ensuring Information Security

- Protecting Stored Files from Unauthorized Access
- Protecting Stored Files from Theft
- 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.
If you want to print a stored fax prior to sending it, be sure to print it from the Document Server menu. Do not print it from the fax menu.

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

Specify each user's access restriction setting for basic authentication.
Each user can be assigned only one administrator role. Assign a different person to each administrator role.

④ Enhanced Network Security

- Safer Communication Using SSL, SNMPv3 and IPsec

Use SSL and IPsec for encrypted data communication.

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

❒ If "Password Policy" is enabled, "Failed" will appear in the "Password Change" log entry each time you create a new administrator using the control panel.

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 fax unit is included in the CC certification coverage. The following options are required for CC conformance:

- HDD Encryption Unit Type A

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

- Memory Unit Type B
- Copy Data Security Unit Type F
- DataOverwriteSecurity Unit Type I
- Gigabit Ethernet Board Type A
- ARDF DF3010
- Platen Cover Type 3800C
- Finisher SR790
- Booklet Finisher SR3020
- Finisher SR3030
- Paper Feed Unit PB3040
- LCIT PB3050
- LCIT RT3000
- Bridge Unit BU3030
- 1 Bin Tray BN3040
- Hand Set Type 1018