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. Note that CC certification has been obtained for English language environments only, but the information that follows is valid for operating systems of any language.

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.

We recommend the purchaser of this machine to instruct every administrator and supervisor of the machine to read the above listed administrator manuals.

Before Applying the Security Functions

Before applying any security functions, administrators must read "Security Reference Errata: Getting Started" and fully understand its content. This document is contained in the "Notes for Security Functions".

Also, administrators must also use the following procedure to check the firmware and hardware versions for CC compliance.

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-Compliant Firmware Versions

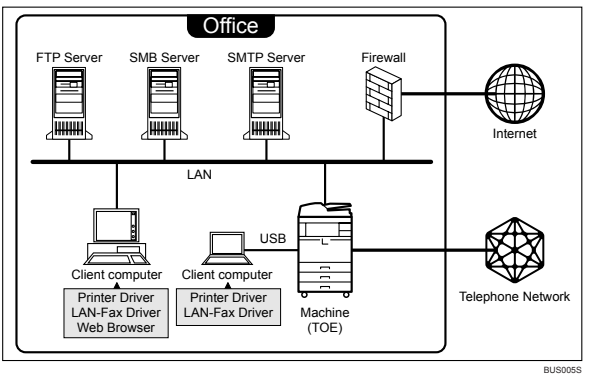
Software	System/Copy	1.14
	Network Support	7.23
	Scanner	01.11
	Printer	1.05
	Fax	05.00.00
	Web Support	1.52
	Web Uapl	1.10
	Network DocBox	1.10C
Hardware	Ic Key	1100
	Ic Hdd	01

Example CC-Compliant 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.

To meet the requirements of the CC certification, client computers must be running a Web browser that is compatible with Windows.

Normal telephone fax lines have been rated as CC-compliant for faxing. IP-SSL-authenticated print jobs and fax transmissions from the client computer are CC-compliant.



Important

- ❒ The CC compliance standard stipulates that installation be performed by an authorized service representative.
- ❒ Versions of Internet Explorer from 6.0 onward are rated as CC certification-compliant.
- ❒ Use RPCS Driver Ver. 7.67 or later and LAN-Fax Driver Ver. 1.60 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 revision to the CC-compliant revisions of the driver.
- ❒ The character set (for user login and administrator passwords) rated for CC certification-compliance is ASCII.
- ❒ The @Remote Service does not meet CC-compliance standards.
- ❒ IP-Fax and Internet Fax are not rated for CC-compliance.

Settings

Before using the machine, specify the following settings:

Also, to keep your environment CC-compliant, configure the following settings and make sure they are not changed after operations begin.

Settings to Specify Using the Control Panel

1 Turn the machine on.

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

3 Press the [User Tools/Counter] key.

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	To specify the machine's static DNS server, press **[Specify]**, and then enter the IPv4 address in "DNS Server 1", "DNS Server 2", and "DNS Server 3". (Enter the IPv4 address in "DNS Server 2" and "DNS Server 3" if required.) To automatically obtain the DNS server's address 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 **[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]**.
Administrator Tools	Extended Security / Change Firmware Structure	Set this to **[Prohibit]**.

Reference

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

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 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 Click [Program/Change Administrator] in the "Device Settings" group, and then click [Change] in the "Login Password" field in "Administrator 1".

Enter the changed password in "New Password" and "Confirm Password", and then click **[OK]**.

Click **[OK]**.

An Authentication Error message appears. Click **[OK]**.

6 Log on as the supervisor.

7 Click [Configuration].

8 Click [Program/Change Administrator] in the "Device Settings" group, and then click [Change] in the "Login Password" field in "Supervisor".

Enter the changed password in "New Password" and "Confirm Password", and then click **[OK]**.

Click **[OK]**.

An Authentication Error message appears. Click **[OK]**.

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

10 Click [Configuration].

11 Click [E-mail] in "Device Settings".

Enter the administrator's e-mail address in "Administrator E-mail Address".

Enter the SMTP server name (or IP address) in "SMTP Server Name".

Click **[OK]**.

12 Click [Device Certificate] in "Security".

The procedures for <Installing the Certificate Issued by the Certificate Authority> and <Creating the Certificate with the Machine> are different.

❖ **Installing the Certificate Issued by the Certificate Authority**

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

① Select the certificate 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]**.

② 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.

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, and then click **[OK]**.
Wait a while for the machine to reset itself.

④ Click **[OK]**.
(The machine requests the certificate. Wait a while for the machine to become usable.)

⑤ Click **[Details]** next to the number of requested certificate.

⑥ Using the text displayed in the "Text for Requested Certificate" field, request the certificate authority to issue the certificate.
For details about the certificate issuance, ask the certificate authority.

⑦ Click **[Back]**.

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

① Click **[Install]** to install from the certificate list.

② In the "Certificate Request" box, enter the text of the device certificate issued by the certificate authority, and then click **[OK]**.

Select the installed certificate in accordance with the following procedure:

① In "S/MIME", select the installed certificate.

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

③ Click **[OK]**.

❖ **Creating the Certificate with the Machine**

Create the certificate with the machine in accordance with the following procedure:

① From the certificate list, select the certificate to install, 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]** before clicking **[Create]**.
To select a certificate other than **[Certificate1]**, you need to specify **[Create]** for the selected certificate.

② 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, and then click **[OK]**.

③ Click **[OK]**.
The machine creates the certificate. Wait a while for the machine to become usable.

Select the installed certificate in accordance with the following procedure:

① In "S/MIME", select the installed certificate.

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

③ Click **[OK]**.

13 Click [SSL/TLS] in "Security".

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

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

Click **[OK]**.

Wait a while for the machine to reset itself.

⓮ Click [Network Security] in "Security".

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

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]**.)

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

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

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

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

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.

⓯ Click [Logs] in "Device Settings".

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

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

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

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

Click **[OK]**.

⓰ Click [User Lockout Policy] in "Security".

Set "Lockout" to **[Active]**.

Set "Number of Attempts before Lockout" to "5" or less.

Click **[OK]**.

⓱ Click [IPsec] in "Security".

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

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

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.
  (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]**.

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

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

Click **[OK]**.

⓲ Click [S/MIME] in "Security".

Set "Encryption Algorithm:" in "Encryption" to **[3DES-168 bit]**.

In "Digest Algorithm" in "Signature", select the digest algorithm that is used for the signature.

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

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

Click **[OK]**.

⓳ 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: in "Protection", "Protect Destination", click **[Change]** (next to "Access Privilege"), 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.
  Also, be sure not to register a Scan to Folder destination to a user.
  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).
  Only users whose login user names are registered in the address book are CC-compliant 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 "Email Encryption", Security Reference.

- To install the LAN-Fax driver, enter the IP address as follows (also described in "Fax Reference Errata", Notes for Security Functions)
  https://(machine's IP address)/printer
  The LAN-Fax driver is CC-compliant under Windows XP.
- Service Mode operations are not CC-certified.
- 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

Compliance 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

② Ensuring Information Security
- Protecting Stored Files from Unauthorized Access
- Protecting Stored Files from Theft
- Using S/MIME to Protect Email Transmission
  Documents from the scanner function that are saved on the machine meet CC-compliance standards.
- Protecting Registered Information in the Address Book
  Address Book backup and restoration are not CC-certified functions.
- Managing Log Files
  Downloading log data via Web Image Monitor is CC-compliant.
- Encrypting Data on the Hard Disk

The printer's Locked Print, Sample Print, Stored Print, and Hold Print functions do not meet CC-compliance standards.
If you want to print a stored fax prior to sending it, be sure to print it from the Document Server screen.

③ Limiting and Controlling Access
- Preventing Modification or Deletion of Stored Data
  Modification of stored data is not a CC-compliant function.
- Preventing Modification of Machine Settings

The feature allowing administrators to specify and manage each user's access restriction setting is CC-compliant.

④ Enhanced Network Security
- Safer Communication Using SSL, SNMPv3 and IPsec

SSL and IPsec have been rated as CC-compliant methods of encryption.

⑤ Other Security Functions

- Service Mode Lock

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.

❒ For maximum usability, this machine is designed to automatically recover from errors. 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-Compliant Environment

In a CC-compliant 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", Notes for Security Functions.

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 Notes for Security Functions:

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 Notes for Security Functions:

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, but configurations that do not include the fax unit are also included in the CC certification coverage. The following options are also included in the CC certification coverage.

- Hard Disk Drive Option Type 5000
- HDD Encryption Unit Type A

Use of the following options does not affect CC compliance.

- Copy Data Security Unit Type F
- DataOverwriteSecurity Unit Type I
- 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
- Key Counter Bracket Type H

Errata

Please note the following corrections to these manuals.

❖ Notes for Security Functions

Topic	Additional Description
Managing Log Files >Attributes of Logs you can Download ❖ **Access Log Information Items**	Item **【Error】** User Lockout Policy **【Corrections】** Lockout/Release

Printed in China
EN GB EN US EN AU D019-7955
D0197955