Notes for Administrator:

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

For safe and correct use, be sure to read the Safety Information in "Read This First" before using the machine.

TABLE OF CONTENTS

1. Notes for Administrators

1. Notes for Administrators

Introduction

This product is a multifunction printer (MFP) certified in an operating environment complying with the requirements of the Common Criteria for Information Technology Security Evaluation (CC certification). Be sure to read the booklet carefully and understand its contents thoroughly.

The official name of IEEE Std. 2600.1^{TM}-2009 is 2600.1, Protection Profile for Hardcopy Devices, Operational Environment A (Version: 1.0, dated June 2009).

Before Applying the Security Functions

The person responsible for acquiring this machine must appoint competent personnel as the administrators (including the machine supervisor) and instruct them to read the administrator manuals listed below.

- Security Guide
- Getting Started
- Notes for Administrators: Using this Machine in a Network Environment Compliant with IEEE Std. 2600.1^{TM}-2009

To securely operate the machine, administrators must keep these manuals handy.

All other manuals are for general users.

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

CC-Certified Operating Environment

CC evaluation was performed under the following environment.
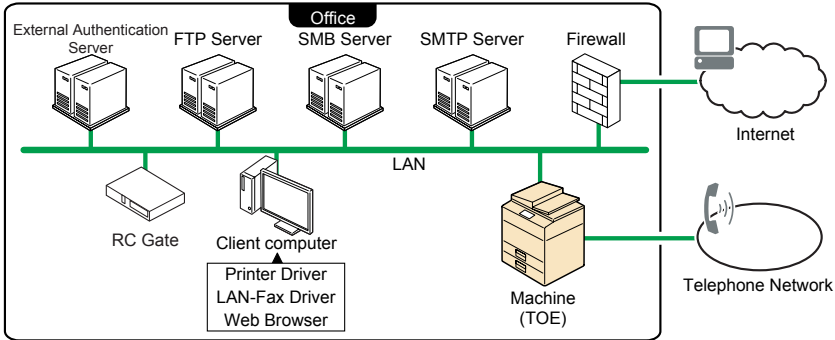
CJL010

IT Products	Names/Versions of Evaluated IT Products
External Authentication Server	Windows Server 2008 / 2008 R2
Printer Driver	PCL6 Driver Ver.1.0.0.0
LAN-Fax Driver	LAN-Fax Driver Ver.1.0.0.0
Web Browser	Internet Explorer 6.0, 7.0, 8.0, and 9.0 for Windows
RC Gate RC Gate is a device for @Remote Service.	Remote Communication Gate A Remote Communication Gate Type BN1 Remote Communication Gate Type BM1

⭐**Important**

- You can connect necessary IT products to the MFP over the network or telephone line in your operating 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.

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

1

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

  - https://(machine's IP address or host name)/printer

- To install the printer driver, enter the machine's IP address or host name in the [URL:] box as follows (also described in "Using the IPP Port" in "Installing the Printer Driver for the Selected Port", Driver Installation Guide):

  - https://(machine's IP address or host name)/printer

Checking Versions for CC Conformance

The version of CC-certified target of evaluation (TOE) is E-1.00. The versions of the firmware and hardware corresponding to version E-1.00 TOE are shown below. When using an MFP, you can display the firmware and hardware versions.

Primary Classification	Secondary Classification	Version
Firmware	System/Copy	1.02
	Network Support	12.68
	Fax	01.01.00
	RemoteFax	01.01.00
	NetworkDocBox	1.00
	Web Support	1.10.1
	Web Uapl	1.00.1
	animation	6.00
	Scanner	01.01
	Printer	1.01
	PCL	1.10
	PCL Font	1.13
	Data Erase Onb	1.03m
	GWFCU3.8-2(WW)	02.00.00
	Engine	1.11:08
	OpePanel	1.01
Hardware	Ic Key	01020714
	Ic Hdd	3330

You can check the firmware and hardware versions from the control panel as follows:

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

Manuals

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

Identifying the model

- Mainly Europe

  "-27"

- Mainly North America

  "-17" or "-18"

- Mainly Asia

  "-29"

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

1. Check the label on the rear of the machine to identify the model.
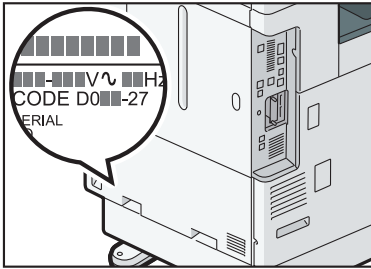
CJL019

2. Check whether the model number on the label ends with "-27".

1. Manual reference numbers for "-27" models

(Paper Manuals)

Manual Name	Reference Number
MP C3003/C3503/C4503/C5503/C6003 series Read This First	D146-7511
Notes for Security Guide	D143-7347
Notes for Users	D146-7582
SOFTWARE LICENSE AGREEMENT	D645-7901

(Manual CD-ROMs)

Manual Name	Reference Number
Manuals MP C3003/C3503/C4503/C5503/C6003 series A	D146-7883
Printer/Scanner Drivers and Utilities RICOH MP C3003/C3503 series MP C3003/C3503 series infotec MP C3003/C3503 series	D146-7854

(Online Manuals)

Manual Name	Reference Number
Notes on Security Functions	D146-7587
Notes for Administrators: Using this Machine in a Network Environment Compliant with IEEE Std. 2600.1^{TM}-2009	D146-7577

2. Manual reference numbers for "-17" or "-18" models

(Paper Manuals)

Manual Name	Reference Number
MP C3003/C3503/C4503/C5503/C6003 series User Guide	D146-7502
MP C3003/C3503/C4503/C5503/C6003 series Read This First	D146-7512
Notes for Security Guide	D143-7348
Notes for Users	D146-7581
SOFTWARE LICENSE AGREEMENT	D645-7901

(Manual CD-ROMs)

Manual Name	Reference Number
Manuals MP C3003/C3503/C4503/C5503/C6003 series	D146-7880

Manual Name	Reference Number
Printer/Scanner Drivers and Utilities RICOH MP C3003/C3503 series LANIER MP C3003/C3503 series SAVIN MP C3003/C3503 series	D146-7852

(Online Manuals)

Manual Name	Reference Number
Notes on Security Functions	D146-7587
Notes for Administrators: Using this Machine in a Network Environment Compliant with IEEE Std. 2600.1^{TM}-2009	D146-7577

3. Manual reference numbers for "-29" models

(Paper Manuals)

Manual Name	Reference Number
MP C3003/C3503/C4503/C5503/C6003 series User Guide	D146-7502
MP C3003/C3503/C4503/C5503/C6003 series Read This First	D146-7515
Notes for Security Guide	D143-7348
Notes for Users	D146-7581
SOFTWARE LICENSE AGREEMENT	D645-7901

(Manual CD-ROMs)

Manual Name	Reference Number
Manuals MP C3003/C3503/C4503/C5503/C6003 series	D146-7880
Printer/Scanner Drivers and Utilities RICOH MP C3003/C3503 series Gestetner MP C3003/C3503 series LANIER MP C3003/C3503 series	D146-7856

(Online Manuals)

Manual Name	Reference Number
Notes on Security Functions	D146-7587
Notes for Administrators: Using this Machine in a Network Environment Compliant with IEEE Std. 2600.1™-2009	D146-7577

Options

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

- Fax Option Type M3

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

- Finisher SR3140
- Booklet Finisher SR3150
- Punch Unit PU3050 NA
- Punch Unit PU3050 EU
- Punch Unit PU3050 SC
- Booklet Finisher SR3170
- Finisher SR3160
- Punch Unit PU3060 NA
- Punch Unit PU3060 EU
- Punch Unit PU3060 SC
- Internal Finisher SR3130
- Punch Unit PU3040 NA
- Punch Unit PU3040 EU
- Punch Unit PU3040 SC
- Paper Feed Unit PB3160
- Paper Feed Unit PB3150
- Caster Table Type M3
- LCIT PB3170
- LCIT RT3030
- Internal Shift Tray SH3070
- Bridge Unit BU3070
- 1 Bin Tray BN3110

- Side Tray Type M3
- Handset HS3020
- ADF Handle TypeC
- Copy Data Security Unit Type G
- Waste Toner Bottle MP C6003
- Unicode Font Package for SAP® 1 License
- Unicode Font Package for SAP® 10 License
- Unicode Font Package for SAP® 100 License

Preparation for Use

To use the MFP in a CC-certified operating environment, the administrator must perform the procedures described on page 12 "Specifying the MFP Settings" and page 31 "Checking the MFP Settings" in advance.

The administrator should read the MFP manual thoroughly before performing the procedures described on page 12 "Specifying the MFP Settings" and page 31 "Checking the MFP Settings".

Specifying the MFP Settings

This section explains how to specify the MFP settings to establish a CC-certified operating environment.

The administrator must specify the MFP settings using the control panel and Web Image Monitor according to the following procedures.

Before specifying the machine settings, log in as the administrator. For details about logging in, see "Administrator Login Method" in "Getting Started", Security Guide.

Procedure 1: Settings to Specify Using the Control Panel

Using the control panel, specify [System Settings], [Copier / Document Server Features], [Printer Features], [Scanner Features], [Facsimile Features], and [User Authentication Management] in the User Tools menu so that they are in the CC-certified ranges.

For details about configuring settings in the User Tools menu, see "Accessing User Tools" in "Read This First", Connecting the Machine/ System Settings.

1. Specifying [System Settings] (1)

The administrator must specify the settings in [System Settings] within the ranges shown in the table on the following page.

For details about how to specify the settings, see "System Settings", Connecting the Machine/ System Settings.

⭐**Important**

- If you set "User Authentication Management" to [Windows Auth.], as described on page 15 "2. Specifying [User Authentication Management]", do not use the server name registered in the Windows server for any of "Administrator 1-4" or "Supervisor" in "Program / Change Administrator".

- To change the supervisor's "Login User Name" and "Login Password", log in as the supervisor.

1

Tab	Item	Settings
Timer Settings	Auto Logout Timer	Select [On], and then set the range for the timer between 60-999 seconds.
Interface Settings	Network ▶Machine IPv4 Address	• Specifying a static IPv4 address Enter the IPv4 address and subnet mask. • Obtaining the DHCP server address automatically Select [Auto-Obtain (DHCP)].
Interface Settings	Network ▶IPv4 Gateway Address	Enter the IPv4 gateway address.
Interface Settings	Network ▶DNS Configuration	Specify this only if you are using a static DNS server. • Specifying a static DNS server Enter the IPv4 address in "DNS Server 1", "DNS Server 2", and "DNS Server 3". (Specify DNS Server 2 and 3 if required.) • Obtaining the DHCP server address automatically Select [Auto-Obtain (DHCP)].
Interface Settings	Network ▶Effective Protocol ▶IPv4	[Active]
Interface Settings	Network ▶Effective Protocol ▶IPv6	[Inactive]
Interface Settings	Network ▶IEEE 802.1X Authentication for Ethernet	[Inactive]
File Transfer	Delivery Option	[Off]

Tab	Item	Settings
Administrator Tools	Media Slot Use ▶Store to Memory Device	[Prohibit]
Administrator Tools	Media Slot Use ▶Print from Memory Storage Device	[Prohibit]
Administrator Tools	Administrator Authentication Management ▶User Management	Set [Admin. Authentication] to [On], and then select [Administrator Tools] in [Available Settings].
Administrator Tools	Administrator Authentication Management ▶Machine Management	Set [Admin. Authentication] to [On], and then select [General Features], [Tray Paper Settings], [Timer Settings], [Interface Settings], [File Transfer], and [Administrator Tools] in [Available Settings].
Administrator Tools	Administrator Authentication Management ▶Network Management	Set [Admin. Authentication] to [On], and then select [Interface Settings], [File Transfer], and [Administrator Tools] in [Available Settings].
Administrator Tools	Administrator Authentication Management ▶File Management	Set [Admin. Authentication] to [On], and then select [Administrator Tools] in [Available Settings].
Administrator Tools	Program / Change Administrator ▶Administrator 1-4	Specify settings for one or more administrators. Specify the administrator's "Login User Name" and "Login Password". Assign all administrator roles (user administrator, machine administrator, network administrator, and file administrator) to a single administrator.
Administrator Tools	Program / Change Administrator ▶Supervisor	Change the supervisor's "Login User Name" and "Login Password".

2. Specifying [User Authentication Management]

The administrator must specify the settings in [User Authentication Management] in [System Settings] within the ranges shown in the following table.

For details about how to specify the settings, see "System Settings", Connecting the Machine/ System Settings.

⭐Important

- Set [User Authentication Management] to [Basic Auth.] or [Windows Auth.].

1. Specifying [Basic Auth.]

Tab	Item	Settings
Administrator Tools	User Authentication Management	[Basic Auth.]
Administrator Tools	User Authentication Management ▶Basic Auth. ▶Available Functions	Specify this in accordance with your operating environment. Do not set this to [Browser].
Administrator Tools	User Authentication Management ▶Basic Auth. ▶Printer Job Authentication	[Entire]

2. Specifying [Windows Auth.]

Tab	Item	Settings
Administrator Tools	Program / Change / Delete Realm ▶Program / Change	Specify "Realm Name", "KDC Server Name", and "Domain Name".
Administrator Tools	User Authentication Management	[Windows Auth.]
Administrator Tools	User Authentication Management ▶Windows Auth. ▶Kerberos Authentication	[On] Select the realm applied to Kerberos authentication.

Tab	Item	Settings
Administrator Tools	User Authentication Management ▶Windows Auth. ▶Printer Job Authentication	[Entire]
Administrator Tools	User Authentication Management ▶Windows Auth. ▶Use Secure Connection (SSL)	[On]
Administrator Tools	User Authentication Management ▶Windows Auth. ▶Group ▶Program / Change ▶* Default Group ▶Available Functions	Uncheck all items. Do not use the global group. You can specify the functions available to users during or after user registration. However, do not include [Browser] in the functions available to users.

3. Specifying [System Settings] (2)

The administrator must specify the settings in [System Settings] within the ranges shown in the table on the following page.

For details about how to specify the settings, see "System Settings", Connecting the Machine/ System Settings.

Tab	Item	Settings
Administrator Tools	Extended Security ▶Restrict Display of User Information	[On]
Administrator Tools	Extended Security ▶Restrict Adding of User Destinations (Fax)	[On]

1

Tab	Item	Settings
Administrator Tools	Extended Security ▶Restrict Adding of User Destinations (Scanner)	[On]
Administrator Tools	Extended Security ▶Restrict Use of Destinations (Fax)	[On]
Administrator Tools	Extended Security ▶Restrict Use of Destinations (Scanner)	[On]
Administrator Tools	Extended Security ▶Transfer to Fax Receiver	[Prohibit]
Administrator Tools	Extended Security ▶Authenticate Current Job	[Access Privilege]
Administrator Tools	Extended Security ▶@Remote Service	Select [Proh. Some Services] if you use @Remote Service. Otherwise, select [Prohibit]. Do not set this to [Do not Prohibit].
Administrator Tools	Extended Security ▶Update Firmware	[Prohibit]
Administrator Tools	Extended Security ▶Change Firmware Structure	[Prohibit]

Tab	Item	Settings
Administrator Tools	Extended Security ▶Password Policy	Set "Complexity Setting" to [Level 1] or [Level 2], press [Change] on the right of "Minimum Character No.", and then set the number of characters to 8 or more. For example, to set the number of characters to 8, press the number key "8", and then "#". Even if you change the password policy, passwords that have already been registered can still be used. The changed password policy will be applied only to passwords specified or changed subsequently.
Administrator Tools	Extended Security ▶Security Setting for Access Violation	[Off]
Administrator Tools	Auto Delete File in Document Server	Select [On] or [Off].
Administrator Tools	LDAP Search	[Off]
Administrator Tools	Service Mode Lock	[On]
Administrator Tools	Auto Erase Memory Setting	Select [On], and then select [NSA], [DoD], or [Random Numbers]. If you set this to [Random Numbers], set [Number of Erase] to three or more.
Administrator Tools	Transfer Log Setting	[Off]
Administrator Tools	Machine Data Encryption Settings	Ensure that the current data has been encrypted. If the data has been encrypted, the following message will appear: "The current data in the machine has been encrypted."
Administrator Tools	Stop Key to Suspend Print Job	[Only Job Being Operated]

4. Specifying [Copier / Document Server Features]

The administrator must specify the settings in [Copier / Document Server Features] within the ranges shown in the following table.

For details about how to specify the settings, see "Copier / Document Server Features", Copy/ Document Server.

Tab	Item	Settings
Administrator Tools	Menu Protect	[Level 2]

5. Specifying [Printer Features]

The administrator must specify the settings in [Printer Features] within the ranges shown in the following table.

For details about how to specify the settings, see "Printer Features", Print.

Tab	Item	Settings
Data Management	Menu Protect	[Level 2]
Data Management	Auto Delete Temporary Print Jobs	Select [On] or [Off].
Data Management	Auto Delete Stored Print Jobs	Select [On] or [Off].
System	Jobs Not Printed As Machn. Was Off	[Do not Print]

6. Specifying [Scanner Features]

The administrator must specify the settings in [Scanner Features] within the ranges shown in the following table.

For details about how to specify the settings, see "Scanner Features", Scan.

Tab	Item	Settings
Initial Settings	Menu Protect	[Level 2]
General Settings	Print & Delete Scanner Journal	[Do not Print: Delete Oldest] or [Do not Print: Disable Send]

7. Specifying [Facsimile Features]

The administrator must specify the settings in [Facsimile Features] within the ranges shown in the following table.

For details about how to specify the settings, see "Facsimile Features", Fax.

Tab	Item	Settings
Initial Settings	Menu Protect	[Level 2]
General Settings	Box Setting	Set all items to [* Not Programmed].
Send Settings	Backup File TX Setting	[Off]
Reception Settings	Reception File Settings ▶Store	[On]
Reception Settings	Reception File Settings ▶Forwarding	[Off]
Reception Settings	Reception File Settings ▶Print	[Off]
Reception Settings	Reception File Settings ▶Memory Lock Reception	[Off]
Initial Settings	Parameter Setting ▶switch 40, bit 0	[1] If the memory for stored received faxes become full, the MFP stops receiving new faxes and keeps the stored ones without printing or deleting them.
Initial Settings	Parameter Setting ▶switch 10, bit 0	[1] Only users who are authorized by the administrator can access, from the control panel, received faxes that are stored.
Initial Settings	Parameter Setting ▶switch 04, bit 7	[0] If this is enabled, previews will not be included in the reports.
Initial Settings	Internet Fax Setting	[Off]
Initial Settings	Email Setting	[On]

1

Tab	Item	Settings
Initial Settings	Folder Setting	[On]

Procedure 2: Settings to Specify Using Web Image Monitor

It is necessary to specify the values in [Device Settings], [Printer], [Fax], [Interface], [Network], [Security] and [Webpage] in [Configuration] in [Device Management] of Web Image Monitor within the CC-certified range.

Before specifying system settings, the administrator should refer to the Web Image Monitor help. The CC-certified Web Image Monitor help can be downloaded from the following URL:

http://support-download.com/services/device/webhlp/nb/gen/v140cc1/en/

The help that appears when the "?" icon (Help button) in Web Image Monitor's header area is clicked may have changed after receiving CC evaluation.

Before specifying the settings, install the Web browser specified in "CC-Certified Operating Environment" in this manual on the client computer, and then connect the client computer and MFP to the network that can be accessed only by the administrator.

For details about how to launch Web Image Monitor, see "Using Web Image Monitor" in "Monitoring and Configuring the Machine", Connecting the Machine/ System Settings.

1. Specifying [Device Settings]

The administrator must specify the settings in [Device Settings] within the ranges shown in the following table.

⭐ **Important**

- Set "Kerberos Authentication" ▶ "Encryption Algorithm" to the values specified when setting "User Authentication Management" to [Windows Auth.], as described on page 15 "2. Specifying [User Authentication Management]"".

Category	Item	Settings
Device Settings	Date/Time ▶Set Date	Set the appropriate date.
Device Settings	Date/Time ▶Set Time	Set the appropriate time.
Device Settings	Date/Time ▶Time Zone	Set the appropriate time zone.

1. Notes for Administrators

1

Category	Item	Settings
Device Settings	Logs ▶Collect Job Logs	[Active]
Device Settings	Logs ▶Job Log Collect Level	[Level 1]
Device Settings	Logs ▶Collect Access Logs	[Active]
Device Settings	Logs ▶Access Log Collect Level	[Level 2]
Device Settings	Email ▶Administrator Email Address	Enter the administrator's email address.
Device Settings	Email ▶SMTP Server Name	Enter the SMTP server name or IP address.
Device Settings	Kerberos Authentication ▶Encryption Algorithm	Check "AES256-CTS-HMAC-SHA1-96", "AES128-CTS-HMAC-SHA1-96", "DES3-CBC-SHA1", and "RC4-HMAC", and uncheck "DES-CBC-MD5".

2. Specifying [Printer]

The administrator must specify the settings in [Printer] within the ranges shown in the following table.

Category	Item	Settings
Printer	Basic Settings ▶Virtual Printer	[Inactive]

3. Specifying [Fax]

The administrator must specify the settings in [Fax] within the ranges shown in the following table.

1

Category	Item	Settings
Fax	IP-Fax Settings ▶Enable H.323	[Off]
Fax	IP-Fax Settings ▶Enable SIP	[Off]
Fax	Parameter Settings ▶LAN-Fax Result Report	[Off]

4. Specifying [Interface]

The administrator must specify the settings in [Interface] within the ranges shown in the following table.

Category	Item	Settings
Interface	Interface Settings ▶USB	[Inactive]

5. Specifying [Network]

The administrator must specify the settings in [Network] within the ranges shown in the following table.

Category	Item	Settings
Network	IPv4 ▶LLMNR	[Inactive]

6. Specifying [Security]

The administrator must specify the settings in [Security] within the ranges shown in the following table.

⭐**Important**

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

- If the FTP or SNMP function is set to [Inactive], some functions become unavailable. For details about the functions that become unavailable, see "Enabling and Disabling Protocols" in the Security Guide.

1

- For details about how to specify Device Certificate, see "Protecting the Communication Path via a Device Certificate", Security Guide.
- For details about specifying IPsec, see "Configuring IPsec", Security Guide.

Category	Item	Settings
Security	Device Certificate ▶Certificate 1 ▶Create	Configure this to create and install the device certificate (self-signed certificate). If you are using a certificate issued by the certificate authority, you do not need to configure this setting. Of the settings for the device certificate (self-signed certificate), set "Algorithm Signature" to one of the following: • sha512WithRSA-4096 • sha512WithRSA-2048 • sha256WithRSA-4096 • sha256WithRSA-2048 • sha1WithRSA-2048 • sha1WithRSA-1024

1

Category	Item	Settings
Security	Device Certificate ▶Certificate 1 ▶Request	Configure this to create the request form for the certificate authority to issue the device certificate. If you are using a self-signed device certificate, you do not need to configure this setting. Of the settings for the device certificate (certificate issued by the certificate authority), set "Algorithm Signature" to one of the following: • sha512WithRSA-4096 • sha512WithRSA-2048 • sha256WithRSA-4096 • sha256WithRSA-2048 • sha1WithRSA-2048 • sha1WithRSA-1024 Submit the application form to request that the certificate authority issue the device certificate. The request method depends on the certificate authority. For details, contact the certificate authority. You can install the certificate issued by the certificate authority via Web Image Monitor.
Security	Device Certificate▶Install	To use the device certificate (issued by the certificate authority), install the certificate by configuring this setting. If using the intermediate certificate as well, install that too.
Security	Device Certificate ▶Install Intermediate Certificate	When using an intermediate certificate, configure this setting to install the certificate.

Category	Item	Settings
Security	Device Certificate ▶Certification ▶S/MIME	Select the installed device certificate.
Security	Device Certificate ▶Certification ▶IPsec	Select the installed device certificate.
Security	Network Security ▶Security Level	[FIPS 140] After setting this to [FIPS 140], be sure to click [OK].
Security	Network Security ▶TCP/IP ▶IPv6	[Inactive]
Security	Network Security ▶HTTP - Port 80 ▶IPv4	[Close] Doing this will also set "IPv4" to [Close] in "Port 80" in "IPP".
Security	Network Security ▶SSL/TLS Version	Set "TLS1.2", "TLS1.1", "TLS1.0", and "SSL3.0" to [Active].
Security	Network Security ▶Encryption Strength Setting	Check "AES", "3DES", and "RC4".
Security	Network Security ▶FTP ▶IPv4	[Inactive]
Security	Network Security ▶sftp ▶IPv4	[Inactive]
Security	Network Security ▶ssh ▶IPv4	[Inactive]

Category	Item	Settings
Security	Network Security ▶WSD (Device) ▶IPv4	[Inactive]
Security	Network Security ▶WSD (Printer) ▶IPv4	[Inactive]
Security	Network Security ▶WSD (Scanner) ▶IPv4	[Inactive]
Security	Network Security ▶SNMP	[Inactive]
Security	S/MIME ▶Encryption Algorithm	Select [AES-128 bit] or [3DES-168 bit]. When using S/MIME, it is necessary to register the user certificate.
Security	S/MIME ▶Digest Algorithm	Select [SHA-512 bit], [SHA-384 bit], [SHA-256 bit] or [SHA1].
Security	S/MIME ▶When Sending Email by Scanner	[Use Signatures]
Security	S/MIME ▶When Transferring by Fax	[Use Signatures]
Security	S/MIME ▶When Sending Email by Fax	[Use Signatures]
Security	S/MIME ▶When Emailing TX Results by Fax	[Use Signatures]

1

Category	Item	Settings
Security	S/MIME ▶When Transferring Files Stored in Document Server (Utility)	[Use Signatures]
Security	IPsec ▶IPsec	Select [Active] or [Inactive]. If you set this to [Inactive], do not use Scan to Folder, and delete Scan to Folder destinations registered in the address book.
Security	IPsec ▶Encryption Key Auto Exchange Settings ▶Address Type	[IPv4]
Security	IPsec ▶Encryption Key Auto Exchange Settings ▶Local Address	The machine's IP address
Security	IPsec ▶Encryption Key Auto Exchange Settings ▶Remote Address	Connected server's IP address
Security	IPsec ▶Encryption Key Auto Exchange Settings ▶Security Level	[Authentication and High Level Encryption]
Security	IPsec ▶Encryption Key Auto Exchange Settings ▶Authentication Method	Select [PSK] or [Certificate].

1

Category	Item	Settings
Security	IPsec ▶Encryption Key Auto Exchange Settings ▶PSK Text	If Authentication Method has been set to [PSK], enter a character string. (Make a note of the entered character string, because it will be required when specifying the delivery server setting.)
Security	IPsec ▶Encryption Key Auto Exchange Settings ▶Hash Algorithm	Select [SHA1], [SHA256], [SHA384], or [SHA512].
Security	IPsec ▶Encryption Key Auto Exchange Settings ▶Encryption Algorithm	Select [3DES], [AES-128-CBC], [AES-192-CBC], or [AES-256-CBC].
Security	IPsec ▶Encryption Key Auto Exchange Settings ▶Diffie-Hellman Group	Select [2] or [14].
Security	IPsec ▶Encryption Key Auto Exchange Settings ▶Authentication Algorithm	Check [HMAC-SHA1-96], [HMAC-SHA256-128], [HMAC-SHA384-192] and [HMAC-SHA512-256], and uncheck [HMAC-MD5-96].
Security	IPsec ▶Encryption Key Auto Exchange Settings ▶Encryption Algorithm Permissions	Check [3DES], [AES-128], [AES-192] and [AES-256], and uncheck [Cleartext] and [DES].
Security	IPsec ▶Encryption Key Auto Exchange Settings ▶PFS	Select [2] or [14].
Security	User Lockout Policy ▶Lockout	[Active]

Category	Item	Settings
Security	User Lockout Policy ▶Number of Attempts before Lockout	1-5
Security	User Lockout Policy ▶Lockout Release Timer	[Active]
Security	User Lockout Policy ▶Lock Out User for	1-9999

7. Specifying [Webpage]

The administrator must specify the settings in [Webpage] within the ranges shown in the following table.

Category	Item	Settings
Webpage	Webpage ▶Web Image Monitor Auto Logout Settings	3-60

Procedure 3: Settings to Specify Using the Control Panel

Using the control panel, specify [System Settings] in the User Tools menu so that they are in the CC-certified ranges.

1. Specifying [System Settings] (1)

The administrator must specify the settings in [System Settings] within the ranges shown in the table on the following page.

For details about how to specify the settings, see "System Settings", Connecting the Machine/ System Settings.

Tab	Item	Settings
Interface Settings	Network ▶Effective Protocol ▶Firmware Update (IPv4)	[Inactive]

1

Tab	Item	Settings
Interface Settings	Network ▶Effective Protocol ▶Firmware Update (IPv6)	[Inactive]

2. Specifying [Facsimile Features]

The administrator must specify the settings in [Facsimile Features] within the ranges shown in the following table.

For details about how to specify the settings, see "Facsimile Features", Fax.

⭐**Important**

- Prior to this, the administrator must register in the address book the users or groups whose access to received faxes stored in the machine's memory is authorized. For details about registering data in the address book, see "Registering Addresses and Users for Facsimile/Scanner Functions", Connecting the Machine/ System Settings.

Tab	Item	Settings
Reception Settings	Stored Reception File User Setting	[On] After setting this to [On], specify the users or groups that can access stored reception files.

Checking the MFP Settings

After completing the procedure described on page 12 "Specifying the MFP Settings", check the log data and ROM version according to the following procedure.

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

1. **Check that the machine is off.**

2. **Turn the machine on.**

3. **Check the details of the log files that were stored in this machine.**

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

    Log Type: Firmware: Structure

    Result: Succeeded

Module Name: G3

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

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: B8DA)

6. **Log off.**

Changing MFP Settings During Operation

Of the settings specified before operation according to the procedure described on page 12 "Specifying the MFP Settings", the following setting can be changed even during operation.

1. Changing [System Settings] Using the Control Panel

Tab	Item	Settings
Timer Settings	Auto Logout Timer	Select [On], and then set the range for the timer between 60-999 seconds.
Interface Settings	Network ▶Machine IPv4 Address	• Specifying a static IPv4 address Enter the IPv4 address and subnet mask. • Obtaining the DHCP server address automatically Select [Auto-Obtain (DHCP)].
Interface Settings	Network ▶IPv4 Gateway Address	Enter the IPv4 gateway address.
Interface Settings	Network ▶DNS Configuration	Specify this only if you are using a static DNS server. • Specifying a static DNS server Enter the IPv4 address in "DNS Server 1", "DNS Server 2", and "DNS Server 3". (Specify DNS Server 2 and 3 if required.) • Obtaining the DHCP server address automatically Select [Auto-Obtain (DHCP)].
Administrator Tools	Program / Change Administrator ▶Administrator 1-4	Specify settings for one or more administrators. Specify the administrator's "Login User Name" and "Login Password". Assign all administrator roles (user administrator, machine administrator, network administrator, and file administrator) to a single administrator.

Tab	Item	Settings
Administrator Tools	Program / Change Administrator ▶Supervisor	Change the supervisor's "Login User Name" and "Login Password".

2. Changing [User Authentication Management] Using the Control Panel

1. Changing [Basic Auth.]

Tab	Item	Settings
Administrator Tools	User Authentication Management ▶Basic Auth. ▶Available Functions	Specify this in accordance with your operating environment. Do not set this to [Browser].

2. Changing [Windows Auth.]

Tab	Item	Settings
Administrator Tools	Program / Change / Delete Realm▶Program / Change	Specify "Realm Name", "KDC Server Name", and "Domain Name".

3. Changing [System Settings] Using the Control Panel

Tab	Item	Settings
Administrator Tools	Extended Security ▶@Remote Service	Select [Proh. Some Services] if you use @Remote Service. Otherwise, select [Prohibit]. Do not set this to [Do not Prohibit].

Tab	Item	Settings
Administrator Tools	Extended Security ▶Password Policy	Set "Complexity Setting" to [Level 1] or [Level 2], press [Change] on the right of "Minimum Character No.", and then set the number of characters to 8 or more. For example, to set the number of characters to 8, press the number key "8", and then "#". Even if you change the password policy, passwords that have already been registered can still be used. The changed password policy will be applied only to passwords specified or changed subsequently.
Administrator Tools	Auto Erase Memory Setting	Select [On], and then select [NSA], [DoD], or [Random Numbers]. If you set this to [Random Numbers], set [Number of Erase] to three or more.

4. Changing [Scanner Features] Using the Control Panel

Tab	Item	Settings
General Settings	Print & Delete Scanner Journal	[Do not Print: Delete Oldest] or [Do not Print: Disable Send]

5. Changing [Device Settings] via Web Image Monitor

Category	Item	Settings
Device Settings	Date/Time ▶Set Date	Set the appropriate date.
Device Settings	Date/Time ▶Set Time	Set the appropriate time.
Device Settings	Date/Time ▶Time Zone	Set the appropriate time zone.

Category	Item	Settings
Device Settings	Email ▶Administrator Email Address	Enter the administrator's email address.
Device Settings	Email ▶SMTP Server Name	Enter the SMTP server name or IP address.

6. Changing [Security] via Web Image Monitor

Category	Item	Settings
Security	Device Certificate ▶Certificate 1 ▶Create	Configure this to create and install the device certificate (self-signed certificate). If you are using a certificate issued by the certificate authority, you do not need to configure this setting. Of the settings for the device certificate (self-signed certificate), set "Algorithm Signature" to one of the following: • sha512WithRSA-4096 • sha512WithRSA-2048 • sha256WithRSA-4096 • sha256WithRSA-2048 • sha1WithRSA-2048 • sha1WithRSA-1024

1

Category	Item	Settings
Security	Device Certificate ▶Certificate 1 ▶Request	Configure this to create the request form for the certificate authority to issue the device certificate. If you are using a self-signed device certificate, you do not need to configure this setting. Of the settings for the device certificate (certificate issued by the certificate authority), set "Algorithm Signature" to one of the following: • sha512WithRSA-4096 • sha512WithRSA-2048 • sha256WithRSA-4096 • sha256WithRSA-2048 • sha1WithRSA-2048 • sha1WithRSA-1024 Submit the application form to request that the certificate authority issue the device certificate. The request method depends on the certificate authority. For details, contact the certificate authority. You can install the certificate issued by the certificate authority via Web Image Monitor.
Security	Device Certificate▶Install	To use the device certificate (issued by the certificate authority), install the certificate by configuring this setting. If using the intermediate certificate as well, install that too.
Security	Device Certificate ▶Install Intermediate Certificate	When using an intermediate certificate, configure this setting to install the certificate.

Category	Item	Settings
Security	Device Certificate ▶Certification ▶S/MIME	Select the installed device certificate.
Security	Device Certificate ▶Certification ▶IPsec	Select the installed device certificate.
Security	S/MIME ▶Encryption Algorithm	Select [AES-128 bit] or [3DES-168 bit]. When using S/MIME, it is necessary to register the user certificate.
Security	S/MIME ▶Digest Algorithm	Select [SHA-512 bit], [SHA-384 bit], [SHA-256 bit] or [SHA1].
Security	IPsec ▶IPsec	Select [Active] or [Inactive]. If you set this to [Inactive], do not use Scan to Folder, and delete Scan to Folder destinations registered in the address book.
Security	IPsec ▶Encryption Key Auto Exchange Settings ▶Local Address	The machine's IP address
Security	IPsec ▶Encryption Key Auto Exchange Settings ▶Remote Address	Connected server's IP address
Security	IPsec ▶Encryption Key Auto Exchange Settings ▶Authentication Method	Select [PSK] or [Certificate].

1

Category	Item	Settings
Security	IPsec ▶Encryption Key Auto Exchange Settings ▶PSK Text	If "Authentication Method" has been set to [PSK], enter a character string. (Make a note of the entered character string, because it will be required when specifying the delivery server setting.)
Security	IPsec ▶Encryption Key Auto Exchange Settings ▶Hash Algorithm	Select [SHA1], [SHA256], [SHA384], or [SHA512].
Security	IPsec ▶Encryption Key Auto Exchange Settings ▶Encryption Algorithm	Select [3DES], [AES-128-CBC], [AES-192-CBC], or [AES-256-CBC].
Security	IPsec ▶Encryption Key Auto Exchange Settings ▶Diffie-Hellman Group	Select [2] or [14].
Security	IPsec ▶Encryption Key Auto Exchange Settings ▶PFS	Select [2] or [14].
Security	User Lockout Policy ▶Number of Attempts before Lockout	1-5
Security	User Lockout Policy ▶Lock Out User for	1-9999

7. Changing [Webpage] via Web Image Monitor

Category	Item	Settings
Webpage	Webpage ▶Web Image Monitor Auto Logout Settings	3-60

Notes for Setting Up and Operation

- 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^{TM}-2009.

- The CC conformance standard stipulates that you request an authorized service representative to set up a CC-conformant environment.

- Before using the MFP, the encryption key to encrypt the data in the machine must be provided by the service representative or be newly created.

- When using Windows authentication, configure settings to force users to choose passwords that meet the criteria of being at least eight characters long and consisting of at least two of these four types of characters: upper case letters, lower case letters, numbers, and symbols. In addition, apply a lockout setting so that users will be temporarily locked out if they repeatedly enter the wrong password and so fail to log in. The temporary lockout must be set to a minute or longer, and the number of failed logins before lockout occurs must be set to up to five.

- Back up the encryption key only when the machine is not operating.

- For faxing, use the public switched telephone network. IP-Fax and Internet Fax are not CC conformant.

- For print jobs and fax transmissions from the client computer, use IPP-SSL authentication.

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

- In the event of a hard disk error, the machine displays a message asking whether or not to initialize the disk and initializes it upon receiving approval. Note however that following the hard disk initialization, user authentication might fail even though the correct password has been entered. If this happens, contact your service representative.

- "Encryption", "User Certificate", and "E-mail Address" must be specified by the administrator using Web Image Monitor. For details about installing the user certificate, see "E-mail Encryption", Security Guide.

- To send files by e-mail using the scanner or fax function, install the user certificate when registering a user in the address book 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.

- 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.

  When you register the Scan to Folder destination in the address book, click [Change] in "Access Privileges" in "Protect Destination" in "Protection", and then select [Read-only] for users who are allowed to access the Scan to Folder destination.

  Configure IPsec for the server selected as the Scan to Folder destination.

1

- Before receiving faxes, specify "Stored Reception File User Setting" in the Fax setting.

- When you configure "Program Special Sender" in the fax mode, do not specify "Forwarding per Sender" or "Memory Lock RX per Sender" before registering or changing special senders.

- The file creator (owner) has the authority to grant [Full Control] privileges to other users for stored documents in the Document Server. However, administrators should tell users that [Full Control] privileges are meant only for the file creator (owner).

- When using Windows authentication, the user login is case sensitive. You will not be able to use the machine if you make a mistake.

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

- 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.

- Obtain log files by downloading them via Web Image Monitor. 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.

- To prevent incorrect timestamps from being recorded in the audit log, ensure that the External Authentication Server or File Server that connects to the MFP is synchronized with the MFP.

- Do not use exported or imported device setting information since it is not CC-conformant.

- Do not restore the address book from an SD card, back up to the computer, or restore from the computer since these actions are not CC-conformant.

- Modification of stored file has not been rated for CC conformance.

Trademarks

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

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

- The product names of Windows XP are as follows:

  Microsoft® Windows® XP Professional

  Microsoft® Windows® XP Home Edition

  Microsoft® Windows® XP Media Center Edition

  Microsoft® Windows® XP Tablet PC Edition

- The product names of Windows Vista are as follows:

  Microsoft® Windows Vista® Ultimate

  Microsoft® Windows Vista® Business

  Microsoft® Windows Vista® Home Premium

  Microsoft® Windows Vista® Home Basic

  Microsoft® Windows Vista® Enterprise

- The product names of Windows 7 are as follows:

  Microsoft® Windows® 7 Home Premium

  Microsoft® Windows® 7 Professional

  Microsoft® Windows® 7 Ultimate

  Microsoft® Windows® 7 Enterprise

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

  Microsoft® Windows Server® 2003 Standard Edition

  Microsoft® Windows Server® 2003 Enterprise Edition

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

  Microsoft® Windows Server® 2003 R2 Standard Edition

  Microsoft® Windows Server® 2003 R2 Enterprise Edition

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

  Microsoft® Windows Server® 2008 Standard

  Microsoft® Windows Server® 2008 Enterprise

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

  Microsoft® Windows Server® 2008 R2 Standard

  Microsoft® Windows Server® 2008 R2 Enterprise

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

  Microsoft® Internet Explorer® 6

  Windows® Internet Explorer® 7

  Windows® Internet Explorer® 8

  Windows® Internet Explorer® 9

Other product names used herein are for identification purposes only and might be trademarks of their respective companies. We disclaim any and all rights to those marks.

MEMO

EN GB EN US EN AU D146-7577