



Notes for Administrators:
Using This Machine in a Network Environment
Compliant with IEEE Std 2600.2™-2009

TABLE OF CONTENTS

1. Notes for Administrators

Introduction.....	3
Before Applying the Security Functions.....	3
CC-Certified Operating Environment.....	4
MFPs Explained in This Manual.....	4
Checking Versions for CC Conformance.....	5
Manuals.....	6
Options.....	13
Preparation for Use.....	15
Specifying the MFP Settings.....	15
Procedure 1: Settings to Specify Using the Control Panel.....	15
Procedure 2: Settings to Specify Using Web Image Monitor.....	22
Procedure 3: Settings to Specify Using the Control Panel.....	30
Changing MFP Settings during Operation.....	31
Notes for Setting up and Operation.....	38
Trademarks.....	40

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 2600.2TM-2009 is U.S. Government Approved Protection Profile - U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std 2600.2TM-2009)(Version: 1.0).

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
- About This Machine
- Notes for Administrators: Using This Machine in a Network Environment Compliant with IEEE Std 2600.2TM-2009

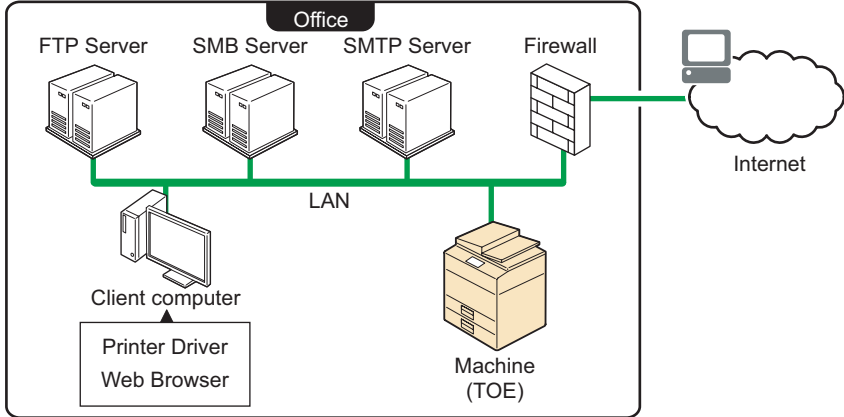
To securely operate the machine, administrators must keep these manuals handy.

All other manuals are for general users.

Before applying any security functions, administrators must read and fully understand "Before Configuring the Security Function Settings" in Security Guide.

CC-Certified Operating Environment

CC evaluation was performed under the following environment.



CJL106

IT Products	Names/Versions of Evaluated IT Products
Printer Driver	PCL6 Driver 1.2.0.0
Web Browser	Internet Explorer 9.0 and 11.0 for Windows

★ Important

- You can connect necessary IT products to the MFP over the network 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 driver. 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 website.
- 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](https://(machine's IP address or host name)/printer)

MFPs Explained in This Manual

Check the rating plate, so that the MFP you are using is included in the models listed below:

Pro C5200S, Pro C5210S

Checking Versions for CC Conformance

The version of CC-certified target of evaluation (TOE) is E-1.01. The versions of the firmware and hardware corresponding to version E-1.01 TOE are shown below. When using an MFP, you can display the firmware and hardware versions.

Machine firmware and hardware

Primary Classification	Secondary Classification	Version
Firmware	System/Copy	1.07
	OpePanel	1.02
	Web Support	1.04
	Network Support	16.46
	Scanner	01.02
	Web Uapl	1.04
	NetworkDocBox	1.00
	OpeFont	1.00
	animation	1.01
	Printer	1.02
	RPCS	3.20.20
	Font EXP	1.00

Primary Classification	Secondary Classification	Version
Firmware	PCL	1.03
	PCL Font	1.09
	PDF	1.02
	PS3 Font	1.17
	Java VM v12 std	12.49.00
	Data Erase Onb	1.05
	PowerSaving Sys	F.L3.08
	MediaLibrary	0.01
	Engine	1.11:02
	ADF	01.000:04
Hardware	Ic Ctlr	03
	Ic Key	01020d0c

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

1. Press the [User Tools] 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:

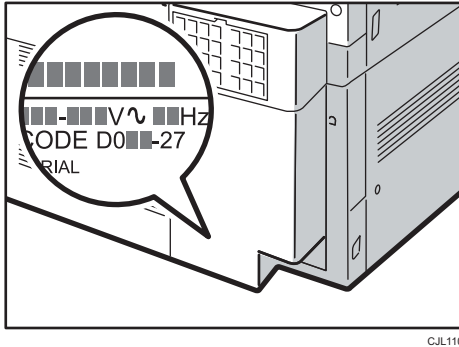
Identifying the model

- Mainly Europe
"-27"
- Mainly North America
"-17"

- 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.



CJL110

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

★ Important

- Do not use the manuals on the supplied CD-ROM.

1. Manual reference numbers for "-27" models

Paper Manuals

Manual Name	Reference Number
Read This First	D260-7002
Notes for Users	D241-7068
SOFTWARE LICENSE AGREEMENT	D241-7237
Notes for Using This Machine Safely	D195-7543A
NOTICE TO USERS	D241-7178
Notes for Users	D257-7081

Online Manuals (Website 1)

Manual Name	Reference Number
About This Machine	D260-7090
Copy/ Document Server	D260-7091
Print	D260-7092

Manual Name	Reference Number
Scan	D260-7093
Troubleshooting	D260-7094
Connecting the Machine/ System Settings	D260-7095
Security Guide	D260-7098
PostScript 3	D257-7097
Paper Settings	D260-7096
Extended Feature Settings	D260-7099

To see the listed manuals, use the computer's browser to access the following website:

https://support.ricoh.com/services/device/ccmanual/ProC5200/en/booklist/int/index_book.htm

Online Manuals (Website 2)

Manual Name	Reference Number
User Guide	D260-7087

To see the listed manuals, use the computer's browser to access the following website:

<https://support.ricoh.com/services/device/ccmanual/ProC5200/en/pdf/User.html>

Online Manuals (Website 3)

Manual Name	Reference Number
Operating Instructions Driver Installation Guide	D257-7068

To see the listed manuals, use the computer's browser to access the following website:

<https://support.ricoh.com/services/device/ccmanual/ProC5200/en/pdf/DriverInstall.html>

Online Manuals (Website 4)

Manual Name	Reference Number
About Open Source Software License	D257-7054

To see the listed manuals, use the computer's browser to access the following website:

<https://support.ricoh.com/services/device/ccmanual/ProC5200/en/pdf/Oss.html>

Online Manuals (Website 5)

Manual Name	Reference Number
Operating Instructions	D260-7088
Guide to Paper	

To see the listed manuals, use the computer's browser to access the following website:

<https://support.ricoh.com/services/device/ccmanual/ProC5200/en/pdf/GuideToPaper.html>

Online Manuals (Website 6)

Manual Name	Reference Number
Notes on Security Functions	D146-7587
Notes for Administrators: Using This Machine in a Network Environment Compliant with IEEE Std 2600.2™-2009	D260-7069

The URLs for the manuals listed above are shown in "1. Manuals Provided with This Machine", Read This First.

2. Manual reference numbers for "-17" models**Paper Manuals**

Manual Name	Reference Number
Read This First	D260-7003
SOFTWARE LICENSE AGREEMENT	D241-7237
Notes for Using This Machine Safely	D195-7543A
Notes for Users	D241-7084
NOTICE TO USERS	D241-7178

Online Manuals (Website 1)

Manual Name	Reference Number
About This Machine	D260-7090
Copy/ Document Server	D260-7091
Print	D260-7092
Scan	D260-7093

Manual Name	Reference Number
Troubleshooting	D260-7094
Connecting the Machine/ System Settings	D260-7095
Security Guide	D260-7098
PostScript 3	D257-7097
Paper Settings	D260-7096
Extended Feature Settings	D260-7099

To see the listed manuals, use the computer's browser to access the following website:

https://support.ricoh.com/services/device/ccmanual/ProC5200/en/booklist/int/index_book.htm

Online Manuals (Website 2)

Manual Name	Reference Number
User Guide	D260-7087

To see the listed manuals, use the computer's browser to access the following website:

<https://support.ricoh.com/services/device/ccmanual/ProC5200/en/pdf/User.html>

Online Manuals (Website 3)

Manual Name	Reference Number
Operating Instructions	D257-7068
Driver Installation Guide	

To see the listed manuals, use the computer's browser to access the following website:

<https://support.ricoh.com/services/device/ccmanual/ProC5200/en/pdf/DriverInstall.html>

Online Manuals (Website 4)

Manual Name	Reference Number
About Open Source Software License	D257-7054

To see the listed manuals, use the computer's browser to access the following website:

<https://support.ricoh.com/services/device/ccmanual/ProC5200/en/pdf/Oss.html>

Online Manuals (Website 5)

Manual Name	Reference Number
Operating Instructions	D260-7088
Guide to Paper	

To see the listed manuals, use the computer's browser to access the following website:

<https://support.rioh.com/services/device/ccmanual/ProC5200/en/pdf/GuideToPaper.html>

Online Manuals (Website 6)

Manual Name	Reference Number
Notes on Security Functions	D146-7587
Notes for Administrators: Using This Machine in a Network Environment Compliant with IEEE Std 2600.2™-2009	D260-7069

The URLs for the manuals listed above are shown in "1. Manuals Provided with This Machine", Read This First.

3. Manual reference numbers for "-29" models**Paper Manuals**

Manual Name	Reference Number
Read This First	D260-7004
SOFTWARE LICENSE AGREEMENT	D241-7237
Notes for Using This Machine Safely	D223-7236
NOTICE TO USERS	D241-7178
Notes for Users	D241-7087

Online Manuals (Website 1)

Manual Name	Reference Number
About This Machine	D260-7090
Copy/ Document Server	D260-7091
Print	D260-7092
Scan	D260-7093

Manual Name	Reference Number
Troubleshooting	D260-7094
Connecting the Machine/ System Settings	D260-7095
Security Guide	D260-7098
PostScript 3	D257-7097
Paper Settings	D260-7096
Extended Feature Settings	D260-7099

To see the listed manuals, use the computer's browser to access the following website:

https://support.ricoh.com/services/device/ccmanual/ProC5200/en/booklist/int/index_book.htm

Online Manuals (Website 2)

Manual Name	Reference Number
User Guide	D260-7087

To see the listed manuals, use the computer's browser to access the following website:

<https://support.ricoh.com/services/device/ccmanual/ProC5200/en/pdf/User.html>

Online Manuals (Website 3)

Manual Name	Reference Number
Operating Instructions	D257-7068
Driver Installation Guide	

To see the listed manuals, use the computer's browser to access the following website:

<https://support.ricoh.com/services/device/ccmanual/ProC5200/en/pdf/DriverInstall.html>

Online Manuals (Website 4)

Manual Name	Reference Number
About Open Source Software License	D257-7054

To see the listed manuals, use the computer's browser to access the following website:

<https://support.ricoh.com/services/device/ccmanual/ProC5200/en/pdf/Oss.html>

Online Manuals (Website 5)

Manual Name	Reference Number
Operating Instructions	D260-7088
Guide to Paper	

1

To see the listed manuals, use the computer's browser to access the following website:

<https://support.ricoh.com/services/device/ccmanual/ProC5200/en/pdf/GuideToPaper.html>

Online Manuals (Website 6)

Manual Name	Reference Number
Notes on Security Functions	D146-7587
Notes for Administrators: Using This Machine in a Network Environment Compliant with IEEE Std 2600.2™-2009	D260-7069

The URLs for the manuals listed above are shown in "1. Manuals Provided with This Machine", Read This First.

Options

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

- Finisher SR4120
- Booklet Finisher SR4130
- Cooling Fan Unit Type M26
- Output Jogger Unit Type M25
- SR4000 series Output Tray for Banner Sheet Type S6
- Punch Unit Type PU3060 NA
- Punch Unit Type PU3060 EU
- Punch Unit Type PU3060 SC
- Finisher SR5070
- Booklet Finisher SR5080
- SR5000 series Output Tray for Banner Sheet Type S6
- Punch Unit PU5020 NA
- Punch Unit PU5020 EU
- Punch Unit PU5020 SC

- Copy Tray Type M26
- LCIT RT4020
- 8¹/₂"×14" PAPER SIZE TRAY TYPE M2
- LCIT RT4050
- Cover Interposer Tray CI4040
- Cover Interposer Tray CI4020
- A3/11" × 17" Tray Unit Type M26
- Multi Bypass Banner Sheet Tray Type S6
- Banner Sheet Guide Tray for A3/11"×17" LCIT Type S6
- Tab Sheet Holder Type M2
- Decurl Unit DU5020
- Buffer Pass Unit Type S6
- Multi-Folding Unit FD4000
- Media Identification Unit Type S3
- Mail Box CS4010

Preparation for Use

To use the MFP in a CC-certified operating environment, the administrator must perform the procedures described on page 15 "Specifying the MFP Settings".

The administrator should read the MFP manual thoroughly before performing the procedures described on page 15 "Specifying 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, or Web Image Monitor.

★ Important

- If a message prompting you to change the password at startup appears, specify passwords for the administrator and the supervisor. For details about specifying the passwords, see "Changing the Administrator's or Supervisor's Password", Notes for Using This Machine Safely.

Procedure 1: Settings to Specify Using the Control Panel

Press the [User Tools] key on the control panel, specify [System Settings], [Copier/Document Server Features], [Printer Features], [Scanner Features], and [User Authentication Management] so that the specified values are in the CC-certified ranges.

For details about configuring settings in the User Tools menu, see "Accessing User Tools", 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.

After specifying Administrator Authentication Management ► File Management, log in as the administrator to specify the MFP settings. For details about logging in as the administrator, see "Administrator Login Method" in "Getting Started", Security Guide.

★ Important

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

Tab	Item	Settings
Timer Settings	Time Zone	Set the appropriate time zone. The specified setting is applied after the machine reboots.
Timer Settings	Daylight Saving Time	Set the appropriate daylight saving time. The specified setting is applied after the machine reboots. Reboot the machine after configuring this setting.
Timer Settings	Set Date	Set the appropriate date.
Timer Settings	Set Time	Set the appropriate time.
Timer Settings	Auto Logout Timer	Select [On], and then set the range for the timer between 10-999 seconds.
Interface Settings	Network ▶ Machine IPv4 Address	<ul style="list-style-type: none"> 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	<p>Specify this only if you are using a static DNS server.</p> <ul style="list-style-type: none"> 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]

Tab	Item	Settings
Interface Settings	Network ▶ Effective Protocol ▶ IPv6	[Inactive]
Interface Settings	Network ▶ IEEE 802.1X Authentication for Ethernet	[Inactive]
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.

Tab	Item	Settings
Administrator Tools	Program / Change Administrator ▶ Supervisor	Change the supervisor's "Login User Name" and "Login Password".
Administrator Tools	Media Slot Use ▶ Store to Memory Device	[Prohibit]
Administrator Tools	Media Slot Use ▶ Print from Memory Storage Device	[Prohibit]

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.

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] and [Fax].
Administrator Tools	User Authentication Management ▶ Basic Auth. ▶ Printer Job Authentication	[Entire]

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 (Scanner)	[On]
Administrator Tools	Extended Security ▶ Restrict Use of Destinations (Scanner)	[On]
Administrator Tools	Extended Security ▶ Authenticate Current Job	[Access Privilege]
Administrator Tools	Extended Security ▶ Update Firmware	[Prohibit]
Administrator Tools	Extended Security ▶ Change Firmware Structure	[Prohibit]
Administrator Tools	Extended Security ▶ Password Policy	<p>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.</p> <p>For example, to set the number of characters to 8, press the number key "8", and then "#".</p> <p>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.</p>
Administrator Tools	Extended Security ▶ Security Setting for Access Violation	[Off]

Tab	Item	Settings
Administrator Tools	Auto Delete File in Document Server	Select [Specify Days], [Specify Hours], 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	Central Management ▶ Address Book	[Do not Manage Centrally]
Administrator Tools	Shift to Main Power-Off When Network Disconnected (mainly Europe)	[Off]
Administrator Tools	Application Authentication Management	Set [Copier], [Printer], [Document Server] and [Scanner] to [On].
Administrator Tools	Document Server Function	Select [On].

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]
System	Auto Store Jobs without User Authent. Info	Make sure that [Off] is selected.

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]
General Settings	Download File Directly From URL Link	[Off]

Procedure 2: Settings to Specify Using Web Image Monitor

It is necessary to specify the values in [Device Settings], [Printer], [Network], [Security], [Webpage] and [Extended Feature Settings] 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:

<https://support.ricoh.com/services/device/webhlp/nb/gen/v211cc1/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.

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	Logs ▶ Collect Eco-friendly Logs	[Active]
Device Settings	Logs ▶ Eco-friendly Log Collect Level	[Level 2]

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.

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 [Network]

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

Category	Item	Settings
Network	IPv4 ▶ LLMNR	[Inactive]

4. 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.
- For details about how to specify Device Certificate, see "Protecting Communication Paths via a Device Certificate", Security Guide.

- For details about specifying IPsec, see "Configuring IPsec Settings", Security Guide.

Category	Item	Settings
Security	Device Certificate <ul style="list-style-type: none">▶Certificate 1▶Create	<p>Configure this to create and install the device certificate (self-signed certificate).</p> <p>If you are using a certificate issued by the certificate authority, you do not need to configure this setting.</p> <p>Of the settings for the device certificate (self-signed certificate), set "Algorithm Signature" to one of the following:</p> <ul style="list-style-type: none">• sha512WithRSA-4096• sha512WithRSA-2048• sha256WithRSA-4096• sha256WithRSA-2048• sha1WithRSA-2048

Category	Item	Settings
Security	Device Certificate ▶ Certificate 1 ▶ Request	<p>Configure this to create the request form for the certificate authority to issue the device certificate.</p> <p>If you are using a self-signed device certificate, you do not need to configure this setting.</p> <p>Of the settings for the device certificate (certificate issued by the certificate authority), set "Algorithm Signature" to one of the following:</p> <ul style="list-style-type: none"> • sha512WithRSA-4096 • sha512WithRSA-2048 • sha256WithRSA-4096 • sha256WithRSA-2048 • sha1WithRSA-2048 <p>Submit the application form to request that the certificate authority issue the device certificate.</p> <p>The request method depends on the certificate authority. For details, contact the certificate authority.</p> <p>You can install the certificate issued by the certificate authority via Web Image Monitor.</p>
Security	Device Certificate ▶ Install	<p>To use the device certificate (issued by the certificate authority), install the certificate by configuring this setting.</p> <p>If using the intermediate certificate as well, install that too.</p>
Security	Device Certificate ▶ Install Intermediate Certificate	<p>When using an intermediate certificate, configure this setting to install the certificate.</p>

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", and "TLS1.0" to [Active], and "SSL3.0" to [Inactive].
Security	Network Security ▶ Encryption Strength Setting	Check "AES", and uncheck "RC4" and "3DES".
Security	Network Security ▶ FTP ▶ IPv4	[Inactive]
Security	Network Security ▶ WSD (Device) ▶ IPv4	[Inactive]
Security	Network Security ▶ WSD (Printer)	[Inactive]

Category	Item	Settings
Security	Network Security ▶ WSD (Scanner)	[Inactive]
Security	Network Security ▶ SNMP	[Inactive]
Security	S/MIME ▶ Encryption Algorithm	Select [AES-256 bit] or [AES-128 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 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

Category	Item	Settings
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].
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	[14]

Category	Item	Settings
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	[14]
Security	User Lockout Policy ▶ Lockout	[Active]
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

5. 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

6. Specifying [Extended Feature Settings]

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

Category	Item	Settings
Extended Feature Settings	Administrator Tools ▶Java™Platform	[Inactive]

Procedure 3: Settings to Specify Using the Control Panel

Using the control panel, specify [System Settings] in the [Machine Features] 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]
Interface Settings	Network ▶Effective Protocol ▶Firmware Update (IPv6)	[Inactive]
Interface Settings	Network ▶Effective Protocol ▶@Remote Service	[Inactive]

Turn the main power of the machine off, and then turn it before using the machine.

Changing MFP Settings during Operation

Of the settings specified before operation according to the procedure described on page 15 "Specifying the MFP Settings", the following setting can be changed even during operation.

1

1. Changing [System Settings] Using the Control Panel

Tab	Item	Settings
Timer Settings	Time Zone	Set the appropriate time zone. The specified setting is applied after the machine reboots.
Timer Settings	Daylight Saving Time	Set the appropriate daylight saving time. The specified setting is applied after the machine reboots. Reboot the machine after configuring this setting.
Timer Settings	Set Date	Set the appropriate date.
Timer Settings	Set Time	Set the appropriate time.
Timer Settings	Auto Logout Timer	Select [On], and then set the range for the timer between 10-999 seconds.
Interface Settings	Network ▶ Machine IPv4 Address	<ul style="list-style-type: none"> 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.

Tab	Item	Settings
Interface Settings	Network ▶ DNS Configuration	Specify this only if you are using a static DNS server. <ul style="list-style-type: none"> 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.
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

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].

3. Changing [System Settings] Using the Control Panel

Tab	Item	Settings
Administrator Tools	Extended Security ▶ Password Policy	<p>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.</p> <p>For example, to set the number of characters to 8, press the number key "8", and then "#".</p> <p>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.</p>
Administrator Tools	Auto Erase Memory Setting	<p>Select [On], and then select [NSA], [DoD], or [Random Numbers].</p> <p>If you set this to [Random Numbers], set [Number of Erase] to three or more.</p>

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	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

1

Category	Item	Settings
Security	Device Certificate ▶ Certificate 1 ▶ Create	<p>Configure this to create and install the device certificate (self-signed certificate).</p> <p>If you are using a certificate issued by the certificate authority, you do not need to configure this setting.</p> <p>Of the settings for the device certificate (self-signed certificate), set "Algorithm Signature" to one of the following:</p> <ul style="list-style-type: none">• sha512WithRSA-4096• sha512WithRSA-2048• sha256WithRSA-4096• sha256WithRSA-2048• sha1WithRSA-2048

Category	Item	Settings
Security	Device Certificate ▶ Certificate 1 ▶ Request	<p>Configure this to create the request form for the certificate authority to issue the device certificate.</p> <p>If you are using a self-signed device certificate, you do not need to configure this setting.</p> <p>Of the settings for the device certificate (certificate issued by the certificate authority), set "Algorithm Signature" to one of the following:</p> <ul style="list-style-type: none"> • sha512WithRSA-4096 • sha512WithRSA-2048 • sha256WithRSA-4096 • sha256WithRSA-2048 • sha1WithRSA-2048 <p>Submit the application form to request that the certificate authority issue the device certificate.</p> <p>The request method depends on the certificate authority. For details, contact the certificate authority.</p> <p>You can install the certificate issued by the certificate authority via Web Image Monitor.</p>
Security	Device Certificate ▶ Install	<p>To use the device certificate (issued by the certificate authority), install the certificate by configuring this setting.</p> <p>If using the intermediate certificate as well, install that too.</p>
Security	Device Certificate ▶ Install Intermediate Certificate	<p>When using an intermediate certificate, configure this setting to install the certificate.</p>


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-256 bit] or [AES-128 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].

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	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 2600.2TM-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.
- Back up the encryption key only when the machine is not operating.
- For print jobs 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 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.

- The file creator (owner) has the authority to grant [Full Control] privileges to other users for stored documents in the Document Server. However, administrators should tell users that [Full Control] privileges are meant only for the file creator (owner).
- A third party may 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 File Server that connects to the MFP is synchronized with the MFP.
- If the power plug is pulled out before the main power is turned off so that the machine is shut down abnormally, the date and time when the main power is turned off (the value for "Main Power Off", which is an attribute of the eco log) is not registered correctly to the "eco" log.
- 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.
- When you specify "HDD Erase Method" in "Erase All Memory", do not select "Format".
- Do not use applications other than "User Tools" in the application list.
- When performing "CCC: Apply Standard Values" in "Administrator Tools" in "System Settings" in Connecting the Machine/ System Settings, check all settings again from "Procedure 1: Settings to Specify Using the Control Panel" to "Procedure 3: Settings to Specify Using the Control Panel" in this manual.
- When you delete all logs, make sure that the following functions are not being used:
 - Scan file storage
 - Scan file transmission
- "Duplicate File" is available for files with "Read-only" permission. The owner of the file created by "Duplicate File" is the user who executed "Duplicate File", not the owner of the original file.

Trademarks

Microsoft, Windows, 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 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 proper names of Internet Explorer 9 and 11 are as follows:

Windows® Internet Explorer® 9

Internet Explorer® 11

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.

