RICOH

imagine. change.

RICOH

RICOH IM 370F/460F

Common Criteria Guide

Version 1.0

November 2023

Document prepared by

Lightship Security

Table of Contents

List of Tables

1   About this Guide

1.1   Overview

1   This guide provides supplemental instructions to achieve the Common Criteria evaluated configuration of the RICOH IM 370F/460F and related information.

1.2   Audience

2   This guide is intended for system administrators and the various stakeholders involved in the Common Criteria evaluation. It is assumed that readers will use this guide in conjunction with the related documents listed in Table 6.

1.3   About the Common Criteria Evaluation

3   The Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408) is an international standard for security certification of IT products and systems. More information is available at https://www.commoncriteriaportal.org/

1.3.1   Protection Profile Conformance

4   The Common Criteria evaluation was performed against the requirements of the Protection Profile for Hardcopy Devices (HCD PP) v1.0 and Protection Profile for Hardcopy Devices, v1.0, Errata #1, June 2017 available at https://www.niap-ccevs.org/Profile/PP.cfm

1.3.2   Evaluated Software and Hardware

5   The TOE includes the RICOH MFP models: IM 370F and IM 460F labeled and marketed under different Ricoh Family Group brand names as noted in Table 1, Table 2.

6   The TSF is executed by the main controller and the operation unit respectively. For all TOE models, the main controller has an Arm Cortex-A53 Dual Core Processor and runs Linux 4.2.8 OS, a customized OS based on NetBSD; the operation unit has an ARM Cortex-A57 Dual Core processor and runs a customized Linux 4.19 OS.

7   The first two numeric digits in the TOE model number correspond to copy speed, e.g. 370 performs 37 copies per minute, 460 performs 46 copies per minute, the alphabetic suffix corresponds to regional fonts and printer languages.

8   Differences between models with different printing speeds are limited to print engine components; differences between branding variants are limited to labels, displays, packaging materials, and documentation. The differences are not security relevant. All TOE models are version JE-1.00-H.

9   MFP Type1: IM 370F/460F (-17, -27, -28, -29 models)

10   MFP Type2: IM 460F/370F (-00, -03 models)

11

Table 1: TOE Models (Type 1)

Branding	Model
RICOH	IM 370F

Branding	Model
nashuatec	IM 460F
Rex Rotary	
Gestetner	

Table 2: TOE Models (Type 2)

Branding	Model
RICOH	IM 370F IM 460F

Table 3: Machine Firmware and Hardware (Type 1 & Type 2)

Primary Classification	Secondary Classification	Version
Firmware	TOE Version	JE-1.00-H
	CTL System	1.04
	Printer	1.00
	RicohACT	2.20
	CheetahSystem	1.04
	iwnnimeml	2.16.204
	simpleprinter	1.00
	smartcopy	1.01
	smartdocumentbo	1.00

Primary Classification	Secondary Classification	Version
	smartfax	1.01
	smartprtstoredj	1.00
	smartscanner	1.01
	stopwidget	1.00

Table 4: Drivers

Drivers	Model
Printer Driver	PCL6 Driver 1.1.0.0
	RPCS Driver 1.0.0.0
LAN-Fax Driver	LAN-Fax Driver 13.1.0.0
	PCFAX Driver 13.1.0.0

1.3.3   Evaluated Functions

12   The following functions have been evaluated under Common Criteria:

a)   **Security Audit.** The TOE generates audit records of user and administrator actions. It stores audit records both locally and on a remote syslog server.

b)   **Cryptographic Support.** The TOE includes a cryptographic module for the cryptographic operations that it performs. The relevant CAVP certificate numbers are noted in the Security Target.

c)   **Access Control.** The TOE enforces access control policy to restrict access to user data. The TOE ensures that documents, document processing job information, and security-relevant data are accessible only to authenticated users who have the appropriate access permissions.

d)   **Storage Data Encryption.** The TOE encrypts data on the eMMC and in NVRAM to protect documents and confidential system information if those devices are removed from the TOE.

e)   **Identification and Authentication.** Except for a defined minimal set of actions that can be performed by an unauthenticated user, the TOE ensures that all users must be authenticated before accessing its functions and data. Users login to the TOE by entering their credentials on the local operation panel, through WIM login, through print or fax drivers, or using network authentication services.

f) **Administrative Roles.** The TOE provides the capability for managing its functions and data. Role-based access controls ensure that the ability to configure the security settings of the TOE is available only to the authorized administrators. Authenticated users can perform copy, printer, scanner, document server and fax operations based on the user role and the assigned permissions.

g) **Trusted Operations.** The TOE performs power-on self-tests to ensure the integrity of the TSF components. It provides a mechanism for performing trusted update that verifies the integrity and authenticity of the upgrade software before applying the updates. It uses an NTP server for accurate time.

h) **TOE Access.** Interactive user sessions at the local and remote user interfaces are automatically terminated by the TOE after a configured period of inactivity.

i) **Trusted Communications.** The TOE protects communications from its remote users using TLS/HTTPS, and communications with the LDAP, FTP, NTP, and SMTP servers using IPsec. The TOE can be configured to use either IPsec or TLS to protect communication with the syslog and SMTP servers.

j) **PSTN Fax-Network Separation.** The TOE restricts information received from or transmitted to the telephone network to only fax data and fax protocols. It ensures that the fax modem cannot be used to bridge the LAN.

13   **NOTE:** No claims are made regarding any other security functionality.

1.3.4   Evaluation Assumptions

14   The following assumptions were made in performing the Common Criteria evaluation. The guidance shown in the table below should be followed to uphold these assumptions in the operational environment.

Table 5: Evaluation Assumptions

Assumption	Guidance
A.PHYSICAL — Physical security, commensurate with the value of the TOE and the data it stores or processes, is assumed to be provided by the environment.	Ensure that the device is hosted in a physically secure environment and that adequate security measures are in place to protect access.
A.NETWORK — The Operational Environment is assumed to protect the TOE from direct, public access to its LAN interface.	Ensure that the device is hosted on a protected network environment.
A.TRUSTED_ADMIN — TOE Administrators are trusted to administer the TOE according to site security policies	Ensure that administrators are trustworthy – e.g. implement background checks or similar controls.
A.TRAINED_USERS — Authorized Users are trained to use the TOE according to site security policies	Ensure that authorized users receive adequate training.

1.4   Conventions

15   The following conventions are used in this guide:

a)   `CLI Command <replaceable>` - This style indicates to you that you can type the word or phrase on the command line and press [Enter] to invoke a command. Text within <> is replaceable. For example:

Use the `cat <filename>` command to view the contents of a file

b)   [key] or [key-combo] – key or key combination on the keyboard is shown in this style. For example:

The [Ctrl]-[Alt]-[Backspace] key combination exits your graphical session and returns you to the graphical login screen or the console.

c)   **GUI => Reference** – denotes a sequence of GUI screen interactions. For example:

Select **File => Save** to save the file.

d)   [REFERENCE] *Section* – denotes a document and section reference from Table 6. For example:

Follow [ADMIN] *Configuring Users* to add a new user.

1.5   Related Documents

16   This guide supplements the below documents which are available on the Ricoh Support site help pages.

Table 6: Related Documents

Reference	
[ADMIN]	RICOH IM 370/460 Series User Guide User Guide
[SECURITY]	RICOH IM 370/460 Series User Guide User Guide Security Reference
[FIRMWARE]	RICOH IM 370/460 Series User Guide Checking Firmware Validity
[WEB IMAGE MONITOR]	RICOH IM 370/460 Series User Guide Operating or Configuring the Machine from Computer (Web Image Monitor)
[REGISTER ADMINISTRATOR]	RICOH IM 370/460 Series User Guide Registering Standard-Privileges Administrators
[FAX]	RICOH IM 370/460 Series User Guide Registering/Changing/Deleting Fax Numbers in the Address Book
[LOGS]	RICOH IM 370/460 Series User Guide

Reference	
	Collecting Logs
[USER MANAGEMENT]	RICOH IM 370/460 Series User Guide Introduction and Basic Operations

17   **NOTE:** The information in this guide supersedes related information in other documentation.

2   Secure Acceptance and Update

2.1   Obtaining the TOE

18   The TOE is delivered via commercial carrier.

2.2   Verifying the TOE

19   To verify the TOE Model, check that the machine's model number on the label to the rear of the machine ends with -00, -03, -17, -27, -28 or -29 which correspond to the branding variants of RICOH IM 370F/460F included in the evaluated configuration.

20   To verify the TOE firmware, the authorized administrator login and use the following steps:

21   On the Operation Panel:

   a)   -Press [Home]

   b)   -Flick the screen to the left and then press the [Settings] icon

   c)   -Press [System Settings]

   d)   -Press [Machine/Control Panel Information]

   e)   -Press [Firmware version]

   The firmware list is displayed.

   On the WIM:

   a)   -Device Management -> Configuration->Firmware Update

2.3   Power-on Self-Tests

22   At system start-up, the TOE performs a firmware validity test to determine if the firmware is valid. If an error occurs and the test fails, a verification error is displayed on the control panel. The firmware validity test error will also display on the Web Image Monitor after the machine starts.

23   The TOE also performs software integrity test at TOE start-up by verifying the digital signature on the TOE software. Any errors are displayed on the Control Panel or on the WIM interface.

24   Additional details on the Power-on self-tests can be found in Checking Firmware Validity in the 'Taking Measures to Prevent Security Threats' Section of the Security Guide.

2.4   Updating the TOE

25   TOE updates are hand delivered by Ricoh service personnel. The update packages are digitally signed and uploaded to the TOE using WIM.

26   For MFP Control Software, the TOE performs the following verifications installing the package:

   a)   Identifies the type of software (e.g., MFP Control, Operation Panel)

     b)   Verifies that the software model name matches the TOE

     c)   Verifies the digital signature on the update package.

1   For Operation Panel software, the TOE performs the following verifications before the installing the package:

     a)   Identifies the type of software (e.g., MFP Control, Operation Panel)

     b)   Verifies that the software model name matches the TOE

     c)   Verifies the digital signature

3   Configuration Guidance

3.1   Installation

27   The TOE is delivered pre-installed with initial settings for CC-mode configuration performed by a Ricoh Authorized Service representative.

3.1.1   Printer and Fax Driver

28   The printer and LAN-Fax driver are downloaded from the Ricoh support site. To install the printer driver, enter the machine's IP address or host name in the [URL] box as follows:

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

29   To install the LAN-Fax driver, enter the following URL in the [Printer URL] box as follow:

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

30   Install the LAN-Fax driver (INF file) in the following location:

31   32-bit driver

32   X86\DRIVERS\LAN-FAX\X86\DISK1

33   64-bit driver

34   X64\DRIVERS\LAN-FAX\X64\DISK1

3.2   Administration Interfaces

35   The TOE provides the following administrator interfaces:

   a) **Operation Panel of the MFP** is an LCD touch screen interface that provides a local user interface where users can perform copy, fax print, network transmission of documents operations. The administrator user can configure the MFP via this local interface.

   b) **Web Image Monitor (WIM)** this is the remote user interface accessible via TLS/HTTPS where users can perform print, copy, fax, storage operations on documents. This interface provides various settings for administrators to perform limited configuration of the MFP. For additional details on how to launch the WIM interface see "Operating or Configuring the Machine from Computer (Web Image Monitor) " in the Introduction and Basic Operations section of the User Guide.

3.3   Initial Configuration

36   Both the Operation Panel and the WIM are used to setup initial configuration of the MFP TOE. Administrator must be registered during the initial setup by entering a username/password combination. Procedures 1 through 3 describe the sequential steps for initial configuration of the TOE.

37   The following warnings are noted:

   a)   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.

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

c) Security attributes are modified at the time they are submitted to the system with the "OK" button. Currently logged in user's access rights will be updated at this time, and it is unnecessary to logout and log back in for the access changes to be reflected.

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

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

f) If the message "SD Card authentication has failed" is displayed, contact RICOH Service Representative.

g) "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 "Encrypting Network Communication" in "Preventing Unauthorized Accesses", Security.

h) 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 will appear next to destinations for which [Encrypt All] has been set.

i) When using Scan to Folder make sure IPsec is enabled and complete the following steps:

   1. The Scan to Folder destination (FTP or SMB server) must be registered in the address book by the administrator.

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

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

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

k) 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.

l) 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).

m) When using Web Image Monitor, users should not access other Web sites. Users should logout of WIM when it is not being used.

n) Obtain log files by downloading them via Web Image Monitor or by automatic log collection. 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.

o) To prevent incorrect timestamps from being recorded in the audit log, ensure that the Audit Server that connects to the MFP is synchronized with the MFP.

p) 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.

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

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

s)   Administrators must not use applications other than the ones registered on the Home screen in "Important" in "Procedure 1: Settings to Specify Using the Control Panel 1" and "Change Langs.Widget".

t)   Except for the applications registered on the Home screen in "Important" in "Procedure 1:Settings to Specify Using the Control Panel 1" and "Change Langs. Widget", administrators must not set any applications to "Function Priority" in "Screen Device Settings" in "System" in "Screen Features".

u)   Except for the applications registered on the Home screen in "Important" in "Procedure 1: Settings to Specify Using the Control Panel 1" and "Change Langs. Widget", administrators must not set any applications to "Function Key Settings" in "Screen Device Settings" in "System" in "Screen Features".

v)   Do not assign "Reception File Settings" to a Quick Operation key in Fax mode.

w)   If you performed "CCC: Save Standard Values" in " Settings for Administrator" of "System Settings" in "Settings", then Please make the following settings. Using the MultiLink-Panel, specify settings [System Settings] and [Fax Settings] in the [Settings] menu.

Specifying [System Settings]

Tab	Item	Settings
Network/Interface	Control Panel: External Interface Software Settings ▶Select IC Card Reader	[Do not Use]
Settings for Administrator	Authentication/Charge ▶Administrator Authentication/User Authentication/App Auth. ▶Register/Change Administrator ▶Set Administrator Login User Name/Login Password ▶Administrator 1-4	Specify settings for one or more administrators. Specify the administrator's "Login User Name" and "Login Password".
Settings for Administrator	Security ▶Extended Security Settings ▶Restrict Adding of User Destinations (Fax)	[On]

Tab	Item	Settings
Settings for Administrator	Security ▶Extended Security Settings ▶Restrict Adding of User Destinations (Scanner)	[On]
Machine	Others ▶Central Management	[Do not Manage Centrally]

Specifying [Fax Settings]

Tab	Item	Settings
Send Settings	Backup File Transmission Setting	[Off]
Reception Settings	Reception File Settings ▶Action on Receiving File ▶Store	[On]
Reception Settings	Reception File Settings ▶Action on Receiving File ▶Forwarding	[Off]
Reception Settings	Stored Reception File User Setting ▶Stored Reception File User Setting	[On] After setting this to [On], specify the users or groups that can access stored reception files.
Detailed Initial Settings	Fax Email Account	[Do not Receive]

It is necessary to specify the values in [Device Settings], [Printer], and [Security] in [Configuration] in [Device Management] of Web Image Monitor.

Category	Item	Settings
Security	Network Security ▶TCP/IP ▶DIGEST ▶SHA1	[Inactive]
Device Settings	Logs ▶Common Settings for All Logs ▶Transfer Logs	[Inactive]

Category	Item	Settings
Device Settings	SYSLOG Transfer ▶Transfer SYSLOG Server	[Active]

x)   When you delete all logs, make sure that the following functions are not being used:

i)   Scan file transmission

y)   If [SHA1] in [DIGEST] in [TCP/IP] in [Network Security] in [Security] in [Configuration] in [Device Management] has been switched from [Active] to [Inactive] on Web Image Monitor, [SSL3.0] is automatically set to [Active]. In such a case set [SHA1] to [Inactive], and then, in [Configuration] in [Device Management] on Web Image Monitor, specify the following setting:

i)   Security -> Network Security -> SSL/TLS Version

ii)   Set "TLS1.2" to [Active] and all others to [Inactive]

z)   Storing a fax from a computer

1. On the computer, open the file to store, and then, on the [File] menu, click [Print].

2. In the printer name list, click "RICOH PC FAX Generic".

3. Click [Print].

4. Select the destination by the registration number in the machine's address book.

1. Click [Specify Destination] tab.

2. Check [Use device address].

3. Enter the registration number in [Device Address:(1-50000)] box.

4. Click [Set as Destination].

5. To select multiple destinations, repeat steps 3 and 4.

5. Check [Send to Document Server] on the [Document Server] tab

6. Click [Send].

・You can also store the file without sending it by clicking [Send] without performing "Specify Destination".

3.3.1   Procedure 1 – Settings Specified using the Operation Panel

38   Follow the instructions in "Registering Standard-Privileges Administrators" to activate the administrator account that would configure the machine. Enter passwords for administrator and supervisor, these are the authorized administrators roles that comprise U.ADMIN and the only roles with permissions to configure the TOE and the TSF.

39   Login to the operation panel as the administrator to configure the settings below.

40   Select "English" from "Change Language". Delete all the icons on the Home screen except for "Copy", "Scanner", "Fax", "Settings", "Quick Print Release", "Printer",

"Document Server", "Address Book", "Substitute RX File". Do not re-register the deleted icons.

3.3.1.1   System Settings

41   The administrator must specify the settings in [System Settings] within the ranges shown in Table 7.

Table 7: System Settings

Tab	Item	Settings
Date/Time/Timer	Date/Time ▶Time Zone	Set the appropriate time zone. The specified setting is applied after the machine reboots.
Date/Time/Timer	Date/Time ▶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.
Date/Time/Timer	Date/Time ▶Set Date	Set the appropriate date.
Date/Time/Timer	Date/Time ▶Set Time	Set the appropriate time.
Date/Time/Timer	Timer ▶Auto Logout Timer	Select [On], and then set the range for the timer between 10-999 seconds. Setting a long time increases the possibility of other people using the device, set the time as short as possible, around 180 seconds.
Network/Interface	IP Address (IPv4) ▶IPv4 Address Configuration	Specifying a static IPv4 address Enter the IPv4 address and subnet mask. Obtaining the DHCP server address automatically Select [Auto-Obtain (DHCP)].

Tab	Item	Settings
Network/Interface	IP Address (IPv4) ▶IPv4 Gateway Address	Enter the IPv4 gateway address.
Network/Interface	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)].
Network/Interface	Effective Protocol ▶IPv4	[Active]
Network/Interface	Effective Protocol ▶IPv6	[Inactive]
Network/Interface	SMB ▶SMB Client Advanced Settings ▶SMBv2/SMBv3	[Active]
Network/Interface	IEEE 802.1X Authentication ▶IEEE 802.1X Authentication for Ethernet	[Inactive]
Network/Interface	Control Panel : Proxy Settings ▶Use Proxy	[Disable]
Network/Interface	Control Panel : Bluetooth ▶Bluetooth	[Off]

Tab	Item	Settings
Network/Interface	Control Panel : External Interface Software Settings ▶Select IC Card Reader	[Do not Use]
Settings for Administrator	Authentication/Charge ▶Administrator Authentication/User Authentication/App Auth. ▶Administrator Authentication Management ▶User Management	Set [Administrator Authentication] to [On], and then select [Administrator Tools] in [Available Settings].
Settings for Administrator	Authentication/Charge ▶Administrator Authentication/User Authentication/App Auth. ▶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].
Settings for Administrator	Authentication/Charge ▶Administrator Authentication/User Authentication/App Auth. ▶Administrator Authentication Management ▶Network Management	Set [Admin. Authentication] to [On], and then select [Interface Settings], [File Transfer], and [Administrator Tools] in [Available Settings].
Settings for Administrator	Authentication/Charge ▶Administrator Authentication/User Authentication/App Auth. ▶Administrator Authentication Management ▶File Management	Set [Admin. Authentication] to [On], and then select [Administrator Tools] in [Available Settings].

Tab	Item	Settings
Settings for Administrator	Authentication/Charge ▶Administrator Authentication/User Authentication/App Auth. ▶Register/Change Administrator ▶Set Administrator Login User Name/Login Password ▶Administrator 1-4	Specify settings for one or more administrators. Specify the administrator's "Login User Name" and "Login Password".
Settings for Administrator	Authentication/Charge ▶Administrator Authentication/User Authentication/App Auth. ▶Register/Change Administrator ▶Set Administrator Privileges	Assign all administrator roles (user administrator, machine administrator, network administrator, and file administrator) to a single administrator.
Settings for Administrator	Authentication/Charge ▶Administrator Authentication/User Authentication/App Auth. ▶Register/Change Administrator ▶Set Administrator Login User Name/Login Password ▶Supervisor	Change the supervisor's "Login User Name" and "Login Password". ⭐Important To change the supervisor's "Login User Name" and "Login Password", log in as the supervisor.
Settings for Administrator	Authentication/Charge ▶Administrator Authentication/User Authentication/App Auth. ▶User Authentication Management	[Basic Authentication]
Settings for Administrator	Authentication/Charge ▶Administrator Authentication/User Authentication/App Auth. ▶User Authentication Management	Specify this in accordance with your operating environment. Set the browser to [Unavailable].

Tab	Item	Settings
	▶Basic Authentication ▶Available Functions	
Settings for Administrator	Authentication/Charge ▶Administrator Authentication/User Authentication/App Auth. ▶User Authentication Management ▶Basic Authentication ▶Available Functions ▶Printer Job Authentication	[Entire]
Settings for Administrator	Authentication/Charge ▶Administrator Authentication/User Authentication/App Auth. ▶Setting for Entering Authentication Password	[Only 1 Byte Characters]
Settings for Administrator	Authentication/Charge ▶Administrator Authentication/User Authentication/App Auth. ▶Application Authentication Management	Set [Copier Function], [Printer Function], [Document Server Function], [Fax Function] and [Scanner Function] to [On].
Settings for Administrator	Authentication/Charge ▶Administrator Authentication/User Authentication/App Auth. ▶User's Own Customization	[Prohibit]
Settings for Administrator	Authentication/Charge ▶Administrator Authentication/User Authentication/App Auth. ▶LDAP Search	[Off]

Tab	Item	Settings
Settings for Administrator	Security ▶Extended Security Settings ▶Restrict Display of User Information	[On]
Settings for Administrator	Security ▶Extended Security Settings ▶Restrict Adding of User Destinations (Fax)	[On]
Settings for Administrator	Security ▶Extended Security Settings ▶Restrict Adding of User Destinations (Scanner)	[On]
Settings for Administrator	Security ▶Extended Security Settings ▶Restrict Use of Destinations (Fax)	[On]
Settings for Administrator	Security ▶Extended Security Settings ▶Restrict Use of Destinations (Scanner)	[On]
Settings for Administrator	Security ▶Extended Security Settings ▶Transfer to Fax Receiver	[Prohibit]
Settings for Administrator	Security ▶Extended Security Settings ▶Authenticate Current Job	[Access Privilege]
Settings for Administrator	Security ▶Extended Security	[Prohibit]

Tab	Item	Settings
	Settings ▶Update Firmware	
Settings for Administrator	Security ▶Extended Security Settings ▶Change Firmware Structure	[Prohibit] After specifying this setting, be sure to click [OK]. If you fail to press [OK], the specified setting will not be applied.
Settings for Administrator	Security ▶Extended Security Settings ▶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. (Note — The TOE requires minimum password length of 8 characters). For example, to set the number of characters to 8, press the number key "8", and then "Done". 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. ⭐Important After specifying this setting, be sure to press [OK]. If you fail to press [OK], the specified setting will not be applied.
Settings for Administrator	Security ▶Extended Security Settings ▶Security Setting for Access Violation	[Off]
Settings for Administrator	Security ▶Service Mode Lock	[On]

Tab	Item	Settings
Settings for Administrator	Security ▶Server Settings ▶Server Function	[Inactive]
Settings for Administrator	Data Management ▶Transfer Log Setting	[Do not Forward]
Settings for Administrator	File Management ▶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." ⭐ Important When setting encryption/unencryption of data in the device, the internal storage is initialized and the device certificate is deleted. If the settings are changed, please create and install a new device certificate and restart TOE. Please install the user certificate after restarting.
Settings for Administrator	File Management ▶Auto Delete File in Document Server	Select [Specify Days], [Specify Hours] or [Off]
Settings for Administrator	File Management ▶Document Server Function	Select [On]
Settings for Administrator	Function Restriction ▶Menu Protect ▶Copier	[Level 2]
Settings for Administrator	Function Restriction ▶Menu Protect ▶Printer	[Level 2]

Tab	Item	Settings
Settings for Administrator	Function Restriction ▶Menu Protect ▶Scanner	[Level 2]
Settings for Administrator	Function Restriction ▶Menu Protect ▶Fax	[Level 2]
Display/Input	Key/Keyboard/Input Assistance ▶Keyboard & Input Methods ▶Switchable Keyboard Settings ▶iWnn IME	[Enable]
Machine	Power/Energy Saving ▶Shift to Main Power-Off When Network Disconnected (mainly Europe)	[OFF]
Machine	Power/Energy Saving ▶Main Power On By Remote Operation	[Inactive]
Machine	External Device ▶Control Panel USB Memory Slot	[Inactive]
Machine	External Device ▶Allow Media Slots Use ▶Store to Memory Storage Device	[Prohibit]
Machine	External Device ▶Allow Media Slots Use ▶Print from Memory Storage Device	[Prohibit]
Machine	Others ▶Central Management	[Do not Manage Centrally]

3.3.1.2   User Authentication Settings

42   The TOE supports local authentication labeled 'Basic Auth' and external authentication via LDAP labeled 'LDAP Auth'. The authorized administrator specifies the settings for user authentication in [System Settings] -> [Settings for Administrator] -> [Authentication/Charge]. The administrator configures the active authentication methods as either Basic Auth or LDAP Auth options using the following settings:

3.3.1.2.1   Basic Authentication Settings

Table 8: Basic Authentication

Tab	Item	Settings
Settings for Administrator	Authentication/Charge ▶Administrator Authentication/User Authentication/App Auth. ▶User Authentication Management	[Basic Authentication]
Settings for Administrator	Authentication/Charge ▶Administrator Authentication/User Authentication/App Auth. ▶User Authentication Management ▶Basic Authentication ▶Available Functions	Specify this in accordance with your operating environment. Set the browser to [Unavailable].
Settings for Administrator	Authentication/Charge ▶Administrator Authentication/User Authentication/App Auth. ▶User Authentication Management ▶Basic Authentication ▶Printer Job Authentication	[Entire]

3.3.1.2.2   LDAP Authentication Settings

43   Prior to configuring the LDAP Authentication settings, an LDAP server must be configured and available for used by the TOE. For details on preparing the LDAP Server in the operational environment, see the Security Guide Section 'Preparing the

Server to Use for User Authentication" and the Settings section "Registering the LDAP Server".

Table 9: LDAP Authentication

Tab	Item	Settings
Settings for Administrator	Authentication/Charge ▶Administrator Authentication/User Authentication/App Auth. ▶User Authentication Management	[LDAP Authentication.]
Settings for Administrator	Authentication/Charge ▶Administrator Authentication/User Authentication/App Auth. ▶User Authentication Management ▶LDAP Authentication. ▶LDAP Servers	Select the LDAP server to authenticate.
Settings for Administrator	Authentication/Charge ▶Administrator Authentication/User Authentication/App Auth. ▶User Authentication Management ▶LDAP Authentication. ▶Available Functions	Specify this in accordance with your operating environment. Set the browser to [Unavailable].
Settings for Administrator	Authentication/Charge ▶Administrator Authentication/User Authentication/App Auth. ▶User Authentication Management ▶LDAP Authentication. ▶Printer Job Authentication	[Entire]

3.3.1.3   Printer Settings

44   The administrator must configure the printer settings within the range specified in Table 10.

Table 10: Printer Settings

Tab	Item	Settings
Data Management/Maintenance	Print Jobs ▶Auto Delete Temporary Print Jobs	Select [On] or [Off].
Data Management/Maintenance	Print Jobs ▶Auto Delete Stored Print Jobs	Select [On] or [Off].
Data Management/Maintenance	Print Jobs ▶Jobs Not Printed as Machine Was Off	[Do not Print]
Data Management/Maintenance	Print Jobs ▶Auto Store Jobs Without User Authentication Information	Make sure that [Off] is selected.
Data Management/Maintenance	Administrator Tools ▶ Prohibit List/Test Print	[On]
Data Management/Maintenance	Administrator Tools ▶Prohibit Printing PS/PDF	[On]

3.3.1.4   Scanner Settings

45   The administrator must configure the scanner settings as specified in Table 11.

Table 11: Scanner Settings

Tab	Item	Settings
Sending Settings	Email (URL Link) ▶Download File Directly From URL Link	[Off]
Others	History Settings ▶Print & Delete Scanner Records	[Do not Print: Disable Send]

3.3.1.5   Fax Settings

46   The administrator must configure the fax settings as specified in Table 12.

Table 12: Fax Settings

Tab	Item	Settings
Send Settings	Backup File Transmission Setting	[Off]
Reception Settings	Reception File Settings ▶Action on Receiving File ▶Store	[On]
Reception Settings	Reception File Settings ▶Action on Receiving File ▶Forwarding	[Off]
Reception Settings	Reception File Settings ▶Action on Receiving File ▶Print	Make sure that this is set to [Off] or is grayed out.
Reception Settings	Reception File Settings ▶Action on Receiving File ▶Memory Lock Reception	[Off]
Reception Settings	Reception File Settings ▶ Action on Receiving File when a Memory Is Full ▶ Receiving When Memory Is Full	[Do not Receive]
Reception Settings	Reception File Settings ▶Reception File Storage Location	[Fax Memory]

Tab	Item	Settings
Reception Settings	Box Setting ▶Register/Change/Delete Box	Set all items to [* No item is registered].
Detailed Initial Settings	Parameter Setting ▶Parameter Setting ▶switch 40, bit 0	[1] If the memory for stored received faxes becomes full, the MFP stops receiving new faxes and keeps the stored ones without printing or deleting them.
Detailed Initial Settings	Parameter Setting ▶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.
Detailed Initial Settings	Parameter Setting ▶Parameter Setting ▶switch 04, bit 7	[0] If this is enabled, previews will not be included in the reports.
Detailed Initial Settings	Internet Fax/Email/Folder ▶Internet Fax Setting	[Off]
Detailed Initial Settings	Internet Fax/Email/Folder ▶Email Setting	[Off]
Detailed Initial Settings	Internet Fax/Email/Folder ▶Folder Setting	[Off]
Detailed Initial Settings	IP-Fax Settings ▶IP-Fax Use Settings	Set [Enable H.323] and [Enable SIP] to [Off].
Detailed Initial Settings	Fax Email Account	[Do not Receive]
Others	Report Output Settings ▶Report Auto Print Settings ▶LAN-Fax Result Report	[Do not Print]

3.3.2   Procedure 2 – Setting Specified using WIM

47   The administrator login to the WIM interface using a web browser from a client computer to configure values for various MFP settings including Device, Printer, Fax, Network, Security and Webpage. For details on launching the WIM interface see the Operating or Configuring the Machine from Computer (Web Image Monitor) page in the User Guide.

3.3.2.1   Device Settings

48   The administrator sets the values in [Device Settings] as specified in Table 13.

Table 13: Device Settings

Category	Item	Settings
Device Settings	System ▶Prohibit printing stored files from Web Image Monitor	[Prohibit]
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	Logs ▶Common Settings for All Logs ▶Transfer Logs	[Inactive]
Device Settings	SYSLOG Transfer ▶Transfer SYSLOG Server	Set to [Active] if you transfer the log to the SYSLOG server, or [Inactive] if you do not. As the default, this is set to [Inactive]. Both [Active] and [Inactive] are acceptable for a CC-certified environment. • If set to [Active], be sure to properly manage the log on the SYSLOG server according to "Important Warnings" in this manual. • In [Settings] ▶ [Device Settings] ▶ [SYSLOG Transfer Setting] ▶ [Transfer Log Setting] on the control panel, you can only select [Inactive], but do not change the setting from the control panel.
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	Email ▶ Use Secure Connection (SSL)	[SMTP over SSL]

3.3.2.2   Excluded Fax Features

49   On the WIM interface, the administrator configures the settings for [Fax] with the values specified in Table 14.

Table 14: Excluded Fax Features

Category	Item	Settings
Fax	Initial Settings ▶Cloud Fax Settings ▶Enable/Disable Cloud Fax	[Disable]
Fax	IP-Fax Settings ▶Enable H.323	[Off]
Fax	IP-Fax Settings ▶Enable SIP	[Off]

3.3.2.3   Network Settings

50   The administrator login to the WIM to configures the network settings listed in Table 15.

Table 15: Network Settings

Category	Item	Settings
Network	IPv4 ▶LLMNR	[Inactive]

3.3.2.4   Security Settings

51   The TOE uses IPsec for communication with LDAP, FTP, Syslog, SMTP and NTP servers. The TOE uses TLSv1.2 for remote administration via WIM and for communication with remote non-administrative users. The TOE can also be configured at initial configuration to use TLS to protect communications with a remote Syslog or SMTP server.

52   If the TLS channel for remote administration is broken unintentionally, the TOE will attempt to re-establish the connection automatically or by prompting the user to retry manually.

53   If the IPsec trusted channel with a remote server is unintentionally disrupted, the TOE will automatically attempt to re-establish the connection and a message will be displayed on the operation panel.

54   While the trusted channel to a remote syslog server is disrupted, the TOE will store audit records locally on the MFP up to the document storage limits. Once the disruption has been corrected the TOE will automatically resume transmission.

55   All pre-shared keys, symmetric keys, and private keys are encrypted and are not accessible through normal interfaces during operation. Instructions for clearing the machine before disposal are provided in the Security Guide.

56   The TOE stores keys and certificates in encrypted form in NVRAM and Flash memory. Destruction of old keys is performed directly without delay in NVRAM; in Flash, it is performed by an internal microcontroller in concert with wear-leveling, bad block management, and garbage collection processes. There are no situations where key destruction may be delayed at the physical layer.

3.3.2.4.1   Installing a certificate on an IPsec Server

57   The authorized administrator must generate a certificate from the TOE device, export it and install it on the server. Use the following steps to export and install the certificate:

58   -Log in to the WIM as the administrator

59   -On the home screen click on Device Management ->Configuration -> Device Certificate -> Export

60   -Select "Base 64 encoded X.509" and "Export"

61   -Place the exported certificate into a location where your IPsec endpoint can make use of it.

62   -In the "Encryption Key Auto Exchange Settings" in "IPsec" in "Security" setting screen, you can select tabs. The tab has "Settings 1" to "Settings 4" and "Default Settings". "Settings 1" to "Settings 4" are applied in order when connecting to IPsec, and if any connection cannot be established, the settings of "Default Settings" are applied.

63   For additional details see the Security Guide section on "Encrypting Network Communication"

3.3.2.4.2   Cryptographic Settings –

64   The authorized administrator must configure the following cryptographic parameters using the WIM.

Table 16: Security Settings

Category	Item	Settings
Security	Root Certificate ►Imported Root Certificate	Using [Browse], select the certificate and click [Import].

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 See the Security Guide for the other necessary settings. If you want to use it as an IPsec certificate, import the root certificate first. ⭐Important Make sure to update the TLS certificate before its expiration. If TLS communication is performed with an expired certificate, there is a risk of impairing the confidentiality of the communication.

Category	Item	Settings
Security	Device Certificate ▶Certificate 1 ▶Request	Configure this to create a certificate request for 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 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. If you want to use it as an IPsec certificate, import the root certificate first.
Security	Device Certificate ▶Install	Use this setting to install the device certificate and any intermediate certificate. See the Security Guide for additional instructions on this setting.
Security	Device Certificate ▶Install Intermediate Certificate	When using an intermediate certificate, configure this setting to install the certificate.
Security	Device Certificate ▶Certification ▶S/MIME	Select the installed device certificate.

Category	Item	Settings
Security	Device Certificate ▶Certification ▶IPsec	Select the installed device certificate.
Security	IPP Authentication ▶User Authentication Function of Main Unit	[OFF]
Security	IPP Authentication ▶Authentication	[Inactive]
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 ▶IPP - Port 631 ▶IPv4	[Close]
Security	Network Security ▶SSL/TLS Version	Set "TLS1.2" to [Active], and "TLS1.3", "TLS1.1", "TLS1.0", and "SSL3.0" to [Inactive].
Security	Network Security ▶Encryption Strength Setting	Check "AES 128bit" and "AES 256bit" and uncheck "CHACHA20 256bit", "RC4" and "3DES".
Security	Network Security ▶TCP/IP ▶KEY EXCHANGE ▶RSA	[Inactive]

Category	Item	Settings
Security	Network Security ▶TCP/IP ▶DIGEST ▶SHA1	[Inactive]
Security	Network Security ▶DIPRINT ▶IPv4	[Inactive]
Security	Network Security ▶LPR ▶IPv4	[Inactive]
Security	Network Security ▶FTP ▶IPv4	[Inactive]
Security	Network Security ▶RSH/RCP ▶IPv4	[Inactive]
Security	Network Security ▶TELNET ▶IPv4	[Inactive]
Security	Network Security ▶Bonjour ▶IPv4	[Inactive]
Security	Network Security ▶NetBIOS over TCP/IPv4 ▶IPv4	[Inactive]
Security	Network Security ▶WSD (Device) ▶IPv4	[Inactive]

Category	Item	Settings
Security	Network Security ▶WSD (Printer)	[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], or [SHA-256 bit].
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]
Security	S/MIME ▶When Transferring Files Stored in Document Server (Utility)	[Use Signatures]
Security	Root Certificate ▶Import Root Certificate	Under [Browse], select the certificate and click [Import].

Category	Item	Settings
Security	IPsec ▶IPsec	[Active]
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 Set the following server IP addresses. FTP server NTP server LDAP server (Note: the evaluated configuration uses IPsec for trusted channel communication with these listed servers required in the TOE operational environment.)
Security	IPsec ▶Encryption Key Auto Exchange Settings ▶Security Level	[Authentication and High-Level Encryption]

Category	Item	Settings
Security	IPsec ▶Encryption Key Auto Exchange Settings ▶Authentication Method	Select [Certificate] or [PSK]. If you select PSK, press the "Change" button for "PSK Text" to set PSK. "PSK Text" is limited (truncated) to 32 characters; is composed of any combination of upper and lower-case characters, numbers and special characters that include and (that include: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")"). Note: It is recommended that long "PSK Text" composed of all permitted characters should be chosen as this is considered more secure.
Security	IPsec ▶Encryption Key Auto Exchange Settings ▶Remote ID	Enter the distinguished name of the root certificate (Subject DN).
Security	IPsec ▶Encryption Key Auto Exchange Settings ▶Hash Algorithm	Select [SHA256], [SHA384], or [SHA512].
Security	IPsec ▶Encryption Key Auto Exchange Settings ▶Encryption Algorithm	Select [AES-128-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-SHA256-128], [HMAC-SHA384-192] and [HMAC-SHA512-256], and uncheck [HMAC-SHA1-96] and [HMAC-MD5-96].
Security	IPsec ▶Encryption Key Auto Exchange Settings ▶Encryption Algorithm Permissions	Check [AES-128] and [AES-256], and uncheck [Cleartext] and [3DES].
Security	IPsec ▶Encryption Key Auto Exchange Settings ▶PFS	[14]
Security	User Lockout Policy ▶Lockout (First Time)	[Active] Lockout (Second Time) to (Fourth Time) can be set as desired.
Security	User Lockout Policy ▶Lockout (First Time) ▶Number of Attempts before Lockout	1-10
Security	User Lockout Policy ▶Lockout (First Time) ▶Lockout Release Timer	[Active]

Category	Item	Settings
Security	User Lockout Policy ▶Lockout (First Time) ▶Lock Out User for	1-9999 The default value for the First Time is [60] minutes. If you set a shorter time, you will be vulnerable to brute force attacks, set a longer time, around 60 minutes. When setting the lockout (Second Time) to (Fourth Time) time, also set a longer time using the default value as a guide. The default value for the Second Time is [120] minutes. The default value for the Third Time is [240] minutes. The default value for the Fourth Time is [480] minutes.
Security	User Lockout Policy ▶Release Lockout When Restarting and Rebooting System	[On]

3.3.2.5 WIM Auto Logout Settings

65   The administrator must configure the values for [Webpage] settings as specified in Table 17.

Table 17: WIM Auto Logout Settings

Category	Item	Settings
Webpage	Webpage ▶Web Image Monitor Auto Logout Settings	3 - 60 Setting a long time increases the possibility of other people using the device, set the time as short as possible, around 3 minutes.

3.3.3   Procedure 3 – Additional Settings Using the Operation Panel

66   After completing the configurations in Procedure 2 using the WIM interface, the administrator must go back to the Operation Panel and login to configure the following additional system and fax settings.

3.3.3.1   System Settings

67   The administrator must configure the values for [System] settings specified in Table 18.

Table 18: System Settings 2

Tab	Item	Settings
Settings for Administrator	Authentication/Charge ▶Administrator Authentication/User Authentication/App Auth. ▶Application Authentication Settings ▶General Settings for Application Authentication	Select [Auth. Not Required] for all applications.
Network/Interface	Effective Protocol ▶Firmware Update (IPv4)	[Inactive] This closes the port used for firmware update. Even if the firmware update function is enabled, firmware update will fail.
Network/Interface	Effective Protocol ▶Firmware Update (IPv6)	[Inactive] This closes the port used for firmware update. Even if the firmware update function is enabled, firmware update will fail.
Network/Interface	Effective Protocol ▶@Remote Service	[Inactive] This closes the port used for the @Remote service.

3.3.3.2   Fax Settings

68   The administrator must configure in the address book the users and groups who are authorized to receive faxes stored by the MFP. See the User Guide Section on 'Registering/Changing/Deleting Fax Numbers in the Address Book'. After users are entered in the address book, the administrator can configure the Fax settings in Table 19.

Table 19: Fax Settings

Tab	Item	Settings
Reception Settings	Stored Reception File User Setting ▶Stored Reception File User Setting	[On] After setting this to [On], specify the users or groups that can access stored reception files. Specify the users who can access stored reception files. By specifying such users, you can limit the users who can view, print and delete stored reception files using the control panel.
Reception Settings	Stored Reception File User Setting ▶Operation Management	[Web and Control Panel]

3.4   Services

3.4.1   Firewall

69   See System Settings

3.4.2   Syslog Server

70   Configure the SYSLOG server use the WIM interface settings from [Configuration] of [Device Management]. Set

71   -Device Settings -> SYSLOG Transfer -> Transfer to SYSLOG Server and select "Active".

72   –Enter the Syslog Destination <IP address> and <port number>

73   –Select 'Inactive' for Verification of Syslog Server Certificate

74   For additional information see "Collecting Logs" in the User Guide.

3.4.3   NTP Server

75   See System Settings

3.4.4   FTP Server

76   See System Settings

3.5   Administration

3.5.1   Administration Interfaces

77   See Administration Interfaces above.

78   Table 20 below shows the management functions available at the different administration interfaces.

Table 20: Management Functions

Management Functions	Enable	Interface(s)
Manage user accounts (users, roles, privileges and available functions list)	Create, modify, delete	Operation Panel, WIM
Manage the document user list for stored documents	Create, modify	Operation Panel, WIM
Configure audit transfer settings	Modify	WIM
Manage audit logs	Query, delete, export	Operation Panel, WIM
Manage Audit Functions	Enable, Disable	Operation Panel, WIM
Manage time and date settings	Modify	Operation Panel, WIM
Configure minimum password length	Modify	Operation Panel, WIM
Configure Password complexity settings	Modify	Operation Panel, WIM
Configure Operation Panel Auto Logout Time	Modify	Operation Panel, WIM
Configure WIM Auto Logout Time	Modify	WIM
Configure number of authentication failure before account lockout	Modify	WIM
Configure account release timer settings	Modify	WIM
Configure PSTN Fax-Line Separation Stored Reception File User	Modify	Operation Panel, WIM
Configure network settings for trusted communications (specify IP addresses and port to connect to the TOE)	Modify	Operation Panel, WIM
Manage SSD Cryptographic key	Create Delete	Operation Panel
Manage Device Certificates	Create, query, modify, delete, upload, download	Operation Panel, WIM

Management Functions	Enable	Interface(s)
Manage TOE Trusted Update	Query, Modify	WIM
Configure IPsec	Modify	WIM
Configure SMTP over IPsec	Modify	WIM
Configure NTP	Modify	WIM
Manage user accounts (Ability to login)	Unlock	WIM

3.6   Management of Security Functions

79   After initial configuration the TOE security functions can be modified and managed via the WIM or the Operation Panel.

3.6.1   Functions Managed via the Operation Panel

80   The following settings on the Operation Panel are used to manage the TOE time services, network services, administrators and the password policy.

Table 21: Changing System Settings

Tab	Item	Settings
Date/Time/Timer	Date/Time ▶Time Zone	Set the appropriate time zone. The specified setting is applied after the machine reboots.
Date/Time/Timer	Date/Time ▶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.
Date/Time/Timer	Date/Time ▶Set Date	Set the appropriate date.
Date/Time/Timer	Date/Time ▶Set Time	Set the appropriate time.

Tab	Item	Settings
Date/Time/Timer	Timer ▶Auto Logout Timer	Select [On], and then set the range for the timer between 10-999 seconds. Setting a long time increases the possibility of other people using the device, set the time as short as possible, around 180 seconds.
Network/Interface	IP Address (IPv4) ▶IPv4 Address Configuration	Specifying a static IPv4 address Enter the IPv4 address and subnet mask. Obtaining the DHCP server address automatically Select [Auto-Obtain (DHCP)].
Network/Interface	IP Address (IPv4) ▶IPv4 Gateway Address	Enter the IPv4 gateway address.
Network/Interface	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)].

Tab	Item	Settings
Settings for Administrator	Authentication/Charge ▶Administrator Authentication/User Authentication/App Auth. ▶Register/Change Administrator ▶Set Administrator Login User Name/Login Password ▶Administrator 1-4	Specify settings for one or more administrators. Specify the administrator's "Login User Name" and "Login Password".
Settings for Administrator	Authentication/Charge ▶Administrator Authentication/User Authentication/App Auth. ▶Register/Change Administrator ▶Set Administrator Privileges	Assign all administrator roles (user administrator, machine administrator, network administrator, and file administrator) to a single administrator.
Settings for Administrator	Authentication/Charge ▶Administrator Authentication/User Authentication/App Auth. ▶Register/Change Administrator ▶Set Administrator Login User Name/Login Password ▶Supervisor	Change the supervisor's "Login User Name" and "Login Password". Note: You must be login as the Supervisor admin to change the login information for the supervisor admin.

Tab	Item	Settings
Settings for Administrator	Security ▶Specifying the Extended Security Functions ▶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 "#". Changes to the password policy apply to passwords that are specified or changed after the policy has been updated. 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. ⭐ Important After specifying this setting, be sure to press [OK]. If you fail to press [OK], the specified setting will not be applied.

3.6.2   Functions Managed via the WIM

81   The following settings are used to manage TOE functions via the WIM interface.

3.6.2.1   SMTP Settings

82   The TOE provides secure communication with an SMTP server. Use the following settings on WIM to manage the SMTP server.

Table 22: SMTP Settings

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.

3.6.2.2   Security Settings

83   The following settings on WIM are used to manage the TOE cryptographic and trusted channel functions as well as the user lockout policy.

Table 23: Changing Security Settings

Category	Item	Settings
Security	Device Certificate ▶Certificate 1 ▶Create	Create and install a self-signed device 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 If you want to use it as an IPsec certificate, import the root certificate first. ⭐ Important Make sure to update the TLS certificate before its expiration. If TLS communication is performed with an expired certificate, there is a risk of impairing the confidentiality of the communication.

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 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. If you want to use it as an IPsec certificate, import the root certificate first.
Security	Device Certificate ▶Install	Install a certificate issued by the certificate authority and any intermediate certificate.
Security	Device Certificate ▶Install Intermediate Certificate	When using an intermediate certificate, configure this setting to install the certificate.
Security	Device Certificate ▶Certification ▶S/MIME	Select the installed device certificate.

Category	Item	Settings
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], or [SHA-256 bit].
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 Set the following server IP addresses. FTP server NTP server LDAP server (Note: the evaluated configuration uses IPsec for trusted channel communication with these listed servers required in the TOE operational environment.)
Security	IPsec ▶Encryption Key Auto Exchange Settings ▶Hash Algorithm	Select [SHA256], [SHA384], or [SHA512].

Category	Item	Settings
Security	IPsec ▶Encryption Key Auto Exchange Settings ▶Encryption Algorithm	Select [AES-128-CBC] or [AES-256-CBC].
Security	IPsec ▶Encryption Key Auto Exchange Settings ▶Authentication Algorithm	Check [HMAC-SHA256-128], [HMAC-SHA384-192], [HMAC-SHA512-256], and uncheck [HMAC-SHA1-96] and [HMAC-MD5-96].
Security	User Lockout Policy ▶Number of Attempts before Lockout	1-10
Security	User Lockout Policy ▶Lock Out User for	1-9999 If you set a shorter time, you will be vulnerable to brute force attacks, set a longer time, around 60 minutes.

3.6.2.3   Auto Logout Settings

84   The TSF initiated termination function can be managed via the WIM with by configuring the value for the following setting.

Table 24: WIM Auto Logout Settings

Category	Item	Settings
Webpage	Webpage ▶Web Image Monitor Auto Logout Settings	3 - 60 Setting a long time increases the possibility of other people using the device, set the time as short as possible, around 3 minutes.

3.6.3   User Management

85   Users accessing the TOE functions are identified and authenticated and allowed to access only the functions that they have permissions to access. The TOE includes an address book of registered users accounts that stores individual user attributes

including username, user role, available function lists. The instructions for managing users are provided in "User Authentication" in the "Introduction and Basic Operations" pages of the User Guide.

86   It should be noted that changes to user security attributes are effective immediately with the press of the "OK" button.

3.6.4   Administrator Roles

87   The System Settings in Procedure 1 above identifies the settings for managing the administrator roles in the TOE.

3.6.5   Default Passwords

88   The administrator and supervisor passwords are blank by default, they must be set as part of the initial configuration.

3.6.6   Password Management

89   The System Settings in Procedure 1 above identify the settings for configuring the TOE password policy.

3.6.7   Setting Time

90   See "Table 7: System Settings" for the settings to configure Time and for the Time settings and "3.3.2.4 Security Settings" for settings to configure access to an NTP server for time synchronization.

3.6.8   Audit Logging

91   The TOE collects audit data in 3 types of logs:

a)   Job log – which logs user actions such as printing, copying, storing documents or faxing documents.

b)   Access Log - which logs identification and authentication events, system events and security operations events. This log includes records of the use of the management functions, login and logout events.

c)   Eco -Friendly Log — Which logs power on and power off events.

92   Only the authorized administrator can access, configure and manage the audit settings. Only the authorized administrator can review and manage the audit logs

93   The TOE limits the number of audit records that it stores in the 3 logs: 4000 job logs, 12,000 access logs and 4,000 eco-friendly logs before the oldest audit record are overwritten. Using the WIM the authorized administrator can download the audit logs and delete them.

94   Additional instructions for managing the audit logs are available in the Collecting Logs Ricoh Help pages,

3.7   U_NORMAL User Access

95   The U_Normal user does not have administrator access to the TOE. They can access TOE protected user data and functions based on the available functions list configured for their user account. The user guide describes the job and operations accessible to the U_Normal user.

4   Clearing the machine for redeployment or at end-of-life

96   All pre-shared keys, symmetric keys, and private keys, are encrypted and are not accessible through normal interfaces during operation.

97   To clear the machine of all customer-supplied information, perform the following steps:

a)   Replace the data encryption key

b)   Replace the device certificate

c)   Perform the Erase All Memory function.

98   This deletion function is outside the scope of the evaluation. See the Security Guide for additional information.

99

5   Annex A: Log Reference

5.1   Format

100   The TOE generates audit records for all required auditable events. Each audit record includes time and date, type of events, user identify, outcome of events.

5.2   Events

101   The TOE generates the following log events.

Table 25: Audit Events

Requirement	Auditable Events	Example Event
FAU_GEN.1	Start-up and shutdown of the audit functions	Start-up of the Audit Function Shutdown of the Audit Function
FDP_ACF.1	Job Completion	Printing via networks LAN fax via networks Scanning documents Copying documents Receiving incoming faxes Creating document data (storing) Reading document data (print, download, fax transmission) Deleting document data
FIA_UAU.1/ FIA_UID.1	Unsuccessful identification	Failure of login operations

Requirement	Auditable Events	Example Event
	Unsuccessful authentication	
FMT_SMF.1	Use of a management function	Use of functions identified in the SFR
FMT_SMR.1	Modification of the group of users that are part of a role (the audit record should identify the type of job)	Modification of MFP Administrator roles
FPT_STM.1	Changes to the time	Date settings (year/month/day), time settings (hour/minute)
FTP_TRP.1 Remote administrator	Failure to establish a session	Failure of communication with WIM
FTP_TRP.1 Remote non-admin users	Failure to establish a session	Failure of communication with WIM
FTP_ITC.1	Failure to establish a session	Failure of communication with the audit server Failure of communication with the authentication server Failure of communication with the FTP server Failure of communication with the NTP server Failure of communication with print driver Failure of communication with fax driver

D0DM-7320