



RICOH

RICOH IM C530F/C530FB

Common Criteria Guide

Version 1.6

July 2023

Document prepared by



www.lightshipsec.com

Table of Contents

1	About this Guide	4
1.1	Overview	4
1.2	Audience	4
1.3	About the Common Criteria Evaluation	4
1.4	Conventions	7
1.5	Related Documents	7
2	Secure Acceptance and Update	8
2.1	Obtaining the TOE	8
2.2	Verifying the TOE	8
2.3	Power-on Self-Tests	9
2.4	Updating the TOE	9
3	Configuration Guidance	9
3.1	Installation	9
3.2	Administration Interfaces	10
3.3	Initial Configuration	10
3.4	Services	29
3.5	Administration.....	30
3.6	Management of Security Functions	31
3.7	U_NORMAL User Access	36
4	Clearing the machine for redeployment or at end-of-life	37
5	Annex A: Log Reference	37

List of Tables

Table 1: TOE Models	4
Table 2: Machine Firmware and Hardware	5
Table 3: Drivers	5
Table 4: Evaluation Assumptions	6
Table 5: Related Documents	7
Table 6: System Settings	12
Table 7: Basic Authentication	19
Table 8 : Printer Settings	19
Table 9 : Scanner Settings	20
Table 10 : Fax Settings	20
Table 11 : Device Settings	22
Table 12: Excluded Printer Features	23
Table 13: Network Settings	23
Table 14 : Security Settings	24

Table 15 : WIM Auto Logout Settings28
Table 16: System Settings 228
Table 17: Fax Settings.....29
Table 18: Management Functions.....30
Table 19: Changing System Settings31
Table 20: SMTP Settings34
Table 21: Changing Security Settings34
Table 22: WIM Auto Logout Settings35
Table 23: Audit Events37

1 About this Guide

1.1 Overview

1 This guide provides supplemental instructions to achieve the Common Criteria evaluated configuration of the RICOH IM C530F/C530FB 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 5.

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 C530 labeled and marketed under different RICOH Family Group brand names as noted in Table 1.

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; the operation unit has an ARM Cortex-A9 Quad Core processor and runs a customized Linux 3.18 OS.

7 The first two numeric digits in the TOE model number correspond to copy speed, e.g. 530 performs 53 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 E-1.10-H.

Table 1: TOE Models

Branding	Model
RICOH	IM C530F
nashuatec	IM C530FB
Rex Rotary	

Branding	Model
Gestetner	
SAVIN	IM C530FB
LANIER	

Table 2: Machine Firmware and Hardware

Primary Classification	Secondary Classification	Version
Firmware	CTL System	7.38
	RicohACT	2.20
	CheetahSystem	7.38
	iwnnimeml	2.8.201
	simpleprinter	1.04
	smartcopy	1.04
	smartfax	1.06
	smartprtstoredj	1.04
	smartscanner	1.03
	stopwidget	1.02
Hardware	Ic Key	12714

Table 3: Drivers

Drivers	Model
Printer Driver	PCL6 Driver 1.0.0.0
LAN-Fax Driver	LAN-Fax Driver 9.5.0.0

1.3.3 Evaluated Functions

9

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 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. The TOE is configured to use 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.

10

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

1.3.4 Evaluation Assumptions

11

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 4: 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

12 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 5. For example:
Follow [ADMIN] *Configuring Users* to add a new user.

1.5 Related Documents

13 This guide supplements the below documents which are available on the [RICOH Support site](#) help pages.

Table 5: Related Documents

Reference	
[ADMIN]	RICOH IM C530 Series User Guide

Reference	
	User Guide
[SECURITY]	RICOH IM C530 Series User Guide User Guide Security Reference
[FIRMWARE]	RICOH IM C530 Series User Guide Checking Firmware Validity
[WEB IMAGE MONITOR]	RICOH IM C530 Series User Guide Using Web Image Monitor
[REGISTER ADMINISTRATOR]	RICOH IM C530 Series User Guide Registering the Administrator Before Using the Machine
[PREPARE SERVER]	RICOH IM C530 Series User Guide Preparing the Server to Use for User Authentication
[FAX]	RICOH IM C530 Series User Guide Registering Fax Numbers in the Address Book
[LOGS]	RICOH IM C530 Series User Guide Collecting Logs
[USER MANAGEMENT]	RICOH IM C530 Series User Guide Introduction and Basic Operations

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

2 Secure Acceptance and Update

2.1 Obtaining the TOE

15 The TOE is delivered via commercial carrier.

2.2 Verifying the TOE

16 To verify the TOE Model, check that the machine's model number on the label to the rear of the machine ends with -17, -27 which correspond to the branding variants of RICOH IM C530F/C530FB included in the evaluated configuration.

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

18 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

This lists all the firmware except for the TPM device driver which is only shown in the Ops panel firmware listing.

2.3 Power-on Self-Tests

19 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.

20 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.

2.4 Updating the TOE

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

22 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

23 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

24 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

25 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

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

27 32-bit driver

28 X86\DRIVERS\LAN-FAX\X86\DISK1

29 64-bit driver

30 X64\DRIVERS\LAN-FAX\X64\DISK1

3.2 Administration Interfaces

31 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 ["Using Web Image Monitor"](#) in the Introduction and Basic Operations section of the User Guide.

3.3 Initial Configuration

32 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.

33 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) For faxing, use the public switched telephone network. IP-Fax and Internet Fax are not CC conformant.
- d) For print jobs and fax transmissions from the client computer, use IPP-SSL authentication.
- e) For printing, set the "Job Type" in the "Basic" tab of the printer driver to [Locked Print].

- f) If the message "SD Card authentication has failed" is displayed, contact RICOH Service Representative.
- g) In the event of a hard disk error, the machine will display options to initialize the disk or not. User authentication might fail after a hard disk initialization, if this happens, contact the service representative.
- 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) Before receiving faxes, specify "Stored Reception File User Setting" in the Fax setting.
- j) 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.
- k) When using Web Image Monitor, users should not access other Web sites. Users should logout of WIM when it is not being used.
- l) Obtain log files by downloading them via Web Image Monitor or by automatic log collection.
- m) 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.
- n) 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.
- o) Do not assign "Reception File Settings" to a Quick Operation key in Fax mode.
- p) When you delete all logs, make sure that the Scan File transmission function is not being used.
- q) 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]

3.3.1 Procedure 1 – Settings Specified using the Operation Panel

- 34 Follow the instructions in "[Registering the Administrator Before Using the Machine](#)" 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.
- 35 Login to the operation panel as the administrator to configure the settings below.
- 36 Select "English" from "Change Language". Delete all the icons on the Home screen except for "Copy", "Scanner", "Fax", "Settings", "Quick Print Release", "Printer", "Address Book", "Substitute RX File". Do not re-register the deleted icons.

3.3.1.1 System Settings

37 The administrator must specify the settings in [System Settings] within the ranges shown in Table 6.

Table 6: 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.
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.

Tab	Item	Settings
Network/Interface	DNS Configuration	<p>Specify this only if you are using a static DNS server.</p> <p>Specifying a static DNS server</p> <p>Enter the IPv4 address in "DNS Server 1", "DNS Server 2", and "DNS Server 3". (Specify DNS Server 2 and 3 if required.)</p> <p>Obtaining the DHCP server address automatically</p> <p>Select [Auto-Obtain (DHCP)].</p>
Network/Interface	Effective Protocol ▶IPv4	[Active]
Network/Interface	Effective Protocol ▶IPv6	[Inactive]
Network/Interface	SMB ▶SMB Client Advanced Settings ▶SMBv2/SMBv3	[Active]
Network/Interface	MLP Network Interface settings	[Wi-Fi Connection]
Network/Interface	Control Panel : Wireless LAN ▶Wi-Fi	[Off]
Network/Interface	Control Panel : Wireless LAN ▶Wireless Direct	[Off]
Network/Interface	Control Panel : Proxy Settings ▶Use Proxy	[Disable]
Network/Interface	Bluetooth ▶Bluetooth	[Off]

Tab	Item	Settings
Network/Interface	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 ▶ Machine Administrator	Specify settings for one Administrator. 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 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.
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. ▶ User's Own Customization	[Prohibit]
Settings for Administrator	Authentication/Charge ▶ Administrator Authentication/User Authentication/App Auth. ▶ LDAP Search	[Inactive]
Settings for Administrator	Security ▶ Extended Security Settings	[On]

Tab	Item	Settings
	<ul style="list-style-type: none"> ▶ Restrict Display of User Information 	
Settings for Administrator	<ul style="list-style-type: none"> Security ▶ Extended Security Settings ▶ Restrict Adding of User Destinations (Fax) 	[On]
Settings for Administrator	<ul style="list-style-type: none"> Security ▶ Extended Security Settings ▶ Restrict Adding of User Destinations (Scanner) 	[On]
Settings for Administrator	<ul style="list-style-type: none"> Security ▶ Extended Security Settings ▶ Restrict Use of Destinations (Fax) 	[On]
Settings for Administrator	<ul style="list-style-type: none"> Security ▶ Extended Security Settings ▶ Restrict Use of Destinations (Scanner) 	[On]
Settings for Administrator	<ul style="list-style-type: none"> Security ▶ Extended Security Settings ▶ Transfer to Fax Receiver 	[Prohibit]
Settings for Administrator	<ul style="list-style-type: none"> Security ▶ Extended Security Settings ▶ Authenticate Current Job 	[Access Privilege]
Settings for Administrator	<ul style="list-style-type: none"> Security ▶ Extended Security Settings ▶ Update Firmware 	[Prohibit]
Settings for Administrator	<ul style="list-style-type: none"> Security ▶ Extended Security 	Set "Complexity Setting" to [Level 1] or [Level 2], press [Change] on

Tab	Item	Settings
	Settings ▶ Password Policy	the right of "Minimum Character No.", and then set the number of characters to 15 or more. (Note — The TOE requires minimum password length of 15 characters). Note: Before configuring Password Policy, please perform the settings described in 3.3.1.2.1.
Settings for Administrator	Security ▶ Extended Security Settings ▶ Security Setting for Access Violation	[Off]
Settings for Administrator	Security ▶ Service Mode Lock	[On]
Settings for Administrator	Security ▶ Server Settings ▶ Server Function	[Inactive]
Settings for Administrator	Data Management ▶ Transfer Log Setting	[Do not Forward] Log forwarding will be configured in the WIM as specified in section 3.3.2 below.
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."
Settings for Administrator	Function Restriction ▶ Menu Protect ▶ Copier	[Level 2]

Tab	Item	Settings
Settings for Administrator	Function Restriction ▶ Menu Protect ▶ Printer	[Level 2]
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	External Device ▶ Control Panel SD Card Slot	[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]

3.3.1.2 User Authentication Settings

38 The TOE is configured to local authentication labeled [Basic Authentication] in its operational environment. The administrator configures User Authentication in [System Settings] -> [Settings for Administrator] with the following settings:

3.3.1.2.1 Basic Authentication Settings

Table 7: 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.
Settings for Administrator	Authentication/Charge ▶ Administrator Authentication/User Authentication/App Auth. ▶ User Authentication Management ▶ Basic Authentication ▶ Printer Job Authentication	[Entire]

3.3.1.3 Printer Settings

39 The administrator must configure the printer settings within the range specified in Table 8.

Table 8 : Printer Settings

Tab	Item	Settings
Data Management/Maintenance	Print Jobs ▶ Auto Delete Temporary Print Jobs	Select [On] or [Off].
Data Management/Maintenance	Print Jobs ▶ Restrict Direct Print Jobs	[Cancel All Direct Print Jobs]
Data Management/Maintenance	Administrator Tools ▶ Prohibit List/Test Print	[On]

3.3.1.4 Scanner Settings

40 The administrator must configure the scanner settings as specified in Table 9Table 9

Table 9 : Scanner Settings

Tab	Item	Settings
Sending Settings	Email (URL Link) ▶ File Emailing Method	[Attach to Email]
Others	History Settings ▶ Print & Delete Scanner Records	[Do not Print: Disable Send]

3.3.1.5 Fax Settings

41 The administrator must configure the fax settings as specified in Table 10.

Table 10 : Fax Settings

Tab	Item	Settings
Reception Settings	Reception File Settings ▶ Action on Receiving File ▶ Forwarding	[Off]

Tab	Item	Settings
Reception Settings	Reception File Settings ▶ Action on Receiving File ▶ Print	[Off]
Detailed Initial Settings	Parameter Setting ▶ Parameter Setting switch 46, bit 6	[1] If this is enabled, "Configure Memory Lock Reception" is enabled.
Detailed Initial Settings	Register Memory Lock ID ▶ Register Memory Lock ID	[Register]
Detailed Initial Settings	Register Memory Lock ID ▶ Memory Lock ID	Enter ID with 4 digits numbers. (0000 can not be set)
Reception Settings	Reception File Settings ▶ Action on Receiving File ▶ Memory Lock Reception	[On]
Reception Settings	Reception File Settings ▶ Reception File Storing Error Setting	[Do not Receive]
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 04, bit 7	[0] If this is enabled, previews will not be included in the reports.

3.3.2 Procedure 2 – Setting Specified using WIM

42 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 [Using Web Image Monitor](#) page in the User Guide.

3.3.2.1 Device Settings

43 The administrator sets the values in [Device Settings] as specified in Table 11.

Table 11 : Device Settings

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]
Device Settings	Logs ▶Common Settings for All Logs ▶Transfer Logs	[Inactive]

Category	Item	Settings
Device Settings	SYSLOG Transfer ▶Transfer to SYSLOG Server	[Active]
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 ▶SMTP ▶Use Secure Connection(SSL)	[On]

3.3.2.2 Excluded Printer Features

44 On the WIM interface, the administrator configures the settings for [printer] with the values specified in Table 12.

Table 12: Excluded Printer Features

Category	Item	Settings
Printer	Permissions for Printer Language to Operate File System ▶PDF,PostScript	[Do not Permit]

3.3.2.3 Network Settings

45 The administrator login to the WIM to configures the network settings listed in Table 13.

Table 13: Network Settings

Category	Item	Settings
Network	IPv4 ▶LLMNR	[Inactive]

3.3.2.4 Security Settings

- 46 The TOE includes FIPS validated cryptographic module which it uses to provide its cryptographic services. The TOE uses TLSv1.2 for remote administration via WIM and for communication with remote non-administrative users.
- 47 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.
- 48 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.
- 49 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](#).
- 50 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 Cryptographic Settings –

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

Table 14 : Security Settings

Category	Item	Settings
Security	Device Certificate ▶Certificate 1 ▶Create	Configure this to create and install the device certificate (self-signed certificate) Set "Algorithm Signature" to one of the following: sha512WithRSA-2048 sha256WithRSA-2048 See the Security Guide for the other necessary settings.

Category	Item	Settings
Security	Device Certificate ▶Certificate 1 ▶Request	Configure this to create a certificate request for the device certificate. Set "Algorithm Signature" to one of the following: sha512WithRSA-2048 sha256WithRSA-2048 Submit the certificate request according to the methods required by the certificate authority. Install the issued certificate using the WIM.
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	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].

Category	Item	Settings
Security	Network Security ▶ Encryption Strength Setting	Check "AES128" and/or "AES256", and uncheck "RC4", "3DES" and "CHACHA20".
Security	Network Security ▶ TCP/IP ▶ KEY EXCHANGE ▶ RSA	[Inactive]
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]

Category	Item	Settings
Security	Network Security ▶ Bonjour ▶ IPv4	[Inactive]
Security	Network Security ▶ NetBIOS over TCP/IPv4 ▶ IPv4	[Inactive]
Security	Network Security ▶ WSD (Device) ▶ IPv4	[Inactive]
Security	Network Security ▶ WSD (Printer)	[Inactive]
Security	Network Security ▶ SNMP	[Inactive]
Security	User Lockout Policy ▶ Lockout	[Active]
Security	User Lockout Policy ▶ Number of Attempts before Lockout	1-10
Security	User Lockout Policy ▶ Lockout Release Timer	[Active]
Security	User Lockout Policy ▶ Lock Out User for	1-9999

3.3.2.5 WIM Auto Logout Settings

52 The administrator must configure the values for [Webpage] settings as specified in Table 15.

Table 15 : WIM Auto Logout Settings

Category	Item	Settings
Webpage	Webpage ▶ Web Image Monitor Auto Logout Settings	3 - 60 minutes Note that the default setting is 60 minutes.

3.3.3 Procedure 3 – Additional Settings Using the Operation Panel

53 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

54 The administrator must configure the values for [System] settings specified in Table 16.

Table 16: 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]
Network/Interface	Effective Protocol ▶ Firmware Update (IPv6)	[Inactive]
Network/Interface	Effective Protocol ▶ @Remote Service	[Inactive]

3.3.3.2 Fax Settings

55 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 Fax Numbers in the Address Book’](#). After users are entered in the address book, the administrator can configure the Fax settings in Table 17.

Table 17: Fax Settings

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

3.4 Services

3.4.1 Firewall

56 See System Settings

3.4.2 Syslog Server

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

58 -Device Settings -> SYSLOG Transfer -> Transfer to SYSLOG Server and select “Active”.

59 -Enter the Syslog Destination <IP address> and <port number>

60 -Select ‘Inactive’ for Verification of Syslog Server Certificate

61 For additional information see [“Collecting Logs”](#) in the User Guide.

62 Note: The TOE rate limits the syslog error events in the audit log. When the TOE detects numerous syslog error events in the audit log it will fall into an error state and mute the syslog error events in the log. The TOE will then re-issue the syslog error audit event once every hour if the error is still present. Once the syslog error has been resolved the TOE automatically comes out of the error state.

63 Note: When a communication error occurs between the TOE and the syslog server, the TOE generates an error message which can be viewed from the Ops panel. The TOE enters into an error state and will not generate any additional errors related to the issue while the error state remains. To clear the error state, communication with the syslog server must be re-established.

3.4.3 LDAP Server

64 LDAP is not used in the evaluated configuration.

3.4.4 NTP Server

65 See System Settings

3.4.5 FTP Server

66 FTP is not used in the evaluated configuration.

3.4.6 SMTP Server

67 See System Settings

3.4.7 CAC/PIV Authentication Solutions

68 For CAC/PIV authentication, follow the installation and configuration guidance in CAC/PIV/SIPR v4.1 Installation & Configuration Guide and CAC PIV SIPR ELPNX SOP Option v2.3 Installation Guide for v4.x.

3.5 Administration

3.5.1 Administration Interfaces

69 See Administration Interfaces above.

70 Table 18 below shows the management functions available at the different administration interfaces.

Table 18: Management Functions

Management Functions	Enable	Interface(s)
Manage user accounts (users, roles, privileges and available functions list)	Create, modify, delete	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

Management Functions	Enable	Interface(s)
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 Device Certificates	Create, query, modify, delete, upload	Operation Panel, WIM
Manage TOE Trusted Update	Query, Modify	WIM
Configure SMTP	Modify	WIM
Configure syslog over TLS	Modify	WIM
Configure NTP	Modify	WIM
Manage user accounts (Ability to login)	Unlock	WIM

3.6 Management of Security Functions

71 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

72 The following settings on the Operation Panel are used to manage the TOE time services, network services, administrators, the password policy and the auto erase memory function.

Table 19: 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.

Tab	Item	Settings
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.
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 ▶ Machine administrator	Specify settings for one administrator. 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 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.
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 15 or more. For example, to set the number of characters to 15, press the number key "1", "5", and then "#". Changes to the password policy apply to passwords that are specified or changed after the policy has been updated.

3.6.2 Functions Managed via the WIM

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

3.6.2.1 SMTP Settings

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

Table 20: 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

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

Table 21: Changing Security Settings

Category	Item	Settings
Security	Device Certificate ▶ Certificate 1 ▶ Create	Create and install a self-signed device certificate. Set "Algorithm Signature" to one of the following: sha512WithRSA-2048 sha256WithRSA-2048
Security	Device Certificate ▶ Certificate 1 ▶ Request	Create a certificate request Set "Algorithm Signature" to one of the following: sha512WithRSA-2048 sha256WithRSA-2048 Submit the request Install the issued certificate

Category	Item	Settings
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	User Lockout Policy ▶Number of Attempts before Lockout	1-10
Security	User Lockout Policy ▶Lock Out User for	1-9999

3.6.2.3 Auto Logout Settings

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

Table 22: WIM Auto Logout Settings

Category	Item	Settings
Webpage	Webpage ▶Web Image Monitor Auto Logout Settings	3 - 60 minutes The default setting is 60 minutes.

3.6.3 User Management

77 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.

78 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

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

3.6.5 Default Passwords

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

3.6.6 Password Management

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

3.6.7 Setting Time

82 See "Table 6: System Settings " for the settings to configure Time.

3.6.8 Audit Logging

83 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.

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

2 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. When a maximum number of records is reached, the records are overwritten based on the following criteria:

- a) When syslog audit transfers are working, the oldest records which have been transferred to the syslog server are overwritten first.
- b) If none of the logs have been transferred to the audit server, the oldest records are overwritten first.

85 Using the WIM, the authorized administrator can download the audit logs and delete them.

86 Additional instructions for managing the audit logs are available in the [Collecting Logs](#) RICOH Help pages,

3.7 U_NORMAL User Access

87 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.

Requirement	Auditable Events	Example Event
		<pre> "Report "Print", "2020- 09-02T17:21:08.0", "2020-09- 02T17:21:14.0", " ", "LT", "normal", Fax: "2020-09-03T09:24:06.0", "2020- 09- 03T09:24:54.0", "Fax: Sending", Failed", "Control Panel", "Failed", "Cancelled by User", "0x00000003", "u1", "0x000 00000001b364" Scan File", "2020-09- 03T09:24:09.0", "2020-09- 03T09:24:10.0" ", "Failed", "Failed", "Data Transf er Interrupted", "0x0000000000 01b364" "Send", "2020-09- 03T09:24:06.0", "2020-09- 03T09:24:54.0", "u1d", "1234", </pre>

Requirement	Auditable Events	Example Event
		<p>Scan: "2020-09-09T16:52:36.0", "2020-09-09T16:52:47.0", "Scanner: Sending", "Succeeded", "Control Panel", "Completed", "0x00000003", "u1", "0x000000000001bee9", "" "Succeeded", "Completed", "" "0x000000000001bee9" "Scan File", "2020-09-09T16:52:36.0", "2020-09-09T16:52:40.0", "Succeeded", "Completed", "0x000000000001bee9", "Send", "2020-09-09T16:52:40.0", "2020-09-09T16:52:47.0", "u1d", "10.20.5.7:/u1"</p> <p>Copy: "2020-09-01T12:41:09.0", "2020-09-01T12:41:19.0", "Copier: Copying", "Succeeded", "Control Panel", "Completed", "0x00000003", "u1", "0x000000000001adf4", "" "Succeeded", "Completed", "" "0x000000000001adf4" "Scan File", "2020-09-01T12:41:09.0", "2020-09-01T12:41:19.0", "Succeeded", "Completed", "0x000000000001adf4"</p>

Requirement	Auditable Events	Example Event
		<pre> HH HH HH HH HH HH HH HH HH HH HH HH HH HH HH 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 HH HH HH HH HH HH 5 5 5 5 5 5555 "" "" "0x00000000000195bf" "" "" "Device Settings" "" "" "" "" "" "" "" "" "" "" "" "" HH HH HH HH HH HH HH HH HH HH HH HH HH HH HH 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 HH "" "" "" "" "" "" "" "" "" "" "" "" "" "" 5555 5555 55 55 5 5 55 5 5 "Num ber of Attempts before Lockout" "4" "" "" "Completed" "" HH HH HH HH HH HH HH HH HH HH HH HH HH HH HH 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 HH HH HH HH HH HH 5 5 5 5 5 5555 "" "" "0x00000000000195bf" "" "" "Device Settings" "" "" "" "" "" "" "" "" "" "" "" "" HH HH HH HH HH HH HH HH HH HH HH HH HH HH HH 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 HH "" "" "" "" "" "" "" "" "" "" "" "" "" "" 5555 5555 55 55 5 5 55 5 5 "Lock Out User for" "2" "" "" "Completed" "" "" "" "" HH HH HH HH HH HH HH HH HH HH HH HH HH HH HH 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 HH HH HH 5 5 5 5555 Changing minimum password length: "2020-09-03T11:29:15.0","2020- 09-03T11:29:15.0","Machine Configuration","Succeeded",,"Su cceded",,"0xfffff88","admin11", "0x000000000001b41a",,"" "Devi ce Settings" "" "" "" "" "" "" "" "" "" "" "" "" HH HH HH HH HH HH HH HH HH HH HH HH HH HH HH 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 HH "" "" "" "" "" "" "" "" "" "" "" "" "" "" 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 HH "" "" "" "" "" "" "" "" "" "" "" "" "" "" 5555 5555 55 55 5 5 55 5 5 "Passw ord Policy" "" "" "" "" "Completed" "" "" 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 HH HH HH HH HH HH HH HH HH HH HH HH HH HH HH 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 HH HH HH HH HH HH 5 5 5 5 5 5555 "" "" "0x000000000001b41a "" "" "Device Settings" "" "" "" "" "" "" "" "" "" "" "" "" HH HH HH HH HH HH HH HH HH HH HH HH HH HH HH 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 HH "" "" "" "" "" "" "" "" "" "" "" "" "" "" 5555 5555 55 55 5 5 55 5 5 "Com plexity Setting","Level1",,"" "Complete </pre>

Requirement	Auditable Events	Example Event
		<pre> "2020-09-09T16:43:57.0"; "2020-09-09T16:43:57.0"; "Collect Encrypted Communication Logs"; "Failed"; "Communication Failure"; "0x00000000"; "0x000000000001bed6"; "Network Attack Detection/Encrypted Communication"; "Encryption Communication"; "443"; "TCP"; "ip: 172.16.200.10"; "52664"; "HTTP"; "SSL"; "Communication Start Request Receiver (In)"; "Start"; "Failed"; </pre>
<p>FTP_TRP.1 Remote administrator</p>	<p>Failure to establish a session</p>	<p>"2020-09-09T16:43:57.0"; "2020-09-09T16:43:57.0"; "Collect Encrypted Communication Logs"; "Failed"; "Communication Failure"; "0x00000000"; "0x000000000001bed6"; "Network Attack Detection/Encrypted Communication"; "Encryption Communication"; "443"; "TCP"; "ip: 172.16.200.10"; "52664"; "HTTP"; "SSL"; "Communication Start Request Receiver (In)"; "Start"; "Failed";</p>
<p>FTP_TRP.1 Remote non-admin users</p>	<p>Failure to establish a session</p>	<p>See remote administration</p>
<p>FTP_ITC.1</p>	<p>Failure to establish a session</p>	<p>Failure of communication with the audit server Failure of communication with print driver Failure of communication with fax driver</p>