



**Ricoh IM 2500/3000/3500/4000/5000/6000
Enhanced Security Firmware**

Common Criteria Guide

Version 1.0

February 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	8
1.5	Related Documents	9
2	Secure Acceptance and Update	11
2.1	Obtaining the TOE	11
2.2	Verifying the TOE	11
2.3	Power-on Self-Tests	11
2.4	Updating the TOE	11
3	Configuration Guidance	13
3.1	Installation	13
3.2	Administration Interfaces	13
3.3	Initial Configuration	13
3.4	Services	41
3.5	Administration	42
3.6	Management of Security Functions	43
3.7	U_NORMAL User Access	49
4	Clearing the machine for redeployment or at end-of-life	50
5	Annex A: Log Reference	50
5.1	Format	50
5.2	Events	50

List of Tables

Table 1: TOE Models	5
Table 2: Machine Firmware and Hardware	5
Table 3: Drivers	7
Table 4: Evaluation Assumptions	8
Table 5: Related Documents	9
Table 6: System Settings	18
Table 7: Basic Authentication	27
Table 8: LDAP Authentication	28
Table 9: Printer Settings	29
Table 10: Scanner Settings	30
Table 11: Fax Settings	30
Table 12: Device Settings	33
Table 13: Excluded Printer Features	34
Table 14: Excluded Fax Features	34
Table 15: Network Settings	35
Table 16: Security Settings	36
Table 17: WIM Auto Logout Settings	39
Table 18: System Settings 2	39
Table 19: Fax Settings	40
Table 20: Management Functions	42
Table 21: Changing System Settings	43

Table 22: SMTP Settings	46
Table 23: Changing Security Settings	47
Table 24: WIM Auto Logout Settings	48
Table 25: Audit Events	50

1 About this Guide

1.1 Overview

- 1 This guide provides supplemental instructions to achieve the Common Criteria evaluated configuration of the RICOH IM 2500/3000/3500/4000/5000/6000 Enhanced Security Firmware 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 2500/3000/3500/4000/5000/6000 Enhanced Security Firmware 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 Intel Goldmont CPU and runs LPUX 6.0 OS, a customized OS based on NetBSD; 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. 2500 performs 25 copies per minute, 3000 performs 30 copies per minute, 3500 performs 35 copies per minute, 4000 performs 40 copies per minute, 5000 performs 50 copies per minute, 6000 performs 60 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 are version JE-1.10-H.

- 9
10

Table 1: TOE Models

Branding	TOE Models
RICOH	IM 2500, IM 2500A, IM 2500G, IM 3000, IM 3000A, IM 3000G, IM 3500, IM 3500A, IM 3500G, IM 4000, IM 4000A, IM 4000G, IM 5000, IM 5000A, IM 5000G, IM 6000, IM 6000G
SAVIN LANIER	IM 2500, IM 2500A, IM 2500G, IM 3000, IM 3000A, IM 3000G, IM 3500, IM 3500A, IM 3500G, IM 4000, IM 4000G, IM 5000, IM 5000G, IM 6000, IM 6000G
nashuatec Rex Rotary Gestetner	IM 2500, IM 2500A, IM 3000, IM 3000A, IM 3500, IM 3500A, IM 4000, IM 4000A, IM 5000, IM 5000A, IM 6000

Table 2: Machine Firmware and Hardware

Primary Classification	Secondary Classification	Version
Firmware	TOE Version	E-1.00-H
	System/Copy	5.37
	Network Support	20.40
	Web Support	3.00.4
	Fax	05.30.00

Primary Classification	Secondary Classification	Version
	Scanner	05.02
	Web Uapl	3.00.3
	NetworkDocBox	5.34
	animation	1.00
	Printer	5.34
	GraphicData	1.01
	MovieData	1.00
	MovieData2	1.00
	MovieData3	1.00
	Data Erase Onb	1.05
	GWFCU3.8-26(WW)	04.00.00
	CheetahSystem	5.37.00
	decolet	3.01.00
	iwnnimeml	2.8.201
	simpleprinter	1.02
	smartprtstoredj	1.02
	smartcopy	1.03
	smartfax	1.06

Primary Classification	Secondary Classification	Version
	smartscanner	1.03
	stopwidget	1.01
Hardware	Ic Ctlr	03
	Ic Key	01024704

Table 3: Drivers

Drivers	Model
Printer Driver	PCL6 Driver 1.0.0.0
LAN-Fax Driver	LAN-Fax Driver 9.5

1.3.3 Evaluated Functions

11

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 HDD 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.
- 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 can be configured to use TLS to protect communication with the syslog, LDAP 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.
- k) **Image Overwrite.** the TOE actively overwrites residual image data stored on the HDD after a document processing job has been completed or cancelled.

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

1.3.4 Evaluation Assumptions

13 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

14 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

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

Table 5: Related Documents

Reference	
[ADMIN]	Ricoh IM 2500/3000/3500/4000/5000/6000 Series User Guide User Guide
[SECURITY]	Ricoh IM 2500/3000/3500/4000/5000/6000 Series User Guide Security Guide
[SECURITY REFERENCE]	Ricoh IM 2500/3000/3500/4000/5000/6000 Series User Guide User Guide Security Reference
[FIRMWARE]	Ricoh IM 2500/3000/3500/4000/5000/6000 Series User Guide Checking Firmware Validity
[WEB IMAGE MONITOR]	Ricoh IM 2500/3000/3500/4000/5000/6000 Series User Guide Using Web Image Monitor
[REGISTER ADMINISTRATOR]	Ricoh IM 2500/3000/3500/4000/5000/6000 Series User Guide Registering Administrators Before Using the Machine
[PREPARE SERVER]	Ricoh IM 2500/3000/3500/4000/5000/6000 Series User Guide Preparing the Server to Use for User Authentication
[LDAP SERVER]	Ricoh IM 2500/3000/3500/4000/5000/6000 Series User Guide Registering the LDAP Server

Reference	
[FAX]	Ricoh IM 2500/3000/3500/4000/5000/6000 Series User Guide Registering Fax Numbers in the Address Book
[LOGS]	Ricoh IM 2500/3000/3500/4000/5000/6000 Series User Guide Collecting Logs
[USER MANAGEMENT]	Ricoh IM 2500/3000/3500/4000/5000/6000 Series User Guide Introduction and Basic Operations

16

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

2 Secure Acceptance and Update

2.1 Obtaining the TOE

17 The TOE is delivered via commercial carrier.

2.2 Verifying the TOE

18 To verify the TOE Model, check that the machine's model number on the label to the rear of the machine ends with -18 which correspond to the branding variants of RICOH IM C2000G/C2500G/C3000G/C3500G/C4500G/C6000G included in the evaluated configuration.

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

20 On the Operation Panel:

- a) -Press [Home]
- b) -Press [Settings]
- 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

21 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.

22 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.

23 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

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

- 25 For MFP Control or FCU Software, the TOE performs the following verifications installing the package:
- a) Identifies the type of software (e.g., MFP Control, Operation Panel, FCU)
 - 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, FCU)
 - b) Verifies that the software model name matches the TOE
 - c) Verifies the digital signature

3 Configuration Guidance

3.1 Installation

26 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

27 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

28 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

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

30 32-bit driver

31 X86\DRIVERS\LAN-FAX\X86\DISK1

32 64-bit driver

33 X64\DRIVERS\LAN-FAX\X64\DISK1

3.2 Administration Interfaces

34 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

35 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.

36 Change the screen type from "Classic" to "Standard" in "Switch Screen Type" in "Administrator Tools" in "System Settings" in "Settings" and reboot the machine.

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

- s) Modification of stored file has not been rated for CC conformance.
- t) When you specify "HDD Erase Method" in "Erase All Memory", do not select "Format".
- u) 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".
- v) 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".
- w) 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".
- x) Do not assign "Reception File Settings" to a Quick Operation key in Fax mode.
- y) 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	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	[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
Printer	Google Cloud Print Settings ▶Google Cloud Print	Select [Off], and then press [Start registration].
Printer	Permissions for Printer Language to Operate File System ▶PDF,PostScript	[Do not Permit]

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

- z) When you delete all logs, make sure that the following functions are not being used:
- i) Scan file transmission
- aa) When switching from [On] to [Off] in [Document Server Function] in [Settings for Administrator] in [System Settings], delete all the received fax documents and specify the following settings again:
1. System Settings
 2. Settings for Administrator -> File Management -> Document Server Function -> Select [On]
 3. Fax Settings
 4. Reception Settings -> Reception File Settings -> Store [On]
 5. Reception Settings -> Reception File Settings -> Print [Off]
The stored fax files can be accessed via Document Server even if the machine is not equipped with the file format converter. For information on how to use it, see Document Server.
- If [Download File Directly From URL Link] in [General Settings] in [Scanner Settings] is set to [Off], the URL of the scanned and stored files cannot be sent by e-mail.
- bb) Sending a fax from a computer
1. On the computer, open the file to send, 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. Click [Send].
 - To store the sent file on the Document Server, check [Send to Document Server] on the [Document Server] tab before clicking [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 Administrators 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.
- 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.
- 41 Uninstall the following applications according to [Uninstalling an Application] in [Installing an Application from Application Site] in [Introduction and Basic Operations].
- CAP Java Card Plug-in
 - CAP NFC Plug-in
 - CAP [uma]-G2 Plug-in
 - CAP User Config.
 - CAP V2 Auth. UI
 - ELP NX

3.3.1.1 System Settings

- 42 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.

Tab	Item	Settings
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	Date/Time ▶ 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
Network/Interface	Effective Protocol ▶IPv4	[Active]
Network/Interface	Effective Protocol ▶IPv6	[Inactive]
Network/Interface	SMB ▶SMB Client Advanced Settings ▶SMBv2/SMBv3	[Inactive]
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]
Network/Interface	External Interface Software Settings ▶Select IC Card Reader	[Do not Use]
Network/Interface	USB Port ▶USB Port	[Inactive]

Tab	Item	Settings
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".
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
	<ul style="list-style-type: none"> ▶ Basic Authentication ▶ Available Functions 	
Settings for Administrator	Authentication/Charge <ul style="list-style-type: none"> ▶ Administrator Authentication/User Authentication/App Auth. ▶ User Authentication Management ▶ Basic Authentication ▶ Available Functions ▶ Printer Job Authentication 	[Entire]
Settings for Administrator	Authentication/Charge <ul style="list-style-type: none"> ▶ Administrator Authentication/User Authentication/App Auth. ▶ Setting for Entering Authentication Password 	[Only 1 Byte Characters]
Settings for Administrator	Authentication/Charge <ul style="list-style-type: none"> ▶ 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 <ul style="list-style-type: none"> ▶ Administrator Authentication/User Authentication/App Auth. ▶ User's Own Customization 	[Prohibit]
Settings for Administrator	Authentication/Charge <ul style="list-style-type: none"> ▶ 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 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 Settings ▶ Update Firmware	[Prohibit]
Settings for Administrator	Security ▶ Extended Security Settings ▶ Change Firmware Structure	[Prohibit] After specifying this setting, be sure to click [OK].
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.

Tab	Item	Settings
		(Note — The TOE requires minimum password length of 15 characters).
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 ▶ Auto Erase Memory Setting	Select [On], and then select [NSA], [DoD], or [Random Numbers]. If you set this to [Random Numbers], set [Number of Erase] to three or more.
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	File Management ▶ Auto Delete File in Document Server	Select [Specify Days], [Specify Hours] or [Off]

Tab	Item	Settings
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]
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]

Tab	Item	Settings
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

43 The TOE is configured to local authentication labeled [Basic Authentication] or external authentication labeled [LDAP Authentication], using an LDAP Server in its operational environment. The TOE supports both methods of user authentication, but both cannot be enforced on the same running instance of the TOE. 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. Set the browser to [Unavailable].

Tab	Item	Settings
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

- 44 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 8: 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.

Tab	Item	Settings
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

45 The administrator must configure the printer settings within the range specified in Table 9.

Table 9: 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]

Tab	Item	Settings
Data Management/Maintenance	Print Jobs ▶ Auto Store Jobs Without User Authentication Information	Select [Off]
Data Management/Maintenance	Administrator Tools ▶ Prohibit List/Test Print	[On]

3.3.1.4 Scanner Settings

46 The administrator must configure the scanner settings as specified in Table 10.

Table 10: 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

47 The administrator must configure the fax settings as specified in Table 11.

Table 11: Fax Settings

Tab	Item	Settings
Send Settings	Backup File Transmission Setting	[Off]
Reception Settings	Reception File Settings ▶ Action on Receiving File ▶ Store	[On]

Tab	Item	Settings
Reception Settings	Reception File Settings ▶ Action on Receiving File ▶ Forwarding	[Off]
Reception Settings	Reception File Settings ▶ Action on Receiving File ▶ Print	[Off]
Reception Settings	Reception File Settings ▶ Action on Receiving File ▶ Memory Lock Reception	[Off]
Reception Settings	Reception File Settings ▶ Reception File Storing Error Setting ▶ When a File Storing Error Occurs	[Do not Receive]
Reception Settings	Reception File Settings ▶ Reception File Storage Location	[Fax Memory]
Reception Settings	Box Setting ▶ Register/Change/Delete Box	Do not specify (register) the items in this setting.
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.

Tab	Item	Settings
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]

3.3.2 Procedure 2 – Setting Specified using WIM

48 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

49 The administrator sets the values in [Device Settings] as specified in Table 12.

Table 12: 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]
Device Settings	Logs ▶ Common Settings for All Logs ▶ Transfer Logs	[Inactive]
Device Settings	SYSLOG Transfer ▶ Transfer SYSLOG Server	[Active]

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.

3.3.2.2 Excluded Printer Features

50 On the WIM interface, the administrator configures the settings for [printer] with the values specified in Table 13.

Table 13: Excluded Printer Features

Category	Item	Settings
Printer	Basic Settings ▶ Virtual Printer	[Inactive]
Printer	Permissions for Printer Language to Operate File System ▶ PDF,PostScript	[Do not Permit]
Printer	Google Cloud Print Settings ▶ Google Cloud Print	Select [Off], and then press [Start registration].

3.3.2.3 Excluded Fax Features

51 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	IP-Fax Settings ▶ Enable H.323	[Off]

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

3.3.2.4 Network Settings

52 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]

3.3.2.5 Security Settings

53 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. TLSv1.2 is also used for communication with Syslog and SMTP and LDAP servers.

54 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.

55 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. All LDAP user authentication attempts will be denied while the trusted channel to an LDAP server is disrupted.

56 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](#).

57 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.

3.3.2.5.1 Cryptographic Settings –

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

Table 16: 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-4096 sha512WithRSA-2048 sha256WithRSA-4096 sha256WithRSA-2048 See the Security Guide for the other necessary 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-4096 sha512WithRSA-2048 sha256WithRSA-4096 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.

Category	Item	Settings
Security	Device Certificate ▶ Certification ▶ S/MIME	Select the installed device certificate.
Security	Network Security ▶ Security Level	[FIPS 140] After setting this to [FIPS 140], be sure to click [OK].
Security	Network Security ▶ TCP/IP ▶ IPv6	[Inactive]
Security	Network Security ▶ HTTP - Port 80 ▶ IPv4	[Close] Doing this will also set "IPv4" to [Close] in "Port 80" in "IPP".
Security	Network Security ▶ SSL/TLS Version	Set "TLS1.2" to [Active], and "TLS1.3", "TLS1.1", and "TLS1.0" to [Inactive].
Security	Network Security ▶ Encryption Strength Setting	Check "AES128" and/or "AES256", and uncheck "3DES".
Security	Network Security ▶ TCP/IP ▶ KEY EXCHANGE ▶ RSA	[Inactive]
Security	Network Security ▶ TCP/IP ▶ DIGEST ▶ SHA1	[Inactive]

Category	Item	Settings
Security	Network Security ▶FTP ▶IPv4	[Inactive]
Security	Network Security ▶WSD (Device) ▶IPv4	[Inactive]
Security	Network Security ▶WSD (Printer)	[Inactive]
Security	Network Security ▶WSD (Scanner)	[Inactive]
Security	Network Security ▶SNMP	[Inactive]
Security	S/MIME ▶Encryption Algorithm	Select [AES-256 bit], or [AES-128 bit]. When using S/MIME, it is necessary to register the user certificate.
Security	S/MIME ▶Digest Algorithm	Select [SHA-512 bit], [SHA-384 bit], or [SHA-256 bit].
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]

Category	Item	Settings
Security	User Lockout Policy ▶ Lock Out User for	1-9999

3.3.2.6 WIM Auto Logout Settings

59 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 minutes Note that the default setting is 60 minutes.

3.3.3 Procedure 3 – Additional Settings Using the Operation Panel

60 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

61 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.

Tab	Item	Settings
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

62 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 19.

Table 19: 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.

3.3.4 Verifying the MFP Settings

63 After completing procedure 1 through procedure 3, check the log data and ROM version with the following steps:

- a) Check that the machine is OFF
- b) Turn the machine ON.
- c) Check the details of the Log files that were stored in the machine. Check that the details for "Log Type", "Result", and "Module Name" in the recorded access log are as follows:
 - i) Log Type: Firmware: Structure
 - ii) Result: Succeeded
 - iii) Module Name: G3
 - iv) For additional details about logs, see “Collecting Logs”, “Managing Devices”, settings.

- d) Login as admin to the Operation Panel and check the fax parameter settings with the following steps:
 - i) Press [Settings]
 - ii) Press [Fax Settings]
 - iii) Press [Detailed Initial Settings]
 - iv) Press [Parameter Settings: Print List]
 - v) Check that the following ROM version matches the one shown in the printed list: [ROM Version]
G3: 04.00.00 (Validation Data: F3AB)
- e) Log off

3.4 Services

3.4.1 Firewall

64 See System Settings

3.4.2 Syslog Server

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

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

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

68 -Select 'Inactive' for Verification of Syslog Server Certificate

69 For additional information see "[Collecting Logs](#)" in the User Guide.

70 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.

71

3.4.3 LDAP Server

72 [Registering the LDAP Server](#) in the Settings page of the online User Guide provides instructions for configuring the LDAP server that the TOE will use for user authentication. Server information to be configured includes:

- a registration name for the LDAP server
- host name or IPv4 address of the LDAP server
- a root folder to store email addresses
- port number used for communication with the LDAP server (636)
- Use Secure Connection (SSL) is set to [ON]
- Digest Authentication

73 Additional settings for the LDAP server are described in Table 8: LDAP Authentication.

3.4.4 CAC/PIV Authentication Solutions

- 74 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

- 75 See Administration Interfaces above.
- 76 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
Configure minimum password length	Modify	Operation Panel
Configure Password complexity settings	Modify	Operation Panel
Configure Operation Panel Auto Logout Time	Modify	Operation Panel
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
Configure image overwrite	Modify	Operation Panel

Management Functions	Enable	Interface(s)
Configure network settings for trusted communications (specify IP addresses and port to connect to the TOE)	Modify	Operation Panel, WIM
Manage HDD Cryptographic key	Create Delete	Operation Panel, WIM
Manage Device Certificates	Create, query, modify, delete, upload, download	Operation Panel, WIM
Manage TOE Trusted Update	Query, Modify	WIM
Configure SMTP over TLS	Modify	WIM
Configure LDAP over TLS	Modify	Operation Panel, WIM
Configure syslog over TLS	Modify	WIM
Manage user accounts (Ability to login)	Unlock	WIM

3.6 Management of Security Functions

77 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

78 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 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.

Tab	Item	Settings
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.
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 <ul style="list-style-type: none"> ▶ 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.
Settings for Administrator	Data Management <ul style="list-style-type: none"> ▶ Auto Erase Memory Setting 	Select [On], and then select [NSA], [DoD], or [Random Numbers]. If you set this to [Random Numbers], set [Number of Erase] to three or more.

3.6.2 Functions Managed via the WIM

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

3.6.2.1 SMTP Settings

80 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 <ul style="list-style-type: none"> ▶ Administrator Email Address 	Enter the administrator's email address.
Device Settings	Email <ul style="list-style-type: none"> ▶ SMTP Server Name 	Enter the SMTP server name or IP address.

3.6.2.2 Security Settings

81 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. Set "Algorithm Signature" to one of the following: sha512WithRSA-4096 sha512WithRSA-2048 sha256WithRSA-4096 sha256WithRSA-2048
Security	Device Certificate ▶Certificate 1 ▶Request	Create a certificate request Set "Algorithm Signature" to one of the following: sha512WithRSA-4096 sha512WithRSA-2048 sha256WithRSA-4096 sha256WithRSA-2048 Submit the request Install the issued certificate
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	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	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

82 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 minutes Note that the default setting is 60 minutes.

3.6.3 User Management

83 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.

84 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

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

3.6.5 Default Passwords

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

3.6.6 Password Management

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

3.6.7 Setting Time

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

3.6.8 Audit Logging

89 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.

90 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.

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

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

3.7 U_NORMAL User Access

93 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

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

95 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.

96 This deletion function is outside the scope of the evaluation. See the [Security Guide](#) for additional information.

5 Annex A: Log Reference

5.1 Format

97 The TOE generates audit records for all required auditable events. Each audit record includes time and date, type of event, user identify (if applicable), and the outcome of events.

5.2 Events

98 The TOE generates the following log events.

Table 25: Audit Events

Requirement	Auditable Events	Additional Details
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	Additional Details
	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_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 print driver Failure of communication with fax driver