RICOH

RICOH Pro C5300S/C5310S

Common Criteria Guide

Version 0.6

December 2020

Document prepared by

www.lightshipsec.com

Table of Contents

List of Tables

1 About this Guide

1.1 Overview

1 This guide provides supplemental instructions to achieve the Common Criteria evaluated configuration of the RICOH PRO C5300S/C5310S 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: Pro C5300S and Pro C5310S 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 ® Atom Processor Apollo Lake (E3940 or E3930) 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 TOE model number correspond to copy speed, e.g. 5300 performs 65 prints per minute, 5310 performs 80 prints 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. The TOE version JE-1.00-H includes the TOE models listed in Table 1, the firmware and hardware listed in Table 2 as well as the printer drivers and LAN Fax Drivers listed in Table 3.

Table 1: TOE Models

Branding	Model
RICOH	RICOH Pro C5300S

Branding	Model
	RICOH Pro C5310S
SAVIN	Savin Pro C5300S
	Savin Pro C5310S
LANIER	Lanier Pro C5300S
	Lanier Pro C5310S
nashuatec	nashuatec Pro C5300S
	nashuatec Pro C5310S
Rex Rotary	Rex Rotary Pro C5300S
	Rex Rotary Pro C5310S
Gestetner	Gestetner Pro C5300S
	Gestetner Pro C5310S
infotec	infotec Pro C5300S
	infotec Pro C5310S

Table 2: Machine Firmware and Hardware

Primary Classification	Secondary Classification	Version
Firmware	System/Copy	1.02
	Network Support	19.21
	Web Support	1.02
	Fax	01.00.00
	Scanner	01.01
	Web Uapl	1.00
	NetworkDocBox	1.01.1

Primary Classification	Secondary Classification	Version
	animation	1.00
	Printer	1.01
	GraphicData	1.01
	MovieData	1.01
	MovieData2	1.01
	MovieData3	1.01
	Data Erase Onb	1.05
	GWFCU3.8-25(WW)	01.00.00
	CheetahSystem	1.02
	decolet	3.00.02
	iwnnimeml	2.8.201
	pptop	1.00
	simpleprinter	1.00
	smartcopy	1.01
	smartfax	1.00
	smartprtstoredj	1.00
	smartscanner	1.00
	stopwidget	1.00

Primary Classification	Secondary Classification	Version
Hardware	Ic Ctlr	03
	Ic Key	01024704

Table 3: Drivers

Drivers	Model
Printer Driver	PCL6 Driver 1.0.0.0
	RPCS Driver 1.0.0.0
LAN-Fax Driver	LAN-Fax Driver 9.5.0.0
	PCFAX Driver 9.3.0.0

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 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. It uses an NTP server for accurate time.

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

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

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.

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	
[INSTALL]	RICOH Pro C5300S/C5310S Series User Guide Introduction and Basic Operations
[ADMIN]	RICOH Pro C5300S/C5310S Series User Guide User Guide Security Reference

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, -29 or -00 which correspond to the branding variants of RICOH PRO C5300S/C5310S 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 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

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

f) In the event of a hard disk error, the machine will display options to initialize the disk or not. Note that user authentication might fail after a hard disk initialization, if this happens, contact the service representative.

g) 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.

h) When using Scan to Folder complete the following steps:

1. The Scan to Folder destination (FTP or SMB server) must be registered in the address book by the administrator.
2. When you register the Scan to Folder destination in the address book, go to "Protection -> Protect Destination -> Access Privileges" Click [Change] and then and then select [Read- only] for users who are allowed to access the Scan to Folder destination.
3. Configure IPsec for the server selected as the Scan to Folder destination

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) 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).

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

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

n) 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.

o) 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.

p) When you specify "HDD Erase Method" in "Erase All Memory", do not select "Format".

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

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

i) Scan file transmission

ii) When switching from [On] to [Off] in [Document Server Function] in [Administrator Tools] in [System Settings], delete all the received fax documents and specify the following settings again:

1. System Settings
2. Administrator Tools -> Document Server Function -> Select [On]
3. Fax Settings
4. Reception Settings -> Reception File Settings -> Store [On]
5. Reception Settings -> Reception File Settings -> Print [Off]

s) 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

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 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.

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 "Copier (Classic)", "Scanner (Classic)", "Fax (Classic)" "settings", "Printer", "Document Server (Classic)", "Address Book", "Fax RX File Widget". 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.

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. **Note:** Set the same range of minutes for auto-logout and the auto-sleep timer.
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	[Active]
Network/Interface	IEEE 802.1X Authentication for Ethernet	[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". **Note:** This operation can only be performed by the supervisor.
Settings for Administrator	Authentication/Charge ▶Administrator Authentication/User Authentication/App Auth. ▶Setting for Entering Authentication Password	[Only 1 Byte Characters]
Settings for Administrator	Authentication/Charge ▶Administrator Authentication/User Authentication/App Auth. ▶Application	Set [Copier Function], [Printer Function], [Document Server Function], [Fax Function] and [Scanner Function] to [On].

Tab	Item	Settings
	Authentication Management	
Settings for Administrator	Authentication/Charge ▶Administrator Authentication/User Authentication/App Auth. ▶User's Own Customization	[Prohibit]
Settings for Administrator	Authentication/Charge ▶Administrator Authentication/User Authentication/App Auth. ▶LDAP Search	[Off]]
Settings for Administrator	Security ▶Extended Security Settings ▶Restrict Display of User Information	[On]
Settings for Administrator	Security ▶Extended Security Settings ▶Restrict Adding of User Destinations (Fax)	[On]
Settings for Administrator	Security ▶Extended Security Settings ▶Restrict Adding of User Destinations (Scanner)	[On]
Settings for Administrator	Security ▶Extended Security Settings ▶Restrict Use of Destinations (Fax)	[On]
Settings for Administrator	Security ▶Extended Security Settings	[On]

Tab	Item	Settings
	▶Restrict Use of Destinations (Scanner)	
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]
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" and “5”, and then "#". Note — The TOE requires minimum of 15 characters. Passwords must be composed of any combination of upper and lower case letters, numbers and the following special characters: [“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, [[“"”, “‘”, “+”, “,”, “-”, “.”, “/”, “:”, “;”, “<”, “=”, “>”, “?”, “[”, “\”, “]”, “_”, “`”, “{”, “|”, “}”, “~”]].

Tab	Item	Settings
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 ▶Job Execution Restrictions When Log Limit is Reached	[Off]
Settings for Administrator	Data Management ▶Transfer Log Setting	[Do not Forward]
Settings for Administrator	File Management ▶Machine Data Encryption Settings	Ensure that the current data has been encrypted. If the data has been encrypted, the following message will appear: "The current data in the machine has been encrypted."
Settings for Administrator	File Management ▶Auto Delete File in Document Server	Select [Specify Days], [Specify Hours] or [Off]
Settings for Administrator	File Management ▶Document Server Function	Select [On]

Tab	Item	Settings
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	[ON]
Machine	Power/Energy Saving ▶Shift to Main Power-Off When Network Disconnected (mainly Europe and Asia)	[Off]
Machine	Power/Energy Saving ▶Main Power On by Remote Operation	[Inactive]
Machine	External Device ▶Control Panel SD Card Slot	[Inactive]
Machine	External Device ▶Control Panel USB Memory Slot	[Inactive]

Tab	Item	Settings
Machine	External Device ▶Allow Media Slots Use ▶Store to Memory Storage Device	[Prohibit]
Machine	Others ▶Central Management	[Do not Manage Centrally]
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 do either local authentication specified as [Basic Authentication] or external authentical using an LDAP Server in its operational environment specified as [LDAP Authentication]. The TOE supports both methods of user authentication. The administrator configures User Authentication in [System Settings] -> [Administrator Tools (System Settings)] with the following settings:

3.3.1.2.1 Basic Authentication Settings

Table 7: Basic Authentication

Tab	Item	Settings
Administrator Tools	Authentication/Charge ▶Administrator Authentication/User Authentication/App Auth. ▶User Authentication Management	[Basic Authentication.]
Administrator Tools	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
Administrator Tools	Authentication/Charge ▶Administrator Authentication/User Authentication/App Auth. ▶User Authentication Management ▶Basic Authentication. ▶Available Functions ▶Printer Job Authentication	[Entire]

3.3.1.2.2 LDAP Authentication Settings

39 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 Sections 'Preparing the Server to Use for User Authentication" and "Registering the LDAP Server"

Table 8: LDAP Authentication

Tab	Item	Settings
Administrator Tools	Authentication/Charge ▶Administrator Authentication/User Authentication/App Auth. ▶User Authentication Management	[LDAP Authentication.]
Administrator Tools	Authentication/Charge ▶Administrator Authentication/User Authentication/App Auth. ▶User Authentication Management ▶LDAP Authentication ▶LDAP Servers	Select the LDAP server to authenticate.

Tab	Item	Settings
Administrator Tools	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]
Administrator Tools	Authentication/Charge ▶Administrator Authentication/User Authentication/App Auth. ▶User Authentication Management ▶LDAP Authentication ▶Printer Job Authentication	[Entire]

3.3.1.3 Printer Settings

40 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 ▶Restrict Direct Print Jobs	[Automatically Store Jobs]
Data Management/Maintenance	Print Jobs ▶Auto Store Jobs Without User Authentication Information	[Off]
Data Management/Maintenance	Administrator Tools ▶ Prohibit List/Test Print	[On]

3.3.1.4 Scanner Settings

41 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

42 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]

Tab	Item	Settings
Reception Settings	Reception File Settings ▶Action on Receiving File ▶Store	[On]
Reception Settings	Reception File Settings ▶Action on Receiving File ▶Forwarding	[Off]
Reception Settings	Reception File Settings ▶Action on Receiving File ▶Print	[Off]
Reception Settings	Reception File Settings ▶Action on Receiving File ▶Memory Lock Reception	[Off]
Reception Settings	Reception File Settings ▶Reception File Storing Error Setting	[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 become 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

43 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.

3.3.2.1 Device Settings

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

Table 12: Settings for Audit Log Collection

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	SYSLOG Transfer →SYSLOG Destination	Enter <IP Address> and <Port number> of the remote syslog server.
Device Settings	SYSLOG Transfer →Verification of SYSLOG Server Certificate	[INACTIVE]
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. **Note:** The TOE uses either IPsec or TLS to provide a trusted channel with the SMTP server.
Device Settings	File Transfer	Enter ‘FTP User Name” and ‘FTP password’. Note: Do not set anything for SMB settings.

3.3.2.2 Printer Settings

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

Table 13: Printer Settings

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

Category	Item	Settings
Printer	Google Cloud Print Settings ▶Google Cloud Print	Select [Off], and then press [Start registration].

3.3.2.3 Fax Settings

46 On the WIM interface, the administrator configures the settings for [Fax] with the values specified in Table 14Table 13.

Table 14: Fax Settings

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

3.3.2.4 Network Settings

47 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

48 The TOE includes FIPS validated cryptographic modules which it uses to provide its cryptographic services. The TOE uses IPsec for communication with LDAP, FTP, Syslog, SMTP and NTP servers. The TOE uses TLSv1.2 for remote administration via WIM and for communication with remote non-administrative users.

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

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

51 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 connection is re-established, the TOE will resume transmission of the audit records. All LDAP user authentication attempts will be denied while the trusted channel to an LDAP server is disrupted.

52 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.

53 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 IPSEC

54 The TOE supports only IKEv1 Main Mode. IKEv1 Aggressive mode must be disabled by using telnet to login to the MFP. In the evaluated configuration, Telnet is disabled by default, enable it using the WIM and go to Security->Network Security and select ‘Enable telnet for IPv4. Use the following steps to disable aggressive mode; disable telnet again once the steps are completed.

a) -Telnet to the MFP using the admin account for login

b) -At the the “msh>” command prompt, enter the command “ipsec aggressive_mode off”

c) -At the“msh>” command prompt, exit the system by enter the command “logout”

d) -At the “Do you save configuration data? (yes/no/return)” prompt enter “yes”.

55 Launch the WIM to configure the following settings

3.3.2.5.2 Installing a certificate on an IPsec Server

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

57 -Log in to the administrator with WIM

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

59 -Select “Base 64 encoded X.509” and export

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

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

62 For additional details see the Security Guide section on “Encrypting Network Communication”

3.3.2.5.3 Cryptographic Settings –

63 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-2048 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-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.

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

Category	Item	Settings
Security	Network Security ▶TCP/IP ▶KEY EXCHANGE ▶RSA	[Inactive]
Security	Network Security ▶TCP/IP ▶DIGEST ▶SHA1	[Inactive]
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. **Note:** It is mandatory to ensure that certificate has an email address RDN that matches the email address that the TOE that is registered in the user account.

Category	Item	Settings
Security	S/MIME ▶Digest Algorithm	Select [SHA-512 bit], [SHA-384 bit], or [SHA-256 bit].
Security	S/MIME ▶When Sending Email by Scanner	[Use Signatures]
Security	S/MIME ▶When Transferring by Fax	[Use Signatures]
Security	S/MIME ▶When Sending Email by Fax	[Use Signatures]
Security	S/MIME ▶When Emailing TX Results by Fax	[Use Signatures]
Security	S/MIME ▶When Transferring Files Stored in Document Server (Utility)	[Use Signatures]
Security	IPsec ▶IPsec	Select [Active]
Security	IPsec ▶Encryption Key Auto Exchange Settings ▶Encapsulation Mode	[Transport Mode]
Security	IPsec ▶Encryption Key Auto Exchange Settings ▶Address Type	[IPv4]

Category	Item	Settings
Security	IPsec ▶Encryption Key Auto Exchange Settings ▶Local Address	The machine's IP address
Security	IPsec ▶Encryption Key Auto Exchange Settings ▶Remote Address	Connected server's IP address Set the IP addresses of all servers that will be protected using IPsec traffic including: FTP server Syslog server SMTP server NTP server LDAP server **Note**: the TOE evaluated configuration supports protection of Syslog and SMTP traffic using either TLS or IPsec.
Security	IPsec ▶Encryption Key Auto Exchange Settings ▶Security Level	[Authentication and High-Level Encryption] Set Default Settings to [PROTECT] Settings 1 through Settings 4, set values [PROTECT] [BYPASS] [DISCARD]
Security	IPsec ▶Encryption Key Auto Exchange Settings ▶Security Policy	[Apply]

Category	Item	Settings
Security	IPsec ▶Encryption Key Auto Exchange Settings ▶Authentication Method	[Certificate] or [PSK]. If you select PSK, press the “Change” button for “PSK Text” to set PSK. “PSK Text” is limited (truncated) to 32 characters; is composed of any combination of upper and lower-case characters, numbers and special characters that include and (that include: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “)”). Note: It is recommended that long “PSK Text” composed of all permitted characters should be chosen as this is considered more secure.
Security	IPsec ▶Encryption Key Auto Exchange Settings ▶Hash Algorithm	Select [SHA256], [SHA384], or [SHA512].
Security	IPsec ▶Encryption Key Auto Exchange Settings ▶Encryption Algorithm	Select [AES-128-CBC] or [AES-256-CBC].
Security	IPsec ▶Encryption Key Auto Exchange Settings ▶Diffie-Hellman Group	[14]
Security	IPsec ▶Encryption Key Auto Exchange Settings ▶Authentication Algorithm	Check [HMAC-SHA256-128], [HMAC-SHA384-192] and [HMAC-SHA512-256], and uncheck [HMAC-SHA1-96] and [HMAC-MD5-96].

Category	Item	Settings
Security	IPsec ▶Encryption Key Auto Exchange Settings ▶Encryption Algorithm Permissions	Check [AES-128] and [AES-256], and uncheck [Cleartext], [DES] and [3DES].
Security	IPsec ▶Encryption Key Auto Exchange Settings ▶PFS	[14]
Security	User Lockout Policy ▶Lockout	[Active]
Security	User Lockout Policy ▶Number of Attempts before Lockout	1-5
Security	User Lockout Policy ▶Lockout Release Timer	[Active]
Security	User Lockout Policy ▶Lock Out User for	1-9999

3.3.2.6 WIM Auto Logout Settings

64 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 The default settings is 60

3.3.3 Procedure 3 – Additional Settings Using the Operation Panel

65 After completing the configurations in Procedure 2 using the WIM interface, the administrator must go back to the Operation Panel and login to continue with the following settings.

3.3.3.1 System Settings

66 The administrator must configure additional values for [System] settings as 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 Management	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

67 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

68 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: 01.00.00 (Validation Data: 2BA7)

e) Log off

3.4 Services

3.4.1 Firewall

69 See System Settings

3.4.2 Syslog Server

70 See Table 12: Settings for Audit Log Collection.

3.4.3 LDAP Server

71 Registering the LDAP Server in the Setup/System 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:

72 -a registration name for the LDAP sever

73 -host name or IPv4 address of the LDAP server

74 -a root folder to store email addresses

75 -port number used for communication with the LDAP server (636)

76 -Use Secure Connection (SSL) is set to [ON]

77 -Digest Authentication

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

3.4.4 NTP Server

79 See System Settings

3.4.5 FTP Server

80 See System Settings

3.4.6 SMTP Server

81 See System Settings

3.4.7 CAC/PIV Authentication Solutions

82 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

83 See Administration Interfaces above.

84 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

Management Functions	Enable	Interface(s)
Configure audit transfer settings	Modify	WIM
Manage audit logs	Query, delete, export	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 WIM
Configure WIM Auto Logout Time	Modify	WIM
Configure number of authentication failure before account lockout	Modify	WIM
Configure account release timer settings	Modify	WIM
Configure PSTN Fax-Line Separation Stored Reception File User	Modify	Operation Panel
Configure image overwrite	Modify	Operation Panel
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
Manage Device Certificates	Create, query, modify, delete, upload, download	Operation Panel[1], WIM
Manage TOE Trusted Update	Query, Modify	Operation Panel, WIM
Configure FTP	Modify	WIM
Configure IPsec	Modify	WIM

[1] Only certificate #1 can be created or deleted on the Operation Panel, that certificate is needed to bootstrap the web server for the WIM.

Management Functions	Enable	Interface(s)
Configure NTP	Modify	WIM
Configure LDAP	Modify	Operation Panel, WIM

3.6 Management of Security Functions

85 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

86 The following settings are available via Operation Panel 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.
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.

Tab	Item	Settings
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)].
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".

Tab	Item	Settings
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:** Only the supervisor admin can change the supervisor's login credentials.
Settings for Administrator	Security ▸Specifying the Extended Security Functions ▸Password Policy	Set "Complexity Setting" to [Level 1] or [Level 2], press [Change] on the right of "Minimum Character No.", and then set the number of characters to 15 or more. Note: Changes to the Password Policy are enforced only on passwords created after the policy is applied.
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.

3.6.2 Functions Managed via the WIM

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

3.6.2.1 SMTP Settings

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

Table 22: SMTP Settings

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

3.6.2.2 Security Settings

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

Table 23: Certificates and User Lockout Policy Settings

Category	Item	Settings
Security	Device Certificate ▶Certificate 1 ▶Create	Configure this setting to 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	Configure this setting to create a certificate request for a certificate authority to issue a new device certificate. Set "Algorithm Signature" to one of the following: sha512WithRSA-2048 sha256WithRSA-2048 Submit the certificate request Install the issued certificate via WIM.

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	Device Certificate ▶Certification ▶S/MIME	Select the installed device certificate.
Security	Device Certificate ▶Certification ▶IPsec	Select the installed device certificate.
Security	S/MIME ▶Encryption Algorithm	Select [AES-256 bit] or [AES-128 bit]. When using S/MIME, it is necessary to register the user certificate.
Security	S/MIME ▶Digest Algorithm	Select [SHA-512 bit], [SHA-384 bit], or [SHA-256 bit].
Security	IPsec ▶IPsec	Select [Active]
Security	IPsec ▶Encryption Key Auto Exchange Settings ▶Local Address	The machine's IP address

Category	Item	Settings
Security	IPsec ▶Encryption Key Auto Exchange Settings ▶Security Level	Set “Default Settings” to “PROTECT” Configure settings 1 through settings 4 with the values: PROTECT BYPASS INACTIVE
Security	IPsec ▶Encryption Key Auto Exchange Settings ▶Encapsulation Mode	[Transport Mode]
Security	IPsec ▶Encryption Key Auto Exchange Settings ▶Remote Address	Connected server's IP address Change the IP address of a server that the TOE uses including: FTP server NTP server LDAP server SMTP server Syslog server
Security	IPsec ▶Encryption Key Auto Exchange Settings ▶Authentication Method	[Certificate] or [PSK]. “PSK Text” is limited (truncated) to 32 characters; is composed of any combination of upper and lower-case characters, numbers and special characters that include and (that include: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “)”). Note: It is recommended that long “PSK Text” composed of all permitted characters should be chosen as this is considered more secure.

Category	Item	Settings
Security	IPsec ▶Encryption Key Auto Exchange Settings ▶Hash Algorithm	Select [SHA256], [SHA384], or [SHA512].
Security	IPsec ▶Encryption Key Auto Exchange Settings ▶Encryption Algorithm	Select [AES-128-CBC] or [AES-256-CBC].
Security	User Lockout Policy ▶Number of Attempts before Lockout	1-5
Security	User Lockout Policy ▶Lock Out User for	1-9999

3.6.2.3 Auto Logout Settings

90 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 The default value is 60.

3.6.3 User Management

91 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 Setup/System Settings pages of the online User Guide.

92 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

93 The System Settings in Procedure 1 above identifies the settings for managing the administrator roles in the TOE. The TOE maintains the administrator and supervisor roles.

3.6.5 Default Passwords

94 The TOE does not include default passwords, administrators are prompted to create administrator login during initial configuration.

3.6.6 Password Management

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

3.6.7 Setting Time

96 See Table 6 for the Time settings and Table 16 for settings to configure access to an NTP server for time synchronization.

3.6.8 Audit Logging

97 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.

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

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

100 Additional instructions for managing the audit logs are available in Collecting Logs in the Security pages of the RICOH online User Guide.

3.7 U_NORMAL User Access

101 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

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

103 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

104 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

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

5.2 Events

106 The TOE generates the following log events.

Table 25: Audit Events

Requirement	Auditable Events	Example Event
FAU_GEN.1	Start-up and shutdown of the audit functions	Tied to startup of the main power: "2020-09-09T17:00:10.0","2020-09-09T17:00:10.0","Main Power On","Completed","Succeeded","0x000000000001beff",,,"","","","","","","",""
		Tied to shutdown of the main power: "2020-09-09T16:58:47.0","2020-09-09T16:58:47.0","Main Power Off","Completed","Succeeded","0x000000000001befe",,,"","","","","","","",""
FDP_ACF.1	Job Completion	**Print:** "2020-09-02T17:21:08.0","2020-09-02T17:21:14.0","Report Printing","Succeeded","Control Panel","Completed",,"0xffffff88","admin1","0x000000000001b303","","","" [illegible] ,,,"Succeeded",,"Completed","","","0x000000000001b303","","","" [illegible] ,,,"Succeeded",,"Completed","","","0x000000000001b303","","","" [illegible] "Print","2020-09-02T17:21:08.0","2020-09-

Requirement	Auditable Events	Example Event
		02T17:21:14.0","","","","","","","1" ,"","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 000000001b364","",,"","",,,"","","" "" "" "" "" "" "" "" "" "" "" "" , ,, , ,,, , , , , , ,, , ,,,,,,,, "" "" "" "" "" "" "" "" "" "" "" , ,, ,, , , ,,,,, ,,,, ,, ,, , , , "" "" "" "" "" "" "" "" "" "" "" "" "" ,, , , , , , ,,, , , , , , , ,, "" "" "" "" "" "" "" "" "" "" "" "" "" , , ,, , , , , , , , , ,,,,, ,,,"Succeeded",,"Completed",,"", "","0x000000000001b364","",,"", "" "" "" "" "" "" "" "" "" "" "" "" "" ,,, , , , ,, , ,,, , , , , , , "" "" "" "" "" "" "" "" "" , , ,,,,,,,,, ,, ,, , , ,,,,, ,,,, ,, "" "" "" "" "" "" "" "" "" "",,"Scan ,, , , ,,, , , , , , File","2020-09- 03T09:24:09.0","2020-09- 03T09:24:10.0","","","","","",,"","", "" "" "" "" "" "" "" "" "" "" "" ,, , , , , , , , , ,,,,, ,,,"Failed",,"Failed","Data Transf er Interrupted","","","0x0000000000 01b364","",,"","",,,"","","",,"","",, "" "" "" "" "" "" "" "" "" "" "" , , , , , , ,, , ,,,,,,,,, ,, ,, , "" "" "" "" "" "" "" "" "" "" "" " , ,,,,, ,,,, ,, ,, , , ,,, , , , " "" "" "" "" "" "" "" "" "" "" "" "","S , , ,,, , , , , , , ,, , , , end","2020-09- 03T09:24:06.0","2020-09- 03T09:24:54.0","u1d","1234","","" " "" "" "" "" , , , , ,,,,, **Scan:** "2020-09-09T16:52:36.0","2020- 09- 09T16:52:47.0","Scanner: Sendi ng","Succeeded","Control Panel ","Completed",,"0x00000003","u 1","0x000000000001bee9","",,"", "" "" "" "" "" "" "" "" "" "" "" "" "" ,,, , , , ,, , ,,, , , , , , , "" "" "" "" "" "" "" "" "" , , ,,,,,,,,, ,, ,, , , ,,,,, ,,,, ,, "" "" "" "" "" "" "" "" "" "" "" "" "" ,, , , ,,, , , , , , ,,, , , , "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" , , , ,, , , ,, , , , , , , , "" "" "" , , ,,,,, ,,,"Succeeded",,"Completed",,"", "","0x000000000001bee9","",,"", "" "" "" "" "" "" "" "" "" "" "" "" "" ,,, , , , ,, , ,,, , , , , , , "" "" "" "" "" "" "" "" "" , , ,,,,,,,,, ,, ,, , , ,,,,, ,,,, ,, "" "" "" "" "" "" "" "" "" "",,"Scan ,, , , ,,, , , , , ,

Requirement	Auditable Events	Example Event
		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","","","","","","",,,,, **Document Server:** "2020-09-03T09:13:24.0","2020-09-03T09:13:28.0","Document Server: Storing","Succeeded","Control Panel","Completed",,"0x00000003","u1","0x0000000000001b349","",,"","",,,"","","","",,"","",,," ","","","","","",,"","",,,,,,,,,"",,"",,"", ,"",,,,,"",,,,"",,"",,"","",,,"","","","", "","",,,"","","","","","","",,"","","",,"", ","","","","","","","","",,,,, ,,,"Succeeded",,"Completed",,"", "","0x000000000001b349","",,"", "",,,"","","","",,"","",,,"","","","","","", ,"","",,,,,,,,,"",,"",,"","","",,,,,"",,,,"",, "",,"","","",,,"","","","","","",,"Scan File","2020-09-03T09:13:24.0","2020-09-03T09:13:28.0","","","","","",,"","", "",,"","","","","","","","","","",,,,, ,,,"Succeeded",,"Completed",,"", "","0x000000000001b349","",,"", "",,,"","","","",,"","",,,"","","","","","", ,"","",,,,,,,,,"",,"",,"","","",,,,,"",,,,"",, "",,"","","",,,"","","","","","",,,"","","", "","","","",,"","","","Store","2020-09-03T09:13:24.0","2020-09-03T09:13:28.0","","","903","COPY0012","0","","","",,,,, **Copy:** "2020-09-01T12:41:09.0","2020-09-01T12:41:19.0","Copier: Copying","Succeeded","Control Panel","Completed",,"0x00000003","u1","0x000000000001adf4","",,"","", ,,"","","","",,"","",,,"","","","","","",,"", ,"",,,,,,,,,"",,"",,"","","",,,,,"",,,,"",,"",, "","","",,"","","","","","",,"","","",""," ,",,,"","","","","",,,"","","",",

Requirement	Auditable Events	Example Event
		","","",,"","","",,"","","","","","","",""," ","",,,,, ,,,"Succeeded",,"Completed",,"", "","0x000000000001adf4","",,""," ",,,"","","","",,"","",,,"","","","","","",, "","",,,,,,,,,,"",,"",,"","","",,,,,"",,,,"",," ",,"","","",,,"","","","","","",,"Scan File","2020-09- 01T12:41:09.0","2020-09- 01T12:41:19.0","","","","","",,"","", "",,"","","","","","","","","","",,,,, ,,,"Succeeded",,"Completed",,"", "","0x000000000001adf4","",,""," ",,,"","","","",,"","",,,"","","","","","",, "","",,,,,,,,,,"",,"",,"","","",,,,,"",,,,"",," ",,"","","",,,"","","","","","",,,"","",""," ","","","",,"","","","Print","2020-09- 01T12:41:09.0","2020-09- 01T12:41:19.0","","","","","","","1" ,"","LT","normal",,,
FIA_UAU.1/ FIA_UID.1	Unsuccessful identification Unsuccessful authentication	Operation Panel "2020-09-03T09:13:00.0","2020- 09- 03T09:13:00.0","Login","Failed", ,"Password Mismatch",,"0x00000000","u1"," 0x000000000001b347","","Auth entication","","",,"Control Panel","","","","",,"","",,,"","","",""," ","",,"","",,,,,,,,,"",,"",,"","","",,,,,"",,, ,"",,"",,"","","",,,"","","","","","","Co mpleted",,"","","","","","","",,"","","" ,,"","","","","","","","","","",,,,,
		WIM "2020-09-09T16:35:58.0","2020- 09- 09T16:35:58.0","Login","Failed", ,"Password Mismatch",,"0x00000000","admi n","0x000000000001bea1","ip:1 72.16.200.10","Authentication"," ","",,"via Network","","","","",,"","",,,"","",""," ","","",,"","",,,,,,,,,"",,"",,"","","",,,,,"" ,,,,"",,"",,"","","",,,"","","","","","","C ompleted",,"","","","","","","",,"","", "",,"","","","","","","","","","",,,,,
FMT_SMF.1		Setting authentication lockout policies:

Requirement	Auditable Events	Example Event
	Use of a management function	"2020-08-26T14:58:16.0","2020-08-26T14:58:16.0","Machine Configuration","Succeeded",,"Succeeded",,"0xffffff88","admin1","0x00000000000195bf","","Device Settings","","",,,"","","","",,"","",,,"",,"","","","","",,"","",,,,,,,,,"",,"",,"","","",,,,,"",,,,"",,"",,"","","",,,"","User Lockout Policy","","","","","Completed",,"","","","","","","",,"","","",,"","","","","","","","","","",,,,, ,,,,,,,"","","0x00000000000195bf","","Device Settings","","",,,"","","","",,"","",,,"",,"","","","","",,"","",,,,,,,,,"",,"",,"","","",,,,,"",,,,"",,"",,"","","",,,"","","Number of Attempts before Lockout","4","","","Completed",,"","","","","","","",,"","","",,"","","","","","","","","","",,,,, ,,,,,,,"","","0x00000000000195bf","","Device Settings","","",,,"","","","",,"","",,,"",,"","","","","",,"","",,,,,,,,,"",,"",,"","","",,,,,"",,,,"",,"",,"","","",,,"","","Lock Out User for","2","","","Completed",,"","","","","","","",,"","","",,"","","","","","","","","",,,,,
		Changing minimum password length: "2020-09-03T11:29:15.0","2020-09-03T11:29:15.0","Machine Configuration","Succeeded",,"Succeeded",,"0xffffff88","admin11","0x000000000001b41a","","Device Settings","","",,,"","","","",,"","",,,"",,"","","","","",,"","",,,,,,,,,"",,"",,"","","",,,,,"",,,,"",,"",,"","","",,,"","Password

Requirement	Auditable Events	Example Event
		Policy","","","","","Completed",,"","","","","","","",,"","",,"","","","","","","","","","",,,,, ,,,,,,,"","","0x000000000001b41a","","Device Settings","","",,,"","","","",,"","",,,"","","","","","",,"",,,,,,,,,,"",,"",,"","","",,,,,"",,,,"",,"",,"","","",,,"","","Complexity Setting","Level1","","","Completed",,"","","","","","","",,"","","",,"","","","","","","","","","",,,,, ,,,,,,,"","","0x000000000001b41a","","Device Settings","","",,,"","","","",,"","",,,"","","","","","",,"",,,,,,,,,,"",,"",,"","","",,,,,"",,,,"",,"",,"","","",,,"","","Minimum Character No.","5","","","Completed",,"","","","","","","",,"","","",,"","","","","","","","","",,,,,
		"2020-09-09T16:35:46.0","2020-09-09T16:35:46.0","Machine Configuration","Succeeded",,"Succeeded",,"0xffffff88","admin1","0x000000000001be8d","","Device Settings","","",,,"","","","",,"","",,,"","","","","","",,"",,,,,,,,,,"",,"",,"","","",,,,,"",,,,"",,"",,"","","",,,"","SYSLOG","","","","","Completed",,"","","","","","","",,"","","",,"","","","","","","","","",,,,, ,,,,,,,"","","0x000000000001be8d","","Device Settings","","",,,"","","","",,"","",,,"","","","","","",,"",,,,,,,,,,"",,"",,"","","",,,,,"",,,,"",,"",,"","","",,,"","","SYSLOG IPAddress","Changed","","","Completed",,"","","","","","","","",,"","","",,"","","","","","","","","","",,,,,

Requirement	Auditable Events	Example Event
FMT_SMR.1	Modification of the group of users that are part of a role	TOE does not specifically modify the group of users that are part of a role.
FPT_SMR.1	Changes to the time	"2020-08-01T08:06:24.0","2020-08-01T08:06:24.0","Date/Time Change","Succeeded","Control Panel","Succeeded",,"0xffffff87","admin","0x000000000001a58a","","System","","",,,"","","","",,"","",,,"","","","","","",,"","",,,,,,,,,"","",,"","",,"","","",,,,,,"",,,,"",,"",,"","","",,,"","","","","","","Completed",,"","","","","","","","",,"","","",,"","","","","","","","","","","",,,,,
FTP_TRP.1 Remote administrator	Failure to establish a session	"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",,"","","","","","","",,"","",,"","","","","","","","","",,,,,,
FTP_TRP.1 Remote non-admin users	Failure to establish a session	See remote administration
FTP_ITC.1	Failure to establish a session	IPsec: "2020-08-19T14:14:00.0","2020-08-19T14:14:00.0","Collect Encrypted Communication Logs","Failed",,"Communication Failure",,"0x00000000","","0x00000000000015c94","","Network Attack Detection/Encrypted Communication","","",,,"","","","",,"","",,,"","","","","","",,"",,,,,,,,,,"","Encryption Communication","500","UDP","i

Requirement	Auditable Events	Example Event
		p:10.20.5.3","500","","IPsec",,"IPsec","Communication Start Request Sender (Out)","","Start",,,"",,"",,"","","",,,"","","","","","","Failed",,"","","","","","","",,"","","",,"","","","","","","","","","",,,,,
		TLS: {"parentLogId":"0000000000018f5f","subLogId":"00080000000000650000000000018f5f","subJobType":"destination.network","desNetSubState":"ended-incomplete","desNetStartTime":"2020-08-25T20:29:51Z","desNetStartValidTimeFlag":"on","desNetEndTime":"2020-08-25T20:30:01Z","desNetEndValidTimeFlag":"on","desNetAddressName":"u1d","desNetAddress":"u1@example.com","desNetSendKind":"mail","desNetSendOwner":"u1d","desNetSendMode":"document","desNetSendPages":"","desNetFileNo":"","desNetErrorInfo":"","desNetSubStatusDetail":"dest-connect-fail","logPart":"1of1"}