FUJI Xerox

ApeosPort C7070 ApeosPort C6570
ApeosPort C5570 ApeosPort C4570
ApeosPort C3570 ApeosPort C3070

Security Function Supplementary Guide

- Before Using the Security Function....2
- Settings for the Secure Operation 1 (Initial Settings Procedures Using Control Panel) 10
- Settings for the Secure Operation 2 (Initial Settings Procedures Using CentreWare Internet Services) 17
- Settings for the Secure Operation 3 (Regular Review by Audit Log) 28
- User Authentication....32
- Self Testing....34
- Software Update....35
- Using IPP Print 36
- Using Private Charge Print from Client PC 37
- Operation on CentreWare Internet Services 38
- Device Digital Certificate Management....40
- Additional Notes 42
- Appendix 44

Before Using the Security Function

This section describes the security functions and confirmation matters.

Preface

This guide is intended for the manager and system administrator of the organization where the device is installed, and describes the setup procedures related to security.
For general users, this guide describes the operations related to security features.

Model	Guide	Manual No.
ApeosPort C7070/C6570/ C5570/C4570/C3570/C3070/ C7070 G/C6570 G/C5570 G/ C4570 G/C3570 G/C3070 G	Reference Guide Main Unit Reference Guide Operations User's Manual	ME9024E2-1 ME9025E2-1 DE6690E2-2

The hash values of the PDF files are described in the Security Target.
Please check that the hash values of your manuals are correct. To compare the hash values, execute the following command from the command prompt.

certutil -hashfile <filename> SHA256

The security features of this model are supported by the following ROM version.

ApeosPort C7070/C6570/C5570/C4570/C3570/C3070/C7070 G/C6570 G/C5570 G/ C4570 G/C3570 G/C3070 G

- Controller ROM Ver. 1.5.3
- FAX ROM Ver. 2.2.1

Important

The product has obtained IT security certification for HCD PP v1.0. If you want to get this guidance used for IT security certification, please email to the contact information below.
Device_Security_Support@fujixerox.co.jp
Please let us know the “Model name”, “Machine number”, “Address”, and “Business office name”.
This certifies that the target of evaluation has been evaluated based on the certain evaluation criteria and methods, and that it conforms to the security assurance requirements.
In order to check if the model you have is the one evaluated in IT security certification, you can see the maker's name "Fuji Xerox" and the model name on the front cover of the machine.
And you can check the ROM versions you have along with the operation described in "Confirm the Device Software Version, Product Code and the System Clock" (P.8).
Note, however, that your ROM and manual may not be the certified version because they may have been updated along with machine improvements.
Please check the state of the delivered machine's corrugated cardboard packaging. If you could not confirm the packaging state at delivery and would like to know the details of the delivered state, please contact our sales representative or customer engineer.

This guide has been prepared on the assumption that the copy function, print function, fax function, scan function, and overwrite storage function are available. Installation is made by a customer engineer. And the print speed and the product name are fixed with initial settings by a customer engineer. You must witness on-site where a customer engineer installs it and confirm the situation.

You can confirm with the feature buttons and menus displayed on the control panel that your model provides copy function, print function, fax function, scan function, and overwrite storage function. For copy function, "Copy" button. For print function, "Private Charge Print" button. For fax function, "Fax" button. For scan function, "Email" button. And you can check that your model provides overwrite storage function with that the control panel shows "Overwrite Storage" on the menu of [Device > Information & Reports].
The default value for System Administrator's ID and password are described in "User's Manual" in machine.

Hardware and software used for the evaluation of the security certification.

The following items were used for the evaluation.

Windows PC

Purpose of use

- General user used it for print feature. 64bit Windows Print Driver (PCL) printer driver was installed on it and was used.
- A general user or the system administrator used a web browser on it for using a function of web service on the device. Microsoft Edge was used as the web browser in the evaluation.
- The system administrator used it for getting the audit logs from the device. PowerShell application was also used for getting it.

SMTP Server

SMTP server was installed for using the mail function. SMTP over TLS protocol was configured for the evaluation.

Precautions for secure use of this product

When installation or delivering the product, please confirm the affiliation of customer engineer by referring to business cards or purchase order sheet and so on.
If you could not attend the operation of the customer engineer at the time of initial installation, please restore factory defaults*.
When you change settings that cannot maintain the security function during operation, please restore factory defaults* and then check the settings again from the beginning according to the procedures in this guide.
This guide has been prepared on the assumption that the Service Representative Restricted Operation function is set to [enabled]. If the maintenance operation is permitted to a customer engineer, please check the details of the operation in advance and witness on-site where a customer engineer. If you could not check that in advance or witness, the TOE cannot keep the secure configuration. In that case, please restore factory defaults* after the maintenance operation and configure settings again according to the procedure of this guide.
For secure operation, prior to disposing of the device, please restore factory defaults*.

* For Restore Factory Defaults operation, you can operate it on [Device > Reset] after setting to disable for Service Representative Restricted Operation.

When you use the product, please do not leave the paper sheets.

Security Features

These models have the following security features:

- Identification, Authentication
- Auditing
- Access control
- Administrative roles
- Trusted operation
- Encryption
- Trusted communications
- PSTN fax-network separation
- Overwrite Storage

Settings for the Secure Operation

For the effective use of the security features, the System Administrator (Device Administrator) must follow the instructions below:

Reference

- For details on the setting procedures, refer to the following sections.
  - "Settings for the Secure Operation 1 (Initial Settings Procedures Using Control Panel)" (P.10)
  - "Settings for the Secure Operation 2 (Initial Settings Procedures Using CentreWare Internet Services)" (P.17)
  - "Settings for the Secure Operation 3 (Regular Review by Audit Log)" (P.28)

If the change fails in each setting procedure, a failure message is displayed after performing the change operation. In that case, check the settings again according to the procedure. If it still fails, please contact our sales representative or customer engineer.

- Set enable firmware update function
  Set to enabled.
- Scan
  Set to disabled.
- Remote Assistance
  Set to disabled.
- Internet Fax
  Set to disabled.
- Password Entry for Control Panel Login
  Set to [On].
- Data Encryption
  Set to enabled.
- Overwrite Storage
  Set to [1 Overwrite] or [3 Overwrites].
- Authentication
  Set to [Login to Local Accounts].
- Private Print
  Set to [According to Print Accounting].
- Direct Print Restricted
  Set to [On].

- SMB
  Set to disabled.
- Fax
  Direct Fax set to disabled.
  Polling / Storage for Remote Devices set to disabled.
- Create Folder for Fax receive
  Create Folder for Fax receive.
- Set Folder Selector for Fax receive
  Select Folder for Fax receive.
- Files Retrieved by Client
  Set to [Force Delete].
- Set Auto Clear
  Set to [On].
- Set Report Print
  Set to [Disabled].
- Self Test
  Set to [On].
- System Administrator Passcode
  Change the default passcode to another passcode of 9 or more characters.
- Maximum Login Attempts
  Set to [5] times.
- Access Control
  Set to [Locked] for [Device Access], and [Lock All] for [APP Access].
  Set to [Job Owner and Administrator] for all [Job Operation Restrictions].
  Set to [System Administrators Only] for [Edit Home] of [Personalization Restrictions].
- User Passcode Minimum Length
  Set to [9] characters.
- TLS
  Set to enabled.
- Certificate
  Set to enabled.
- FIPS140-2
  Set to enabled.
- HTTP
  Set to [Only HTTPS].
- TCP/IP
  Set to IPv4.
- WebDAV
  Set to disabled.
- Set Receive E-mail (POP3)
  Set to disabled.
- IPP
  Set to enabled.
- IPsec
  Set to disabled.

- SNMP
  Set to disabled.
- WSD
  Set to disabled.
- LPD
  Set to disabled.
- Port 9100
  Set to disabled.
- FTP Client
  Set to disabled.
- SFTP
  Set to disabled.
- SOAP
  Set to disabled.
- Bonjour
  Set to disabled.
- USB
  Set to disabled.
- NFC
  Set to disabled.
- CSRF
  Set to enabled.
- Service Representative Restricted Operation
  Set to [Enabled], and enter a passcode of 9 or more characters.
- Audit Log
  Set to enabled.
- Browser Session Timeout
  Set to [6].
- Custom Services
  Set to [Disabled].
- Plugin
  Set to [Disabled].
- Disabling PJL data read/write commands
  Disabling PJL data read/write commands.
- Regular Review by Audit Log
  Set to import the Audit Log automatically.
- Print Files in Folder with internet Services
  Set to [Disabled].

Note
- WSD stands for Web Services on Devices.

Important
- The security will not be warranted if you do not correctly follow the above setting instructions.
- The fax-network separation feature requires no special setting by the System Administrator.
- Receiving fax data specifying remote folder is rejected when Service Representative Restricted Operation is enabled.

For Optimal Performance of the Security Features

The manager (of the organization that the device is used for) needs to follow the instructions below:

- The manager needs to assign appropriate people as system and device administrators, and manage and train them properly.
- The system administrator need to train users about the device operation and precautions according to the policies of their organization and the product guidance.
- The device needs to be placed in a secure or monitored area where the device is protected from unmanaged physical access.
- If the network where the device is installed is to be connected to external networks, configure the network properly to block any unauthorized external access.
- To make it difficult to guess your password, users and administrators need to set passcode according to the following rules.
  - Do not use an easily guessed character strings passcode.
  - A passcode needs to contain numeric and alphabetic characters, and symbols.
- Users and administrators need to manage and operate the device so that their user IDs and passcodes may not be disclosed to another person.
- Users need to select "Prompt User for Entry when Submitting Job" on [Accounting Configuration] of printer driver, to set a user ID and a passcode certainly every time printing.
- Shared Folder operation is outside the scope of evaluation, and system administrators must not create folders.
- [Folder Selector by Telephone Number / G3 ID] is outside the scope of evaluation, and system administrators must not use the feature.
- Job Flow Sheet must not be linked to Folder. The operation that Job Flow Sheet linked to Folder is outside the scope of evaluation.
- Folder created by general users must not be used for Fax receive. Storing Fax data into the folder created by general users is outside the scope of evaluation. When a Job Flow Sheet with Print enabled is linked to Folder, Auto Start of the Job Flow must be disabled. There is concern that fax receive documents can be output and left unattended, resulting in information leak.
- For secure operation, all of the remote trusted IT products that communicate with the device shall implement the communication protocol in accordance with industry standard practice with respect to RFC/other standard compliance (TLS) and shall work as advertised.

■ TLS

For the TLS client (Web browser, Printer Driver, Audit Server) and the TLS server (Mail Server) that communicate with the device, select a data encryption suite from the following.

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA

- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384

Important
- For secure operation, while you are using CentreWare Internet Services, please do not access other web site, and do not use other applications. Otherwise the usage environment can be attacked via other websites or other applications by an attacker.
- For preventing TLS vulnerability, you should set the device address in the proxy exclusion list of browser.
  By this setting, secure communication will be ensured because the device and the remote browser communicate directly without proxy server, and thus you can prevent man-in-the-middle attack.
- When there is no operation in CentreWare Internet Services for the set period of session timeout, it will automatically logout. Logout explicitly when leaving a client PC within the set period of session timeout. System administrators must ensure that all users follow this guidance. Otherwise unauthorized users can operate this device using CentreWare Internet Services that have not been logged out.

Note • NTP server connection is outside the scope of evaluation.

Confirm the Device Software Version, Product Code and the System Clock

Before making initial settings, the System Administrator (Device Administrator) needs to check the Software Version of the device, product code and the system clock of the device.

How to check by Control Panel

1. Select [Device].
2. Select [Information & Reports].
3. Select [Software Version].
   You can identify the software versions of the components of the device on the screen.

How to check by Print Report

1. Select [Device].
2. Select [Information & Reports].
3. Select [Print Reports].

4 Select [Printer Reports].

5 Select [Configuration Report].
You can identify the software versions of the components of the device and product code by Print Report.

How to check the System Clock

1 Select [Local User].

2 Enter the system administrator's ID and Password with the keypad displayed.

3 Select [OK].

4 Select [Close] for warning message.

5 Select [Device].

6 Select [System Settings].

7 Select [System Clock/Timers].
You can check the time and the date of the system clock. If you need to change the time and the date, refer to the following procedures.

8 Select the required option.

9 Change the required setting.

10 Select [OK].

Settings for the Secure Operation 1 (Initial Settings Procedures Using Control Panel)

This section describes the initial settings related to security features, and how to set them on the device's control panel.
If a reboot confirmation screen is displayed after changing the settings, reboot this device.
If you want to continue to changing the settings, please log in as the System Administrator.

Set Data Encryption

1. Select [System Settings] on the [Device] screen.
2. Select [Reset].
3. Select [Restore Factory Defaults].
4. Select [Restore]. (After restore factory defaults, this device will restart.)
5. Select [System Settings] on the [Device] screen.
6. Select [Other Settings].
7. Select [Data Encryption].
8. Select [On].
9. Select [OK].
10. Select [Yes] to make the change.
11. Select [Yes] to reboot.

Note
- The encryption key is regenerated by restoring the factory defaults.
- Restoring factory resets takes about an hour.

Set Password Entry for Control Panel Login

1. Select [Local User].
2. Enter the System Administrator's ID and Password with the keypad displayed.
3. Select [OK].
4. Select [Close] for warning message.
5. Select [Authentication / Accounting] on the [Device] screen.
6. Select [Authentication / Security Settings].

7 Select [Authentication].

8 Select [Password Policy].

9 Select [Password for Control Panel Login].

10 Select [On].

11 Select [OK]

Set Overwrite Storage

1 Select [Authentication / Accounting] on the [Device] screen.

2 Select [Authentication / Security Settings].

3 Select [Overwrite Storage].

4 Select [Number of Overwrites].

5 Select [1 Overwrite] or [3 Overwrites] on the [Device] screen.

6 Select [OK].

Note

- After copy, fax, scan or print is completed*, the data is deleted from the storage area used for each operation and then automatically overwritten with blank data. Also, the document data in the Mailbox is deleted when it is retrieved or deleted, and then overwritten automatically. * complete successfully, error, and suspension
- If the device is turned off during the overwriting, unfinished files may remain on the storage. The overwriting will resume if you turn the device on again with the unfinished files remaining on the storage.

Set Authentication

1 Select [Authentication / Accounting] on the [Device] screen.

2 Select [Authentication / Security Settings].

3 Select [Authentication].

4 Select [Login Type].

5 Select [Log In to Local Accounts].

6 Select [OK].

7 Press Home button.

After configuring authentication setting, create user accounts according to [11 Authentication and Accounting Function] in *Reference Guide Operations.*

Note • In the case of [Local Accounts], when a user is deleted, the Folder and private print data related to the user are deleted.

* Authentication method set by steps above is applied to operations from the following interfaces.

- Control Panel
- CentreWare Internet Services
- Print Drivers

Set Private Print

1. Select [Authentication/ Accounting] on the [Device] screen.
2. Select [Authentication / Security Settings].
3. Select [Authentication].
4. Select [Charge/Private Print Settings].
5. Select [Receive Control].
6. Select [According to Print Accounting].
7. Select [Save as Private Charge Print Job] for [Job Login Success].
8. Select [Delete Job] for [Job Login Failure].
9. Select [Delete Job] for [Job Without User ID].
10. Select [OK].

Set Disable Direct Print Feature

1. Select [Device].
2. Select [Authentication / Accountings].
3. Select [Authentication / Security Settings].
4. Select [Disable Direct Print Feature].
5. Select [On].
6. Select [OK].

Set SMB

1. Select [Device].
2. Select [Connectivity & Network Setup].
3. Select [Port Settings].

4 Select [SMB Client].

5 Select [Port Status].

6 Select [Disabled].

Set Fax

1 Select [Device].

2 Select [App Settings].

3 Select [Fax Settings].

4 Select [Fax Control].

5 Select [Direct Fax].

6 Select [Disabled].

7 Select [Polling / Storage for Remote Devices].

8 Select [Disabled].

9 Select [OK]

10 Press Home button.

Create Folder for Fax receive

If a user with System Administrator role (but not System Administrator's user ID) is not created, please create it with reference to "Reference Guide Operations".

1 Log in as a user with System Administrator role. (but not System Administrator’s user ID)

2 Select [Send from Folder].

3 Press [+] button.

4 Select a box.

5 Enter folder name and press [Next].

6 Select [Check Folder Passcode] switch to disable.

7 Select [OK] twice and press Home button.

Set Folder Selector for Fax receive

1 Select [Device].

2 Select [App Settings].

3 Select [Fax Settings].

4 Select [Fax Control].

5 Select [Folder Selector Setup].

6 Select [Enabled].

7 Press [<] button twice.

8 Select [Fax Received Options] on [Fax Settings] page.

9 Select [Folder Selector Setup].

10 Select a line to be configured.

11 Select [On].

12 Enter folder number (three digits) created in “Create Folder for Fax receive”.

13 Select [OK].

14 Select [OK].
Back to 10 and repeat steps for all lines.

15 Press Home button.

Set Files Retrieved By Client

1 Select [Device].

2 Select [App Settings].

3 Select [Send from Folder Settings].

4 Select [Files Retrieved By Client].

5 Select [Force Delete].

6 Press [<] button twice and press Home button.

Set Auto Clear

Note • The number of seconds can be set from 10 to 900.

1 Select [Device].

2 Select [System Settings].

3 Select [System Clock/Timers].

4 Select [Auto Clear].

5 Select [On].

6 Press [-] button to set [30] seconds.

7 Select [OK].

Set Report Print

1 Select [Device].

2 Select [System Settings].

3 Select [Reports].

4 Select [Print Reports] switch to disable.

5 Press Home button.

Set Self Test

1 Select [Device].

2 Select [Maintenance].

3 Select [Power on Self Test].

4 Select [On].

5 Press [<] button and press Home button.

Set Scan

1 Scroll to the bottom of the display, select [Customize].

2 Select [Edit Home].

3 Select [X] to delete the [Scan].

4 Select [Done].

Remote Assistance

1 Select [Customize].

2 Select [Edit Home].

3 Select [X] to delete the [Remote Assistance].

4 Select [Done].

Internet Fax

1 Select [Customize].

2 Select [Edit Home].

3 Select [X] to delete the [Internet Fax].

4 Select [Done].

Settings for the Secure Operation 2 (Initial Settings Procedures Using CentreWare Internet Services)

This section describes the initial settings related to security features, and how to set them on CentreWare Internet Services.
Set up IP address according to [Device] > [Connectivity & Network Setup] > [Protocol Settings] in *Reference Guide Operations* before using CentreWare Internet Services.
If a reboot confirmation screen is displayed after changing the settings, reboot this device.

Preparations for settings on the CentreWare Internet Services

- Prepare a computer supporting the TCP/IP protocol to use CentreWare Internet Services.
- CentreWare Internet Services supports the browsers that satisfy TLS conditions.

1. Open your Web browser, enter the TCP/IP address of the device in the Address or Location field, and press the <Enter> key.
2. Click [Log In].
3. Enter the System Administrator's ID and the password.
4. Click [Close].
5. Click [Close] for warning message.

Change the System Administrator's Password

1. Click [System Administrator] on the [Home] page.
2. Click [Profile].
3. Click [Change Password].
4. Enter old password in the [Current Password] box.
5. Enter a new System Administrator's password of 9 or more characters in the [New Password] box.
6. Enter the same System Administrator's password in the [Retype Password] box.
7. Click [Save].

Note • Characters which can be used for Password :
Alphabets (upper-case and lower-case), digits, and the following special characters.
(“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, ” (space)”, “””, “‘”, “+”, “,”, “-“, “/”, “:”, “;”, “<”, “=”, “>”, “?”, “[“, “\”, “]”, “_”, “`”, “{“, “|”, “}”, “~”)

Set Limit Login Attempts

1. Click [Permissions] on the Home page.
2. Click [Authentication].
3. Click [Advanced Settings].
4. Click [Limit Login Attempts of System Administrator].
5. Click [Enable] switch to enable.
6. Enter [5] for [Login Attempts].
7. Click [Save].
8. Click [Limit Login Attempts of Local User].
9. Click [Enable] switch to enable.
10. Enter [5] for [Login Attempts].
11. Click [Save].

Set Access Control

1. Click [Permissions] on the Home page.
2. Click [Permissions] and click [Access Control].
3. Click [Device Control Panel Access] for [Device Access].
4. Select [Locked].
5. Click [System Settings Access] for [Device Access].
6. Select [Locked].
7. Click [Lock All] for [App Access].
8. Select [Job Owner and Administrator] for all [Job Operation Restrictions].
9. Click [System Administrators Only] for [Edit Home] of [Personalization Restrictions].
10. Click [Save].

Job Operation Restriction

1. Click [Jobs] on the Home page.

2 Click [Jobs Settings].

3 Click [Hide Job Details] for [Active Jobs View].

4 Select [Yes].

5 Click [Save].

Set User Password Minimum Length

This feature is only applicable to Local Authentication mode.

1 Click [Permissions] on the Home page.

2 Click [Authentication].

3 Click [Password Policy].

4 Click [Minimum Length].

5 Select [Restrict].

6 Set [9] for [Minimum Number of Characters to Restrict].

7 Click [Save].

Set TLS

1 Click [System] on the Home page.

2 Click [Security].

3 Click [Certificate Settings] for [Certificates].

4 Select [Device Certificates] in the pull-down menu.

5 Select [Generate Self-Signed Certificate] in the [Create] menu.

6 Set the details as necessary for [Create Self-Signed Certificate].

7 Click [Start].

8 Click [Close] twice.

9 Click [SSL/TLS Settings] for [Network Security].

10 Select [TLS 1.2 or Later] for [Protocol Version].

11 Click [Enable TLS 1.3] switch to disable.

12 Select [SSL/TLS] for [SMTP - SSL / TLS Communication].

13 Click [Verify Remote Server Certificate] switch to enable.

14 Click [Save].

Note
- You should import the CA certificate according to the same procedure as "Configuring Certificates" (P.20) prior to enabling [Verify Remote Server Certificate].
- You can find how to create Self-Sighed Certification in "Device Digital Certificate Management" (P.40).

Configuring Certificates

Import the certificate of the mail server, etc. to which this device connects.

1 Click [System] on the Home page.

2 Click [Security].

3 Click [Certificate Settings] for [Certificates].

4 Click [Import].

5 Select the file to be imported by clicking [Select].

6 As necessary, enter [Password] and [Retype Password].

7 Click [Start].

Set FIPS140-2

1 Click [System] on the Home page.

2 Click [Security].

3 Click [FIPS140-2] for [Network Security].

4 Click [On].

5 Click [Save].

Set HTTP

1 Click [Network] on the Home page.

2 Click [HTTP] for [Protocols].

3 Click [Port (HTTP/HTTPS)] for [HTTP].

4 Select [Enable HTTPS only].

5 Click [Save].

Set CSRF

1. Click [Network] on the Home page.
2. Click [HTTP] for [Protocols].
3. Click [CSRF Protection] switch to enable.
4. Click [Save].

Set TCP/IP

1. Click [Network] on the Home page.
2. Click [Ethernet] for [Connections].
3. Click [Edit] for [Common].
4. Click [IP Mode].
5. Select [IPv4 Mode].
6. Click [Save].

Set WebDAV

1. Click [Network] on the Home page.
2. Click [WebDAV] for [Protocols].
3. Click [Port] switch for disable.
4. Click [Save].

Set Receive E-mail (POP3)

1. Click [Network] on the Home page.
2. Click [POP3] for [Protocols].
3. Click [Port (Receive Email)] switch to disable.
4. Click [Save].

Set IPP

1. Click [Network] on the Home page.

2 Click [IPP] for [Protocols].

3 Click [Port] switch to enable.

4 Click [Save].

Set IPsec

1 Click [Network] on the Home page.

2 Click [IPsec] for [Protocols].

3 Click [Enable] switch to disable.

4 Click [Save].

Set WSD

1 Click [Network] on the Home page.

2 Click [WSD] for [Protocols].

3 Click [Port (Scan to Desktop)] switch to disable.

4 Click [Port (Print from Desktop)] switch to disable.

5 Click [Save].

Note • WSD stands for Web Services on Devices.

Set LPD

1 Click [Network] on the Home page.

2 Click [LPD] for [Protocols].

3 Click [Port] switch to disable.

4 Click [Save].

Set Port9100

1 Click [Network] on the Home page.

2 Click [Port 9100] for [Protocols].

3 Click [Port] switch to disable.

4 Click [Save].

Set FTP Client

1. Click [Network] on the Home page.
2. Click [FTP Client] for [Protocols].
3. Click [FTP Client Port] switch to disable.
4. Click [Save].

Set SFTP

1. Click [Network] on the Home page.
2. Click [SFTP] for [Protocols].
3. Click [SFTP Client Port] switch to disable.
4. Click [Save].

Set SOAP

1. Click [Network] on the Home page.
2. Click [SOAP] for [Protocols].
3. Click [Port] switch to disable.
4. Click [Save].

Set SNMP

1. Click [Network] on the Home page.
2. Click [SNMP] for [Protocols].
3. Click [Port] switch to disable.
4. Click [Save].

Set Bonjour

1. Click [Network] on the Home page.
2. Click [Bonjour] for [Protocols].
3. Click [Port] switch to disable.

4 Click [Save].

Set USB

Note • Depending on the device's configuration, this setup menu would not be shown.

1 Click [Network] on the Home page.

2 Click [USB] for [Connections].

3 Click [Enable] switch to disable.

4 Click [Save].

Set NFC

1 Click [Network] on the Home page.

2 Click [NFC] for [Connections].

3 Click [Enable] switch to disable

4 Click [Save]

Set Service Representative Restricted Operation

1 Click [System] on the Home page.

2 Click [Security].

3 Click [Service Representative Operation Settings].

4 Click [Enabled] switch to enable.

5 Enter a password of 9 or more characters in the [Maintenance Password] box.

6 Enter the same password in the [Retype Maintenance Password] box.

7 Click [Save].

Note • Characters which can be used for Password :
Alphabets (upper-case and lower-case), digits, and the following special characters.
(“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, ” (space)”, “”””, “’”, “+”, “,”, “-“, “/”, “:”, “;”, “<”, “=”, “>”, “?”, “[“, “\”, “]”, “_”, “`”, “{“, “|”, “}”, “~”)

Set Audit Log

1 Click [System] on the Home page.

2 Click [Logs].

3 Click [Audit Log].

4 Click [Enabled] switch to enable.

5 Click [Save].

Set Browser Session Timeout

1 Click [System] on the Home page.

2 Click [Timeouts].

3 Enter the "6" in the [Auto Clear (Internet Services)] box.

4 Click [Save].

Note
- Session Timeout Period can be specified in the range for 1 to 240 minutes.
- This guide recommends the session timeout period is 6 minutes considering the time required for input and output large size files. If you set a short time for security, the file transfer may fail. In that case, please set the session timeout period to an appropriate value.
- When there is no operation in CentreWare Internet Services for the set period of session timeout.

Set Custom Service

1 Click [App] on the Home page.

2 Click [Custom Services Settings].

3 Click [Enabled] switch to disable.

4 Click [Save].

Set Plugin

1 Click [System] on the Home page.

2 Click [Plug-in Settings].

3 Click [Embedded Plug-ins] switch to disable.

Set Software Update

1 Click [System] on the Home page.

2 Click [Software Update].

3 Click [Enable] to enable.

4 Reboot this device and login as Administrator.

5 Click [System] on the Home page.

6 Click [Software Update].

7 Click [Software Download via Network].

8 Click [Enable].

9 Click [Save].

Disabling PJL data read/write

1 Click [System] on the Home page.

2 Click [Defaults].

3 Click [PJL File System Command].

4 Click [Disable] switch to disable.

5 Click [Save].

Print Files in Folder with internet Services

1 Click [System] on the Home page

2 Click [Security]

3 Click [Print Files in Folder with internet Services]

4 Click [Disabled] and Click [Save]

Set SMTP

1 Click [Network] on the Home page.

2 Click [SMTP] for [Protocols].

3 Click [Port (Send Email)] switch to enable.

4 Click [Port (Email Notification)] switch to disable.

5 Click [Port (Receive Email)] switch to disable.

6 Set device email address for [Device's Email Address].

7 Set port number* for [Email / Internet Fax Port Number].

8 Set port number* for [Direct Internet Fax Port Number].

*Please check the port number of SSL/TLS communication for system administrator.

9 Click [SSL/TLS] for [SSL/TLS Communication].

10 Select [Off] for [Email Send Authentication].

11 Click [Save].

Settings for the Secure Operation 3 (Regular Review by Audit Log)

This section describes the automatic importing method of the Audit Log feature using the Audit Server.
The Audit Log is regularly reviewed by the Security Administrator, often with the aid of third party analyzing tools. The audit log helps to assess attempted security breaches, identify actual breaches, and prevent future breaches.
The important events of the device such as device failure, configuration change, and user operation are traced and recorded based on when and who operated what function.
Auditable events are stored with time stamps into one file ("audit log file") within the internal storage. Up to 15,000 events can be stored. When the number of recorded events exceeds
15,000, the oldest audit log file is overwritten and a new audit event is stored.
The audit log file remains on the device whenever it is retrieved from the device to Audit Server. It means that the same audit event may be included in the audit log file by a time interval of retrieving. However, if it takes the long time interval over the upper limit of the number of the audit events in the file, A number of new audit events might overwrite the same number of older audit events. Therefore, the system administrator should design the appropriate time interval under the usage environment of the device. The size of the audit log file containing 15,000 events is about 1.5M Bytes. According to the interval of retrieval and the free size of the storage space, the system administrator should determine the number of log files to be preserved, and delete the older log files. When using the following PowerShell script, the name of log files includes the time stamp indicating the date and the time when the file was downloaded. You can find the events recorded in a duration with the name of the log file.

The system administrator should check if the audit log file is retrieved appropriately in the target folder which the operation script file of PowerShell is stored before using the device formally. The system administrator should modify the operation script file of PowerShell as appropriate.

There is no function to delete the audit log data stored in the device.

Import the Audit Log File

TLS communication must be enabled in order to access the logged data.

Procedures described below should be performed in the following environment.

- PC client with Windows OS
- PowerShell version3.0 or later installed
- The execution policy of PowerShell should be configured to execute the operation script file of PowerShell.

1 Create PowerShell script file with the contents below.

```
# Replace "12345" with actual Login ID of system administrator
$USER = "12345"
# Replace "passcode" with actual Passcode of system administrator
$PASS = "passcode"
# Replace "127.0.0.1" with actual URL of target device
$Uri = "https://127.0.0.1"
```

```
$Uri_Login = $Uri+"/LOGIN.CMD"
$Uri_AuditLogGet = $Uri+"/ALOGEXPT.CMD"
$Uri_Logout = $Uri+"/LOGOUT.CMD"

# Define download file name rule
$date_time = Get-Date -Format "yyyy-MMdd-HHmmss"
$DownloadPath = "./auditfile_${date_time}.txt"

# Download audit log
$USER_B64 =
[Convert]::ToBase64String(([System.Text.Encoding]::Default).GetBytes($USER))
$PASS_B64 =
[Convert]::ToBase64String(([System.Text.Encoding]::Default).GetBytes($PASS))
$cred = "NAME=${USER_B64}&PSW=${PASS_B64}"
$referer = $Uri + "/home/index.html"

$ProgressPreference = 'SilentlyContinue'

[Net.ServicePointManager]::SecurityProtocol =
[Net.ServicePointManager]::SecurityProtocol -bor
[Net.SecurityProtocolType]::Tls12

Invoke-WebRequest -Uri $Uri_Login -SessionVariable mySession -Method Post -Body $cred
-Headers @{ "Referer" = $referer }
Invoke-WebRequest -Uri $Uri_AuditLogGet -OutFile $DownloadPath -DisableKeepAlive -
WebSession $mySession
Invoke-WebRequest -Uri $Uri_Logout -WebSession $mySession
```

Important
- To perform TLS connection from a client PC to the device via PowerShell, the SSL server certificate which is installed in the device should be installed on Windows PC as Trusted Root Certificate.
- This PowerShell script contains the system administrator's ID and password, the script file should be kept carefully so that the information is not disclosed.

2 Register the PowerShell script created at step 1 into Task Scheduler in Windows.

Refer to Help in Windows for the details of Task Scheduler. The typical configuration of Task Scheduler is shown below. Please note that the appropriate configuration should selected under the usage environment of the customer.
Operation: execution of PowerShellf

Operation > Setting > Program/Script: "< the directory path of PowerShell>"

Operation > Setting >Parameters: "Command <the directory path of script file>"

Operation > Setting > Start: "<Path where the script file runs, and the audit log is retrieved>"

File Format of the Exported Audit Log

The following information is recorded in imported audit log data, check regularly whether there are not breaches by accessing or attempt.

■ Header information

Item	Export Format	Description
Format Version	Integer	The setting value is "3".

Item	Export Format	Description
Device's IP Address	Character string that consists of half-size alphanumeric characters (a to z, 0 to 9), dot(.), colon(:)	Displays the IP address (IPv4 or IPv6)
Coding Method	String	Fixed to UTF8.
Time Zone	-720 to 720	Displays time difference based on GMT. The unit is minute, and the value is negative if the time zone is west of Meridian.
Date Format	YYYY/MM/DD, MM/DD/YYYY, or DD/MM/YYYY	Displays the date format.

■ **Audit log information**

Item	Export Format	Description
Log ID Integer	(1 to 60000)	ID that is assigned when audit event occurs is exported.
Date	String	Date of audit-event occurrence is exported.
Time	hh:mm:ss	Time of audit-event occurrence (hour, minute, and second) is exported.
Audit Event ID	Hexadecimal integer (0x0000 to 0xffff)	ID that corresponds to audit event is exported.
Logged Events	String	Name of the user who caused audit event to occur is exported.
User Name	String	Name of the user who caused audit event to occur is exported. "KO" for the system administrator. "CE" for the Customer Engineer. User ID for other users. "-" for ones whose user ID is unknown.
Description	String	Character string that describes the details of audit event is exported.
Status	String	Character string that represents the status or processing result of occurred audit-event is exported.
Optionally Logged Items	String	Optionally logged information of audit event is exported.

e.g.:The following audit log is recorded, when someone tried to login under ID(User1), and the login failed due to an invalid password.

Item	Description
Log ID	1
Date	01/01/2018
Time	10:00:00
Logged Events	Login/Logout
User Name	User1
Description	Login
Status	Failed (Invalid Password)
Optionally Logged Items	-

Operations recorded in the Audit Log File

The operations recorded in the audit log file are as follows.

- User Identification/Authentication (using Control Panel)
- User Identification/Authentication (using CentreWare Internet Services)
- User Identification/Authentication (using Printer Driver)
- Use of management functions (using Control Panel)
- Use of management functions (using CentreWare Internet Services)
- Start-up and shutdown (TOE)
- Use of Copy, Print, Scan, Fax and Retrieve functions (using Control Panel)
- Use of Job Management and Job History functions (using Control Panel)
- Use of Job Status and Job History (using CentreWare Internet Services)
- Use of Retrieve function (using CentreWare Internet Services)
- Use of Print function (using CentreWare Internet Services)
- External Audit Server
- Firmware Update
- PSTN

Reference

- For details on contents recorded in audit logs, refer to "Audit Log Reference Guide" provided on our official website.

The export method of Audit Log from CentreWare Internet Services

The following describes methods for export the Audit Log.

1. Click [System] on the Home page.
2. Click [Logs].
3. Click [Audit Log].
4. Click [Export] of [Export Audit Log].

User Authentication

This section describes the operation of user authentication.
Before using, all services and configuring settings, a user must be authenticated with an ID and a password.

1 Enter the "User ID" from keypad.

2 Select [Next] on the touch screen.

3 Enter the "Password" from keypad.

4 Select [OK] on the touch screen.

All features on the control panel become available.

Note
- Before entering the User ID and the password, select [Registered User] or [System Administrator] when remote authentication is used.
- When using [Login to Local Accounts], only the system administrator's ID is pre-registered on the device. Other user IDs are not registered. For details on how to register User ID, refer to "Device" > "Authentication / Accounting" > "Accounting" > "Create / View User Accounts" in the *Reference Guide Operations*.

Users are classified into the following three types.

- System Administrator

  System Administrator users can register and change system settings to adapt to the environment to be used. The users are registered on the device or a remote server.

  System Administrator consist of “Key Operator” which is pre-configured in factory, and “System Administrator” which is assigned to users who are added in the environment to be used.

- General User

  General User can use the basic function of the device, but cannot be allowed to configure the system settings. The users are registered on the device or a remote server. Users who are registered on the device are assigned to General User as the initial role.

- Unauthenticated User

  Unauthenticated User is a role for users who haven’t logged in the device.
  Unauthenticated User cannot use the device at all.

The available operations for documents and jobs are different depending on the roles assigned to the login users.

Important
- Since System Administrator role has a strong permission, to ensure proper operation, assigning the role should be necessary minimum. And please do not assign “Account Administrator” to users since it is outside the scope of the evaluation for the security certification.

As for Private Print feature, General User can perform the following operations for the data and the jobs stored his/her own Private Charge Print folder.
- preview, print, delete the print data
- change the number of copies
- cancel the processing job

But General User cannot operate the print data and the job stored by others.
System Administrator (including Key Operator) can operate all the print data and jobs regardless of owner.

As for Network Scan feature, General User can perform the following operations for the scanned data and jobs started by oneself.

- Preview the scanned image in the case of activating “Preview” in scan operation
- Cancel the processing scan job

But General User cannot operate the scanned data and the job started by others.
System Administrator (including Key Operator) can operate all the scanned data and jobs regardless of owner.

As for Copy feature, General User can perform the following operations for the copy data and jobs started by oneself.

- Change the number of copies for the copy job started by oneself
- Restart and Cancel the processing copy job

But General User cannot operate the copy data and the job started by others.
System Administrator (including Key Operator) can operate all the copy data and jobs regardless of owner.

As for Fax Send feature, General User can perform the following operations for the fax send data and jobs started by oneself.

- Preview the scanned image in the case of activating “Preview” in fax send operation
- Cancel the processing fax send job

But General User cannot operate the fax send data and the job started by others.
System Administrator (including Key Operator) can operate all the copy data and jobs regardless of owner.

Received Fax data is stored into the folder specified with “Folder Selector Setup”. The following operations are allowed to the owner of the folder in which the data was stored.

- Retrieve
- Print
- Delete

The user who doesn’t have the ownership for the folder cannot operate the received fax data. However, Key Operator can operate the data stored in all the folder regardless of the owner.
As for Scan to Folder feature, the following operations are allowed to the owner of the folder in which the data was stored.

- Preview
- Print
- Delete
- Change the number of copies to be printed
- Change the selection of the paper

The user who doesn’t have the ownership for the folder cannot operate the scanned data. However, Key Operator can operate the data stored in all the folder regardless of the owner.

Self Testing

This section describes the Power on Self Test function.
The device can execute a Self Test function to verify the integrity of executable code and setting data.
The device verifies the area of NVRAM and SEEPROM including setting data at initiation, and displays an error on the control panel at error occurrence.
However, an error is not detected for the data on audit logs and time and date as these are not included in the target.
Also, when Self Test function is set at initiation, the following tests are performed.

The device calculates the checksum of Controller ROM to confirm if it matches the specified value, and displays an error (117-311) on the control panel at error occurrence.

The device calculates the checksum of Fax ROM to confirm if it matches the specified value, and displays an error (033-321) on the control panel at error occurrence.

The device performs known-answer-test of random number generator, and displays an error (116-321) on the control panel at error occurrence.

The device tests the entropy source, and displays an error (024-371) on the control panel at error occurrence.

When an error message is displayed, switch off the device power, make sure that the touch screen is blank and then switch on the device power. If the same message is displayed again, contact our Customer Support Center.

Software Update

Firmware of the device can be upgraded by CentreWare Internet Services.

Initiate firmware update from a client PC

1. Click [System] on the Home page.
2. Click [Software Update].
3. Select the file to be imported by clicking [Select] for [Specify File for Software Update].
4. Click [Start].

When the signature verification of the firmware is successful and the authenticity of the new firmware can be confirmed, the upgrade status is displayed on the control panel.

Download Mode

PROCESSING XX/XX

After the upgrade process is completed, the device reboots automatically and the login screen is displayed on the control panel.
Check the software version from the control panel. If the version has been updated, the upgrade has been completed successfully.

If the firmware signature verification fails, the error message is displayed on the control panel as below.

Download Mode

FILE TRANSFER ERROR 017-759

Please press power button to reboot. In this case, check the new firmware is correct and try this procedure again. If it still fails, please contact our sales representative or customer engineer.

Note
- Check the following settings again.

  "Settings for the Secure Operation 1 (Initial Settings Procedures Using Control Panel)" (P.10)

  •Set enable firmware update function

  "Settings for the Secure Operation 2 (Initial Settings Procedures Using CentreWare Internet Services)" (P.17)

  •Set Software update

Using IPP Print

You need to install the printer driver on your PC with the following procedure in order to use IPP Print feature.
(The following explanation is an example of using Windows 10)

1. Login as a user who has Administrator role.
2. Select “Devices” icon in “Settings” screen.
3. Click “Add a printer or scanner” button in “Printers & scanners” screen, then click “The printer that I want isn’t listed” link.
4. Select “Select a shared printer by name” and input the printer address as follows, then click “Next” button.

   Printer address: “https://<IP address or host name of the device>/ipp“
5. Click “Have Disk” button on Add Printer Wizard.
6. Select the folder where the printer driver is stored, and the select the INF file, and click “Open” button.

Important
- You need to store the SSL server certificate of the device in the Trusted Root Certification Authorities on the Client PC so that the PC can communicate with the device with IPPS.

Using Private Charge Print from Client PC

In order to submit Private Charge Print jobs correctly, you need to configure the Windows Printer, and specify the User ID and the password of the user which is registered in the device.
(The following explanation is an example of using Windows 10)

1 On the property of the Windows Printer, Click “Accounting” button in “Configuration” tab.

2 On “Accounting” dialog, select “Prompt User for Entry when Submitting Job”.

Important • For secure usage, please do not select “Always Use Default User Details” on “Accounting” dialog.

When you submit a print job, you can select the following values for “Job Type” on Printer Property, but any types of jobs, except for “Create Background Form”, are stored as Private Charge Print jobs. The “Create Background Form” type of jobs are stored as background forms in the device, and never printed out.

Available Values for “Job Type”
“Normal Print”, “Secure Print”, “Sample Set”, “Delayed Print”, “Store in Remote Folder”, “Create Background Form”

Operation on CentreWare Internet Services

On Client PC, you can operate the machine remotely via CentreWare Internet Services using Web Browser.
This section shows available operation on each services, [Home], [App], [Jobs] of CentreWare Internet Services.

Home

The [Home] service displays the information of machine, trays, consumables, counter, and support.

Note • Although there is a [Submit] button, device with the setting in this guidance shows job error when you operate this button.

App

The [App] page displays the list of applications. The [Send from Folder] application allows you to configure folders. By clicking [Send from Folder] button, the list of folder is shown. You can operate create, edit, delete the folder and show the list of files in the folder. This page displays the folder number and folder name. By clicking the folder name, [File List] screen is shown.
The [File List] displays the list of files in the folder. When the User ID logged in CentreWare Internet Services matches the owner of the specified folder, the list of files in the specified folder is available. If the User ID logged in CentreWare Internet Services doesn't match the owner of the specified folder, “Unable to select because you do not have access” message is prompted. However, when you log in as Key Operator, you can see the list of files for all folders.

- Type
  Displays the type of job of the file.
- File Name
  Displays the file name.
- Date & Time
  Displays the date and time when a file was stored in the folder.
- Page Count
  Displays the page count of the stored files.
  The [File List] allows you to retrieve, delete the specified file.

<Retrieve>
When you check the check box at the left of a file in the folder and then click the [Retrieve] button, the [Retrieve Files from Folder] screen appears, where you can retrieve the file with the following settings.

- Retrieving Format
  Specify the file format when retrieving a file. You can select either TIFF/JPEG, PDF, DocuWorks.
- MRC High Compression
  Set whether to compress the file at a high compression rate.
- Specific Color
  Displays whether the Specific Color feature is available when retrieving a file.

Jobs

The [Jobs] tabs displays the details of jobs executed via protocols or on the device control panel. This page allows you to delete pending print jobs.
The [Jobs] page displays [Owner], [Type], [Status], [Quantity] of active jobs. When the job is waiting user operation due to some reasons, the alert information shows on [Notifications] in [Home] service.

Device Digital Certificate Management

You can configure the digital certificate settings of the device using CentreWare Internet Services. This feature allows you to create a self-signed certificate for SSL communication and to import a certificate to the device. Also you can generate a Certificate Signing Request (CSR) file.

Create New Certificate

On the Home page, Click [System] > [Security] > [Certificate Settings]. Select the type of certificate to create from pull-down menu and then select the [Generate Self-Sighed Certificate] or [Create Certificate Signing Request (CSR)] from [Create] menu.
When [Generate Self-Signed Certificate] is selected, the [Create Self-Signed Certificate] screen is displayed.
When [Create Certificate Signing Request (CSR)] is selected, the [Create Certificate Signing Request] screen is displayed.

Create Self-Signed Certificate

Configure the settings below and click the [Start] button to set the self-signed certificate to the device. If the self-signed certificate has already been created, it will be overwritten.

- Digital Signature Algorithm

  Select [RSA/SHA-256], [RSA/SHA-384], [RSA/SHA-512], [ECDSA/SHA-256], [ECDSA/SHA-384] or [ECDSA/SHA-512].

- Public Key Size (When [RSA/SHA-256], [RSA/SHA-384] or [RSA/SHA-512] is selected.)

  Select [2,048 Bits] or [3,072 Bits].

- Elliptic Curve (When [ECDSA/SHA-256], [ECDSA/SHA-384] or [ECDSA/SHA-512] is selected.)

  Select [P-256], [P-384] or [P-521].

- Issuer

  Enter the issuer of the certificate using up to 64 characters.

- Days of Validity

  Enter the validity date of the certificate between 1 and 9,999.

Certificate Signing Request (CSR)

Configure the settings below and then click the [Start] button to display the [Download Certificate Signing Request (CSR)] screen.

- Digital Signature Algorithm

  Select [RSA/SHA-256], [RSA/SHA-384], [RSA/SHA-512], [ECDSA/SHA-256], [ECDSA/SHA-384] or [ECDSA/SHA-512].

- Public Key Size (When [RSA/SHA-256], [RSA/SHA-384] or [RSA/SHA-512] is selected.)

  Select [2,048 Bits] or [3,072 Bits].

- Elliptic Curve (When [ECDSA/SHA-256], [ECDSA/SHA-384] or [ECDSA/SHA-512] is selected.)

  Select [P-256], [P-384] or [P-521].

- 2 Letter Country Code

  Enter the Country Code of the device location in two alphabets.

- State / Province Name

  Enter the prefecture name of the device location up to 16 alphanumeric characters. This item can be omitted.

- Locality Name

  Enter the city, ward, town, or village name of the device location up to 32 alphanumeric characters. This item can be omitted.

- Organization Name

  Enter the organization name that applies for the certificate up to 32 alphanumeric characters.

- Organization Unit

  Enter the department name that applies for the certificate up to 32 alphanumeric characters.

- Common Name

  Displays the host name of the device. The host name can be edited on [Description] under the [Properties] tab.

- Email Address

  Displays the E-mail address of the device. The E-mail address can be edited on [Description] under the [Properties] tab.

Import Certificate

Configure the settings below and click the [Import] button to set the specified certificate to the device.

- Certificate

  Specify the file to import.

  The available formats are X.509(DER/PEM), PKCS#7(DER), and PKCS#12(DER).

- Password

  Enter the password to decode data in PKCS#12 format. Up to 32 characters can be entered.

  The password will be displayed as asterisks (***) or bullets (●●●).

- Retype Password

  Re-enter the password for verification.

  The password will be displayed as asterisks (***) or bullets (●●●).

Additional Notes

PSTN fax – network separation

The device has fax modem function and provides capability to transfer fax data on public switched telephone network. The device supports only ITU-T G3 mode.
The device doesn't have data modem capability, and only fax image format data can be transferred via the fax line.
Fax line is completely isolated from Ethernet, and data on fax line cannot interfere data on Ethernet.

Audit Log

The events shown in the table below are recorded in audit log.

Reference

- For details on contents recorded in audit logs, refer to "Audit Log Reference Guide" provided on our official website.

Auditable event	Name	Description	Status
Start-up and shutdown of the audit functions	System Status	Started normally (cold boot)	-
		Started normally (warm boot)	
		Shutdown requested	
Job completion	Job Status	Print	Completed, Canceled by User
		Copy	
		Scan	
		Fax	
		Mailbox	
		Print Reports	
Unsuccessful User authentication Unsuccessful User identification (using Control Panel)	Login/Logout	Login	Failed (Invalid UserID), Failed (Invalid Password)
Unsuccessful User authentication Unsuccessful User identification (using CentreWare Internet Services and Audit Server)	Login/Logout	Login	Failed (Invalid UserID), Failed (Invalid Password)
Unsuccessful User authentication Unsuccessful User identification (using Printer Driver)	Job Status	Print	Aborted

Auditable event	Name	Description	Status
Use of management functions	Device Settings	View Security Setting	Successful
		Change Security Setting	
		Switch Authentication Mode	
		Edit User	Successful
		Add User	
		Delete User	
	Device Config	Software	Updated
	Audit Policy	Audit Log	Enable/Disable
Modification to the group of Users that are part of a role	Device Settings	Edit User	Successful
Changes to the time	Device Settings	Adjust Time	Successful
Failure to establish session (TLS/ IPSec)	Communication	Trusted Communication	Failed (Include the protocol, the destination, the reason of failure)

Appendix

List of Operation Procedures

The device provides security management functions and user interfaces listed in the table below only to Machine Administrator and Authenticated Users with System Administrator Privileges.
Authenticated Users without System Administrator Privileges can perform only change of own password.

Item	Using Control Panel	Using CentreWare Internet Services	Default
How to check the Clock	[Device] > [System Settings] > [System Clock/Timers].	-	-
Set Scan	[Customize] > [Edit Home]	-	On
Remote Assistance	[Customize] > [Edit Home]	-	On
Internet Fax	[Customize] > [Edit Home]		On
Web Applications	[Customize] > [Web Applications]	-	On
Set Password Entry for Control Panel Login	[Device] > [Authentication/ Accounting] > [Authentication/ Security Settings] > [Authentication] > [Password Policy] > [Password Entry for Control Panel Login]	-	Off
Set Data Encryption	[Device] > [System Settings] > [Other Settings] > [Data Encryption]	-	Off
Set Overwrite Storage	[Device] > [Authentication/ Accounting] > [Authentication/ Security Settings] > [Overwrite Storage]	[System] > [Security] > [Overwrite Storage]	Off (Panel) Off (CWIS)
Set Authentication	[Device] > [Authentication/ Accounting] > [Authentication/ Security Settings] > [Authentication] > [Login Type]	[Properties] > [Authentication]	Off
Set Private Print	[Device] > [Authentication/ Accounting] > [Authentication/ Security Settings] > [Authentication] > [Charge/Private Print Settings] > [Receive Control]	-	Print
Set Direct Print	[Device] > [Authentication/ Accounting] > [Authentication/ Security Settings] > [Disable Direct Print Feature]	-	Off
Set SMB	[Device] > [Connectivity & Network Setup] > [Port Settings] > [SMB Client]	-	On
Set Fax	[Device] > [App Settings] > [Fax Settings] > [Fax Control] > [Direct Fax]	-	On
	[Device] > [App Settings] > [Fax Settings] > [Fax Control] > [Polling / Storage for remote Devices]	-	On
Create Folder for Fax receive	[Send from Folder] > [+]	[App] > [Send from Folder] > [View]	-

Item	Using Control Panel	Using CentreWare Internet Services	Default
Set Folder Selector for Fax receive	[Device] > [App Settings] > [Fax Settings] > [Fax Control] > [Folder Selector Setup] [Device] > [App Settings] > [Fax Settings] > [Fax Received Options] > [Folder Selector Setup]	-	Off
Set Files Retrieved By Client	[Device] > [App Settings] > [Send from Folder Settings] > [Files Retrieved By Client] > [Force Delete]	-	Delete according to Folder settings
Set Software Update	[Device] > [System Settings] > [Other Settings] > [Software Download]	[System] > [Software Update]	Off
Set Software Download via Network	-	[System] > [Software Update] > [Software Download via Network]	Off
Specify File for Software Update	-	[System] > [Software Update] > [Specify File for Software Update]	-
Set Auto Clear	[Device] > [System Settings] > [System Clock/Timers] > [Auto Clear]	[System] > [Timeouts]	30 seconds
Set Report Print	[Device] > [System Settings] > [Reports] > [Enable Print Reports]	-	On
Set Self Test	[Device] > [Maintenance] > [Power on Self Test]	[System] > [Security] > [Power on Self Test]	Off
Set User Password Minimum Length	[Device] > [Authentication/ Accounting] > [Authentication/ Security Settings] > [Authentication] > [Password Policy] > [Minimum Password Length]	[Permission] > [Authentication] > [Password Policy] > [Minimum Length]	Off
Change the System Administrator Password	[Device] > [Authentication/ Accounting] > [Authentication/ Security Settings] > [Administrator Settings] > [Administrator Password]	[System Administrator] > [Profile]	-
Set Limit Login Attempts	[Device] > [Authentication/ Accounting] > [Authentication/ Security Settings] > [Authentication] > [Invalid Login Settings] > [Maximum Login Attempts - Administrator]	[Permissions] > [Authentication] > [Advanced Settings] > [Limit Login Attempts of System Administrator]	5
	[Device] > [Authentication/ Accounting] > [Authentication/ Security Settings] > [Authentication] > [Invalid Login Settings] > [Maximum Login Attempts - Local User]	[Permissions] > [Authentication] > [Advanced Settings] > [Limit Login Attempts of Local User]	5

Item	Using Control Panel	Using CentreWare Internet Services	Default
Set Access Control	[Device] > [Authentication/ Accounting] > [Authentication/ Security Settings] > [Authentication] > [Access Control] > [System Settings Access]	[Permissions] > [Permissions] > [Access Control] > [Device Access] > [System Settings Access]	On
	[Device] > [Authentication/ Accounting] > [Authentication/ Security Settings] > [Authentication] > [Access Control] > [Device Access]	[Permissions] > [Permissions] > [Access Control] > [Device Access] > [Device Control Panel Access]	On
	[Device] > [Authentication/ Accounting] > [Authentication/ Security Settings] > [Authentication] > [Access Control] > [App Access]	[Permissions] > [Permissions] > [Access Control] > [App Access]	On
Set Job	[Device] > [Authentication/ Accounting] > [Authentication/ Security Settings] > [Job Status Default] > [Active Jobs View]	[Jobs] > [Jobs Settings] > [Active Jobs View]	On
	[Device] > [Authentication/ Accounting] > [Authentication/ Security Settings] > [Job Status Default] > [Job Operation Restrictions]	[Permissions] > [Permissions] > [Access Control] > [Job Operation Restrictions]	-
Set Personalization	-	[Permissions] > [Permissions] > [Access Control] > [Personalization Restrictions] > [Edit Home]	Unlocked
Set TLS	-	[System] > [Security] > [Certificates] > [Certificate Settings] > [Device Certificates]	-
	[Device] > [Connectivity & Network Setup] > [Security Settings] > [SSL/TLS Settings]	[System] > [Security] > [Network Security] > [SSL/TLS Settings]	-
Configuring Certification	-	[System] > [Security] > [Certificate] > [Certificate Settings] > [Import]	-
Set FIPS140-2	[Device] > [Connectivity & Network Setup] > [Security Settings] > [Other Settings] > [FIPS 140 Validation Mode]	[System] > [Security] > [Network Security] > [FIPS 140-2]	Off
Set HTTP	[Device] > [Connectivity & Network Setup] > [Security Settings] > [SSL/TLS Settings] > [HTTP - SSL/TLS Communication]	[Network] > [Protocols] > [HTTP] > [Port (HTTP/HTTPS)]	-
Set TCP/IP	[Device] > [Connectivity & Network Setup] > [Protocol Settings] > [TCP/IP - Common Settings]	[Network] > [Connections] > [Ethernet] > [Common] > [Edit]	-
Set WebDAV	[Device] > [Connectivity & Network Setup] > [Port Settings] > [WebDAV]	[Network] > [Protocols] > [WebDAV]	On
Set Receive E-mail (POP3)	[Device] > [Connectivity & Network Setup] > [Port Settings] > [Receive E-mail]	[Network] > [Protocols] > [POP3]	Off

Item	Using Control Panel	Using CentreWare Internet Services	Default
Set IPP	[Device] >[Connectivity & Network Setup] > [Port Settings] > [IPP]	[Network] > [Protocols] > [IPP]	Off
Set IPsec	[Device] > [Connectivity & Network Setup] > [Security Settings] > [IPsec Settings]	[Network] > [Protocols] > [IPsec]	Off
Set WSD	[Device] >[Connectivity & Network Setup] > [Port Settings] > [WSD]	[Network] > [Protocols] > [WSD]	On
Set LPD	[Device] >[Connectivity & Network Setup] > [Port Settings] > [LPD]	[Network] > [Protocols] > [LPD]	On
Set Port9100	[Device] >[Connectivity & Network Setup] > [Port Settings] > [Port 9100]	[Network] > [Protocols] > [Port 9100]	On
Set FTP Client	[Device] >[Connectivity & Network Setup] > [Port Settings] > [FTP Client]	[Network] > [Protocols] > [FTP Client]	On
Set SFTP	-	[Network] > [Protocols] > [SFTP]	On
Set SOAP	[Device]> [Connectivity & Network Setup] > [Port Settings] > [SOAP]	[Network] > [Protocols] > [SOAP]	On
Set SNMP	[Device] > [Connectivity & Network Setup] > [Port Settings] > [SNMP]	[Network] > [Protocols] > [SNMP]	On
Set Bonjour	[Device] > [Connectivity & Network Setup] > [Port Settings] > [Bonjour]	[Network] > [Protocols] > [Bonjour]	On
Set USB	[Device] > [Connectivity & Network Setup] > [Port Settings] > [USB]	[Network] > [USB]	On
Set NFC	-	[Network] > [NFC]	On
Set CSRF	-	[Network] > [Protocols] > [HTTP] >[CSRF Protection:]	Off
Set Service Representative Restricted Operation	[Device] > [System Settings] > [Other Settings] > [Service Rep.Restricted Operation]	[System] > [Security] > [Service Representative Operation Settings]	Off
Set Audit Log, Import the Audit LogFile	[Device] > [Audit Log Settings]	[System] > [Logs] > [Audit Log]	Off
Set Browser Session Time out	-	[System] > [Timeouts] > [Auto Clear (Internet Services)]	20
Set Custom Service	-	[App] > [Custom Services Settings]	On
Set Plugin	[Device] > [System Settings] > [Plug-in Settings] > [Embedded Plug-ins]	[System] > [Plug-in Settings] > [Embedded Plug-ins]	On
Print Files in Folder with internet Services	-	[System] > [Security] > [Print Files in Folder with internet Services]	Disabled

Note • WSD stands for Web Services on Devices.

Fault Codes

This section describes fault codes.
An error message and fault code (***-***) are displayed on the touch screen if printing terminated abnormally because of an error, or a malfunction occurred in the device.
For faxing, a fault code is also displayed on an Activity Report and a Transmission Report Job Undelivered.
Refer to the fault codes in the following table to resolve problems.

Important • If a fault code is displayed, any print data remaining in the device and information stored in the device's memory is not secured.

If a fault code is displayed that is not listed in the following table, or if you cannot resolve an error despite following the instructions describes in the table, contact our Customer Support Center. The contact number is printed on the label or card attached to the device.

Fault Code	Cause and Remedy	
016-210 **016-211** **016-212** **016-213** **016-214** **016-215**	**[Cause]**	An error occurred in the software.
	[Remedy]	Switch off the device power, make sure that the touch screen is blank, and then switch on the device power. If the error still is not resolved, contact our Customer Support Center.
016-400	**[Cause]**	The user name or password for 802.1x authentication does not match in the setting of Ethernet 1.
	[Remedy]	Confirm and correctly enter the user name or password in the setting of Ethernet 1. If the error still is not resolved, check whether the network environment is set correctly.
016-401	**[Cause]**	The 802.1x authentication method cannot be processed in the setting of Ethernet 1.
	[Remedy]	Set the authentication method of the device to the same method as set for the authentication server in the setting of Ethernet 1.
016-402	**[Cause]**	The authentication connection of Ethernet 1 timed out.
	[Remedy]	Confirm the network connection of Ethernet 1 and switch setting of the authentication device physically connected to the device via a network, and check whether it is connected to the device correctly.
016-403	**[Cause]**	The root certificate of Ethernet 1 did not match.
	[Remedy]	Confirm the authentication server and store the root certificate of the server certificate of the authentication server into the device. If you cannot acquire the root certificate of the server certificate, set [Server Certificate Verification] of [IEEE 802.1x Settings] of Ethernet 1 to [Disabled] on the touch screen.
016-404	**[Cause]**	802.1x authentication error for Ethernet 1 occurred.
	[Remedy]	Execute the operation again. If the same message is displayed again, contact our Customer Support Center.
016-405	**[Cause]**	An error occurred in the certificate stored in the device.
	[Remedy]	Initialize the certificate.

Fault Code	Cause and Remedy	
016-406	**[Cause]**	An error occurred in the SSL client certificate.
	[Remedy]	Take one of the following measures: **1.** Store an SSL client certificate in the device, and set it as the SSL client certificate. **2.** If an SSL client certificate cannot be set on the device, select an option other than [EAP-TLS] in [Authentication Method].
016-450	**[Cause]**	The SMB host name already exists.
	[Remedy]	Change the host name.
016-454	**[Cause]**	Unable to retrieve the IP address from DNS.
	[Remedy]	Confirm the DNS configuration and IP address retrieve setting.
016-503	**[Cause]**	Unable to resolve the SMTP server name when sending e-mail.
	[Remedy]	Check on CentreWare Internet Services whether the SMTP server settings are correct. Also, confirm whether the DNS server settings are correct.
016-513	**[Cause]**	An error occurred in connecting to the SMTP server. Probable causes are as follows: **1.** The SMTP server or network may be overloaded. **2.** The source port number for SMTP is incorrect.
	[Remedy]	For 1, wait for a while, and then execute the operation again. For 2, confirm whether the source port number for SMTP is correct.
016-522	**[Cause]**	LDAP server SSL authentication error. Unable to acquire an SSL client certificate.
	[Remedy]	The LDAP server is requesting an SSL client certificate. Set an SSL client certificate on the device.
016-523	**[Cause]**	LDAP server SSL authentication error. The server certificate data is incorrect.
	[Remedy]	The device cannot trust the SSL certificate of the LDAP server. Register the root certificate for the LDAP server's SSL certificate to the device.
016-524	**[Cause]**	LDAP server SSL authentication error. The server certificate will expire soon.
	[Remedy]	Change the SSL certificate of the LDAP server to a valid one. You can clear this error by selecting [Disabled] for [LDAP - SSL/TLS Communication] under [SSL/TLS Settings] on the device; however, note that selecting this option does not ensure the validity of the LDAP server.
016-525	**[Cause]**	LDAP server SSL authentication error. The server certificate has expired.
	[Remedy]	Change the SSL certificate of the LDAP server to a valid one. You can clear this error by selecting [Disabled] for [LDAP - SSL/TLS Communication] under [SSL/TLS Settings] on the device; however, note that selecting this option does not ensure the validity of the LDAP server.

Fault Code	Cause and Remedy
016-526	**[Cause]** LDAP server SSL authentication error. The server name does not match the certificate. **[Remedy]** Set the same LDAP server address to the device and to the SSL certificate of the LDAP server. You can clear this error by selecting [Disabled] for [LDAP - SSL/TLS Communication] under [SSL/TLS Settings] on the device; however, note that selecting this option does not ensure the validity of the LDAP server.
016-527	**[Cause]** LDAP server SSL authentication error. This is an SSL authentication internal error. **[Remedy]** An error occurred in the software. Contact our Customer Support Center.
016-703	**[Cause]** The device received an e-mail specified with an invalid folder number. **[Remedy]** For errors occurring during e-mail reception: Take one of the following measures: • Register the specified folder number, and request the sender to send the e-mail again. • Request the sender to send to an available folder. If the error still is not resolved, contact our Customer Support Center.
016-704	**[Cause]** The folder is full, and storage capacity is insufficient. **[Remedy]** Delete unnecessary files from the folder, and save the file.
016-705	**[Cause]** Probable causes are as follows: **1.** You have specified the device for the folder registry for the scanned document. However, the Scanner Kit* is not installed. **2.** You have not used the print driver for the device. **3.** The device received a Secure Print, Print Stored File, Charge Print, or Private Charge Print job with no storage installed. *: An optional component is required for some models. For more information, contact our Customer Support Center. **[Remedy]** For 1, press the Home button, and check whether [Scan to PC] is displayed. If [Scan to PC] is displayed, then check whether the scanned document can be stored in a folder. If unable to store it in the folder, install the Scanner Kit. For 2, use the print deriver appropriate for the device. For 3, check whether the storage is installed on the device. If the storage is not installed: • If you do not need to use the feature, select [Not Installed] under [Storage] on the [Options] tab of the print driver. • If you need to use the feature, install the storage. If the storage is installed: • Select [Installed] under [Storage] on the [Options] tab of the print driver. If the error still is not resolved, contact our Customer Support Center.

Fault Code	Cause and Remedy	
016-706	**[Cause]**	The storage space is insufficient because the number of Secure Print users exceeded the maxi-mum limit.
	[Remedy]	Delete unnecessary files from the device, and delete unnecessary Secure Print users.
016-711	**[Cause]**	The upper limit for the e-mail size has been exceeded.
	[Remedy]	Take one of the following measures, and then try sending the mail again. • Reduce the number of pages of the document. • Lower the resolution with [Resolution]. • Reduce the magnification with [Reduce/Enlarge]. • Ask your system administrator to increase the value set for [Maximum Total Data Size]. • For color scanning, set [MRC High Compression] to [On] under [File Format].
016-713	**[Cause]**	The passcode entered does not match the passcode set on the folder.
	[Remedy]	Enter the correct passcode.
016-714	**[Cause]**	The specified folder does not exist.
	[Remedy]	Create a new folder or specify an existing folder.
016-764	**[Cause]**	Unable to connect to the SMTP server.
	[Remedy]	Consult the SMTP server administrator.
016-765	**[Cause]**	Unable to send the e-mail because the hard disk on the SMTP server is full.
	[Remedy]	Consult the SMTP server administrator.
016-766	**[Cause]**	An error occurred on the SMTP server.
	[Remedy]	Consult the SMTP server administrator.
016-767	**[Cause]**	Unable to send the e-mail because the address is not correct.
	[Remedy]	Confirm the address, and try sending again.
016-768	**[Cause]**	Unable to connect to the SMTP server because the device's mail address is incorrect.
	[Remedy]	Confirm the device's mail address.
016-769	**[Cause]**	The SMTP server does not support delivery receipts (DSN).
	[Remedy]	Send e-mail without setting delivery receipts (DSN).
016-774	**[Cause]**	Unable to process compression conversion because of insufficient storage space.
	[Remedy]	Delete unnecessary data from the storage to free up disk space.

Fault Code	Cause and Remedy	
016-781	**[Cause]**	Probable causes are as follows: **1.** The mail server cannot be found during e-mail sending (TCP/IP session establishment failed). **2.** The device received an SMTP server error from the mail server during e-mail sending.
	[Remedy]	For 1, take one of the following measures: • Check whether the network cables are plugged in securely. • Check whether the IP address of the SMTP server when an IP address is used for server specification. For 2, enter the host name using ASCII characters. Available ASCII characters are as follows: • alphabets • numerals Check whether or not ASCII characters are used in [Device] > [Connectivity & Network Setup] > [Device's E-mail Address/Host Name].
018-405	**[Cause]**	An error occurred during LDAP authentication.
	[Remedy]	The account is disabled in the active directory of the authentication server, or the access is set to disabled. Consult your network administrator.
018-596	**[Cause]**	An error occurred during LDAP server authentication.
	[Remedy]	Execute the operation again. If the error still is not resolved, contact our Customer Support Center.
018-781	**[Cause]**	An LDAP server protocol error occurred as a result of the Address Book operation. Connection to the server cannot be established for the Address Book query.
	[Remedy]	Take one of the following measures: • Confirm the network cable connection. • If the network cable connection has no problem, confirm the active status of the target server. • Check whether the server name has been correctly set for [LDAP Server/Directory Service Settings] under [Remote Authentication Server/Directory Service].

Fault Code	Cause and Remedy	
018-782 018-783 018-784 018-785 018-786 018-787 018-788 018-789 018-790 018-791 018-792 018-793 018-794 018-795 018-796 018-797	**[Cause]**	An LDAP server protocol error occurred as a result of the Address Book operation. The server re-turned RFC2251 Result Message for Address Book query.
	[Remedy]	Have your network administrator confirm the LDAP server status.
027-452	**[Cause]**	IP address of IPv4 already exists.
	[Remedy]	Change the IP address of IPv4 set on the device or the IP address of IPv4 on the network device.
027-500	**[Cause]**	Unable to connect to the SMTP server.
	[Remedy]	Specify the SMTP server name correctly or specify the server by using its IP address.
027-706	**[Cause]**	Unable to find the S/MIME certificate associated with the device's e-mail address when sending e-mail.
	[Remedy]	Import the S/MIME certificate corresponding to the mail address to the device.
027-707	**[Cause]**	The S/MIME certificate associated with the device's email address has expired when sending e-mail.
	[Remedy]	Ask the sender to issue a new S/MIME certificate and import the certificate to the device.
027-708	**[Cause]**	The S/MIME certificate associated with the device's email address is not reliable.
	[Remedy]	Import a reliable S/MIME certificate to the device.
027-709	**[Cause]**	The S/MIME certificate associated with the device's email address has been discarded when sending e-mail.
	[Remedy]	Import a new S/MIME certificate to the device.
027-710	**[Cause]**	No S/MIME certificate is attached to the received e-mail.
	[Remedy]	Ask the sender to send the e-mail with an S/MIME certificate attached.
027-711	**[Cause]**	No S/MIME certificate can be obtained from the received e-mail.
	[Remedy]	Import the sender's S/MIME certificate to the device, or ask the sender to send S/MIME signature mail with an S/MIME certificate attached.

Fault Code	Cause and Remedy	
027-712	**[Cause]**	The received S/MIME certificate has expired, or is an unreliable certificate.
	[Remedy]	Ask the sender to send the e-mail with a valid S/MIME certificate attached.
027-713	**[Cause]**	The received e-mail has been discarded because it may have been altered on its transmission route.
	[Remedy]	Inform this error to the sender, and ask the sender to send the e-mail again.
027-714	**[Cause]**	The received e-mail has been discarded because the address in its From field is different from the mail address in the S/MIME signature mail.
	[Remedy]	Inform the sender that the mail addresses differ, and ask the sender to send the e-mail again.
027-715	**[Cause]**	The received S/MIME certificate has not been registered on the device, or has not been set for use on the device.
	[Remedy]	Import the sender's S/MIME certificate to the device, or change settings to use the S/MIME certificate on the device if the S/MIME certificate has already been registered.
027-716	**[Cause]**	The received S/MIME certificate has been discarded because the certificate was unreliable.
	[Remedy]	Ask the sender to send the e-mail with a reliable S/MIME certificate attached.
027-717	**[Cause]**	Unable to obtain SMTP server address for e-mail transmissions from the DNS server.
	[Remedy]	Check whether the DNS server is set correctly.

ApeosPort C7070/C6570/C5570/C4570/C3570/C3070
Security Function Supplementary Guide

ME8996E2-1_20210122 (Edition 1)
January 2021
Fuji Xerox Co., Ltd.