Version 1.0.1

Xerox® PrimeLink® C9065/C9070 Printer

Security Function Supplementary Guide

Table of Contents

1. Before Using the Security Function

This section describes the certified security functions and the items to be confirmed.

Preface

This guide is intended for the manager and system administrator of the organization where the machine is installed, and describes the setup procedures related to security.

For general users, this guide describes the operations related to security features.

For information on the other features available for the machine, refer to the following guidance.

Xerox® PrimeLink® C9065/C9070 Printer System Administrator Guide:
Version 1.0

Xerox® PrimeLink® C9065/C9070 Printer User Guide:
Version 1.0

The hash values of the PDF files are described in the Security Target disclosed at the Xerox (http://www.office.xerox.com/digital-printing-equipment/enus.html) and JISEC (http://www.ipa.go.jp/security/jisec/jisec_e/) website.
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 Manual version might be changed when the manual content is updated.

The security features of the Xerox® PrimeLink® C9065/C9070 Printer is supported by the following ROM versions respectively.

Xerox® PrimeLink® C9065/C9070 Printer

Controller ROM	Ver. 1.1.3
FAX ROM	Ver. 2.2.1

Important:

The machine has obtained IT security certification for HCD PP v1.0.

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 "Xerox" and the model name "Xerox PrimeLink C9065" or "Xerox PrimeLink C9070"displayed on the control panel when the machine starts up. And you can check the ROM versions along with the operation described in "Confirm the Machine ROM Version, Product Code and the System Clock" (P. 8).

Your ROM and user documentation may not be the certified version because they may have been updated along with machine improvements.

For the latest information concerning your machine, download the latest versions from http://www.support.xerox.com/support

Please check the state of the delivered machine's corrugated cardboard packaging (Including Option). 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. If you have such inquiries as the following, please contact us:

- Inquiries about the machine's functions
- All other inquiries.

And you check the product code of Fax Kit as shown below.

Product Name	Product Code
KIT 1 LINE FAX + IFAX US/DMO-W	EC103350
KIT 3 LINE FAX + IFAX US/DMO-W	EC103351

This guide has been prepared on the assumption that the security functions, fax function, scan function, and network scan function are available. You need to purchase and install Fax Kit. The machine installed other optional products is out of the target of evaluation. 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 the security functions, fax function, scan function, and network scan function. For the security function, you can check with “Overwrite Hard Disk” in the setup menu. For fax function, “Fax” button. For scan function, “Store to Folder” button. For network scan function, “Scan to PC” button.

You can find the detailed operation to see the buttons in Appendix "List of Operation Procedures". And the default value for System Administrator's ID and password are described in “System Administrator Settings” of “Authentication / Security Settings” in User Guide.

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. “PCL6 Driver – Xerox User Interface – Microsoft Certified” 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 machine. Microsoft Edge was used as the web browser in the evaluation.

- The system administrator used it for getting the audit logs from the machine. 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

If you could not attend the operation of the customer engineer at the time of initial installation, please perform Delete All Data.

When you change settings that cannot maintain the security function during operation, please perform Delete All Data 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 perform Delete All Data after the maintenance operation and configure settings again according to the procedure of this guide.

For secure operation, prior to disposing of the machine, please perform Delete All Data by resetting [Data Encryption].

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

Security Features

Xerox® PrimeLink® C9065/C9070 Printer has the following security features:

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

Settings for the Secure Operation

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

For details on the setting procedures, refer to the following sections.

" Initial Settings Procedures Using Control Panel" (P. 10)

" Initial Settings Procedures Using Embedded Web Server " (P.16)

" Disabling PJL data read/write commands" (P.21)

" Regular Review by Audit Log" (P.27)

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.

Item	Description
Passcode Entry from Control Panel	Set to [Enabled].
Overwrite Hard Disk	Default [3 Overwrites].
Data Encryption	Default [On].
Authentication	Set to [Login to Local Accounts]
Private Print	Set to [Save as Private Charge Print].
Files Retrieved Client	Set to [Force Delete]
Fax	Direct Fax det 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.
Auto Clear	Default [on].
Report Print	Set to [Disabled].
Self-Test	Set to [on].
Software Download	Set to [Enabled].
System Administrator Passcode	Change the default passcode to another passcode of 9 or more characters.
Maximum Login Attempts	Default [5] Times.
Scheduled Image Overwrite	Set to [Enabled] as necessary.
Access Control	Set to [Locked] for Device Access and Service Access.
User Passcode Minimum Length	Set to [9] characters.
SMB	Set to [Disabled]
WebDAV	Set to [Disabled].
Receive E-mail	Default [Disabled].
IPP	Default [Enabled].
SSL/TLS	Set to [Enabled].
TCP/IP	Set to [IPv4].
Service Representative Restricted Operation	Set to [Enabled] and enter a passcode of 9 or more characters.
Audit Log	Set to [Enabled].
IPSec	Set to [Enabled].
SNMP	Set to [Disabled].
WSD Scan	Set to [Disabled].
WSD Print	Set to [Disabled].
LPD	Set to [Disabled].
Port 9100	Set to [Disabled].
FTP Client	Set to [Disabled].

SOAP	Set to [Disabled].
S/MIME	Set to [Enabled].
USB	Set to [Disabled].
Bonjour	Set to [Disabled].
CSRF	Set to [Enabled].
Embedded Plug-ins	Set to [Disabled].
Upgrades	Set to [Enabled].
FIPS140 Validation Mode	Set to [Enabled].
PostScript Passwords	Set new password
Disabling PJL data read/write commands	Disabling PJL data read/write commands.

Note:

WSD stands for Web Services on Device.

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.

Data Restoration

The enciphered data cannot be restored in the following conditions.

- When a problem occurs in the hard disk.
- Without the correct encryption key.
- Without the correct System Administrator ID and passcode when setting [Service Representative Restricted Operation] to [On].

Starting Use of the Data Encryption Feature and Changing the Settings

When data encryption is started or ended, or when the encryption key is changed, the machine must be restarted. The corresponding recording area (the Hard Disk) is reformatted when restarting. In this case, the previous data is not guaranteed.

The recording area stores the following data:

- Spooled print data
- Print data including the secure print and sample print
- Forms for the form overlay feature
- Folder settings (Folder name, passcode, etc.)
- Files in Folder

- Address book data

Important:

Be sure to save all necessary settings and files before starting to use the data encryption feature or changing the settings.

An error occurs if the connected hard disk does not match the encryption settings.

Use of the Overwrite Hard Disk

In order to protect the data stored on the hard disk from unauthorized retrieval, you can set the overwrite conditions to apply them to the data stored on the hard disk.

You can select the number of overwrite passes as one or three times. When [1 Overwrite] is selected, "0" is written to the disk area. [3 Overwrites] ensures higher security than [1 Overwrite].

The feature also overwrites temporarily saved data such as copy documents.

Important:

If the machine is powered off during the overwriting operation, unfinished files may remain on the hard disk. When the power is restored, the overwriting operation will resume with the unfinished files remaining on the hard disk.

Service Representative Restricted Operation

Specifies whether the Service Representative has full access to the security features of the machine, including the ability to change System Administrator settings.

For the C9065/C9070 Printer, select [On] and then set [Maintenance Passcode] to restrict the Service Representative from entering the System Administration mode.

Important:

If the System Administrator's ID and the passcode are lost when [Service Rep. Restricted Operation] is set to [On], neither you nor the Xerox representative will be able to change any setting in the System Administration mode.

For Optimal Performance of the Security Features

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

- The manager needs to assign appropriate people as machine and system administrators and manage and train them properly.

- The system administrator need to train users about the machine operation and precautions according to the policies of their organization and the product guidance.
- The machine needs to be placed in a secure or monitored area where the machine is protected from unmanaged physical access.
- If the network where the machine 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 guessable password.
    - A password needs to contain numeric and alphabetic characters, and symbols.
- Users and administrators need to manage and operate the machine 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, and 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 the remote trusted IT products that communicate with the machine 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, Audit Server) and the TLS server (Mail Server) that communicate with the machine, 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 the Embedded Web Server, please do not access other web sites, 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 machine address in the browser proxy exception list. By this setting, secure communication will be ensured because the machine 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 Embedded Web Server for 20 minutes, it will automatically logout. Logout explicitly when leaving a client PC within 20 minutes. System administrator must ensure that all users follow this guidance. Otherwise unauthorized users can operate this device using Embedded Web Server that have not been logged out.
- PostScript password must be set. Otherwise unauthorized users can exploit the user data using PostScript.

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

Confirm the Machine ROM Version, Product Code and the System Clock

Before making initial settings, the System Administrator (Machine Administrator) needs to check the ROM version of the machine, product code and the system clock of the machine.

How to Check by Control Panel

1. Press the <Machine Status> button on the control panel.
2. Select [Software Version] on the [Device information] screen.

   You can identify the software versions of the components of the machine on the screen.

How to Check by Print Report

1. Press the <Machine Status> button on the control panel.
2. Select [Print Reports] on the [Device information] screen.
3. Select [Printer Reports] on the touch screen.
4. Select [Configuration Reports].
5. Press the <Start> button on the control panel.

   You can identify the software versions of the components of the machine and product code by Print Report.

How to Check the System Clock

1. Press the <Log In/Out> button on the control panel.
2. Enter the System Administrator's Login ID with the keypad displayed.

3. Select [Enter] on the touch screen.
4. Press the <Machine Status> button on the control panel.
5. Select [Tools] on the touch screen.
6. Select [System Settings].
7. Select [Common Service Settings].
8. Select [Device Clock/Timers].
9. You can check the time and the date of the internal clock. If you need to change the time and the date, refer to the following procedures.
10. Select the required option.
11. Select [Change Settings].
12. Change the required setting.
13. Select [Save].
14. Select [Close].

2. Initial Settings Procedures Using Control Panel

This section describes the initial settings related to Security Features, and how to set them on the machine's control panel.

Set Passcode Entry from Control Panel Login

1. Press the <Log In/Out> button on the control panel.
2. Enter the system administrator's ID with the keyboard displayed.
3. Select [Enter]
4. Select [Close] for warning message.
5. Press the <Machine Status> button on the control panel.
6. Select [Tools].
7. Select [Authentication/Security Settings] on the [Tools] screen.
8. Select [Authentication].
9. Select [Passcode Policy].
10. Select [Passcode Entry from Control Panel].
11. Select [Change Settings].
12. Select [On].
13. Select [Save].
14. Select [Close].

Set Overwrite Hard Disk

1. Select [Authentication/Security Settings] on the [Tools] screen.
2. Select [Overwrite Hard Disk].
3. Select [Number of Overwrites].
4. Select [1 Overwrite] or [3 Overwrites].
5. Select [Save].

Set Data Encryption

1. Select [System Settings] on the [Tools] screen.

2. Select [Common Service Settings].
3. Select [Other Settings].
4. Select [Data Encryption].
5. Select [Change Settings].
6. Select [On].
7. Select [Save].
8. Select [Yes] to make the change.
9. Select [Yes] to reboot.

Set Authentication

1. Select [Authentication/Security Settings] on the [Tools] screen.
2. Select [Authentication].
3. Select [Login Type].
4. Select [Login to Local Accounts].
5. Select [Save].
6. To exit the [Tools] screen, press the <Services> button on the control panel.
7. Select [Reboot Now] on the confirmation screen.

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

Set Private Print

1. Log in as system administrator.
2. Press the <Machine Status> button on the control panel.
3. Select [Tools].
4. Select [Authentication/Security Settings] on the [Tools] screen.
5. Select [Authentication].
6. Select [Charge/Private Print Settings].
7. Select [Received Control].
8. Select [Change Settings].
9. Select [According to Print Accounting].
10. Select [Save As Private Charge Print Job] for [Job Login Success].
11. Select [Delete Job] for [Job Login Failure].
12. Select [Delete Job] for [Job without User ID].
13. Select [Save] twice.

14. Select [Close].

Set Files Retrieved Client

1. Select [System Settings] on the [Tools] screen.
2. Select [Folder Service Settings].
3. Select [3. Files Retrieved Client].
4. Select [Force Delete]

Set SMB

1. Select [System Settings] on the [Tools] screen.
2. Select [Connectivity & Network Setup].
3. Select [Port Settings].
4. Select [SMB Client].
5. Select [Change Settings].
6. Select [Port Status].
7. Select [Change Settings].
8. Select [Disabled].
9. Select [Save].
10. Select [Close] twice.

Set Fax

If the Fax option is installed, the following procedure must be performed.

1. Select [System Settings] on the [Tools] screen.
2. Select [Fax Service Settings].
3. Select [Fax Control].
4. Select [Direct Fax].
5. Select [Change Settings].
6. Select [Disabled].
7. Select [Save].
8. Select [Polling / Storage for Remote Devices].
9. Select [Change Settings].
10. Select [Disabled].

11. Select [Save].
12. Select [Close].
13. To exit the [Tools] screen, press the <Services> button on the control panel.
14. Select [Reboot Now] on the confirmation screen.

Create Folder for Fax receive

If the Fax option is installed, the following procedure must be performed.

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

1. Log in as a user with System Administrator role (but not System Administrator's user ID).
2. Select [Setup & Calibration] on the [Tools] screen.
3. Select [Setup]
4. Select [Create Folder].
5. Select a box.
6. Select [Off] for [Check Folder Passcode].
7. Select [Save].
8. Select [1. Folder Name] on [Create/Delete] screen and enter a folder name and select [Save].
9. Select [Close] on [Crate/Delete] screen to close it.

Set Folder Selector for Fax receive

If the Fax option is installed, the following procedure must be performed.

1. Select [System Settings] on the [Tools] screen.
2. Select [Fax Service Settings].
3. Select [Fax Control].
4. Select [Folder Selector Setup].
5. Select [Change Settings].
6. Select [Enabled].
7. Select [Save].
8. Select [Close].
9. Select [Fax Received Options].
10. Select [Folder Selector Setup].
11. Select a line to be configured and select [Change Settings].
12. Select [On].

13. Enter folder number (three digits) created in “Create Folder for Fax receive”.
14. Select [Save].
    Back to *11* and repeat steps for all lines.
15. Select [Close] twice.

Set Software Download

1. Select [System Settings] on the [Tools] screen.
2. Select [Common Service Settings].
3. Select [Other Settings].
4. On the [Other Settings] screen, select [Software Download].
5. Select [Change Settings].
6. Select [Enabled].
7. Select [Save].
8. To exit the [Common Service Settings] screen, select [Close].

Set Auto Clear

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

1. Select [System Settings] on the [Tools] screen.
2. Select [Common Service Settings].
3. Select [Device Clock/Timers].
4. Select [Auto Clear].
5. Select [Change Settings].
6. Select [On].
7. Select [Save].
8. To exit the [Device Clock/Timers] screen, select [Close].

Set Report Print

1. Select [System Settings] on the [Tools] screen.
2. Select [Common Service Settings].
3. Select [Reports].
4. Select [Print Reports Button].

5. Select [Disabled].
6. Select [Save].
7. To exit the [Reports] screen, select [Close].

Set Self Test

1. Select [System Settings] on the [Tools] screen.
2. Select [Common Service Settings].
3. Select [Maintenance].
4. Select [Power on Self Test].
5. Select [On].
6. Select [Save].
7. To exit the [Maintenance] screen, select [Close].
8. To exit the [Tools] screen, press the <Services> button on the control panel.
9. Select [Reboot Now] on the confirmation screen.

3. Initial Settings Procedures Using Embedded Web Server

This section describes the initial settings related to Security Features, and how to set them on Embedded Web Server.

Set up IP address according to [Tools] > [System Settings] > [Connectivity & Network Setup] > [Protocol Settings] in User Guide before using Embedded Web Server.

Preparations for Settings on the Embedded Web Server

Prepare a computer supporting the TCP/IP protocol to use Embedded Web Server. Embedded Web Server supports the browsers that satisfy " TLS" (P.8)conditions.

1. Open your Web browser, enter the TCP/IP address of the machine in the Address or Location field, and press the <Enter> key.
2. Enter the System Administrator's ID and the passcode.
3. Click [OK].
4. Click [OK] for warning message.
5. Display the [Properties] screen by clicking the [Properties] tab.

Set User Passcode Minimum Length

This feature is only applicable to Local Authentication mode.

1. Click [Security] on the [Properties] screen.
2. Click [User Details Setup].
3. Set [9] for [Minimum Passcode Length].
4. Click [Apply].
5. Click [Reboot Device].

Change the System Administrator's Passcode

1. Click [Security] on the [Properties] screen.
2. Click [System Administrator Settings].

3. Enter the System Administrator's ID in the [Administrator's Login ID] box.
4. Enter a new System Administrator's passcode of 9 or more characters in the [Administrator's Passcode] box.
5. Enter the new System Administrator's passcode in the [Retype Administrator's Passcode] box.
6. Click [Apply].

Note

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

Set Maximum Login Attempts

1. Click [Security] on the [Properties] screen.
2. Click [User Details Setup].
3. Enter [5] in the both [System Administrator] and [Local User] box for [Login Attempts Limit].
4. Click [Apply].

Set Scheduled Image Overwrite

Note: Set as necessary.

1. Click [Security] on the [Properties] screen.
2. Click [On Demand Overwrite].
3. Click [Scheduled].
4. Check the [Enabled] box for [Scheduled Image Overwrite].
5. Select [Daily], [Weekly], or [Monthly] for [Frequency]
6. Set [Day], [Hour], and [Minutes],
7. Click [Apply].

Set Access Control

1. Click [Security] on the [Properties] screen.
2. Click [Authentication Configuration].
3. Click [Next].
4. Click [Configure] for [Device Access].

5. Select [Locked] for [Service Pathway], [Job Status Pathway], and [Machine Status Pathway].
6. Click [Apply].
7. Click [Authentication Configuration].
8. Click [Next].
9. Click [Configure] for [Service Access].
10. Click [Lock All].
11. Click [Apply].
12. Click [Job Status Default].
13. Click [Active Jobs View].
14. Select [Yes] for [Hide Job Details].
15. Click [Apply].
16. Click [Job Operation Restriction].
17. Select [Job Owner and administrator] for all operations.
18. Click [Apply].
19. Click [Reboot Device].

Set TLS

1. Click [Security] on the [Properties] screen.
2. Click [Device Digital Certificate Management].
3. Click [Create New Certificate].
4. Select [Self-Signed Certificate].
5. Click the [Continue].
6. Set the details as necessary.
7. Click [Apply].
8. Click [SSL / TLS Settings].
9. Select the [Enabled] check box for [HTTP - SSL / TLS Communication]
10. Select [SSL / TLS] for [SMTP - SSL / TLS Communication].
11. Select the [Only Over SSL / TLS] check box for [IPP].
12. Select the [Enabled] check box for [Verify Remote Server Certificate].
13. Select [TLS1.2] check box for [Protocol Version].
14. Click [Apply].
15. Click [Reboot Device].

Note:

You should import the CA certificate according to the same procedure as "Configuring Certificates" (P.19) when enabling [Verify Remote Server Certificate].

You can find how to create Self-Sighed Certification in "11 Device Digital Certificate Management" (P.37).

Configuring Certificates

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

1. Click [Security] on the [Properties] screen.
2. Click [Device Digital Certificate Management].
3. Click [Upload Signed Certificate].
4. Enter a file name for the file you want to import or select the file to be imported by clicking [Browse].
5. Enter [Password] and enter the [Retype Password] as necessary.
6. Click [Import].

Set TCP/IP

1. Click [Connectivity] on the [Properties] screen.
2. Click [Protocols].
3. Click [TCP/IP].
4. Select [IPv4] for [IP Mode].
5. Click [Apply].

Set WebDAV

1. Click [Connectivity] on the [Properties] screen.
2. Click [Port Setting].
3. Uncheck the [Enabled] box for [WebDAV].
4. Click [Apply].

Set Receive E-mail

1. Click [Connectivity] on the [Properties] screen.
2. Click [Port Setting].
3. Uncheck the [Receive E-mail] box.
4. Click [Apply].

Set IPP

1. Click [Connectivity] on the [Properties] screen.
2. Click [Port Setting].
3. Check the [Enabled] box for [IPP].
4. Click [Apply].

Set WSD Scan

1. Click [Connectivity] on the [Properties] screen.
2. Click [Port Settings].
3. Uncheck the [Enabled] box for [WSD Scan].
4. Click [Apply].
   Note • WSD stands for Web Services on Devices

Set WSD Print

1. Click [Connectivity] on the [Properties] screen.
2. Click [Port Settings].
3. Uncheck the [Enabled] box for [WSD Print].
4. Click [Apply].

Set LPD

1. Click [Connectivity] on the [Properties] screen.
2. Click [Port Settings].
3. Uncheck the [Enabled] box for [LPD].
4. Click [Apply].

Set Port9100

1. Click [Connectivity] on the [Properties] screen.
2. Click [Port Settings].

3. Uncheck the [Enabled] box for [Port9100].
4. Click [Apply].

Set FTP Client

1. Click [Connectivity] on the [Properties] screen.
2. Click [Port Settings].
3. Uncheck the [Enabled] box for [FTP Client].
4. Click [Apply].

Set Browser Refresh

1. Click [General Setup] on the [Properties] screen.
2. Click [Internet Services Settings].
3. Enter the “0” in the [Auto Refresh Interval] box.
4. Click [Apply].

Set IPSec

1. Click [Security] on the [Properties] screen.
2. Click [IPSec].
3. Uncheck the [Enabled] box for [Protocol].

Set SOAP

1. Click [Connectivity] on the [Properties] screen.
2. Click [Port Settings].
3. Uncheck the [Enabled] box for [SOAP].
4. Click [Apply].

Set SNMP

1. Click [Connectivity] on the [Properties] screen.
2. Click [Port Settings].
3. Uncheck the [Enabled] box for [SNMP].
4. Click [Apply].

Set Bonjour

1. Click [Connectivity] on the [Properties] screen.
2. Click [Port Settings]
3. Uncheck the [Enabled] box for [Bonjour].
4. Click [Apply].

Set AirPrint

1. Click [Connectivity] on the [Properties] screen.
2. Click [Protocols]
3. Click [AirPrint]
4. Uncheck the [Enabled] box for [AirPrint].
5. Click [Apply].

Set Mopria

1. Click [Status] on the [Properties] screen.
2. Click [Reboot Device].
3. Log in as system administrator.
4. Click [Properties].
5. Click [Connectivity] on the [Properties] screen.
6. Click [Protocols]
7. Click [Mopria]
8. Uncheck the [Enabled] box for [Mopria].
9. Click [Apply].

Set USB

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

1. Click [Services] on the [Properties] screen.
2. Click [USB]
3. Click [General]
4. Uncheck the [Enabled] box for [Store to USB:] and [Media Print:].
5. Click [Apply].
6. Click [Connectivity] on the [Properties] screen.
7. Click [Port Settings].
8. Uncheck the [Enabled] box for [USB].
9. Click [Apply].

Set CSRF

1. Click [Connectivity] on the [Properties] screen.
2. Click [Protocols]
3. Click [HTTP]
4. Check the [Enabled] box for [CSRF Protection:].
5. Click [Apply].

Set Service Representative Restricted Operation

1. Click [Security] on the [Properties] screen.
2. Click [Service Representative Restricted Operation].
3. Check the [Enabled] box for [Restricted Operation].
4. Enter a passcoge in the [Maintenance Passcode] box.
5. Enter the passcoge in the [Retype Maintenance Passcode] box.
6. Click [Apply].

Set Audit Log

1. Click [Security] on the [Properties] screen.
2. Click [Audit Log].
3. Check the [Enabled] box for [Audit Log].

4. Click [Apply].

Set Embedded Plug-ins

1. Click [Security] on the [Properties] screen.
2. Click [Plug-in Settings] on the [Properties] screen.
3. Click [Embedded Plug-ins].
4. Uncheck the [Enabled] box for [Embedded Plug-ins].
5. Click [Apply].
6. Select [Reboot Now] on the confirmation screen.

Set Upgrades

1. Click [Services] on the [Properties] screen.
2. Click [Device Software].
3. Click [Upgrades].
4. Click [Enabled].
5. Click [Apply].

Set FIPS140 Validation Mode

1. Click [Security] on the [Properties] screen.
2. Click [FIPS140 Validation Mode].
3. Check the [Enabled] box for [FIPS140 Validation Mode].
4. Click [Apply].

Set PostScript passwords

Important:

PostScript password must be set. Otherwise unauthorized users can exploit the user data using PostScript.

1. Make a PostScript file containing the following statement. “new password” must be more than eight characters within 32 characters and including both numeric and alphabetic characters.

```
%!
<</Password (0)
 /SystemParamsPassword (new password)
 /StartJobPassword (new password)
```

>> setsystemparams

2. Specify the file as a print file in “Print” tab of Embedded Web Server, then carry out “Submit Job”.

4. Disabling PJL data read/write commands

To disable data read/write by PJL commands, create PJL command file with contents below and send it as a print job to the device by LPR command or similar.

@PJL JOB PASSWORD=<current password>
@PJL DEFAULT DISKHIDE=ON
@PJL DEAFULT PASSWORD=<new password>
@PJL EOJ

<current password> is not specified by factory default and enter arbitrary string. <new password> must be string of characters (A~Z, a~z, 0~9) with length between 8 and 255.

(Note)
It is necessary to enable LPD port temporally for sending the PJL command file by LPR command from Windows PC. LPD port must be disable through the steps on the page 20.
LPR Port Monitor feature must be enabled when LPR command is sent from Windows PC.
To send PJL command file to the device, execute LPR command on command prompt as follows.

lpr -S "IP address of device" -P lp "PJL command file name"

5. Regular Review by Audit Log

This section describes 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 machine 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 longtime 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

The following describes methods for importing the Audit Log. TLS communication must be enabled to access to 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 "11111" with actual Login ID of system administrator
$USER = "11111"
# Replace "x-admin" with actual Passcode of system administrator
$PASS = "x-admin"

# Replace "127.0.0.1" with actual URL of target device
$Uri = https://127.0.0.1/auditfile.txt

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

```
# Download audit log
$secpasswd = ConvertTo-SecureString $PASS -AsPlainText -Force
$cred = New-Object System.Management.Automation.PSCredential($USER, $secpasswd)
$ProgressPreference = 'SilentlyContinue'
[Net.ServicePointManager]::SecurityProtocol =
[Net.ServicePointManager]::SecurityProtocol -bor
[Net.SecurityProtocolType]::Tls12
Invoke-WebRequest -Uri $Uri -OutFile $DownloadPath -Credential $cred -DisableKeepAlive
```

(Note) 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.

(Note) 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 PowerShell
   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>"

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

   Log ID: Consecutive numbers as an audit log identifier
   Date/Time: The date and time when an event was recorded
   Audit Event ID: The audited event identifier
   Logged Events: Various acts and processing object storing audit log
   User Name: The user name that generated an auditable event
   Description: Description on events
   Status: Status or result of event processing
   Optionally Logged Items: Additional information recorded to audit log (except common record items)

   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 Embedded Web Server)
- User Identification/Authentication (using Printer Driver)
- Use of management functions (using Control Panel)
- Use of management functions (using Embedded Web Server)
- 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 Embedded Web Server)
- Use of Retrieve function (using Embedded Web Server)
- Use of Print function (using Embedded Web Server)
- External Audit Server
- Firmware Update
- PSTN

6. 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 passcode.

1. Enter the "User ID" from keypad.
2. Select [Next] on the touch screen.
3. Enter the "Passcode" from keypad.
4. Select [Enter] 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 "Tools" > "Authentication / Security Settings" > "Authentication" > "Create / View User Accounts" in the User Guide.

   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 "Tools" > "Authentication / Security Settings" > "Authentication" > "Create / View User Accounts" in the User Guide.

   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 machine 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.

7. Self Testing

This section describes the Power on Self Test function.

The machine can execute a Self Test function to verify the integrity of executable code and setting data.

The machine 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, stop using the device and contact our Customer Support Center.

8. Firmware Upgrade

This section describes procedures to upgrade firmware of the device.

Firmware of the device can be upgraded by Embedded Web Server.

Initiate firmware upgrade from Embedded Web Server

Refer to "Preparations for settings on the Embedded Web Server" section for required set up to use Embedded Web Server.

1. Click [Services] on the [Properties] screen.
2. Click [Device Software].
3. Click [Manual Upgrade].
4. Select the file to be imported by clicking [Browse].
5. Click [Install Software].

After several minutes, the following message (A) is displayed on Embedded Web Server.

Updating device software...
The device will reboot itself upon completion of the software installation.
The entire process may take several minutes.
Meanwhile, the Internet communication between this Web User Interface and the device will be lost.

At the same time, if the signature verification of the firmware is successful and the authenticity of the new firmware can be confirmed, the following the message (B) is displayed on the control panel.

Software download in process, please do not interrupt.
An automatic reboot will occur when the download is complete.

After more several minutes, the following message (C) is displayed on the control panel.

Download Mode
PROCESSING

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 is falsified, the message (A) is displayed on Embedded Web Server and the message (B) is displayed on the control panel. After that the message (C) is NOT displayed and the following message (D) is displayed on the control panel.

Download Mode
FILE TRANSFER ERROR 017-759

In this case, reboot the device and check the new firmware to be updated 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.

- 2. Initial Settings Procedures Using Control Panel
  Set Software Download
- 3. Initial Settings Procedures Using Embedded Web Server
  Set Upgrades

9. 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.

Note: 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.

10. Using Private Charge Print from Client PC

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 machine.

(The following explanation is an example of using Windows 10)

1. On the property of the Windows Printer, Click "Accounting" in "Configuration" tab.
2. On "Accounting" tree, select as follows.

   "System": "Local Accounting"
   "Print-Time Prompt": "Always Prompt"

11. Device Digital Certificate Management

You can configure the digital certificate settings of the device using Embedded Web Server. 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

Select the type of certificate to create and then click the [Continue] button.

When [Self-Signed Certificate] is selected, the [Device Digital Certificate Management] (Create Self-Signed Certificate) screen is displayed.

When [Certificate Signing Request (CSR)] is selected, the [Device Digital Certificate Management] (Certificate Signing Request (CSR)) screen is displayed.

Create Self-Signed Certificate

Configure the settings below and click the [Apply] 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
  Select [2,048 Bits] or [3,072 Bits].
- Elliptic Curve
  elect [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 [Apply] button to display the [Device Digital Certificate Management] (Certificate Signing Request (CSR) Details) screen.

- Digital Signature Algorithm
  Select [RSA/SHA-1], [RSA/SHA-256], [RSA/SHA-384], [RSA/SHA-512], [ECDSA/SHA-1], [ECDSA/SHA-256], [ECDSA/SHA-384] or [ECDSA/SHA-512].
- Public Key Size
  Select [2,048 Bits] or [3,072 Bits].
- Elliptic Curve
  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.

Upload Signed Certificate

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

- 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 (●●●).
- Certificate
  Specify the file to import.
  The available formats are X.509(DER/PEM), PKCS#7(DER), and PKCS#12(DER).

12. Authentication for the secure operation

The machine has a unique Authentication feature that restricts the authority to use functions.

This section contains information for System Administrators and general users on the features used to change the settings and on the setting procedures.

Overview of Authentication

Users Controlled by Authentication

The following explains the different user types that are controlled by the Authentication feature.

Users are classified into the following four types. The Authentication feature restricts operations according to the user type.

- Machine Administrator
- Authenticated Users (with System Administrator Privileges)
- Authenticated Users (with no System Administrator Privileges)
- Unauthenticated Users

Machine Administrator

The Machine Administrator uses a special user ID.

Only the Machine Administrator can change the Machine Administrator ID and the Machine Administrator Passcode.

The Machine Administrator is a user who can enter the System Administration mode and change the machine settings that are related to security features and services that are restricted.

To enter the System Administration mode, enter the Machine Administrator ID into the user ID entry field on the authentication screen.

Authenticated Users (with System Administrator Privileges)

These are users to whom the System Administrator privileges are granted.

When a restricted service is used, this type of user must enter his/her user ID on the authentication screen.

This type of user has the same privileges as those of the Machine Administrator in operating the machine, except the following:

- Operating Folder
- Changing the passcode of the Machine Administrator.

Authenticated Users (with No System Administrator Privileges)

These are users who are registered on the machine or the remote server, and to whom System Administrator privileges are not granted.

When a restricted service is used, this type of user must enter his/her user ID on the authentication screen.

Unauthenticated Users

These are users who are not registered with the machine.

An Unauthenticated User cannot use services that are restricted.

Local Machine Authentication (Login to Local Accounts)

Local machine authentication uses the user information that is registered on the machine to manage authentication.

The print data that are sent from a computer can be received on the machine after a user is authenticated by the cross-checking of the authentication information that is pre-configured on a client's driver with the registered authentication information on the machine.

For more information on the configuring of a driver, refer to the online help provided for the driver.

Remote Authentication (Login to Remote Accounts)

Remote authentication uses a remote authentication server (LDAP or Kerberos Server) and authenticates users based on the user information managed on the server. User information cannot be registered on the machine.

Functions Controlled by Authentication

The following explains the functions that are restricted by the Authentication feature. The restriction depends on which method is selected from the following:

- Local Access
- Remote Access

For more information on the restrictions on the operations on Folder using the Authentication feature, refer to "Authentication for Folder".

Local Access

Direct operation of the machine from the control panel is called Local Access. The functions restricted by Local Access are as follows.

Device Access

- All Services Pathway - verifies users when users access a service screen.
- Job Status Pathway - verifies users when users access the Job Status screen.
- Machine Status Pathway - verifies users when users access the Machine Status screen.

Service Access

- Copy
- Scan to Folder
- E-mail
- Network Scanning
- Scan to PC
- Send from Folder
- Print

Feature Access

- Print File from Folder
- Retrieve File from Folder

Service Access control per user

- Service access and print & copy quota can be controlled per user.

The system administrator can limit print & copy quota per user via the control panel and Embedded Web Server.

When print or copy volume exceeds the registered number, the user cannot use the function. The counted number needs to be cleared by system administrator.

Remote Access

Operation of the machine through a network using Embedded Web Server is called Remote Access.

The functions restricted by Remote Access are as follows.

Print

Printing is limited to the print jobs sent from a computer.

To use the Accounting feature, use the print driver to set account information such as user ID and passcode.

If verification using account information fails for a print job, the print data will be either saved in the machine or deleted depending on the Charge Print settings.

Embedded Web Server

If the Authentication feature is enabled, authentication is required to access the Embedded Web Server home page even if you are not using the Authentication feature for any service.

Authentication for Folder

The following explains the restricted operations on Folders when the Authentication feature is enabled.

Note:

When a user account is deleted, the Folder associated with the account are also deleted. Any files stored in the Folder will also be deleted.

Authenticated Users who are given the System Administrator privileges do not have the privileged level of access to Folder.

Types of Folder

The following two types of Folder can be used with the machine.

Machine Administrator Shared Folder

The Machine Administrator Shared Folder is a Folder created by a Machine Administrator. When the Authentication feature is enabled, all Authenticated Users can share this Folder.

Only the Machine Administrator can change the settings.

To create a Machine Administrator Shared Folder, operate the machine as a Machine Administrator.

Personal Folder

This is a Folder created by an Authenticated User by using the Authentication feature. Only the Authenticated User who created the Folder can use it.

Operations available for Folder

The following table shows whether each operation on each Folder is available for each user type when the Authentication feature is enabled.

Folder Operation	System Administrator and Authenticated Users		
	Machine Administrator Shared Folder	Personal Folder (owner)	Personal Folder (other)
Create	-	✓	-
Display	✓	✓	-
Delete	✓	✓	-
Change Settings	-	✓	-
Display File	✓	✓	-

Delete File	✓	✓	-
Store File	✓	✓	-
Print File	✓	✓	-

Folder Operation	Machine Administrator	
	Machine Administrator Shared Folder	Personal Folder
Create	✓	-
Display	✓	✓
Delete	✓	✓
Change Settings	✓	✓
Display File	✓	✓
Delete File	✓	✓
Store File	✓	✓
Print File	✓	✓

✓ : Operation available

- : Operation not available

Maximum Login Attempts

This feature protects the settings from being changed by someone impersonating an authenticated user. If authentication for a user's ID fails more than specified times continuously, access is denied. The login attempt count is applied to the attempts from the control panel, EWS, the printer client and the audit server.

You can specify a login attempt count from 1 to 10.

Note:

- The failure count is reset when the machine is restarted.
- To cancel the access rejection state, restart the machine by switching off and on the power.

13. Operation Using Control Panel

This section describes the operation using control panel to use security features for System Administrator and authenticated users.

User Authentication

Before using all services and configuring settings, a user must be authenticated with an ID and a passcode.

1. Press the <Log In/Out> button on the control panel.
2. Enter the "User ID" from keypad.
3. Select [Next Input] on the touch screen.
4. Enter the "Passcode" from keyboard.
5. Select [Enter] on the touch screen.

All features on the control panel become available.

Important:

When another user interrupt and uses the machine by using the interrupt mode, the user needs to logout before canceling the interrupt mode.

Example:
User A is authenticated > interrupt mode > User B login > job complete > User B logout > cancel the interrupt mode

Note:

Before entering the user ID and the password, select "Registered User" or "System Administrator" when remote authentication is used.

Only the Machine Administrator's ID (default: "admin") is pre-registered in the machine, but other user IDs are not.

In a remote authentication server, on the other hand, the Machine Administrator's ID is not pre-registered.

Although "admin" can be registered as a user ID, it cannot be registered as the Machine Administrator's ID in the machine.

Create/View User Accounts

This feature allows you to register user account information, such as User IDs, user names and passcodes, and to restrict the numbers of copied, printed, and scanned pages for each user. Up to 1,000 users can be registered.

On the Tools screen

1. Select [Authentication] under [Authentication / Security Settings].
2. Select [Create/View User Accounts] under [Authentication].
3. Select a User ID number.

4. Press [Create/Delete].
5. When a new user account is to be created, a keyboard screen is displayed. Enter a user ID, and then select [Save].
6. Configure the required settings.
7. Select [Close].

User ID

Allows you to enter a User ID using the screen keyboard. You can enter up to 32 alphanumeric characters including spaces as a User ID.

User Name

Allows you to enter a user name using the screen keyboard. You can enter up to 32 alphanumeric characters including spaces as a user name.

Passcode

Allows you to enter a passcode using the screen keyboard. You can enter 4 to 12 alphanumeric characters.

Note:

The [Passcode] button appears when you have chosen the use of a passcode and you have enabled [Local Accounts] in [Authentication/Security Settings].

E-mail Address

Allows you to enter the e-mail address. The specified address that is displayed on the [E-mail] screen is set as the sender's address of the machine. You can enter up to 128 characters.

Note:

The [E-mail Address] button appears when you have enabled [Local Accounts] in [Authentication/Security Settings].

Device Access

Displays the [No. XXXX - Device Access] screen. Select [Enabled] or [Disabled] to specify feature access permissions.

Service Access

Displays the [No. XXXX - Service Access] screen. Select [Copy Service], [Fax Service], [Scan Service] or [Print Service] to specify feature access permissions and account limits for that service.

Feature Access - Displays the [Account No. XXXX - {Service} - Feature Access] screen. Select the access permissions for each service for that account.

Change Account Limit - Displays the [Account No. XXXX - {Service} Limit] screen. Enter an account limit for [Color] and [Black] to specify the maximum number of pages allowed to be processed by that account. The maximum number of pages that can be entered is 9,999,999.

User Role

Allows you to select the privileges that are given to the user. Select from [User], [System Administrator] or [Account Administrator].

Note:

The [User Role] button appears when you have enabled [Local Accounts] in [Authentication/Security Settings].

Reset Total Impressions

Deletes all the data tracked for the selected account.

Reset Account

Clears all settings and data for the selected account.

Change User Passcode by General User

This feature allows Authenticated Users (users who are authenticated by the procedure described in "User Authentication") to change the registered passcode.

This feature is only applicable to Local Authentication mode.

On the Tools screen

1. Select [User Details Setup].
2. Select [Change Passcode].
3. Enter the current passcode and select [Next].
4. On the [Change Passcode] screen, select [Keyboard].
5. Enter a new passcode of 9 or more characters in [New Passcode] and select [Next].
6. In [Retype Passcode], select [Keyboard].
7. Enter the same passcode and select [Save] twice.

Job Deletion by System Administrator

This feature allows only system administrators to delete the active jobs.

Deleting the Copy, Scan job

1. Press the red [Stop] button on the control panel.
2. On the touch screen, touch [Resume] to continue the job, or touch [Cancel] to cancel the job completely.

Deleting the printing Job

1. On the control panel, press [Job Status] button. The Active Jobs tab displays.
2. Touch the desired job, then press [Delete] from the pop-up menu.
3. A confirmation window appears. Select [Delete job] to cancel the job completely.

Deleting the sending Scan Job

1. On the control panel, press [Job Status] button. The Active Jobs tab displays.
2. Touch the desired job, then press [Delete] from the pop-up menu.

Folder / Stored File Settings

This section describes the features that allow a System Administrator to configure various settings for Folder that is created for saving confidential scanned files.

Folder Service Settings

This feature allows you to specify whether to discard files once received from a client.

1. Select [Folder Service Settings] under [System Settings].
2. Change the required settings.
3. Select [Close].

Files Retrieved By Client

Specifies when and how to delete files in Folder after they are retrieved.

Print & Delete Confirmation Screen

Specifies whether to display a confirmation message screen when deleting a file.

Quality/File Size for Retrieval

Specifies the Quality/File Size level.

Stored File Settings

This feature allows you to select whether the files stored in a Folder are automatically deleted. You can set how long files are kept and when they are deleted.

You can also select whether to delete individual files.

1. Select [Stored File Settings] under [System Settings].
2. Change the required settings.
3. Select [Close].

Expiration Date for Files in Folder

Specifies whether to delete files from Folder when the specified period elapses. Enter the number of days to store files within the range from 1 to 14 days, and enter the time when files are to be deleted using the scroll buttons or the numeric keypad.

Stored Job Expiration Date

Specifies the retention period for a stored file. Selecting [On] allows you to specify a retention period within the range from 4 to 23 hours, in 1 hour increments.

Note:

If the machine is turned off before the specified period elapses, the stored file will be deleted when the machine is turned back on.

Print Order for All Selected Files

Specifies the print order for a stored file from the following menu.

- Date & Time Oldest File
- Date & Time Newest File
- File Name Ascending
- File Name Descending

Create Folder

This feature allows users to create Folder for saving confidential scanned files. Scanned files in Folder can be imported to computers.

1. Select [Create Folder] on the [Setup Menu] screen.
2. Select a Folder number to create a new Folder.
3. Select [Create/Delete].
4. Select [Off] for [Check Folder Passcode].
5. Change the required settings.
6. Select [Close].

Note:

By selecting [Delete Folder], you can delete all files in the Folder.

Folder Name

Specifies the Folder name. Enter a name (up to 20 characters) to be assigned to the Folder.

Delete Files after Retrieval

Specifies whether to delete files in the Folder after they are printed out or retrieved,.

Delete Expired Files

Specifies whether to delete files in the Folder after the preset time or period elapses.

Send from Folder

1. This section describes the Folder features that allow you to check, print, or delete files in the private Folder that is displayed on the [Send from Folder] screen.

However, some Folders may require you to enter a passcode, depending on the operation you attempt. Private Folders created by other users are inactive and inaccessible to you.

2. Press the <Services Home> button on the control panel.
3. Select [Send from Folder] on the touch screen.
1. Select the [Folder name] to be displayed on the screen.
2. Select the Folder to be opened. Then the files stored in the Folder appear.

File Name/ Date & Time

Sorts the files by their names or by the dates they were stored. You can change the sorting order of the list by selecting the same option again. The order is indicated with an upward (ascending order) or downward (descending order) triangle shown to the right of the name of the option selected.

Refresh

Updates the list of files in the Folder.

Select All Files

Selects all the files in the Folder so that you can print or delete them all at once.

Print

Prints the selected file(s).

Delete

Deletes the selected file(s).

Private Charge Print

The Private Charge Print feature temporarily stores files per user ID until a user logs in and manually prints them from the machine's control panel.

This feature only displays files of a logged-in user and thus provides security and privacy of files stored in the machine.

1. Press the <Job Status> button on the control panel.
2. Select [Private Charge Print] on the [Secure Print Jobs & More] screen.

Note:

If you enter the screen with System Administrator's ID, a list of authentication user IDs is displayed. Select a user ID from the list or enter the displayed number in [Go to] and select [Job List]. Then, the files stored for the selected user ID are displayed.

3. Select a file to be printed or deleted.
4. Select the required option.

Refresh

Refreshes the displayed information.

Select All

Selects all the files in the list.

Delete

Deletes a file selected in the list.

Print

Prints a file selected in the list. After being printed, the file is deleted.

Note:

The displayed jobs are sent from a PC via the print driver. For more information, refer to Print Driver Online Help.

14. Operation Using Embedded Web Server

This section describes the operation using Embedded Web Server to use security features for System Administrator and authenticated users.

The Embedded Web Server program uses the embedded Web User Interface which enables communication between a networked computer and the machine via HTTP. Embedded Web Server can be used to check each job and the machine status, or to change the network settings.

Note:

This service must be installed and set up by the System Administrator prior to use. For more information on the installation and setups of the Embedded Web Server feature, refer to the System Administration Guide. Some of the Embedded Web Server features have restricted access. Contact a System Administrator for further assistance.

Accessing Embedded Web Server

Follow the steps below to access Embedded Web Server. On a client computer on the network, launch an internet browser.

In the URL field, enter "http://" followed by the IP address or the Internet address of the machine. Then, press the <Enter> key on the keyboard.

For example, if the Internet address (URL) is vvv.xxx.yyy.zzz, enter it in the URL field as shown below:

http://vvv.xxx.yyy.zzz

The IP address can be entered in either IPv4 or IPv6 format. Enclose the IPv6 address in square brackets.

IPv4: http://xxx.xxx.xxx.xxx

IPv6: http://[xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx]

If a port number is set, append it to the IP address or the Internet address as follows. In the following example, the port number is 80.

URL: http://vvv.xxx.yyy.zzz:80

IPv4: http://xxx.xxx.xxx.xxx:80

IPv6: http://[xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx]:80

The home page of Embedded Web Server is displayed.

Note:

When the Authentication feature is enabled, you are required to enter your user ID and your password. You need to enter your user ID and your password to access Embedded Web Server to configure and use the security functions of the machine.

When your access to Embedded Web Server is encrypted, enter "https://" followed by the IP address or the Internet address, instead of "http://".

Print

This section describes how to specify printing and paper parameters, enter accounting information, and select the delivery method for your print job.

Follow the steps below to select the features available on the [Print] tab.

1. Click [Print] on the Main Panel of the home page.
2. The [Job Submission] page is displayed.
3. Job Submission allows you to print the files stored in your computer. Specify the following settings and click [Start] to submit the job.

Feature		Setting items
Print	Quantity	Enter the number of sets to print. You can enter a number between 1 and 999.
	Collated	Specify whether to collate printouts or not.
	2-Sided Printing	Allows you to select from 1 sided prints or 2 sided prints (head to head or head to toe).
	Staple	Allows you to select the position for stapling from the drop-down menu.
	Hole Punch	Allows you to select the position for punching from the drop-down menu.
	Output Destination	Allows you to select output trays from the drop-down menu.
Paper	Paper Supply	Allows you to select the paper tray from the drop-down menu.
	Paper Size	Allows you to select the output paper size.
	Paper Type	Allows you to select the type of the paper to be used.
Delivery	Immediate Print	In the case of user authentication mode, regardless of these settings, print data will be stored to the authenticated user's private charge print.
	Sample Set	
	Delayed Print	
	Secure Print	
File Name		Allows you to specify the file to be printed. If you click the [Browse] button next to the [File Name] edit box, the [Choose File] dialog box opens, and you can select the file to be printed. You can print only files with the following extensions: .pdf, .tif, .jpg, and .xps.
Submit Job		Click this button to print the file.

Scan (Folder Operation)

This section describes how to configure Folder.

Follow the steps below to select the features available on the [Scan] tab.

1. Click [Scan] on the Main Panel of the home page.
2. Select [Folder] on the [Scan] screen.
3. The [Folder] page is displayed.

Folder icons

If you click the icon of a registered Folder, the [Folder: List of Files] page for the Folder is displayed.

Folder Number

Displays the Folder numbers. If you click the number of a registered Folder, the [Folder: List of Files] page for the Folder is displayed.

Folder Name

Displays the names of Folders. If you click the name of a registered Folder, the [Folder: List of Files] page for the Folder is displayed.

Number of Files in this Folder

Displays the number of files stored in each Folder.

File List

If you click [File List], the [Folder: List of Files] page for the selected Folder is displayed.

Delete

If you click [Delete], the selected Folder is displayed.

Edit

If you click [Edit], the [Edit Folder] page for the selected Folder is displayed.

Create

If you click [Create], the [Folder Setup] page for the selected Folder is displayed.

Folder: List of Files

The following table shows the setting items available on the [Folder: List of Files] page.

Item	Description
Folder Number	Displays the Folder number of the selected Folder.
Folder Name	Displays the name of the selected Folder.

File Number		Displays the file numbers of the files stored in the
File Name		Displays the names of the files.
Date & Time		Displays the dates on which the files were stored.
Compression Format		Displays the compression formats of the files.
Page Count		Displays the page counts of the files.
Type		Displays the job types of the files.
Retrieve	Retrieve Page	Selects whether or not to retrieve one page of the selected file.
	Page Number	Enters the page number of the page to be retrieved.
	Retrieving Format	Specifies the file format to be used when retrieving the page.
	Add Thumbnail	Selects whether or not to add a thumbnail.
Print File	Paper Supply	Selects the paper tray to be used to print the selected
	Output Destination	Selects the output tray.
	Quantity	Selects the number of copies to print.
	2-Sided Printing	Selects whether to print only on one side or both sides of
	Staple	Allows you to select the position for stapling from the drop-down menu.
	Hole Punch	Allows you to select the position for punching from the drop-down menu.
	Batch Print	Allows you to set batch printing.
Delete		Deletes the selected files in the folder.

Edit Folder

The following table shows the setting items available on the [Edit Folder] page.

Item		Description
Folder	Folder Number	Displays the number of the selected Folder.
	Folder Name	To change the Folder name, enter a new Folder name.
	Folder Passcode	To change the passcode, enter a new passcode with up to 20 characters. Leave the text box blank if you do not set a passcode.
	Retype Passcode	Re-type the passcode for verification.
	Check Folder Passcode	Allows you to select whether and when the passcode for the Folder is required.
	Owner	Displays the owner of the Folder. If the Folder is a shared
	Delete Files after Print or Retrieve	Allows you to set whether to automatically delete files after they are printed. Note: Retrieved files are not deleted.
	Delete Expired Files	Allows you to set whether to automatically delete files when they reach the specified expiration dates.

	Number of Files in this Folder	Displays the number of files stored in the Folder.

Folder Setup

The following table shows the setting items available on the [Create] page.

Item		Description
Folder	Folder Number	Displays the number of the selected Folder.
	Folder Name	Enter the name of the Folder.
	Folder Passcode	Enter a new passcode with up to 20 characters. Leave the text box blank if you do not set a passcode.
	Retype Passcode	Re-type the passcode for verification.
	Check Folder Passcode	Allows you to select whether and when the passcode for the Folder is required.
	Delete Files after Print or Retrieve	Allows you to set whether to automatically delete files after they are printed. Note: Retrieved files are not deleted.
	Delete Expired Files	Allows you to set whether to automatically delete files when they reach the specified expiration dates.

Import the files

The following describes methods for importing files that are stored on the machine's Folder. Select [Folder Number] or [Folder: List of Files] on the [Folder] page.

Place a check next to each file to be imported and click [Retrieve] or [Print File].

Note:

To retrieve a color file as a JPEG, place a check next to [Retrieve Page], and specify the page number.

Printing Job Deletion

This page allows only System Administrators to delete the active print jobs.

1. Click [Jobs] tab on the Main Panel of the home page.
2. Select the desired job on the [Active Jobs] screen.
3. Click the [Delete] button.
4. A confirmation window appears. Select [OK] to cancel the job completely.

Change User Passcode by System Administrator (Using Embedded Web Server)

This feature is only applicable to Local Authentication mode.

1. Open your Web browser, enter the TCP/IP address of the machine in the Address or Location field, and press the <Enter> key.
2. Enter System Administrator's ID and the passcode if prompted.
3. Click the [Properties] tab.
4. Click [Security].
5. Click [Authentication Configuration].
6. Click [Next].
7. Enter the user number in [Account Number] and click [Edit].
8. Enter a new passcode of 9 or more characters in [Passcode].
9. Enter the same passcode in [Retype Passcode] and click [Apply].

15. Problem Solving

This section describes solutions to problems that you may come across while using the machine and Embedded Web Server. The machine has certain built-in diagnostic capabilities to help you identify problems and faults and displays error messages on the control panel and web browser, whenever problems or conflicts occur.

Fault Clearance Procedure

If a fault or a problem occurs, there are several ways in which you can identify the type of the fault. Once a fault or a problem is identified, specify the probable cause, and then apply the appropriate solution.

- If a fault occurs, first refer to the screen messages and animated graphics to clear the fault according to the specified order.
- Also refer to the fault codes displayed on the touch screen in the Machine Status mode. Refer to the Fault Codes table below for an explanation of some fault codes and corresponding corrective actions.
- When you have problems in fixing the fault, contact a System Administrator for assistance.
- In some cases, the machine may need to be turned off and then on.

Caution:

If you do not leave at least 20 seconds between a power off and a power on, the hard disk in the machine may be damaged.

You should call for service representative if the problem persists or a message indicates so.

Note:

Even when the power of the machine fails, all the queued jobs will be saved because the machine is equipped with the hard disk drive. The machine will resume processing the queued jobs when the power of the machine is turned back on.

Fault Codes

This section explains error codes.

If a printing job ends abnormally due to an error, or a malfunction occurs in the machine, an error message code (***-***) is displayed.

Refer to error coded in the following table to rectify problems.

Important:

If an error code is displayed, any print data remaining on the machine and information stored in the machine's memory are not warranted.

If an error code that is not listed in the following table is displayed, or if an error persists after you follow the listed solution, contact our Customer Support Center. The contact number is printed on the label or the card attached on the machine.

Error 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 machine power, make sure that the touch screen is blank, and then switch on the machine power. If the error still is not resolved, contact our Customer Support Center.
016-402	[Cause] The authentication connection timed out. [Remedy] Confirm the network connection and switch setting of the authentication device physically connected to the machine via a network, and check whether it is connected to the machine correctly.
016-403	[Cause] The root certificate did not match. [Remedy] Confirm the authentication server and store the root certificate of the server certificate of the authentication server into the machine. If you cannot acquire the root certificate of the server certificate, set [Server Certificate Verification] of [IEEE 802.1x Settings] to [Disabled] on the touch screen.
016-405	[Cause] An error occurred in the certificate stored in the machine. [Remedy] Initialize the certificate.
016-406	[Cause] An error occurred in the SSL client certificate. [Remedy] Take one of the following measures: Store an SSL client certificate in the machine, and set it as the SSL client certificate. If the SSL client certificate cannot be set, select an authentication method other than SSL.
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 the Embedded Web Server if the SMTP server settings are correct. Also, check the DNS server settings.
016-504	[Cause] Unable to resolve the POP3 server name when sending email. [Remedy] Check on Embedded Web Server if the POP3 server settings are correct. Also, check the DNS server settings. are correct.
016-505	[Cause] Unable to login to the POP3 server when sending e-mail. [Remedy] Check on Embedded Web Server if the user name and password used in the POP3 server are correct.
016-513	[Cause] An error occurred in connecting to the SMTP server. [Remedy] The SMTP server or network may be overloaded. Wait for a while, and then execute the operation again.
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 machine.

016-523	[Cause] LDAP server SSL authentication error. The server certificate data is incorrect. [Remedy] The machine cannot trust the SSL certificate of the LDAP server. Register the root certificate for the LDAP server's SSL certificate to the machine.
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 machine; 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 machine; however, note that selecting this option does not ensure the validity of the LDAP server.
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 machine 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 machine; 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.
016-533	[Cause] Kerberos server authentication protocol error [Remedy] The time difference between the machine and the Kerberos server exceeded the clock skew limit value set on the Kerberos server. Check whether the clocks on the machine and Kerberos server are correctly set. Also check whether the summer time and the time zone are correctly set on the machine and Kerberos server.
016-534	[Cause] Kerberos server authentication protocol error [Remedy] The domain set on the machine does not exist on the Kerberos server, or the Kerberos server address set on the machine is invalid for connection. Check whether the domain name and the server address have been correctly set on the machine. For connection to Microsoft® Windows Server® 2003 or Microsoft® Windows Server® 2008, specify the domain name in uppercase.
016-539	[Cause] Kerberos server authentication protocol error [Remedy] An error occurred in the software. Contact our Customer Support Center.
016-574	[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because the host or server name of the FTP server could not be resolved. [Remedy] Check the connection to the DNS server. Check if the FTP server name is registered correctly on the DNS server.
016-575	[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because the DNS server address was not registered. [Remedy] Specify the correct DNS server address. Or, specify the destination FTP server using its IP address.
016-576	[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because it could not connect to the FTP server. [Remedy] Ensure that both the destination FTP server and the machine are available for network communications, by checking the following: The IP address of the server is set correctly. The network cables are plugged in securely.

016-577	[Cause] Unable to connect to the FTP service of the destination server. [Remedy] Take one of the following actions: Check if the FTP service of the server is activated. Check if the FTP port number of the server is correctly registered on the machine.
016-578	[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature due to unsuccessful login to the FTP server. [Remedy] Check if the login name (user name and password are correct.
016-579	[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because the scanned image could not be saved in the FTP server after connection. [Remedy] Check if the FTP server's save location is correct.
016-580	[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because the file or folder name on the FTP server could not be retrieved after connection. [Remedy] Check the access privilege to the FTP server.
016-581	[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because the suffix of the file or folder name exceeded the limit after connection. [Remedy] Change the file name, or change the destination folder on the FTP server. Or, move or delete files from the destination folder.
016-582	[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because file creation was not successful on the FTP server after connection. [Remedy] Take one of the following actions: Check if the specified file name can be used in the save location. Check if enough space is available in the save location.
016-583	[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because lock folder creation was not successful on the FTP server after connection. [Remedy] Take one of the following actions: If any lock directory (.LCK) exists in the forwarding destination, delete it manually, then try executing the job again. Check if the specified folder name can be used in the save location. Check if the same folder name exists in the save location. Check if enough space is available in the save location.
016-584	[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because folder creation was not successful on the FTP server after connection. [Remedy] Take one of the following actions: Check if the specified folder name can be used in the save location. Check if the same folder name exists in the save location. Check if enough space is available in the save location.
016-585	[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because file deletion was not successful on the FTP server after connection. [Remedy] Check the access privilege to the FTP server.
016-586	[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because lock folder deletion was not successful on the FTP server after connection. [Remedy] Take one of the following actions: Check the access privilege to the FTP server. If any lock directory (.LCK) exists in the forwarding destination, delete it manually, then retry executing the job.
016-587	[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because folder deletion was not successful on the FTP server after connection. [Remedy] Check the access privilege to the FTP server.

016-588	[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because the data could not be written in the FTP server after connection. [Remedy] Check if enough space is available in the save location.
016-589	[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because the data could not be read from the FTP server after connection. [Remedy] Check the access privilege to the FTP server.
016-593	[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because an internal error occurred after connection to the FTP server. [Remedy] Try again. If the error persists, contact our Customer Support Center.
016-594 016-595 016-596	[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because a network error occurred. [Remedy] Try again. If the error persists, contact our Customer Support Center.
016-703	[Cause] The machine received e-mail which specified 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 hard disk capacity is insufficient. [Remedy] Delete unnecessary files from the folder, and save the file.
016-705	[Cause] Secure print documents cannot be registered because of hard disk malfunction. [Remedy]Contact the Customer Support Center. Refer to Secure Print.
016-706	[Cause] The hard disk space is insufficient because the number of Secure Print users exceeded the maximum limit. [Remedy] Delete unnecessary files from the machine, 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 machine's mail address is incorrect. [Remedy] Confirm the machine's mail address.

016-769	[Cause] The SMTP server does not support delivery receipts (DSN). [Remedy] Send e-mail without setting delivery receipts (DSN).
016-773	[Cause] The IP address of the machine is not set correctly. [Remedy] Check the DHCP settings. Or set the fixed IP address to the machine.
016-774	[Cause] Unable to process compression conversion because of insufficient hard disk space. [Remedy] Delete unnecessary data from the hard disk to free up disk space.
016-781	[Cause] Unable to connect to the SMTP server. Unable to establish a connection between the machine and the server. Although the connection between the machine and the server has been established, ASCII characters are not used for the host name specified on the machine. [Remedy] Take one of the following measures: Check whether the network cables are plugged in securely. Enter the host name using ASCII characters in [Tools] > [Connectivity & Network Setup] > [Machine's E-mail Address/Host Name].
016-788	[Cause] Failed to retrieve a file from the Web browser. [Remedy] Take one of the following measures, and then execute the operation again: Reload the browser page. Restart the browser. Switch off the machine power, make sure that the touch screen is blank, and then switch on the machine power.
016-791	[Cause] Failed to access to the destination computer or the save location for Network Scanning. [Remedy] Check the directory configuration and files on the server, the access privileges for the destination or the location, and check if you are authorized to access the specified destination computer or server.
018-400	[Cause] When IPSec is enabled, there is an inconsistency in IPSec settings as follows: The password is not set when [Authentication Method] is set to [Preshared Key]. An IPSec certificate is not set when [Authentication Method] is set to [Digital Signature]. [Remedy]Check the IPSec settings, and enable IPSec again: When [Authentication Method] is set to [Preshared Key], set the password. When [Authentication Method] is set to [Digital Signature], set an IPSec certificate.
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.
018-502	[Cause] The machine failed to transfer data using SMB of the Scan to PC service because computers allowed to login are restricted. [Remedy] Confirm the property information for the specified user, and check whether the computers allowed to login to the server are restricted.
018-505	[Cause] Failed to log into the destination computer while transferring data using SMB of the Scan to PC service. [Remedy] Check whether the user name and password of the SMTP server registered in the machine is correct.

018-543	[Cause] The machine failed to transfer data using SMB of the Scan to PC service because one of the following problems occurred on the shared name of the SMB server when logging in to the SMB server: The specified shared name does not exist on the server. Invalid characters are used in the specified shared name. When the server is Macintosh, the specified shared name may not have an access right. [Remedy] Confirm the specified shared name, and set the name correctly.
018-547	[Cause] The machine failed to transfer data using SMB of the Scan to PC service because the number of users logging into the SMB server exceeded the limit when logging in to the SMB server. [Remedy] Take one of the following measures: Confirm how many users can access the shared folder. Check whether the number of login users have exceeded the limit.
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].
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 returned 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 machine 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 machine's e-mail address when sending e-mail. [Remedy] Import the S/MIME certificate corresponding to the mail address to the machine.

027-707	[Cause] The S/MIME certificate associated with the machine's email address has expired. [Remedy] Ask the sender to issue a new S/MIME certificate and import the certificate to the machine.
027-708	[Cause] The S/MIME certificate associated with the machine's email address is not reliable. [Remedy] Import a reliable S/MIME certificate to the machine.
027-709	[Cause] The S/MIME certificate associated with the machine's email address has been discarded. [Remedy] Import a new S/MIME certificate to the machine.
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.
027-711	[Cause] No S/MIME certificate was obtained from the received e-mail. [Remedy] Import the sender's S/MIME certificate to the machine, or attach an S/MIME certificate to S/MIME signature mail sent from the sender.
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.
027-713	[Cause] The received e-mail has been discarded because it might be altered on its transmission route. [Remedy] Tell the sender about it, and ask to send the e-mail again.
027-714	[Cause] The received e-mail has been discarded because the address in its From field was not the same as the mail address in the S/MIME signature mail. [Remedy] Tell the sender that the mail addresses are not identical, and ask to send the e-mail again.
027-715	[Cause] The received S/MIME certificate has not been registered on the machine, or has not been set to use on the machine. [Remedy] Import the sender's S/MIME certificate to the machine, or change settings to use the S/MIME certificate on the machine when 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.
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.

16. Security @ Xerox

For the latest information on security and operation concerning your device, see the Xerox® Security Information website located at http://www.xerox.com/information-security/.

17. 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.

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 Embedded Web Server, and Audit Server)	Login/Logout	Login	Failed Web User Interface
Unsuccessful User authentication Unsuccessful User identification (using Printer Driver)	Job Status	Print	Aborted
	Device Settings	View Security Setting	Successful

Use of management functions		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)	Communication	Trusted Communication	Failed (Include the protocol, the destination, the reason of failure)

18. Appendix

List of Operation Procedures

Item	Using Control Panel	Using Embedded Web Server	Default
Check the Clock	[System Settings] > [Common Service Settings] > [Device Clock/Timers].	-	-
Use Passcode Entry from Control Panel	[Authentication/Security] > [Authentication] > [Passcode Policy] > [Passcode Entry from Control Panel]	-	Off
Set Overwrite Hard Disk	[Authentication/Security Settings] > [Overwrite Hard Disk]	[Properties] > [Security] > [On Demand Overwrite] > [Immediate] > [Number of Overwrites]	1
Set Data Encryption	[System Settings] > [Common Service Settings] > [Other Settings] > [Data Encryption]	-	-
Set Authentication	[Authentication/Security Settings] > [Authentication] > [Login Type]. [System Settings] > [Connectivity & Network Setup] > [Remote Authentication/Directory Service]	[Security] > [Authentication Configuration]	Off
Set Private Print	[Authentication/Security Settings] > [Authentication] > [Charge/Private Print Settings].	-	-
Set Auto Clear	[System Settings]>[Common Service Settings] > [Device Clock/Timers] > [Auto Clear]	-	60
Set Repot Print	[System Settings] > [Common Service Settings] > [Reports] > [Print Reports Button]	-	-
Set Self Test	[System Settings] > [Common Service Settings] > [Maintenance] > [Power on Self Test]	-	-
Set Software Download	[System Settings] > [Common Service Settings] > [Other Settings] > [Software Download].	[Properties] > [Services] > [Device Software] > [Upgrades]	On
Set Upgrades	-	[Properties] > [Services] > [Device Software] > [Upgrades]	On
Manual Upgrade	-	[Properties] > [Services] > [Device Software] > [Manual Upgrade]	-
Change the System Administrator Passcode	[Authentication/Security Settings] > [System Administrator Settings] > [System Administrator's Passcode]	[Security] > [System Administrator Settings]	-
Set Maximum Login Attempts	[Authentication/Security Settings] > [Authentication > [Invalid Login Settings]	[Security] > [User Details Setup] > [Login Attempts Limit]	5
Set Scheduled Image Overwrite	[Authentication/Security Settings] > [Overwrite Hard Disk] > [Scheduled Image Overwrite].	[Security] > [On Demand Overwrite] > [Scheduled]	Off
Run Image Overwrite	[Authentication/Security Settings] > [Overwrite Hard Disk] > [Run Image Overwrite]	[Security] > [On Demand Overwrite] > [Manual]	-

Set Access Control	[Authentication/Security Settings] > [Authentication] > [Access Control]	[Security] > [Authentication Configuration] > [Next]> [Device Access] or [Service Access]	Off
Set User Passcode Minimum Length	[Authentication/Security Settings] > [Authentication] > [Passcode Policy] > [Minimum Passcode Length]	[Security] > [User Details Setup] > [Minimum Passcode Length]	0
Set SMB	[System Settings] > [Connectivity & Network Setup] > [Port Setting]	[Connectivity] > [Port Setting]	On
Set WebDAV	[System Settings] > [Connectivity & Network Setup] > [Port Setting]	[Connectivity] > [Port Setting]	On
Set Receive E-mail	[Connectivity & Network Setup] > [Port Setting]	[Connectivity] > [Port Setting]	Off
Set IPP	[System Settings] > [Connectivity & Network Setup] > [Port Setting]	[Connectivity] > [Port Setting]	On
Set SSL/TSL	[System Settings] > [Connectivity & Network Setup] > [Security Settings] > [SSL/TLS Settings]	[Security] > [SSL/TLS Settings]	Off
Set Service Representative Restricted Operation	[System Settings] > [Common Service Settings] > [Other Settings] > [Service Rep. Restricted Operation].	[Security] > [Service Representative Restricted Operation]	Off
Set Browser Refresh	-	[General Setup] > [Internet Services Settings] > [Auto Refresh Interval]	On
Set Audit Log, Import the Audit LogFile	-	[Security] > [Audit Log].	Off
Configuring Device Certificates	-	[Security] > [Device Digital Certificate Management] > [Upload Signed Certificate].	-
Set IPSec	[System Settings] > [Connectivity & Network Setup] > [Security Settings] > [IPSec Settings]	[Security] > [IPSec]	Off
Set SNMP	[System Settings] > [Connectivity & Network Setup] > [Port Setting]	[Connectivity] > [Port Settings]	Off
Set S/MIME	[System Settings] > [Connectivity & Network Setup] > [Security Settings] > [S/MIME Settings]	[Security] > [SSL/TLS Settings] > [S/MIME Communication]	Off
Set USB	-	[Service] > [USB] > [General]	On
Set Bonjour	[System Settings] > [Connectivity & Network Setup] > [Port Setting]	[Connectivity] > [Port Settings]	On
Set CSRF	-	[Connectivity & Network Setup] > [Protocol] > [HTTP]	Off
Set FIPS140 Validation Mode	-	[Security] > [Set FIPS140 Validation Mode].	Off
Create/View User Account Change Service Access per user	[Authentication/Security Settings] > [Authentication] > [Create/View User Accounts] > [Account Number]	[Security] > [Authentication Configuration] > [Next]> [Account Number] > [Edit]	-

Change User Passcode by General User	[User Details Setup] > [Change Passcode]	-	-
Folder Service Setting	[System Settings] > [Folder Service Setting]	-	-
Stored File Setting	[System Settings] > [Stored File Setting]	-	-
Create Folder	[Setup Menu] > [Create Folder]	Scan Tab > [Folder] > [Create]	-
Change User Passcode by System Administrator	[Authentication/Security Settings] > [Authentication] > [Create/View User Accounts]	[Security] > [Authentication Configuration] > [Next]> [Account Number] > [Edit]	-
Set SOAP	[System Settings] > [Connectivity & Network Setup] > [Port Setting]	[Connectivity] > [Port Settings]	On