Xerox® VersaLink® C405DN
Multifunction Printer
Security Function Supplementary Guide

Version 1.0 (20221019): October, 2022

Contents

1 Before Using the Security Features

This section describes the security features and confirmation matters.

Preface

This guide describes the setup procedures related to security. This manual is mainly intended for the manager and system administrator of the organization where the machine is installed. This manual also describes useful information for general users about the operations related to security features.

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

Model	Guidance	Version
VersaLink C405DN Multifunction Printer	Xerox VersaLink C405 Color Multifunction Printer User Guide	Version 1.6
	Xerox VersaLink Series Multifunction and Single Function Printers System Administrator Guide	Version 2.1
	Xerox VersaLink C405 Quick Use Guide	Rev A

NOTE :

- The hash values of the PDF files are described in the Security Target disclosed at the Xerox (https://www.xerox.com/information-security/common-criteria-certified/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 product has obtained IT security certification for HCD PP v1.0 by the following ROM version.

VersaLink C405DN
Controller ROM Ver. 1.90.3

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 vendor's name "Xerox" and the model name 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, and the System Clock” section.
Your ROM and guidance may not be the certified version because they may have been updated along with machine improvements.

Please check the state of the delivered machine’s 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 service representative.

This guide has been prepared on the assumption that fax function are available. Installation is made by a service representative. And the print speed and the product name are fixed with initial settings by a service representative. You must witness on-site where a service representative 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 fax function after settings according to the procedure of this guide. For fax function, please confirm “fax” button.

You can find the detailed operation to see the buttons in Appendix “List of Operation Procedures”.
The default administrator password is the device serial number.
You can obtain the serial number from the Control Panel or from the configuration report.

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 Print 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 webservice on the device. Microsoft Edge was used as the web browser in the evaluation.
- The system administrator used it for getting the audit logs from the device.

SMTP Server

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

Precautions for secure use of this product

When installation or delivering the product, please confirm the affiliation of service representative or the person who is assigned by vendor by referring to business cards or purchase order sheet and so on.

If you could not attend the operation of the service representative at the time of initial installation, please reset to factory defaults*.

When you change settings that cannot maintain the security function during operation, please reset to factory defaults* and then check the settings again from the beginning according to the procedures in this guide.

This guide has been prepared on the assumption that the Service Representative Restricted Operation

function is set to [enabled]. If the maintenance operation is permitted to a service representative, please check the details of the operation in advance and witness on-site where a service representative. If you could not check that in advance or witness, the TOE cannot keep the secure configuration. In that case, please reset to factory defaults* after the maintenance operation and configure settings again according to the procedure of this guide.
For secure operation, prior to disposing of the machine, please reset to factory defaults*.

* Operation of reset to factory defaults

You can operate it on [Device > Resets] after setting to disable for Service Representative Restricted Operation.

When you use the product, please do not leave the paper sheets. For details on the service representative restricted operation, refer to “Set Service Representative Restricted Operation”.

Security Features

The machine has the following security features:

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

Settings for the Secure Operation

For the effective use of the security features, the System Administrator (Machine Administrator) must configure settings by referring to the following sections.

- Settings for the Secure Operation (Initial Settings Procedures Using Control Panel)
- Settings for the Secure Operation (Initial Settings Procedures Using Embedded Web Server)
- Regular Review by Audit Log

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 service representative.

Below is the list of setting items and their values that need to be set.

Item	Description
Reset to Factory Defaults	Reset at once
Fax Forwarding	Disable

USB	Disable
User Password Minimum Length	9
Change the System Administrator's Password	New password of 9 or more characters
Audit Log	Enabled
Startup page	Do Not Auto Print
TLS	Enable
Authentication	Local
Maximum Login Attempts	Any of 1-10
Access Control for Guest user	No access
Access Control for Basic user	Custom Permissions
Job Operation Restriction	Restrict
Auto Clear	30 (seconds)
Browser Session Timeout	6 (minutes)
Self Test	Enable
Service Representative Restricted Operation	Enable
Direct Print	Disable
Import Machine Certificate	If necessary
Certificate Validation	Enable
FIPS140-2	Enable
Secure Print	Enable
PJL data read/write	Disable
Remote Services Upload	Disable
PostScript Password	New password of 9 or more characters
Software Download	Enable
Plugin	Off
TCP/IP	IPv4
USB	Off
NFC	Off
AirPrint	Off
Google Cloud Print	Off
Mopria	Off
Bonjour	Disable
FTP Client	Off
HTTP	HTTPS
CSRF	Enable
IPP	IPPS
IPSec	Off
LPD	Off
Port9100	Off
S/MIME	Off
SFTP	Off
SMB	Disable

Email/SMTP	Enable
SNMP	Disable
SNTP	Off
SOAP	Disable
WSD	Disable
USB	Off
EIP	Disable
Secure Fax Receive	Enable
Direct Fax	Not Allowed
My Folder	Hide
Scan to Desktop	Hide
@PrintByXerox	Hide
Scan to	Hide
App Gallery	Hide

NOTE :

- WSD stands for Web Services on Devices.

IMPORTANT:

- The security will not be warranted if you do not correctly follow the above setting instructions.
- This manual has been prepared on the assumption that the Service Representative Restricted Operation function is set to **Enabled**. The security may not be warranted when maintenance operation is permitted to a service representative .
- The fax-network separation feature requires no special setting by the System Administrator.

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 this models, select **On** and then set **Maintenance Password** to restrict the Service Representative from entering the System Administration mode.

NOTE :

If the System Administrator's password is 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 device is used for) needs to follow the instructions below.

- The manager needs to assign appropriate people as system and device administrators, and manage and train them properly.
- The system administrator needs to train users about the device operation and precautions according to the policies of their organization and the product guidance.
- The device needs to be placed in a secure or monitored area where the device is protected from unmanaged physical access.
- If the network where the device is installed is to be connected to external networks, configure the network properly to block any unauthorized external access.
- To make it difficult to guess your password, users and administrators need to set passcode according to the following rules.
  - ✓ Do not use an easily guessed character strings passcode.
  - ✓ A passcode needs to contain numeric and alphabetic characters, and symbols.
- Users and administrators need to manage and operate the device so that their user IDs and passcodes may not be disclosed to another person.
- Administrators need to remove the user accounts when users leave their organization.
- The users need to set the **Secure Print** for **Job Type** on printer driver.
- For secure operation, all of the remote trusted IT products that communicate with the device shall implement the communication protocol in accordance with industry standard practice with respect to RFC/other standard compliance (TLS) and shall work as advertised.

1) TLS

For the TLS client (Web browser, Printer Driver, 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

NOTE :

- While you are using the **Embedded Web Server**, do not access other web sites, and do not use other applications. Otherwise the usage environment can be attacked via other websites or other application by an attacker.
- When you leave your computer while you are using **Embedded Web Server**, make sure to lock the screen in order to prevent unexpected operations by others.

- When you change **Login Method** or prior to disposing of the machine, please initialize the machine by executing **Reset to Factory Default** so that user data cannot be accessed by unexpected users who shouldn't have the access right.
- When there is no operation in Embedded Web Server for the set period of session timeout, it will automatically logout. Logout explicitly when leaving a client PC within the set period of session timeout. System administrators must ensure that all users follow this guidance. Otherwise unauthorized users can operate this device using Embedded Web Server that have not been logged out.
- For preventing TLS vulnerability, you should set the device address in the proxy exclusion list of browser. By this setting, secure communication will be ensured because the device and the remote browser communicate directly without proxy server, and thus you can prevent man-in-the-middle attack.
- NTP server connection is outside the scope of evaluation.

Confirm the Machine ROM Version and Serial Number

Before making initial settings, you need to check the Controller ROM version of the machine, Serial Number and the system clock of the machine.

Check the Machine ROM Version

Identify the Controller ROM version the machine on the screen.

1. Select Device on the control panel.
2. Select About.
3. Check the Software Version.

Check the Serial Number

The Serial Number is the default value for System Administrator’s password.

1. Select Device on the control panel.
2. Select About.
3. Check the Serial Number.

Print the Configuration Report

Identify the Controller ROM version of the machine.

1. Select Device on the control panel
2. Select About.
3. Select Information Pages.
4. Select Configuration Report.

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. Please log in as the System Administrator to set. If a reboot confirmation screen is displayed after changing the settings, reboot this device. If you want to continue to change the settings, please log in as the System Administrator.

Login as System Administrator

Before configuring settings, a user must be authenticated with the System Administrator's ID and a password. When you log in as the System Administrator at the first time, you must change the default password (Serial Number).

1. Select Log In on the control panel.
2. Select admin.
3. Enter the password (Serial Number) from the keypad.
4. Select OK.
5. Select Change Password.
6. Enter the new password.
7. Enter the confirm password.
8. Select OK.

NOTE :

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

Reset to Factory Defaults

Before configuring settings, please re-generate the data encryption key as below,

1. Select Device on the control panel.
2. Select Resets.
3. Select Reset to Factory Defaults.
4. Select Reset. (After reset to factory defaults, this device will restart.)
5. After the device restart, Select [Next] for Language in the Installation Wizard.
6. Select [No, Thanks] for Xerox Easy Assist App in the Installation Wizard.
7. Select [Ethernet] for Network Connection in the Installation Wizard.
8. Select [Next] for Ethernet in the Installation Wizard.
9. Select [Skip] for Proxy Server in the Installation Wizard.
10. Select [Next] for About in the Installation Wizard.

11. Select [Next] for Date & Time in the Installation Wizard.
12. Select [Next] for Measurements in the Installation Wizard.
13. Select [Skip] for LDAP in the Installation Wizard.
14. Clear the check boxes for Email, Fax and Scan To and select [Next] for Set Up Apps in the Installation Wizard.
15. Select [Skip] for Security Settings in the Installation Wizard.
16. Select [Done] for Install Complete in the Installation Wizard, this device will reboot automatically.

NOTE :

- Restoring factory defaults takes about an hour.

Login as System Administrator again

1. Select Log In on the control panel.
2. Select admin.
3. Enter the password (Serial Number) from the keypad.
4. Select OK.
5. Select Change Password.
6. Enter the new password of 9 or more characters.
7. Enter the confirm password.
8. Select OK.

NOTE :

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

Check the System Clock

1. Select General on the Device screen.
   Check the time, the date and time zone of the system clock. If you need to change the time and the date, refer to the following procedures.
2. Select Date & Time.
3. Select Time Zone.
4. Select the required setting for Region.
5. Select OK.
6. Select Date & Time.
7. Change the required setting.
8. Select OK twice.
9. Press the <Home> button.

Set Fax Forwarding

For the secure operation of the machine, follow the procedure below to set Fax Forwarding to Disabled if you can change the setting.

1. Select Apps on the Device screen.
2. Select Fax.
3. Select Fax Forwarding.
   If you cannot change the setting, you need not to change it because the default value is disabled.
4. Select Off.
5. Select OK.

Set USB

1. Press the <Home> button.
2. Select Customize.
3. Select Guest.
4. Select [X] of the [USB] button.
5. Select [Done].

3 Initial Settings Procedures Using Embedded Web Server

This section describes the initial settings related to security features, and how to set them on the **Embedded Web Server**. Please set up IP address according to “Initial Setup in the Embedded Web Server” section in System Administrator guide. If a reboot confirmation screen is displayed after changing the settings, reboot this device. If you want to continue configuration the settings, please log in as the System Administrator.

Preparations for Settings on the Embedded Web Server

Prepare a computer supporting the TCP/IP protocol to use the **Embedded Web Server**.
Embedded Web Server supports the browsers that satisfy TLS conditions.

1. Open your Web browser, enter the TCP/IP address of the machine to the URL bar, and press the <**Enter**> key.
2. Select **Log In** on the Embedded Web Server.
3. Select **admin**.
4. Enter the password.
5. Select **Log In**.

Set User Password Minimum Length

Follow the procedure below to specify the minimum number of digits allowed for a password.
This feature is only applicable to Local Authentication mode.

1. Select Permissions.
2. Select Login/Logout Settings
3. Select Password Rules.
4. Enter 9 in Minimum Length.
5. Select **OK**.
6. Select **Restart Later** if prompted.

Set Audit Log

Follow the procedure below to configure the Audit Logs settings.

1. Select **System**.
2. Select **Logs**.

3. Select Audit Log.
4. Enable this service.
5. Select **OK**.
6. Select **Restart Later** if prompted.

Set Startup Page

Follow the procedure below to configure the startup page.

1. Select **System**.
2. Select Defaults and Policies.
3. Select Startup Page.
4. Select Do Not Auto Print
5. Select **OK**.
6. Select Restart Later if prompted

Set TLS

The **Embedded Web Server** requires TLS communication between a network connected computer and the machine.

1. Select **System**.
2. Select **Security**.
3. Select Security Certificates.
4. Select Device Certificates > Create > Create Self-Signed Certificate
5. Set the details as necessary to create Self-Signed Certificate.
6. Select Create.
7. Restart device manually.
8. After the device restart, log in as Administrator.
9. Select System
10. Select Security
11. Select SSL/TLS Settings.
12. Select Protocol version : TLS 1.2 or Later
13. Select Enable TLS 1.3 : Off
14. Select TLS Security Level : Compatibility Mode
15. Select HTTP - SSL/TLS Communication : On
16. Select SMTP - SSL/TLS Communication : SSL/TLS
17. Select Verify Remote Server Certificate : On
18. Select **OK**.
19. Select **Restart Now** if prompted.

NOTE :

- For secure operation, you should import the CA certificate according to the same procedure as "Import Machine Certificates" section in this guide prior to enabling Verify Remote Server Certificate.
- You can find how to create Self-Sighed Certification in “Device Digital Certificate Management” section in this guide.

Set Authentication

Follow the procedure below to configure the authentication settings.

1. Select Permissions.
2. Select Login/Logout Settings.
3. Select **Local**. (Select Type in their user name)
4. Select **OK**.
5. Select **Change**.

   The Machine automatically restarts.

Set Maximum Login Attempts

Follow the procedure below to specify maximum login attempts.

1. Select Permissions.
2. Select Login/Logout Settings.
3. Select Authentication Settings.
4. Select Limit Login Attempts of System Administrator.
5. Enable Limit Login Attempts of System Administrator.
6. Enter any of [1] to [10] in Failed Login Attempt Limit.
7. Select Limit Login Attempts of Local User.
8. Enable Limit Login Attempts of Local User.
9. Enter any of [1] to [10] in Failed Login Attempts Limit.
10. Select **OK** twice.

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.

Set Access Control

Follow the procedure below to configure the access control settings.

For Guest User

<Control Panel Permissions>

1. Select Permissions.
2. Select **Edit** for Guest Access.
3. Select Device User Role.
4. Select **No Access** for Control Panel Permissions.

<Device Website Permissions>

5. Select **Custom Permissions** for Device Website Permissions.
6. Select **Setup**.
7. Select **Home**.
8. Select **Restrict**.

9. Select **OK**.
10. Select Hide for Address Book Page, Jobs Page, and Remote Control.
11. Select **OK**.
12. Select **Close**.
13. Select **OK**.

<Printing Permissions>

14. On the **Permission** screen, Select **Edit** for Guest Access.
15. Select Printing User Role.
16. Select **Custom Permissions** for Printing Permissions.
17. Disable all services for **Allowed Job Types**.
18. Select **OK**.

For Basic User

<Control Panel Permissions>

19. On the **Permission** screen, select Roles.
20. Select Device User Roles.
21. Select **Edit** for Basic User.
22. Select **Custom Permissions** for Control Panel Permissions.
23. Select **Setup**.
24. Select **Device**.
25. Select **Hide** for View Information Pages (under About) and Support Page.
26. Select **Hide** for View Software Update.
27. Select **Hide** for View General, Apps, and Connectivity.
28. Select **Hide** for View Network Information.
29. Select **OK**.

30. Select **Jobs**.
31. Select **Hide** for Delete Jobs.
32. Select **Hide** for View Secure Fax.
33. Select **OK**.

34. Select Personalization.
35. Select **Hide** for Customize Home Screen.
36. Select **OK**.

37. Select AirPrint(Scan).
38. Select Hide for Access AirPrint(Scan)
39. Select OK

40. Select Remote Scanning.
41. Select Hide for Access Remote Scanning
42. Select OK
43. Select Close

<Device Website Permissions>

44. Select **Custom Permissions** for Device Website Permissions.
45. Select **Setup**.
46. Select Remote Control.
47. Select **Hide** for Access Remote Control.
48. Select **OK**.
49. Select Close.
50. Select OK.

<Printing Permissions>

51. On the **Permission** screen, select **Roles**.
52. Select Printing User Roles.
53. Select **Edit** for Basic Printing User.
54. Select Custom Permissions.
55. Disable Normal Print, Personal, Sample Set, Public Saved for Allowed Job Types.
56. Select **OK**.

Set Job Operation Restriction

For the secure operation of the machine, follow the procedure below.

1. Select **Jobs**.
2. Select Policies.
3. Select Conceal Job Names : Conceal All Job Names.
4. Select Job Operation Restrictions : Restrict
5. Select Secure Print Job Settings : Manual Release of Secure Print Jobs
6. Select **OK**.
7. Select Restart Later if prompted.

Set Auto Clear

Follow the procedure below to configure the Auto Clear settings.

1. Select **System**.
2. Select **Timeouts**.
3. Enter a time for Reset Device Control Panel : 30 (seconds)
4. Select **OK**.
5. Select **Restart Later** if prompted.

NOTE :

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

Set Browser Session Timeout

For the secure operation of the machine, follow the procedure below.

1. Select **System**.

2. Select **Timeouts**.
3. Enter a time for Device Website Timeout : 6 (minutes)
4. Select **OK**.
5. Select **Restart Later** if prompted.

NOTE :

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

Set Self Test

Follow the procedure below to configure the Self Test settings.

1. Select **System**.
2. Select **Security**.
3. Select Firmware Verification.
4. Select **On**.
5. Select **OK**.
6. Select **Restart Later** if prompted.

Set Service Representative Restricted Operation

Follow the procedure below to restrict the operation of service representatives.

1. Select **System**.
2. Select **Security**.
3. Select Customer Service Engineer Access Restriction.
4. Enable this service.
5. Enter a password of 9 or more characters in **Maintenance Password** and **Retype Maintenance Password**.
6. Select **OK**.
7. Select **Enable** twice.
8. Select **Restart Now** if prompted.

Set Direct Print

Follow the procedure below to configure the Direct Print.

1. Select **System**.
2. Select **Security**.
3. Select Allow Direct Print.
4. Select Disabled.
5. Select OK.

Set Import Machine Certificates

Import the Certificates for the mail server, etc. to which this device connects.

6. Select **System**.
7. Select **Security**.
8. Select Security Certificates.
9. Select **Import**.
10. Select **Select**.
11. Select a certificate.
12. Enter **Password**, and enter **Retype Password** if necessary.
13. Select **Import**.
14. Select Close twice.

Set Certificate Validation

Follow the procedure below to configure the Certificate Path Validation settings.

1. Select **System**.
2. Select **Security**.
3. Select Certificate Path Validation.
4. Select **On**.
5. Select **OK**.
6. Select **Restart Later** if prompted.

Set FIPS140-2

For the secure operation of the machine, follow the procedure below.

1. Select **System**.
1. Select **Security**.
2. Select FIPS 140-2 : On.
3. Select OK twice.
4. Select **Restart Later** if prompted.

Set Secure Print

Follow the procedure below to configure the Secure Print settings.

1. Select **System**.
2. Select Defaults and Policies.
3. Select **Allowed Print Job Types** for Printer Settings.
4. Select Personal, Secure, and Saved Only.
5. Select **OK**.
6. Select **Restart Later** if prompted.

7. Select **Close**.

Set PJL data read/write

Follow the procedure below to configure the Disabling PJL data read/write

1. Select **System**.
2. Select Defaults and Policies.
3. Select PJL File System Command.
4. Select Disabled.
5. Select **OK**.
6. Select **Restart Later** if prompted.
7. Select Close.

Set Remote Services Upload

Follow the procedure below to configure the Remote Services Upload.

1. Select System
2. Select Remote Services Upload
3. Click Disable. If Enable button is displayed, you need not this setting.
4. Select Customer for the message “Who is disabling?”.
5. Input appropriate word for “Why are you disabling Remote Services Upload?”.
6. Select Disabled.

Set PostScript Password

Follow the procedure below to configure the PostScript Password.

1. Select System.
2. Select PDL Settings.
3. Select PostScript.
4. Enter 9 or more characters in Password.
5. Enter 9 or more characters in Retype Password.
6. Select OK.

NOTE :

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

Set Software Download

Follow the procedure below to configure the Software Download settings.

1. Select **System**.

2. Select Software Update.
3. Click Enable and confirm the message "Software updates are enabled.".
   If the message and Disable are displayed, you need not to click.
4. Select **Never** for check automatically.
5. Select **Restart Now** if prompted.

Set Plugin

For the secure operation of the machine, follow the procedure below.

1. Select System.
2. Select Plug-in Settings.
3. Select Plug-in Feature : Off
4. Select **Restart Later** if prompted.
5. Select Close.

Set TCP/IP

For the secure operation of the machine, follow the procedure below.

1. Select Connectivity.
2. Select Ethernet.
3. Select Edit for Common.
4. Select IP Mode : IPv4.
5. Select OK.
6. Select **Restart Now** if prompted.
7. Select Close.

Set USB

For the secure operation of the machine, follow the procedure below to set **USB** to **Disabled**.

1. Select Connectivity.
2. Select USB.
3. Select Off for Enable to disable.
4. Select OK.
5. Select **Restart Later** if prompted.

Set NFC

For the secure operation of the machine, follow the procedure below.

1. Select Connectivity.
2. Select NFC.
3. Select Off.
4. Select OK.
5. Select **Restart Later** if prompted.

Set AirPrint

For the secure operation of the machine, follow the procedure below.

1. Select Connectivity.
2. Select AirPrint for Mobile Printing.
3. Select Off.
4. Select OK.
5. Select **Restart Later** if prompted.

Set Google Cloud Print

For the secure operation of the machine, follow the procedure below.

1. Select Connectivity.
2. Select Google Cloud Print for Mobile Printing.
3. Select Off.
4. Select OK.
5. Select **Restart Later** if prompted.

Set Mopria

For the secure operation of the machine, follow the procedure below.

1. Select Connectivity.
2. Select Mopria for Mobile Printing.
3. Select Off.
4. Select OK.
5. Select **Restart Now** if prompted.

Set Bonjour

For the secure operation of the machine, follow the procedure below to set **Bonjour** to **Disabled**.

1. Select Connectivity.
2. Select **Bonjour** for Protocols.
3. Disable **Port**.
4. Select **OK**.
5. Select **Restart Later** if prompted.

Set FTP Client

For the secure operation of the machine, follow the procedure below.

1. Select Connectivity.
2. Select FTP for Protocols.
3. Select FTP Client Port : Off.

4. Select **OK**.
5. Select **Restart Later** if prompted.

Set HTTP

For the secure operation of the machine, follow the procedure below.

1. Select Connectivity.
2. Select HTTP for Protocols.
3. Select Enable HTTP : Off.
4. Select Enable HTTPS : On.
5. Select **OK**.
6. Select **Restart Later** if prompted.

Set CSRF

Follow the procedure below to configure the CSRF settings.

1. Select Connectivity.
2. Select **HTTP** for Protocols.
3. Enable CSRF Protection.
4. Select **OK**.
5. Select **Restart Later** if prompted.

Set IPP

Follow the procedure below to configure the IPP settings.

1. Select Connectivity.
2. Select **IPP** for Protocols.
3. Enable **Port**.
4. Disable Alternate Port (IPP)
5. Select **OK**.
6. Select **Restart Later** if prompted.

Set IPsec

For the secure operation of the machine, follow the procedure below.

1. Select Connectivity.
2. Select IPsec for Protocols.
3. Select Enable : Off.
4. Select **OK**.
5. Select **Restart Later** if prompted.

Set LPD

For the secure operation of the machine, follow the procedure below.

1. Select Connectivity.
2. Select LPD for Protocols.
3. Select Off for Port.
4. Select **OK**.
5. Select **Restart Later** if prompted.

Set Port9100

For the secure operation of the machine, follow the procedure below.

1. Select Connectivity.
2. Select Port9100 for Protocols.
3. Select Off for Port.
4. Select **OK**.
5. Select **Restart Later** if prompted.

Set S/MIME

For the secure operation of the machine, follow the procedure below.

1. Select Connectivity.
2. Select S/MIME for Protocols.
3. Select Off.
4. Select **OK**.
5. Select **Restart Later** if prompted.

Set SFTP

For the secure operation of the machine, follow the procedure below.

1. Select Connectivity.
2. Select SFTP for Protocols.
3. Select Off for SFTP Client Port.
4. Select **OK**.
5. Select **Restart Later** if prompted.

Set SMB

For the secure operation of the machine, follow the procedure below to set **SMB** to **Disabled**.

1. Select Connectivity.
2. Select **SMB** for Protocols.
3. Disable **Port**.
4. Select **OK**.
5. Select **Restart Now** if prompted.

Set Email/SMTP

Follow the procedure below to configure the E-mail settings.

1. Select **Apps**.
2. Select **Email**.
3. Select **Setup**.
4. Select Email Submission : On.
5. Select Email Notification : Off.
6. Set Email Address for Device Email.
7. Select Server Address for SMTP Server.
8. Set Server Address.
9. Select **OK**.
10. Set a port number for Outgoing SMTP Port Number.
11. Select **OK**.
12. Select **Restart Later** if prompted.

Set SNMP

For the secure operation of the machine, follow the procedure below to set **SNMP** to **Disabled**.

1. Select Connectivity.
2. Select **SNMP** for Protocols.
3. Disable **Port**.
4. Select **OK**.
5. Select **Restart Later** if prompted.

Set SNTP

For the secure operation of the machine, follow the procedure below.

1. Select Connectivity.
2. Select SNTP for Protocols.
3. Select Off.
4. Select **OK**.
5. Select **Restart Later** if prompted.

Set SOAP

For the secure operation of the machine, follow the procedure below to set **SOAP** to **Disabled**.

1. Select Connectivity.
2. Select **SOAP** for Protocols.
3. Disable **Port**.
4. Select **OK**.
5. Select **Restart Later** if prompted.

Set WSD

For the secure operation of the machine, follow the procedure below to set **WSD** to **Disabled**.

1. Select Connectivity.
2. Select WSD (Web Services on Devices).
3. Disable WSD Scan, and WSD Print
4. Select **OK**.
5. Select **Restart Now** if prompted.

Set USB

For the secure operation of the machine, follow the procedure below to set **USB** to **Disabled,** if USB App is displayed.

1. Select **Apps**.
2. Select **USB**.
3. Select Hide Display on Device.
4. Select Hide Scan to and Print From.
5. Select **Restart Later** if prompted.

Set EIP

For the secure operation of the machine, follow the procedure below to set **EIP** to **Disabled**.

1. Select **Apps**.
2. Select EIP Settings.
3. Disable all services and Restart Later if prompted each time.
4. Select EIP Web Services.
5. Disable all services and Restart Later if prompted each time.

Set Secure Fax Receive

Follow the procedure below to configure the Secure Fax Receive settings.

1. Select **Apps**.
2. Select **Fax**.
3. Select Secure Fax Receive for General Settings and Policies.
4. Enable this service.
5. Set a passcode.
6. Select **OK**.
7. Select **Restart Now** if prompted.

Set Direct Fax

For the secure operation of the machine, follow the procedure below to set **Direct Fax** to **Disabled**.

1. Select **Apps**.

2. Select **Fax**.
3. Select Direct Fax for General Settings and Policies.
4. Select Not Allowed.
5. Select **OK**.
6. Select **Restart Later** if prompted.

Set My Folder

For the secure operation of the machine, follow the procedure below to set **My Folder** to **Disabled**.

1. Select **Apps**.
2. Select My Folder.
3. Select **Hide** for Display on Device.

Set Scan to Desktop

For the secure operation of the machine, follow the procedure below to set **Scan to Desktop** to **Disabled**.

1. Select **Apps**.
2. Select Scan to Desktop.
3. Select **Hide** for Display on Device.

Set @PrintByXerox

For the secure operation of the machine, follow the procedure below.

1. Select **Apps**.
2. Select @PrintByXerox.
3. Select Hide for Display on Device.

Set Scan to

For the secure operation of the machine, follow the procedure below.

1. Select **Apps**.
2. Select Scan to.
3. Select Hide for Display on Device.

Set App Gallery

For the secure operation of the machine, follow the procedure below to delete **App Gallery** application.

1. Select **Apps**.
2. Select Xerox App Gallery.
3. Select Hide for Display on Device.

Set Remote Control Panel

For the secure operation of the machine, follow the procedure below.

1. Select **Home**.
1. Select Remote Control Panel.
2. Select off.
3. Select Close.

4 Regular Review by Audit Log

This section describes the automatic importing method of the Audit Log feature using the Audit Server. The Audit Log is regularly reviewed by the Security Administrator, often with the aid of third-party analyzing tools. The audit log helps to assess attempted security breaches, identify actual breaches, and prevent future breaches.
The important events of the device such as device failure, configuration change, and user operation are traced and recorded based on when and who operated what function. Auditable events are stored with time stamps into one file ("audit log file") within the internal storage. Up to 15,000 events can be stored. When the number of recorded events exceeds 15,000, the oldest audit log file is overwritten, and a new audit event is stored. The audit log file remains on the device whenever it is retrieved from the device to Audit Server. It means that the same audit event may be included in the audit log file by a time interval of retrieving. However, if it takes the long-time interval over the upper limit of the number of the audit events in the file, A number of new audit events might overwrite the same number of older audit events. Therefore, the system administrator should design the appropriate time interval under the usage environment of the device. The size of the audit log file containing 15,000 events is about 1.5M Bytes. According to the interval of retrieval and the free size of the storage space, the system administrator should determine the number of log files to be preserved and delete the older log files. When using the following PowerShell script, the name of log files includes the time stamp indicating the date and the time when the file was downloaded. You can find the events recorded in a duration with the name of the log file. The system administrator should check if the audit log file is retrieved appropriately in the target folder which the operation script file of PowerShell is stored before using the device formally. The system administrator should modify the operation script file of PowerShell as appropriate. There is no function to delete the audit log data stored in the device.

Import the Audit log

TLS communication must be enabled in order to access the logged data. Procedures described below should be performed in the following environment.

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

1. Create PowerShell script file with the contents below.

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

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

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

# Download audit log
$USER_B64 = [Convert]::ToBase64String(([System.Text.Encoding]::Default).GetBytes($USER))
$PASS_B64 = [Convert]::ToBase64String(([System.Text.Encoding]::Default).GetBytes($PASS))
$cred = "NAME=${USER_B64}&PSW=${PASS_B64}"
$referer = $Uri + "/home/index.html"
$ProgressPreference = 'SilentlyContinue'
[Net.ServicePointManager]::SecurityProtocol =
[Net.ServicePointManager]::SecurityProtocol -bor
[Net.SecurityProtocolType]::Tls12

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

IMPORTANT:

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

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

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

   Operation: execution of 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>"

File Format of the Exported Audit log

The following information is recorded in imported audit log data, check regularly whether there are

not breaches by accessing or attempt.

Header Information

Item	Export Format	Description
Format Version	Integer	The setting value is “3”.
Device’s IP Address	Character string that consists of half-size alphanumeric characters (a to z, 0 to 9),dot(.), colon(:)	Displays the IP address (IPv4 or IPv6)
Coding Method	String	Fixed to UTF8.
Time Zone	-720 to 720	Displays time difference based on GMT. The unit is minute, and the value is negative if the time zone is west of Meridian.
Date Format	YYYY/MM/DD, MM/DD/YYYY, or DD/MM/YYYY	Displays the date format.

Audit log information

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

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

Item	Description
Log ID	1
Date	01/01/2018
Time	10:00:00
Logged Events	Login/Logout
User Name	User1
Description	Login

Status	Failed (Invalid Password)
Optionally Logged Items	-

Operations recorded in the Audit Log File

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

- User Identification/Authentication (using Control Panel)
- User Identification/Authentication (using 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, 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)
- Firmware Update
- PSTN

The export method of Audit Log from Embedded Web server

The following describes methods for export the Audit Log.
The audit logs are only available to System Administrators and can be downloaded via Embedded Web Server for viewing and analyzing them. The logged data cannot be viewed from the local UI.
In addition, TLS communication must be enabled in order to access the logged data.

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. Select **Log In**.
3. Select **admin**.
4. Enter the password from keyboard.
5. Select Log In.
6. Select **System**.
7. Select **Logs**.
8. Select Audit Log.
9. Select **Export**.

5 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 of verification.
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 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 (116-321) 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 sales representative or service representative.

6 Software Update

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

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. Select **Log In**.
3. Select **admin**.
4. Enter the password from keyboard.
5. Select Log In.
6. Select **System**.
7. Select Software Update.
8. In the Update with File Specified area, click **Select**.
9. Navigate to the location of the firmware, then select the file.
10. Click Install Now.

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

Download Mode
PROCESSING XX/XX

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

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

SOFTWARE UPGRADE FAILED 017-759
Please press power button to reboot. In this case, check the new firmware is correct and try this procedure again. If it still fails, please contact our sales representative or service representative.

7 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.

8 Using Secure Print

The Secure 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 <home> button.
2. Select Jobs.
3. Select Personal & Secure Jobs.
4. Select your folder.
5. Select a job to be printed or Delete All or Print All.

Note: After a Secure Print job is printed, it is deleted automatically.

9 Device Digital Certificate Management

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

In the Embedded Web Server, log in as administration, then click [System] > [Security] > [Security Certificate]. Select the type of certificate to create from pull-down menu and then select the [Create Self-Sighed Certificate] or [Create Certificate Signing Request (CSR)] from [Create] menu.

When [Create Self-Signed Certificate] is selected, the [Create Self-Signed Certificate] screen is displayed.
When [Create Certificate Signing Request (CSR)] is selected, the [Create Certificate Signing Request] screen is displayed.

Create Self-Signed Certificate

Configure the settings below to set the self-signed certificate to the device. If the self-signed certificate has already been created, it will be overwritten.

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

Public Key Length (When [RSA/SHA-256], [RSA/SHA-384] or [RSA/SHA-512] is selected.)
Select [2,048 Bits] or [3,072 Bits].

Elliptic Curve (When [ECDSA/SHA-256], [ECDSA/SHA-384] or [ECDSA/SHA-512] is selected.)
Select [P-256], [P-384] or [P-521].

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

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

Certificate Signing Request (CSR)

Configure the settings below to set the Certificate Signing Request.

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

Public Key Length (When [RSA/SHA-256], [RSA/SHA-384] or [RSA/SHA-512] is selected.)
Select [2,048 Bits] or [3,072 Bits].

Elliptic Curve (When [ECDSA/SHA-256], [ECDSA/SHA-384] or [ECDSA/SHA-512] is selected.)
Select [P-256], [P-384] or [P-521].

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

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

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

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

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

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

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

Import Certificate

Configure the settings below to set the specified certificate to the device.

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

Password
Enter the password to decode data in PKCS#12 format. Up to 32 characters can be entered.
The password will be displayed as asterisks (***) or bullets (●●●).

Retype Password
Re-enter the password for verification.
The password will be displayed as asterisks (***) or bullets (●●●).

The digital certificate appears in the list of Installed certificates.

10 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.

Users Controlled by Authentication

The following explains the 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

The machine administrator uses a special user ID. Only the machine administrator is able to change the Machine Administrator Password. 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. When you log in as the Machine Administrator at the first time, you must change the default password (Serial Number).

Authenticated Users (with System Administrator Privileges)

Users to whom the system administrator privileges are granted. To use a restricted service, this type of users must enter their user IDs on the authentication screen. When you log in at the first time, you must change the default password.
This type of users have the same privileges as the machine administrator in operating the machine, however, they cannot change the Machine Administrator Password.

Authenticated Users (with no System Administrator Privileges)

Users who are registered on the machine or the remote server, and to whom system administrator privileges are not granted. When you log in at the first time, you must change the default password. To use a restricted service, this type of users must enter their user IDs on the authentication screen.

Unauthenticated Users (Guest Users)

These are users who are not registered with the machine. Unauthenticated Users cannot use services that are restricted.

Roles

Role is used to control the permissions on printer features and access to some settings.
You can create and assign roles to users to give them appropriate permissions.
The following shows the types of roles.

System Administrator

System Administrator is assigned to the system administrator account by default.
The System Administrator role cannot be customized.

Basic User

Basic User is automatically assigned to a user with no device user role assigned, and Basic Printing User is automatically assigned to a user with no printing user role assigned.
Features other than setup and configuration are allowed by default.
You can customize the basic user permissions.

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.

As for Secure Print feature, general User can perform the following operations for the data and the jobs stored Secure Print folder by oneself.
- 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 delete 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 delete 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.
- 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 delete 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 delete all the send data and jobs regardless of owner.

As for Fax receive feature, received Fax data is stored into the Secure fax receive folder. System Administrator (include Key Operator) can print and delete the data and jobs.

Login Method

Local Authentication (Login to Local Accounts)

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

Functions Controlled by Access Method

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

Local Access (Control Panel Permissions)

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

Everything Except Setup

Users can access everything except setup and configuration functions.

Copy Only

Users can use Copy Apps only. No access to Scanning Apps, Printing Apps, status or set up functions.

Access All

Users can access all functions.

Custom Permissions

Users can choose the services to be customized.

Authentication for Secure Fax Receive

The following explains the restricted operations on Secure Fax Receive when the Authentication

feature is enabled.

NOTE :

- Authenticated Users who are given the System Administrator privileges can access to Secure Fax Receive jobs according to the settings described previously.
- The machine has a single Secure Fax Receive folder to hold received fax jobs.
- After a Secure Fax Recieve document is printed, it is deleted automatically.
- If there are both secure print and fax receive jobs, only secure print job is displayed in Personal & Secure.

Maximum Login Attempts by System Administrator and Basic User

This feature protects the settings from being changed by someone impersonating your system administrator or Basic User. If authentication for a system administrator's ID or Basic User fail more than specified times continuously, access is denied.
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.

11 Operation Using Control Panel

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

User Authentication

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

1. Select a UserID on the touch screen.
2. Enter the password.
3. Select OK

All features on the control panel become available.

NOTE :

- When using Local Authentication, only the System Administrator's ID is pre-registered on the machine. Other user IDs are not registered. For details on how to register User IDs, refer to the “Operation Using Embedded Web Server”.

Print from Secure Fax Receive folder

This section describes the Secure Fax Receive features that allow you to check or print files in the Secure Fax Receive folder that is displayed on the Jobs screen.

1. Press the <home> button.
2. Select Jobs.
3. Select Personal & Secure Jobs.
4. Select Secure Fax Receive folder.
5. Select a job to be printed or Print All.

NOTE :

- The machine has a single Secure Fax Receive folder to hold received fax jobs.
- Only System Administrators can print a secure fax receive jobs according to the settings described previously.
- When there is at least one Secure Fax, the Secure Fax folder appears at the top of the Secure Jobs list.

Print and delete Secure Print jobs

The Secure 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 <home> button.
2. Select Jobs.
3. Select Personal & Secure Jobs.
4. Select a job to be printed or Delete All or Print All.

12 Operation Using Embedded Web Server

This section describes the operation using **Embedded Web Server** to use security features for System Administrators 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 create/edit User accounts, to check each job and the machine status, or to change the network settings.

NOTE :

For information of the **Embedded Web Server** feature, refer to the User 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://”.

User Authentication

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

Log in to the **Embedded Web Server**.

1. Select **Log In**.
2. Select the user account from the list, or enter the user name.
3. Enter the password.
4. Select **Log In**.

All features on the **Embedded Web Server** become available.

Create User Accounts

This feature allows you to register user account information, such as User IDs and passwords.
This feature is only applicable to Local Authentication mode.

1. Select Permissions.
2. Select **Add** for User Accounts.
3. Enter a user ID for **User Name**.
4. Enter a password for **Password**.
5. Enter the same password for **Retype Password**.
6. Select **Add**.

User ID (User Name)

Allows you to enter a User ID using Web Browser. You can enter up to 64 alphanumeric characters as a User ID.

Password

Allows you to enter a password using Web Browser. You can enter up to 64 alphanumeric characters.

E-mail Address

Allows you to enter the e-mail address. The specified address that is displayed on the **Email “From” Address** field is set as the sender’s address of the machine. You can enter up to 128 characters.

User Role

Allows you to select the privileges that are given to the user. Select from **Basic User** or **System Administrator**.

Change User Password by Authenticated Users

This feature allows Authenticated Users (users who are authenticated by the procedure described in "User Authentication") to change the registered password.
This feature is only applicable to Local Authentication mode.

1. Select the user icon on upper right corner on the **Embedded Web Server**.
2. Select My Profile.
3. Select Change Password.
4. Enter the old password in **Old Password**.
5. Enter the new password in **New Password**.
6. Enter the new password in **Retype New Password**.
7. Select **OK**.

13 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	
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)	Login/Logout	Login	Failed (Invalid UserID), Failed (Invalid Password)
Unsuccessful User identification (using Printer Driver)	Job Status	Print	Aborted
Use of management functions	Device Settings	View Security Setting	Successful
		Change Security Setting	
		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)

14 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 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.

NOTE :

- You should call for service representative if the problem persists or a message indicates so.
- Even when the power of the machine fails, all the queued jobs will be saved because the machine is equipped with the storage device. 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 codes in the following table to rectify problems.

NOTE :

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.
016-513	[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.
016-705	[Cause] Secure print documents cannot be registered. [Remedy] Use the Printer Driver appropriate for the machine. If the error still is not resolved, contact our Customer Support Center.
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 password entered does not match the password set on the folder. [Remedy] Enter the correct password.
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..
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.

15 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/.

16 Appendix

List of Operation Procedures

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

Item	Using Control Panel	Using Embedded Web Server	Configurable value	Default	Settings
Set Fax Forwarding	Device > Apps > Fax	-	On / Off	Off	Off
Set USB	Customize > USB	-	On / Off	On	Off
Set User Password Minimum Length	-	Permissions > Login/Logout Settings > Password Rules	1-63	4	9
Set Audit Log	-	System > Logs > Audit Logs	On / Off	Off	On
Set Startup Page	-	System > Defaults and Policies > Startup Page	Auto Print Do Not Auto Print	Auto Print	Do Not Auto Print
Set TLS	-	System > Security > SSL/TLS Settings > Protocol version	On / Off	Off	TLS1.2 or Later
	-	System > Security > SSL/TLS Settings > Enable TLS1.3	On / Off	Off	Off
Set Authentication	-	Permissions > Login/Logout Settings	Simple / Local / Network	Simple	Local
Set Maximum Login Attempts	-	Permissions > Login/Logout Settings > Authentication Settings > Limit Login Attempts of System Administrator	1-10	5	Any of 1 to 10
	-	Permissions > Login/Logout Settings > Authentication Settings > Limit Login Attempts of Local User	1-10	5	Any of 1 to 10
Set Access Control （Guest user） Control Panel	-	Permissions > Guest Access > Device User Role	No Access / Everything Except Setup / Copy only / Access All / Custom Permissions	Everything Except Setup	No Access
Device Website			Everything Except Setup / Home Only / Custom Permissions	Everything Except Setup	Custom Permissions - Restrict

	-	Permissions > Guest Access > Printing User Role	Unlimited Printing / Weekdays, 08:00 to 17:00 / Eco-Friendly / Custom Permissions	Unlimited Printing	Custom Permissions - Disable all services for Allowed Job Types
Set Access Control （Basic user） Control Panel	-	Permissions > Roles > Device User Role	Everything Except Setup / Copy Only / Access All / Custom Permissions	Access All	Custom Permissions
Device Website	-		Everything Except Setup / Home Only / Custom Permissions	Everything Except Setup	Custom Permissions
	-	Permissions > Roles > Printing User Role	Unlimited Printing / Weekdays, 08:00 to 17:00 / Eco-Friendly / Custom Permissions	Unlimited Printing	Custom Permissions
Set USB	-	Apps > USB	Display / Hide	Display	Hide
Set Job Operation Restriction	-	Jobs > Policies > Job Operation Restrictions	Restrict / Don’t Restrict	Don’t Restrict	Restrict
Set Auto Clear	Device > General > System Timeout	System > Timeouts > Reset Device Control Panel	10-900 seconds	90	30
Set Browser Session Timeout	-	System > Timeouts > Reset Device Website	1-240 minutes	20	6
Set Self Test	-	System > Security > Firmware Verification	On / Off	Off	On
Set Service Representative Restricted Operation	-	System > Security > Customer Service Engineer Access Restriction	On / Off	Off	On
Import Machine Certificates	-	System > Security > Security Certificates	-	-	-
Set Certificate Validation	-	System > Security > Certificate Path Validation	On / Off	Off	On
Set FIPS140-2	-	System > Security	On/ Off	On	On
Set Secure Print	-	System > Defaults and Policies > Printer Settings > Allowed Print Job Types	Personal, Secure, and Saved Only / All Jobs	All Jobs	Personal, Secure, and Saved Only

Set Disabling PJL data read/write	-	System > Defaults and Policies > PJL File System Command	Enable / Disable	Disable	Disable
Set Remote Services Upload	-	System > Remote Services Upload	Enable / Disable	Enable	Disable
Set Software Download	-	System > Software Update	Enable / Disable	Enable	Enable
Set Plugin	-	System > Plug-in Settings > Plug-in Feature	On / Off	Off	Off
Set TCP/IP	-	Connectivity > Ethernet	IPv4 / IPv6	Auto	IPv4
Set USB	-	Connectivity > USB	On / Off	On	Off
Set NFC	-	Connectivity > NFC	On / Off	On	Off
Set AirPrint	-	Connectivity > AirPrint	On / Off	On	Off
Set Google Cloud Print	-	Connectivity > Google Cloud Print	On / Off	Off	Off
Set Mopria	-	Connectivity > Mopria	On / Off	On	Off
Set Bonjour	-	Connectivity > Bonjour	Enable / Disable	Enable	Disable
Set FTP Client	-	Connectivity > FTP	On / Off	On	Off
Set HTTP	Device > Connectivity	Connectivity > Protocols	HTTP / HTTPS	HTTP	HTTPS
Set CSRF	-	Connectivity > HTTP > CSRF Protection	On / Off	Off	On
Set IPP	-	Connectivity > Protocols	On / Off	On	On
Set IPSec	-	Connectivity > Protocols	On / Off	Off	Off
Set LPD	-	Connectivity > Protocols	On / Off	On	Off
Set Port9100	-	Connectivity > Protocols	On / Off	On	Off
Set S/MIME	-	Connectivity > Protocols	On / Off	Off	Off
Set SFTP	-	Connectivity > Protocols	On / Off	Off	Off
Set SMB	-	Connectivity > Protocols	On / Off	On	Off
Set Email	Device > Connectivity > SMTP	Apps > Email > Email Submission	On / Off	On	On
	-	Apps > Email > Email Notification	On / Off	On	Off
Set SNMP	-	Connectivity > Protocols	On / Off	On	Off
Set SNTP	-	Connectivity > Protocols	On / Off	On	Off
Set SOAP	-	Connectivity > Protocols	On / Off	On	Off
Set WSD	-	Connectivity > Protocols > WSD Scan	On / Off	On	Off
	-	Connectivity > Protocols > WSD Print	On / Off	On	Off
Set EIP	-	Apps > EIP Settings	On / Off	On	Off
Set Secure Fax Receive	-	Apps > Fax > Secure Fax Receive	On / Off	Off	On

Set Direct Fax	-	Apps > Fax > Direct Fax	Allow / Not Allowed	Allow	Not Allowed
Set My Folder	-	Apps > My Folder	Show / Hide	Show	Hide
Set Scan to Desktop	-	Apps > Scan to Desktop	Show / Hide	Show	Hide
Set @PrintByXerox	-	Apps > @PrintByXerox	Show / Hide	Show	Hide
Set Scan to	-	Apps > Scan to	Show / Hide	Show	Hide
Set App Gallery	-	Apps > Xerox App Gallery	Show / Hide	Show	Hide

Note:

WSD stands for Web Services on Devices.