Xerox® VersaLink® B7025/B7030/B7035 Multifunction Printer

Security Function Supplementary Guide

Document Version 1.0: March 2018

Contents

1 Before Using the Security Features

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

Preface

This manual 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.

- Xerox® VersaLink B7025/B7030/B7035 Multifunction Printer User Guide: Version 2.0

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.
- The Manual version might be changed when the manual content is updated.

The security features of the Xerox® VersaLink B7025/B7030/B7035 are supported by the following ROM versions.

Controller ROM	Ver. 1.10.33
Fax ROM	Ver. 2.0.8

NOTE :

The machine has obtained IT security certification for Common Criteria EAL2+ALC_FLR.2.
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.
Your ROM and guidance may not be the certified version because they may have been updated along with machine improvements.
For the latest information concerning your device, download the latest versions from http://www.support.xerox.com/support.

- 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 customer engineer.

- If you have such inquiries as the following, please contact us（www.xerox.com/support):
  - Inquiries about the machine's functions
  - All other inquiries.
- This manual has been prepared on the assumption that the security functions, fax function are available. If your model provides the said functions as optional ones, you need to purchase and install Optional Kit.
  HDD Model requires Hard Disk Drive, if your model provides as optional one, you need to purchase and install Hard Disk Drive.
  You can check whether your model has the said functions by checking whether icons for the functions appear on the control panel or by checking Configuration Report.
- You can identify the product codes for the models and the expected options in the List of Product Codes in "Appendix".

Security Features

The machine has the following security features:

- Hard Disk Data Overwrite (HDD Model)
- Hard Disk Data Encryption (HDD Model)
- Flash Memory Encryption (Diskless Model)
- User Authentication
- System Administrator's Security Management
- Customer Engineer Operation Restriction
- Security Audit Log
- Internal Network data protection
- Self Test
- Information Flow Security / Fax Flow Security

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 Embedded Web Server)
- Settings for the Secure Operation (Initial Settings Procedures Using Control Panel)
- Regular Review by Audit Log
- Self Testing
- Authentication for the secure operation
- Operation using Control Panel
- Operation using Embedded Web Server

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

EIP	disabled.
My Folder	
Dropbox	
GoogleDrive	
OneDrive	
Scan to Desktop	
USB	
App Gallery	
Authentication	Local or Network
Access Control for Guest user	Non-access
Access Control for Basic user	Restricted
Maximum Login Attempts	5
User Password Minimum Length	9
TLS	Enabled
Certificate Validation	
Google Cloud Print	Disabled
Bonjour	
IPP	Enabled
SOAP	Disabled
SNMP	
SMB	
WSD Scan	
CSRF	Enabled
LDAP Server	Set the LDAP Server information
S/MIME	Enabled
Email	
Direct Fax	Disabled
Secure Fax Receive	Enabled
Service Representative Restricted Operation	Enabled Enter a password of 9 or more characters.
Self Test	Enabled
Auto Clear	
Store Print	
Audit Log	
Software Download	Disabled
IPSec	Enabled
Overwrite Hard Disk (HDD Model only)	
Fax Forwarding	Disabled

NOTE :

- The security will not be warranted if you do not correctly follow the above setting instructions.
- Once you have configured settings to deviate from this manual, please initialize the machine by executing **Reset to Factory Default** before you correct the settings according to the procedures.
- 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 customer engineer.
- The Information Flow Security / Fax Flow Security feature requires no special setting by the System Administrator.

Use of the Overwrite Hard Disk (HDD Model only)

In order to protect the data stored on the hard disk from unauthorized retrieval, you can set the overwrite conditions to apply them to the data stored on the hard disk.
The feature also overwrites temporarily saved data such as copy documents.

NOTE :

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

Service Representative Restricted Operation

Specifies whether the Service Representative has full access to the security features of the machine, including the ability to change System Administrator settings.
For the VersaLink B7025/B7030/B7035, 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 Optimized Performance of the Security Features

The management organization needs to follow the instructions below:

- Assign appropriate personnel as machine and system administrators, provide training, and ensure proper oversight.
- Train users about the machine operation and precautions according to the policies of their organization and the product guidance.
- The machine needs to be placed in a secure or monitored area where the machine is protected from unmanaged physical access.
- If the machine is on the internal network that connects to external networks, configure the network properly to block any unauthorized external access.
- Users and administrators need to set password and Pre-Shared Key according to the following rules for the client PC and the machine's setup.
  - Do not use an easily guessable password.
  - A password needs to contain both numeric and alphabetic characters.
- Administrators need to set the account policies on the remote authentication server as follows.
  - Set password policy to 9 or more characters.
  - Set account lockout policy to 5 times.
- Administrators need to remove the user accounts when users leave their organization.
- Users and administrators need to manage and operate the machine so that their user IDs and passwords may not be disclosed to another person.
- 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 machine must implement the communication protocol in accordance with industry standard practice with respect to RFC/other standard compliance (TLS, IPSec, S/MIME) and must work as advertised.

1) TLS

For the TLS client (Web browser) and the TLS 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

2) S/MIME

For the machine and E-mail clients, select an Encryption Method/Message Digest Algorithm from the following:

- 3Key Triple-DES/168bit, AES/128bit, AES/192bit, AES/256bit
- SHA1, SHA256

3) IPSec

For the IPSec host that communicates with the machine, select an Encryption Method/Message Digest Algorithm from the following:

- AES (128bit)/SHA1/SHA256/SHA384/SHA512
- 3Key Triple-DES (168bit)/SHA1/SHA256/SHA384/SHA512

NOTE :

- While you are using the **Embedded Web Server**, do not access other web sites, and do not use other applications.
- 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.
- For preventing SSL vulnerability, you should set the machine address in the proxy exclusion list of browser. By this setting, you can prevent man-in-the-middle attack because the machine and the remote browser communicate directly without proxy server.
- NTP server connection is outside the scope of evaluation.

Confirm the Machine ROM Version and the System Clock

Before making initial settings, the System Administrator needs to check the ROM version of the machine and the system clock of the machine.

Login as System Administrator

1. Select Log In on the control panel.
2. Select admin.
3. Enter the password from the keypad.
4. Select OK.

Check the Machine ROM Version

1. Select Device on the control panel.
2. Select About.

Identify the firmware versions of the components of the machine on the screen.

Print the Configuration Report

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

Identify the firmware versions of the components of the machine.
If the machine contains HDD option, Configuration Report shows “Hard Disk Total Size” in “Device Configuration” section. Please check the installed Fax Kit contains three lines in “Fax Service”

section.

Check the System Clock

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

2 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**.

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**.

Change the System Administrator's Password

1. Select **Permissions**.
2. Select **admin**.
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**.

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.

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**.

Set DropBox

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

1. Select **Apps**.
2. Select **Print and Scan** for Dropbox.
3. Select **Delete App**.
4. Select **Delete**.

Set GoogleDrive

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

1. Select **Apps**.
2. Select **Print and Scan** for GoogleDrive.
3. Select **Delete App**.
4. Select **Delete**.

Set OneDrive

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

1. Select **Apps**.
2. Select **Print and Scan** for OneDrive.
3. Select **Delete App**.
4. Select **Delete**.

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**.

Set USB

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

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 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 **Delete App**.
4. Select **Delete**.

Set Authentication

Follow the procedure below to configure the authentication settings.

1. Select **Permissions**.
2. Select **Login/Logout Settings**.

Configure the Local Authentication or Network Authentication Settings in the following procedures.

To use Local Authentication

3. Select **Local**.
4. Select **OK**.
5. Select **Change**.
   The Machine automatically restarts.

To use Kerberos Network Authentication.

6. Select **Network**.
7. Select **Kerberos (Windows ADS)**.
8. Select **Next**.
9. Set Realm and Server Address.
10. Select **OK**.
11. Select **Restart Now** if prompted.

To use LDAP Network Authentication.

12. Select **Network**.
13. Select **LDAP**.
14. Select **Next**.
15. Select **LDAP Servers / Directory Services**.
16. Set Server Information and Advanced Settings.
17. Select **OK**.
18. Select **Restart Later** if prompted.
19. Select **Done**.

20. Select **Change**.
    The machine automatically restarts.

Set Access Control

Follow the procedure below to configure the access control settings.

1. Select **Permissions**.
2. Select **Edit** for Guest Access.
3. Select **Device User Role**.
4. Select **No Access** for Control Panel Permissions.
5. Select **Custom Permissions** for Device Website Permissions.
6. Select **Setup**.
7. Select **Home**.
8. Select **Restrict**.
9. Select **OK**.
10. Select **Close**.
11. Select **OK**.
12. Select **Restart Later** if prompted.

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

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

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

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

37. Select **Close**.

38. Select **Custom Permissions** for Device Website Permissions.
39. Select **Setup**.
40. Select **Jobs**.
41. Select **Hide** for Delete Jobs.
42. Select **Close**.
43. Select **OK**.

44. On the **Permission** screen, select **Roles**.
45. Select **Printing User Roles**.
46. Select **Edit** for Basic Printing User.
47. Select **Custom Permissions**.
48. Disable **Normal Print**, **Personal, Sample Set**, **Public Saved** for Allowed Job Types.
49. Select **OK**.

Set Maximum Login Attempts

Follow the procedure below to specify maximum login attempts.

1. Select **Permissions**.
2. Select **Login/Logout Settings**.
3. Select **Edit** for Advanced Settings.
4. Select **Limit Login Attempts of System Administrator**.
5. Enable **Limit Login Attempts of System Administrator**.
6. Enter 5 in Failed Login Attempt Limit.
7. Select **OK** twice.

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 **Password Rules**.
3. Enter 9 in Minimum Length.
4. Select **OK**.
5. 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 **SSL/TLS Settings**.
4. Enable **HTTP - SSL/TLS Communication**.
5. Enable **LDAP - SSL/TLS Communication**.
6. Select **OK**.
7. Select **Restart Now** if prompted.

NOTE :

- For secure operation, you should enable **Verify Remote Server Certificate**, and import the CA certificate according to the same procedure as "Import Machine Certificates".

Import Machine Certificates

Import the Certificates for SSL, IPSec, S/MIME.

1. Select **System**.
2. Select **Security**.
3. Select **Security Certificates**.
4. Select **Import**.
5. Select **Select**.
6. Select a certificate.
7. Enter **Password**, and enter **Retype Password** if necessary.
8. Select **Import**.
9. Select **Close**.

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 Google Cloud Print

For the secure operation of the machine, follow the procedure below to set **Google Cloud Print** to **Disabled**.

1. Select **Connectivity**.
2. Select **Google Cloud Print**.
3. Disable **Google Cloud Print**.
4. Select **OK**.
5. Select **Restart Later** 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**.
3. Disable **Port**.
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**.
3. Enable **Port**.
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**.
3. Disable **Port**.
4. Select **OK**.
5. 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**.
3. Disable **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**.
3. Disable **Port**.
4. Select **OK**.

5. Select **Restart Now** if prompted.

Set WSD Scan

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

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

Set CSRF

Follow the procedure below to configure the CSRF settings.

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

Set LDAP Server

Configure the LDAP server settings for directory service.

1. Select **Connectivity**.
2. Select **LDAP**.
3. Select **LDAP Servers / Directory Services**.
4. Set Server Information and Advanced Settings.
5. Select **OK**.
6. Select **Restart Later** if prompted.

Set User Role

Configure the user role settings for network authentication mode.

1. Select **Permission**.
2. Select **Roles**.
3. Select **Setup LDAP Permissions Groups**.
4. Select **LDAP**.
5. Select **OK**.
6. Select **Restart Now** if prompted.

7. On the **Permission** screen, select **Roles**.
8. Select **Edit LDAP Groups**.
9. Select **+**.
10. Enter an administrator group.

11. Select the search mark.
12. Select a searched group.
13. Select **Next**.
14. Select **System Administrator**.
15. Select **Next**.
16. Select **+**.
17. Enter a general user group.
18. Select the search mark.
19. Select a searched group.
20. Select **Next**.
21. Select **Basic User Role**.
22. Select **Next**.
23. Select **Basic Printing User Role**.
24. Select **Next**.

Set S/MIME

Enable the S/MIME communication to use the e-mail encryption and digital signature features.
Before making the S/MIME setting, you need to import an S/MIME certificate according to the same procedure as "Import Machine Certificates".
To use E-mail with this machine, the E-mail function needs to be enabled and configured.

1. Select **Connectivity**.
2. Select **S/MIME**.
3. Enable **S/MIME**.
4. Select **OK**.
5. Select **Restart Now** if prompted.

Set Email

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

1. Select **Apps**.
2. Select **Email**.
3. Select **Setup**.
4. Set Email Address for Device Email.
5. Select Server Address for SMTP Server.
6. Set Server Address.
7. Select **OK**.
8. Set a port number for Outgoing SMTP Port Number.
9. Select **OK**.
10. Select **Restart Later** if prompted.
11. Select **Encryption** for Scan To Apps General Settings.
12. Enable **Encrypt Email**.
13. Select **OK**.
14. Select **Restart Later** 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**.
4. Select **Not Allowed**.
5. Select **OK**.
6. Select **Restart Later** if prompted.

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**.
4. Enable this service.
5. Set a passcode.
6. Select **OK**.
7. Select **Restart Now** 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 Later** if prompted.

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 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.
4. Enter a time for Reset Device Website.
5. Select **OK**.
6. Select **Restart Later** if prompted.

Set Store Print

Follow the procedure below to configure the Store 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 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 Software Download

Follow the procedure below to configure the Software Download settings.

1. Select **System**.
2. Select **Software Update**.
3. Select **Disable**.
4. Select **Disable**.
5. Select **Restart Now** if prompted.

Set IPSec

Before setting **Digital Signature** for **IKE Authentication Method**, you need to import an IPSec certificate according to the same procedure as "Import Machine Certificates".

1. Select **Connectivity**.
2. Select **IPSec**.
3. Enable **IPSec**
4. Select **Preshared Key** or **Digital Signature** for IKE Authentication Method.
5. When you select **Preshared Key**, enter a preshared key of 9 or more characters in **Preshared Key** and **Retype Preshared Key**.
   When you select **Digital Signature**, select the certificate name in **Device Certificate**.
6. Enter the IP Address in Specify Destination IPv4 Address.
7. Enter the IP Address in Specify Destination Ipv6 Address.
8. Select **Enabled** or **Disabled** for Communicate with Non-IPSec Device.
9. Select **OK**.
10. Select **Restart Now** if prompted.

Set Overwrite Hard Disk

Follow the procedure below to configure the Data Overwrite settings.
This feature is only applicable to HDD Model.

1. Select **System**.
2. Select **Security**.
3. Select **Edit** for Disk Overwrite.
4. Enable **Data Overwrite After Job Completion**.
5. Select **OK**.
6. Select **Restart Now** if prompted.

3 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.

Login as System Administrator

Before configuring settings, a user must be authenticated with an administrator's ID and a password.

1. Select Log In on the control panel.
2. Select admin.
3. Enter the password from the keypad.
4. Select OK.

Set Fax Forwarding

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

1. Select Apps on the Device screen.
2. Select Fax.
3. Select Fax Forwarding.
4. Select Off.
5. Select OK.

4 Regular Review by Audit Log

This section describes the importing method of the Audit Log feature using the System Administrator client via Embedded Web Server.
The Audit Log is regularly reviewed by the Security Administrator, often with the aid of third party analyzing tools. The audit log helps to assess attempted security breaches, identify actual breaches, and prevent future breaches.
The important events of the machine such as device failure, configuration change, and user operation are traced and recorded based on when and who operated what function.
Auditable events are stored with time stamps into the internal storage device. 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.
There is no deletion function.

Import the Audit Log File

The following describes methods for importing 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** on the Internet Service.
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**.

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	-

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 machine calculates the checksum of Controller ROM to confirm if it matches the specified value, and displays an error on the control panel at error occurrence.

6 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.

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. 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. 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.

Login Method

Local Authentication (Login to Local Accounts)

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

Remote Authentication (Login to Network Accounts)

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

Functions Controlled by 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)

Remote Access (Device Website Permissions)

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.

- Address Book
- AirPrint (Scan)
- Copy
- Device
- Email
- Fax
- ID Card Copy
- Jobs
- My Folder
- Remote Scanning
- Scan To
- Scan to Desktop
- USB

Remote Access (Device Website Permissions)

Operation of the machine through a network using Embedded Web Server is called Remote Access. The functions restricted by Remote Access are as follows.

Everything Except Setup

Users can access everything except: Apps, Connectivity, Permissions, and System

Home Only

Users only have access to the Home page.

Custom Permissions

Users can choose the services to be customized: Address Book or Jobs

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.

Maximum Login Attempts by System Administrator

This feature protects the settings from being changed by someone impersonating your system administrator. If authentication for a system administrator's ID fails 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.

7 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”.
- When using Network Authentication, the user information registered on a remote authentication server is used. The System Administrator's ID on the machine is not registered on a remote authentication server.

Job Deletion by Authenticated Users

This feature allows only authenticated users to delete the active jobs.
Cancels the current or pending job. Select a table row or status indicator that you want to delete. Then select the Delete button.

Deleting the Copy, Scan, Fax Send, Print job

1. Press the <home> button.
2. Select Jobs.
3. Select the job to be deleted.
4. Select Delete.

Deleting the receiving fax jobs, the spooling print jobs

1. Press the <home> button.
2. Select Jobs.
3. Select the job to be deleted.
4. Select Delete.

NOTE :

Only System Administrators are allowed this operation.

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.

8 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**.

NOTE :

- Enter the user name for the Network authentication. For the Local authentication, the user identification varies depending on the settings.
- When the Network authentication system is Kerberos, entering the realm or domain is required. For Kerberos, enter the user name and realm in the UPN format (<username>@<realm>).

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**.

Job Deletion by Authenticated Users

This feature allows only authenticated users to delete the active jobs.
Cancels the current or pending job. Select a table row or status indicator that you want to delete. Then select the **Delete** button.

Deleting the Copy, Scan, Fax Send, Print job

1. Log in to the **Embedded Web Server**.
2. Select **Jobs**.
3. Select the job to be deleted.
4. Select **Delete**.

Deleting the receiving Fax jobs, the spooling Print job

1. Log in to the **Embedded Web Server**.
2. Select **Jobs**.
3. Select the job to be deleted.
4. Select **Delete**.

NOTE :

Only System Administrators are allowed this operation.

9 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. RemedyCheck 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.

10 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/.

11 Appendix

List of Operation Procedures

	Using Control Panel	Using Embedded Web Server	Default
Check the Clock	Device > General > Date & Time	System > Date & Time	-
Change Password	-	Permissions > Change Password	-
Set EIP	-	Apps > EIP Settings	On
Set My Folder	-	Apps > My Folder	On
Set Dropbox	-	Apps > Print and Scan for Dropbox	On
Set GoogleDrive	-	Apps > Print and Scan for GoogleDrive	On
Set OneDrive	-	Apps > Print and Scan for OneDrive	On
Set Scan to Desktop	-	Apps > Scan to Desktop	On
Set USB	-	Apps > USB	On
Set App Gallery	-	Apps > Xerox App Gallery	On
Set Authentication	-	Permissions > Login/Logout Settings	Simple
Set Access Control （Guest user）	-	Permissions > Guest Access > Device User Role or Printing User Role	-
Set Access Control （Basic user）	-	Permissions > Roles > Device User Role or Printing User Role	-
Set Maximum Login Attempts	-	Permissions > Login/Logout Settings > Advanced Settings > Limit Login Attempts of System Administrator	5
Set User Password Minimum Length	-	Permissions > Password Rule > Length	4
Set TLS	Device > Connectivity > HTTPS	System > Security > SSL/TLS Settings	Off
Import Machine Certificates	-	System > Security > Security Certificates	-
Set Certificate Validation	-	System > Security > Certificate Path Validation	Off
Set Google Cloud Print	-	Connectivity > Google Cloud Print	On
Set Bonjour	-	Connectivity > Protocols	On
Set IPP	-	Connectivity > Protocols	On
Set SOAP	-	Connectivity > Protocols	On
Set SNMP	-	Connectivity > Protocols	On
Set SMB	-	Connectivity > Protocols	On
Set WSD(Scan)	-	Connectivity > Protocols	On
Set CSRF	-	Connectivity > Protocols > HTTP > CSRF Protection	Off

Set LDAP Server	Device > Connectivity > LDAP	Connectivity > Protocols > LDAP	-
Set User Role	-	Permissions > Roles > Setup LDAP Permissions Groups	-
Set S/MIME	-	Connectivity > Protocols	Off
Set Email	-	Apps > Email	Off
Set Direct Fax	-	Apps > Fax > General Settings and Policies	On
Set Secure Fax Receive	-	Apps > Fax > General Settings and Policies > Secure Fax Receive	Off
Set Service Representative Restricted Operation	-	System > Security > Customer Service Engineer Access Restriction	Off
Set Self Test	-	System > Security > Firmware Verification	Off
Set Auto Clear	Device > General > System Timeout	System > Timeouts	On
Set Store Print	-	System > Defaults and Policies > Printer Settings > Allowed Print Job Types	All Jobs
Set Audit Log	-	System > Logs > Audit Logs	Off
Set Software Download	-	System > Software Update	On
Set IPSec	-	Connectivity > Protocols	Off
Set Overwrite (HDD Model only) Hard Disk	-	System > Security	Off
Set Fax Forwarding	Device > Apps > Fax	-	Off

List of Product Codes

Model or Option	Product Code	Applicable USB initial kit
Xerox VersaLink B7025	TL200653(Diskless) TL200654(Diskless) TL200662(Diskless) TL200655 TL200656 TL200663 TL200657 TL200658 TL200664	EC103358, EC103360, EC103361, EC103362, EC103363
Xerox VersaLink B7030	TL200653(Diskless) TL200654(Diskless) TL200662(Diskless) TL200655 TL200656 TL200663 TL200657 TL200658 TL200664	EC103364, EC103366, EC103367, EC103368, EC103369
Xerox VersaLink B7035	TL200653(Diskless) TL200654(Diskless) TL200662(Diskless) TL200655 TL200656 TL200663 TL200657 TL200658 TL200664	EC103370, EC103372, EC103373, EC103374, EC103375
3 Line Fax Kit	EC103351	N/A
HDD Kit (HDD Model Only)	EC103355	N/A