Version 1.0
May 2013

Xerox® Color 560/570 Printer

Security Function Supplementary Guide

Table of Contents

1. Before Using the Security Function

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

Preface

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

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

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

Xerox® Color 550/560/570 Printer System Administrator Guide:
Version 1.0 May 2013

Xerox® Color 550/560/570 Printer User Guide:
Version 1.0 May 2013

The security features of the Xerox® Color 560/570 Printer are supported by the following ROM versions.

Controller+PS ROM	Ver. 1.208.1
IOT ROM	Ver. 64.19.0
IIT ROM	Ver. 6.16.1
ADF ROM	Ver. 12.11.0

Important:

The machine has obtained IT security certification for Common Criteria EAL3+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 user documentation 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.

Security Features

Xerox® Color 560/570 Printer has the following security features:

- Hard Disk Data Overwrite
- Hard Disk Data Encryption
- User Authentication
- System Administrator's Security Management
- Customer Engineer Operation Restriction
- Security Audit Log
- Internal Network data protection
- Self-Test
- Information Flow Security

Settings for the Secure Operation

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

Item	Description
Passcode Entry from Control Panel	Set to [Enabled].
The System Administrator Passcode	Change the system administrator passcode to another passcode of 9 or more characters.
Maximum Login Attempts	Default [5] Times.
Service Representative Restricted Operation	Set to [On], and enter a passcode of 9 or more characters.
Overwrite Hard Disk	Default [3 Overwrites].
Data Encryption	Default [On].
Scheduled Image Overwrite	Set to [Enabled].
Authentication	Set to [Login to Local Accounts] or [Login to Remote Accounts].
Access Control	Set to [Locked] for Device Access and Service Access.
Private Print	Set to [Save as Private Charge Print].
User Passcode Minimum Length	Set to [9] characters.
Direct Fax	Set to [Disable]: when remote authentication is used.
Auto Clear	Default [Enabled].
Report Print	Set to [Disable].
Self-Test	Set to [Enabled].
Software Download	Set to [Disabled].
SMB	Set to [Disabled] for [NetBEUI].
Receive E-mail	Default [Disabled].

WebDAV	Set to [Disabled].
IPP	Default [Enabled].
SSL/TLS	Set to [Enabled].
IPSec	Set to [Enabled].
SNMPv1/v2c	Set to [Disabled].
SNMPv3	Set to [Enabled].
S/MIME	Set to [Enabled].
Audit Log	Set to [Enabled].
Browser Refresh	Set to [Disabled].
Job Deletion	Set to [Administrator Only].

Important:

The security will not be effective if you do not correctly follow the above setting instructions.
The Information Flow Security feature requires no special settings by System Administrator.
When you set Data Encryption [On] again, enter an encryption key of 12 characters.

Data Restoration

The enciphered data cannot be restored in the following conditions.

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

Starting Use of the Data Encryption Feature and Changing the Settings

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

The recording area stores the following data:

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

Important:

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

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

Use of the Overwrite Hard Disk

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

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

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

Important:

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

Service Representative Restricted Operation

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

For the Color 560/570 Printer, select [On] and then set [Maintenance Passcode] to restrict the Service Representative from entering the System Administration mode.

Important:

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

For Optimal Performance of the Security Features

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

- The manager needs to assign appropriate people as system and machine administrators, and manage and train them properly.
- The manager and system administrators need to train users about the security policies and procedures of their organization.

- The machine needs to be placed in a secure or monitored area where the machine is protected from unmanaged physical access.
- If the network where the machine is installed is to be connected to external networks, configure the network properly to block any unauthorized external access.
- The users must set a user ID and a passcode on [Accounting Configuration] of printer driver.
- Users and administrators need to set passcodes and an encryption key according to the following rules for the client PC login and the machine's setup:

  - Do not use easily guessed character strings for passcodes.

  - A passcode needs to contain both numeric and alphabetic characters.
- Users and administrators need to manage and operate the machine so that their user IDs and passcodes may not be disclosed to another person.
- Administrators need to set the account policy in the remote authentication server as follows:

  - Set password policy to [9 or more characters].

  -Set account lockout policy to [5 times].
- For secure operation, all of the remote trusted IT products that communicate with the machine shall implement the communication protocol in accordance with industry standard practice with respect to RFC/other standard compliance (SSL/TLS, IPSec, SNMPv3, S/MIME) and shall work as advertised.
- The settings described below are required for both the machine's configuration and the client's configuration.

  1) SSL/TLS

     For the SSL client (Web browser) and the SSL server that communicate with the machine, select a data encryption suite from the following:
     - SSL_RSA_WITH_RC4_128_SHA
     - SSL_RSA_WITH_3DES_EDE_CBC_SHA
     - TLS_RSA_WITH_AES_128_CBC_SHA
     - TLS_RSA_WITH_AES_256_CBC_SHA

     (The recommended browser is Microsoft® Internet Explorer 6/7/8/9)

  2) S/MIME

     For the machine and e-mail clients, select an Encryption Method/Message Digest Algorithm from the following:
     - RC2 (128bit)/SHA1
     - 3Key Triple-DES (168bit)/SHA1

  3) IPSec

     For the IPSec host that communicates with the machine, select an Encryption Method/Message Digest Algorithm from the following:
     - AES (128bit)/SHA1
     - 3Key Triple-DES (168bit)/SHA1

  4) SNMPv3

     The encryption method of SNMPv3 is fixed to DES. Set [Message Digest Algorithm] to [SHA1].

Important:

- For secure operation, while you are using the Xerox® CentreWare® Internet Services, do not access other web sites.
- For secure operation, when you change [Authentication Type], initialize the hard disk by resetting [Data Encryption] and changing [encryption key].

- For preventing SSL vulnerability, you should set the machine address in the proxy exclusion list of browser.
  With this setting, secure communication will be ensured because the machine and the remote browser communicate directly without proxy server, and thus you can prevent man-in-the-middle attacks.

Confirm the Machine ROM Version and the System Clock

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

How to Check by Control Panel

1. Press the <Machine Status> button on the control panel.
2. Select [Machine information] on the touch screen.
3. Select [Software Version] on the [Machine information] screen.
4. You can identify the software versions of the components of the machine on the screen.

How to Check by Print Report

1. Press the <Machine Status> button on the control panel.
2. Select [Print Reports] on the [Machine information] screen.
3. Select [Printer Reports] on the touch screen.
4. Select [Configuration Reports].
5. Press the <Start> button on the control panel.
6. You can identify the software versions of the components of the machine by Print Report.

How to Check the System Clock

1. Press the <Log In/Out> button on the control panel.
2. Enter the System Administrator's Login ID and the passcode if prompted
3. Select [Enter] on the touch screen.
4. Press the <Machine Status> button on the control panel.
5. Select [Tools] on the touch screen.
6. Select [System Settings].
7. Select [Common Service Settings].
8. Select [Machine Clock/Timers].

You can check the time and the date of the internal clock. If you need to change the time and the date, refer to the following procedures.

9. Select the required option.
10. Select [Change Settings].
11. Change the required setting. Use the scroll bars to switch between screens.
12. Select [Save].

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.

Authentication for Entering the System Administration Mode

1. Press the <Log In/Out> button on the control panel.
2. Enter the system administrator's ID with the keyboard displayed.
3. Select [Next] on the touch screen.
4. Enter the system administrator's passcode from the keyboard when passcode is required.
5. Select [Enter] on the touch screen.
6. Press the <Machine Status> button on the control panel.
7. Select [Tools].

Use Passcode Entry from Control Panel

1. Select [Authentication/Security Settings] on the [Tools] screen.
2. Select [Authentication].
3. Select [Passcode Policy].
4. On the [Passcode Policy] screen, select [Passcode Entry from Control Panel].
5. Select [Change Settings].
6. On the [Passcode Entry from Control Panel] screen, select [On].
7. Select [Save].
8. To exit the [Passcode Policy] screen, select [Close].

Change the System Administrator's Passcode

1. Select [Authentication/Security Settings] on the [Tools] screen.
2. Select [System Administrator Settings].
3. Select [System Administrator's Passcode].
4. Select [New Passcode].
5. Enter a new passcode of 9 or more characters using the keyboard displayed, and then select [Save].
6. Select [Retype Passcode].
7. Enter the same passcode, and then select [Save].
8. Select [Save].
9. A confirmation window appears. Select [Yes] to confirm your entry.

Set Maximum Login Attempts

1. Select [Authentication/Security Settings] on the [Tools] screen.
2. Select [Authentication].
3. Select [Maximum Login Attempts By System Administrator].
4. On the [Maximum Login Attempts] screen, select [Limit Attempts].
5. With [▲] and [▼], set [5].
6. Select [Save].

Set Service Representative Restricted Operation

1. Select [System Settings] on the [Tools] screen.
2. Select [Common Service Settings].
3. Select [Other Settings].
4. On the [Other Settings] screen, select [Service Rep. Restricted Operation].
5. Select [Change Settings].
6. Select [On].
7. Select [Maintenance Passcode].
8. Select [New Passcode].
9. Enter a new passcode of 9 or more characters by using the keyboard displayed, and then select [Save].
10. Select [Save].
11. Select [Retype Password/Passcode].

12. Enter the same passcode by using the keyboard displayed, and then select [Save].
13. Select [Save].
14. Select [Yes] to apply the change.
15. A confirmation window appears. Select [Yes] to confirm your entry.
16. To exit the [Other Settings] screen, select [Close].

Set Overwrite Hard Disk

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

Set Scheduled Image Overwrite

1. Select [Authentication/Security Settings] on the [Tools] screen.
2. Select [Overwrite Hard Disk].
3. Select [Scheduled Image Overwrite].
4. On the [Scheduled Image Overwrite] screen, select [Daily], [Weekly], or [Monthly].
5. Set [Day], [Hour],and [Minutes],
6. Select [Save].

Set Data Encryption

1. Select [System Settings] on the [Tools] screen.
2. Select [Common Service Settings].
3. Select [Other Settings].
4. On the [Other Settings] screen, select [Data Encryption].
5. Select [Change Settings].
6. Select [On].
7. Select [New Encryption Key].
8. Enter a new encryption key of 12 characters by using the keyboard displayed, and then select [Save].
9. Select [Re-enter the Encryption Key]
10. Enter the same passcode, and then select [Save].
11. Select [Save].
12. Select [Yes] to apply the change.

13. Select [Yes] to reboot.

Set Authentication

1. Select [Authentication/Security Settings] on the [Tools] screen.
2. Select [Authentication].
3. Select [Login Type].
4. On the [Login Type] screen, select [Login to Local Accounts] or [Login to Remote Accounts].
5. Select [Save].

When [Login to Remote Accounts] is selected in step 4, proceed to steps 6 to 12.

6. Select [System Settings] on the [Tools] screen.
7. Select [Connectivity & Network Setup].
8. Select [Remote Authentication Server Setting].
9. Select [Authentication System Setup].
10. Select [Authentication System].
11. Select [Change Settings].
12. On the [Authentication System] screen, select [LDAP] or [Kerberos].
13. Select [Save].
14. To exit the [Remote Authentication Server Setting] screen, select [Close].

Set Access Control

1. Select [Authentication/Security Settings] on the [Tools] screen.
2. Select [Authentication].
3. Select [Access Control].
4. Select [Device Access].
5. On the [Device Access] screen, select [Locked] for [Service Pathway], [Job Status Pathway], and [Machine Status Pathway].
6. Select [Save].
7. Select [Service Access].
8. On the [Service Access] screen, select an item and then select [Change Settings].
9. Select [Locked].
10. Select [Save].

Perform steps 8 and 10 for each item.

11. Select [Close].
12. Select [Feature Access].
13. On the [Feature Access] screen, select an item by [Change Settings].
14. Select [Locked].

15. Select [Save].

Perform steps 13 and 15 for each item.

16. To exit the [Access Control] screen, select [Close].

Set Private Print

1. Select [Authentication/Security Settings] on the [Tools] screen.
2. Select [Authentication].
3. Select [Charge/Private Print Settings].
4. On the [Charge/Private Print Settings] screen, select [Received Control].
5. Select [Change Settings].

When [Login to Local Accounts] is selected

1) On the [Receive Control] screen, select [According to Print Auditron].
2) Select [Save As Private Charge Print Job] for [Job Login Success].
3) Select [Delete Job] for [Job Login Failure].
4) Select [Delete Job] for [Job without User ID].

When [Login to Remote Accounts] is selected

1) On the [Receive Control] screen, select [Save As Private Charge Print Job].

6. Select [Save].
7. To exit the [Charge/Private Print Settings] screen, select [Close].

Set User Passcode Minimum Length

This feature is only available in Local Authentication mode.

1. Select [Authentication/Security Settings] on the [Tools] screen.
2. Select [Authentication].
3. Select [Passcode Policy].
4. On the [Passcode Policy] screen, select [Minimum Passcode Length].
5. Select [Change Settings].
6. On the [Minimum Passcode Length] screen, select [Set].
7. With [▲] and [▼], set [9].
8. Select [Save].
9. To exit the [Passcode Policy] screen, select [Close].

Set Direct Fax

When remote authentication is used, use the following procedure to set [Direct Fax] to [Disabled].

1. Select [System Settings] on the [Tools] screen.
2. Select [Fax Service Settings].
3. Select [Fax Control].
4. Select [Direct Fax].
5. Select [Change Settings].
6. Select [Disabled].
7. Select [Save].
8. To exit the [Fax Control] screen, select [Close].

Set Auto Clear

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

Set Report Print

1. Select [System Settings] on the [Tools] screen.
2. Select [Common Service Settings].
3. Select [Reports].
4. Select [Print Reports Button].
5. Select [Disabled].
6. Select [Save].
7. To exit the [Reports] screen, select [Close].

Set Self Test

1. Select [System Settings] on the [Tools] screen.
2. Select [Common Service Settings].
3. Select [Maintenance].
4. Select [Power on Self Test].
5. Select [On].
6. Select [Save].
7. To exit the [Maintenance] screen, select [Close].

Set Software Download

1. Select [System Settings] on the [Tools] screen.
2. Select [Common Service Settings].
3. Select [Other Settings].
4. On the [Other Settings] screen, select [Software Download].
5. Select [Change Settings].
6. Select [Disabled].
7. Select [Save].
8. To exit the [Common Service Settings] screen, select [Close].
9. To exit the [Tools] screen, press the <Services> button on the control panel.
10. Select [Reboot now] on the confirmation screen.

3. Initial Settings Procedures Using Xerox® CentreWare® Internet Services

This section describes the initial settings related to Security Features, and how to set them on Xerox® CentreWare® Internet Services.

Preparations for Settings on the Xerox® CentreWare® Internet Services

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

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

Set SMB

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

Set WebDAV

When Remote Authentication is used, follow the procedure below to set [WebDAV] to [Disabled].

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

Set Receive E-mail

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

Set IPP

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

Set LDAP Server

1. Click [Connectivity] on the [Properties] screen.
2. Click [Protocols].
3. Click [LDAP].
4. Select [LDAP Server].
5. On each menu, set the LDAP server information.
6. Click [Apply].

Note:

You can configure the settings of the administrator group on the machine so that the members of that group have the System Administrator authority to access to the machine.

In the [System Administrator Access Group] boxes, enter a name for the group. Entries should be in base DN format (for instance, cn=admin, cn=users, dc=xerox, dc=com).

You can also restrict the use of the Copy, Scan, Print, and other features by entering a name for the group in the [Service Access Group] boxes.

Set Kerberos Server

1. Click [Security] on the [Properties] screen.
2. Click [Remote Authentication Servers].
3. Select [Kerberos Server].
4. On each menu, set the Kerberos server information.
5. Click [Apply].

Note:

When a Kerberos server is used as a remote authentication server, you can configure the settings of the administrator group on the machine by setting the [System Administrator Access Group] for the LDAP server.

Set SSL/TSL

1. Click [Security] on the [Properties] screen.
2. Click [Machine Digital Certificate Management].
3. Click [Create New Self Signed Certificate].
4. Select [Self-Signed Certificate] and Click the [Continue].
5. Set the size of the Public Key to [1024Bits].
6. Set Issuer as necessary.
7. Click [Apply].
8. Click [SSL/TLS Settings].
9. Select the [Enabled] check box for [HTTP - SSL/TLS Communication] and [LDAP- SSL/TLS Communication].
10. Click [Apply].
11. Click [Reboot Machine].

Note:

For secure operation, check the [Enabled] box for [Verify Remote Server Certificate], and import the CA certificate according to the same procedure as that in "Configuring Machine Certificates."

If SMTP server has SSL/TLS function and if you want to use secure e-mail, configure [SMTP- SSL/TLS Communication].

Configuring Machine Certificates

1. Click [Security] on the [Properties] screen.
2. Click [Machine Digital Certificate Management].
3. Click [Upload Signed Certificate].
4. Enter a file name for the file you want to import, or select the file to be imported by clicking [Browse].
5. Enter a password in [Password], and then retype the password in [Retype Password] for confirmation.
6. Click [Import].

Set IPSec

Before setting [Digital Signature] for [IKE Authentication Method], you need to import an IPSec certificate according to the same procedure as that in "Configuring Machine Certificates."

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

For the [Pre-Shared Key] setting, proceed to steps 4 and 5.

For the [Digital Signature] setting, proceed to steps 6 through 11.

4. Select [Pre-Shared Key] for [IKE Authentication Method].

This is used to ensure confidentiality of communications between the machine and a client computer, or the machine and a server.

5. Enter a Pre-Shared Key in the [Shared Key] box and the [Verify Shared Key] box.

Next, proceed to set the IPSec address.

6. Click [Certificate Management] in [Security].
7. Select [IPSec] for Certificate Purpose.
8. Click [Display the list], and check a desirable certificate.
9. Click [Certificate Details].
10. Click [Use this certificate].
11. On the [IPSec] screen, select [Digital Signature] for IKE Authentication Method.

Next, proceed to set the IPSec address.

Set IPSec Address

1. Enter the IP Address in the [Specify Destination IPv4 Address] box on the [IPSec] screen.
2. Enter the IP Address in the [Specify Destination Ipv6 Address] box.
3. Select [Enabled] or [Disabled] from the [Communicate with Non-IPSec Device] dropdown list.

4. Click [Apply].
5. Click [Reboot Machine].

Note:

When you select [Enabled] from the [Communicate with Non-IPSec Device] dropdown list, the machine allows communications with non-IPSec devices other than the devices that are specified in [Specify Destination IPv4 Address] or [Specify Destination IPv6 Address].

Set SNMPv3

1. Click [Connectivity] on the [Properties] screen.
2. Click [Protocols].
3. Click [SNMP Configuration].
4. Check the [Enable SNMPv3 Protocol] box.
5. Uncheck the [Enable SNMPv1/v2c Protocols] box.
6. Click [Apply].
7. Click [Edit SNMPv3 Properties] and check [Account Enabled] for [Administrator Account].
8. Enter a new Authentication Password (minimum 8 characters).
9. Enter the new Authentication Password again to confirm it.
10. Enter a new Privacy Password (minimum 8 characters).
11. Enter the new Privacy Password again to confirm it.
12. Check [Account Enabled] for [Print Drivers/Remote Clients Account].
13. Click [Apply].

Note:

Be sure to change Authentication Password and Privacy Password from the default password.

In using SNMPv3, use the IPSec protocol simultaneously. You need to set the IP address of the client for SNMPv3 according to the procedures in "Set IPSec Address" and enter the IP Address in the [Specify Destination IPv4/IPv6 Address] box.

Since the machine cannot communicate by SNMPv1/v2, you need to uncheck [SNMP status Enabled] for the port setting on the client's printer driver.

Set S/MIME

To use e-mail with this machine, the e-mail function needs to be enabled and configured as described in the System Administrator Guide's "Scan to E-mail."

Before making the S/MIME setting, you need to import an S/MIME certificate according to the same procedure as that in "Configuring Machine Certificates."

1. Click [Configuration Overview] on the [Properties] screen.
2. Click [Settings] for [E-mail].
3. Click [Configure] for [E-mail Settings], and enter the machine's E-mail address in the [From address] box.
4. Click [Apply].
5. Click [Security] on the [Properties] screen.
6. Click [Certificate Management].
7. Select [S/MIME] for [Certificate Purpose].
8. Click [Display the list], and check a desirable certificate.
9. Click [Certificate Details].
10. Click [Use this certificate].
11. Click [SSL/TLS Settings].
12. Check the [Enabled] box for [S/MIME Communication].
13. Click [Apply].
14. Click [Reboot Machine].

After the machine is restarted, refresh the browser and click the [Properties] tab.

15. Click [Security].
16. Click [S/MIME Settings].
17. Uncheck the [Enabled] check box for [Receive Untrusted E-mail].
18. Select [Always add signature] for [Digital Signature - Outgoing E-mail].
19. Click [Apply].

Set Browser Refresh

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

Set Job Deletion

1. Click [General Setup] on the [Properties] screen.
2. Click [Job Management].
3. Select [Administrators Only] for [Job Deletion].
4. Click [Apply].
5. Click the [Reboot Machine] button.

Important:

This feature allows the user to pause an active copy, print, scan job while it is being processed by the machine.

But only system administrators can cancel the paused job. For secure operation, please delete the job completely.

Set Audit Log

1. Open your Web browser, enter the TCP/IP address of the machine in the Address or Location field, and press the <Enter> key.
2. Enter the Administrator ID and the password, when prompted.
3. Click the [Properties] tab.
4. Click [Security].
5. Click [Audit Log].
6. Check the [Enabled] box for [Audit Log].
7. Click [Apply].

4. Regular Review by Audit Log

This section describes the setting procedure and the importing method of the Audit Log feature using the System Administrator client via Xerox® CentreWare® Internet Services.

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 NVRAM. When the number of stored events reaches 50, the 50 logs on NVRAM are stored into one file ("audit log file") within the internal HDD. 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 Xerox® CentreWare® Internet Services for viewing and analyzing.

The logged data cannot be viewed from the local UI.

In addition, SSL/TLS communication must be enabled in order to access to 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. Enter the Administrator ID and the password, when prompted.
3. Click the [Properties] tab.
4. Click [Audit Log].
5. Click [Export as text file].

5. Self Testing

This section describes the Self Test function.

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

The machine verifies the area of NVRAM and SEEPROM including setting data at initiation, and displays an error on the control panel at error occurrence.

However, an error is not detected for the data on audit logs and time and date as these are not included in the target.

Also, when Self Test function is set at initiation, the 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.

Note:

If any abnormal condition such as internal program modification is found during the program diagnosis, the machine stops starting up and records the information in the audit log.

The information may not be recorded in the audit log depending on the status of program malfunction.

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.

Overview of Authentication

Users Controlled by Authentication

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

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

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

Machine Administrator

The Machine Administrator uses a special user ID.

Only the Machine Administrator is able to change the Machine Administrator ID, and the Machine Administrator Passcode.

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

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

Authenticated Users (with System Administrator Privileges)

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

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

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

- Operating Folder and job flow sheets
- Changing the passcode of the Machine Administrator.

Authenticated Users (with No System Administrator Privileges)

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

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

Unauthenticated Users

These are users who are not registered with the machine.

An Unauthenticated User cannot use services that are restricted.

Local Machine Authentication (Login to Local Accounts)

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

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

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

Remote Authentication (Login to Remote Accounts)

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

Functions Controlled by Authentication

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

- Local Access
- Remote Access

For more information on the restrictions on the operations on Folder and job flow sheets using the Authentication feature, refer to “Authentication for Job Flow Sheets and Folder”.

Local Access

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

Device Access

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

Service Access

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

Feature Access

- Print File from Folder
- Retrieve File from Folder

Service Access control per user

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

The system administrator can limit print & copy quota per user via the control panel and Xerox® CentreWare® Internet Services.

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

Remote Access

Operation of the machine through a network using Xerox® CentreWare® Internet Services is called Remote Access.

The functions restricted by Remote Access are as follows.

Print

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

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

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

Xerox® CentreWare® Internet Services

If the Authentication feature is enabled, authentication is required to access the Xerox® CentreWare® Internet services home page even if you are not using the Authentication feature for any service.

Authentication for Folder

The following explains the restricted operations on job flow sheets and Folder when the Authentication feature is enabled.

Note:

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

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

Types of Folder

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

Machine Administrator Shared Folder

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

Only the Machine Administrator can change the settings.

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

Personal Folder

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

Operations available for Folder

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

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

Store File		✓	✓	-
Print File		✓	✓	-
Job Flow Sheet	Display	✓	✓	-
	Link	-	✓	-
	Auto Run	✓	✓	-
	Manual Run	✓	✓	-

Folder Operation		Machine Administrator	
		Machine Administrator Shared Folder	Personal Folder
Create		✓	-
Display		✓	✓
Delete		✓	✓
Change Settings		✓	✓
Display File		✓	✓
Delete File		✓	✓
Store File		✓	✓
Print File		✓	✓
Job Flow Sheet	Display	✓	✓
	Link	✓	✓
	Auto Run	✓	✓
	Manual Run	✓	✓

✓ : Operation available

- : Operation not available

Note:

When job flow sheets not available for operation, depending on changes made to the authentication status, are linked to a Folder, you can still use them except for changing/copying them. If you remove the link, the job flow sheets will no longer be displayed and will be disabled.

7. Operation Using Control Panel

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

User Authentication

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

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

All features on the control panel become available.

Important:

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

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

Note:

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

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

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

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

Create/View User Accounts

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

On the Tools screen

1. Select [Create/View User Accounts] under [Authentication].
2. Select a User ID number.
3. Press [Create/Delete].
4. When a new user account is to be created, a keyboard screen is displayed. Enter a user ID, and then select [Save].
5. Configure the required settings.
6. Select [Close].

User ID

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

User Name

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

Passcode

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

Note:

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

E-mail Address

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

Note:

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

Account Limit

Displays the [Account No. XXX - Account Limit] screen. Select [Copy Service], [Scan Service] or

[Print Service] to specify feature access permissions and account limits for that service.

Feature Access - Displays the [Account No. xxx - Feature Access] screen. Select the access permissions for each service for that account.

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

User Role

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

Note:

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

Reset Total Impressions

Deletes all the data tracked for the selected account.

Reset Account

Clears all settings and data for the selected account.

Change User Passcode by General User

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

This feature is only applicable to Local Authentication mode.

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

Job Deletion by System Administrator

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

Deleting the Copy, Scan job

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

Deleting the printing Job

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

Deleting the sending Scan Job

1. On the control panel, press [Job Status] button. The Active Jobs tab displays.

2. Touch the desired job, then press [Delete] from the pop-up menu.

Folder / Stored File Settings

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

Folder Service Settings

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

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

Files Retrieved By Client

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

Print & Delete Confirmation Screen

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

Quality/File Size for Retrieval

Specifies the Quality/File Size level.

Stored File Settings

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

You can also select whether to delete individual files.

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

Expiration Date for Files in Folder

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

Stored Job Expiration Date

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

Note:

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

Print Order for All Selected Files

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

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

Create Folder

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

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

Note:

By selecting [Delete Folder], you can delete all files in the Folder and all job flow sheets created through the Folder.

Folder Name

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

Delete Files after Retrieval

Specifies whether to delete files in the Folder after they are printed out or retrieved, or after they are transferred and printed out through a Job Flow sheet.

Delete Expired Files

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

Send from Folder

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

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

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

File Name/ Date & Time

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

Refresh

Updates the list of files in the Folder.

Select All

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

Print

Prints the selected file(s).

Delete

Deletes the selected file(s).

Private Charge Print

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

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

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

Note:

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

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

Refresh

Refreshes the displayed information.

Select All

Selects all the files in the list.

Delete

Deletes a file selected in the list.

Print

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

Note:

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

8. Operation Using Xerox® CentreWare® Internet Services

This section describes the operation using Xerox® CentreWare® Internet Services to use security features for System Administrator and authenticated users.

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

Note:

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

Accessing Xerox® CentreWare® Internet Services

Follow the steps below to access Xerox® CentreWare® Internet Services. 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 Xerox® CentreWare® Internet Services 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 Xerox® CentreWare Internet Services to configure and use the security functions of the machine.

When your access to Xerox® CentreWare Internet Services is encrypted, enter https:// followed by the IP address or the Internet address, instead of "http://".

Print

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

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

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

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

Scan (Folder Operation)

This section describes how to configure Folder.

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

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

Folder icons

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

Folder Number

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

Folder Name

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

Number of Files in this Folder

Displays the number of files stored in each Folder.

File List

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

Delete

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

Edit

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

Create

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

Folder: List of Files

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

Item		Description
Folder Number		Displays the Folder number of the selected Folder.
Folder Name		Displays the name of the selected Folder.
File Number		Displays the file numbers of the files stored in the
File Name		Displays the names of the files.
Date & Time		Displays the dates on which the files were stored.
Compression Format		Displays the compression formats of the files.
Page Count		Displays the page counts of the files.
Type		Displays the job types of the files.
Retrieve	Retrieve Page	Selects whether or not to retrieve one page of the
	Page Number	Enters the page number of the page to be retrieved.
	Retrieving	Specifies the file format to be used when retrieving the
Print File	Paper Supply	Selects the paper tray to be used to print the selected
	Output Destination	Selects the output tray.
	Quantity	Selects the number of copies to print.
	2 Sided Printing	Selects whether to print only on one side or both sides of
Delete		Deletes the selected files in the folder.

Edit Folder

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

Item		Description
Folder	Folder Number	Displays the number of the selected Folder.
	Folder Name	To change the Folder name, enter a new Folder name.
	Folder Passcode	To change the passcode, enter a new passcode with up to 20 characters. Leave the text box blank if you do not set a passcode.
	Retype Passcode	Re-type the passcode for verification.
	Check Folder Passcode	Allows you to select whether and when the passcode for the Folder is required.
	Owner	Displays the owner of the Folder. If the Folder is a shared
	Delete Files after Print or Retrieve	Allows you to set whether to automatically delete files after they are printed. Note: Retrieved files are not deleted.
	Delete Expired Files	Allows you to set whether to automatically delete files when they reach the specified expiration dates.
	Number of Files in this Folder	Displays the number of files stored in the Folder.
Link Job Flow Sheet to this Folder	Sheet Order	Select the display order of job flow sheets to be displayed in the [Job Flow Sheet List] page.

Folder Setup

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

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

Import the files

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

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

Note:

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

Printing Job Deletion

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

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

Change User Passcode by System Administrator (Using Xerox® CentreWare® Internet Services)

This feature is only applicable to Local Authentication mode.

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

9. Problem Solving

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

Fault Clearance Procedure

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

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

Caution:

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

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

Note:

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

Fault Codes

This section explains error codes.

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

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

Important:

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

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

Error Code	Cause and Remedy
016-210 016-211 016-212 016-213 016-214 016-215	[Cause] An error occurred in the software. [Remedy] Switch off the machine power, make sure that the touch screen is blank, and then switch on the machine power. If the error still is not resolved, contact our Customer Support Center.
016-402	[Cause] The authentication connection timed out. [Remedy] Confirm the network connection and switch setting of the authentication device physically connected to the machine via a network, and check whether it is connected to the machine correctly.
016-403	[Cause] The root certificate did not match. [Remedy] Confirm the authentication server and store the root certificate of the server certificate of the authentication server into the machine. If you cannot acquire the root certificate of the server certificate, set [Server Certificate Verification] of [IEEE 802.1x Settings] to [Disabled] on the touch screen.
016-405	[Cause] An error occurred in the certificate stored in the machine. [Remedy] Initialize the certificate.
016-406	[Cause] An error occurred in the SSL client certificate. [Remedy] Take one of the following measures: Store an SSL client certificate in the machine, and set it as the SSL client certificate. If the SSL client certificate cannot be set, select an authentication method other than SSL.
016-450	[Cause] The SMB host name already exists. [Remedy] Change the host name.
016-454	[Cause] Unable to retrieve the IP address from DNS. [Remedy] Confirm the DNS configuration and IP address retrieve setting.
016-503	[Cause] Unable to resolve the SMTP server name when sending e-mail. [Remedy] Check on the Xerox® CentreWare® Internet Services if the SMTP server settings are correct. Also, check the DNS server settings.
016-504	[Cause] Unable to resolve the POP3 server name when sending email. [Remedy] Check on Xerox® CentreWare® Internet Services if the POP3 server settings are correct. Also, check the DNS server settings. are correct.
016-505	[Cause] Unable to login to the POP3 server when sending e-mail. [Remedy] Check on Xerox® CentreWare® Internet Services if the user name and password used in the POP3 server are correct.
016-513	[Cause] An error occurred in connecting to the SMTP server. [Remedy] The SMTP server or network may be overloaded. Wait for a while, and then execute the operation again.

016-522	[Cause] LDAP server SSL authentication error. Unable to acquire an SSL client certificate. [Remedy] The LDAP server is requesting an SSL client certificate. Set an SSL client certificate on the machine.
016-523	[Cause] LDAP server SSL authentication error. The server certificate data is incorrect. [Remedy] The machine cannot trust the SSL certificate of the LDAP server. Register the root certificate for the LDAP server's SSL certificate to the machine.
016-524	[Cause] LDAP server SSL authentication error. The server certificate will expire soon. [Remedy] Change the SSL certificate of the LDAP server to a valid one. You can clear this error by selecting [Disabled] for [LDAP - SSL/TLS Communication] under [SSL/TLS Settings] on the machine; however, note that selecting this option does not ensure the validity of the LDAP server.
016-525	[Cause] LDAP server SSL authentication error. The server certificate has expired. [Remedy] Change the SSL certificate of the LDAP server to a valid one. You can clear this error by selecting [Disabled] for [LDAP - SSL/TLS Communication] under [SSL/TLS Settings] on the machine; however, note that selecting this option does not ensure the validity of the LDAP server.
016-526	[Cause] LDAP server SSL authentication error. The server name does not match the certificate. [Remedy] Set the same LDAP server address to the machine and to the SSL certificate of the LDAP server. You can clear this error by selecting [Disabled] for [LDAP - SSL/TLS Communication] under [SSL/TLS Settings] on the machine; however, note that selecting this option does not ensure the validity of the LDAP server.
016-527	[Cause] LDAP server SSL authentication error. This is an SSL authentication internal error. [Remedy] An error occurred in the software. Contact our Customer Support Center.
016-533	[Cause] Kerberos server authentication protocol error [Remedy] The time difference between the machine and the Kerberos server exceeded the clock skew limit value set on the Kerberos server. Check whether the clocks on the machine and Kerberos server are correctly set. Also check whether the summer time and the time zone are correctly set on the machine and Kerberos server.
016-534	[Cause] Kerberos server authentication protocol error [Remedy] The domain set on the machine does not exist on the Kerberos server, or the Kerberos server address set on the machine is invalid for connection. Check whether the domain name and the server address have been correctly set on the machine. For connection to Microsoft® Windows Server® 2003 or Microsoft® Windows Server®2008, specify the domain name in uppercase.
016-539	[Cause] Kerberos server authentication protocol error [Remedy] An error occurred in the software. Contact our Customer Support Center.
016-574	[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because the host or server name of the FTP server could not be resolved. [Remedy] Check the connection to the DNS server. Check if the FTP server name is registered correctly on the DNS server.
016-575	[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because the DNS server address was not registered. [Remedy] Specify the correct DNS server address. Or, specify the destination FTP server using its IP address.

016-576	[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because it could not connect to the FTP server. [Remedy] Ensure that both the destination FTP server and the machine are available for network communications, by checking the following: The IP address of the server is set correctly. The network cables are plugged in securely.
016-577	[Cause] Unable to connect to the FTP service of the destination server. [Remedy] Take one of the following actions: Check if the FTP service of the server is activated. Check if the FTP port number of the server is correctly registered on the machine.
016-578	[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature due to unsuccessful login to the FTP server. [Remedy] Check if the login name (user name and password are correct.
016-579	[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because the scanned image could not be saved in the FTP server after connection. [Remedy] Check if the FTP server's save location is correct.
016-580	[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because the file or folder name on the FTP server could not be retrieved after connection. [Remedy] Check the access privilege to the FTP server.
016-581	[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because the suffix of the file or folder name exceeded the limit after connection. [Remedy] Change the file name, or change the destination folder on the FTP server. Or, move or delete files from the destination folder.
016-582	[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because file creation was not successful on the FTP server after connection. [Remedy] Take one of the following actions: Check if the specified file name can be used in the save location. Check if enough space is available in the save location.
016-583	[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because lock folder creation was not successful on the FTP server after connection. [Remedy] Take one of the following actions: If any lock directory (.LCK) exists in the forwarding destination, delete it manually, then try executing the job again. Check if the specified folder name can be used in the save location. Check if the same folder name exists in the save location. Check if enough space is available in the save location.
016-584	[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because folder creation was not successful on the FTP server after connection. [Remedy] Take one of the following actions: Check if the specified folder name can be used in the save location. Check if the same folder name exists in the save location. Check if enough space is available in the save location.
016-585	[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because file deletion was not successful on the FTP server after connection. [Remedy] Check the access privilege to the FTP server.

016-586	[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because lock folder deletion was not successful on the FTP server after connection. [Remedy] Take one of the following actions: Check the access privilege to the FTP server. If any lock directory (.LCK) exists in the forwarding destination, delete it manually, then retry executing the job.
016-587	[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because folder deletion was not successful on the FTP server after connection. [Remedy] Check the access privilege to the FTP server.
016-588	[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because the data could not be written in the FTP server after connection. [Remedy] Check if enough space is available in the save location.
016-589	[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because the data could not be read from the FTP server after connection. [Remedy] Check the access privilege to the FTP server.
016-593	[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because an internal error occurred after connection to the FTP server. [Remedy] Try again. If the error persists, contact our Customer Support Center.
016-594 016-595 016-596	[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because a network error occurred. [Remedy] Try again. If the error persists, contact our Customer Support Center.
016-703	[Cause] The machine received e-mail which specified an invalid folder number. [Remedy] For errors occurring during e-mail reception: Take one of the following measures: Register the specified folder number, and request the sender to send the e-mail again. Request the sender to send to an available folder. If the error still is not resolved, contact our Customer Support Center.
016-704	[Cause] The folder is full, and hard disk capacity is insufficient. [Remedy] Delete unnecessary files from the folder, and save the file.
016-705	[Cause] Secure print documents cannot be registered because of hard disk malfunction. [Remedy]Contact the Customer Support Center. Refer to Secure Print.
016-706	[Cause] The hard disk space is insufficient because the number of Secure Print users exceeded the maximum limit. [Remedy] Delete unnecessary files from the machine, and delete unnecessary Secure Print users.
016-711	[Cause] The upper limit for the e-mail size has been exceeded. [Remedy] Take one of the following measures, and then try sending the mail again. Reduce the number of pages of the document. Lower the resolution with [Resolution]. Reduce the magnification with [Reduce/Enlarge]. Ask your system administrator to increase the value set for [Maximum Total Data Size]. For color scanning, set [MRC High Compression] to [On] under [File Format].
016-713	[Cause] The passcode entered does not match the passcode set on the folder. [Remedy] Enter the correct passcode.
016-714	[Cause] The specified folder does not exist. [Remedy] Create a new folder or specify an existing folder.
016-764	[Cause] Unable to connect to the SMTP server. [Remedy] Consult the SMTP server administrator.
016-765	[Cause] Unable to send the e-mail because the hard disk on the SMTP server is full. [Remedy] Consult the SMTP server administrator.

016-766	[Cause] An error occurred on the SMTP server. [Remedy] Consult the SMTP server administrator.
016-767	[Cause] Unable to send the e-mail because the address is not correct. [Remedy] Confirm the address, and try sending again.
016-768	[Cause] Unable to connect to the SMTP server because the machine's mail address is incorrect. [Remedy] Confirm the machine's mail address.
016-769	[Cause] The SMTP server does not support delivery receipts (DSN). [Remedy] Send e-mail without setting delivery receipts (DSN).
016-773	[Cause] The IP address of the machine is not set correctly. [Remedy] Check the DHCP settings. Or set the fixed IP address to the machine.
016-774	[Cause] Unable to process compression conversion because of insufficient hard disk space. [Remedy] Delete unnecessary data from the hard disk to free up disk space.
016-781	[Cause] Unable to connect to the SMTP server. Unable to establish a connection between the machine and the server. Although the connection between the machine and the server has been established, ASCII characters are not used for the host name specified on the machine. [Remedy] Take one of the following measures: Check whether the network cables are plugged in securely. Enter the host name using ASCII characters in [Tools] > [Connectivity & Network Setup] > [Machine's E-mail Address/Host Name].
016-788	[Cause] Failed to retrieve a file from the Web browser. [Remedy] Take one of the following measures, and then execute the operation again: Reload the browser page. Restart the browser. Switch off the machine power, make sure that the touch screen is blank, and then switch on the machine power.
016-791	[Cause] Failed to access to the destination computer or the save location for Network Scanning. [Remedy] Check the directory configuration and files on the server, the access privileges for the destination or the location, and check if you are authorized to access the specified destination computer or server.
018-400	[Cause] When IPSec is enabled, there is an inconsistency in IPSec settings as follows: The password is not set when [Authentication Method] is set to [Preshared Key]. An IPSec certificate is not set when [Authentication Method] is set to [Digital Signature]. [Remedy]Check the IPSec settings, and enable IPSec again: When [Authentication Method] is set to [Preshared Key], set the password. When [Authentication Method] is set to [Digital Signature], set an IPSec certificate.
018-405	[Cause] An error occurred during LDAP authentication. [Remedy] The account is disabled in the active directory of the authentication server, or the access is set to disabled. Consult your network administrator.
018-502	[Cause] The machine failed to transfer data using SMB of the Scan to PC service because computers allowed to login are restricted. [Remedy] Confirm the property information for the specified user, and check whether the computers allowed to login to the server are restricted.

018-505	[Cause] Failed to log into the destination computer while transferring data using SMB of the Scan to PC service. [Remedy] Check whether the user name and password of the SMTP server registered in the machine is correct.
018-543	[Cause] The machine failed to transfer data using SMB of the Scan to PC service because one of the following problems occurred on the shared name of the SMB server when logging in to the SMB server: The specified shared name does not exist on the server. Invalid characters are used in the specified shared name. When the server is Macintosh, the specified shared name may not have an access right. [Remedy] Confirm the specified shared name, and set the name correctly.
018-547	[Cause] The machine failed to transfer data using SMB of the Scan to PC service because the number of users logging into the SMB server exceeded the limit when logging in to the SMB server. [Remedy] Take one of the following measures: Confirm how many users can access the shared folder. Check whether the number of login users have exceeded the limit.
018-596	[Cause] An error occurred during LDAP server authentication. [Remedy] Execute the operation again. If the error still is not resolved, contact our Customer Support Center.
018-781	[Cause] An LDAP server protocol error occurred as a result of the Address Book operation. Connection to the server cannot be established for the Address Book query. [Remedy] Take one of the following measures: Confirm the network cable connection. If the network cable connection has no problem, confirm the active status of the target server. Check whether the server name has been correctly set for [LDAP Server/Directory Service Settings] under [Remote Authentication Server/Directory Service].
018-782 018-783 018-784 018-785 018-786 018-787 018-788 018-789 018-790 018-791 018-792 018-793 018-794 018-795 018-796 018-797	[Cause] An LDAP server protocol error occurred as a result of the Address Book operation. The server returned RFC2251 Result Message for Address Book query. [Remedy] Have your network administrator confirm the LDAP server status.
027-452	[Cause] IP address of IPv4 already exists. [Remedy] Change the IP address of IPv4 set on the machine or the IP address of IPv4 on the network device.
027-500	[Cause] Unable to connect to the SMTP server. [Remedy] Specify the SMTP server name correctly or specify the server by using its IP address.

027-706	[Cause] Unable to find the S/MIME certificate associated with the machine's e-mail address when sending e-mail. [Remedy] Import the S/MIME certificate corresponding to the mail address to the machine.
027-707	[Cause] The S/MIME certificate associated with the machine's email address has expired. [Remedy] Ask the sender to issue a new S/MIME certificate and import the certificate to the machine.
027-708	[Cause] The S/MIME certificate associated with the machine's email address is not reliable. [Remedy] Import a reliable S/MIME certificate to the machine.
027-709	[Cause] The S/MIME certificate associated with the machine's email address has been discarded. [Remedy] Import a new S/MIME certificate to the machine.
027-710	[Cause] No S/MIME certificate is attached to the received e-mail. [Remedy] Ask the sender to send the e-mail with an S/MIME certificate.
027-711	[Cause] No S/MIME certificate was obtained from the received e-mail. [Remedy] Import the sender's S/MIME certificate to the machine, or attach an S/MIME certificate to S/MIME signature mail sent from the sender.
027-712	[Cause] The received S/MIME certificate has expired, or is an unreliable certificate. [Remedy] Ask the sender to send the e-mail with a valid S/MIME certificate.
027-713	[Cause] The received e-mail has been discarded because it might be altered on its transmission route. [Remedy] Tell the sender about it, and ask to send the e-mail again.
027-714	[Cause] The received e-mail has been discarded because the address in its From field was not the same as the mail address in the S/MIME signature mail. [Remedy] Tell the sender that the mail addresses are not identical, and ask to send the e-mail again.
027-715	[Cause] The received S/MIME certificate has not been registered on the machine, or has not been set to use on the machine. [Remedy] Import the sender's S/MIME certificate to the machine, or change settings to use the S/MIME certificate on the machine when the S/MIME certificate has already been registered.
027-716	[Cause] The received S/MIME certificate has been discarded because the certificate was unreliable. [Remedy] Ask the sender to send the e-mail with a reliable S/MIME certificate.
027-717	[Cause] Unable to obtain SMTP server address for e-mail transmissions from the DNS server. [Remedy] Check whether the DNS server is set correctly.

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

Item	Using Control Panel	Using Xerox® CentreWare® Internet Services	Default
Check the Clock	[System Settings] > [Common Service Settings] > [Machine Clock/Timers].	-	-
Use Passcode Entry for Control Panel	[Authentication/Security Settings] > [Authentication] > [Passcode Policy] > [Passcode Entry from Control Panel]	-	Off
Change the System Administrator Passcode	[Authentication/Security Settings] > [System Administrator Settings] > [System Administrator's Passcode]	[Security] > [System Administrator Settings]	-
Set Maximum Login Attempts	[Authentication/Security Settings] > [Authentication > [Maximum Login Attempts By System Administrator]	[Security] > [System Administrator Settings]	5
Set Service Representative Restricted Operation	[System Settings] > [Common Service Settings] > [Other Settings] > [Service Rep. Restricted Operation].	[Security] > [Service Representative Restricted Operation]	Off
Set Overwrite Hard Disk	[Authentication/Security Settings] > [Overwrite Hard Disk]	-	On
Set Scheduled Image Overwrite	[Authentication/Security Settings] > [Overwrite Hard Disk] > [Scheduled Image Overwrite].	[Security] > [On Demand Overwrite] > [Scheduled]	Off
Run Image Overwrite	[Authentication/Security Settings] > [Overwrite Hard Disk] > [Run Image Overwrite]	[Security] > [On Demand Overwrite] > [Manual]	-
Set Data Encryption	[System Settings] > [Common Service Settings] > [Other Settings] > [Data Encryption]	-	On
Set Authentication	[Authentication/Security Settings] > [Authentication] > [Login Type]. [System Settings] > [Connectivity & Network Setup] > [Remote Authentication/Directory Service]	[Security] > [Authentication Configuration]	Off
Set Access Control	[Authentication/Security Settings] > [Authentication] > [Access Control]	[Security] > [Authentication Configuration] > [Next]> [Device Access] or [Service Access]	Off
Set Private Print	[Authentication/Security Settings] > [Authentication] > [Charge/Private Print Settings].	-	Off
Set User Passcode Minimum Length	[Authentication/Security Settings] > [Authentication] > [Passcode Policy] > [Minimum Passcode Length]	[Security] > [User Details Setup] > [Minimum Passcode Length]	0
Set Direct Fax	[System Settings] > [Fax Service Settings] > [Fax Control] > [Direct Fax]	-	On

Set Auto Clear	[System Settings]>[Common Service Settings] > [Machine Clock/Timers] > [Auto Clear]	-	On
Set Repot Print	[System Settings] > [Common Service Settings] > [Reports] > [Print Reports Button]	-	On
Set Self Test	[System Settings] > [Common Service Settings] > [Maintenance] > [Power on Self Test]	-	
Set Software Download	[System Settings] > [Common Service Settings] > [Other Settings] > [Software Download].	-	On
Set SMB	-	[Connectivity] > [Port Setting]	On
Set WebDAV	[System Settings] > [Connectivity & Network Setup] > [Port Setting]	[Connectivity] > [Port Setting]	On
Set Receive E-mail	[Connectivity & Network Setup] > [Port Setting]	[Connectivity] > [Port Setting]	Off
Set IPP	[System Settings] > [Connectivity & Network Setup] > [Port Setting]	[Connectivity] > [Port Setting]	On
Set LDAP	-	[Connectivity] > [Protocols] > [LDAP] > [LDAP Server]	-
Set Kerberos	-	[Security] > [Remote Authentication Servers] > [Kerberos Server]	-
Set SSL/TSL	[System Settings] > [Connectivity & Network Setup] > [Security Settings] > [SSL/TLS Settings]	[Security] > [SSL/TLS Settings]	Off
Configuring Machine Certificates	-	[Security] > [Machine Digital Certificate Management] > [Upload Signed Certificate].	-
Set IPSec	[System Settings] > [Connectivity & Network Setup] > [Security Settings] > [IPSec Settings]	[Security] > [IPSec]	Off
Set SNMPv3	-	[Connectivity] > [Protocols] > [SNMP Configuration]	Off
Set S/MIME	[System Settings] > [Connectivity & Network Setup] > [Security Settings] > [S/MIME Settings]	[Security] > [SSL/TLS Settings] > [S/MIME Communication]	Off
Set Browser Refresh	-	[General Setup] > [Internet Services Settings] > [Auto Refresh Interval]	On
Set Job Deletion	-	[General Setup] > [Job Management] > [Job Deletion]	All User
Set Audit Log, Import the Audit LogFile	-	[Security] > [Audit Log].	Off
Create/View User Account Change Service Acces per user	[Authentication/Security Settings] > [Authentication] > [Create/View User Accounts] > [Account Number]	[Security] > [Authentication Configuration] > [Next]> [Account Number] > [Edit]	-

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