Xerox 4112/4127 Copier/Printer
Security Function Supplementary Guide

Version 1.0, February 2010

Table of Contents

Before Using the Security Function

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.

And 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 4112/4127 Copier/Printer System Administration Guide

: Version 3.0 May 2009

Xerox 4112/4127 Copier/Printer User Guide

: Version 3.0 May 2009

Xerox 4112/4127 Copier/Printer is supported by the following ROM version.

Controller+PS ROM	Ver. 1.211.8
IOT ROM	Ver. 46.18.0
IIT ROM	Ver. 15.6.1
IIT Option ROM	Ver. 14.0.4
ADF ROM	Ver. 12.2.7

Important:

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

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.

Note, however, that your ROM and Guidance may not be the certified version because it may have been updated along with machine improvements.

Security Features

Xerox 4112/4127 Copier/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

Settings for the Secure Operation

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

Passcode Entry from Control Panel	Set to [On].
The System Administrator Passcode	Change the default passcode "x-admin" to another passcode of 9 or more characters.
Maximum Login Attempts	Default [5] Times.
Service Rep. Restricted Operation	Set to [On], and then enter a passcode of 9 or more characters.
Overwrite Hard Disk	Set to [1 Overwrite] or [3 Overwrites].
Data Encryption	Set to [On]
Scheduled Image Overwrite	Set to [Enabled].
Authentication	Set to [Login to Local Accounts]
Access Control	Set to [Locked] for Device Access , Service Access and Feature Access
Private Print	Set to [Save in Private Charge Print]
User Passcode Minimum Length	Set to [9] characters.
SMB	Set to [Disabled] for [NetBEUI]
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]

Important:

- The security will not be warranted if you do not correctly follow the above setting instructions.
- 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 trouble occurs in the hard disk.
- When you have forgotten the encryption key.
- When you have forgotten the System Administrator ID and a passcode when making [Service Rep. Restricted Operation] set 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 data stored on the hard disk from unauthorized retrieval, you can set the overwrite conditions to apply to data stored on the hard disk.

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

The setting 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. The overwriting operation will resume if you power the machine on again 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 4112/4127 Copier/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 user ID and passcode are lost when [Service Rep. Restricted Operation] is set to [On], not only you but also we are no longer 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:

- Assign appropriate persons as system and machine administrators, and manage and train them properly.
- 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 have to set a user ID and a passcode certainly on accounting configuration of printer driver.
- Users and administrators have to set passcodes and encryption key according to the following rule for the client PC login and the machine's setup.
  ・Do not use an easily guessed character strings passcodes.
  ・Passcodes have to contain both numeric and alphabetic.
- For secure operation, all of the remote trusted IT products that communicate with the machine implement the communication protocol in accordance with industry standard practice with respect to RFC/other standard compliance (SSL/TLS, IPSec, SNMPv3, S/MIME) and work as advertised.
- The settings described below are required same as the machine's configuration.

1. SSL/TLS
   Set the SSL client（WEB browser） and SSL server that communicate with the machine as following data encryption suite
   ・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
   （Specifically, recommended browser is Microsoft internet Explorer 6/7/8, Mozilla Firefox 2.x/3.x）
2. S/MIME
   Set the machine and mail clients as following Encryption Method/Message Digest Algorithm.
   ・RC2(128bit)/SHA1
   ・3Key Triple-DES(168bit)/SHA1
3. IPSec
   Set the IPSec host that communicates with the machine as following Encryption Method/Message Digest Algorithm.
   ・AES(128bit)/SHA1
   ・3Key Triple-DES(168bit)/SHA1
4. SNMPv3
   Encryption Method of SNMPv3 is DES fixed. Set the Message Digest Algorithm to SHA1.

Important:

For secure operation, while you are using the CentreWare Internet Services, please do not access other web site.

Please do not use FTP Server and Backup Restore function, because they have not been evaluated.

Confirm the Machine ROM version and the System Clock

Before initial settings, the System Administrator (Machine Administrator) has to check the machine ROM version 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.

You can identify the software versions of the components of 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.

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

How to check the Clock

1. Press the <Log In / Out> button on the control panel.
2. Enter the System Administrator’s Login ID and Passcode if prompted (default 11111, x-admin).
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 date of internal clock. If it is required to change, refer to following procedures.

1. Select the required option.
2. Select [Change Settings].
3. Change the required setting. Use the scroll bars to switch between screens.
4. Select [Save].

Initial Settings Procedures Using Control Panel

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

Use Passcode Entry from Control Panel

1. Press the <Log In/Out> button on the control panel.
2. Enter "11111" with the numeric keypad or the keyboard displayed. This is the factory default "ID".
3. Select [Enter] on the touch screen.
4. Select [Tools].
5. Select [Authentication/Security Settings].
6. Select [Authentication].
7. Select [Passcode Policy].
8. On the [Passcode Policy] screen, select [Passcode Entry from Control Panel].
9. Select [Change Settings].
10. On the [Passcode Entry from Control Panel] screen, select [On].
11. Select [Save].
12. To exit the [Passcode Policy] screen, select [Close] in the upper right corner of the screen.
13. To exit the [Tools] screen, select [Close] in the upper right corner of the screen.
14. Select [Reboot Now] on the confirmation screen.

Authentication for entering the System Administration mode

1. Press the <Log In/Out> button on the control panel.
2. Enter "11111" with the keyboard displayed. This is the factory default "ID".
3. Select [Next] on the touch screen.
4. Enter "x-admin" for passcode from the keyboard.
5. Select [Enter] on the touch screen.
6. Select [Tools].

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. On the [System Administrator's Passcode] screen, Select [Keyboard].
5. Enter a new passcode of 9 or more characters in [New Passcode], and select [Save].
6. In [Retype Passcode], select [Keyboard].
7. Enter the same passcode, and select [Save] twice.
8. In the [Do you want to change the System Administrator’s Passcode?] screen, select [Yes].

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 Rep. 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 [Keyboard], and enter a new passcode of 9 or more characters in [New Passcode].
9. Select [Save].
10. Select [Keyboard], and enter the same passcode in [Retype Passcode].
11. Select [Save].
12. Select [Save] twice.
13. In the [Do you want to proceed?] screen, select [Yes].
14. In the [Do you still want to proceed?] screen, select [Yes].

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 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 [Keyboard], and enter a New Encryption Key of 12 characters.
8. Select [Save].
9. Select [Keyboard], and Re-enter the Encryption Key.
10. Select [Save] twice.
11. Select [Yes] to make the change.
12. Select [Yes] to Reboot.

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] or [Weekly] or [Monthly].
5. Set [Day], [Hour], [minutes],
6. Select [Save].

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].
5. Select [Save]

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 [All Services Pathway].
6. Select [Save].
7. Select [Service Access].

8. On the [Service Access] screen, select [Locked] for all Items by [Change Settings].
9. Select [Save].
10. Select [Feature Access].
11. On the [Feature Access] screen, select [Locked] for all Items by [Change Settings].
12. To exit the [Access Control] screen, select [Close] in the upper right corner of the screen.

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].
6. On the [Receive Control] screen, select [According to Print Auditron].
7. Select [Save as Private Charge Print Job] for [Job Login Success] selection.
8. Select [Delete Job] for [Job Login Failure] selection.
9. Select [Delete Job] for [Job Without User ID] selection.
10. Select [Save].
11. To exit the [Charge/Private Print Settings] screen, select [Close] in the upper right corner of the screen.

Set User Passcode Minimum Length

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] in the upper right corner of the screen.
10. To exit the [Tools] screen, press the < Services> button on the control panel.

Initial Settings Procedures Using CentreWare Internet Services

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

Preparations for settings on the CentreWare Internet Services

Prepare a computer supporting the TCP/IP protocol to use CentreWare Internet Services.

CentreWare Internet Services supports the browsers satisfied "SSL/TLS" conditions.

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

Set SMB

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

Set SSL/TSL

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

Configuring Machine certificates

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

Set IPSec

Note: Before setting [Digital Signature] for [IKE Authentication Method], you will have to import an IPSec certificate according to same procedure as "Configuring Machine Certificates"

1. Click [+] on the left of the [Security] folder on the [Properties] screen.
2. Click [IPSec].
3. Enable the [Protocol] by placing a check mark in the [Enabled] box.
   Choose [Pre-Shared Key] setting (4 - 5) or [Digital Signature] setting .
4. Select [Pre-Shared Key] for IKE Authentication Method. This is to use the Shared Secret (between this device and remote computers also possessing the secret).
5. Enter a Pre-Shared Key in the [Shared Key] and [Verify Shared Key] box.
   Please set the IPSec address successively.
6. Click [Certificate Management] in the [Security] folder.
7. Select [IPSec] for Certificate Purpose.
8. Click the [Display the list] button, and check a desirable Certificate.
9. Click the [Certificate Details] button.
10. Click the [Use this certificate] button.
11. On the [IPSec] screen, Select [Digital Signature] for IKE Authentication Method.
    Please set the IPSec address successively.

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 the [Apply] button.
5. Click the [Reboot Machine] button.

Set SNMPv3

1. Click [+] on the left of the [Connectivity] folder on the [Properties] screen.
2. Click [+] on the left of the [Protocols] folder.
3. Click [SNMP Configuration].
4. Check the [Enable SNMPv3 Protocol] box.
5. Uncheck the [Enable SNMP v1/v2c Protocols] box.
6. Click the [Apply] button.
7. Click the [Edit SNMPv3 Properties] button and check the [Account Enabled] for [Administrator Account].
8. Enter a new Authentication Password (minimum 8 characters).
9. Enter the Confirm Authentication Password.
10. Enter a new Privacy Password (minimum 8 characters).
11. Enter the Confirm Privacy Password.
12. Check the [Account Enabled] for [Print Drivers/Remote Clients Account].
13. Click the [Apply] button.

Note:

- Authentication Password and Privacy Password have to be changed certainly from default Password.
- In using SNMPv3, use the IPSec protocol simultaneously. Therefore the IP address of the client for SNMPv3 have to be set according to the procedures "Set IPSec Address" .
  Enter the IP Address in the [Specify Destination IPv4 Address] box.
- Since the machine cannot communicate by SNMP v1/v2c, the port setting on the client Print Driver have to be select [LPR] for [Protocol], and uncheck the [SNMP status Enabled].

Set S/MIME

Note:

- To use E-mail with this machine, E-mail function has to be enabled and configured as stated in the System Administration Guide’s "E-mail".
- Before S/MIME setting, you will have to Import an S/MIME certificate according to same procedure as "Configuring Machine Certificates".

1. Click [Configuration Overview] on the [Properties] screen.
2. Click [Settings] for [E-mail].
3. Click the [Configure] button for [E-mail Settings], and enter the machine’s E-mail address in the [From address] box.
4. Click the [Apply] button.
5. Click [+] on the left of the [Security] folder on the [Properties] screen.
6. Click [Certificate Management].
7. Select [S/MIME] for [Certificate Purpose].
8. Click the [Display the list] button, and check a desirable Certificate.
9. Click the [Certificate Details] button.
10. Click the [Use this certificate] button.

11. Click [SSL/TLS Settings].
12. Check the [Enabled] box for [S/MIME Communication].
13. Click the [Apply] button.
14. Click the [Reboot Machine] button.
15. After the machine is restarted, refresh the browser and Click [Properties] tab.
16. Click [+] on the left of the [Security] folder.
17. Click [S/MIME Settings].
18. Uncheck the [Enabled] check box for [Receive Untrusted Email].
19. Click the [Apply] button.

Regular Review by Audit Log

This section describes the setting and importing method for the Audit Log from the System Administrator client via CentreWare Internet Services.

The Audit Log, regularly reviewed by the Security Administrator, often with the aid of third party analyzing tools, helps to assess attempted security breaches, identify actual breaches, and prevent future breaches.

The important events of TOE 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 is 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.

Set Audit Log

1. Open your Web browser and enter the TCP/IP address of the machine in the Address or Location field, press the <Enter> key.
2. Supply the Administrator ID and Password, when prompted.
3. Click the [Properties] tab.
4. Click [+] on the left of the [Security] folder.
5. Click [Audit Log].
6. Check the [Enabled] box for [Audit Log].
7. Click the [Apply] button.
8. 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 CentreWare Internet Services for viewing and analysis. The logged data is not viewable from the local UI. And additionally requires the enabling of SSL/TLS encryption for Accessing to the logged data.

1. Open your Web browser and enter the TCP/IP address of the machine in the Address or Location field, press the <Enter> key.
2. Supply the Administrator ID and Password, when prompted.
3. Click the [Properties] tab.
4. Click [Audit Log].
5. Click [Export as text file].

User Authentication and Passcode Change

This section describes the operation of user authentication and its Passcode Change.

User Authentication

Before the use of all services and settings, user needs ID and Passcode Authentication.

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.

In this state, all features are able to utilize from control panel.

Important

In the case of interrupting when other people use the machine, please logout by <Log In/Out> button before canceling the interrupt mode.

Example) User A is authenticated → interrupt mode →User B login →job complete →User B logout →cancel the interrupt mode

Change User Passcode by General User

This feature allows Authenticated Users (the procedure as described "User Authentication ") to change the registered passcode.

1. Authenticate by the procedure as described [User Authentication].
2. Select [User Details Setup].
3. Select [Change Passcode] .
4. Enter the Current Passcode and select [Next].
5. On the Change Passcode screen, Select [Keyboard].
6. Enter a new passcode from 9 or more characters in [New Passcode], and select [Next].
7. In [Retype Passcode], select [Keyboard].
8. Enter the same passcode, and select [Save] twice.

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

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

Operation Using CentreWare Internet Services

This chapter contains information on the operation of using CentreWare Internet Services, to use security features for System Administrator and authenticated users.

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

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

NOTE: This feature is not available on a machine in which the direct printing feature is not configured.

Accessing CentreWare Internet Services

Follow the steps below to access CentreWare Internet Services.

At a client workstation on the network, launch an internet browser.

In the URL field, enter “http://” followed by the IP address or 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 the following in the URL field:

http://vvv.xxx.yyy.zzz

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

NOTE: The IPV6 format is supported on Windows Vista only.

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 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 CentreWare Internet Services is displayed.

NOTE: In the case of the Authentication feature is enabled, you may be required to enter the user ID and password (if one is set up). This is required to access CentreWare Internet Services to configure and use the security function of the machine.

NOTE: When your access to CentreWare Internet Services is encrypted, enter

“https://” followed by the IP address or Internet address, instead of “http://”.

Print

This page allows you 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.

Click [Print] on the Main Panel of the home page.

The [Job Submission] page is displayed.

Job Submission Allows you to print 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 to 999.
	Collated	Specify whether to collate printouts or not.
	2 Sided Printing	Allows you to select 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.
	Staple	Allows you to select the number and location of staples.
	Output Destination	Allows you to select output trays from the drop down menu.
Paper	Paper Supply	Allows you to select the paper tray from the drop down menu
	Paper Size	Allows you to select the output paper size.
	Paper Type	Allows you to select the type of the paper to be used.
Delivery	Immediate Print	In the case of user authentication mode, regardless these set, 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 print. Clicking the [Browse] button next to the [File Name] edit box opens the [Choose File] dialog box where you can select the file to print. You can print only files with the following exceptions. : .pdf, .tif, .pcl, .ps, and .txt.
Submit Job		Click this button to print the file.

Scan (Folder Operation)

This page allows you to configure Folder.

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

Click [Scan] on the Main Panel of the home page.

Select the Folder hot link.

The [Folder] page is displayed.

Folder icons

Clicking the icon of a registered Folder displays [Folder: List of Files] page for the Folder.

Folder Number

Displays the Folder numbers. Clicking the number of a registered Folder displays the [Folder: List of Files] page for the Folder.

Folder Name

Displays the names of Folders. Clicking the name of a registered Folder displays the [Folder: List of Files] page for the Folder.

Number of Files in this Folder

Displays the number of files stored in each Folder.

File List

Displays the [Folder: List of Files] page for the selected Folder.

Delete

Deletes the selected Folder.

Edit

Displays the [Edit Folder] page for the selected Folder.

Create

Displays the [Folder Setup] page for the selected Folder.

Folder: List of Files

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

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 Folder.
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 Note: You can not retrieve Copied document	Retrieve Page	Select whether or not to retrieve one page of the selected file.
	Page Number	Enter the page number of the page to be retrieved.
	Retrieving Format	Specify the file format to be used when retrieving the page.
Print File	Paper Supply	Select the paper tray to be used to print the selected file.
	Output Destination	Select the output tray.
	Quantity	Select the number of copies to print.
	2 Sided Printing	Select whether to print only on one side or both sides of paper.
Delete		Deletes the selected files in the folder.

Edit Folder

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

Folder	Folder Number	Displays the number of the selected Folder.
	Folder Name	Displays the name of the selected Folder.
	Folder Passcode	Displays the passcode to the Folder. To change the passcode, enter it with up to 20 characters. Leave the text box blank if not setting 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 id a shared Folder, this shows "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.

Folder	Folder Number	Displays the number of the selected Folder.
	Folder Name	Displays the name of the Folder.
	Folder Passcode	Displays the passcode to the Folder. To change the passcode, enter it with up to 20 characters. Leave the text box blank if not setting 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 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.

Problem Solving

This chapter describes solutions to problems that you may come across while using the machine and CentreWare Internet Services. The machine has certain built-in diagnostic capabilities to help 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 problem occurs, there are several ways in which you can identify the type of fault. Once a fault or problem is identified, establish the probable cause, and then apply the appropriate solution.

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

CAUTION: Failure to leave at least 20 seconds between a power off and a power on can result in damage to the hard disk in the machine.

- If the problem persists, or a message indicates that you should call for service.

NOTE: At the time of the power failure, because the machine is equipped with the hard disk drive, all the queued jobs will be saved. The machine will resume processing queued jobs when the power to the machine is back on.

Fault Codes

When a fault occurs, the touch screen displays a message on how to clear the fault.

Some faults indicate customer maintenance, while others require the attention of the Key Operator and/or System Administrator.

For information on the fault codes, refer to the user Guide.

Appendix

List of Setting Procedures

Item	Using Control Panel	Using CentreWare Internet Services
Check the Clock	[System Settings] > [Common Service Settings] > [Machine Clock/Timers].	-
Use Passcode Entry from Control Panel	[Authentication/Security] > [Authentication] > [Passcode Policy] > [Passcode Entry from Control Panel]	-
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]
Set Service Rep. Restricted Operation	[System Settings] > [Common Service Settings] > [Other Settings] > [Service Rep. Restricted Operation].	[Security] > [Service Representative Restricted Operation]
Set Overwrite Hard Disk	[Authentication/Security Settings] > [Overwrite Hard Disk]	-
Set Data Encryption	[System Settings] > [Common Service Settings] > [Other Settings] > [Data Encryption]	-
Set Scheduled Image Overwrite	[Authentication/Security Settings] > [Overwrite Hard Disk] > [Scheduled Image Overwrite].	[Security] > [Scheduled Image Overwrite]
Set Authentication	[Authentication/Security Settings] > [Authentication] > [Login Type].	[Security] > [Authentication Configuration]
Set Access Control	[Authentication/Security Settings] > [Authentication] > [Access Control]	[Security] > [Authentication Configuration] > [Next] > [Device Access]
Set Private Print	[Authentication/Security Settings] > [Authentication] > [Charge/Private Print Settings].	-
Set User Passcode Minimum Length	[Authentication/Security Settings] > [Authentication] > [Passcode Policy] > [Minimum Passcode Length]	[Security] > [User Details Setup] > [Minimum Passcode Length]
Set SMB	-	[Connectivity] > [Port Setting]
Set SSL/TSL	[System Settings] > [Connectivity & Network Setup] > [Security Settings] > [SSL/TLS Settings]	[Security] > [Machine Digital Certificate Management] > [Create New Self Signed Certificate] > [SSL/TLS Settings]
Configuring Machine Certificates	-	[Security] > [Machine Digital Certificate Management] > [Upload Signed Certificate].
Set IPSec	[System Settings] > [Connectivity & Network Setup] > [Security Settings] > [IPSec Settings]	[Security] > [IPSec]
Set SNMPv3	-	[Connectivity] > [Protocols] > [SNMP Configuration]
Set S/MIME	[System Settings] > [Connectivity & Network Setup] > [Security Settings] > [S/MIME Settings]	[Security] > [SSL/TLS Settings] > [S/MIME Communication]
Set Audit Log, Import the Audit LogFile	-	[Security] > [Audit Log].
Create/View User Account	[Authentication/Security Settings] > [Authentication] > [Create/View User Accounts]	[Security] > [Authentication Configuration] > [Next] > [Account Number] > [Edit]
Change User Passcode by General User	[User Details Setup] > [Change Passcode]	-
Folder Service	[System Settings] > [Folder Service Setting]	-

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]