WorkCentre 7425/7428/7435

Security Function Supplementary Guide

Version 1.0, August 2009

Table of Contents

Before Using the Security Function 5

Preface 5

Security Features 6

Settings for the Secure Operation 6

Data Restoration 7

Starting use of the data encryption feature and changing the settings 7

Use of the Overwrite Hard Disk 8

Service Representative Restricted Operation 8

For Optimal Performance of the Security features 9

Confirm the Machine ROM version and the System Clock 10

How to check by Control Panel 10

How to check by Print Report 10

How to check the Clock 10

Initial Settings Procedures Using Control Panel 11

Authentication for entering the System Administration mode 11

Change the System Administrator's Passcode 11

Set Maximum Login Attempts 11

Set Service Rep. Restricted Operation 12

Set Overwrite Hard Disk 12

Set Scheduled Image Overwrite 12

Set Authentication 13

Set Access Control 13

Set Private Print 13

Set User Passcode Minimum Length 14

Initial Settings Procedures Using CentreWare Internet Services 15

Preparations for settings on the CentreWare Internet Services 15

Set SMB 15

Set SSL/TSL 16

Configuring Machine certificates 16

Set IPSec 17

Set IPSec Address 17

Set SNMPv3 18

Set S/MIME 19

Regular Review by Audit Log 20

Set Audit Log 20

Import the Audit Log File 20

Authentication for the Secure Operation 21

Overview of Authentication 21

Users Controlled by Authentication 21

Machine Administrator 21

Authenticated Users (with System Administrator Privileges) ... 22
Authenticated Users (with No System Administrator Privileges) ... 22
Unauthenticated Users ... 22
Local Machine Authentication (Login to Local Accounts) ... 22
Functions Controlled by Authentication ... 23
Local Access ... 23
Remote Access ... 23
Authentication for Folder ... 25
Types of Folder ... 25
Machine Administrator Shared Folder ... 25
Only Machine Administrator can change the settings. ... 25
Personal Folder ... 25
Operations available for Folder. ... 26
Operation Using Control Panel ... 28
User Authentication ... 28
Create/View User Accounts ... 28
On the Tools screen, ... 28
User ID ... 29
User Name ... 29
Passcode ... 29
E-mail Address ... 29
Account Limit ... 29
User Role ... 29
Reset Total Impressions ... 29
Reset Account ... 29
Change User Passcode by General User ... 30
Folder / Stored File Settings ... 31
Folder Service Settings ... 31
Files Retrieved By Client ... 31
Print & Delete Confirmation Screen ... 31
Quality/File Size for Retrieval ... 31
Stored File Settings ... 32
Expiration Date for Files in Folder ... 32
Stored Job Expiration Date ... 32
Minimum Passcode Length for Stored Job ... 32
Print Order for All Selected Files ... 32
Create Folder ... 33
Folder Name ... 33
Check Folder Passcode ... 33
Delete Files After Retrieval ... 33
Delete Expired Files ... 33
Send from Folder ... 34
File Name/Stored Date ... 34
Refresh ... 34

Select All.....34
Print.....34
Delete.....34
Private Charge Print.....35
Refresh.....35
Select All.....35
Delete.....35
Print.....35
Operation Using CentreWare Internet Services..... 36
Accessing CentreWare Internet Services.....37
Print.....38
Scan (Folder Operation).....39
Folder icons.....39
Folder Number.....39
Folder Name.....39
Number of Files in this Folder.....39
File List.....39
Delete.....39
Edit.....39
Create.....39
Folder: List of Files.....40
Edit Folder.....40
Folder Setup.....41
Import the files.....41
Change User Passcode by System Administrator (Using CentreWare Internet Services) 42
Problem Solving..... 43
Fault Clearance Procedure.....43
Fault Codes.....44
Appendix..... 48

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.

WorkCentre 7425/7428/7435 System Administrator Guide

:Version 1.0, January 2009

WorkCentre 7425/7428/7435 User Guide

:Version 1.0, January 2009

WorkCentre 7425/7428/7435 is supported by the following ROM version.

Controller+PS ROM	Ver. 1.180.9
IOT ROM	Ver. 40.10.0
IIT ROM	Ver. 22.13.1
ADF ROM	Ver. 20.0.0

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

WorkCentre 7425/7428/7435 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
- FAX 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:

Passcode Entry from Control Panel	Default [On].
The System Administrator Passcode	Change the default passcode "1111" 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	Default [On]
Scheduled Image Overwrite	Set to [Enabled].
Authentication	Set to [Login to Local Accounts]
Access Control	Set to [Locked] for Device Access and Service 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]
SNMP v1/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.
- FAX Flow Security feature requires no special setting 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 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. When [3 Overwrites] is selected, overwriting is carried out with the method recommended by the National Security Agency (NSA). [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 WorkCentre 7425/7428/7435, 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, Netscape 7.x, 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.

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 admin, 1111).
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.

Authentication for entering the System Administration mode

1. Press the <Log In/Out> button on the control panel.
2. Enter "admin" with the keyboard displayed. This is the factory default "ID".
3. Select [Next] on the touch screen.
4. Enter "1111" 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 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. 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" (1.8) 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" (3.4).

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 (6 -11).
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

12. Enter the IP Address in the [Specify Destination IPv4 Address] box on the [IPSec] screen.
13. Enter the IP Address in the [Specify Destination Ipv6 Address] box.
14. Select [Enabled] or [Disabled] from the [Communicate with Non-IPSec Device] dropdown list.
15. Click the [Apply] button.
16. 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" (3.5).
  Enter the IP Address in the [Specify Destination IPv4 Address] box.
- Since the machine cannot communicate by SNMP v1/v2, 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 Administrator Guide’s "Scan to E-mail".
- Before S/MIME setting, you will have to Import an S/MIME certificate according to same procedure as "Configuring Machine Certificates" (3.4).

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.

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].

Authentication for the Secure Operation

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

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

Overview of Authentication

This section is an overview of the Authentication feature used with the machine.

Users Controlled by Authentication

The following is an explanation about 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 (default of admin).

Only The Machine Administrator is able to change the Machine Administrator ID(default of admin), and the Machine Administrator Passcode(default of 1111).

This is a user who can enter the System Administration mode and change the machine settings related to security features and services that is 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 who are assigned the System Administrator privileges.

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

This type of user has the same privileges as the Machine Administrator for machine operations, except:

- 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 and assigned no System Administrator privileges.

When a restricted service is used, this type of user must enter a 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 registered on the machine to manage authentication.

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

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

Functions Controlled by Authentication

The following explains the functions that are restricted by the Authentication feature.

Restriction depends on which of the following two ways the machine is used.

- Local Access
- Remote Access

For more information on the restrictions to Folder and job flow sheets using the Authentication feature, refer to Authentication for Job Flow Sheets and Folder on 5.2.

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

Service Access

- Copy
- Fax
- Internet Fax
- Scan to Folder
- E-mail
- Network Scanning
- Scan to PC
- Send from Folder
- Stored Programming
- Job Flow Sheets
- Custom Services

Feature Access

- Print File from Folder
- Retrieve File from Folder

Remote Access

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

The functions restricted by Remote Access are as follows.

Print

Printing is limited to 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.

Direct Fax

Direct Fax from a computer is restricted.

To use the Authentication feature, use the fax driver to set authentication information such as user ID and passcode.

The fax jobs sent to the machine that fail authentication are set to Charge Print and are either saved to the machine or deleted, depending on the selected setup option.

CentreWare Internet Services

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

Authentication for Folder

The following explains the restrictions for 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.

NOTE: When the Authentication feature is used with a remote account server, the user information stored in the machine may be temporarily deleted to restrict user access. When this happens, the Folder and job flow sheets associated with the user will also be deleted. When using a remote authentication server to manage authentication, use of Folder and job flow sheets in the System Administration mode is recommended.

NOTE: For Folder and job flow sheets, Authenticated Users who are given the System Administrator privileges have the same access level as Authenticated Users with no System Administrator privileges.

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, this Folder is shared by all Authenticated Users.

Only 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 using the Authentication feature.

Only the Authenticated User that created the Folder can use it.

The following explains the operations available. When the Authentication feature is not enabled

Operations available for Folder.

The following table shows the relationship with the Folder for each user type when the Authentication feature is enabled.

Folder Operation		**System Administrator and Authenticated Users**		
		Shared by Machine Administrator	**Personal (owner)**	**Personal (other)**
Create		X	O	X
Display		O	O	X
Delete		O	O	X
Change Settings		X	O	X
Display File		O	O	X
Delete File		O	O	X
Store File[*1]		O	O	X
Print File[*1]		O	O	X
Job Flow Sheet	Display	O	O	X
	Link	X	O	X
	Auto Run	O	O	X
	Manual Run	O	O	X

Folder Operation		Machine Administrator	
		Shared by Machine Administrator	Personal
Create		O	X
Display		O	O
Delete		O	O
Change Settings		O	O
Display File		O	O
Delete File		O	O
Store File*1		O	O
Print File*1		O	O
Job Flow Sheet	Display	O	O
	Link	O	O
	Auto Run	O	O
	Manual Run	O	O

O: Operation available

X: Operation not available

*1: When files are stored or retrieved using a Folder, authentication is not applicable to the following operations.

- Confidential fax reception
- Confidential Internet Fax reception
- Retrieving files that use scan driver or Folder Viewer 3

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 release the link, the job flow sheet will no longer be displayed and will be disabled.

Operation Using Control Panel

This chapter contains information on the operation of using control panel to use security features for System Administrator and authenticated users.

User Authentication

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

6. Press the <Log In / Out> button on the Control Panel.
7. Enter the “User ID“ from keypad.
8. Press [Next] on the touch screen.
9. Enter the “Passcode“ from keyboard.
10. Press [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

Create/View User Accounts

This feature allows you to register user account information, such as User IDs, user names and passcodes, and to impose restrictions on the numbers of copied, faxed, 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 is the sender's address displayed on the [E-mail] screen. 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], [Fax 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.

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 can be entered within the range of 1-9,999,999 pages.

NOTE: [Account Limit] cannot be selected for the fax services.

User Role

Allows you to select the privileges to give to the user. Select from [User], [System Administrator].

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

Reset Total Impressions

Deletes all 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 (the procedure as described "User Authentication " (6.1)) to change the registered passcode.

1. Authenticate by the procedure as described [User Authentication](6.1).
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.

Folder / Stored File Settings

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

Folder Service Settings

This feature allows you to specify whether to discard files once received from a client and whether received Internet Fax files can be forwarded.

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 files stored in a Folder are automatically deleted. You can set how long files are kept and time of the deletion.

You can also select whether individual files are deleted or not.

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 in the range from 1 to 14 days, and enter the time 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 in the range of 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.

Minimum Passcode Length for Stored Job

Set the minimum number of allowed passcode digits between 0 and 12 digits. A passocde is required when Secure Print or Private Charge Print files are to be stored or printed. A passcode must have digits equal to or longer than the value specified here.

NOTE: Specify "0" if you do not set passcodes, or the minimum number of passcode digits.

Print Order for All Selected Files

Specifies the print order for a stored file from 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 incoming FAX files or scanned files. FAX files in Folder can be printed out at a convenient time and 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 [On] or [Off] for [Check Folder Passcode]

NOTE: If you select [On], go to step 5 to register a passcode. The machine will not allow the Folder to be accessed unless the registered passcode is entered. If you select [Off], skip to step 8.

5. Enter a passcode (up to 20 digits max.) using the numeric keypad on the control panel.
6. Select the required [Target Operation] option.
7. Select [Save].
8. Change the required settings.
9. 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.

Check Folder Passcode

Checks the passcode for the target operation. Select an option for restricting access to the Folder through the passcode. If you select [Save (Write)], the passcode entry screen appears when an attempt is made to edit any file in the Folder. If you select [Print/Delete (Read)], the passcode entry screen appears when an attempt is made to print out or delete any file in 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 displayed on the [Send from Folder] screen.

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

1. Press the <All Services> 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/Stored Date

Sorts the files by their names or the dates they were stored. Selecting the same option again toggles the order in which they are listed, as 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 to files stored in the machine.

1. Press the <Log In/Out> button.

2. Enter your user ID and Passcode using the screen keypad or numeric keypad on the control panel, and select [Confirm].

3. Select [Charge Print] on the [Secure Print Jobs & More] screen.

NOTE: If you entered the screen with System Administrator's ID, a list of authentication user IDs will be displayed. Select the desired user ID from the list or enter it in [Go to], and select [File List]. The files stored for the selected user ID will be displayed.

4. Select a file to print or delete.

5. Select the required option.

Refresh

Refreshes the displayed information.

Select All

Selects all files in the list.

Delete

Deletes a file selected in the list.

Print

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

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

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	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.

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 or retrieved.
	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 or retrieved.
	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.

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 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.

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 System Administrator.

The following table represents some of the fault codes relating to security functions and their corresponding corrective actions. These may appear in the Faults List available in the Machine Status mode.

Code	Description and Remedy
016-210 **016-211** **016-212** **016-213** **016-214**	An error occurred on the software option settings. Turn the power off and on. Contact the Xerox Welcome Center if the problem persists.
016-454	Unable to retrieve the IP address from DNS. Check the DNS configuration and IP address retrieve setting.
016-455	Connection to the SNTP server was timed out. Check the network cable connection and IP address of the SNTP server.
016-456	Received a message from the SNTP server saying that it was not synchronized with the standard time source. Check the SNTP server settings.
016-502	An error occurred during writing data. Contact the Xerox Welcome Center.
016-503	Unable to resolve the name of the SMTP server when e-mail was transmitted. Check if the SMTP server is set correctly using CentreWare Internet Services. Also, check that the DNS server is set correctly.
016-504	Unable to log in to the POP3 server when transmitting e-mail. Check if the user name and password used for the POP3 server are set correctly using CentreWare Internet Services.
016-505	Unable to log in to the POP3 server when transmitting e-mail. Check if the user name and password used for the POP3 server are set correctly using CentreWare Internet Services.
016-513	An SMTP server connection timeout error occurred. The SMTP server or network is overloaded. Wait for a while, and try again.
016-574	The machine failed to transfer data via FTP using the Scan to PC service because the host or server name of the FTP server could not be resolved. Check the connection to the DNS server. Check if the FTP server name is registered correctly on the DNS server.
016-575	The machine failed to transfer data via FTP using the Scan to PC service because the DNS server address was not registered. Specify the correct DNS server address. Or, specify the destination FTP server using its IP address.
016-576	The machine failed to transfer data via FTP using the Scan to PC service because it could not connect to the FTP server. Ensure that both the destination FTP server and the machine are available for network communication by checking the following: • The IP address of the server is set correctly. • The network cables are plugged in securely.
016-577	Connection to the FTP service of the destination server failed. 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	The machine failed to transfer data via FTP using the Scan to PC service due to unsuccessful login to the FTP server. Check if the login name (user name) and password are correct.
016-579	The machine failed to transfer data via FTP using the Scan to PC service because the scanned image could not be saved in the FTP server after connection. Check if the FTP server's save location is correct.
016-580	The machine failed to transfer data via FTP using the Scan to PC service because the file or folder name on the FTP server could not be retrieved after connection. Check the access privilege to the FTP server.

016-581	The machine failed to transfer data via FTP using the Scan to PC service because the suffix of the file or folder name exceeded the limit after connection. Change the file name, or change the destination folder on the FTP server. Or, move or delete files from the destination folder.
016-582	The machine failed to transfer data via FTP using the Scan to PC service because file creation was not successful on the FTP server after connection. 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	The machine failed to transfer data via FTP using the Scan to PC service because lock folder creation was not successful on the FTP server after connection. Take one of the following actions: • If any lock directory (.LCK) exists in the forwarding destination, delete it manually, and 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	The machine failed to transfer data via FTP using the Scan to PC service because folder creation was not successful on the FTP server after connection. 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	The machine failed to transfer data via FTP using the Scan to PC service because file deletion was not successful on the FTP server after connection. Check the access privilege to the FTP server.
016-586	The machine failed to transfer data via FTP using the Scan to PC service because lock folder deletion was not successful on the FTP server after connection. 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, and then retry executing the job.
016-587	The machine failed to transfer data via FTP using the Scan to PC service because folder deletion was not successful on the FTP server after connection. Check the access privilege to the FTP server.
016-588	The machine failed to transfer data via FTP using the Scan to PC service because the data could not be written in the FTP server after connection. Check if enough space is available in the save location.
016-589	The machine failed to transfer data via FTP using the Scan to PC service because the data could not be read from the FTP server after connection. Check the access privilege to the FTP server.
016-593	The machine failed to transfer data via FTP using the Scan to PC service because an internal error occurred after connection to the FTP server. Try again. If the problem persists, contact the Xerox Welcome Center.
016-594 **016-595**	The machine failed to transfer data via FTP using the Scan to PC service because a network error occurred. Try again. If the problem persists, contact the Xerox Welcome Center.
016-703	An e-mail specifying a non-registered or invalid Folder number was received. When sending a fax or Internet Fax: • Contact the Xerox Welcome Center. When receiving e-mail, fax, or Internet Fax: • Register the Folder with the specified number. • Send an e-mail to a valid Folder. • Contact the Xerox Welcome Center if the problem persists.
016-704	The hard disk ran out of space, because the Folders are full. Delete unnecessary documents from the Folders.
016-705	Unable to register the secure print document, Folder document, or billing data using the print driver, or unable to register the scanned document in the Folder, because the hard disk drive may not be installed properly on the machine, or may be damaged. Contact the Xerox Welcome Center.
016-706	The hard disk ran out of space, because the number of users for secure printing reached its maximum. Delete unnecessary documents or users registered for the Secure Print feature.
016-711	Refer to 016-985.
016-713	The input passcode does not match the Folder passcode. Enter the correct passcode.
016-714	The specified Folder does not exist. Create a new Folder or specify an existing Folder.

016-748	Unable to print due to insufficient hard disk space. Reduce the number of pages in print data, for instance by dividing the print data, or by printing one copy at a time when making multiple copies.
016-764	Unable to connect to the SMTP server. Contact the System Administrator.
016-765	Unable to send e-mail due to insufficient hard disk space on the SMTP server. Contact the System Administrator.
016-766	An error occurred on the SMTP server. Contact the System Administrator.
016-767	Unable to send e-mail due to the wrong e-mail address. Verify the e-mail address, and try sending the e-mail again.
016-768	Unable to connect to the SMTP server due to the incorrect e-mail address of the machine. Check the e-mail address of the machine.
016-769	The SMTP server does not support delivery confirmation (DSN). Send e-mail without setting confirmation.
016-770	The direct fax function is prohibited. Check with the System Administrator whether the function is enabled. If enabled, contact the Xerox Welcome Center.
016-771	Unable to retrieve the scan data repository address. Confirm the DNS connection. Alternatively, set the scan data repository domain name to the DNS.
016-772	Unable to retrieve the scan data repository address. Specify the correct DNS address. Alternatively, set scan data repository address to the IP address.
016-773	The IP address of the machine is not set correctly. Check the DHCP environment. Alternatively, manually specify an IP address of the machine.
016-774	Unable to process compression conversion due to insufficient hard disk space. Delete unnecessary data from the disk.
016-781	Unable to connect to the server during file forwarding by a Network Scanning server application. Ask the System Administrator to check the network and server.
016-788	Failed to retrieve the file from the web browser. Take one of the following actions, and then try retrieving again. • Refresh the browser page. • Restart the browser. • Switch the machine off and then back on.
016-789	The mail processing was interrupted due to insufficient hard disk space. Lower the image resolution or reduction/enlargement ratio, or divide the document into smaller segments to send.
016-790	The number of the e-mails in the e-mail job exceeded the value specified in [Maximum Split Count]. Take one of the following actions: 1. Lower the scan resolution for the e-mail job. 2. Lower the image magnification for the e-mail job. 3. Increase the value in [Maximum Data Size per E-mail].
016-791	Access to the destination for the Scan to PC service or to the Network Scanning server application failed. Check if you are authorized to access the specified destination or server.
016-793	The hard disk has run out of space. Delete unnecessary data, or initialize the hard disk if the saved data is not needed.
016-982	The hard disk has run out of space. Delete unnecessary data from the hard disk or documents in Folders.
016-985	The e-mail size exceeds the maximum size. Try one of the following procedures, and resend the e-mail. • Reduce the number of pages in the document. • Lower the scan resolution in [Resolution]. • Reduce the document size using [Reduce/Enlarge]. • Increase the maximum value in [Maximum E-mail Size] on the [Tools] screen.
018-400	An IPSec setting error occurred. The preshared key or device certificate, which is required for the selected authentication method, is not specified. Specify the preshared key or device certificate according to the authentication method.
018-502	Your computer is not permitted to log in to the SMB server. Check the properties settings of your user account to see if your computer has access permission to the SMB server.

018-505	One of the following problems has occurred. If the error occurred during SMB authentication: • The user ID or passcode you entered was not correct, and thus the authentication failed. • The time setting of the SMB server and that of the machine do not match(Windows Server 2003 only).If the error occurred during SMB file transfer using Scan to PC: • The user ID or passcode you entered was not correct, and thus the login to the SMB server failed. • The time setting of the SMB server and that of the machine do not match(Windows Server 2003 only). • The user is not permitted to use Windows Sharing (Mac OS X 10.4 only). Take one of the following actions. • Check with the System Administrator for the correct user ID and passcode. • Make sure to match the time setting of the SMB server and that of the machine (Windows Server 2003 only). • Check if you are permitted to use Windows Sharing (Mac OS X 10.4 only).
018-524	A network error occurred. The probable cause are as follows: 1) The DNS server is not registered on the machine, but the server is specified in the job template with the domain name. 2) The protocol (SMB, FTP, etc.) specified in the job template is not enabled on the machine.
018-529	During the Custom Services scanning process, another Custom Services scan job was requested. Wait for a while, and try again.
018-530	A Custom Services authentication error occurred. Check the authentication settings.
018-543	The following problems were identified with the shared name specified when you logged into the SMB server to save scan data using the Scan to PC service. • The shared name does not exist on the server. • The shared name includes illegal characters. • Macintosh computers do not have access right to the shared name. Make sure that the shared name you specified is correct.
018-547	The maximum number of users had already been reached when you logged in to the SMB server to save scan data using the Scan to PC service. Take one of the following actions: • Check the maximum number of users that are allowed to simultaneously access the shared folder. • Check whether the number of users that are allowed to simultaneously access the server has reached the maximum.
027-706	There was no S/MIME certificate tied to the e-mail address when sending email. Import an S/MIME certificate for the e-mail address into the machine.
027-707	The S/MIME certificate tied the e-mail address when sending e-mail has expired. Obtain a new S/MIME certificate, and import into the machine.
027-708	The S/MIME certificate tied the e-mail address when sending e-mail is untrusted. Import a trusted S/MIME certificate into the machine.
027-709	The S/MIME certificate tied the e-mail address when sending e-mail has been revoked. Import a new S/MIME certificate into the machine.
027-710	The S/MIME certificate to receive e-mail was not present. Contact the sender, and ask them to send e-mail with an S/MIME certificate.
027-711	The sender's S/MIME certificate was not retrieved from the received e-mail. Import the sender's S/MIME certificate into the machine, or attach an S/MIME certificate to the sender's S/MIME signature e-mail.
027-712	The received e-mail S/MIME certificate has expired or is untrusted. Contact the sender, and ask them to send e-mail with a valid certificate.
027-713	The received e-mail was rejected, because it had been altered, possibly the transmission route had been falsified. Contact the sender to notify them about the possibility of falsification, and request them to resend the e-mail.
027-714	The received e-mail was rejected, because the "From" field differs from the S/MIME signature e-mail address. Contact the sender, tell them about the possibility of impersonation, and ask them to resend the e-mail.
027-715	The received e-mail S/MIME certificate is not registered on the machine or is not supported on the machine. Import the sender's S/MIME certificate into the machine, or if already registered, enable the certificate so that it can be used on the machine.
027-716	The received e-mail was rejected, because the S/MIME certificate was untrusted. Contact the sender, and ask them to send e-mail with a trusted certificate.

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 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]