Version 1.1

Jun 12, 2008

Xerox WorkCentre 7328/7335/7345 Security Function Supplementary Guide

Xerox WorkCentre 7328/7335/7345 Security Function Supplemental Guide

1 Before Using the Security Function

1.1 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 User Guide and System Administrator's Guide.
Xerox WorkCentre 7328/7335/7345 is supported by the following ROM version.

Controller+PS ROM	Ver. 1.221.100
IOT ROM	Ver. 3.0.4
IIT ROM	Ver. 20.4.1
ADF ROM	Ver. 11.6.5

Note
The machine has obtained information security certification for Common Criteria EAL2.
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 may not be the certified version because it may have been updated along with machine improvements.

1.2 Security Features

Xerox WorkCentre 7328/7335/7345 has the following security features:

- Overwrite Hard Disk
- Data Encryption
- User Authentication
- System Administrator Authentication
- Service Rep. Restricted Operation
- Audit Log
- Network data protection
- Fax Flow Security

1.3 Settings for the Secure Operation

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

1. Passcode Entry from Control Panel
   Set to [On].
2. The System Administrator Passcode
   Change the default passcode "x-admin" to another passcode of 9 or more characters.
3. Maximum Login Attempts
   Set to [5] Times.
4. Service Rep. Restricted Operation
   Set to [On].
5. Overwrite Hard Disk
   Set to [1 Overwrite] or [3 Overwrite].
6. Data Encryption
   Set to [On], and then enter an encryption key of 12 characters.
7. Scheduled Image Overwrite
   Set to [Enabled].
8. Authentication
   Set to [Local]

9. User Passcode Minimum Length
   Set to [9] characters.
10. Private Printer
   Set to [Save in private charge print]
11. SSL/TLS
   Set to [Enabled]
12. IPSec
   Set to [Enabled]
13. SNMPv3
   Set to [Enabled]
14. S/MIME
   Set to [Enabled]
15. SMB
   Set to [Disabled]
16. Audit Log
   Set to [Enabled]

Note
The security will not be warranted if you do not correctly follow the above setting instructions.
Fax Flow Security features requires no special setting by System Administrator.

1.4 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].

1.5 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
- Mailbox and job flow sheet settings (box name, passcode. etc.)
- Documents in mailboxes
- Address book data

Important
Be sure to save all necessary settings and documents 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.

1.6 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.
- The users and administrators have to set passcodes and encryption key according to the following rule.
  ･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 same settings are required as the machine’s configuration described bellow.

    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　1.x/2.x）
    2. S/MIME
       Set the machine and mail client as following Shared Key/hash function.
       ・RC2(128bit)/SHA1
       ・3Key Triple-DES(168bit)/SHA1
    3. IPSec
       Set the IPSec host that communicate with the machine as following Shared Key/hash function.
       ・AES(128bit)/SHA1
       ・3Key Triple-DES(168bit)/SHA1
    4. SNMPv3
       Shared key encryptosystem of SNMPv3 is DES fixed. Hash function is select to SHA1.

1.7 Confirm the Machine ROM version and Clock

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

1.7.1 How to check by Control Panel

1. Press the <Machine Status> button on the control panel.
2. Press the [Software Version] on the Machine information screen.

You can identify the software versions of the components of machine on the screen.

1.7.2 How to check by Print Report

1. Press the <Machine Status> button on the control panel.
2. Press the [Print Reports] on the Machine information screen.
3. Press the [Printer Reports] on the touch screen.
4. Press the [Configuration Reports] on the touch screen.
5. Press the <Start> button on the control panel.

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

1.7.3 How to check the Clock

1. Press the <Log In / Out> button on the Control Panel.
2. Press the "11111" key on the numeric keypad. This is the factory default "ID”.
3. Press [Enter] on the touch screen.
4. Press the <Machine Status> button on the Control Panel.
5. Press the [Tools] tab.
6. Press the [System Settings].
7. Press [Common Service Settings].
8. Press [Machine Clock/Timers].

You can Check the time and date of internal clock. If it is required to change, refer to following procedures.

Select the required option.

Select [Change Settings].

Change the required setting. Use the scroll bars to switch between screens.

Select [Save].

2 Initial Setting Procedures

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

2.1 Use Passcode Entry from Control Panel

1. Press the <Log In / Out> button on the Control Panel.
2. Press the "11111" key on the numeric keypad. This is the factory default "ID".
3. Press [Enter] on the touch screen.
4. Press the <Machine Status> button on the Control Panel.
5. Press the [Tools] tab.
6. Press the [Authentication/Security Settings].
7. Press [Authentication].
8. Press [Passcode Policy].
9. On the Passcode Policy screen, Press [Passcode Entry from Control Panel].
10. On the Passcode Entry from Control Panel screen, select the [On] button.
11. Press the [Save] button.
12. To exit the Authentication screen, press the rectangular Close button in the upper right corner of the screen.
13. Press the [Reboot] button.

2.2 Preparations for settings on the machine's control panel

1. Press the <Log In / Out> button on the Control Panel.
2. Enter "11111" key on the numeric keypad. This is the factory default "ID.
3. Press [Next] on the touch screen.
4. Enter "x-admin" for passcode from keyboard.
5. Press [Enter] on the touch screen.
6. Press the <Machine Status> button on the Control Panel.
7. Press the [Tools] tab.

2.3 Change the System Administrator Passcode

1. On the Tools screen,
2. Press the [Authentication/Security] Settings.
3. Press [System Administrator Settings].
4. Press [System Administrator's Passcode].
5. On the 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.
9. In the [System Administrator Settings] screen, select [Save].
10. Press the [Save] button.
11. Press [Next], then press the keyboard button.
12. If necessary, to exit the System Administrator Settings screen, press the rectangular Close button in the upper right corner of the screen.

NOTE: Be careful not to register a passcode that can be easily cracked and not to store the registered passcode in a location that is easily accessible to other persons.
Important If the system administrator's user ID and passcode are forgotten, the machine configuration will not be able to recover in case of malfunction.
NOTE: This feature is also able to utilize from CentreWare Internet Services.
[Security] folder>[System Administrator Settings]

2.4 Set Maximum Login Attempts

If authentication of system administrator ID fails repeatedly, you can set a limit beyond which further tries are not allowed.

On the Tools screen,

1. Press the [Authentication/Security Settings].
2. Press [Authentication].
3. Press [Maximum Login Attempts By System Administrator].
4. On the Login Attempt screen, select the [Limit Attempts] button.
5. With [ ] and [ ], set [5].
6. Press the [Save] button.
7. If necessary, to exit the Authentication screen, press the rectangular Close button in the upper right corner of the screen.

NOTE:

If the authentication failed more then the specified number of times, the machine displays the following message:

“You have made the maximum number of attempts to access the system. Access denied”

NOTE: This feature is also able to utilize from CentreWare Internet Services.

[Security] folder>[System Administrator Settings]

2.5 Set Service Rep. Restricted Operation

This feature protects the machine settings from being changed by an outsider pretending to be our customer engineer. Make sure not to lose the system administrator’s ID and passcode. Otherwise, the various settings that are only available in system administrator mode cannot be changed.

If the system administrator’s 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 administrator mode.

If you lose the system administrator’s ID and passcode, the electric component board of the machine must be replaced in order to change any setting in the system administrator mode. In that case, you will be charged for the electrical component board and handling cost.

On the Tools screen,

1. Press the [System Settings].
2. Press [Common Service Settings].
3. Press [Other Settings].
4. On the Setting screen, select the [Service Rep. Restricted Operation].
5. Select [Change Settings].
6. Select [On].
7. Select [Save].
8. In the [Do you want to proceed?] screen, select [Yes].
9. In the [Do you still want to proceed?] screen, select [Yes].

2.6 Set Overwrite Hard Disk

On the Tools screen,

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

When copy, fax, scan, or print processing is completed, the data is deleted from the hard disk and the area on which the deleted data was stored is automatically overwritten with blank data.

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.

The data is erased by overwriting once, but overwriting three times makes it even more definite that the data cannot be recovered. Even if it can be, however, it takes longer.

During the overwriting process, processing of normal operations may be slowed down.

2.7 Set Data Encryption

By setting data encryption, when data is written to the hard disk, the data is automatically encrypted. The encryption prevents unauthorized access to the stored data. In order to activate this feature, set an encryption key.

On the Tools screen,

1. Press the [System Settings].
2. Press [Common Service Settings].
3. Press [Other Settings].
4. On the Setting screen, select the [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 Reenter the Encryption Key.
10. Select [Save].
11. Select [Yes] to make the change.
12. Select [Yes] to Reboot.

2.8 Set Scheduled Image Overwrite

On the Tools screen,

1. Press [Authentication/Security Settings].
2. Press [Overwrite Hard Disk].
3. Press [Scheduled Image Overwrite].
4. On the Setting screen, Select [Daily] or [Weekly] or [Monthly].
5. Set [Day], [Hour], [minutes],
6. Select [Save].

NOTE: This feature is also able to utilize from CentreWare Internet Services.
[Security] folder>[Scheduled Image Overwrite]

2.9 Set Authentication

On the Tools screen,

1. Press the [Authentication/Security Settings].
2. Press [Authentication].
3. Press [Login Type].
4. On the Login Type screen, select the [Login to Local Accounts] button.
5. Press the [Save] button.

If necessary, to exit the Authentication screen, press the rectangular Close button in the upper right corner of the screen.
NOTE: This feature is also able to utilize from CentreWare Internet Services.
[Security] folder>[Authentication Configuration]

2.10 Set Private Print

On the Tools screen,

1. Press the [Authentication/Security Settings].
2. Press [Authentication].
3. Press [Charge/Private Print Settings].
4. On the Print Settings screen, select the [Received Control].
5. Select [Change Settings].
6. On the Received Control screen, select the [save in private charge print] button for “Job Login Success” selection.
7. Press the [Save] button.

If necessary, to exit the Authentication screen, press the rectangular Close button in the upper right corner of the screen.

2.11 Set User Passcode Minimum Length

On the Tools screen,

1. Press the [Authentication/Security Settings].
2. Press [Authentication].
3. Press [Passcode Policy].
4. On the Passcode Policy screen, Press [Minimum Passcode Length].
5. On the Minimum Passcode Length screen, with [▼] and [▲], set [9.
6. Press the [Save] button.

If necessary, to exit the Authentication screen, press the rectangular Close button in the upper right corner of the screen.

2.12 Preparations for settings on the CentreWare Internet Services

·Ensure the machine is fully functional on the network.
·Ensure that the TCP/IP and HTTP protocols are configured on the device and fully functional.
This is required to access CentreWare Internet Services to configure the machine.

1. At Your Workstation:
2. Open your Web browser and enter the TCP/IP address of the machine in the Address or Location field, Press [Enter].
3. Enter the System Administrator's ID and passcode if prompted.
4. Click the [Properties] tab.

2.13 Disable SMB

On the Properties screen,

1. Click [+] on the left of the [Connectivity] folder.
2. Click on [Port Setting]
3. Uncheck the SMB [Enabled] box .
4. Click [Apply].

2.14 Creating a self signed certificate (for SSL server) and SSL/TSL Client

On the Properties screen,

1. Click [+] on the [Security] folder.
2. Click on [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 on [SSL/TLS Settings].
8. Select the [Enable] check box for [HTTP - SSL / TLS Server Communication].
9. Click [Apply].
10. Click [Reboot Machine].

NOTE: This feature is also able to utilize from Control Panel.
「Connectivity & Network Setup」>「Security Settings」>「SSL/TLS Settings」

2.15 Configuring Machine certificates

1. Open your Web browser and enter the TCP/IP address of the machine in the Address or Location field Press [Enter].
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 [Machine Digital Certificate Management].
6. Click [Upload Signed Certificate].
7. Enter a file name for the file you want to import, or select the file to be imported by clicking the [Browse] button.
8. Enter the [Password], and Enter the [Retype Password].
9. Click the [Import] button.

2.16 Set IPsec

On the Properties screen,
1. Click [+] on the left of the [Security] folder.
2. Select [IP Sec] in the directory tree.
3. Enable the Protocol by placing a checkmark 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.

Before this setting , you will have to Import an IPSec certificate according to same procedure as configuring Machine certificates.

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

Set IPSec Address

12. Enter the IP Address in the [Specify Destination IPv4 Address:] box.
13. Enter the IP Address in the [Specify Destination Ipv6 Address:] box.
14. Select [Enabled] or [Disabled] from the Communicate with Non-IPSec Device drop-down list,
15. Click [Apply].
16. Click [Reboot Machine].

NOTE: This feature is also able to utilize from Control Panel.
「Connectivity & Network Setup」>「Security Settings」>「IPSec Settings」

2.17 Set SNMPv3

On the Properties screen,
1. Click [+] on the left of the [Connectivity] folder.
2. Click [+] on the left of the [Protocols] folder.
3. Click on [SNMP Configuration]
4. Check the [Enable SNMP v3 Protocol] box .
5. Click [Apply].
6. Click the [Edit SNMP v3 Properties button] and check the [Account Enabled] for Administrator Account.
7. Enter a new Authentication password (minimum 8 characters)
8. Enter the Confirm Authentication Password:
9. Enter a new Privacy Password (minimum 8 characters):
10. Enter the Confirm Privacy Password:
11. Check the [Account Enabled] for Print Drivers/Remote Clients Accounts.
12. Click [Apply].

Note: Authentication password and Privacy Password have to be changed certainly from default Password.
Note: 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 2.16 Set IPsec 12.Enter the IP Address in the [Specify Destination IPv4 Address:] box.

2.18 Set S/MIME

On the Properties screen,
1. Enter the Machine's E-mail Address, under the Description hot link.
   Also note that to use E-mail with this machine, E-Mail has to be enabled and configured as stated in the Scan to E-mail section of System Administrator Guide.
2. Before setting, you will have to Import an S/MIME certificate according to same procedure as configuring Machine

certificates.

3. Click on [Certificate Management].
4. Select the [S/MIME] for Certificate Purpose.
5. Click [Display the list], and check a desirable Certificate.
6. Click [Certificate Details].
7. Click [Use this certificate].
8. Click [+] on the left of [Security] folder.
9. Click on [SSL/TLS Settings].
10. Check the [Enable] box for [S/MIME Communication]
11. Click [Apply].
12. Click [Reboot Machine].
    Refresh the browser and Click [Properties] tab.
13. Click [+] on the left of the [Security] folder.
14. Click [S/MIME Settings].
15. Remove the [Enable] check box for [Receive Untrusted E-mail]
16. Click [Apply].

NOTE: This feature is also able to utilize from Control Panel.
「Connectivity & Network Setup」>「Security Settings」>「S/MIME Settings」

2.19 Set Audit Log

On the Properties screen,

1. Click [+] on the left of the [Security] folder.
2. Click on [Audit Log].
3. Check the [Enabled] box for Audit Log.
4. Click [Apply].

3 Authentication

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.

3.1 Overview of Authentication

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

3.1.1 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.

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

The System Administrator (Machine Administrator)

The System Administrator uses a special user ID called System Administrator ID(default of 11111).
Only The System Administrator is able to change the System Administrator ID(default of 11111), and the System Administrator Passcode(default of x-admin).
Also The System Administrator uses settings related to Security Features and services that is restricted, the user must enter the System Administrator ID and System Administrator Passcode on the authentication screen.

Authenticated Users (with System Administrator Privileges)

These are users who are assigned the System Administrator privileges.
When this type of user uses settings related to Security Features and services that are restricted, the user must enter their User ID and user Passcode on the authentication screen.

Authenticated Users (with No System Administrator)

These are users who are assigned no System Administrator privileges.
When this type of user uses services that are restricted, the user must enter their user ID and user Passcode 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.

3.1.2 Local Machine Authentication

This machine is used set to Local Machine Authentication mode.
Local Machine Authentication uses the user information registered for the Accounting feature to manage authentication. You need, therefore, to enable the Authentication feature when you use Local Machine Authentication. The print or fax data sent directly from a computer can be received on the machine after being authenticated by cross-checking the authentication information pre-configured on a client's fax print driver with the one registered on the machine.
For more information, refer to Fax Print Driver Online Help.

3.1.3 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

When the System Administrator's ID and passcode are not correct, authentication becomes unsuccessful and re-input will be required.
Five unsuccessful authentications occurs, machine needs to reboot.

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 the [All Services] 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 Mailbox
- E-mail
- Network Scanning
- Scan to PC
- Send from Mailbox
- Stored Programming
- Job Flow Sheets
- Custom Services

Feature Access

- Color Copying
- Print Documents from Mailbox
- Retrieve Documents from Mailbox

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 Authentication 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.

NOTE: Printing is not limited when [Login Type] is set to [Remote Access] in the System Administrator mode.

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.

NOTE: Direct Fax is not restricted when [Login Type] is set to [Remote Access] in the System Administrator mode.

3.2 Authentication for Mailboxes

The following explains the restrictions for mailboxes when the Authentication feature is enabled.

NOTE: When a user account is deleted, the mailboxes and job flow sheets associated with the account are also deleted. Any documents stored in the mailboxes 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 mailboxes and job flow sheets associated with the user will also be deleted. When using a remote authentication server to manage authentication, use of mailboxes and job flow sheets in the System Administrator mode is recommended.

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

3.2.1 Types of Mailboxes

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

Machine Administrator Shared Mailbox

The Machine Administrator Shared Mailbox is a mailbox created by a Machine Administrator.
When the Authentication feature is enabled, this mailbox is shared by all Authenticated Users.

Only Machine Administrator can change the settings.
To create a Machine Administrator Shared Mailbox, operate the machine as a Machine Administrator.

Personal Mailbox

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

The ways to operate mailboxes that can be used with the machine differ depending on whether the Authentication feature is enabled. The following explains when the Authentication feature is enabled

When the Authentication Feature is Enabled

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

Mailbox Operation		System Administrator and Authenticated Users		
		Shared by Machine Administrator	Personal (owner)	Personal (other)
Create		X	O	X
Display		O	O	X
Delete		X	O	X
Change Settings		X	O	X
Display Document		O	O	X
Delete Document		O	O	X
Store Document[*1]		O	O	X
Print Document[*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

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

O: Operation available
X: Operation not available
[*1]: When storing documents into, or retrieving documents from the mailbox, authentication is not applicable to the following operations.

- Confidential fax reception
- Confidential Internet Fax reception
- Retrieving documents that use scan driver or Mailbox Viewer 3

NOTE: When job flow sheets not available for operation, depending on changes made to the authentication status, are linked to a mailbox, 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.

4 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.

4.1 User Authentication

Before the use of all services and settings, user needs ID and Passcode Authentication.
The following explains procedures of User Authentication.

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

Press a Service button on the touch screen, or press the <Machine Status> button on the Control Panel.

4.2 Create/View User Accounts

This feature allows a System Administrator to register user account information, such as user IDs, user names and passcodes, and to impose restrictions on the numbers of copy, fax, print, and scan pages allowed 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 UserID 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].

UserID
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.

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.

NOTE: This feature is also able to utilize from CentreWare Internet Services.
[Security] folder>[Authentication Configuration]

4.3 Reset User Accounts

This feature allows you to reset the parameters set for all users (accounts) and clear all data tracked by the machine. It also allows you to print an Auditron report for all services.

1. Select [Reset User Accounts] under [Authentication].
2. Select [Print Report] or [Reset].
3. Select [Close].

All User Accounts
Resets/Prints all parameters of all accounts.

All Feature Access Settings
Resets/Prints the access settings for all features.

All Account Limits
Resets/Prints the upper limit imposed on the total number of pages to be copied and/ or scanned. Resetting the account limits for all accounts returns them to the default value of 9,999,999.

Total Impressions
Resets/Prints all data tracked for all accounts including the System Administrator.

Meter (Print Jobs)
Resets/Prints all data about the number of prints recorded by the machine.

Print Report
Prints the report that allows you to see the user-account parameters and records before resetting them.

Reset
Resets selected parameters or records.

NOTE: This feature is also able to utilize from CentreWare Internet Services.
[Security] folder>[Authentication Configuration]

4.4 Change User Passcode

This feature allows an Authenticated User to change the registered passcode.

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

NOTE: Be careful not to register a passcode that can be easily cracked and not to store the registered passcode in a location that is easily accessible to other persons.

NOTE: This feature is also able to utilize from CentreWare Internet Services.
[Security] folder>[Authentication Configuration]

4.5 Mailbox Stored Document Settings

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

1. Select [Mailbox/Stored Document Settings] under [System Settings].
2. Select the required feature.

4.5.1 Mailbox Service Settings

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

1. Select [Mailbox Service Settings] under [Mailbox/Stored Document Settings].
2. Change the required settings.

Documents Retrieved By Client

Specifies when and how to delete documents in mailboxes after they are retrieved.

Delete according to Mailbox Settings

Specifies documents be deleted according to the settings made for the individual mailbox.

Force Delete

Specifies that documents be deleted immediately after they are retrieved.

Print & Delete Confirmation Screen

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

4.5.2 Stored Document Settings

This feature allows you to select whether documents stored in a mailbox are automatically deleted. You can set how long documents are kept and time of the deletion.

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

1. Select [Stored Document Settings] under [Mailbox/Stored Document Settings].
2. Change the required settings.
3. Select [Close].

Mailbox Document Expiration Date

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

Stored Document Expiration Date

Specifies the retention period for a stored document. 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 document will be deleted when the machine is turned back on.

Min. Passcode Length for Stored Job

Set the minimum number of allowed passcode digits between 0 and 12 digits. A passcode is required when Secure Print or Private Charge Print documents 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.

4.6 Create Mailbox

This feature allows users to create mailboxes for saving confidential incoming fax documents or scanned documents. Fax documents in mailboxes can be printed out at a convenient time and scanned documents in mailboxes can be imported to computers.
The documents can also be exported from computers to the mailbox by specifying the registered mailbox using the print driver.

1. Select [Create Mailbox] on the [Setup Menu] screen.
2. Select a mailbox number to create a new mailbox.
3. Select [Create/Delete].
4. Select [On] or [Off] for [Check Mailbox Passcode],

NOTE: If you select [On], go to step 5 to register a passcode. The machine will not allow the mailbox to be accessed unless the registered passcode is entered. If you select [Off], skip to step 7.

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].

NOTE: By selecting [Delete Mailbox], you can delete all documents in the mailbox and all job flow sheets created through the mailbox.

Mailbox Name

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

Check Passcode

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

Delete Documents After Retrieval

Specifies whether to delete documents in the mailbox after they are printed out or retrieved, or after they are transferred and printed out through a job flow sheet.

Delete Expired Documents

Specifies whether to delete documents in the mailbox after the preset time or period elapses.

4.7 Send from Mailbox

This section describes the mailbox features that allow you to check, print, or delete documents in the private mailboxes displayed on the [Send from Mailbox] screen.
Some mailboxes, however, may require you to enter a passcode, depending on the operation you attempt. Private mailboxes created by other users are inactive and inaccessible to you.

1. Press the <All Services> button on the control panel.

NOTE: If the Authentication feature is enabled, you may be required to enter a user ID and a passcode (if one is set up). If you need assistance, contact the System Administrator.

2. Select [Send from Mailbox] on the touch screen.

Go to
Allows you to specify the first mailbox number to be displayed on the screen, using the numeric keypad on the control panel.

3. Select the mailbox to be opened. Then the documents stored in the mailbox appear.

Document Name/Stored Date
Sorts the documents 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 documents in the mailbox.

Select All
Selects all the documents in the mailbox, so that you can print or delete them all at once.

Print
Prints the selected document(s).

Delete
Deletes the selected document(s).

Job Flow Settings
Displays the [Job Flow Settings] screen.

4.8 Private Charge Print

This feature allows you to check locally stored documents, print stored documents, and delete stored documents.

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

When the Private Charge Print feature is enabled under [Authentication/Security Settings] > [Authentication] > [Charge/Private Print Settings], this feature allows you to print or delete documents stored for each authentication user ID.

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

NOTE: If you entered the screen with the 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 [Document List]. The documents stored for the selected user ID will appear.

4. Select a document to print or delete.
5. Select the required option.

Refresh
Refreshes the displayed information.

Select All
Selects all documents in the list.

Delete
Deletes a document selected in the list.

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

5 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 the System Administrator for further assistance.

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

5.1 Target Computers

The operating systems and web browsers that can be used for CentreWare Internet Services are as follows.

OS	Web Browsers
Windows 2000 Pro	Internet Explorer 6.0 SP1 Netscape 7.1 Navigator
Windows XP Pro	Internet Explorer 6.0 SP1 Netscape 7.1 Navigator Mozilla Firefox 1.5
Windows Vista	Internet Explorer 7.x
Mac OS 9.2	Netscape 7.02 Navigator
Mac OS X 10.3.9	Netscape 7.1 Navigator Safari 1.3

5.2 Accessing CentreWare Internet Services

Follow the steps below to access CentreWare Internet Services.

1. At a client workstation on the network, launch an internet browser.
2. 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://”.

5.3 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.

1. Click [Print] on the Main Panel of the home page.
2. The [Job Submission] page is displayed.

Job Submission Allows you to print documents stored in your computer. Specify the following settings, and click [Start] to submit the job.

Feature		Setting items
Printing	**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.

5.4 Mailbox

This page allows you to configure mailboxes.

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

1. Click [Scan] on the Main Panel of the home page.
2. Select the Mailbox hot link.
3. The [Mailbox] page is displayed.

Mailbox icons

Clicking the icon of a registered mailbox displays [Mailbox Document List] page for the mailbox.

Mailbox Number

Displays the mailbox numbers. Clicking the number of a registered mailbox displays the [Mailbox Document List] page for the mailbox.

Mailbox Name
Displays the names of mailboxes. Clicking the name of a registered mailbox displays the [Mailbox Document List] page for the mailbox.

Number of Documents in this Mailbox
Displays the number of documents stored in each mailbox.

Document List
Displays the [Mailbox Document List] page for the selected mailbox.

Delete
Deletes the selected mailbox.

Edit
Displays the [Edit Mailbox] page for the selected mailbox.

Create
Displays the [Mailbox Setup] page for the selected mailbox.

5.4.1 Mailbox Document List

The following table shows the setting items available on the [Mailbox Document List] page.

Mailbox Number		Displays the mailbox number of the selected mailbox.
Mailbox Name		Displays the name of the selected mailbox.
Document Number		Displays the document numbers of the documents stored in the mailbox.
Document Name		Displays the names of the documents.
Stored Date		Displays the dates on which the documents were stored.
Compression Format		Displays the compression formats of the documents.
Page Count		Displays the page counts of the documents.
Type		Displays the job types of the documents.
Retrieve	**Retrieve Page**	Select whether or not to retrieve one page of the selected document.
	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 Document	**Paper Supply**	Select the paper tray to be used to print the selected document.
	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.

5.4.2 Edit Mailbox

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

Mailbox	Mailbox Number	Displays the number of the selected mailbox.
	Mailbox Name	Displays the name of the selected mailbox.
	Mailbox Passcode	Displays the passcode to the mailbox. 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 Mailbox Passcode	Allows you to select whether and when the passcode for the mailbox is required.
	Owner	Displays the owner of the mailbox. If the mailbox id a shared mailbox, this shows "Shared".
	Linked Job Flow Sheet	Displays the name of the job flow sheet linked to the mailbox. This is only displayed when the mailbox has a linked job flow sheet.
	Auto Start Job Flow Sheet	Allows you to enable or disable the linked job flow sheet. This is only displayed when the mailbox has a linked job flow sheet.
	Delete Documents after Print or Retrieve	Allows you to set whether to automatically delete documents after they are printed or retrieved.
	Delete Expired Documents	Allows you to set whether to automatically delete documents when they reach the specified expiration dates.
	Number of Documents in this Mailbox	Displays the number of documents stored in the mailbox.
Link Job Flow Sheet to this Mailbox	Sheet Type	Select the type of sheets to be displayed in the [Job Flow Sheet List] page.
	Sheet Order	Select the display order of job flow sheets to be displayed in the [Job Flow Sheet List] page.
	Display Job Flow Sheets List	Displays the [Job Flow Sheet List] page, which allows you to link job flow sheets to mailboxes and delete/edit/create job flow sheets.

5.4.3 Mailbox Setup

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

Mailbox	Mailbox Number	Displays the number of the selected mailbox.
	Mailbox Name	Displays the name of the mailbox.
	Mailbox Passcode	Displays the passcode to the mailbox. 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 Mailbox Passcode	Allows you to select whether and when the passcode for the mailbox is required.
	Delete Documents after Print or Retrieve	Allows you to set whether to automatically delete documents after they are printed or retrieved.
	Delete Expired Documents	Allows you to set whether to automatically delete documents when they reach the specified expiration dates.

5.4.4 Import the documents

The following describes methods for importing documents stored on the machine's mailbox.

1. Select [Mailbox Number] or [Document List] on the [Mailbox] page.
2. Place a check next to each document to be imported, and click [Retrieve] or [Print Document].

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

5.5 Import the Audit Log File

The following describes methods for importing the Audit Log .

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 Audit Log is enabled from the Audit Log hot link on the Properties tab of Internet Services, accessed from a networked workstation running a web browser (Refer to 2.19).
And additionally requires the enabling of SSL/TLS encryption for Accessing to the logged data.

Access to the logged data is also accomplished from the Audit Log hot link on the Properties tab of Internet Services as follows.
The logged data is not viewable from the local UI.

1. Open your Web browser and enter the TCP/IP address of the machine in the Address or Location field. Press Enter.
2. Supply the Administrator ID and Password, when prompted.
3. Click the Properties tab.
4. Click the Audit Log hot link.
5. Select the [Save as Text File].

Events tracked in the Audit Log, include: Starting and Stopping of the machine, Login/Logout events, Changes to system settings, and job completions.
The machine generates audit logs that track events/actions (e.g., copy/print/scan/fax job submission) to logged in users, and each log entry contains a timestamp.
The audit logs are only available to system administrators and can be downloaded via the web interface for viewing and analysis.
By adopting a policy of regularly downloading and saving the audit logs, users can satisfy the tracking requirements for transmission of data outside of the local environment.

Audit Log file is saved in the HDD maximum of 15000 affairs, and if it exceeds 15000 old data will be deleted every 50 affairs and the newest data will be overwritten.
There is no deletion function.

6 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.

6.1 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 the Key Operator 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.

6.2 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.
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
16-210 16-211 16-212 16-213 16-214	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.
016-703	An e-mail specifying a non-registered or invalid mailbox 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 mailbox with the specified number. • Send an e-mail to a valid mailbox. • Contact the Xerox Welcome Center if the problem persists.
016-704	The hard disk ran out of space, because the mailboxes are full. Delete unnecessary documents from the mailboxes.
016-705	Unable to register the secure print document, mailbox document, or billing data using the print driver, or unable to register the scanned document in the mailbox, 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 mailbox passcode. Enter the correct passcode.
016-714	The specified mailbox does not exist. Create a new mailbox or specify an existing mailbox.
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.
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.
016-793	The hard disk has run out of space. Delete unnecessary data or initialize the hard disk if the saved data are not needed anymore.
016-982	The hard disk has run out of space. Delete unnecessary data from the hard disk or documents in mailboxes.
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] using the Key Operator access.