



Xerox WorkCentre 7120

Security Function Supplementary Guide

Table of Contents

Before Using the Security Function	4
Preface.....	4
Security Features.....	5
Settings for the Secure Operation	5
Data Restoration.....	6
Starting use of the data encryption feature and changing the settings.....	6
Use of the Overwrite Hard Disk.....	7
Service Representative Restricted Operation.....	7
For Optimal Performance of the Security features	8
Confirm the Machine ROM version and the System Clock.....	9
How to check by Control Panel	9
How to check by Print Report.....	9
How to check the Clock	9
Initial Settings Procedures Using Control Panel	10
Use Passcode Entry from Control Panel.....	10
Authentication for entering the System Administration mode	10
Change the System Administrator's Passcode	11
Set Maximum Login Attempts	11
Set Service Rep. Restricted Operation.....	11
Set Overwrite Hard Disk	11
Set Data Encryption.....	12
Set Scheduled Image Overwrite	12
Set Authentication	12
Set Access Control	13
Set Private Print	13
Set User Passcode Minimum Length	14
Set Direct Fax.....	14
Preparations for settings on the CentreWare Internet Services.....	15
Set SMB	15
Set WebDAV.....	15
Set LDAP	15
Set SSL/TSL.....	16
Configuring Machine certificates.....	16
Set IPSec.....	16
Set SNMPv3.....	17
Set S/MIME.....	18
Regular Review by Audit Log	19
Set Audit Log.....	19
Import the Audit Log File	19
Authentication for the Secure Operation	20
Overview of Authentication.....	20

Users Controlled by Authentication.....	20
Machine Administrator.....	20
Authenticated Users (with System Administrator Privileges)	21
Authenticated Users (with No System Administrator Privileges).....	21
Unauthenticated Users	21
Local Machine Authentication (Login to Local Accounts).....	21
Remote Authentication (Login to Remote Accounts)	21
Authentication for Folder	24
Types of Folder	24
Operation Using Control Panel.....	26
User Authentication.....	26
Create/View User Accounts	26
Change User Passcode by General User	28
Folder / Stored File Settings	29
Folder Service Settings.....	29
Stored File Settings	29
Create Folder	30
Send from Folder.....	31
Private Charge Print.....	33
Operation Using CentreWare Internet Services	34
Accessing CentreWare Internet Services	35
Print.....	36
Scan (Folder Operation).....	37
Folder: List of Files	38
Edit Folder	38
Folder Setup	39
Import the files	39
Change User Passcode by System Administrator (Using CentreWare Internet Services)	40
Problem Solving.....	41
Fault Clearance Procedure	41
Fault Codes.....	42
Appendix	49

Before Using the Security Function

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

Preface

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

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 7120 System Administrator Guide

:Version 1.0, May 2010

WorkCentre 7120 User Guide

:Version 1.0, May 2010

The security features of the WorkCentre 7120 is supported by the following ROM versions.

Controller ROM	Ver. 1. 201.6
IOT ROM	Ver.4.21.0
ADF ROM	Ver. 7.06.50

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 7120 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 Set to [On]
- Scheduled Image Overwrite Set to [Enabled].
- Authentication Set to [Login to Local Accounts] or [Login to Remote Accounts]
- Access Control Set to [Locked] for Device Access and Service Access
- Private Print Set to [Save in Private Charge Print]
- User Passcode Minimum Length Set to [9] characters.
- Direct Fax Set to [Disable]: when remote authentication is used.
- SMB Set to [Disabled] for [NetBEUI]
- WebDAV Set to [Disabled] : when remote authentication is used.
- 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. [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 7120, 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.
- Administrators have to set the account policy in the LDAP server as follows.
 - set password policy to [9 or more characters]
 - set account lockout policy to [5 times]
- For secure operation, all of the remote trusted IT products that communicate with the machine implement the communication protocol in accordance with industry standard practice with respect to RFC/other standard compliance (SSL/TLS, IPSec, SNMPv3, S/MIME) and work as advertised.
- The settings described below are required same as the machine's configuration.
 1. SSL/TLS
Set the SSL client (WEB browser) and SSL server that communicate with the machine as following data encryption suite
 - SSL_RSA_WITH_RC4_128_SHA
 - SSL_RSA_WITH_3DES_EDE_CBC_SHA
 - TLS_RSA_WITH_AES_128_CBC_SHA
 - TLS_RSA_WITH_AES_256_CBC_SHA(Specifically, recommended browser is Microsoft internet Explorer 6/7/8, Mozilla Firefox 2.x/3.x)
 2. S/MIME
Set the machine and mail clients as following Encryption Method/Message Digest Algorithm.
 - RC2(128bit)/SHA1
 - 3Key Triple-DES(168bit)/SHA1
 3. IPSec
Set the IPSec host that communicates with the machine as following Encryption Method/Message Digest Algorithm.
 - AES(128bit)/SHA1
 - 3Key Triple-DES(168bit)/SHA1
 4. SNMPv3
Encryption Method of SNMPv3 is DES fixed. Set the Message Digest Algorithm to SHA1.

Important:

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

For secure operation, when you Change [Authentication Type], please initialize the hard disk by reset [Data Encryption] and changing the [encryption key].

For preventing SSL vulnerability, you should set the machine address in proxy exclusion list of browser.

By this setting, secure communication will be ensured because the machine and the remote browser communicate directly without Proxy server, and you can prevent man-in-the-middle attack.

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.

Use Passcode Entry from Control Panel

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

Authentication for entering the System Administration mode

1. Press the <Log In/Out> button on the control panel.
2. Enter "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 Data Encryption

1. Select [System Settings] on the [Tools] screen.
2. Select [Common Service Settings].
3. Select [Other Settings].
4. On the [Other Settings] screen, select [Data Encryption].
5. Select [Change Settings].
6. Select [On].
7. Select [Keyboard], and enter a New Encryption Key of 12 characters.
8. Select [Save].
9. Select [Keyboard], and Re-enter the Encryption Key.
10. Select [Save] twice.
11. Select [Yes] to make the change.
12. Select [Yes] to Reboot.

Set Scheduled Image Overwrite

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

Set Authentication

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

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

6. Select [System Settings] on the [Tools] screen.
7. Select [Connectivity&Network Setup].
8. Select [Remote Authentication/Directory Service].

9. Select [Authentication System Setup].
10. On the [Authentication System] screen, Select [LDAP].
11. Select [Close].
12. To exit the [Remote Authentication/Directory Service] screen, select [Close] in the upper right corner of the screen.

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].

When [Login to Local Accounts] is selected

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

When [Login to Remote Accounts] is selected

- 1) On the [Receive Control] screen, select [Save As Private Charge Print Job].
6. Select [Save].
7. To exit the [Charge/Private Print Settings] screen, select [Close] in the upper right corner of the screen.

Set User Passcode Minimum Length

Note: This feature is only applicable to Local Authentication mode.

1. Select [Authentication/Security Settings] on the [Tools] screen.
2. Select [Authentication].
3. Select [Passcode Policy].
4. On the [Passcode Policy] screen, select [Minimum Passcode Length].
5. Select [Change Settings].
6. On the [Minimum Passcode Length] screen, select [Set].
7. With [▲] and [▼], set [9].
8. Select [Save].
9. To exit the [Passcode Policy] screen, select [Close] in the upper right corner of the screen.
10. To exit the [Tools] screen, press the < Services> button on the control panel.

Set Direct Fax

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

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

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 WebDAV

Note • When remote authentication is used, use the following procedure to disable WebDAV.

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

Set LDAP

1. Click [+] on the left of the [Connectivity] folder on the [Properties] screen.
2. Click [+] on the left of the [Protocols] folder.
3. Click [+] on the left of the [LDAP] folder.

4. Select [LDAP Server].
5. On the each menu, set the LDAP Server information.
6. 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] and [LDAP- SSL / TLS Communication].
9. Click the [Apply] button.
10. Click the [Reboot Machine] button.

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

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

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.

Remote Authentication (Login to Remote Accounts)

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

Note • The user information used for remote authentication can be stored in the machine. For details, refer to Administrator Guide.

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.

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
- Print
- Job Flow Sheets

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	X
	Link	X	X
	Auto Run	O	X
	Manual Run	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
	Link	O
	Auto Run	O
	Manual Run	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.

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

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

Important

In the case of interrupting when other people use the machine, please logout before canceling the interrupt mode.

Example:

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

Note: Before enter the User ID and password, please select "Registered User" or "System Administrator" when remote authentication is used

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

In an LDAP server, on the other hand, the system administrator's ID is not pre-registered.

Although "admin" can be registered as a user ID, it cannot be the system administrator's ID.

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,

6. Select [Create/View User Accounts] under [Authentication].
7. Select a User ID number.
8. Press [Create/Delete].
9. When a new user account is to be created, a keyboard screen is displayed. Enter a user ID, and then select [Save].
10. Configure the required settings.
11. 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.

Note: This feature is only applicable to Local Authentication mode.

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 passcode 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.
1. Select [Send from Folder] on the touch screen.
2. Select the [Folder name] to be displayed on the screen.
3. 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.
	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.
Delete		Deletes the selected files in the folder.

Edit Folder

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

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

Folder Setup

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

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

Import the files

The following describes methods for importing files stored on the machine's Folder.

=Select [Folder Number] or [Folder: List of Files] on the [Folder] page.

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

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

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

Note: This feature is only applicable to Local Authentication mode.

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.

If an error caused the printing to end abnormally or a malfunction occurred in the printer, then an error message code (***.***) is displayed.

Refer to the following table for error codes and information on how to rectify the problem. If an error code not described in the following tables is displayed, or the problem persists even after you have tried the following solutions, contact the Customer Support Center.

Tip

If an error code is displayed, all print data of the printer as well as print data stored in the builtin memory of the machine is discarded.

Errors are divided into the following **Categories**:

This section explains error codes.

If an error caused printing to end abnormally, or a malfunction occurred in the machine, then an error message code (* * * - * * *) is displayed.

For faxing, an error code is also displayed on [Activity Reports] and [Transmission Report - Job Undelivered]. Refer to the following table for error codes to rectify problems.

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

If an error code appears that is not listed in the table below, or if an error persists after following the listed solution, contact our Customer Support Center. The contact number is printed on the label or card attached on the machine. Errors are classified into the following categories.

- C: Copy
- P: Print
- F: Fax
- S: Scan
- M: Mail
- O: Others

Error Code	Category						Cause and Remedy
	C	P	F	S	M	O	
016-210 016-211 016-212 016-213 016-214	✓			✓			Cause: An error occurred in the software settings. Remedy: Power-cycle the printer. Contact the Customer Support Center.
016-450						✓	Cause: The SMB host name already exists. Remedy: Change the host name. For information about network settings, refer to the System Administration Guide.

016-454					✓	Cause: Unable to retrieve IP address from DNS. Remedy: Check the DNS configurations and IP address retrieve method. For information about network settings, refer to the System Administration Guide.
016-455					✓	[Cause] Connection to the SNTP server was timed out. [Remedy] Check the network cable connection and the IP address of the SNTP server. Refer to "Machine Clock/Timers" .
016-456					✓	[Cause] Received from the SNTP server a message saying that it was not synchronized with the standard time source. [Remedy] Check the SNTP server settings. Refer to "Machine Clock/Timers" .
016-503					✓	[Cause] Unable to resolve the SMTP server name when sending email. [Remedy] Check on the CentreWare Internet Services if the SMTP server settings are correct. Also, check the DNS server settings.
016-504					✓	[Cause] Unable to resolve the POP3 server name when sending email. [Remedy] Check on CentreWare Internet Services if the POP3 server settings are correct. Also, check the DNS server settings.
016-505					✓	[Cause] Unable to login to the POP3 server when sending e-mail. [Remedy] Check on CentreWare Internet Services if the user name and password used in the POP3 server are correct.
016-513				✓		[Cause] A time-out occurred while the machine was waiting for a response from the SMTP server. [Remedy] The server or network may be overloaded. Wait for a while, and try again.
016-574				✓		[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because the host or server name of the FTP server could not be resolved. [Remedy] Check the connection to the DNS server. Check if the FTP server name is registered correctly on the DNS server.
016-575				✓		[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because the DNS server address was not registered. [Remedy] Specify the correct DNS server address. Or, specify the destination FTP server using its IP address.
016-576				✓		[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because it could not connect to the FTP server. [Remedy] Ensure that both the destination FTP server and the machine are available for network communications, by checking the following: □ The IP address of the server is set correctly. The network cables are plugged in securely.
016-577				✓		[Cause] Unable to connect to the FTP service of the destination server. [Remedy] Take one of the following actions: □ Check if the FTP service of the server is activated. □ Check if the FTP port number of the server is correctly registered on the machine.
016-578				✓		[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature due to unsuccessful login to the FTP server. [Remedy] Check if the login name (user name) and password are correct.
016-579				✓		[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because the scanned image could not be saved in the FTP server after connection. [Remedy] Check if the FTP server's save location is correct.
016-580				✓		[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because the file or folder name on the FTP server could not be retrieved after connection. [Remedy] Check the access privilege to the FTP server.
016-581				✓		[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because the suffix of the file or folder name exceeded the limit after connection. [Remedy] Change the file name, or change the destination folder on the FTP server. Or, move or delete files from the destination folder.

016-582				✓		<p>[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because file creation was not successful on the FTP server after connection.</p> <p>[Remedy] Take one of the following actions: □ Check if the specified file name can be used in the save location. □ Check if enough space is available in the save location.</p>
016-583				✓		<p>[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because lock folder creation was not successful on the FTP server after connection.</p> <p>[Remedy] Take one of the following actions: □ If any lock directory (.LCK) exists in the forwarding destination, delete it manually, then try executing the job again. □ Check if the specified folder name can be used in the save location. □ Check if the same folder name exists in the save location. □ Check if enough space is available in the save location.</p>
016-584				✓		<p>[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because folder creation was not successful on the FTP server after connection.</p> <p>[Remedy] Take one of the following actions: □ Check if the specified folder name can be used in the save location. □ Check if the same folder name exists in the save location. □ Check if enough space is available in the save location.</p>
016-585				✓		<p>[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because file deletion was not successful on the FTP server after connection.</p> <p>[Remedy] Check the access privilege to the FTP server.</p>
016-586				✓		<p>[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because lock folder deletion was not successful on the FTP server after connection.</p> <p>[Remedy] Take one of the following actions: □ Check the access privilege to the FTP server. □ If any lock directory (.LCK) exists in the forwarding destination, delete it manually, then retry executing the job.</p>
016-587				✓		<p>[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because folder deletion was not successful on the FTP server after connection.</p> <p>[Remedy] Check the access privilege to the FTP server.</p>
016-588				✓		<p>[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because the data could not be written in the FTP server after connection.</p> <p>[Remedy] Check if enough space is available in the save location.</p>
016-589				✓		<p>[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because the data could not be read from the FTP server after connection.</p> <p>[Remedy] Check the access privilege to the FTP server.</p>
016-593				✓		<p>[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because an internal error occurred after connection to the FTP server.</p> <p>[Remedy] Try again. If the error persists, contact our Customer Support Center.</p>
016-594 016-595 016-596				✓		<p>[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because a network error occurred.</p> <p>[Remedy] Try again. If the error persists, contact our Customer Support Center.</p>
016-703					✓	<p>Cause: Mail specifying a non-registered or invalid mailbox number was received.</p> <p>Remedy: Take one of the following actions: Request the sender to register the mailbox with the specified number. Request the sender to send to a valid mailbox.</p>
016-704					✓	<p>Cause: Documents stored in the mailbox have reached the hard disk capacity limit.</p> <p>Remedy: Remove unnecessary documents from the mailbox, and save the document. Refer to Delete Documents After Retrieval .</p>

016-705		✓		✓			Cause: Secure print documents cannot be registered because of hard disk malfunction. Remedy: Contact the Customer Support Center. Refer to Secure Print.
016-706		✓					Cause: The maximum number of Secure Print users has been exceeded and no space is available on the hard disk. Remedy: Remove unnecessary documents stored on the printer, and delete unnecessary Secure Print users. For information about Secure Print, refer to Secure Print . For information about mailboxes, refer to Delete Documents AfterRetrieval
016-711					✓	✓	Cause: The configured maximum e-mail size has been exceeded. Remedy: Take one of the following actions and resend the e-mail: Decrease document pages Reduce the Scan Resolution Reduce the Scan Magnification Have the system administrator increase your Maximum Send E-mail Data Size
016-713						✓	Cause: The password set to the mailbox and the inputted password were not in agreement. Remedy: Enter the correct password.
016-714						✓	Cause: Specified mailbox does not exist. Remedy: Create a mailbox or specify the existing mailbox.
016-764					✓		Cause: Could not connect to the SMTP server. Remedy: Contact the SMTP Server Administrator.
016-765					✓		Cause: Could not send mail as the hard disk on the SMTP server was full. Remedy: Contact the SMTP Server Administrator.
016-766					✓		Cause: An error occurred on the SMTP server. Remedy: Contact the SMTP Server Administrator.
016-767					✓		Cause: Could not send mail as the mail address was wrong. Remedy: Check the mail address and transmit again.
016-768					✓		Cause: Could not connect to the SMTP server as the mail address of the machine was incorrect. Remedy: Check the mail address of the machine.
016-769					✓		Cause: The SMTP server does not support confirmation of mail distribution (DSN). Remedy: Send mail without setting confirmation of mail distribution (DSN).
016-770			✓				[Cause] Direct Fax is disabled. [Remedy] Check the system administrator if Direct Fax is available. If it is available, contact our Customer Support Center.
016-771 016-772				✓			Cause: Unable to retrieve scan data repository address from the CentreWare scan service. Remedy: Check the DNS address or define the scan data repository address by its IP address.
016-773						✓	Cause: The IP address for the machine is not set properly. Remedy: Check the DHCP environment or specify a fixed IP address for the machine. For information about network settings, refer to the System Administration Guide.
016-774		✓	✓			✓	Cause: Compression conversion is not possible due to insufficient hard disk space. Remedy: Remove unnecessary data from the hard disk to increase free disk space.

016-781				✓		<p>[Cause] Unable to connect to the FTP server.</p> <ul style="list-style-type: none"> •Unable to establish a connection between the machine and the server. •The ASCII characters are not used for the host name specified on the machine, though the connection between the machine and the server has been established. <p>[Remedy] Take one of the following actions:</p> <ul style="list-style-type: none"> •Make sure the network cables are plugged in securely. •Enter the host name using ASCII characters in [Tools] > [System Settings] > [Connectivity & Network Setup] > [Machine's E-mail Address/Host Name].
016-788					✓	<p>Cause: Failed to load a file from the Web browser. Remedy: Perform the following actions, and try again. Reload the browser page Restart the browser Power-cycle the machine</p>
016-791					✓	<p>[Cause] Failed to access to the destination computer or the save location for Network Scanning. [Remedy] Check the directory configuration and files on the server, the access privileges for the destination or the location, and check if you are authorized to access the specified destination computer or server.</p>
018-400					✓	<p>[Cause] When IPSec is enabled,there is an inconsistency in IPSec settings as follows.</p> <ul style="list-style-type: none"> •The password is not set when [Authentication Method] is set to [Preshared Key] •An IPSec certificate is not set set when [Authentication Method] is set to [Digital Signature] <p>[Remedy]Check the IPSec settings, and enable IPSec again.</p> <ul style="list-style-type: none"> • When [Authentication Method] is set to [Preshared Key], set the password. • When [Authentication Method] is set to [Digital Signature],set an IPSec certificate.
018-502				✓		<p>[Cause] During the transfer using [SMB] of the [Scan to PC] feature, the login to the server was failed because the computers permitted to log in were limited. [Remedy] Check the property information for the specified user, and check if the server sets the login limit for computers.</p>

018-505					✓	<p>[Cause] If an error occurred during SMB authentication, the probable causes are as follows: <input type="checkbox"/> Authentication failed because of the incorrect user name or incorrect password.</p> <ul style="list-style-type: none"> •The time does not match on the SMB server and the machine. (This may occur when Windows Server 2003 is used.) •When the destination computer is Macintosh, the specified user has not been registered as a user who is permitted to use Windows Sharing. <p>If an error occurred during data transfer via SMB, the probable causes are as follows:</p> <ul style="list-style-type: none"> •Login to the SMB server failed while transferring the scanned image, due to the incorrect user name or incorrect password. •The time does not match on the SMB server and the machine. (This may occur when Windows Server 2003 is used.) •When the destination computer is Macintosh, the specified user has not been registered as a user who is permitted to use Windows Sharing. <p>[Remedy] Take one of the following actions, and try again:</p> <ul style="list-style-type: none"> •Check the user name and password with the network administrator. •When using Windows Server 2003, make sure to match the time set on the SMB server and the machine. •When the destination computer is Macintosh, specify a user who is permitted to use Windows Sharing. <p>The password cannot be retrieved. If you have forgotten the password, reset the password.</p> <p>To reset the password:</p> <ol style="list-style-type: none"> 1) Select [Start] > [Programs] > [Administrative Tools] > [Active Directory Users and Computers] on the Active Directory domain controller where the user information is set. 2) Display the user information by selecting [Domains] > [Users] from the left side frame of the [Active Directory Users and Computers] window. 3) Right-click the appropriate user from the right side frame of the [Active Directory Users and Computers] window, then select [Reset Password].
018-543				✓		<p>[Cause] During the transfer using [SMB] of the [Scan to PC] feature, logging in to the SMB server failed because one of the following problems occurred on the shared name of the SMB server.</p> <ul style="list-style-type: none"> •The specified shared name does not exist on the server. •Unavailable characters are used in the specified shared name. •When the server is Macintosh, the specified shared name may not have an access right. <p>[Remedy] Confirm the specified shared name, and set the name correctly.</p>
018-547				✓		<p>[Cause] During the transfer using [SMB] of the [Scan to PC] feature, the number of login users to the SMB server have exceeded the limit.</p> <p>[Remedy] Take one of the following actions:</p> <ul style="list-style-type: none"> •Check how many users can access to the shared folder. •Check whether the number of login users have exceeded the limit.
027-452					✓	<p>Cause: IP address already exists. Remedy: Change the IP address. For information about network settings, refer to the System Administration Guide.</p>
027-500				✓	✓	<p>Cause: Unable to resolve SMTP server name during answer E-mail send. Remedy: Check that the SMTP server settings from CWIS are correct.</p>
027-706					✓	<p>[Cause] Unable to find the S/MIME certificate associated with the machine's e-mail address when sending e-mail. [Remedy] Import the S/MIME certificate corresponding to the mail address to the machine.</p>
027-707					✓	<p>[Cause] The S/MIME certificate associated with the machine's email address has expired. [Remedy] Ask the sender to issue a new S/MIME certificate and import the certificate to the machine.</p>

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

Appendix

List of Setting Procedures

Item	Using Control Panel	Using CentreWare Internet Services	Default
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]	-	On
Change the System Administrator Passcode	[Authentication/Security Settings] > [System Administrator Settings] > [System Administrator's Passcode]	[Security] > [System Administrator Settings]	-
Set Maximum Login Attempts	[Authentication/Security Settings] > [Authentication] > [Maximum Login Attempts By System Administrator]	[Security] > [System Administrator Settings]	5
Set Service Rep. Restricted Operation	[System Settings] > [Common Service Settings] > [Other Settings] > [Service Rep. Restricted Operation].	[Security] > [Service Representative Restricted Operation]	Off
Set Overwrite Hard Disk	[Authentication/Security Settings] > [Overwrite Hard Disk]	-	On
Set Data Encryption	[System Settings] > [Common Service Settings] > [Other Settings] > [Data Encryption]	-	Off
Set Scheduled Image Overwrite	[Authentication/Security Settings] > [Overwrite Hard Disk] > [Scheduled Image Overwrite].	[Security] > [On Demand Overwrite] > Scheduled	Off
Set Authentication	[Authentication/Security Settings] > [Authentication] > [Login Type].	[Security] > [Authentication Configuration]	Off
Set Access Control	[Authentication/Security Settings] > [Authentication] > [Access Control]	[Security] > [Authentication Configuration] > [Next] > [Device Access]	Off
Set Private Print	[Authentication/Security Settings] > [Authentication] > [Charge/Private Print Settings].	-	Off
Set User Passcode Minimum Length	[Authentication/Security Settings] > [Authentication] > [Passcode Policy] > [Minimum Passcode Length]	[Security] > [User Details Setup] > [Minimum Passcode Length]	0
Set Direct Fax	[System Settings] > [Fax Service Settings] > [Fax Control] > [Direct Fax]	-	On
Set SMB	-	[Connectivity] > [Port Setting]	On

Set WebDAV	「Connectivity&Network Setup」> [Port Setting]	[Connectivity] > [Port Setting]	On
Set LDAP	-	[Connectivity] > [Protocol] > [LDAP] > [LDAP Server]	-
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]	Off
Configuring Machine Certificates	-	[Security] > [Machine Digital Certificate Management] > [Upload Signed Certificate].	-
Set IPSec	[System Settings] > [Connectivity & Network Setup] > [Security Settings] > [IPSec Settings]	[Security] > [IPSec]	Off
Set SNMPv3	-	[Connectivity] > [Protocols] > [SNMP Configuration]	Off
Set S/MIME	[System Settings] > [Connectivity & Network Setup] > [Security Settings] > [S/MIME Settings]	[Security] > [SSL/TLS Settings] > [S/MIME Communication]	Off
Set Audit Log, Import the Audit LogFile	-	[Security] > [Audit Log].	Off
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]	-