Xerox Color 550/560 Printer

Security Function Supplementary Guide

Table of Contents

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.

Xerox Color 550/560 Printer System Administrator Guide
: Version 1.0: August 2010 (701P50980_en)
Xerox Color 550/560 Printer User Guide
: Version 1.0: August 2010 (701P50979_en)

The security features of the Xerox Color 550/560 Printer is supported by the following ROM versions.

Controller ROM	Ver. 1.203.1
IOT ROM	Ver. 62.23.0
IIT ROM	Ver. 6.13.0
ADF ROM	Ver. 12.4.0

Important:
The machine has obtained IT security certification for Common Criteria EAL3+ALC_FLR.2.

This certifies that the target of evaluation has been evaluated based on the certain evaluation criteria and methods, and that it conforms to the security assurance requirements.

Note: However, that your ROM and Guidance may not be the certified version because it may have been updated along with machine improvements.
For the latest information on security and operation concerning your device, please download the latest edition of Guidance from http://www.support.xerox.com/support

Security Features

Xerox Color 550/560 Printer has the following security features:

- Hard Disk Data Overwrite

- Hard Disk Data Encryption

- User Authentication

- System Administrator's Security Management

- Customer Engineer Operation Restriction

- Security Audit Log

- Internal Network data protection

- Self Test

- Information Flow Security

Settings for the Secure Operation

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

- Passcode Entry from Control Panel   Default [On].
- The System Administrator Passcode characters.   Change the default passcode "1111" to another passcode of 9 or more
- 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   Default [3 Overwrites].
- Data Encryption   Default [On]
- Scheduled Image Overwrite   Set to [Enabled].
- Authentication   Set to [Login to Local Accounts] or [Login to Remote Accounts]
- Access Control   Set to [Locked] for Device Access and Service Access
- Private Print   Set to [Save as Private Charge Print]
- User Passcode Minimum Length   Set to [9] characters.
- Direct Fax   Set to [Disable]: when remote authentication is used.
- Auto Clear   Default [Enabled].
- Report Print   Set to [Disable].
- Self Test   Set to [Enabled]

- Software Download   Set to [Disabled]

- SMB   Set to [Disabled] for [NetBEUI]

- WebDAV   Set to [Disabled]

- Receive E-mail   Default [Disabled]

- IPP   Default [Enabled]

- 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]

- Browser Refresh   Set to [Disabled] :

- Job Deletion   Set to [Administrator Only].

Important:

The security will not be warranted if you do not correctly follow the above setting instructions.

The Information 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 Color 550/560 Printer, select [On] and then set [Maintenance Passcode] to restrict the Service Representative from entering the System Administration mode.

Important:
If the System Administrator's user ID and passcode are lost when [Service Rep. Restricted Operation] is set to [On], not only you but also we are no longer able to change any setting in the System Administration mode.

For Optimal Performance of the Security features

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

- Assign appropriate persons as system and machine administrators, and manage and train them properly.

- The manager and system administrators have to train users about the security policies and procedures of their organization.

- The machine have to be placed in a secure or monitored area that provides protection from unmanaged physical access to the machine.

- 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 passcode.
  ・A passcode has to contain both numeric and alphabetic characters.

- Users and administrators have to manage and operate it so that own user ID and passcode may not be disclosed to another person.

- Administrators have to set the account policy in the remote authentication server as follows.
  ・Set password policy to [9 or more characters]
  ・Set account lockout policy to [5 times]

- For secure operation, all of the remote trusted IT products that communicate with the machine 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, the recommended browser is Microsoft internet Explorer 6/7/8, Mozilla Firefox 2.x/3.x)

2.) S/MIME

   Set the machine and E-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

The encryption Method of SNMPv3 is DES fixed. Set [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. With 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 attacks.

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

Authentication for entering the System Administration mode

1. Press the <Log In/Out> button on the control panel.
2. Enter "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. Press the <Machine Status> button on the control panel.
7. Select [Tools].

Use Passcode Entry from Control Panel

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

Change the System Administrator's Passcode

1. Select [Authentication/Security Settings] on the [Tools] screen.
2. Select [System Administrator Settings].
3. Select [System Administrator's Passcode].
4. Select [New Passcode].
5. Enter a new passcode of 9 or more characters using the keyboard displayed, and then select [Save].
6. Select [Retype Passcode].

7. Enter the same passcode, and then select [Save].

8. Select [Save].

9. A confirmation window appears. Select [Yes] to confirm your entry.

Set Maximum Login Attempts

1. Select [Authentication/Security Settings] on the [Tools] screen.

2. Select [Authentication].

3. Select [Maximum Login Attempts By System Administrator].

4. On the [Maximum Login Attempts] screen, select [Limit Attempts].

5. With [▲] and [▼], set [5].

6. Select [Save].

Set Service 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 [New Passcode].

9. Enter a new passcode of 9 or more characters using the keyboard displayed, and then select [Save].

10. Select [Save].

11. Select [Retype Password/Passcode].

12. Enter the same passcode using the keyboard displayed, and then select [Save].

13. Select [Save].

14. Select [Yes] to make the change.

15. A confirmation window appears. Select [Yes] to confirm your entry.

16. To exit the [Other Settings] screen, select [Close].

Set Overwrite Hard Disk

1. Select [Authentication/Security Settings] on the [Tools] screen.

2. Select [Overwrite Hard Disk].

3. Select [Number of Overwrites].

4. On the [Number of Overwrites] screen, select [1 Overwrite] or [3 Overwrites].

5. Select [Save].

Set Scheduled Image Overwrite

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

Set Data Encryption

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

Set Authentication

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

   When [Login to Remote Accounts] is selected in step 4, proceed to steps 6 to 12.
6. Select [System Settings] on the [Tools] screen.
7. Select [Connectivity & Network Setup].
8. Select [Remote Authentication/Directory Service].
9. Select [Authentication System Setup].
10. Select [Authentication System].
11. Select [Change Settings].
12. On the [Authentication System] screen, Select [LDAP] or [Kerberos].
13. Select [Save].
14. To exit the [Remote Authentication/Directory Service] screen, select [Close].

Set Access Control

1. Select [Authentication/Security Settings] on the [Tools] screen.

2. Select [Authentication].

3. Select [Access Control].

4. Select [Device Access].

5. On the [Device Access] screen, select [Locked] for [All Services Pathway].

6. Select [Save].

7. Select [Service Access].

8. On the [Service Access] screen, select an item and then select [Change Settings].

9. Select [Locked].

10. Select [Save].
    Perform steps 8 and 10 for each item.

11. Select [Close].
12. Select [Feature Access].
13. On the [Feature Access] screen, select an Item by [Change Settings].
14. Select [Locked].
    Perform steps 13 and 15 for each item.
15. To exit the [Access Control] screen, select [Close].

Set Private Print

1. Select [Authentication/Security Settings] on the [Tools] screen.

2. Select [Authentication].

3. Select [Charge/Private Print Settings].

4. On the [Charge/Private Print Settings] screen, select [Received Control].

5. Select [Change Settings].

When [Login to Local Accounts] is selected

   1) On the [Receive Control] screen, select [According to Print Auditron].

   2) Select [Save As Private Charge Print Job] for [Job Login Success].

   3) Select [Delete Job] for [Job Login Failure].

   4) Select [Delete Job] for [Job without User ID].

When [Login to Remote Accounts] is selected

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

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

Set User Passcode Minimum Length

Note: This feature is only available in Local Authentication mode.

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

Set Direct Fax

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 [Change Settings].
6. Select [Disabled].
7. Select [Save].
8. To exit the [Fax Control] screen, select [Close].

Set Auto Clear

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

Set Report Print

1. Select [System Settings] on the [Tools] screen.

2. Select [Common Service Settings].

3. Select [Reports].

4. Select [Print Reports Button].

5. Select [Disabled].

6. Select [Save].

7. To exit the [Reports] screen, select [Close].

Set Self Test

1. Select [System Settings] on the [Tools] screen..

2. Select [Common Service Settings].

3. Select [Maintenance].

4. Select [Power on Self Test].

5. Select [On]

6. Select [Save].

7. To exit the [Maintenance] screen, select [Close].
8. Select [Reboot now] on the confirmation screen.

Set Software Download

1. Select [System Settings] on the [Tools] screen.

2. Select [Common Service Settings].

3. Select [Other Settings].

4. On the [Other Settings] screen, select [Software Download].

5. Select [Change Settings].

6. Select [Disabled].

7. Select [Save].

8. To exit the [Common Service Settings] screen, select [Close].

9. To exit the [Tools] screen, press the <Services> button on the control panel.

Initial Settings Procedures Using CentreWare Internet Services

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

Preparations for settings on the CentreWare Internet Services

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

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

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

Set SMB

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

Set WebDAV

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

Set Receive E-mail

1. Click [Connectivity] on the [Properties] screen.
2. Click [Port Setting].

3. Uncheck the [Recieve E-mail] box.

4. Click the [Apply] .

Set IPP

1. Click [Connectivity] on the [Properties] screen.

2. Click [Port Setting].

3. Check the [Enabled] box for [IPP].

4. Click the [Apply] .

Set LDAP Server

1. Click [Connectivity] folder on the [Properties] screen.

2. Click [Protocols].

3. Click [LDAP].

4. Select [LDAP Server].

5. On the each menu, set the LDAP Server information.

6. Click the [Apply] .

Note: You can configure the administrator group on the machine so that the members of that group will have System Administrator access to the machine.
In [System Administrator Access Group] boxes, enter a name for the group.
Entries should be in base DN format (for instance, cn=admin, cn=users, dc=xerox, dc=com).
You can also place restrictions on the use of the Copy, Fax, Scan, Print, and other features, by enter a name for the group in [Service Access Group] boxes,

Set Kerberos Server

1. Click the [Security] on the [Properties] screen.

2. Click the [Remote Authentication Servers].

3. Select [Kerberos Server].

4. On the each menu, set the Kerberos Server information.

5. Click the [Apply] .

Note: When an Kerberos server is used as a remote authentication server, you can configure the administrator group on the machine by setting the System Administrator Access Group on the LDAP server.

Set SSL/TSL

1. Click [Security] on the [Properties] screen.

2. Click [Machine Digital Certificate Management].

3. Click the [Create New Self Signed Certificate] .

4. Set the size of the Public Key as necessary.

5. Set Issuer as necessary.

6. Click the [Apply] .

7. Click [SSL/TLS Settings].

8. Select [Enabled] check box for [HTTP - SSL / TLS Communication] and [LDAP- SSL / TLS Communication].

9. Click the [Apply] .

10. Click the [Reboot Machine] .

Note: For secure operation, check the [Enabled] box for [Verify Remote Server Certificate], and import the CA certificate according to the same procedure as in "Configuring Machine Certificates".
If SMTP server has SSL/TLS function and you want to use secure e-mail, configure the [SMTP-SSL/TLS Communication].

Configuring Machine certificates

1. Click [Security] on the [Properties] screen.

2. Click [Machine Digital Certificate Management].

3. Click the [Upload Signed Certificate] .

4. Enter a file name for the file you want to import, or select the file to be imported by clicking the [Browse] .

5. Enter the [Password], and Enter the [Retype Password].

6. Click the [Import] .

Set IPSec

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

1. Click [Security] on the [Properties] screen.

2. Click [IPSec].

3. Check the [Enabled] box for [Protocol].
   For the [Pre-Shared Key] setting, proceed to steps 4 to 5.
   For the [Digital Signature] setting, proceed to steps 6 to 11.

4. Select [Pre-Shared Key] for IKE Authentication Method.
   This is used to ensure confidentiality of communications between the machine and a client computer, or the machine and a server.

5. Enter a Pre-Shared Key in the [Shared Key] and [Verify Shared Key] box.
   Please set the IPSec address successively.

6. Click [Certificate Management] in [Security].

7. Select [IPSec] for Certificate Purpose.

8. Click the [Display the list] , and check a desirable Certificate.

9. Click the [Certificate Details] .

10. Click the [Use this certificate] .

11. On the [IPSec] screen, Select [Digital Signature] for IKE Authentication Method.
    Set the IPSec address successively.

Set IPSec Address

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

Note: When you select [Enabled] for [Communicate with Non-IPSec Device] setting, the machine allows communications with non-IPSec devices other than specified for [Specify Destination IPv4 Address] or [Specify Destination IPv6 Address].

Set SNMPv3

1. Click [Connectivity] on the [Properties] screen.
2. Click [Protocols].
3. Click [SNMP Configuration].
4. Check the [Enable SNMPv3 Protocol] box.
5. Uncheck the [Enable SNMP v1/v2c Protocols] box.
6. Click the [Apply] .
7. Click the [Edit SNMPv3 Properties]   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] .

Note: Authentication Password and Privacy Password have to be changed certainly from default Password.
In using SNMPv3, use the IPSec protocol simultaneously. Therefore the IP address of the client for SNMPv3 have to be set according to the procedures "Set IPSec Address", Enter the IP Address in the [Specify Destination IPv4/IPv6 Address] box.
Since the machine cannot communicate by SNMP v1/v2, the port setting on the client Printer Driver have to be unchecked 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".

1. Click [Configuration Overview] on the [Properties] screen.
2. Click [Settings] for [E-mail].
3. Click the [Configure] for [E-mail Settings], and enter the machine's E-mail address in the [From address] box.
4. Click the [Apply] .
5. Click [Security] on the [Properties] screen.
6. Click [Certificate Management].
7. Select [S/MIME] for [Certificate Purpose].
8. Click the [Display the list] , and check a desirable Certificate.
9. Click the [Certificate Details] .
10. Click the [Use this certificate] .
11. Click [SSL/TLS Settings].
12. Check the [Enabled] box for [S/MIME Communication].
13. Click the [Apply] .
14. Click the [Reboot Machine] .
    After the machine is restarted, refresh the browser and Click [Properties] tab.
15. Click [Security].
16. Click [S/MIME Settings].
17. Uncheck the [Enabled] check box for [Receive Untrusted E-mail].
18. Select [Always add signature] for [Digital Signature - Outgoing E-mail].
19. Click the [Apply] .

Set Browser Refresh

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

Set Job Deletion

1. Click [General Setup] on the [Properties] screen.
2. Click [Job Management].

3. Select [Administrators Only] for [Job Deletion].
4. Click the [Apply] .
5. Click the [Reboot Machine] .

Important:

Allows the user to pause an active copy, print, scan or Embedded Fax job while it is being processed by the machine.

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

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 [Security] .
5. Click [Audit Log].
6. Check the [Enabled] box for [Audit Log].
7. Click the [Apply] .

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.
In addition, SSL/TLS communication must be enabled in order to access 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].

Self Testing

This section describes the Self Test function and its setting procedure from the Control Panel.

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

The machine verifies the area of NVRAM and SEEPROM including setting data at initiation, and displays an error on the control panel at error occurrence.
Also, when Self Test function is set at initiation, The machine calculates the checksum of Controller ROM to confirm if it matches the specified value, and displays an error on the control panel at error occurrence.

Set Self Test

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

Authentication for the Secure Operation

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

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

Overview of Authentication

Users Controlled by Authentication

The following 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 or remote server, 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 or Kerberos 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

Service Access control per user

- Service access and print & copy quota control can be set per user.
  The system administrator sets copy & quota limitation per user via the control panel and CWIS.
  When print or copy volume exceed the registered number, the user can not use the function. The counted number needs to be cleared by system administrator.

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.

In Local Authentication mode, 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.

Operations available for Folder.

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

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

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

O: Operation available

X: Operation not available

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

• Confidential fax reception

• Confidential Internet Fax reception

• Retrieving files that use scan driver or Folder Viewer 3

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

Operation Using Control Panel

This section 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, a user must be authenticated with an ID and passcode.

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

All features on the control panel become available.

Important:
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 a remote authentication 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,

1. Select [Create/View User Accounts] under [Authentication].
2. Select a User ID number.

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

User ID

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

User Name

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

Passcode

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

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

E-mail Address

Allows you to enter the E-mail address. The specified address is the sender's address displayed on the [E-mail] screen. Enter up to 128 characters.

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

Account Limit

Displays the [Account No. XXX - Account Limit] screen. Select [Copy Service], [Fax Service], [Scan Service] or [Print Service] to specify feature access permissions and account limits for that service.

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

Account Limit - Displays the [Account No. xxx - {Service} Limit] screen. Enter an account limit for [Color] and [Black] to specify the maximum number of pages allowed to be processed by that account. The maximum number can be entered within the range of 1-9,999,999 pages.

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

User Role

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

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

Reset Total Impressions

Deletes all data tracked for the selected account.

Reset Account

Clears all settings and data for the selected account.

Change User Passcode by General User

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

Note: This feature is only applicable to Local Authentication mode.
Authenticate by the procedure as described [User Authentication]

1. Select [User Details Setup].
2. Select [Change Passcode] .
3. Enter the Current Passcode and select [Next].
4. On the Change Passcode screen, Select [Keyboard].
5. Enter a new passcode 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.

Job Deletion by System Administrator

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

Deleting the Copy, Scan, Fax scan job

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

Deleting the printing Job

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

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

3. A confirmation window appears. Select [Delete job] to cancel the job completely.

Deleting the sending Job(Scan, Fax) and receiving job(Fax).

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

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

Folder / Stored File Settings

This section describes the features that allow a System Administrator to configure various settings for Folder 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.

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.

Delete Files After Retrieval

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

Delete Expired Files

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

Send from Folder

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

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

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

File Name/Stored Date

Sorts the files by their names or the dates they were stored. Selecting the same option again toggles the order in which they are listed, as indicated with an upward (ascending order) or downward (descending order) triangle shown to the right of the name of the option selected.

Refresh

Updates the list of files in the Folder.

Select All

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

Print

Prints the selected file (s).

Delete

Deletes the selected file (s).

Private Charge Print

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

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

1. Press the <Log In/Out> button.
2. Enter your user ID and Passcode using the screen keypad or numeric keypad on the control panel, and select [Confirm].
3. Press the <Job Status> button on the control panel.
4. Select [Private 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.

5. Select a file to print or delete.
6. 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 Section 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.

> 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.

1. Click [Print] on the Main Panel of the home page.
2. The [Job Submission] page is displayed.
3. Job Submission Allows you to print 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.

1. Click [Scan] on the Main Panel of the home page.
2. Select the Folder hot link.
3. 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 id a shared Folder, this shows "Shared".

	Delete Files after Print or Retrieve	Allows you to set whether to automatically delete files after they are printed . Note: Retrieved files are not deleted .
	Delete Expired Files	Allows you to set whether to automatically delete files when they reach the specified expiration dates.
	Number of Files in this Folder	Displays the number of files stored in the Folder.
Link Job Flow Sheet to this Folder	Sheet Order	Select the display order of job flow sheets to be displayed in the [Job Flow Sheet List] page.

Folder Setup

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

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

Import the files

The following describes methods for importing files stored on the machine's Folder.
=Select [Folder Number] or [Folder: List of Files] on the [Folder] page.
Place a check next to each file to be imported, and click [Retrieve] or [Print File].

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

Printing Job Deletion

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

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

Change User Passcode by System Administrator (Using 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 [Security].
5. Click [Authentication Configuration].
6. Click the [Next] .
7. Enter the user number in [Account Number] and Click [Edit] .
8. Enter a new passcode from 9 or more characters in [Passcode].
9. Enter the same passcode in [Retype Passcode] and click the [Apply] .

Problem Solving

This section 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

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.

Error Code	Cause and Remedy
016-210 016-211 016-212 016-213 016-214 016-215	[Cause] An error occurred in the software. [Remedy] Switch off the machine power, make sure that the touch screen is blank, and then switch on the machine power. If the error still is not resolved, contact our Customer Support Center.
016-402	[Cause] The authentication connection timed out. [Remedy] Confirm the network connection and switch setting of the authentication device physically connected to the machine via a network, and check whether it is connected to the machine correctly.
016-403	[Cause] The root certificate did not match. [Remedy] Confirm the authentication server and store the root certificate of the server certificate of the authentication server into the machine. If you cannot acquire the root certificate of the server certificate, set [Server Certificate Verification] of [IEEE 802.1x Settings] to [Disabled] on the touch screen.
016-405	[Cause] An error occurred in the certificate stored in the machine. [Remedy] Initialize the certificate.
016-406	[Cause] An error occurred in the SSL client certificate. [Remedy] Take one of the following measures: Store an SSL client certificate in the machine, and set it as the SSL client certificate. If the SSL client certificate cannot be set, select an authentication method other than SSL.
016-450	[Cause] The SMB host name already exists. [Remedy] Change the host name.
016-454	[Cause] Unable to retrieve the IP address from DNS. [Remedy] Confirm the DNS configuration and IP address retrieve setting.

016-503	[Cause] Unable to resolve the SMTP server name when sending 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. are correct.
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] An error occurred in connecting to the SMTP server.
	[Remedy] The SMTP server or network may be overloaded. Wait for a while, and then execute the operation again.
016-522	[Cause] LDAP server SSL authentication error. Unable to acquire an SSL client certificate.
	[Remedy] The LDAP server is requesting an SSL client certificate. Set an SSL client certificate on the machine.
016-523	[Cause] LDAP server SSL authentication error. The server certificate data is incorrect.
	[Remedy] The machine cannot trust the SSL certificate of the LDAP server. Register the root certificate for the LDAP server's SSL certificate to the machine.
016-524	[Cause] LDAP server SSL authentication error. The server certificate will expire soon.
	[Remedy] Change the SSL certificate of the LDAP server to a valid one. You can clear this error by selecting [Disabled] for [LDAP - SSL/TLS Communication] under [SSL/TLS Settings] on the machine; however, note that selecting this option does not ensure the validity of the LDAP server.
016-525	[Cause] LDAP server SSL authentication error. The server certificate has expired.
	[Remedy] Change the SSL certificate of the LDAP server to a valid one. You can clear this error by selecting [Disabled] for [LDAP - SSL/TLS Communication] under [SSL/TLS Settings] on the machine; however, note that selecting this option does not ensure the validity of the LDAP server.
016-526	[Cause] LDAP server SSL authentication error. The server name does not match the certificate.
	[Remedy] Set the same LDAP server address to the machine and to the SSL certificate of the LDAP server. You can clear this error by selecting [Disabled] for [LDAP - SSL/TLS Communication] under [SSL/TLS Settings] on the machine; however, note that selecting this option does not ensure the validity of the LDAP server.
016-527	[Cause] LDAP server SSL authentication error. This is an SSL authentication internal error.
	[Remedy] An error occurred in the software. Contact our Customer Support Center.
016-533	[Cause] Kerberos server authentication protocol error
	[Remedy] The time difference between the machine and the Kerberos server exceeded the clock skew limit value set on the Kerberos server. Check whether the clocks on the machine and Kerberos server are correctly set. Also check whether the summer time and the time zone are correctly set on the machine and Kerberos server.

016-534	[Cause] Kerberos server authentication protocol error [Remedy] The domain set on the machine does not exist on the Kerberos server, or the Kerberos server address set on the machine is invalid for connection. Check whether the domain name and the server address have been correctly set on the machine. For connection to Windows 2003 Server or Windows 2008 Server, specify the domain name in uppercase.
016-539	[Cause] Kerberos server authentication protocol error [Remedy] An error occurred in the software. Contact our Customer Support Center.
016-574	[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because the host or server name of the FTP server could not be resolved. [Remedy] Check the connection to the DNS server. Check if the FTP server name is registered correctly on the DNS server.
016-575	[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because the DNS server address was not registered. [Remedy] Specify the correct DNS server address. Or, specify the destination FTP server using its IP address.
016-576	[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because it could not connect to the FTP server. [Remedy] Ensure that both the destination FTP server and the machine are available for network communications, by checking the following: The IP address of the server is set correctly. The network cables are plugged in securely.
016-577	[Cause] Unable to connect to the FTP service of the destination server. [Remedy] Take one of the following actions: Check if the FTP service of the server is activated. Check if the FTP port number of the server is correctly registered on the machine.
016-578	[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature due to unsuccessful login to the FTP server. [Remedy] Check if the login name (user name) and password are correct.
016-579	[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because the scanned image could not be saved in the FTP server after connection. [Remedy] Check if the FTP server's save location is correct.
016-580	[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because the file or folder name on the FTP server could not be retrieved after connection. [Remedy] Check the access privilege to the FTP server.
016-581	[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because the suffix of the file or folder name exceeded the limit after connection. [Remedy] Change the file name, or change the destination folder on the FTP server. Or, move or delete files from the destination folder.
016-582	[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because file creation was not successful on the FTP server after connection. [Remedy] Take one of the following actions: Check if the specified file name can be used in the save location. Check if enough space is available in the save location.

016-583	[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because lock folder creation was not successful on the FTP server after connection. [Remedy] Take one of the following actions: If any lock directory (.LCK) exists in the forwarding destination, delete it manually, then try executing the job again. Check if the specified folder name can be used in the save location. Check if the same folder name exists in the save location. Check if enough space is available in the save location.
016-584	[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because folder creation was not successful on the FTP server after connection. [Remedy] Take one of the following actions: Check if the specified folder name can be used in the save location. Check if the same folder name exists in the save location. Check if enough space is available in the save location.
016-585	[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because file deletion was not successful on the FTP server after connection. [Remedy] Check the access privilege to the FTP server.
016-586	[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because lock folder deletion was not successful on the FTP server after connection. [Remedy] Take one of the following actions: Check the access privilege to the FTP server. If any lock directory (.LCK) exists in the forwarding destination, delete it manually, then retry executing the job.
016-587	[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because folder deletion was not successful on the FTP server after connection. [Remedy] Check the access privilege to the FTP server.
016-588	[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because the data could not be written in the FTP server after connection. [Remedy] Check if enough space is available in the save location.
016-589	[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because the data could not be read from the FTP server after connection. [Remedy] Check the access privilege to the FTP server.
016-593	[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because an internal error occurred after connection to the FTP server. [Remedy] Try again. If the error persists, contact our Customer Support Center.
016-594 **016-595** **016-596**	[Cause] The machine failed to transfer data using [FTP] of the [Scan to PC] feature because a network error occurred. [Remedy] Try again. If the error persists, contact our Customer Support Center.
016-703	[Cause] The machine received e-mail which specified an invalid folder number. [Remedy] For errors occurring during fax or Internet fax transmission: Contact our Customer Support Center. For errors occurring during e-mail/fax/Internet fax reception: Take one of the following measures: Register the specified folder number, and request the sender to send the e-mail/fax/Internet fax again. Request the sender to send to an available folder. If the error still is not resolved, contact our Customer Support Center.

016-704	[Cause] The folder is full, and hard disk capacity is insufficient.
	[Remedy] Delete unnecessary files from the folder, and save the file.
016-705	[Cause] Secure print documents cannot be registered because of hard disk malfunction.
	[Remedy]Contact the Customer Support Center.
	Refer to Secure Print.
016-706	[Cause] The hard disk space is insufficient because the number of Secure Print users exceeded the maximum limit.
	[Remedy] Delete unnecessary files from the machine, and delete unnecessary Secure Print users.
016-711	[Cause] The upper limit for the e-mail size has been exceeded.
	[Remedy] Take one of the following measures, and then try sending the mail again.
	Reduce the number of pages of the document.
	Lower the resolution with [Resolution].
	Reduce the magnification with [Reduce/Enlarge].
	Ask your system administrator to increase the value set for [Maximum Total Data Size].
	For color scanning, set [MRC High Compression] to [On] under [File Format].
016-713	[Cause] The passcode entered does not match the passcode set on the folder.
	[Remedy] Enter the correct passcode.
016-714	[Cause] The specified folder does not exist.
	[Remedy] Create a new folder or specify an existing folder.
016-764	[Cause] Unable to connect to the SMTP server.
	[Remedy] Consult the SMTP server administrator.
016-765	[Cause] Unable to send the e-mail because the hard disk on the SMTP server is full.
	[Remedy] Consult the SMTP server administrator.
016-766	[Cause] An error occurred on the SMTP server.
	[Remedy] Consult the SMTP server administrator.
016-767	[Cause] Unable to send the e-mail because the address is not correct.
	[Remedy] Confirm the address, and try sending again.
016-768	[Cause] Unable to connect to the SMTP server because the machine's mail address is incorrect.
	[Remedy] Confirm the machine's mail address.
016-769	[Cause] The SMTP server does not support delivery receipts (DSN).
	[Remedy] Send e-mail without setting delivery receipts (DSN).
016-770	[Cause] Direct Fax is restricted.
	[Remedy] Consult your system administrator whether Direct Fax is available. If it is available, contact our Customer Support Center.
016-773	[Cause] The IP address of the machine is not set correctly.
	[Remedy] Check the DHCP settings. Or set the fixed IP address to the machine.
016-774	[Cause] Unable to process compression conversion because of insufficient hard disk space.
	[Remedy] Delete unnecessary data from the hard disk to free up disk space.

016-781	[Cause] Unable to connect to the SMTP server. Unable to establish a connection between the machine and the server. Although the connection between the machine and the server has been established, ASCII characters are not used for the host name specified on the machine. [Remedy] Take one of the following measures: Check whether the network cables are plugged in securely. Enter the host name using ASCII characters in [Tools] > [Connectivity & Network Setup] > [Machine's E-mail Address/Host Name].
016-788	[Cause] Failed to retrieve a file from the Web browser. [Remedy] Take one of the following measures, and then execute the operation again: Reload the browser page. Restart the browser. Switch off the machine power, make sure that the touch screen is blank, and then switch on the machine power.
016-791	[Cause] Failed to access to the destination computer or the save location for Network Scanning. [Remedy] Check the directory configuration and files on the server, the access privileges for the destination or the location, and check if you are authorized to access the specified destination computer or server.
018-400	[Cause] When IPSec is enabled, there is an inconsistency in IPSec settings as follows: The password is not set when [Authentication Method] is set to [Preshared Key]. An IPSec certificate is not set when [Authentication Method] is set to [Digital Signature]. [Remedy]Check the IPSec settings, and enable IPSec again: When [Authentication Method] is set to [Preshared Key], set the password. When [Authentication Method] is set to [Digital Signature], set an IPSec certificate.
018-405	[Cause] An error occurred during LDAP authentication. [Remedy] The account is disabled in the active directory of the authentication server, or the access is set to disabled. Consult your network administrator.
018-502	[Cause] The machine failed to transfer data using SMB of the Scan to PC service because computers allowed to login are restricted. [Remedy] Confirm the property information for the specified user, and check whether the computers allowed to login to the server are restricted.
018-505	[Cause] Failed to log into the destination computer while transferring data using SMB of the Scan to PC service. [Remedy] Check whether the user name and password of the SMTP server registered in the machine is correct.
018-543	[Cause] The machine failed to transfer data using SMB of the Scan to PC service because one of the following problems occurred on the shared name of the SMB server when logging in to the SMB server: The specified shared name does not exist on the server. Invalid characters are used in the specified shared name. When the server is Macintosh, the specified shared name may not have an access right. [Remedy] Confirm the specified shared name, and set the name correctly.

018-547	[Cause] The machine failed to transfer data using SMB of the Scan to PC service because the number of users logging into the SMB server exceeded the limit when logging in to the SMB server. [Remedy] Take one of the following measures: Confirm how many users can access the shared folder. Check whether the number of login users have exceeded the limit.
018-596	[Cause] An error occurred during LDAP server authentication. [Remedy] Execute the operation again. If the error still is not resolved, contact our Customer Support Center.
018-781	[Cause] An LDAP server protocol error occurred as a result of the Address Book operation. Connection to the server cannot be established for the Address Book query. [Remedy] Take one of the following measures: Confirm the network cable connection. If the network cable connection has no problem, confirm the active status of the target server. Check whether the server name has been correctly set for [LDAP Server/Directory Service Settings] under [Remote Authentication Server/Directory Service].
018-782 018-783 018-784 018-785 018-786 018-787 018-788 018-789 018-790 018-791 018-792 018-793 018-794 018-795 018-796 018-797	[Cause] An LDAP server protocol error occurred as a result of the Address Book operation. The server returned RFC2251 Result Message for Address Book query. [Remedy] Have your network administrator confirm the LDAP server status.
027-452	[Cause] IP address of IPv4 already exists. [Remedy] Change the IP address of IPv4 set on the machine or the IP address of IPv4 on the network device.
027-500	[Cause] Unable to connect to the SMTP server. [Remedy] Specify the SMTP server name correctly or specify the server by using its IP address.
027-706	[Cause] Unable to find the S/MIME certificate associated with the machine's e-mail address when sending e-mail. [Remedy] Import the S/MIME certificate corresponding to the mail address to the machine.

027-707	[Cause] The S/MIME certificate associated with the machine's email address has expired. [Remedy] Ask the sender to issue a new S/MIME certificate and import the certificate to the machine.
027-708	[Cause] The S/MIME certificate associated with the machine's email address is not reliable. [Remedy] Import a reliable S/MIME certificate to the machine.
027-709	[Cause] The S/MIME certificate associated with the machine's email address has been discarded. [Remedy] Import a new S/MIME certificate to the machine.
027-710	[Cause] No S/MIME certificate is attached to the received e-mail. [Remedy] Ask the sender to send the e-mail with an S/MIME certificate.
027-711	[Cause] No S/MIME certificate was obtained from the received 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.
027-717	[Cause] Unable to obtain SMTP server address for e-mail transmissions from the DNS server. [Remedy] Check whether the DNS server is set correctly.

Security @ Xerox

For the latest information on security and operation concerning your device, see the Xerox Security Information website located at www.xerox.com/security.

Appendix

List of Operation 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 Scheduled Image Overwrite	[Authentication/Security Settings] > [Overwrite Hard Disk] > [Scheduled Image Overwrite].	[Security] > [On Demand Overwrite] > [Scheduled]	Off
Run Image Overwrite	[Authentication/Security Settings] > [Overwrite Hard Disk] > [Run Image Overwrite]	[Security] > [On Demand Overwrite] > [Manual]	-
Set Data Encryption	[System Settings] > [Common Service Settings] > [Other Settings] > [Data Encryption]	-	On
Set Authentication	[Authentication/Security Settings] > [Authentication] > [Login Type].	[Security] > [Authentication Configuration]	Off
Set Access Control	[Authentication/Security Settings] > [Authentication] > [Access Control]	[Security] > [Authentication Configuration] > [Next]> [Device Access] or [Service Access]	Off
Set Private Print	[Authentication/Security Settings] > [Authentication] > [Charge/Private Print Settings].	-	Off
Set User Passcode Minimum Length	[Authentication/Security Settings] > [Authentication] > [Passcode Policy] > [Minimum Passcode Length]	[Security] > [User Details Setup] > [Minimum Passcode Length]	0
Set Direct Fax	[System Settings] > [Fax Service Settings] > [Fax Control] > [Direct Fax]	-	On

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

General User			
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]	-