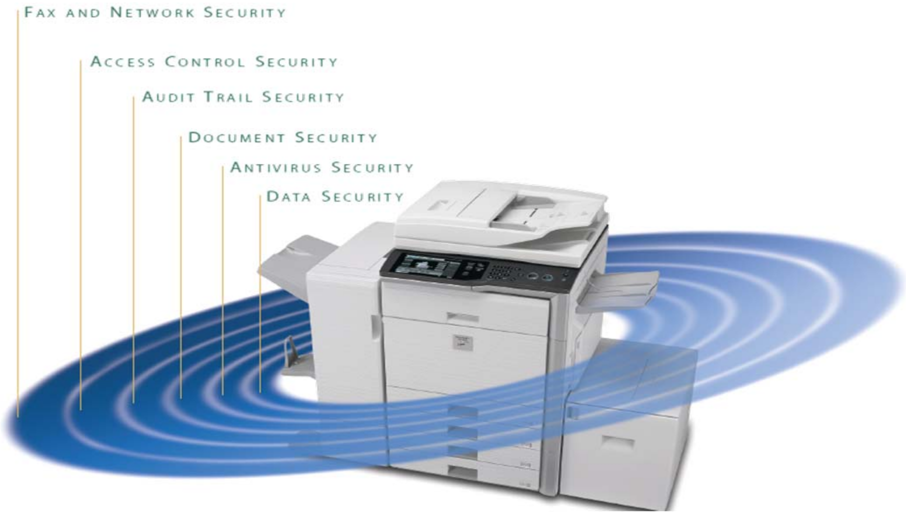
SHARP

Sharp Imaging and Information Company of America

The New Sharp Standard Security vs. the Data Security Kit



The New Sharp Security Suite Features

- Sharp offers their customers 2 levels of security for new MFP's:

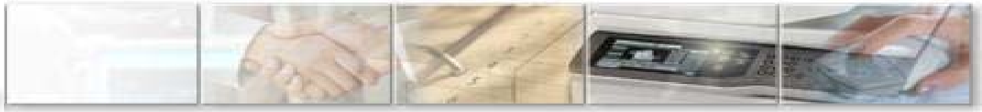
1. New Standard Security

Standard Feature

2. Optional Data Security Kit

Optional Feature

Please note: Standard Security ***does not*** include the advanced features of the Data Security Kit



The New Sharp Standard Security Suite

New & Enhanced Standard Security Features

Standard Feature

1. Manual Overwrite (End of lease feature)

NEW

At the push of a button, this feature erases all personal and confidential information stored on the machine, restoring to virtually
the same condition as when it first left the factory floor. This provides any size business with peace of mind that comes from knowing that its confidential and/or protected information is secure even at trade in

2. Auto Security Mode (Persistent security feature)

NEW

This feature leverages both 256 bit encryption as well as overwrite protection to ensure that the company’s data is protected day-in and Day-out, and not just at trade-in.

1. Manual Overwrite (End of lease feature)

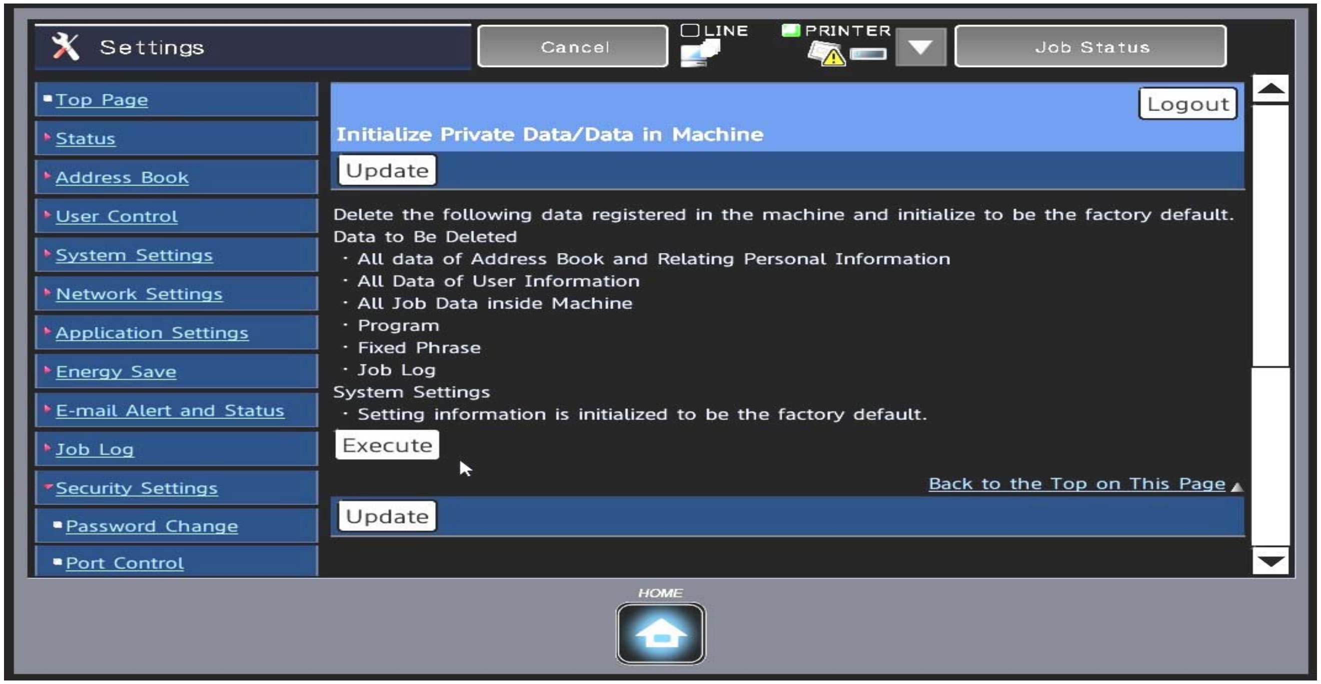
NEW

Standard Feature

- At the push of a button, you can delete all of the personal information including the address book and data transmission logs simultaneously to assure your security.

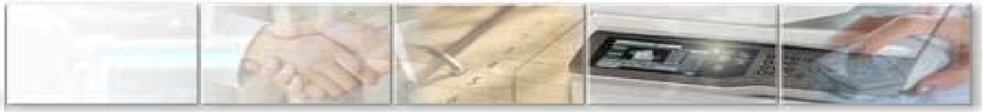
- If this function is executed, the MFP will print a notice indicating the deletion process was completed.

- User selectable: 1-7 times
- Method: Random string
- Areas included:
  - Image data
  - Doc Filing
  - FAX ROM
  - Job Status
  - Address Book



Initialize Private Data/Data in Machine

Delete the following data registered in the machine and initialize to be the factory default.
Data to Be Deleted
・All data of Address Book and Relating Personal Information
・All Data of User Information
・All Job Data inside Machine
・Program
・Fixed Phrase
・Job Log
System Settings
・Setting information is initialized to be the factory default.



2.Security Mode (Persistent Security) “Automatic”

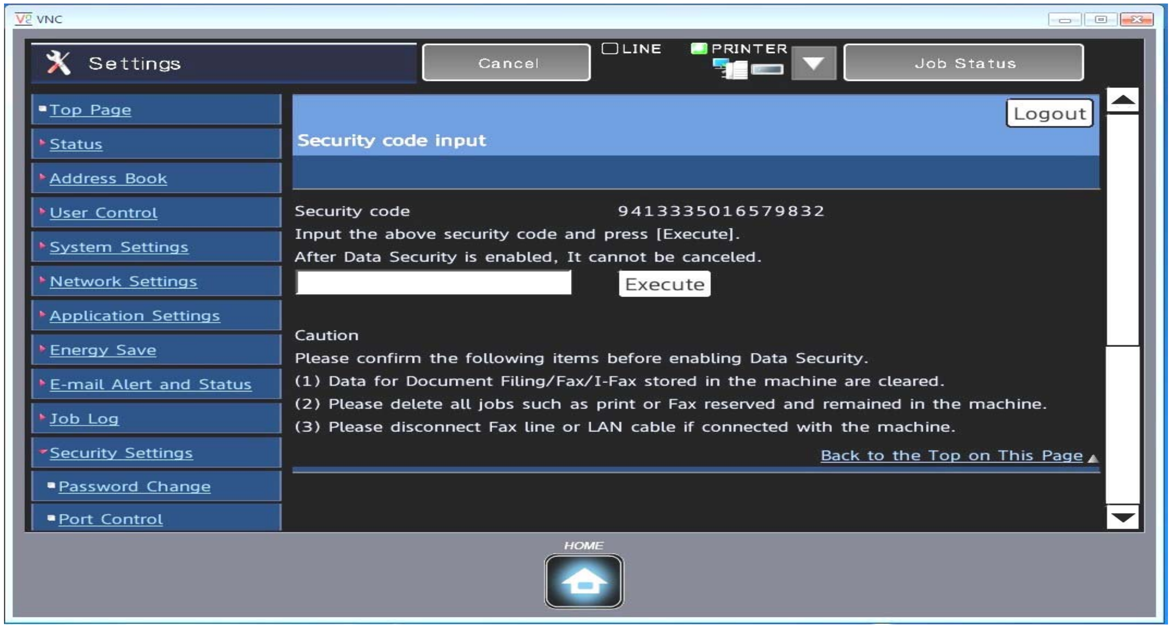
NEW

Standard Feature

- ***Automatic Overwrite After Every Job***
  - User selectable 1-7 times
  - Method: Random string (0’s & 1’s)
  - Areas: Image data (including FAX)

- ***Encryption 256-bit (Job and DF data)***

- ***Password Lock (3x → 5min lock)***
  - If a login fails three times in succession, a warning is displayed and further login is disabled for five minutes.
  - This prevents an unauthorized person from attempting to guess a password. (The number of failed login attempts is retained even if the power is turned off.)



Security code input

Security code 9413335016579832

Input the above security code and press [Execute].

After Data Security is enabled, It cannot be canceled.

Caution

Please confirm the following items before enabling Data Security.

(1) Data for Document Filing/Fax/I-Fax stored in the machine are cleared.

(2) Please delete all jobs such as print or Fax reserved and remained in the machine.

(3) Please disconnect Fax line or LAN cable if connected with the machine.

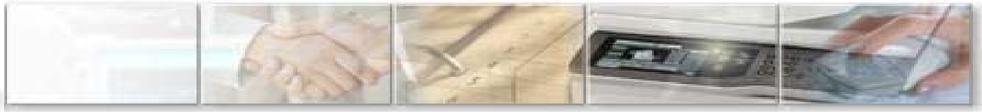
Standard Security Features

Standard Feature

- ## *Authority Group and Access Control*
  - Advanced account management enables administrators to set authority groups for access to features of the MFP including network scanning and email communications.

- ## *User Authentication*
  - Two types of user authentication
    - 1. Authenticate to the internal database of the MFP
    - 2. Authenticate via Active Directory

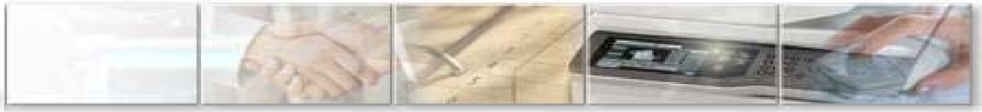
- ## *Document Control*
  - Confidential Printing
    - Requires users to enter a PIN code in order to print a queued document.
  - Secure Fax Release
    - Ensures received fax documents are held in memory until an authorized user enters a PIN.



Standard Security Features

Standard Feature

- ***Port Control***
  - Enables or disables main system ports and sets the port numbers.

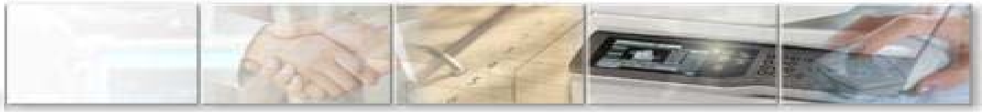


Standard Security Feature

Standard Feature

- ***Filter Address Setting***

  – Access to the machine from the preset IP address or MAC address can be limited.
  However, the machine cannot be accessed from the MAC address if it is contained in the disabled IP address range.

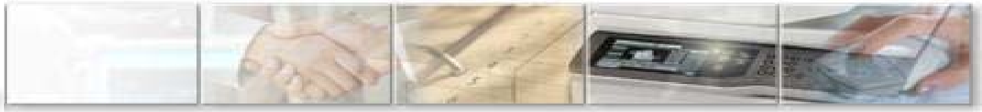


Standard Security Feature

Standard Feature

SSL Settings

- SSL can be used for data transmission over a network. SSL is a protocol that enables the encryption of information communicated over a network. Encrypting data makes it possible to transmit and receive sensitive information safely.
  Data encryption can be set by the following protocols.
  - Server Port
  - HTTPS: Apply SSL encryption to HTTP communication.
  - IPP-SSL: Apply SSL encryption to IPP communication.
  - Redirect HTTP to HTTPS in Setting mode (Web version) Access: When this setting is enabled, all communication that attempts to access the machine by HTTP is redirected to HTTPS.
  - Client Port
  - HTTPS: Apply SSL encryption to HTTP communication.
  - FTPS: Apply SSL encryption to FTP communication.
  - SMTP-SSL: Apply SSL encryption to SMTP communication.
  - POP3-SSL: Apply SSL encryption to POP3 communication.
  - LDAP-SSL: Apply SSL encryption to LDAP communication.



Standard Security Feature

Standard Feature

IEEE 802.1X Authentication Settings

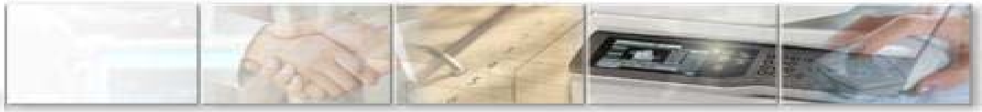
- IEEE 802.1X can be used to authenticate a user to allow use of the machine.
- IEEE 802.1X protocol defines port-based for both wired and wireless networks.
- Use IEEE 802.1X authentication to allow only authenticated devices to use network, and protect against network abuse by third parties.
- You can enable or disable IEEE 802.1X authentication with this setting. The IEEE 802.1X details can be set with Setting mode (Web version). Depending on the Web page settings, connection to the machine may not be allowed, or the settings may not allow printing, scanning, or Setting mode (Web version) display. In this case, deselect this setting and change the Setting mode (Web version) settings.

Standard Security Feature

Standard Feature

IPSEC Settings

- When IPSec is used, data can be sent and received safely without the need to configure settings for IP packet encryption in a Web browser or other higher-level application.
- This setting is only used to enable or disable IPSec; the detailed IPSec settings are configured with Setting mode (Web version).
- When enabling this settings, take the following notes:
  - It may take time to reflect on the machine settings, and you cannot connect to the machine during this time.
  - If the Setting mode (Web version) settings are not correctly selected, connection to the machine may not be allowed, or the settings may not allow printing, scanning, or Setting mode (Web version) display. In this case, deselect this setting and change the System Settings (on Web pages).



Standard Security Feature

Standard Feature

Tracking Information Print

- Prints the tracking information at the top or bottom of output pages when copy or print job is executed.
- Item Description Print tracking information settings
  - Set this option to print the tracking information.
- Print Data
  - The following information can be printed. Serial number, characters, account job ID, login name/user number, date and time
- Print Color Select
  - Select a print color.
- Print Position
  - Set a print position on each page.
- Select the Job to Print
  - Set a job to print the tracking information.

Standard Security Feature

Standard Feature

Pattern Print

- Select Hidden Pattern Print Setting:
  - The hidden pattern print function is effective at preventing unauthorized copying as the specified text emerges in the background on output sheets.

Sharp Data Security Kit

Optional Feature

- If you require more security features you have the option to purchase the Data Security Kit (DSK).

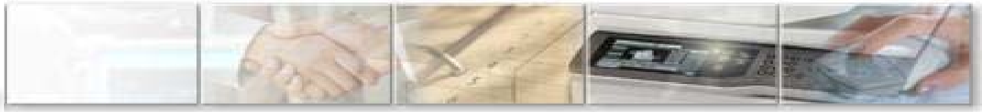
- The DSK provides the highest level of security and meets stringent government requirements.

Commercial Data Security Kit

Optional Feature

- Why install the Data Security Kit?
  - Government requirements
    - The Health Insurance Portability and Accountability Act (HIPAA)
    - The Sarbanes–Oxley Act (SOX)
    - The Gramm–Leach–Bliley Act (GLB)
  - IEEE 2600 Security requirements for copier/MFP
  - Required for Tandem Print/Copy
  - Required for Common Access Card Support (CAC)

- What industries use the Data Security Kit?
  - Government
  - Insurance
  - Legal
  - Healthcare
  - Financial
  - Education

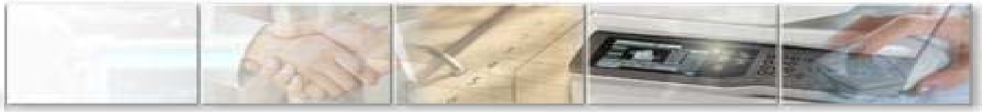


Data Clearance (Automatic)

Optional Feature

- **Power-up Auto Clear up to 7X**
  - This function is used to automatically clear all data in the machine when the power switch is turned on. The following types of data can be cleared:
    - All Memory
    - File Data (Including protected/confidential files)
    - Quick File Data(Including protected files)
    - Job Status Jobs Completed List

- **Auto Clear at Job End up to 7X**



Data Clearance (Manual)

Optional Feature

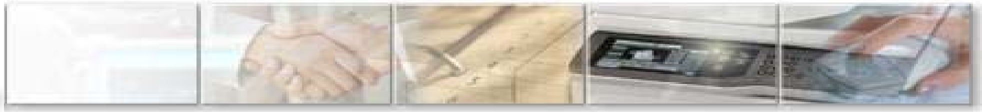
- **Number of times Data Clear Function can be repeated up to 7X for items below.**
- **Factory default setting is 1.**
  - **Clear All Memory**
    - This program is used to manually clear all data from the memory and hard disk of the machine. The following types of data are not cleared with this setting. Use "Clear Address Book and Registered Data" to clear the following types of data:
      - User Information
      - Individual/Group/Program/Relay Broadcast Memory Box*/Resend
      - Polling Memory/Confidential Memory Box*
      - Sender Data
      - Allow/Reject Reception Setting Data (including polling pass code number)
      - Forward Information
      - Image data stored in a memory box is cleared by executing "Clear All Memory".
  - **Clear Document Filing Data**
    - This function is used to clear data stored using the document filing function including:
      - Data whose property is set to "Protect" or "Confidential" is also cleared.
      - File Data (Including protected/confidential files) checkbox:
        - Select this checkbox to clear all files stored using "File" in the main folder and in custom folders.
      - Quick File Data (Including protected files)checkbox:
        - Select this checkbox to clear all files stored using " Quick File ".

Data Clearance (Manual continued)

Optional Feature

- **Clear All Data in Job Status Jobs Completed List**
  - This is used when you need to clear all data of the items below, which appear in the job status jobs completed screen.(The job status jobs completed screen appears when the [Complete] key (job status screen selector key) of the job status screen is tapped.)
- Printer user names
- Image send destinations
- Senders of faxes that are received

- **Clear Address Book Data and Registered Data in the MFP**
  - This function is used to clear the items indicated below, which cannot be cleared or initialized using "Clear All Memory" or "Restore Factory Defaults" (➞ Settings (Administrator) > "Storing/Calling of System Settings" > "Restore Factory Defaults"). The following types of data can be cleared:
- User Information
- Individual/Group/Program/Relay Broadcast Memory Box/Resend
- Polling Memory/Confidential Memory Box
- Sender Data
- Allow/Reject Reception Setting



Administrator Password / User Password Protection

Optional Feature

- When the data security kit is installed, password entry will be locked for 5 minutes if:
  - An incorrect administrator password is entered 3 times in a row when the user authentication function **is not** enabled
  - An incorrect administrator password **or** user password is entered 3 times in a row when the user authentication function **is** enabled

Authority group registration

Optional Feature

- When the data security kit is installed, the following items are added to the "Authority Group Registration" menu screen in the Admin setting mode :
    - Approve Print Jobs other than Print Hold Job
    - Document filing approval settings

– This screen is displayed by selecting :

- "Settings (Administrator)" > "User Control" > "Authority Group List".

Optional Feature

Confidential folder & file lockout

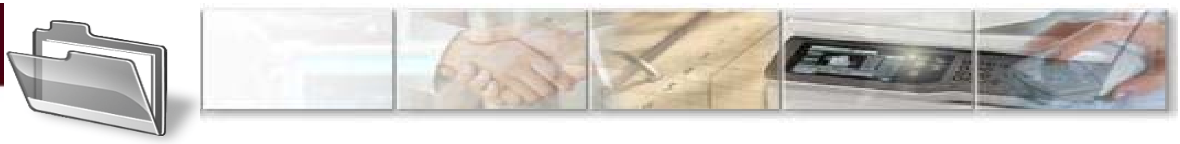
- If an incorrect password is entered 3X in a row for a confidential file or folder,
- the file will be locked . To unlock the folder or file, use "Release Lock on File/Folder Operation"

Tandem copying and printing restrictions

Optional Feature

Tandem Copying			
		Client Machine	
		DSK: Yes	DSK: No
Main machine	DSK: Yes	The tandem function can be used. Data is encrypted and cleared from both the master and slave machines.	The tandem function cannot be used.
	DSK: No	The tandem function can be used. Data is encrypted and cleared from the slave machine.	The regular tandem function can be used.

Tandem Printing			
		Client Machine	
		DSK: Yes	DSK: No
Main machine	DSK: Yes	The tandem function can be used. Data is encrypted and cleared from both the master and slave machines.	The tandem function can be used. Data is encrypted and cleared from the slave machine.
	DSK: No	The tandem function can be used. Data is encrypted and cleared from the slave machine.	The regular tandem function can be used.



File search of document filing area

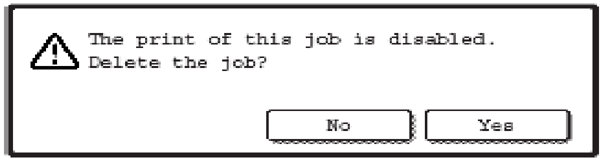
Optional Feature

- The password entry setting will not appear in the document filing search screen

Encrypted PDF Lockout

Optional Feature

- When a job is printed by encrypted PDF direct printing (when the PS3 expansion kit is installed), the job will appear in the spool queue of the job status screen and a password must be entered to begin printing.
- If an incorrect password is entered 3 times in a row when the data security kit installed, the message "Operation is disabled. Please see your administrator for your assistance.” will be displayed for 6 seconds and printing will be locked. If you tap a file in the spool screen for which an incorrect password was entered 3 times, the following screen will appear:

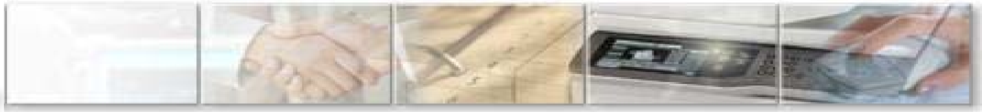


The print of this job is disabled.
Delete the job?

FTP Pull Print

Optional Feature

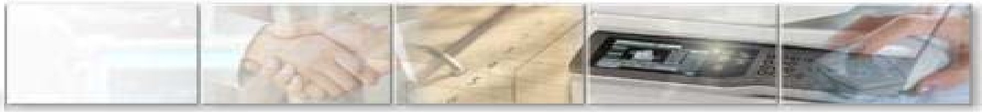
- When the machine is used as a network printer and the FTP Pull Print function is used, the data security kit enables authentication of the user by means of a "User Name" and "Password" for the FTP server. (The Pull Print function allows a file on a previously stored FTP server to be printed directly from the operation panel of the machine without using the printer driver.)
- User authentication is enabled by selecting the [Enable User Authentication] checkbox on the machine for configuring FTP Pull Print settings. This checkbox appears when the data security kit is installed, and is initially selected (a checkmark appears).



Transferring copied data

Optional Feature

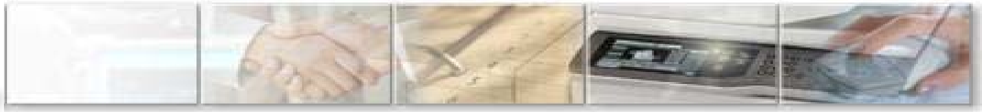
- When web pages are used to copy data stored with the document filing function to a computer, the copied data can only be transferred back to the original machine from which it was copied.



Disable Settings

Optional Feature

- Disabling Document Filing
  - This program is used to restrict the filing modes of the document filing function.
    - Document filing modes (Quick File Mode, Sharing Mode, and Confidential Mode) can be separately disabled in each mode in which document filing operates (Copy, Printer, Scan to HDD, and Image Send mode).
  - Forced Retention of Print Jobs
    - Printing in print mode other than from the operation panel of the machine can be prohibited. This setting can be used to prevent sensitive documents left on the output tray from being taken by a third party, which could result in the leaking of sensitive information.



Display Settings

Optional Feature

- Disabling of Data List Print
  - This program is used to disable printing of any of the following lists that are printed using "List Print (User)" in the setting mode:
    - All Custom Setting List
    - Sending Address List
    - Document Filing Folder List

- Job Status Display Settings
  - You can select whether or not filenames of print jobs and destination names of image send jobs are displayed in the job status screen of the touch panel. If you do not want to display this information for security reasons, select the appropriate checkboxes.

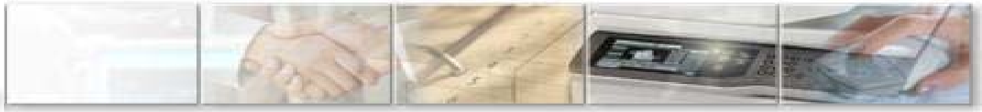
– Jobs Completed List Display Setting

  - You can select whether or not the job status completed jobs screen (job status screen selector key) is displayed. If you prefer not to have the information (print mode user names, image send destinations, senders of faxes that are received, etc.) that is stored and shown in the job status completed jobs screen be displayed for security reasons, use this setting to hide the screen.

Optional Feature

Document control function

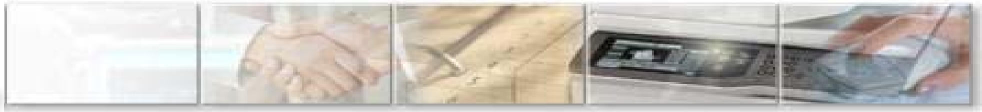
- Embeds a document control pattern on the paper when print jobs, copies, and received faxes are printed. Prevents secondary copying, faxing and other operations of a printed document. The document control function can be used to print with an embedded document control pattern in the following modes:
  - Copy (color / black and white)
  - Printer (color / black and white)
  - Document Filing Print (color / black and white)
  - Internet Fax Receive (black and white only)
  - Direct SMTP Receive (black and white only)
  - Fax Receive (black and white only)
  - List Print (black and white only)



Document control

Optional Feature

- Print Settings
- Printer Driver



Additional Authority Items

Optional Feature

- Document filing approval setting
- Approve Print Jobs other than Print Hold Job
- Authentication at FTP pull print
- System Log

Restrictions

- Storage backup / Device cloning – Export encrypted data only
- Filing data back-up – encrypted data is exported
- Document Filing Setting>“Delete All Quick Files”
- Deletion of Filtering Function by Password on Data Search
- Entering of Password for Hold Setting for Received Data Printing