SHARP

Data Security Kit Notice

Version: Q1-1

This notice contains very important information. Please keep the notice in a safe place where it will not be lost.

Use in Advanced Security Mode

The matters to note when the machine is operated in the Advanced Security Mode described in the "Setting a high level of security" of the Operation Manual of the data security kit are described below.

Restricted Function

- Once you change into the Advanced Security Mode, you cannot return to the status before change.
  - Even after executing [Initialize Private Data/Data in Machine], the Advanced Security Mode is maintained.
- Password requirements are changed as below.
  - Minimum password length: The value specified by the administrator (5-32 letters, default: 5)
- When selecting authority group, you cannot select the guest authority, or the scanner prohibited authority. If you want to select one of those authority, refer to the "Authority Group" of the "User's Manual" and create an authority group equivalent to each authority in [User Control]→[Access Control Settings]→[Authority Group] of "Settings (administrator)".
- User authentication function is always enabled. In addition, the User Authentication by User Number, the User Authentication by Quick Authentication, the User Authentication by IC Card and the Device Account Mode function are disabled.
- Audit log is always enabled. Internal storage cannot be selected for the storing destination of the audit log, as well as [Save/Delete Audit Log] are disabled.
- Only the administrator is allowed to edit the Address Book (add, modify, delete).
- The following copy features will be disabled:
  Tandem Copy, Sending While Copying, Program Registration, and Call Program
- The following printer features will be disabled:
  Tandem Print, Sending While Printing, Submit Print Job, FTP Print, E-mail Print, Network Folder Direct Print, USB Memory Direct Print, and Print Release
- Printing with the printer driver is available only when IPP-SSL/TLS feature is enabled in Windows8.1 or above.
  - See the "Software Setup Guide" of the machine with the data security kit installed for the print using IPP-SSL/TLS feature.
  - When a printer driver is installed, the machine in the Advanced Security Mode will not be searched automatically. You need to check the IP address of the target machine in advance.
- Print ports (LPD, Raw, WSD) and external print services (AirPrint, IPP Everywhere) will be disabled.
- The following scanner features will be disabled:
  Scan to Desktop, Scan to Network Folder, PC Scan Mode (TWAIN), Send Destination Link, Scan to External Memory Device, Sharpdesk Mobile, Program Registration, and Call Program
- The following Fax (Facsimile) features will be disabled:
  F-code memory boxes, PC-Fax, Internet Fax, Forwarding Received Data, Program Registration, and Call Program
- It is only the administrator and the user who belongs to the Authority Group with the access authority to the received fax data who is allowed to access (display, print, and/or delete) received fax data.
- The following Document Filing features will be disabled:
  Quick File Folder, Save in External Memory Device, Save to PC, and Filing Data Backup
- A web browser supporting TLS 1.2 is required for the web page setting.
- Wireless LAN, mDNS, and Proxy will be disabled. And in principle, network communication without using SSL/TLS are disabled.
- The functions of the machine using USB Host/Device function except for Firmware Update will be disabled. And the functions of Remote Firmware Update will be disabled.
- In addition, the following features will be disabled:
  Bluetooth, Sharp OSA, Public Folder/NAS, Cloud Link, Mobile Link, Save Job Log, Easy Connect by NFC/QR code, Data Import/Export, Storage Backup, Device Cloning, Storing/Calling of System Settings, Restore Factory Defaults, E-mail Alert and Status, Data Entry, Voice Alert, Apply Security Policy

Procedure before operation

- Changing into the Advanced Security Mode should be performed by the administrator.
- It is better to change into the Advanced Security Mode before putting the machine with the data security kit installed into operation than after.
- If you change the machine which has already been in use into the Advanced Security Mode, execute [Clear All Memory] and [Clear Address Book and Registered Data], by referring to the "Data Clearance Settings" of the Operation Manual of the data security kit, to eliminate any unencrypted data or residue on deletion before changing into the Advanced Security Mode. And if any programs of Copy/Fax Send/Scan, device certificates, and certificate signing requests (CSRs) are registered, delete them all.
- Perform the following operation before changing into the Advanced Security Mode.
  - Perform initial installation settings of the machine by referring to the "User's Manual" bundled with the machine.
  - Disable [IPv6] in [System Settings]→[Network Settings]→[Interface Settings] of "Settings (administrator)".
  - Change the password of default administrator (admin) into the one with 5 letters or longer.
  - Prepare a syslog server which supports TLS 1.2 as the audit server, and change [Storage/Send Settings] of audit log into the audit server by referring to the "SYSTEM SETTINGS" of the "User's Manual". In addition, if the setting before change is [Stored to Storage], export the audit logs stored so far to PC by [Save/Delete Audit Log].
  - If user authentication by the external account application of Sharp OSA is used, change into the internal authentication or the network authentication.
  - When the machine is connected with Fax line or network, keep the modular cable or the LAN cable disconnected until the changing into the Advanced Security Mode is completed.
- Operation of changing into the Advanced Security Mode can be performed on the operation panel by the default administrator (admin) only.
  - Start the changing into the Advanced Security Mode by tapping [Execute] key in [System Settings]→[Security Settings]→[Advanced Security Settings] of "Settings (administrator)".
  - It takes some times from start to end of the changing into the Advanced Security Mode. Be sure not to leave the spot until the processing is completed and pay sufficient attention to the breakage of power supply of the machine during the processing.
  - After completing the changing into the Advanced Security Mode, check to see that the item of [Advanced Security Settings] is not displayed in [System Settings] → [Security Settings] of "Settings (administrator)", for the purpose of confirming that the Advanced Security Mode has been changed.
- After completing the changing into the Advanced Security Mode, perform the following operations.
  - Connect the LAN cable and connect it to the network, import the Certificate Authority certificate that signed the server certificate used in the audit server as the sending destination of the audit log on the web page, then reboot the machine.
  - In order to operate securely, specify [Minimum Password Length] into 15 digits or more from [System Settings] → [Security Settings] → [Password Change] of "Settings (administrator)" after login with the default administrator (admin). Further change the length of administrator's password including the default administrators into the value which satisfies the specified minimum password length.
  - The password requirements are changed as below by changing into the Advanced Security Mode including the change of the minimum password length.
    - Password length: Minimum password length specified above or more and 255 digits or less

    Users of which password don't satisfy the requirement cannot log in. The administrator should change their passwords so that they should satisfy the requirements and inform the users the changed passwords.
  - In [System Settings] → [Common Settings] → [Operation Settings] → [Condition Settings] of "Settings (administrator)", set the time of [Auto Clear Setting] as short as possible to the extent that there is no inconvenience with use.
  - If you use an external server as the user authentication, prepare a LDAP server which supports TLS 1.2 as the authentication server, and register the authentication server by [System Settings] → [Network Settings] → [LDAP Settings] of "Settings (administrator)", then import the Certificate Authority certificate that signed the server certificate of the registered authentication server on [System Settings] → [Security Settings] → [Certificate Management] → [CA Certificate Management] of "Settings (administrator)" on the web page. Further, in [System Settings] → [Authentication Settings] → [Default Settings] of "Settings (administrator)", select [LDAP] for [Authentication Server Settings], select the registered authentication server for [Default Network Authentication Server Settings], check [Specify network server access control], then execute [Submit].

- If you use Scan to E-mail, prepare SMTP server which supports TLS 1.2 as a mail sending server, register the mail sending server in [System Settings] → [Network Settings] → [Services Settings] → [SMTP] of "Settings (administrator)" and import the Certificate Authority certificate that signed the server certificate of the registered mail sending server in [System Settings] → [Security Settings] → [Certificate Management] → [CA Certificate Management] of "Settings (administrator)" on the web page.
- If you use Scan to FTP, prepare FTP server which supports TLS 1.2 as a sending destination file server, import the Certificate Authority certificate that signed the server certificate of the sending destination file server in [System Settings] → [Security Settings] → [Certificate Management] → [CA Certificate Management] of "Settings (administrator)" on the Web page.
- When you use Fax, connect the modular cable and connect it to PSTN Fax line. Further refer to the "User's Manual" of the machine and perform the initial setting relating to the Fax setting. In addition, create a authority group in which [Access to Fax Data] is specified as [Allowed] with [User Authority] as the model in [User Control] → [Access Control Settings] → [Authority Group] of "Settings (administrator)", then specify the created authority group for [Authority Group] of users who are allowed to access to the received Fax data (display, print, delete) other than the administrator in [User Control] → [User Settings] → [User List] of "Settings (administrator)".

Caution in operation

- The administrator should not change the setting instructed by this material in principle. If the setting is changed, you need to return the setting into the one at the time of the completion of procedure before operation, based on this material.
- Self-test is performed when powering on the machine. It takes ten or more seconds. The machine cannot be used until the test is completed. If the test is not completed successfully because the function related to encryption doesn't work properly or the firmware is damaged, "Call for service." is displayed on the operation panel or nothing is displayed on the operation panel and the machine stops operation. If the machine causes the same phenomenon even after the powering off/on, please contact your dealer or nearest authorized service representative.
- User who fails in user authentication cannot use the machine.
- When operating on the Web page, check that the used web browser should support TLS 1.2 and use it with TLS 1.2 enabled.
- When operating on the Web page, do not view or operate web pages provided by other than the machine until the operation is finished to keep off any security interactions.
- When printing with the printer driver, select [Job Handling] tab on the printing preferences window of the printer driver and specify the following setting, then perform the printing.
  - Select [Hold Only] for [Document Filing].
  - Select other than [Quick File] for [Stored to] and specify [PIN Code].
  - Select [Login Name/Password] for [Authentication] and enter the login name and the password of the user who can use the machine into [Login Name] and [Password] respectively.
- When using the printing with the printer driver and if the PC completed the sending but the machine doesn't receive the data, the setting of the printer driver may be wrong. Check whether the setting of the printer driver is made correctly and then execute the printing again. If the setting is made correctly, but the printing data still cannot be received, please contact your dealer or nearest authorized service representative.
- Only the administrator and the users of [Login Name] entered on the printing preferences window of the printer driver when executing print from PC can display, edit, print or delete the data stored in the storage of the machine by the printing with the printer driver.
- Only the user who has executed the scanning document can display or edit the scanned document data in Copy, Scan or Fax Sending.
- Only the administrator and the users who belong to the Authority Group with access authority to the received Fax data can display, print or delete the received Fax data.
- Only the administrator or the user who executed the data storing can display, edit, re-operate or delete the stored data by Document Filing.
- User other than the administrator cannot select the jobs of other users as well as cancel/delete them. The jobs of other users are masked to display with "*****" partially in displaying the job list.
- All users including the administrator cannot alter the job displayed on [Job Status].
- If the Firmware should be updated due to taking countermeasure against defects, the service engineer should switch the machine to the maintenance mode and operate.
- Customer's consent is needed for the maintenance mode operation by the service engineer. If you agree, please enter the password of the default administrator (admin) on the operation panel. This consent is valid until the day after the following day. However, if the Clock Adjust is changed during this period, the consent becomes invalid. In that case the password should be entered again.

- After completing the operation by the service engineer, check to see the operation panel display whether is returned to the normal mode from the maintenance mode. If you find an icon of "TEST" at the upper right of the screen, the maintenance mode is not terminated yet. Please contact the service engineer. After returning to the normal mode, the administrator should check that the settings indicated in this material are not changed. If any setting is changed, please return them to the settings at the time of the completion of procedure before operation based on this material.
- When unable to connect to the audit server, displayed a warning message on the operation panel and the web page screen. Unsent audit logs are temporarily stored in the main unit until they are successfully sent to the audit server. If there are more than 32,000 unsent audit logs, only the built-in administrator (admin) will be restricted from logging in. This limit will be lifted if there are less than 28,000. If the number of unsent audit logs reaches 40,000, new audit logs will not be retained and will be lost.
- To maintain security, the administrator should make sure that every user of the machine complies the above-mentioned cautions.

CA Certificate Management Function

When operating the machine with the data security kit installed in the Advanced Security Mode, the server certificate of the communication counterpart is verified to prevent man-in-the-middle attack. Therefore, for the communication with various servers, the Certificate Authority certificate that signed the server certificate of the communication counterpart should be acquired in advance and imported to the machine. This function is to import those certificate to the machine and to display or delete the imported certificate. Only the administrator is allowed to use. The operation method of this function is described below.

Import of certificate

STEP1: Select [System Settings] → [Security Settings] → [Certificate Management] → [CA Certificate Management] of "Settings (administrator)" on the Web page.
STEP2: Click [Import] button.
STEP3: Click [Browse] button and select the certificate to import.
STEP4: Check to see that the path of [Import settings from File] is correct and click [Execute] button.
- When the import is successful, the screen will be switched to the one showing “Your request was successfully processed. Your setting will be valid after you power down and then restart the copier.” When the import is failed, a warning message will be displayed.
- If the import is failed, check to see that the file selected at the STEP3 is a certificate file. If the import is failed in spite of selecting a certificate file, please contact your dealer or nearest authorized service representative.

STEP5: Click [Reboot Now] button and reboot the machine.
STEP6: After the machine reboots, select [System Settings] → [Security Settings] → [Certificate Management] → [CA Certificate Management] of "Settings (administrator)" and check whether the certificate selected at STEP3 exists in the displayed list.

Display of imported certificate

Operation from the operation panel:
STEP1: Select [System Settings] → [Security Settings] → [Certificate Management] → [CA Certificate Management] of "Settings (administrator)".
STEP2: Select one certificate in the list and tap the subject name.
- Display the contents of the selected certificate.
- Tapping [Back] key to return to the previous screen.

Operation from the Web page:
STEP1: Select [System Settings] → [Security Settings] → [Certificate Management] → [CA Certificate Management] of "Settings (administrator)".
STEP2: Select one certificate in the list and click the subject name.
- Display the contents of the selected certificate.
- Clicking [Back] button to return to the previous screen.

Deletion of imported certificate

Operation from the operation panel:
STEP1: Select [System Settings] → [Security Settings] → [Certificate Management] → [CA Certificate Management] of "Settings (administrator)".
STEP2: Select one or more certificate in the list and tap each checkbox to check.
- Tap the checked checkbox again to cancel the check.
- Multiple certificates can be selected and deleted at one time.
- Tap [Select All] key to check the checkboxes of all certificates at one time.
- Tap [Clear Checked] key to cancel all the checks at one time.

STEP3: Tap [Delete] key.
- The confirmation dialog will be displayed.

STEP4: Tap [OK] key displayed in the confirmation dialog.
- When the deletion is completed, the screen will be switched to the one showing “Your request was successfully processed. Your setting will be valid after you power down and then restart the copier.”

STEP5: Tap [Reboot Now] key and reboot the machine.

STEP6: After the machine reboots, select [System Settings] → [Security Settings] → [Certificate Management] → [CA Certificate Management] of "Settings (administrator)" and check to see that any certificate selected at STEP2 doesn't exist in the displayed list.

Operation from the Web page:

STEP1: Select [System Settings] → [Security Settings] → [Certificate Management] → [CA Certificate Management] of "Settings (administrator)".

STEP2: Select one or more certificate in the list and click each checkbox to check.

- Click the checked checkbox again to cancel the check.
- Multiple certificates can be selected and deleted at one time.
- Click [Select All] button to check the checkboxes of all certificates at one time.
- Click [Clear Checked] button to cancel all the checks at one time.

STEP3: Click [Delete] button.

- The confirmation dialog will be displayed.

STEP4: Click [OK] button displayed in the confirmation dialog.

- When the deletion is completed, the screen will be switched to the one showing "Your request was successfully processed. Your setting will be valid after you power down and then restart the copier."

STEP5: Click [Reboot Now] button and reboot the machine.

STEP6: After the machine reboots, select [System Settings] → [Security Settings] → [Certificate Management] → [CA Certificate Management] of "Settings (administrator)" and check to see that any certificate selected at STEP2 doesn't exist in the displayed list.

Response when various operation is executed

The responses when executing various operations of the machine operating in the Advanced Security Mode are described below. See the "Start Guide" bundled with of the machine with the data security kit installed for the "User's Manual". If you have any questions about the description, please contact your dealer or nearest authorized service representative.

Powering ON of the machine

- When the powering on is successful, the login screen will be displayed on the operation panel.
- When the powering on is failed, "Call for service." will be displayed on the operation panel or nothing will be displayed on the operation panel and the machine will stop operation.
  - Refer to the "User's Manual" and the "Use in Advanced Security Mode" in this document and power off and on.

Powering OFF of the machine

- When the powering off is started, "Now turning off the power." will be displayed. When the powering off is completed, the operation panel will be blacked out.

User Authentication

- When the authentication is successful on the operation panel, the home screen of the logged in user will be displayed. When the authentication is successful on the web page, the setting screen will be displayed.
- When the authentication is failed, "Authentication failed." will be displayed on the login screen.
  - Check the entered login name, password and authentication destination and perform authentication again.
- If the authentication is performed with the account locked, "Account is currently locked." will be displayed on the login screen.
  - Refer to the "About the lockout function" in the Operation Manual of the data security kit and release the lock, then perform authentication again.

Printing with the Printer Driver

- When the printing is executed from PC, no response is returned concerning whether the print data received from PC are stored in the machine successfully or unsuccessfully.
  - Login as the administrator or the user entered in the printing preferences window of the printer driver. Select the folder of storing destination entered in the printing preferences window of the printer driver in [Document Filing] of the operation panel or [Document Operations] → [Document Filing] of the web page. When the storing is successful, the file including the print data will be displayed on the file selection screen.
  - When the storing is successful, refer to the "PRINTER" of the "User's Manual" and execute printing of the stored print data on the operation panel.
  - When the storing is failed, refer to the "User's Manual" and the "Use in Advanced Security Mode" in this document and solve the problem, then execute the printing again.
- No response is returned concerning the completion of the printing of stored print data.
  - When the printing is completed, the job of print execution will be displayed on the screen [Job Status] → [Print] → [Complete] and "OK" will be displayed on the [Status].
  - The printing may be interrupted due to out of paper etc. Refer to the message displayed on the operation panel and the "User's Manual" and solve the problem, then restart the printing.

Copy

- No response is returned concerning the completion of the copy.
  - When the copy is completed, the job of copy execution will be displayed on the screen [Job Status] → [Print] → [Complete] and “OK” will be displayed on the [Status].
  - The copy may be interrupted due to out of paper etc. Refer to the message displayed on the operation panel and the "User’ s Manual" and solve the problem, then restart the copy.

Scan Sending (E-mail, File Server)

- No response is returned concerning the success of the sending.
  - When the sending is successful, the job of sending execution will be displayed on the screen [Job Status] → [Scan] → [Complete] and “Send OK” will be displayed on the [Status].
- When the sending is failed, a warning message will be displayed on the operation panel. (Example: “Selected servers are not found.”, “Communication with selected server is lost while sending image.”)
  - Refer to the message displayed on the operation panel and the "User’ s Manual" and the "Use in Advanced Security Mode" in this document and solve the problem, then execute the sending again.

Fax Sending

- When the sending is successful, beep the sound of sending completion.
  - The job of sending execution will be displayed on the screen [Job Status] → [Fax] → [Complete] and “Send OK” is displayed on the [Status].
- If the sending destination is busy and the recall is specified, the sending is executed again after a while automatically.
  - Refer to the "FACSIMILE" of the "User’s Manual" for detail.
- If a communication error has occurred at the sending and the recall is specified, the sending is executed again after a while automatically.
  - Refer to the "FACSIMILE" of the "User’s Manual" for detail.
- If the sending is failed including recalling, beep the sound of sending error.
  - The job of sending execution will be displayed on the screen [Job Status]→[Fax]→[Complete] and the cause of failure will be displayed on the [Status]. Refer to the "FACSIMILE" of the "User’s Manual" for detail.

Fax Receiving

- When reception begins, the information indicator brinks in white. A beep sounds when reception ends.
  - Refer to the "FACSIMILE" of the "User’s Manual" for detail.

Document Filing

- When the data storing is completed, “Data has been encrypted and stored.” will be displayed.
  - Login as the administrator or the user who executed the data storing. Select the folder of storing destination in [Document Filing] of the operation panel or [Document Operations] → [Document Filing] of the web page, then the stored file will be displayed on the file selection screen.
- When the deletion is executed on the operation panel and the deletion of the data is started, “Data is being cleared.” will be displayed. When the deletion is completed, this message will disappear. When the deletion is executed on the web page and the deletion is completed, “Your request was successfully processed.” will be displayed.
- Refer to the "Copy" of this section, for the response of print by re-operation. Refer to the "Scan Sending (E-mail, File Server)" of this section, for the response of E-mail Sending or File Server Sending by re-operation. Refer to the "Fax Send" of this section, for the response of Fax sending by re-operation.

Display of Job Status

- The job list corresponding to the selected tab and the processing status will be displayed.
  - When logged in with a user other than the administrator, the jobs of the other users are masked partially with “*****” to display.

Stopping/Deleting of Job in Job Queue

- No response is returned concerning the completion of stopping/deleting of the job.
  - When the stopping/deleting of the job is completed, the stopped/deleted job will be eliminated in the list of Job Queue.

Addition/Change of User for Internal Authentication

- When the addition/change is successful, the screen will be switched to [User List] screen.
- When the addition/change is failed, the messages urging to enter the required items or correct wrong input will be displayed. (Example: “PIN code/password must be from 15 to 255 one byte characters.”, “The selected login name has been used. Enter another one.”)
  - Refer to the displayed messages, the "BEFORE USING THE MACHINE" of the "User’s Manual" and the "Use in Advanced Security Mode" in this document, then perform the addition/change again.

Deletion of User for Internal Authentication

- No response is returned concerning the completion of deletion.
  - When the deletion is completed, the user selected at the execution will be eliminated from the user list.
- When the user be deleted, delete the data storage in the machine associated with the deleted user.

Addition/Change of Authority Group

- When the addition/change is successful, the screen will be switched to [Authority Group] screen and “Your request was successfully processed. Your setting will be valid after you login again.” will be displayed.
- When the addition/change is failed, the messages urging to enter the required items or correct wrong input will be displayed. (Example: “Please enter Group Name.”)
  - Refer to the displayed messages and the "BEFORE USING THE MACHINE" of the "User’s Manual", then perform the addition/change again.

Return Authority Group to Factory Default State

- When the returning of status is completed, “Your request was successfully processed.” will be displayed.
  - When the returning of status is completed, the authority group selected at the execution will be eliminated from the group list.

Addition/Change of Address Book

- When the addition/change is successful on the operation panel, “Registration is completed.” will be displayed. When the addition/change is successful on the web page, “Your request was successfully processed.” will be displayed.
- When the addition/change is failed, the messages urging to enter the required items or correct wrong input will be displayed. (Example: “This number is already used.”, “Please enter Address Name.”)
  - Refer to the displayed messages, the "User’s Manual", then perform the addition/change again.

Deletion of Address Book

- When the deletion is executed by selecting individual address on the operation panel, “Your request was successfully processed.” will be displayed at the completion of deletion. When "Delete All" is executed on the operation panel and the deletion is started, “All addresses in Address Book are being deleted. Please wait.” will be displayed. When the deletion is completed, this display will disappear. When the deletion is completed on the web page, “Your request was successfully processed.” will be displayed.
  - When the deletion is completed, the address selected at the execution will be eliminated from the Address Book.

Change of Date/Time

- When the change is completed, “Your request was successfully processed.” will be displayed and the changed date and time will be shown in [Current Date].

Creation of Device Certificate

- When the creation is successful, “Your request was successfully processed.” will be displayed.
- When the creation is failed, the messages urging to enter the required items or correct wrong input will be displayed. (Example: “Enter Common Name.”, “Certification start date contains non-numeric value.”)
  - Refer to the displayed messages and the "SYSTEM SETTINGS" of the "User’s Manual", then perform the creation again.

Deletion of Device Certificate

- When the deletion is completed, “Your request was successfully processed.” will be displayed.
  - The device certificate selected at the execution will be eliminated from the list on the [Device Certificate Management] screen.
  - If you delete the device certificate in use for secure communications such as SSL/TLS, please reboot the machine just after the successful deletion.

Creation of Certificate Signing Request (CSR)

- When the creation is successful, “Your request was successfully processed.” will be displayed and you can check the certificate information of the created certificate signing request (CSR).
  - After the creation is successful, press [Save] button and save the file with the certificate information on your PC.
- When the creation is failed, the messages urging to enter the required items or correct wrong input will be displayed. (Example: “Enter Common Name.”, “Enter Country/Region.”)
  - Refer to the displayed messages and the "SYSTEM SETTINGS" of the "User’s Manual", then perform the creation again.

Deletion of Certificate Signing Request (CSR)

- When the deletion is completed, “Your request was successfully processed.” will be displayed.
  - The Certificate Signing Request (CSR) selected at the execution will be eliminated from the list on the [Certificate Signing Request (CSR) Management] screen.

Installation of Public Key Certificate

- When the installation is successful, “Your request was successfully processed.” will be displayed.
- When the installation is failed, the messages urging to enter the required items or correct wrong input will be displayed. (Example: “Please enter File Name.”, “Certificate is not installed.”)
  - Refer to the displayed messages and the "SYSTEM SETTINGS" of the "User’s Manual", then perform the installation again.

Selection of Device Certificate

- When the selection is completed, the screen will be switched and “Your request was successfully processed. Your setting will be valid after you power down and then restart the copier.” will be displayed.
  - Press [Reboot Now] button on the screen. The machine reboots.

Removal of Device Certificate

- When the removal is completed, the screen will be switched and “Your request was successfully processed. Your setting will be valid after you power down and then restart the copier.” will be displayed.
  - Press [Reboot Now] button on the screen. The machine reboots.

Change of Minimum Password Length

- When the change is completed, “Your request was successfully processed.” will be displayed.
  - After the change is completed, users who specify the passwords which don’t satisfy the changed minimum password length cannot log in. Refer to the "Use in Advanced Security Mode" in this document, then change the password.

Change of Identification and Authentication Method

- When the change is completed on the operation panel, “The change is reflected and the operation is reset.” will be displayed. When the change is completed on the web page, “Your request was successfully processed.” will be displayed.

Setting of Automatic Logout Time

- When the setting is completed on the operation panel, “The change is reflected and the operation is reset.” will be displayed. When the change is completed on the web page, “Your request was successfully processed.” will be displayed.

Setting of Audit Log Sending Destination

- When the setting is successful, the screen will be switched and “Your request was successfully processed. Your setting will be valid after you power down and then restart the copier.” will be displayed.
  - Press [Reboot Now] button on the screen. The machine reboots.
- When the setting is failed, the messages urging to enter the required items or correct wrong input will be displayed. (Example: “Port Number value must be 65535 or less.”, “Port Number contains non-numeric characters.”)
  - Refer to the displayed messages and the "SYSTEM SETTINGS" of the "User’s Manual", then perform the setting again.

Addition/Change of LDAP Server

- When the addition/change is successful, the screen will be switched to [LDAP Settings] screen.
- When the addition/change is failed, the messages urging to enter the required items or correct wrong input will be displayed. (Example: “Please enter LDAP Server.”, “Port Number contains non-numeric characters.”)
  - Refer to the displayed messages and the "SYSTEM SETTINGS" of the "User’s Manual", then perform the addition/change again.

Setting of IP Address

- When the setting is successful, the screen will be switched and “Your request was successfully processed. Your setting will be valid after you power down and then restart the copier.” will be displayed.
  - Press [Reboot Now] button on the screen. The machine reboots.
- When the setting is failed, the messages urging to enter the required items or correct wrong input will be displayed. (Example: “Please enter IPv4 Address.”, “Incorrect format for IPv4 Address.”)
  - Refer to the displayed messages and the "SYSTEM SETTINGS" of the "User’s Manual", then perform the setting again.

Setting of E-mail Sending Server

- When the setting is successful, “Your request was successfully processed.” will be displayed.
- When the setting is failed, the messages urging to enter the required items or correct wrong input will be displayed. (Example: “Port Number contains non-numeric characters.”, “Please enter Reply e-mail Address.”)
  - Refer to the displayed messages and the "SYSTEM SETTINGS" of the "User’s Manual", then perform the setting again.

Import of Certificate Authority certificate

- When the import is successful, the screen will be switched and “Your request was successfully processed. Your setting will be valid after you power down and then restart the copier.” will be displayed.
  - Press [Reboot Now] button on the screen. The machine reboots.
- When the import is failed, the messages urging to enter the required items or correct wrong input will be displayed. (Example: “Please enter File Name.”, “It failed to read a file because the specified file was not found or the file was invalid.”)
  - Refer to the displayed messages and the "CA Certificate Management Function" of this document, then perform the import again.

Deletion of Certificate Authority certificate

- When the deletion is completed, the screen will be switched and “Your request was successfully processed. Your setting will be valid after you power down and then restart the copier.” will be displayed.
  - Press [Reboot Now] button on the screen. The machine reboots.
  - The certificate selected at the execution will be eliminated from the list on the [CA Certificate Management] screen.

Query of Firmware Version

- The firmware version is displayed.

Firmware Update

- All users including the administrator cannot confirm the response concerning the success/failure of firmware update, because it is done by the service engineer who is permitted by the administrator.
  - The success/failure of the firmware update should be confirmed by the version of the firmware after update is executed.
  - If the firmware update is failed, please contact the service engineer who executed the firmware update.

Initialize Private Data/Data in Machine

- The audit log in this machine is also deleted by initialization. If the save destination of the audit log is set to an external server, confirm that it is sent successfully before starting initialization. If the save destination of the audit log is set to the internal storage, export it as necessary before starting initialization.
- If the save destination of the audit log is set to an external server, the audit log of event name Change Setting, additional information “Initialize Private Data / Data in Machine” and “Execute” will be sent when initialization is started.
- After the initialization is completed, the machine will reboot. After rebooting, the report of completion of initialization will be output and the message of completion of initialization will be displayed on the operation panel.
- If some error has occurred during the initialization, “Call for service.” will be displayed on the operation panel.
  - Please contact your dealer or nearest authorized service representative.