KONICA MINOLTA

Giving Shape to Ideas

bizhub 4750/4050

for PKI Card System

User's Guide

Security Operations

2015. 4
Ver. 1.04

Contents

3 User Operations

1 Security

1 Security

1.1 Introduction

Thank you for purchasing our product.

This User's Guide contains the operating procedures and precautions to be used when using the security functions offered by the bizhub 4750/4050 machine. To ensure the best possible performance and effective use of the machine, read this manual thoroughly before using the security functions. The Administrator of the machine should keep this manual for ready reference. The manual should be of great help in finding solutions to operating problems and questions.

This User's Guide (Ver. 1.04) covers the following.

TOE Name	bizhub 4750/bizhub 4050 PKI Card System Control Software
Controller Firmware	A6F730G0273999P

Compliance with the ISO15408 Standard

When the Enhanced Security Mode on this machine is set to [ON], more enhanced security functions are available.

The security functions offered by the bizhub 4750/4050 machine comply with ISO/IEC15408 (level: EAL3).

Operating Precautions

The machine gives an alarm message or an alarm sound (peep) when a wrong operation is performed or a wrong entry is made during operation of the machine. (No "peep" alarm sound is issued if a specific sound setting in Sound Setting of Accessibility Setting is set to [OFF].) If the alarm message or alarm sound is given, perform the correct operation or make the correct entry according to the instructions given by the message or other means.

The Administrator of the machine should not leave the machine with the setting screen left displayed after the access to that mode is completed or in the middle of the mode. If it is absolutely necessary to leave the machine, the Administrator of the machine should log off from the mode.

The Administrator of the machine should make sure that each individual general user logs off from the current mode whenever the access to that mode is completed or if the user leaves the machine in the middle of the mode with the mode screen left displayed.

If an error message appears during operation of the machine, perform steps as instructed by the message. For details of the error messages, refer to the User's Guide furnished with the machine and that furnished with the Authentication Unit. If the error cannot be remedied, contact your service representative.

NOTICE

This machine permits duplicate login operations performed by the service engineer, the Administrator of the machine, and the user.

- The Administrator of the machine should make sure that, when the service engineer changes the settings, neither the Administrator of the machine nor the user performs the login operation.
- The Administrator of the machine should make sure that no user is allowed to perform the login operation when the Administrator of the machine changes or deletes user information or user data.
- To prevent settings of the machine from being duplicated, the Administrator of the machine should not attempt to change the settings in a condition of having logged onto a mode simultaneously from the control panel and the client PC.

INSTALLATION CHECKLIST

This Installation Checklist contains items that are to be check by the Service Engineer installing this machine. The Service Engineer should check the following items, then explain each checked item to the Administrator of the machine.

To Service Engineer

Make sure that each of these items is properly carried out by checking the box on the right of each item.

1.	Perform the following steps before installing this machine.	
	Check with the Administrator to determine if the security functions of this machine should be enhanced. If the functions should be enhanced, check the following. If the security functions are not to be enhanced, quit the operation without checking the following.	☐
	I swear that I would never disclose information as it relates to the settings of this machine to anybody, or perform malicious or intentional act during setup and service procedures for the machine.	☐
	When giving a copy of the User's Guide, explain the following to the administrator A digital signature is assigned to the data certified by ISO15408. To ensure integrity of the file, have the administrator of the machine confirm the digital signature using the property of the provided data file in the user's PC environment.	☐
	When giving the User's Guide Security Operations to the Administrator of the machine, check that the User's Guide is the security-compatible version and explain to the Administrator that it is security-compatible.	☐
2.	After this machine is installed, refer to the Service Manual and perform the following steps.	
	Check that the Firmware version of [Controller F/W] and [Boot F/W] checked with the Service Manual match the values shown in the Firmware Version screen. If the version of the [Controller F/W] does not match, explain to the Administrator of the machine that the firmware requires rewriting and rewrite the firmware. If the version of the [Boot F/W] does not match, suspend the installation procedure and contact Konica Minolta.	☐
	Check that the PKI function has been properly set up in accordance with the PKI card system setup instructions.	☐
3.	After this machine is installed, refer to this User's Guide and perform the following steps.	
	Check that the Administrator Password has been set by the Administrator of the machine.	☐
	Check that the Encryption Key has been set by the administrator of the machine.	☐
	Check that external server (Active Directory only) has been set by the administrator of the machine.	☐
	Check that Password Rules has been set to [ON] by the Administrator of the machine.	☐
	Check that the various functions to be disabled manually have been properly disabled by the administrator of the machine.	☐
	Let the Administrator of the machine set Enhanced Security Mode to [ON].	☐
	Explain to the administrator that the settings for the security functions for this machine have been specified.	☐

When the above steps have been properly carried out, the Service Engineer should make a copy of this page and give the original of this page to the Administrator of the machine. The copy should be kept at the corresponding Service Representative for filing.

Product Name		Company Name	User Division Name	Person in charge
Customer (Administrator of Machine)				
Service Representative			-	

1.2 Security Functions

Setting the Enhanced Security Mode to [ON] will validate the security function of this machine. For details of the settings of different security functions to be changed by turning [ON] the Enhanced Security Mode, see page 2-6.

A password that can be set must meet the requirements of the Password Rules. The machine does not accept setting of an easily decipherable password. For details of the Password Rules, see page 1-9.

If a wrong password has been entered three cumulative times during password authentication, the machine determines that it is unauthorized access through Prohibited Functions When Authentication Error, prohibiting any further entry of the password. By prohibiting the password entry operation, the machine prevents unauthorized use or removal of data, thereby ensuring secured used of the machine. This function is not, however, governed by authentication by the ISO15408.

When the machine is to be discarded, or use of a leased machine is terminated at the end of the leasing contract, the data erase function overwrites and erases all data stored in all spaces of the HDD. The function also resets all passwords saved in the memory area on the MFP board to factory settings, preventing leak of data. For details of items to be cleared by data erase function, see page 1-9.

Check Count Clear Conditions

The following are the conditions for clearing or resetting the check count of the number of wrong entries at the time of authentication.

NOTICE

The check count is cleared or reset by restarting the machine. If there is any user who frequently turns ON and OFF the machine, warn him or her of the fact or take necessary steps.

<Administrator Settings>

- Authentication of Administrator Settings is successful.
- The machine is restarted

1.3 Data to be Protected

The underlying concept of this machine toward security is "to protect data that can be disclosed against the intention of users."

The following types of image files that have been saved in the machine and made available for use by its users are protected while the machine is being used.

- Encrypted document transmitted to the machine using a dedicated printer driver and an IC card from the client PC and saved in the machine
- Image files which have been scanned for transmission to a user mail address through e-mail (S/MIME)

The following types of data saved in the HDD are protected when use of a leased machine is terminated at the end of the leasing contract, the machine is to be discarded, or when the HDD is stolen.

- Encrypted document
- Scanned image files
- Image files other than Encrypted document
- Image files of jobs in the queue state other than Scanned image files
- Data files left in the HDD data space, used as image files and not deleted through the general deletion operation
- Temporary data files generated during print image file processing

1.4 Precautions for Operation Control

This machine and the data handled by this machine should be used in an office environment that meets the following conditions. The machine must be controlled for its operation under the following conditions to protect the data that should be protected.

Roles and Requirements of the Administrator

The Administrator should take full responsibility for controlling the machine, thereby ensuring that no improper operations are performed.

<To Achieve Effective Security>

- A single individual person who is capable of taking full responsibility for controlling the machine should be appointed as the Administrator to make sure that no improper operations are performed.
- When an SMTP server (mail server), a DNS server, a user information control system, or a WebDAV server is to be used, the Administrator of the machine should periodically check that the corresponding administrator of the server appropriately manages the server to allow no settings to be changed without permission.

Password Usage Requirements

The administrator must control the Administrator Password and Encryption Key appropriately so that they may not be leaked. These passwords should not be ones that can be easily guessed.

<To Achieve Effective Security>

- Make absolutely sure that only the administrator knows the Administrator Password and Encryption Key.
- The administrator must change the Administrator Password and Encryption Key at regular intervals.
- The administrator should make sure that any number that can easily be guessed from birthdays, employee identification numbers, and the like is not set for the Administrator Password and Encryption Key.
- If the Administrator Password has been changed by the Service Engineer, the administrator should change the Administrator Password as soon as possible.
- Upon change of the Administrators, the old Administrator of the machine should promptly have the new one change the Administrator password.

Network Connection Requirements for the Machine

If the LAN is to be connected to an outside network, no unauthorized attempt to establish connection from the external network should be permitted.

<To Achieve Effective Security>

- If the LAN, in which the machine is installed, is connected to an outside network, install a firewall or similar network device to block any access to the machine from the outside network and make the necessary settings.
- Provide an appropriate network control at all times to make sure that no other copying machine is connected without prior notice to the office LAN to which this machine is connected.

User information control system control requirements

The administrator of the machine and the server administrator are required to apply patches to, or perform account control for, this machine and the user information control system connected to the office LAN in which the machine is installed to ensure operation control that achieves appropriate access control.

<To Achieve Effective Security>

- Apply patches so that the user information management system is always up-to-date.
- Change the corresponding account information promptly as soon as user authorities are changed.
- Delete the corresponding account information promptly as soon as the specific user is transferred.

Security function operation setting operating requirements

The administrator of the machine should observe the following operating conditions.

- The administrator should make sure that the machine is operated with the settings described in the installation checklist made properly in advance.
- The administrator should make sure of correct operation control so that the machine is used with the Enhanced Security Mode set to [ON].
- When the Enhanced Security Mode is turned [OFF], the administrator is to make various settings according to the installation checklist and then set the Enhanced Security Mode to [ON] again. For details of settings made by the service engineer, contact your service representative.
- When the machine is to be discarded or use of a leased machine is terminated at the end of the leasing contract, the administrator should use the Overwrite All Data function to thereby prevent data to be protected from leaking.

Operation and control of the machine

The administrator of the machine should perform the following operation control.

- The administrator of the machine should log off from the Administrator Settings whenever the operation in the Administrator Settings is completed. The administrator of the machine should also make sure that each individual user logs off from the User Authentication mode after the operation in the User Authentication mode is completed, including operation of the Encrypted document.
- The administrator of the machine should set the Encryption Key according to the environment, in which this machine is used.
- The administrator of the machine should make sure that each individual user updates the OS of the user's terminal and applications installed in it to eliminate any vulnerabilities.

The administrator of the machine disables the following functions and operates and manages the machine under a condition in which those functions are disabled.

Function Name	Setting Procedure
USB Memory Print Function	Using [Administrator Settings] ▸▸ [System Settings] ▸▸ [Folder Settings] ▸▸ [External Memory Function Settings], set [Print Document] to [OFF].

Machine Maintenance Control

The Administrator of the machine should perform the following maintenance control activities.

- Provide adequate control over the machine to ensure that only the Service Engineer is able to perform physical service operations on the machine.
- Provide adequate control over the machine to ensure that any physical service operations performed on the machine by the Service Engineer are overseen by the Administrator of the machine.
- Some options require that Enhanced Security Mode be turned [OFF] before they can be used on the machine. If you are not sure whether a particular option to be additionally purchased is fully operational with the Enhanced Security Mode turned [ON], contact your Service Representative.

Implementing digital signature properly

The administrator of the machine should make the setting for adding a digital signature by selecting either [Always add signature] or [Select when sending]. He or she should make sure that the digital signature is added whenever an IC card owner sends highly confidential image data to the client PC.

Operating conditions for the IC card and IC card reader

The machine supports the following types of IC card and IC card reader.

- The types of IC cards supported by the machine are the Common Access Card (CAC) and Personal Identity Verification (PIV).
- The type of IC card reader supported by the machine is AU-211P/Identive SCR-3310/SCR-3310v2. Be sure to use the IC card reader provided by the Service Representative. For details, contact your Service Representative.

The service representative is to install the IC card reader to the USB port on the front side of the machine. The administrator of the machine should make sure that the user will not relocate the IC card reader to any other USB port. Operation through any other USB port is not guaranteed.

The administrator of the machine should also make sure that no inadequate device is connected to the connector of the IC card reader.

IC card owner requirements

The administrator of the machine should make sure that operating rules that specify the following operations exist within the organization and that the operations are implemented according to the rules.

- The person responsible within the organization that uses the machine should distribute the IC card issued for use by the organization to a specific person who is authorized to own the IC card.
- The person responsible within the organization that uses the machine should prohibit the user from transferring or lending the IC card to any third person and make sure that the user reports any lost IC card. If the IC card is lost, the system is at risk of being illegally accessed. In such cases, the registered user in question should be deleted from the external server, so that the lost IC card is disabled for authentication.
- The person responsible within the organization that uses the machine should make sure that each IC card user removes his or her IC card from the card reader and never leaves the card in the card reader after he or she completes the operation of the machine.

1.5 Miscellaneous

Password Rules

According to certain Password Rules, registration of a password consisting of a string of a single character or change of a password to one consisting of a string of a single character is rejected for the Administrator Password. For the Administrator Password, the same password as that currently set is not accepted.

Study the following table for more details of the number of digits and characters that can be used for each password.

NOTICE

Before setting the Enhanced Security Mode, be sure to enable the Password Rules. For details of the settings of the Password Rules, see page 2-8

Types of passwords	No. of digits	Characters
Administrator Password	8 to 16 digits *	• Numeric characters: 0 to 9 • Alpha characters: upper and lower case letters • Symbols: !, #, $, %, &, ', (,), *, ,, -, ., /, :, ;, <, =, >, ?, @, [, \,], ^, _, `, {, |, }, ~, +, SPACE Selectable from among a total of 94 characters • "" cannot be used

*: The minimum number of characters set in [Set Minimum Password Length] must be set for the password. The default value is 12.

Precautions for Use of Various Types of Applications

When the Encrypted document function is to be used, be sure to install the dedicated printer driver in the client PC.

Encrypting communications

Effective 2014, do not use the 1024-bit RSA and SHA-1. Or, an increased risk results of falsification and leakage of data to be protected.

Items of Data Cleared by Data Erase Function

The data erase function clears the following items of data.

NOTICE

Perform "Restore All" from the control panel of the machine, and not via the network.

The encryption key is not deleted even if Restore All or Overwrite All Data is performed. For the detailed deleting procedure, see page 2-22.

Items of Data Cleared	Description	Method
Enhanced Security Mode	Set to [OFF]	Overwrite All Data HDD Format Restore All
Password Rules	Sets [OFF] and disables [Set Minimum Password Length]	Restore All
Encrypted document	Deletes all Encrypted document saved in Encrypted document User Box	Overwrite All Data HDD Format
Image files	• Image files other than Encrypted document • Image files of jobs in the queue state other than Scanned image files • Data files left in the HDD data space, used as image files and not deleted through the general deletion operation • Temporary data files generated during print image file processing	Overwrite All Data HDD Format
Administrator Password	Clears the currently set password, resetting it to the factory setting	Overwrite All Data Restore All

Items of Data Cleared	Description	Method
S/MIME certificate	Deletes the currently set S/MIME certificate	Overwrite All Data HDD Format
External Server	Deletes the currently set external server	Overwrite All Data HDD Format Restore All
Time Adjustment Setting (NTP)	Set to [Disable]	Restore All

General functions and operations

For details of general functions and settings of this machine, refer to the User's Guide furnished with the machine.

HDD Format

Execute HDD format when, for example, to initialize the HDD (to be reset to the default state) or when the HDD is replaced with a referent one. Executing HDD format deletes data saved in the machine's HDD.

- For details of items that are cleared by HDD Format, see page 1-9.
- HDD formatting turns [OFF] the Enhanced Security Mode. So, it must be turned [ON] again. For details of settings, see page 2-6.

Upgrading of the firmware

If upgrading of the firmware has been performed by the service engineer, the Administrator of the machine must execute [Restore All]. Execute [Restore All] after the firmware has been upgraded. For details of the execution of [Restore All], see page 2-26.

- For details of items of data to be cleared by [Restore All], see page 1-9.
- The execution of [Restore All] will turn [OFF] the Enhanced Security Mode. So, it must be turned [ON] again. For details of settings, see page 2-6.

Software used in the machine

The following lists the types of software and their versions used for the ISO15408 evaluation for this machine.

The user should appropriately manage the software used with the machine on his or her own responsibility.

Software	Version, etc.
OS (Operating System)	Windows 7 Professional SP1
Internet Explorer	Ver. 11
Printer Driver	KONICA MINOLTA 4750 Series • PCL 6 v1.1.5.0
ActivClient	v7.0.2.25
IC card reader driver	A6F70Y0-A401-G00-00

2 Administrator Operations

2 Administrator Operations

2.1 Accessing the Administrator Settings

This machine implements authentication of the user of the Administrator Settings function through the Administrator Password that verifies the identity as the Administrator of the person who accesses the function. During the authentication procedure, the Administrator Password entered for the authentication purpose appears as "*" or "●" on the display. A failure in authentication as a result of the entry of a wrong password is counted as unauthorized access.

NOTICE

Make sure that none of the general users of the machine will know the Administrator Password.

If the Administrator Password is forgotten, it must be set again by the Service Engineer. Contact your Service Representative.

2.1.1 Accessing the Administrator Settings

The machine does not accept access to the Administrator Settings under any of the following conditions. Wait for some while before attempting to gain access to the Administrator Settings again.

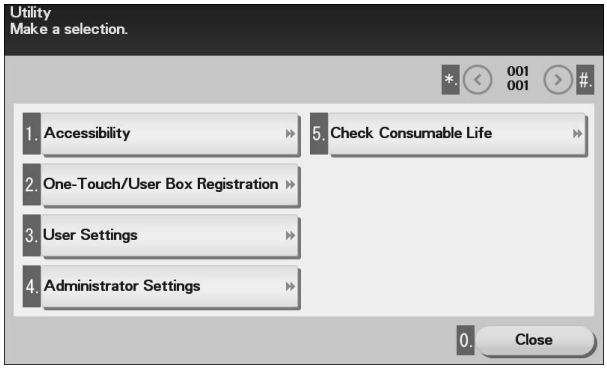
- There is a job being executed by the machine.
- There is a reserved job (timer TX, fax redial waiting, etc.) in the machine.
- Immediately after the power switch has been turned ON.
- A malfunction code is displayed on the machine.

<From the Control Panel>

✔ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.

1 Touch [Utility].

2 Touch [Administrator Settings].



3 Enter the Administrator Password from the keyboard.

➔ Touch [C] to clear all characters.
➔ Touch [ ] to delete the last character entered.
➔ Touch [Shift] to show the upper case/symbol screen.
➔ Touch [Cancel] to go back to the previous screen.

4 Touch [OK].

➔ If a wrong Administrator Password is entered, a message that tells that the Administrator Password does not match appears. Enter the correct Administrator Password.
➔ A failure in authentication as a result of the entry of a wrong password is counted as unauthorized access. If the cumulative number of unauthorized accesses reaches three during operation of the machine, the machine is set into an access lock state and prohibits any subsequent password entry operations. To cancel the access lock state, turn off, then on, the power switch of the machine. When the power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. This interval is necessary to ensure that the machine functions properly.

5 Press the [Reset] key to log off from the Administrator Settings.

<From PageScope Web Connection>

NOTICE

PageScope Web Connection cannot be used when the Enhanced Security Mode has been set to [ON]. To use the PageScope Web Connection, temporarily turn [OFF] the Enhanced Security Mode; then, from the control panel, select [Administrator Settings] ►► [Network Settings] and select [Enable] for [HTTP Server Settings] and perform settings for the PageScope Web Connection.

After the PageScope Web Connection has been used, make necessary settings according to Installation Checklist and then turn [ON] the Enhanced Security Mode again. For details of settings made by the service engineer, contact your service representative.

✔ If an attempt is made to log on to the Administrator Mode while a job is being executed, the machine gives a message that tells that it is now impossible to log on to the Administrator Mode. Click [OK] and try logging on to the Administrator Mode after the execution of the job is completed.

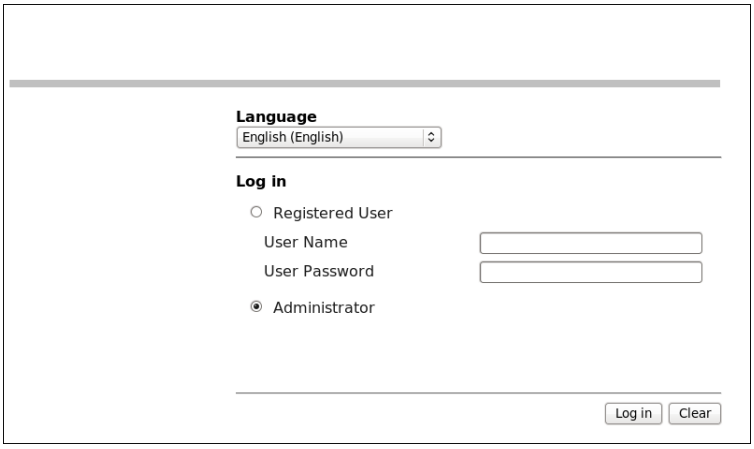
✔ Do not leave the machine with the Administrator Mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Mode.

1 Start the Web browser.

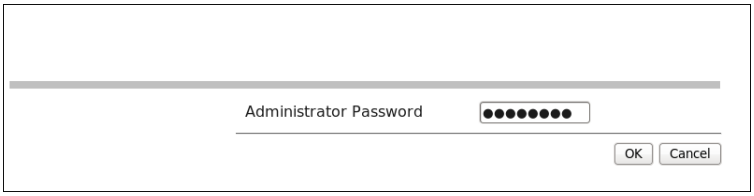
2 Enter the IP address of the machine in the address bar.

3 Press the [Enter] key to start PageScope Web Connection.

4 Click the Administrator radio button and [Log in].



5 Enter the Administrator Password in the password box.



➔ When accessing the Administrator Mode using the PageScope Web Connection, enter the same Administrator Password as that for the machine.

6 Click [OK].

➔ If a wrong Administrator Password is entered, a message that tells that the authentication has failed appears. Enter the correct Administrator Password.

➔ A failure in authentication as a result of the entry of a wrong password is counted as unauthorized access. If the cumulative number of unauthorized accesses reaches three during operation of the machine, the machine is set into an access lock state and prohibits any subsequent password entry operations. To cancel the access lock state, turn off, then on, the power switch of the machine. When the power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. This interval is necessary to ensure that the machine functions properly.

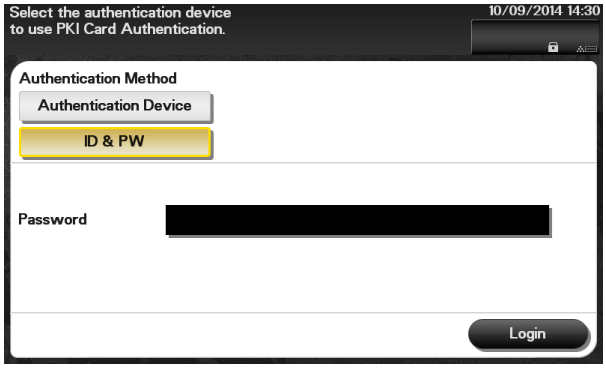
7 Click [Log out]. This allows you to log off from the Administrator Mode.

2.1.2 Accessing the User Mode

You can log on to the User Mode as an administrator. In the User Mode, you can check or delete a job, which is disabled in Administrator Settings.

✔ Do not leave the machine with the User Mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the User Mode.

1 Touch [ID & PW].



2 Touch the [Password] field.

3 Enter the Administrator Password from the keyboard.

➔ Touch [C] to clear all characters
➔ Touch [⌫] to delete the last character entered.
➔ Touch [Shift] to show the upper case/symbol screen.
➔ Touch [Cancel] to go back to the previous screen.

4 Touch [OK].

5 Touch [Access] or [Login].

➔ If a wrong Administrator Password is entered, a message that tells that the Administrator Password does not match appears. Enter the correct Administrator Password.
➔ A failure in authentication as a result of the entry of a wrong password is counted as unauthorized access. If the cumulative number of unauthorized accesses reaches three during operation of the machine, the machine is set into an access lock state and prohibits any subsequent password entry operations. To cancel the access lock state, turn off, then on, the power switch of the machine. When the power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. This interval is necessary to ensure that the machine functions properly.

6 Touch [Access] or [Close] to log off from the User Mode.

2.2 Enhancing the Security Function

When access to the machine by the Administrator of the machine through the Administrator Settings from the control panel is authenticated, the machine enables setting of the Enhanced Security Mode that allows settings for enhancing each of different security functions to be converted all at once.

In the Enhanced Security Mode, the machine allows selection of whether to use the Enhanced Security Mode or not. When the Enhanced Security Mode is set to [ON], the security function is enhanced by automatically setting such functions as that which determines whether each password meets predetermined requirements.

The following settings must first be made before the Enhanced Security Mode is set to [ON].

Settings to be Made in Advance	Description
Administrator Password	Meets the Password Rules. The factory setting is "12345678."
Encryption Key	Set the Encryption Key.
Password Rules	Set to [ON].
Service settings	Calls for setting made by the Service Engineer. For details, contact your Service Representative.

Setting the Enhanced Security Mode to [ON] changes the setting values of the following functions.

Function Name	Factory Setting	When Enhanced Security Mode is set to [ON]
Public Access	Restrict	Restrict (not to be changed)
Print without Authentication	Restrict	Restrict (not to be changed)
User Name List	OFF	OFF (not to be changed)
Registering and Changing Address by the user	Allow	Restrict (to be changed)
S/MIME	S/MIME: Disable Digital Signature: Do not add signature E-mail Text Encryption Method: 3DES	S/MIME: Enable (not to be changed) Digital Signature: Select when sending E-mail Text Encryption Method: 3DES, AES-128, AES-192, AES-256 (not to be changed to DES or RC-2)
FTP Server	Enable	Disable (Selection can be made between [Enable] and [Disable])
SNMPv1/v2c	Read/Write enabled	Only Read is enabled (not to be changed)
SNMP v3 Settings	Restrict	Restrict (not to be changed)
Administrator Password Change Via Network (Pagescope Web Connection)	Enabled	Restrict
Network firmware update protect	Invalid	Valid
CS Remote Care	Usable	Remote device setting disabled
OpenAPI	Enable	Disable (not to be changed)
TCP Socket	Enable	Disable (not to be changed)
HTTP Server	Enable	Disable (not to be changed)

NOTICE

When Password Rules is set to [ON] the characters and the number of digits used for each password are restricted. For details of the Password Rules, see page 1-9.

The Enhanced Security Mode is set to [OFF], if the Administrator of the machine executes any of the following functions. Set the Enhanced Security Mode to [ON] again.

- [HDD Format] is executed.
- [Overwrite All Data] is executed.
- [Restore All] of [Initialize] is executed.
- [Network Settings] of [Initialize] is executed.
- [Restore System] of [Initialize] is executed.

2.2.1 Setting the Password Rules

✔ For the procedure to call the Administrator Settings on the display, see page 2-2.

✔ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.

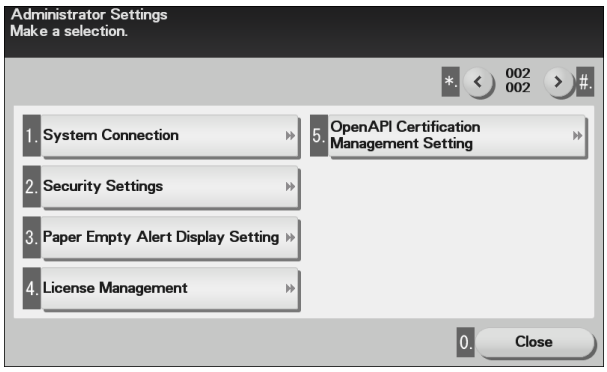
NOTICE

Before enabling the Password Rules, change the currently set password so as to meet the Password Rules. For details of the Password Rules, see page 1-9.

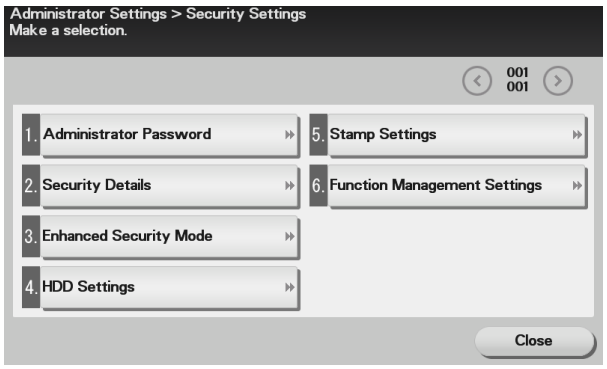
1 Call the Administrator Settings on the display from the control panel.

2 Touch [ ].

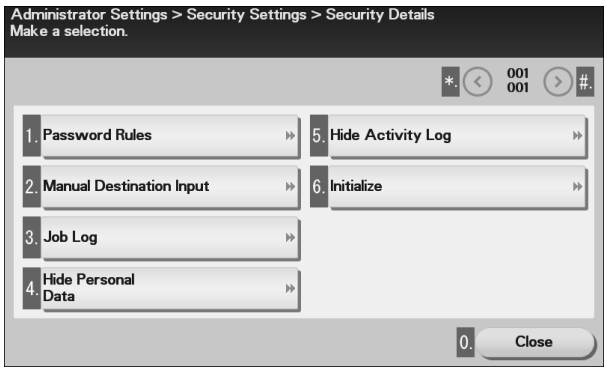
3 Touch [Security Settings].



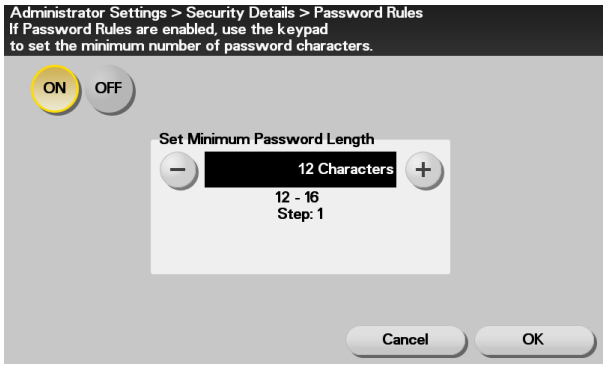
4 Touch [Security Details].



5 Touch [Password Rules].



6 Select [ON] and set [Set Minimum Password Length] (12 to 16 characters).



7 Touch [OK].

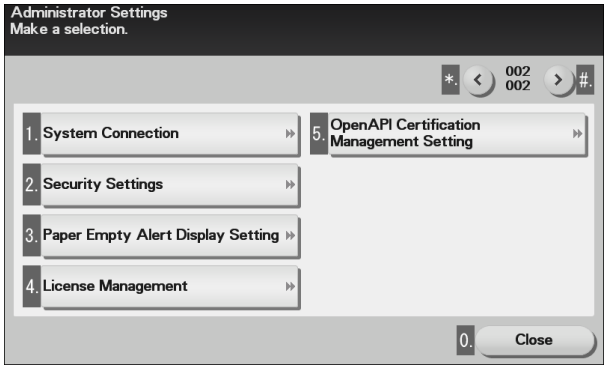
2.2.2 Setting the Enhanced Security Mode

- ✔ For the procedure to call the Administrator Settings on the display, see page 2-2.
- ✔ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.
- ✔ The Enhanced Security Mode is factory-set to [OFF]. Be sure to turn [ON] the Enhanced Security Mode so as to enable the security function of the machine.

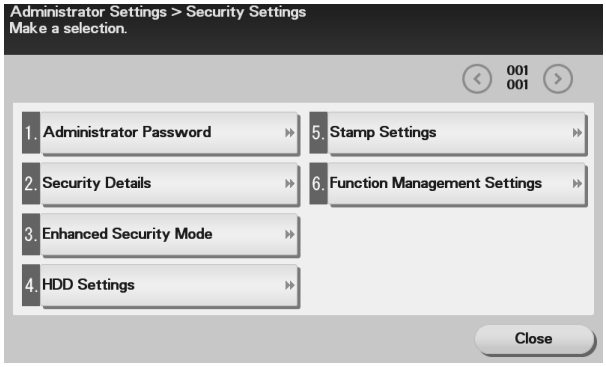
1 Call the Administrator Settings on the display from the control panel.

2 Touch [ ].

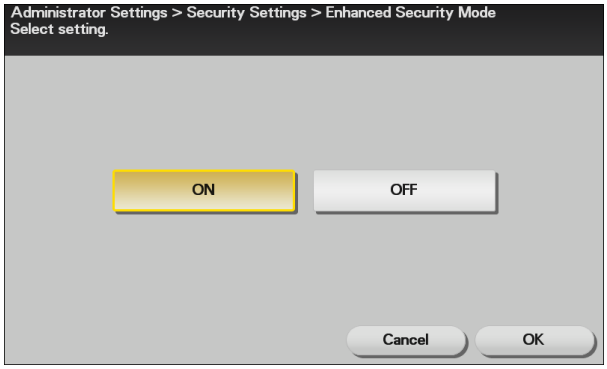
3 Touch [Security Settings].



4 Touch [Enhanced Security Mode].

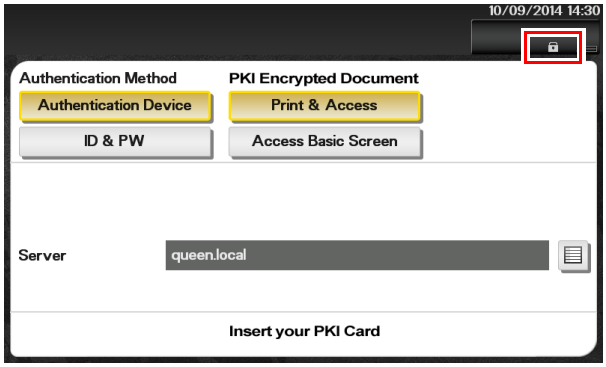


5 Select [ON] to enable the Enhanced Security Mode and touch [OK].
Touch [OK], then the machine restarts automatically.



➔ [ON] can be selected only if the Administrator of the machine has made the necessary settings beforehand. For details of the necessary settings, see page 2-6.

➔ If the Enhanced Security Mode is properly set to [ON], a key icon appears at the portion enclosed by a red frame of the screen, indicating that the machine is in the Enhanced Security Mode.



2.3 Setting the External Server

When access to the machine by the administrator of the machine through the Administrator Settings is authenticated, the machine enables setting of the external server.

The external server that can be used for authentication is Active Directory only. Operate the machine in Active Directory.

NOTICE

PageScope Web Connection cannot be used when the Enhanced Security Mode has been set to [ON]. To use the PageScope Web Connection, temporarily turn [OFF] the Enhanced Security Mode; then, from the control panel, select [Administrator Settings] ▸▸ [Network Settings] and select [Enable] for [HTTP Server Settings] and perform settings for the PageScope Web Connection.

After the PageScope Web Connection has been used, make necessary settings according to Installation Checklist and then turn [ON] the Enhanced Security Mode again. For details of settings made by the service engineer, contact your service representative.

Setting the External Server

✔ For the procedure to access the Administrator Mode, see page 2-2.

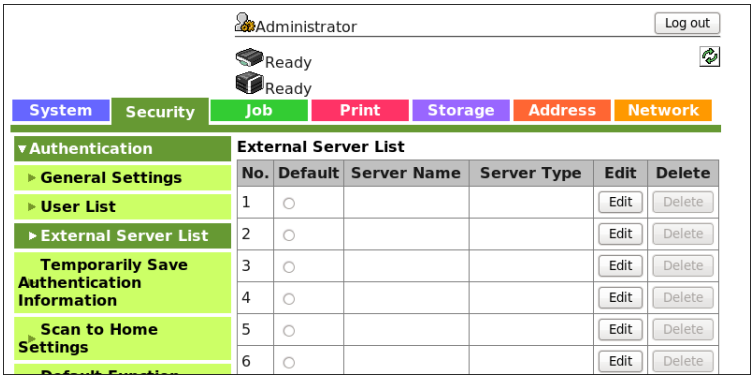
✔ Do not leave the machine with the setting screen of Administrator Mode left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Mode.

1 Start PageScope Web Connection and access the Administrator Mode.

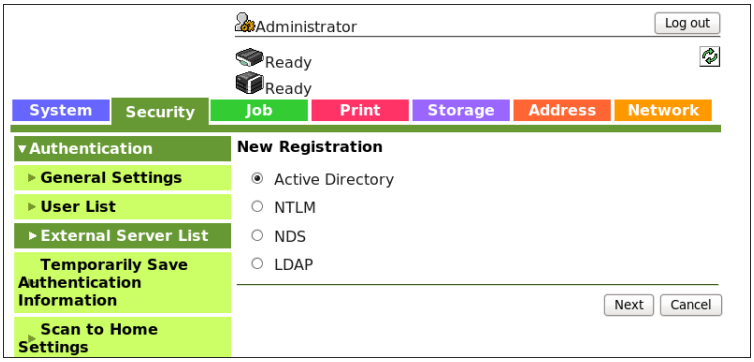
2 Click the [Security] tab.

3 Click [Authentication] ▸▸ [External Server List] from the menu.

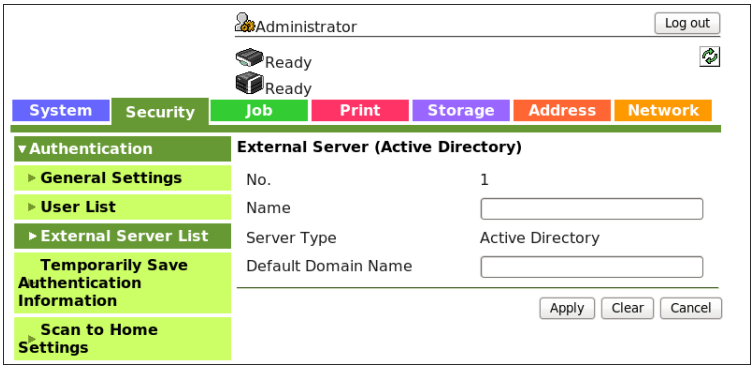
4 Click [Edit].



5 Select [Active Directory] and click [Next].



6 Make the necessary settings.



➔ A Sever Name that already exists cannot be redundantly registered.

7 Click [Apply].

2.4 System Auto Reset Function

When access to the machine by the Administrator of the machine through the Administrator Settings from the control panel is authenticated, the machine enables setting of the operation of the system auto reset function.

If no operations are performed for a predetermined period of time during access to the Administrator Settings or user mode (during setting of User Authentication) from the control panel, the system auto reset function automatically causes the user to log off from the mode.

The predetermined period of time, after which the system auto reset function is activated, can be selected from among nine values between 1 min. and 9 min. System auto reset can also be set to [OFF]. If no operations are performed for 1 min. even with system auto reset set to [OFF], the function causes the user to log off from the mode automatically.

NOTICE

The condition in which the user authentication using the IC card is granted remains valid and the system auto reset function does not cause the user to log off from the mode until the IC card is removed. Do not leave the machine with the IC card inserted in the card reader.

Reference

- Processing of a specific job, however, takes precedence over the system auto reset function. That is, even if a predetermined period of time elapses during which no operations are performed, once the processing of the specific job has been started, the system auto reset function does not cause the user to log off from the mode. The user logs off from the mode after the lapse of a predetermined period of time after the processing of the specific job is completed.

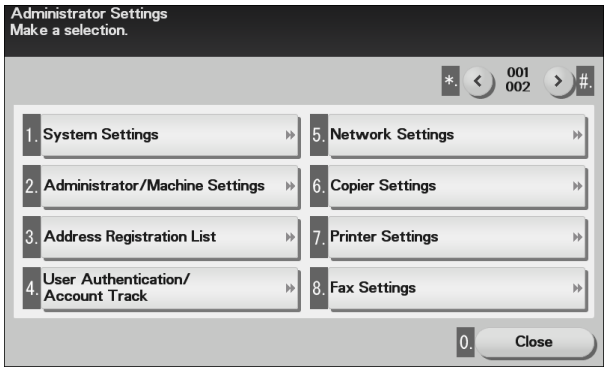
Setting the System Auto Reset function

✔ For the procedure to call the Administrator Settings on the display, see page 2-2.

✔ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.

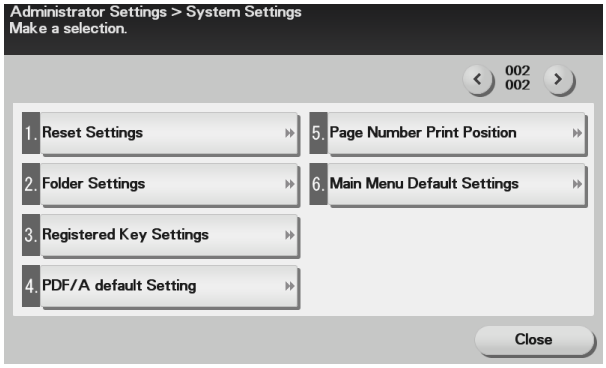
1 Call the Administrator Settings on the display from the control panel.

2 Touch [System Settings].

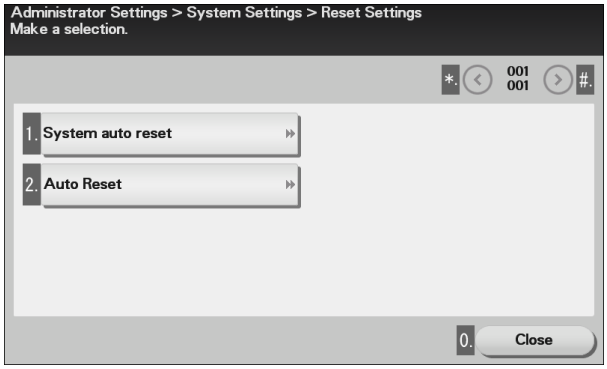


3 Touch [ ].

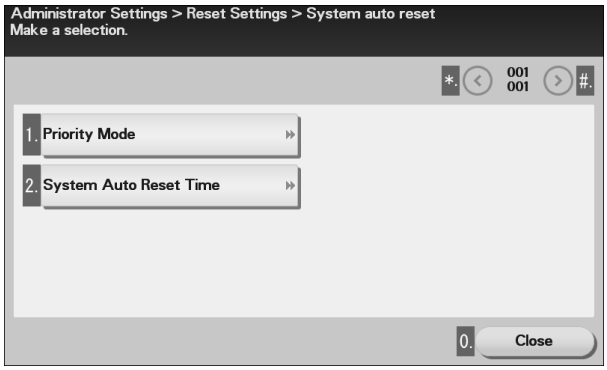
4 Touch [Reset Settings].



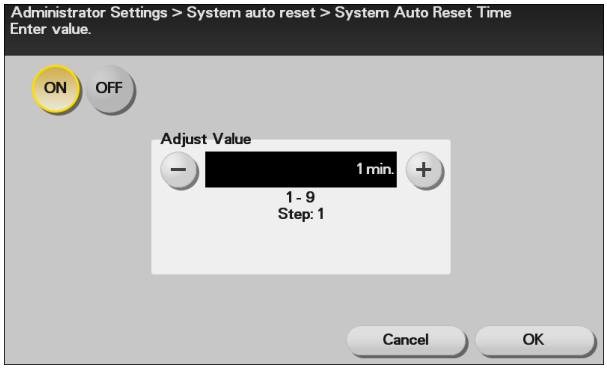
5 Touch [System auto reset].



6 Touch [System Auto Reset Time].



7 Select [ON], and enter the period of time (1 min. to 9 min.) after which system auto reset is activated using [-]/[+] key.



➔ If no operations are performed for 1 min. even with system auto reset set to [OFF], the function is activated to cause the user to log off from the mode automatically.

➔ The time for system auto reset can be set to a value between 1 min. and 9 min., variable in 1-min. increments.

8 Touch [OK].

2.5 Changing the Administrator Password

When access to the machine by the Administrator of the machine through the Administrator Settings from the control panel is authenticated, the machine enables the operation of changing the Administrator Password required for accessing the Administrator Settings.

The Administrator Password entered for the authentication purpose appears as "*" on the display.

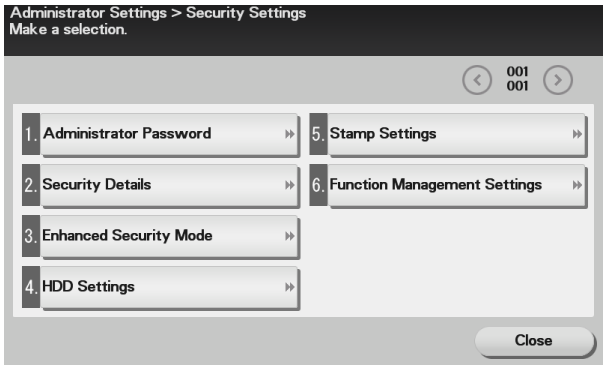
Changing the Administrator Password

✔ For the procedure to call the Security Settings screen on the display, see steps 1 through 3 of page 2-10.

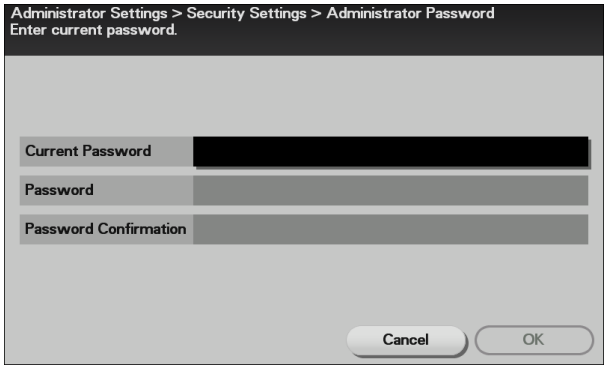
✔ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.

1 Call the Security Settings screen on the display from the control panel.

2 Touch [Administrator Password].



3 Touch the [Current Password] field.



4 Enter the currently set Administrator Password from the keyboard.

➔ Touch [C] to clear all characters.

➔ Touch [⌫] to delete the last character entered.

➔ Touch [Shift] to show the upper case/symbol screen.
➔ Touch [Cancel] to go back to the previous screen.

5 Touch [OK].

➔ If a wrong Administrator Password is entered, a message that tells that the Administrator Password does not match appears. Enter the correct Administrator Password.
➔ A failure in authentication as a result of the entry of a wrong password is counted as unauthorized access. If the cumulative number of unauthorized accesses reaches three during operation of the machine, the machine is set into an access lock state and prohibits any subsequent password entry operations. To cancel the access lock state, turn off, then on, the power switch of the machine. When the power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. This interval is necessary to ensure that the machine functions properly.

6 Touch the [Password] field.

7 Enter the new 12-to-16-digit Administrator Password from the keyboard, and touch [OK].

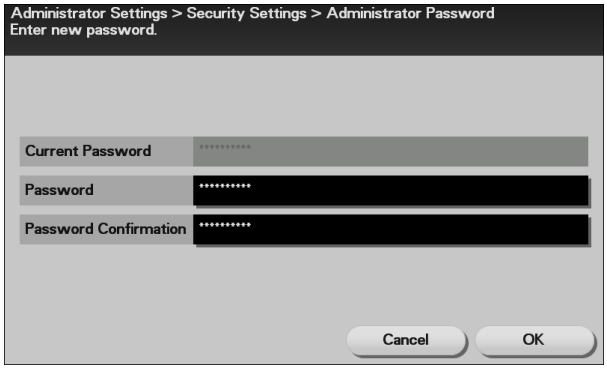
➔ Touch [C] to clear all characters.
➔ Touch [ ] to delete the last character entered.
➔ Touch [Shift] to show the upper case/symbol screen.
➔ Touch [Cancel] to go back to the previous screen.

8 Touch the [Password Confirmation] field.

9 To prevent entry of a wrong Administrator Password, enter the new 12-to-16-digit Administrator Password once again, and touch [OK].

➔ Touch [C] to clear all characters.
➔ Touch [ ] to delete the last character entered.
➔ Touch [Shift] to show the upper case/symbol screen.
➔ Touch [Cancel] to go back to the previous screen.

10 Touch [OK].



➔ If the entered Administrator Password does not meet the requirements of the Password Rules, a message that tells that the entered Administrator Password cannot be used appears. Enter the correct Administrator Password. For details of the Password Rules, see page 1-9.
➔ If the entered Administrator Password does not match, [OK] cannot be touched. Enter the correct Administrator Password.

2.6 Protecting Data in the HDD

When access to the machine by the administrator of the machine through the Administrator Settings from the control panel is authenticated, the machine enables the operation for setting and deleting the Encryption Key.

By setting the Encryption Key, the data stored in the HDD is encrypted, thereby protecting the data in the HDD. The Encryption Key entered is displayed as "*."

NOTICE

If the HDD develops a fault, call your Service Representative.

The following shows setting conditions for the Encryption Key. Perform settings for the Encryption Key fitting these conditions.

No. of digits	Characters
20 digits	• Numeric characters: 0 to 9 • Alpha characters: upper and lower case letters • Symbols: !, ", #, $, %, &, ', (,), *, ,, -, ., /, :, ;, <, =, >, ?, @, [, \,], ^, _, `, {, |, }, ~, +, SPACE Selectable from among a total of 95 characters An Encryption Key consisting of identical characters only cannot be registered or changed.

Reference

- When an Encryption Key (encryption word) is set using HDD Encryption Setting, an Encryption Key with a key length of 256 bits is generated. The generated encryption key is used to encrypt or decrypt data through AES encryption algorithm.

2.6.1 Setting the Encryption Key (encryption word)

✔ For the procedure to call the Security Settings screen on the display, see steps 1 through 3 of page 2-10.

✔ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.

✔ To prevent data from leaking as a result of reinstallation of the HDD on another machine, a unique value that varies from one machine to another must be set for the encryption key.

✔ Do not set any number that can easily be guessed from birthdays, employee identification numbers, and the like for the Encryption Key.

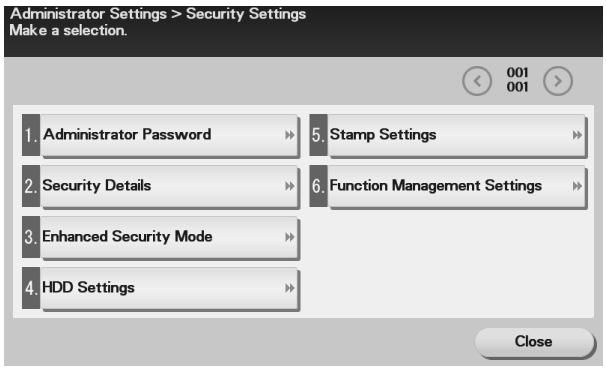
✔ Make sure that nobody but the administrator of the machine comes to know the Encryption Key.

✔ If only the Encryption Key is to be set while the machine is being used without setting the Encryption Key (not covered by certification of ISO15408), the Service Engineer must perform some setting procedures in advance. For details, contact your Service Representative.

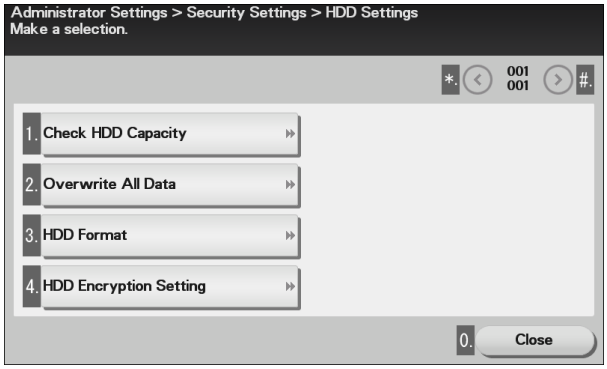
✔ Executing HDD Format erases data in the HDD. It is recommended that important data should be saved in a backup medium in advance. Execution of HDD Format will also reset the setting values of different functions to the default values. Set the Enhanced Security Mode to [ON] again.

1 Call the Security Settings screen on the display from the control panel.

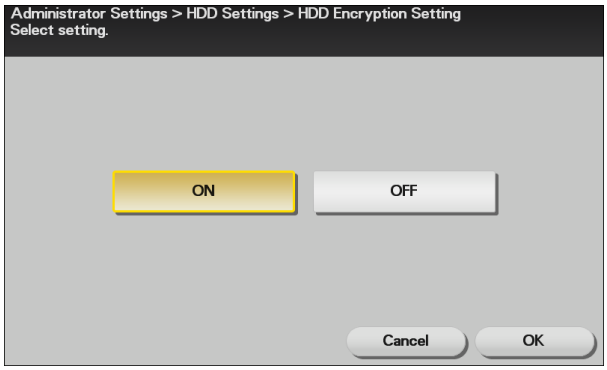
2 Touch [HDD Settings].



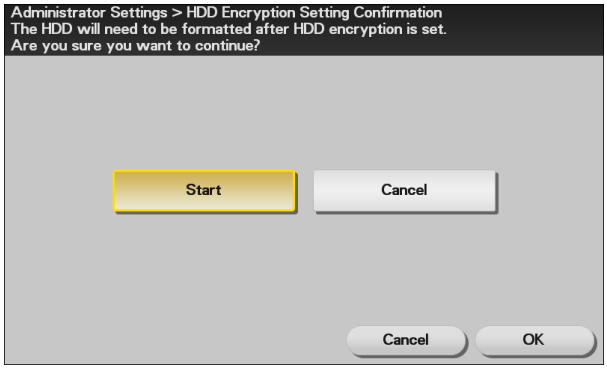
3 Touch [HDD Encryption Setting].



4 Select [ON] and touch [OK].



5 A confirmation message appears. Select [Start] and touch [OK].



➔ Changing the setting of HDD Encryption Setting (switching between ON and OFF) will format the HDD. For details of items that are cleared by HDD Format, see page 1-9.

6 Touch the [Value] field.

7 Enter the 20 digits Encryption Key from the keyboard, and [OK].

➔ If the entered Encryption Key does not meet the setting requirements, [OK] cannot be touched.
➔ Touch [C] to clear all characters.
➔ Touch [ ] to delete the last character entered.
➔ Touch [Shift] to show the upper case/symbol screen.
➔ Touch [Cancel] to go back to the previous screen.

8 Touch [OK].
The machine restarts automatically.

2.6.2 Deleting the encryption key

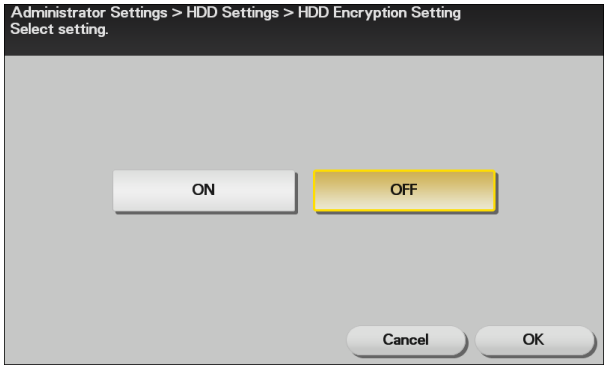
✔ For the procedure to call the HDD Encryption Setting screen on the display, see steps 1 through 3 of page 2-19.

✔ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.

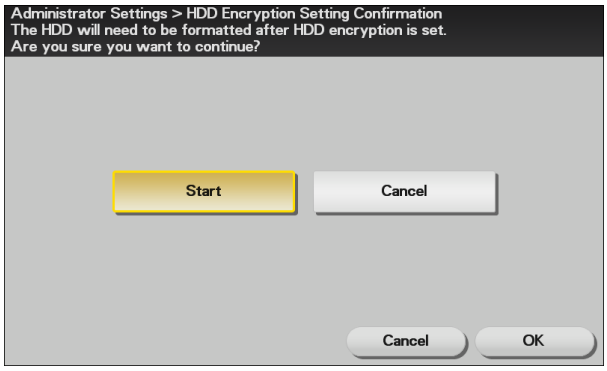
✔ The encryption key cannot be deleted with the Enhanced Security Mode set to [ON].

1 Call the HDD Encryption Setting screen on the display from the control panel.

2 Select [OFF], and touch [OK].



3 A confirmation message appears. Select [Start], and touch [OK].
The machine restarts automatically.



➔ Changing the setting of HDD Encryption Setting (switching between ON and OFF) will format the HDD. For details of items that are cleared by HDD Format, see page 1-9.

2.7 Erasing data when the machine is to be discarded or use of a leased machine is terminated

When access to the machine by the Administrator of the machine through the Administrator Settings from the control panel is authenticated, the machine enables setting of the operations of the Overwrite All Data and Restore All functions.

When the machine is to be discarded or use of a leased machine is terminated at the end of the leasing contract, be sure to erase all data to prevent data left in the machine from leaking. Different methods of erase apply depending on the data space. See the table below for more details.

Data space	Erase method
HDD, Memory area on the MFP board	Overwrite All Data
Memory area on the MFP board	Restore All

NOTICE

Perform erase operations for all of HDD and memory area on the MFP board.

When erase operations are performed, make sure that the operation is normally terminated for data in each of the three different data spaces. If an error occurs during execution of the erase operations, contact your Service Representative for appropriate action.

The Enhanced Security Mode is set to [OFF], if Overwrite All Data or Restore All is executed.

The encryption key is registered in the memory area on the MFP board, but is not deleted even if Restore All or Overwrite All Data is performed. After Restore All or Overwrite All Data is performed, the encryption key must be deleted manually. For details, see page 2-22.

2.7.1 Setting the Overwrite All Data

The HDD Overwrite Method offers the choice of eight different modes, [Mode 1] through [Mode 8]. Overwrite All Data takes about less than one hour in [Mode 1] at the minimum and about 9 hours in [Mode 8] at the maximum.

Mode	Description
Mode 1	Overwrites once with "0x00".
Mode 2	Overwrites with "random numbers" ▸▸ "random numbers" ▸▸ "0x00".
Mode 3	Overwrites with "0x00" ▸▸ "0xff" ▸▸ "random numbers" ▸▸ verifies.
Mode 4	Overwrites with "random numbers" ▸▸ "0x00" ▸▸ "0xff".
Mode 5	Overwrites with "0x00" ▸▸ "0xff" ▸▸ "0x00" ▸▸ "0xff".
Mode 6	Overwrites with "0x00" ▸▸ "0xff" ▸▸ "0x00" ▸▸ "0xff" ▸▸ "0x00" ▸▸ "0xff" ▸▸ "random numbers".
Mode 7	Overwrites with "0x00" ▸▸ "0xff" ▸▸ "0x00" ▸▸ "0xff" ▸▸ "0x00" ▸▸ "0xff" ▸▸ "0xaa".
Mode 8	Overwrites with "0x00" ▸▸ "0xff" ▸▸ "0x00" ▸▸ "0xff" ▸▸ "0x00" ▸▸ "0xff" ▸▸ "0xaa" ▸▸ verifies.

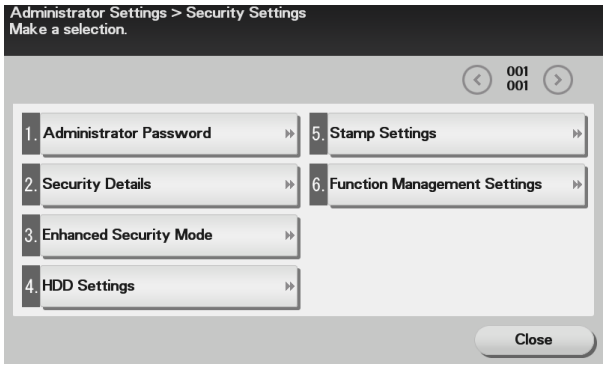
✔ For the procedure to call the Security Settings screen on the display, see steps 1 through 3 of page 2-10.

✔ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.

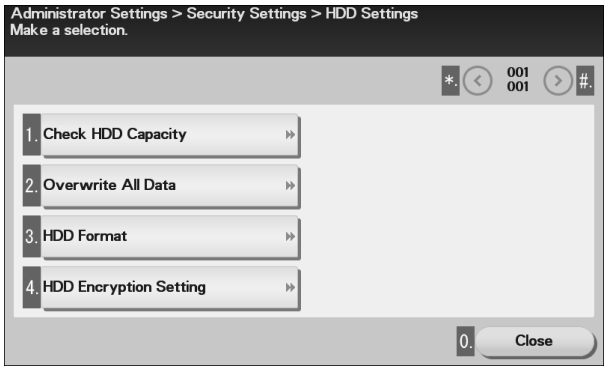
✔ For details of items that are cleared, see page 1-9.

1 Call the Security Settings screen on the display from the control panel.

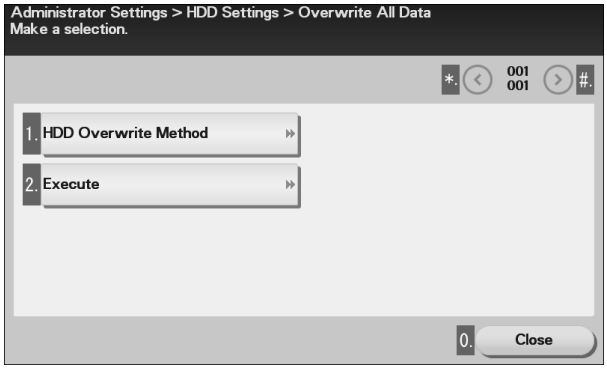
2 Touch [HDD Settings].



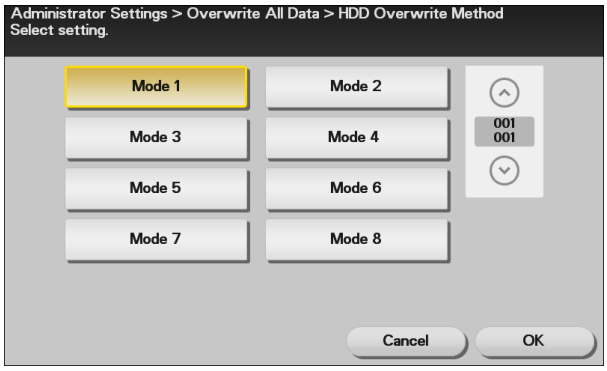
3 Touch [Overwrite All Data].



4 Touch [HDD Overwrite Method].

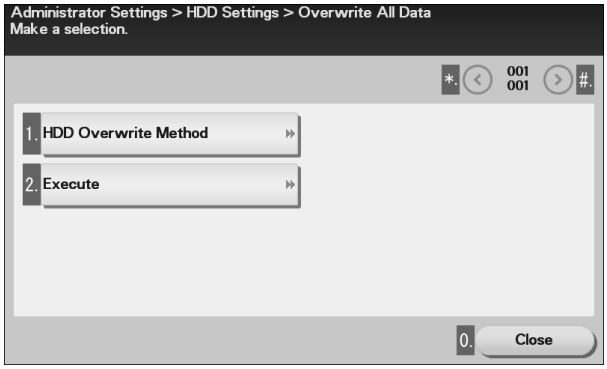


5 Select the desired mode.

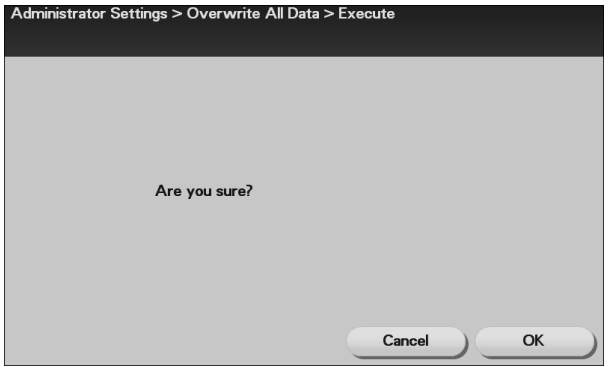


6 Touch [OK].

7 Touch [Execute].



8 A confirmation message appears. Touch [OK].



➔ Do not turn off the power switch of the machine during execution of Overwrite All Data. If the power switch is inadvertently turned off during the execution of Overwrite All Data and the machine, as a result, fails to recognize the HDD or develops other fault, contact your Service Representative.

2.7.2 Setting the Restore All

The memory area on the MFP board is initialized and reset to the default state.

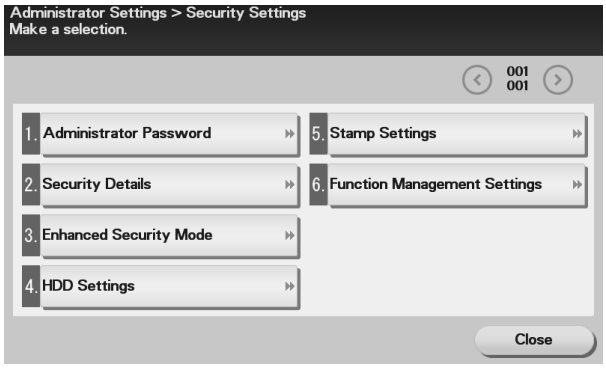
NOTICE

Perform "Restore All" from the control panel of the machine, and not via the network.

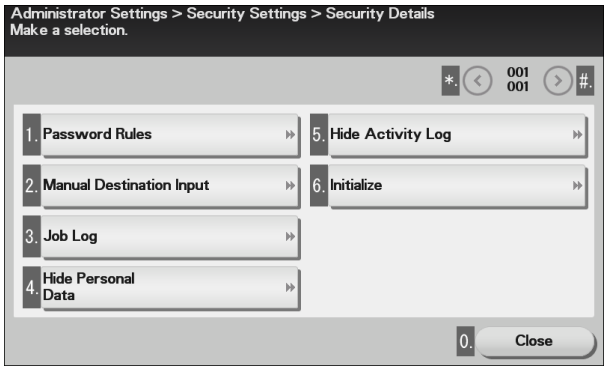
- ✔ For the procedure to call the Security Settings on the display, see steps 1 through 3 of page 2-10.
- ✔ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.
- ✔ For details of items that are cleared, see page 1-9.

1 Call the Security Settings on the display from the control panel.

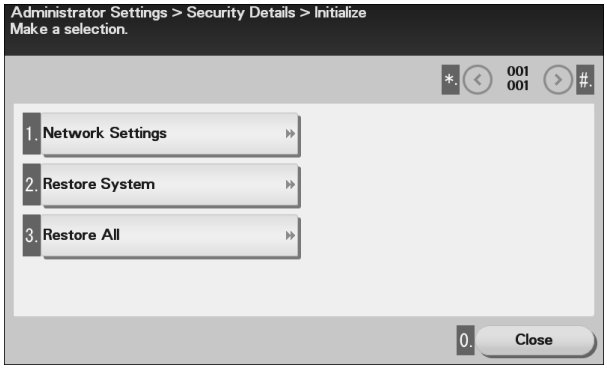
2 Touch [Security Details].



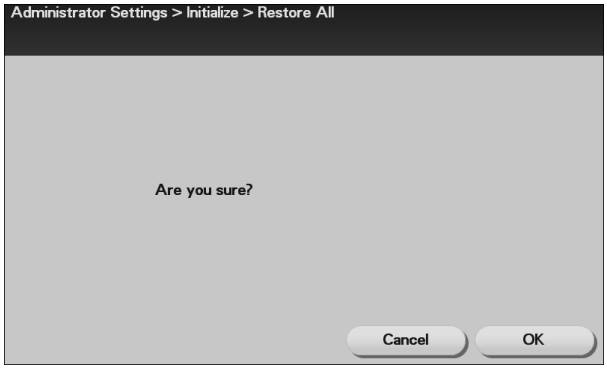
3 Touch [Initialize].



4 Touch [Restore All].



5 A confirmation message appears. Touch [OK].



➔ Do not turn off the power switch of the machine during execution of Restore All. If the power switch is inadvertently turned off during the execution of Restore All and the machine, as a result, develops a fault, contact your Service Representative.

2.8 S/MIME Communication Setting Function

When access to the machine by the administrator of the machine through the Administrator Settings is authenticated, the machine enables the setting of encryption of text of e-mail transmitted and received between the PC and the machine.

NOTICE

PageScope Web Connection cannot be used when the Enhanced Security Mode has been set to [ON]. To use the PageScope Web Connection, temporarily turn [OFF] the Enhanced Security Mode; then, from the control panel, select [Administrator Settings] ▸▸ [Network Settings] and select [Enable] for [HTTP Server Settings] and perform settings for the PageScope Web Connection.

After the PageScope Web Connection has been used, make necessary settings according to Installation Checklist and then turn [ON] the Enhanced Security Mode again. For details of settings made by the service engineer, contact your service representative.

To send S/MIME communications, it becomes necessary to register the certificate at the destination. Set 1024 bits or more for the key length of the RSA public key for the certificate of each destination.

Do not use any invalid certificate, as an increased risk results of data to be protected being tampered with or leaked.

2.8.1 Setting the S/MIME Communication

✔ For the procedure to access the Administrator Mode, see page 2-2.

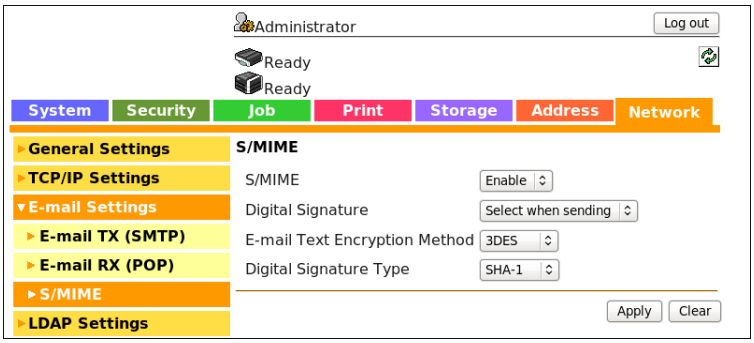
✔ Do not leave the machine with the Administrator Mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Mode.

1 Start PageScope Web Connection and access the Administrator Mode.

2 Click the [Network] tab.

3 Click [E-mail Setting] ▸▸ [S/MIME] from the menu.

4 Make the necessary settings.



➔ For encryption method, select the strong [3DES], [AES-128], [AES-192], or [AES-256]. If the mail software being used does not support AES, encrypted mail messages may be received, but they cannot be decrypted. Use AES-compliant mail software or select the encryption method that is the strongest of all compliant with the currently used mail software.

➔ Each encryption method represents the following.

Name	Encryption Algorithm	Encryption Key Length
[3DES]	3 key triple DES	168 bits
[AES-128]	AES	128 bits
[AES-192]	AES	192 bits
[AES-256]	AES	256 bits

5 Click [Apply].

2.8.2 Registering the certificate

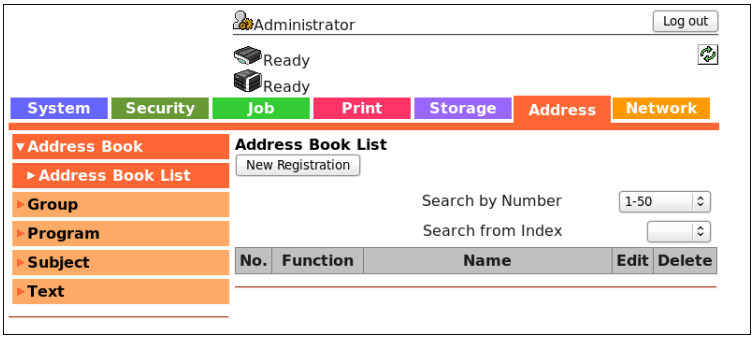
✔ For the procedure to access the Administrator Mode, see page 2-2.

✔ Do not leave the machine with the Administrator Mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Mode.

1 Start PageScope Web Connection and access the Administrator Mode.

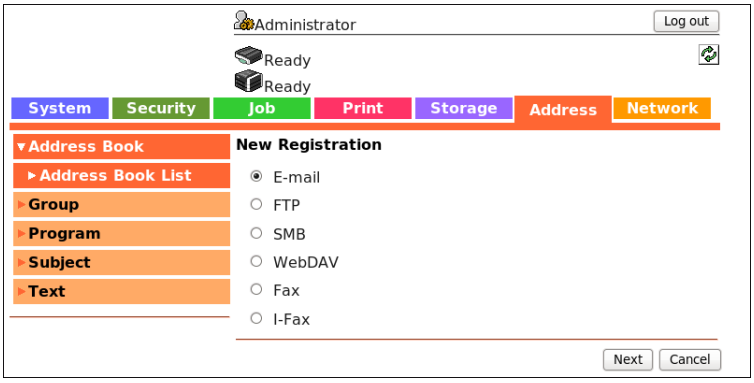
2 Click the [Address] tab.

3 Click [New Registration].

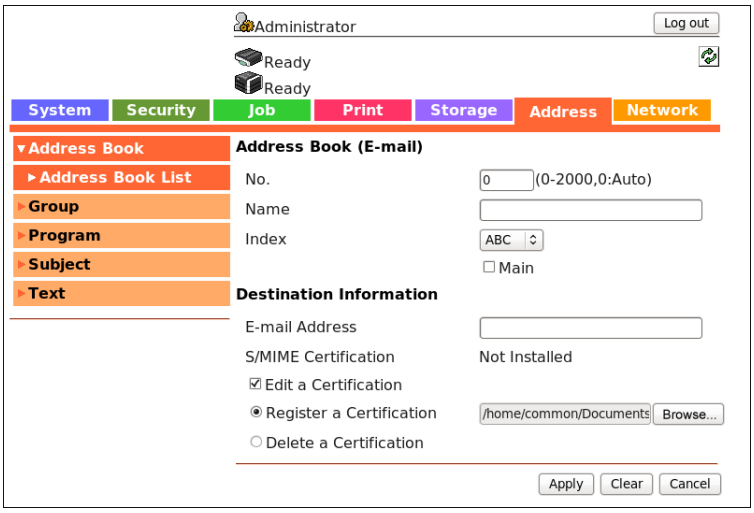


➔ To change the details of a previously registered destination, click [Edit].

4 Select [E-mail] and click [Next].



5 Click to select the [Edit a Certification] check box, and through [Browse], set the certification. If certification is to be deleted, select [Delete a Certification].



➔ Set 1024 bits or more for the key length of the RSA public key for the certificate of each destination.

6 Make the necessary settings.

➔ A number that already exists cannot be redundantly registered.

➔ Settings are all cleared if [Apply] is clicked with data entered for each item not meeting the requirements.

7 Click [Apply].

2.9 TCP/IP Setting Function

When access to the machine by the Administrator of the machine through the Administrator Settings is authenticated, the machine enables setting of the IP Address and registration of the DNS Server.

2.9.1 Setting the IP Address

✔ For the procedure to call the Administrator Settings on the display, see page 2-2.

✔ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.

1 Call the Administrator Settings on the display from the control panel.

2 Touch [Network Settings].

3 Touch [TCP/IP Setting].

4 Touch [IPv4 Settings].

5 Touch [IP Address].

6 Touch the [Value] field, and set the IP Address.

7 Touch [OK].

8 Touch [OK] and touch [Close].

2.9.2 Registering the DNS Server

NOTICE

PageScope Web Connection cannot be used when the Enhanced Security Mode has been set to [ON]. To use the PageScope Web Connection, temporarily turn [OFF] the Enhanced Security Mode; then, from the control panel, select [Administrator Settings] ►► [Network Settings] and select [Enable] for [HTTP Server Settings] and perform settings for the PageScope Web Connection.

After the PageScope Web Connection has been used, make necessary settings according to Installation Checklist and then turn [ON] the Enhanced Security Mode again. For details of settings made by the service engineer, contact your service representative.

✔ For the procedure to access the Administrator Mode, see page 2-2.

✔ Do not leave the machine with the Administrator Mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Mode.

1 Start PageScope Web Connection and access the Administrator Mode.

2 Click the [Network] tab and [DNS Settings] from [TCP/IP Settings] menu.

3 Enter the address in the DNS Server box.

4 Make the necessary settings.

5 Click [Apply].

2.10 E-Mail Setting Function

When access to the machine by the Administrator of the machine through the Administrator Settings is authenticated, the machine enables setting of the SMTP Server (E-Mail Server).

Setting the SMTP Server (E-Mail Server)

✔ For the procedure to call the Network Settings screen on the display, see steps 1 through 2 of page 2-31.

✔ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.

1 Call the Network Settings screen on the display from the control panel.

2 Touch [E-mail Settings].

3 Touch [E-Mail TX (SMTP)].

4 Touch [Enable] and touch [OK].

5 Touch [Close].

3 User Operations

3 User Operations

3.1 User Authentication Function

To authenticate a user before he or she actually uses the machine, user authentication is performed using the IC card and PIN code. The IC card reader installed in the machine is used to read the IC card. The PIN code entered is displayed as "*" during the authentication procedure.

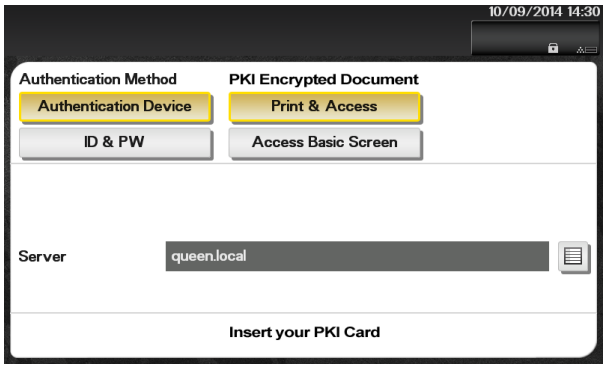
If a document is saved in the PKI Encrypted Document User Box of this machine, the print data of the user in question saved in the PKI Encrypted Document User Box of this machine can be automatically printed after the authentication by means of the IC card on the control panel is successful. Because printing occurs after user authentication is performed via the control panel of this machine, it is suitable for printing highly confidential documents.

User authentication using the IC card

✔ Contact the administrator of the machine if the server is not registered.

✔ Do not leave the machine while you are in the user operation mode. If it is absolutely necessary to leave the machine, be sure first to log off from the user operation mode.

1 Insert the IC card into the IC card reader connected to the machine.



➔ If any document is saved in the PKI Encrypted Document User Box, after selecting [Print & Access] or [Access Basic Screen], insert the IC card into the IC card reader.

Login Method	Description
[Print & Access]	The user operation mode screen is called to the screen after the PKI Encrypted document of the corresponding user is printed.
[Access Basic Screen]	Only the ordinary login procedure is applicable and no PKI Encrypted document are printed.

➔ If there are two or more PKI Encrypted documents are involved, all of them will be printed. To select and print only a specific document, select [Access Basic Screen] and select the specific document from those in the PKI Encrypted Document User Box. For the detailed procedure to access the PKI Encrypted document, see page 3-4.

2 Touch the [PIN Code] field.

3 From the keyboard, enter the PIN code registered in the IC card and touch [OK].

➔ Touch [C] to clear all characters.
➔ Touch [ ] to delete the last character entered.
➔ Touch [Shift] to show the upper case/symbol screen.
➔ Touch [Cancel] to go back to the screen shown in step 2.

4 Touch [OK].

➔ The PKI Encrypted Document is automatically deleted as soon as the printing is normally terminated.
➔ If a wrong PIN code is entered two or more consecutive times, the IC card is put into a locked state and becomes no longer valid for authentication. If the IC card is locked, contact the IC card administrator. This machine is not useful for unlocking the IC card.
➔ If the IC card is locked, a message appears that tells that the IC card cannot be used. Contact the IC card administrator.
➔ The number of consecutive failure count for the locking depends on the setting made on the IC card side.
➔ If authentication fails, the permissible authentication failure count appears.

5 To log off, pull out the IC card from the IC card reader.

➔ Do not leave the machine with the IC card inserted in the card reader.

3.2 Encrypted Document Function

This function is used when a document encrypted by the dedicated printer driver and IC card from the PC side is saved in the machine. The PKI encrypted document saved in the machine can be decrypted only by an encrypted IC card, which makes this function just right for printing highly confidential documents.

Accessing the Encrypted document

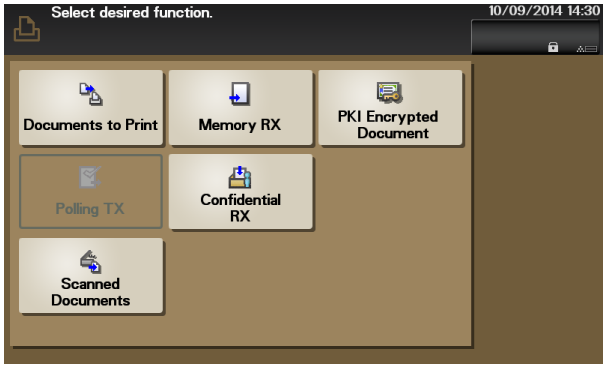
✔ For the logon procedure, see page 3-2.

✔ Do not leave the machine while you are in the user operation mode. If it is absolutely necessary to leave the machine, be sure first to log off from the user operation mode.

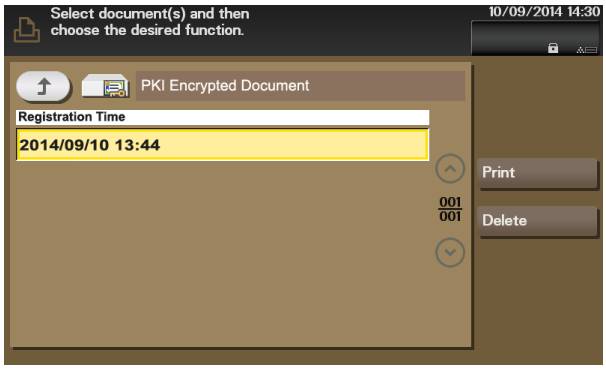
1 Using the IC card, log on to the machine.

2 Touch [Document Print/Delete].

3 Touch [PKI Encrypted Document].



4 Select the desired PKI Encrypted Document and touch [Print].



➔ The PKI Encrypted Document is automatically deleted as soon as the printing is normally terminated.

➔ To delete PKI Encrypted Document, select the specific document and touch [Delete].

3.3 Scan to Me Function

The machine allows all users who have been authenticated with the IC card to operate the Scan to Me function.

Scan to Me encrypts the image file scanned by the user on this machine using the IC card and transmits it as a mail data file of S/MIME to the mail address of the IC card user.

NOTICE

When using this function, be sure to transmit data using Digital Signature.

Scan to Me procedure

✔ For the logon procedure, see page 3-2.

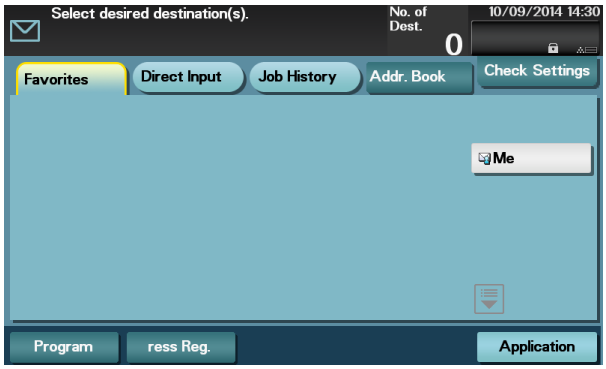
✔ Do not leave the machine while you are in the user operation mode. If it is absolutely necessary to leave the machine, be sure first to log off from the user operation mode.

1 Using the IC card, log on to the machine.

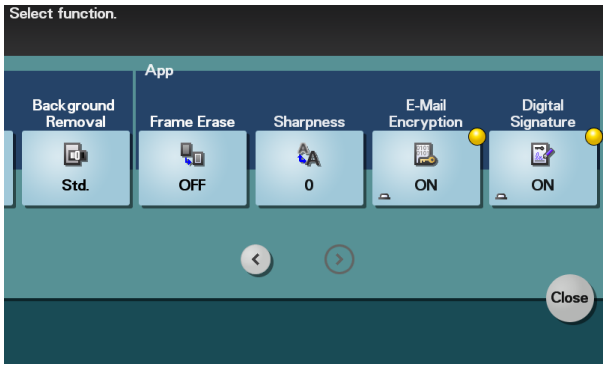
2 Load the original.

3 Touch [Scan to E-mail].

4 Touch [Application].



5 Select [E-Mail Encryption] and [Digital Signature].



6 Touch [Close].

7 Touch [Me].

8 Touch [Start].

➔ Do not pull out the IC card until the e-mail transmission is completed. The transmission file is discarded if the IC card is pulled out during transmission.

KONICA MINOLTA

http://konicaminolta.com

A6F7-9572B-00