KONICA MINOLTA

Giving Shape to Ideas

bizhub

554e/454e/364e/284e/224e

for PKI Card System

User's Guide

Security Operations

2014. 2
Ver. 1.01

Contents

1 Security

2 Administrator Operations

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 554e/454e/364e/284e/224e 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. 1.01) describes bizhub 554e/bizhub 454e/bizhub 364e/bizhub 284e/bizhub 224e PKI Card System Control Software (MFP Controller: A61F0Y0-0100-G00-09pki).

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 554e/454e/364e/284e/224e 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 exit from the current mode to return to the basic screen whenever the access to that mode is completed or if he or she leaves the machine with the mode screen left displayed.

The administrator of the machine should make sure that each individual general user exits from the current mode to return to the basic screen whenever the access to that mode is completed or if the user leaves the machine 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.

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.	Completed
	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 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 (MFP Controller, CheckSum) indicated in the Service Manual matches the values shown in the Firmware Version screen. If there is a mismatch in the Firmware version number, explain to the administrator of the machine that upgrading of the Firmware is necessary and perform upgrading of the Firmware.	□
	Set the CE Password.	□
	Make the service settings necessary for the Enhanced Security Mode.	□
	Check that the SSD mounted on the machine is the type for the exclusive use for this machine.	□
	Check that the Fax Kit has been mounted and set up properly, if fax functions are to be used.	□
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 has been set by the administrator of the machine.	□
	Let the administrator of the machine set Enhanced Security Mode to [ON].	□
	The language, in which the contents of the User's Guide Security Operations have been evaluated, is English. Explain the way how to get the manual in the language, in which it is evaluated.	□
	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 2-10.

A password that can be set must 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 is entered, during password authentication, a predetermined number of times (once to three times) or more set by the administrator of the machine, 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.

By setting the Encryption Key, the data saved in the HDD is encrypted, thereby protecting the data in the HDD. Note, however, that the Encryption Key does not prevent the HDD from being physically removed. Make sure of a good operation control.

When the machine is to be discarded or use of a leased machine is terminated at the end of the leasing contract, the Overwrite All Data 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 and the SSD board to factory settings, preventing data from leaking. For details of the Overwrite All Data function, see page 2-27. For details of items to be cleared by Overwrite All Data 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 by the Enhanced Security Mode.

<Administrator Settings>

- Authentication of Administrator Settings is successful.

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 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 using an SMTP server (mail server) or an DNS server, each server should be appropriately managed by the administrator and should be periodically checked to confirm that settings have not been 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.

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.

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 should control the operation of the machine by setting an appropriate value for the Ticket Hold Time Setting.
  – To set the Ticket Hold Time Setting, touch [Utility] - [Administrator Settings] - [User Authentication/Account Track] - [General Settings] - [↓] - [Ticket Hold Time Setting] on the MFP control panel.
- The administrator of the machine should control the operation of the machine with the TCP Socket (ASCII Mode) setting disabled.
  – To change the TCP Socket (ASCII Mode) setting, select from the control panel of the MFP [Utility] - [Administrator Settings] - [Network Settings] - [Forward (2/3)] - [TCP Socket Settings] and then set [TCP Socket (ASCII Mode)] to [OFF].
- The administrator of the machine should control the operation of the machine without using the following setting.
  – From the control panel of the MFP, select [Utility] - [Administrator Settings] - [Network Settings] - [SMB Settings] and then set [SMB Server Settings] to [OFF].
  – From the control panel of the MFP, select [Utility] - [Administrator Settings] - [Network Settings] - [SMB Settings] and then set [WINS/NetBIOS Settings] to [OFF].
  – From the control panel of the MFP, select [Utility] - [Administrator Settings] - [Network Settings] - [SMB Settings] and then set [Direct Hosting Setting] 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. 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 rear right 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.

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 and Encryption Key. For the Administrator Password and Encryption Key, the same password as that currently set is not accepted.

Study the following table for more details of the number and types of characters that can be used for each password. For details of the settings of the Password Rules, see page 2-8.

Types of passwords	Number of characters	Types of characters
Administrator Password	8 to 64 characters*	• Numeric characters: 0 to 9 • Alpha characters: upper and lower case letters • Symbols: !, #, $, %, &, ', (,), *, ,, -, ., /, :, ;, <, =, >, ?, @, [, \,], ^, _, `, {, |, }, ~, + • Special characters (68 characters) Selectable from among a total of 161 characters
Encryption Key	20 characters	• Numeric characters: 0 to 9 • Alpha characters: upper and lower case letters • Symbols: !, #, $, %, &, ', *, +, -, ., /, =, <, @, ^, _, `, {, |, }, ~ Selectable from among a total of 83 characters

*: 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 Overwrite All Data Function

The Overwrite All Data function clears the following items of data.

Items of Data Cleared	Description
Password Rules	Sets [Invalid] and disables [Set Minimum Password Length]
Encrypted document	Deletes all Encrypted document saved in Encrypted document User Box
Scanned image files	Deletes all Scanned image files
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
Encryption Key	Clears the currently set Encryption Key
Administrator Password	Clears the currently set password, resetting it to the factory setting (1234567812345678)
S/MIME certificate	Deletes the currently set S/MIME certificate
External Server	Deletes the currently set external server
Loadable driver	Deletes the currently set loadable driver
Daylight Saving Time	Set to [No]
Time Adjustment Setting (NTP)	Set to [OFF]

Items of Data Cleared	Description
Time/date data	Varies corrected data, if the time-of-day data is corrected due to, for example, the daylight saving time

Fax functions

An optional Fax Kit is required for using fax functions. Contact your Service Representative.

General functions and operations

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

2 Administrator Operations

2 Administrator Operations

2.1 Accessing the Administrator Settings

In Administrator Settings, the settings for the machine system and network can be registered or changed.

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.

When the Enhanced Security Mode is set to [ON], the number of times in which authentication fails is counted.

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

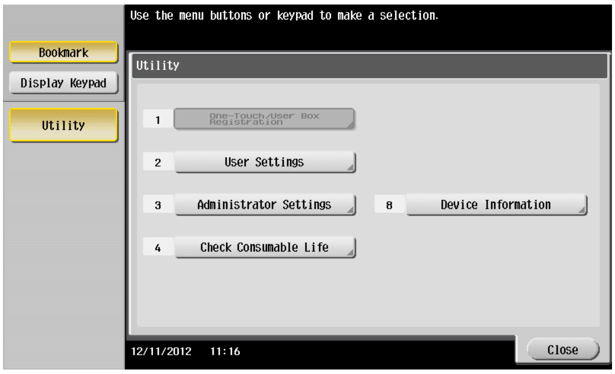
The machine does not accept access to the Administrator Settings under any of the following conditions. Wait for some while before attempting to gain access to the Administrator Settings again.

- The Administrator Settings has been logged on to through access made from the PC.
- A remote operation is being performed from an application on the PC.
- 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 main power switch has been turned ON.
- A malfunction code is displayed on the machine.

✔ 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.

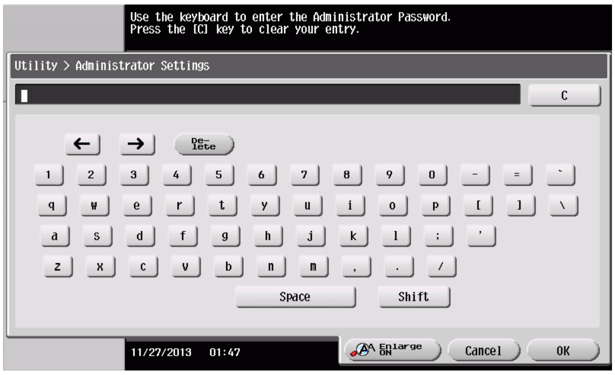
1 Touch [Menu] ▸▸ [Utility].

2 Touch [Administrator Settings].



Use the menu buttons or keypad to make a selection.

3 Enter the Administrator Password from the keyboard.



Use the keyboard to enter the Administrator Password.
Press the [C] key to clear your entry.

Utility > Administrator Settings

- ➔ Touch [C] to clear all characters.
- ➔ Touch [Delete] 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.
- ➔ If the Enhanced Security Mode is set to [ON], entry of a wrong password is counted as unauthorized access. If a wrong Administrator Password is entered a predetermined number of times (once to three times) or more set by the administrator of the machine, a message appears saying that the machine accepts no more Administrator Passwords because of unauthorized access for any subsequent entry of the Administrator Password. The machine is then set into an access lock state.
  To cancel the access lock state, settings must be made by the Service Engineer; or, turn off, and then turn on, the main power switch of the machine. If the main power switch is turned off and on, the access lock state is canceled after the lapse of time set for [Release Time Settings]. When the main power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. If there is no wait period between turning the main power switch off, then on again, the machine may not function properly.
  Here is the sequence, through which the main power switch and sub power key are turned on and off:
  Turn off the sub power key ►► Turn off the main power switch ►► Turn on the main power switch ►► Turn on the sub power key

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

2.1.2 Accessing the User Mode

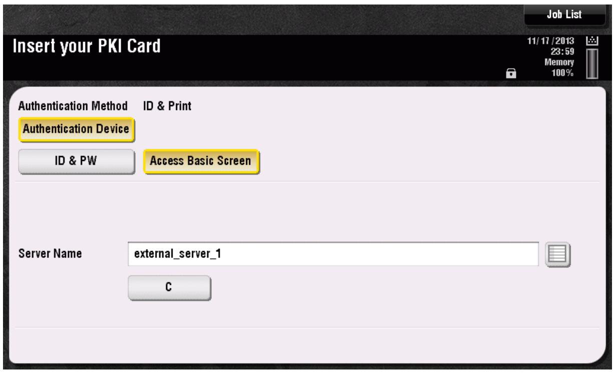
You can log on to the User Mode as an administrator. In the User Mode, you can check or delete a job, which is disabled in Administrator Settings.

Reference

- The authority relating to box settings is the same as that of 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].



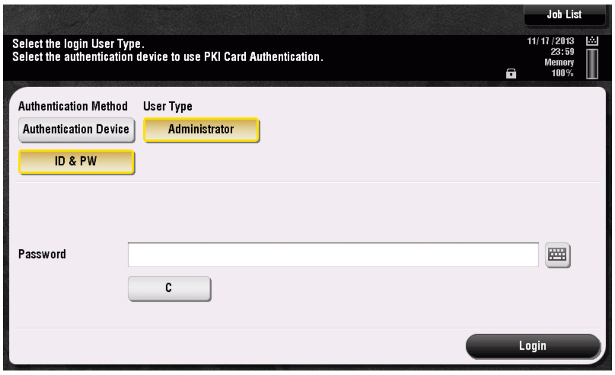
Insert your PKI Card

Authentication Method: Authentication Device

ID & Print: Access Basic Screen

Server Name: external_server_1

2 Touch the keyboard icon in the [User Name] field.



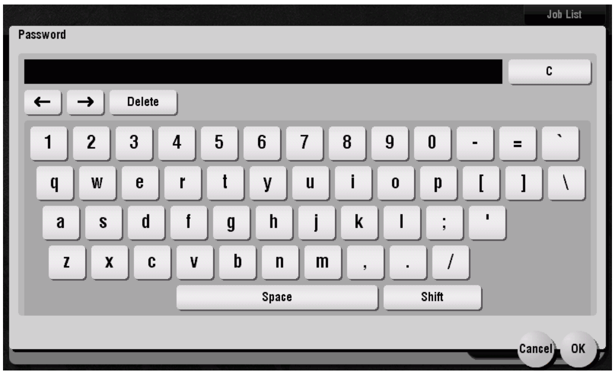
Select the login User Type.
Select the authentication device to use PKI Card Authentication.

Authentication Method: ID & PW

User Type: Administrator

Password

3 Enter the Administrator Password from the keyboard.



➔ Touch [C] to clear all characters

➔ Touch [Delete] 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 authentication has failed appears. Enter the correct Administrator Password.

➔ If the Enhanced Security Mode is set to [ON], entry of a wrong password is counted as unauthorized access. If a wrong Administrator Password is entered a predetermined number of times (once to three times) or more set by the administrator of the machine, a message appears saying that the machine accepts no more Administrator Passwords because of unauthorized access for any subsequent entry of the Administrator Password. The machine is then set into an access lock state.
To cancel the access lock state, settings must be made by the Service Engineer; or, turn off, and then turn on, the main power switch of the machine. If the main power switch is turned off and on, the access lock state is canceled after the lapse of time set for [Release Time Settings]. When the main power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. If there is no wait period between turning the main power switch off, then on again, the machine may not function properly.
Here is the sequence, through which the main power switch and sub power key are turned on and off:
Turn off the sub power key ▸▸ Turn off the main power switch ▸▸ Turn on the main power switch ▸▸ Turn on the sub power key

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. If the Enhanced Security Mode is set to [ON], a count is taken of the number of unauthorized accesses to the Administrator Settings. A function is also set that determines whether Administrator Password meets predetermined requirements. The security function is thus enhanced in the Enhanced Security Mode.

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

NOTICE

First, set the Encryption Key. To set the Encryption Key, HDD Format must first be executed. Execution of the HDD Format clears various setting values. For details of items that are cleared by HDD Format, see page 2-7.

If initialization is executed by the Service Engineer, the Password Rules are set to [Invalid] and the Administrator Password is reset to the factory setting (1234567812345678). To set the Administrator Password and turn [ON] the Enhanced Security Mode again.

Settings to be Made in Advance	Description
Administrator Password	Meet the Password Rules. The factory setting is "1234567812345678."
Encryption Key	Set the Encryption Key.
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.

NOTICE

If an attempt is made to change a setting that has been changed as a result of setting the Enhanced Security Mode to [ON], a screen may appear indicating that the Enhanced Security Mode is to be canceled. Note that executing this screen will cancel the Enhanced Security Mode.

The description "not to be changed" given in parentheses in the table below indicates that the specific setting cannot be changed with the Enhanced Security Mode set to [ON].

Function Name	Factory Setting	When Enhanced Security Mode is set to [ON]
Password Rules	Invalid	Enable (not to be changed) If [Enable] is set for Password Rules, the types and number of characters to be used for each password are limited. For details of the Password Rules, see page 1-9.
Prohibited Functions When Authentication Error	Mode 1	Mode 2 (not to be changed): Three times is set. * The number of times can be changed to once, twice, or three times.
Release Time settings	5 min.	The setting value should be 5 min. or more (no value less than 5 can be set)
Public User Access	Restrict	Restrict (not to be changed)
User Box Administrator Setting	Restrict	Restrict (not to be changed)
S/MIME Encryption Method	3DES	3DES (not to be changed to DES or RC-2)
FTP Server	ON	OFF (not to be changed)
SNMPv1/v2c Settings	Read setting: Enable Write setting: Invalid	Read setting: Enable, Write setting: Invalid (not to be changed)
SNMP v3 Settings	Restrict	Restrict (not to be changed)
Print Data Capture	Allow	Restrict (not to be changed)

Function Name	Factory Setting	When Enhanced Security Mode is set to [ON]
Registering and Changing Address by the user (Address Book and Program)	Allow	Restrict (not to be changed)
Initialize (Network Settings)	Enabled	Restrict (not to be changed)
Image Log Transfer Settings	OFF	OFF (not to be changed)
Remote Panel Settings (Server Settings/Client Settings)	OFF	OFF (not to be changed)
PSWC Settings	OFF	OFF (not to be changed)
OpenAPI Access Setting	Restrict	Restrict (not to be changed)
TCP Socket Settings	OFF	OFF (not to be changed)
Machine Update Settings	OFF	OFF (not to be changed)
IWS Settings	OFF	OFF (not to be changed)
HDD backup data Settings	Restrict	Restrict (not to be changed)

2.2.1 Items cleared by HDD Format

Following are the items that are cleared by HDD Format.

Whenever HDD Format is executed, be sure to set the Enhanced Security Mode to [ON] again.

Items of Data Cleared	Description
Enhanced Security Mode	Set to [OFF]
Encrypted document	Deletes all Encrypted document saved in Encrypted document User Box
External server	Deletes the external server
S/MIME certificate	Deletes the currently set S/MIME certificate

2.2.2 Setting the Password Rules

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

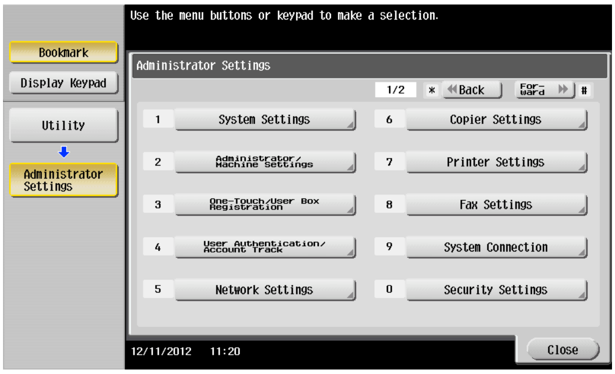
✔ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.

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.

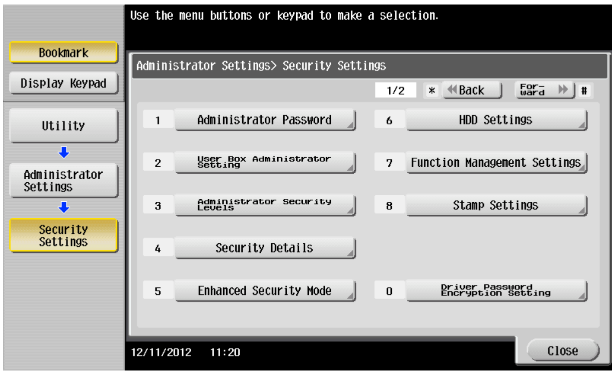
2 Touch [Security Settings].



Use the menu buttons or keypad to make a selection.

Administrator Settings

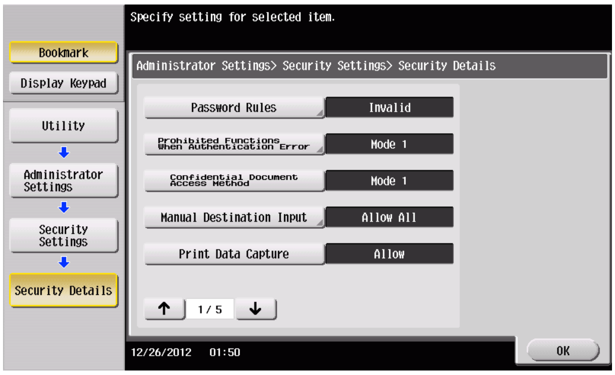
3 Touch [Security Details].



Use the menu buttons or keypad to make a selection.

Administrator Settings> Security Settings

4 Touch [Password Rules].



Specify setting for selected item.

Administrator Settings> Security Settings> Security Details

Password Rules: Invalid

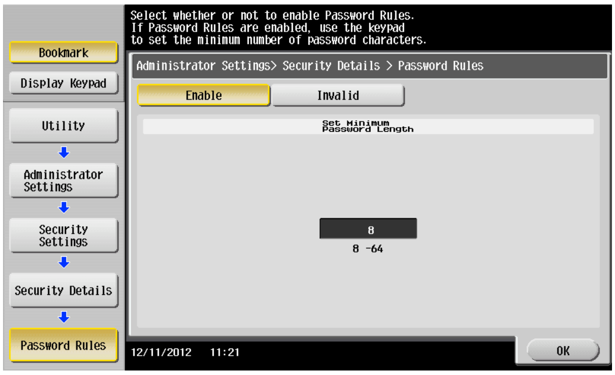
Prohibited Functions When Authentication Error: Mode 1

Confidential Document Access Method: Mode 1

Manual Destination Input: Allow All

Print Data Capture: Allow

5 Select [Enable] and set [Set Minimum Password Length] (8 to 64 characters).



Select whether or not to enable Password Rules.
If Password Rules are enabled, use the keypad
to set the minimum number of password characters.

Administrator Settings> Security Details > Password Rules

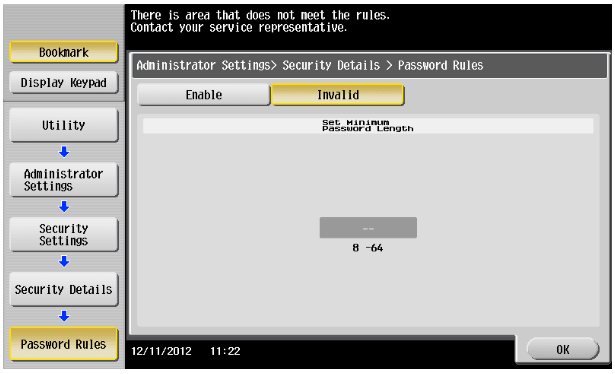
Set Minimum Password Length

8

8 -64

12/11/2012 11:21

➔ The following screen appears if the previously required settings are yet to be made by the Service Engineer. Contact your Service Representative.



There is area that does not meet the rules.
Contact your service representative.

Administrator Settings> Security Details > Password Rules

Set Minimum Password Length

--

8 -64

12/11/2012 11:22

6 Touch [OK].

2.2.3 Setting the Enhanced Security Mode

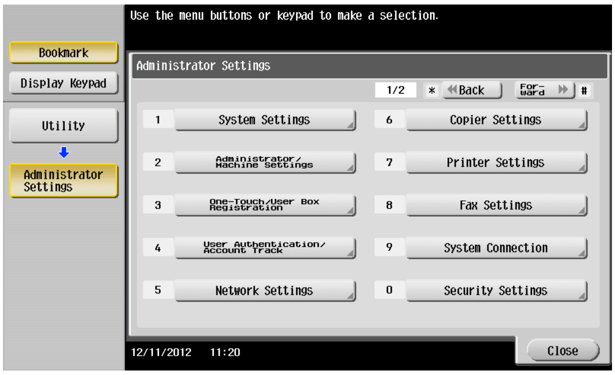
✔ For the procedure to call the Administrator Settings on the display, see page 2-2.

✔ 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 [Security Settings].

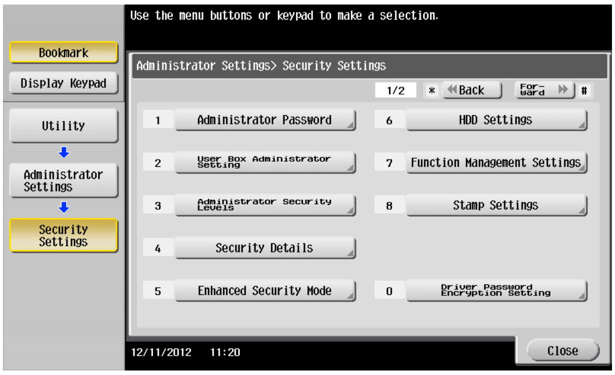


Use the menu buttons or keypad to make a selection.

Administrator Settings

12/11/2012 11:20

3 Touch [Enhanced Security Mode].

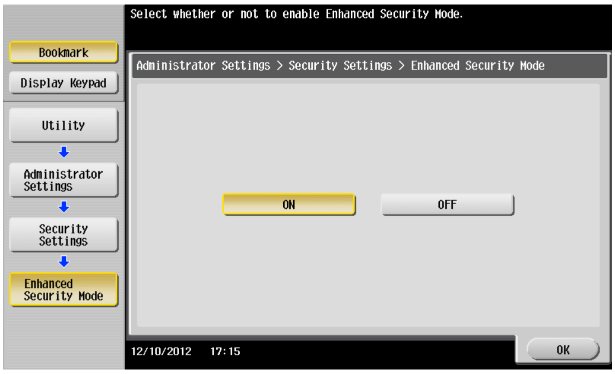


Use the menu buttons or keypad to make a selection.

Administrator Settings> Security Settings

12/11/2012 11:20

4 Select [ON] to enable the Enhanced Security Mode and touch [OK].

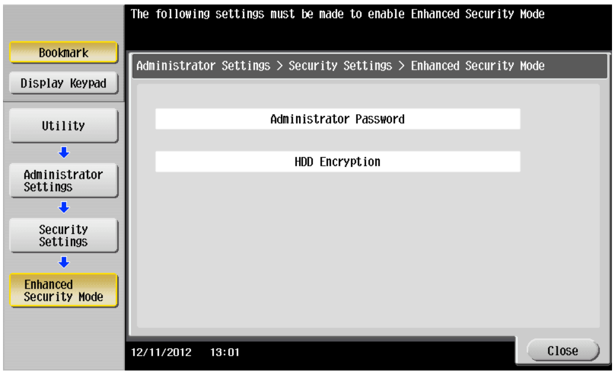


Select whether or not to enable Enhanced Security Mode.

Administrator Settings > Security Settings > Enhanced Security Mode

12/10/2012 17:15

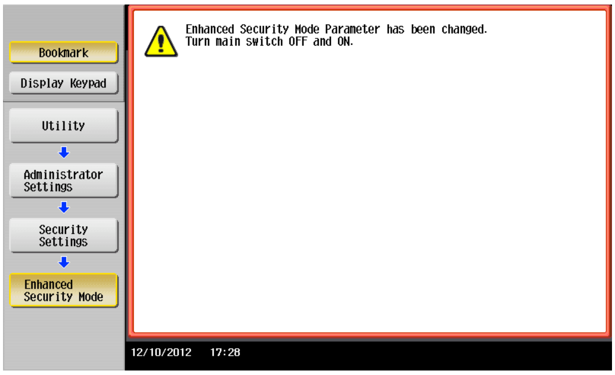
➔ The following screen appears if the previously required settings are yet to be made by the administrator of the machine. Make the necessary settings according to the corresponding set procedure.



The following settings must be made to enable Enhanced Security Mode

Administrator Settings > Security Settings > Enhanced Security Mode

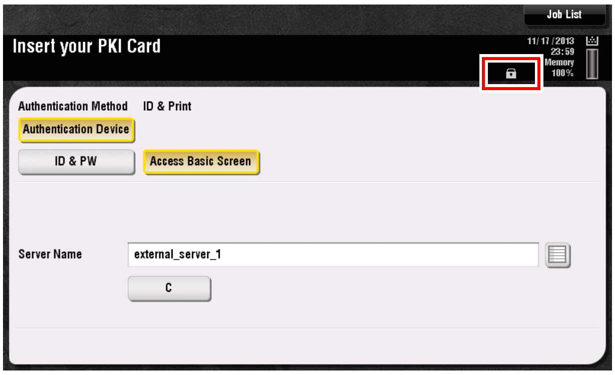
5 Make sure that a message appears prompting you to turn OFF and then ON the main power switch. Now, turn OFF and then turn ON the main power switch.



Enhanced Security Mode Parameter has been changed.
Turn main switch OFF and ON.

➔ When the main power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. if there is no wait period between turning the main power switch off, then on again, the machine may not function properly.
Here is the sequence, through which the main power switch and sub power key are turned on and off:
Turn off the sub power key ►► Turn off the main power switch ►► Turn on the main power switch ►► Turn on the sub power key

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



Insert your PKI Card

Authentication Method ID & Print

Server Name external_server_1

2.3 Preventing Unauthorized Access

When access to the machine by the administrator of the machine through the Administrator Settings is authenticated, the machine enables setting of the operation of Prohibited Functions When Authentication Error. The machine then takes a count of the number of unsuccessful accesses to the Administrator Settings to prohibit the authentication operation.

Either [Mode 1] or [Mode 2] can be selected for Prohibited Functions When Authentication Error. The factory setting is [Mode 1]. If the Enhanced Security Mode is set to [ON], the setting is changed to [Mode 2] (check count: three times). It is nonetheless possible to change the check count to select from among once, twice, or three times.
If [Mode 2] is selected, the Release Time Settings function is enabled. When the Administrator Settings is set into the access lock state, the main power switch is turned off and on and, after the lapse of a predetermined period of time after the machine is turned on again, the access lock state of the Administrator Settings is canceled. The Release Time Settings function allows the period of time, after the lapse of which the access lock state of the Administrator Settings is canceled, to be set in the range between 1 and 60 min. The factory setting is 5 min. For details of each mode, see the table below.

Mode	Description
Mode 1	If authentication fails, the authentication operation (entry of the password) is prohibited for 5 sec.
Mode 2	If authentication fails, the authentication operation (entry of the password) is prohibited for 5 sec. The number of times, in which authentication fails, is also counted and, when the failure count reaches a predetermined value, the authentication operation is prohibited and the machine is set into an access lock state.

NOTICE
If the access lock state of the Administrator Settings is canceled by the Service Engineer, the setting of the Release Time Settings function is not applied.

Making any of the following settings when the Enhanced Security Mode is set to [ON] will cancel the Enhanced Security Mode.

- Changing [Prohibited Functions When Authentication Error] to [Mode 1]
- Changing the check count for [Prohibited Functions When Authentication Error] to four times or more
- Setting [Release Time Settings] to 1 to 4 min.

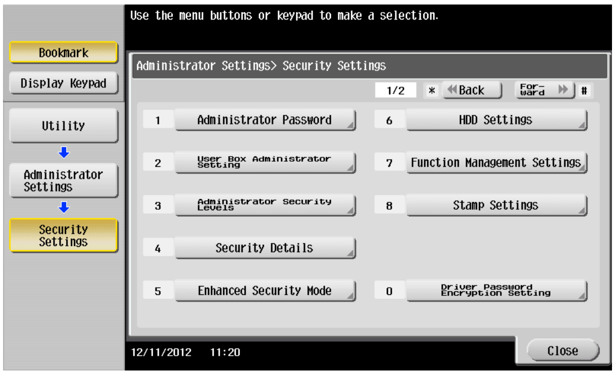
Setting Prohibited Functions When Authentication Error

✔ For the procedure to call the Security Settings screen on the display, see steps 1 and 2 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.

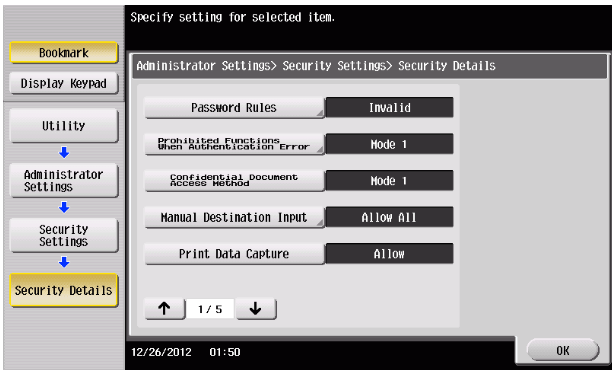
2 Touch [Security Details].



Use the menu buttons or keypad to make a selection.

Administrator Settings> Security Settings

3 Touch [Prohibited Functions When Authentication Error].



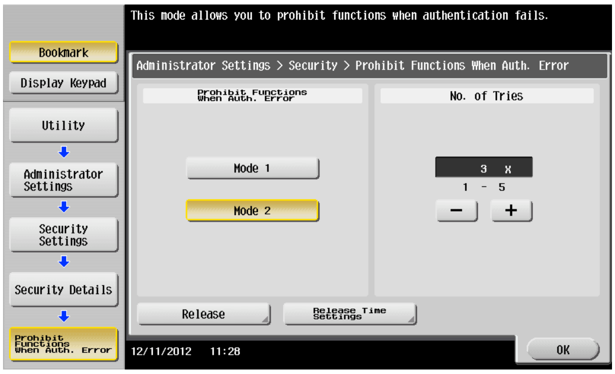
Specify setting for selected item.

Administrator Settings> Security Settings> Security Details

Password Rules	Invalid
Prohibited Functions When Authentication Error	Mode 1
Confidential Document Access Method	Mode 1
Manual Destination Input	Allow All
Print Data Capture	Allow

12/26/2012 01:50

4 Touch [Mode 2].



This mode allows you to prohibit functions when authentication fails.

Administrator Settings > Security > Prohibit Functions When Auth. Error

Prohibit Functions When Auth. Error: Mode 2

No. of Tries: 3 x (1 - 5)

12/11/2012 11:28

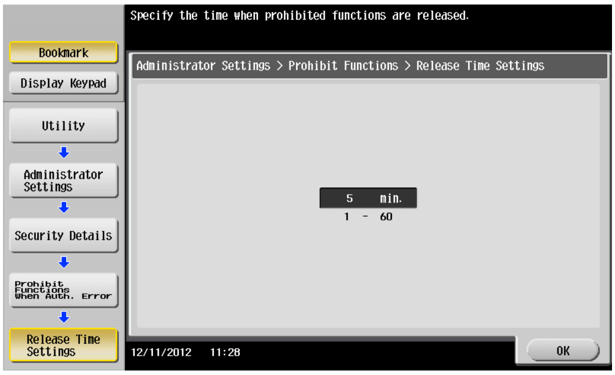
➔ Select [Mode 2] when the Enhanced Security Mode is set to [ON]. Selecting [Mode 1] will cancel the Enhanced Security Mode.

➔ Set three times or less when the Enhanced Security Mode is set to [ON]. Setting four times or more will cancel the Enhanced Security Mode.

➔ To change the check count, touch [+] to increase the count or [-] to decrease it.

5 Touch [Release Time Settings].

6 Touch [C] and, from the keypad, enter the time, after the lapse of which the access lock state of the Administrator Settings is canceled.



Specify the time when prohibited functions are released.

Administrator Settings > Prohibit Functions > Release Time Settings

5 min. (1 - 60)

12/11/2012 11:28

➔ Touch [Display Keypad] to display the keypad.

➔ Release Time can be set to any value between 1 min. and 60 min. in 1-min. increments. An input data error message appears when any value falling outside the range of 1 to 60 min. is set. Enter the correct Release Time.

➔ Set 5 min. or more when the Enhanced Security Mode is set to [ON]. Setting 1 to 4 min. will cancel the Enhanced Security Mode.

7 Touch [OK].

2.4 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.

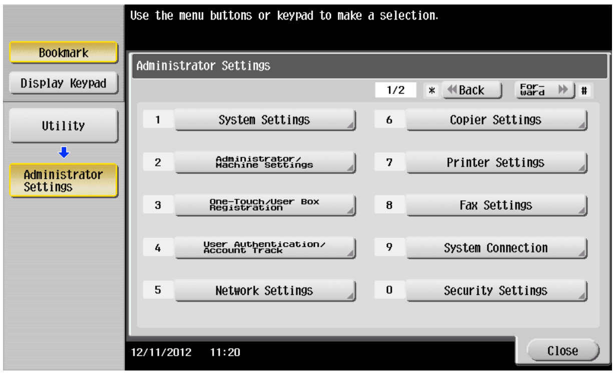
Setting the External Server

✔ 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 [User Authentication/Account Track].

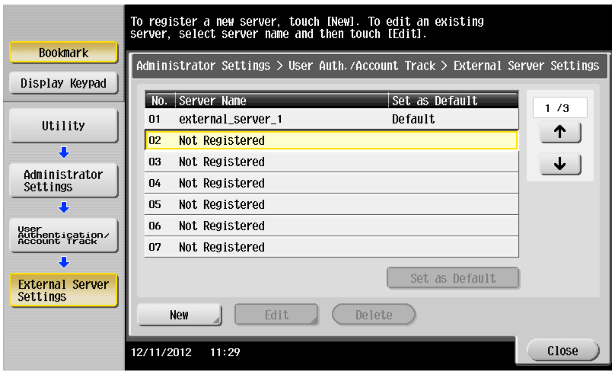


Use the menu buttons or keypad to make a selection.

3 Touch [External Sever Settings].

4 Touch the specific Sever Registration key, in which no sever has been registered.

5 Touch [New].



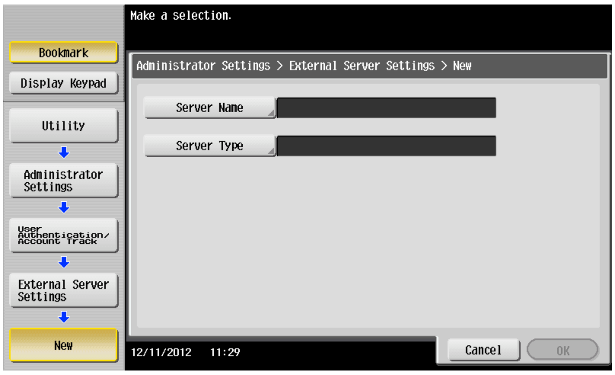
To register a new server, touch [New]. To edit an existing server, select server name and then touch [Edit].

Administrator Settings > User Auth./Account Track > External Server Settings

No.	Server Name	Set as Default
01	external_server_1	Default
02	Not Registered	
03	Not Registered	
04	Not Registered	
05	Not Registered	
06	Not Registered	
07	Not Registered	

➔ To change or delete a previously registered server, touch [Edit] or [Delete].

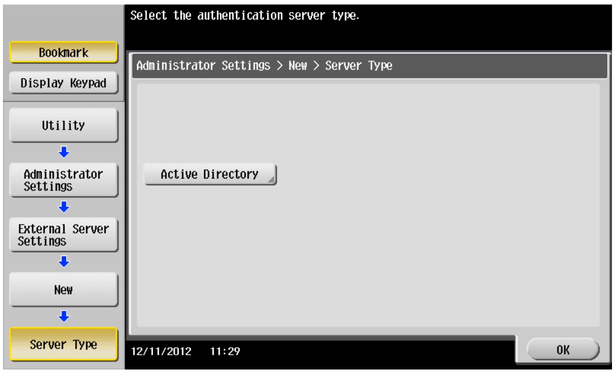
6 Touch [Server Type].



Make a selection.

Administrator Settings > External Server Settings > New

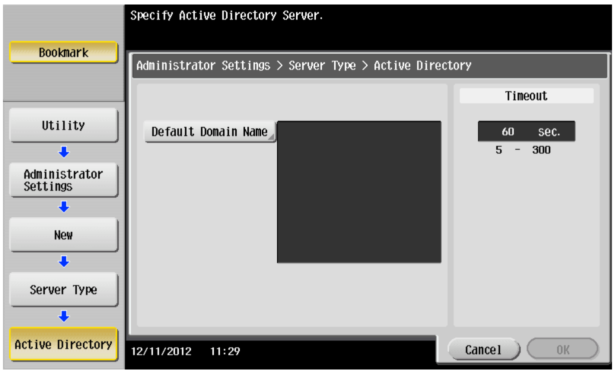
7 Touch [Active Directory].



Select the authentication server type.

Administrator Settings > New > Server Type

8 Touch [Default Domain Name].

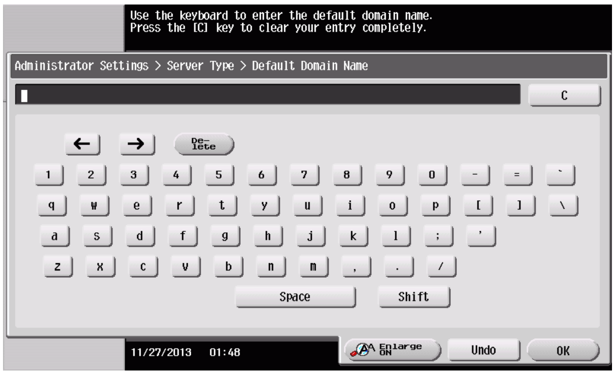


Specify Active Directory Server.

Administrator Settings > Server Type > Active Directory

Timeout 60 sec. 5 - 300

9 From the keyboard, enter the Domain Name and touch [OK].

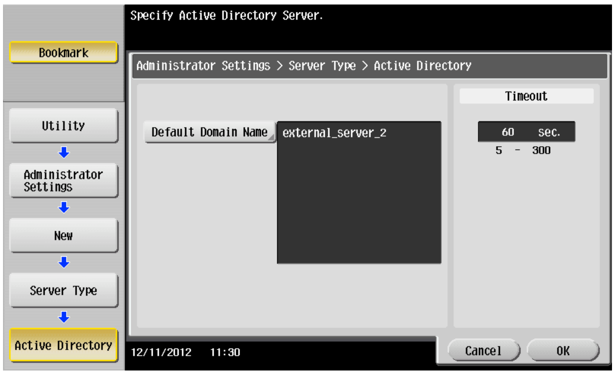


Use the keyboard to enter the default domain name.
Press the [C] key to clear your entry completely.

Administrator Settings > Server Type > Default Domain Name

➔ Touch [C] or touch [Undo] to clear the value entered last.
➔ Touch [Delete] to delete the last character entered.
➔ Touch [Shift] to show the upper case/symbol screen.

10 Touch [OK].



Specify Active Directory Server.

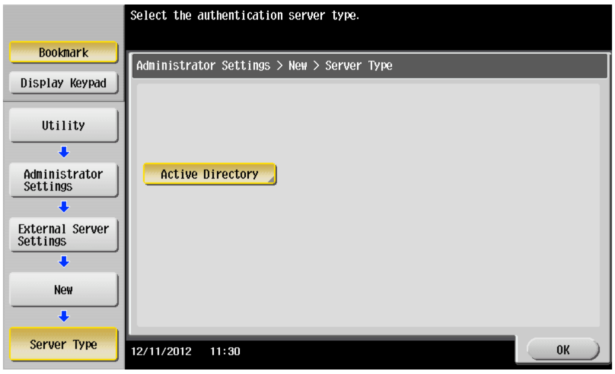
Administrator Settings > Server Type > Active Directory

Default Domain Name: external_server_2

Timeout: 60 sec. (5 - 300)

12/11/2012 11:30

11 Touch [OK].



Select the authentication server type.

Administrator Settings > New > Server Type

12/11/2012 11:30

12 Make the necessary settings.

➔ If the Sever Name is yet to be entered, [OK] cannot be touched. Be sure to enter the Sever Name.

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

13 Touch [OK].

14 Touch [Close].

➔ If two or more external servers have been registered, select any desired server and touch [Set as Default].

2.5 System Auto Reset Function

When access to the machine by the administrator of the machine through the Administrator Settings 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.

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.

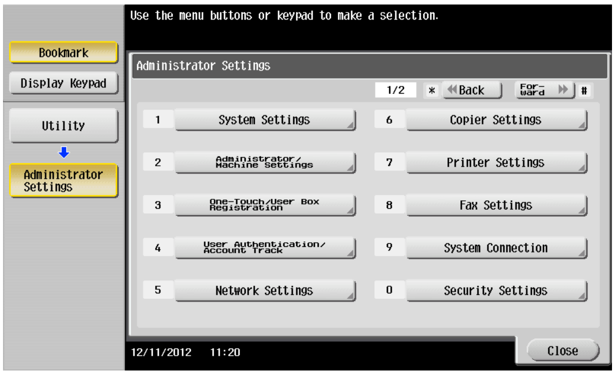
Setting the System Auto Reset function

✔ 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.

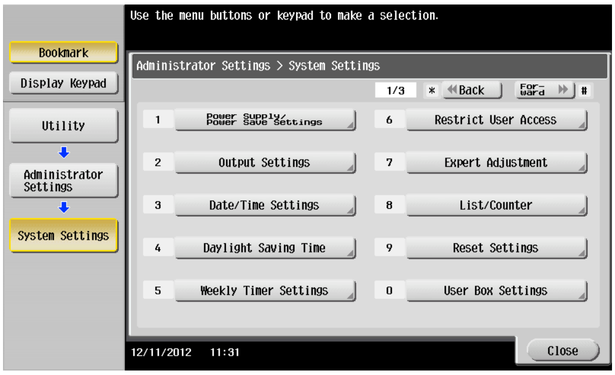
1 Call the Administrator Settings on the display from the control panel.

2 Touch [System Settings].



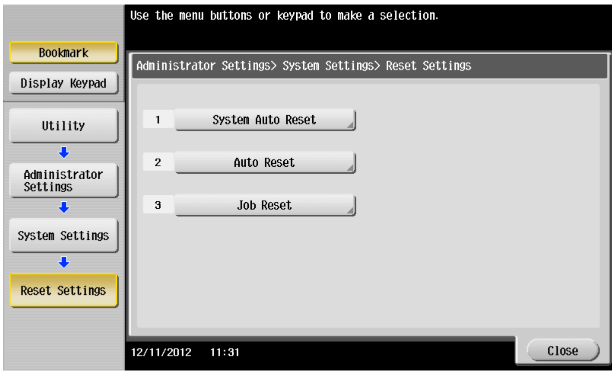
Use the menu buttons or keypad to make a selection.

3 Touch [Reset Settings].



Use the menu buttons or keypad to make a selection.

4 Touch [System Auto Reset].

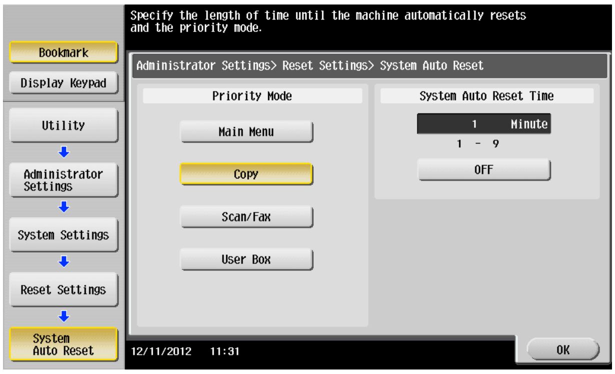


Use the menu buttons or keypad to make a selection.

Administrator Settings> System Settings> Reset Settings

12/11/2012 11:31

5 Touch [C] and enter the period of time (1 min. to 9 min.) after which System Auto Reset is activated from the keypad.



Specify the length of time until the machine automatically resets and the priority mode.

Administrator Settings> Reset Settings> System Auto Reset

System Auto Reset Time: 1 Minute (1 - 9)

12/11/2012 11:31

- ➔ Touch [Display Keypad] to display the keypad.
- ➔ The time for System Auto Reset can be set to a value between 1 min. and 9 min., variable in 1-min. increments. An input data error message appears when any value falling outside the range of 1 to 9 min. is set. Enter the correct System Auto Reset Time.
- ➔ 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.
- ➔ Touch [C] to clear all characters.

6 Touch [OK].

2.6 Changing the Administrator Password

When access to the machine by the administrator of the machine through the Administrator Settings 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.

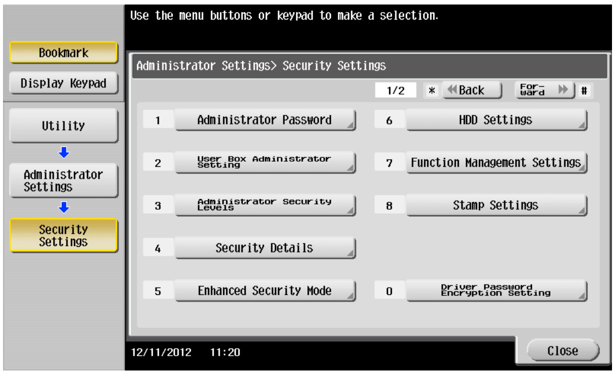
Changing the Administrator Password

✔ For the procedure to call the Security Settings screen on the display, see steps 1 and 2 of page 2-12.

✔ 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.

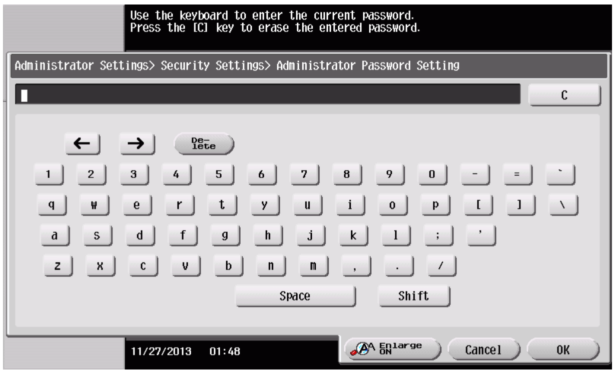
2 Touch [Administrator Password].



Use the menu buttons or keypad to make a selection.

Administrator Settings> Security Settings

3 Enter the currently set Administrator Password from the keyboard.



Use the keyboard to enter the current password.
Press the [C] key to erase the entered password.

Administrator Settings> Security Settings> Administrator Password Setting

➔ Touch [C] to clear all characters.

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

➔ Touch [Shift] to show the upper case/symbol screen.

➔ Touch [Cancel] to go back to the Security Settings screen.

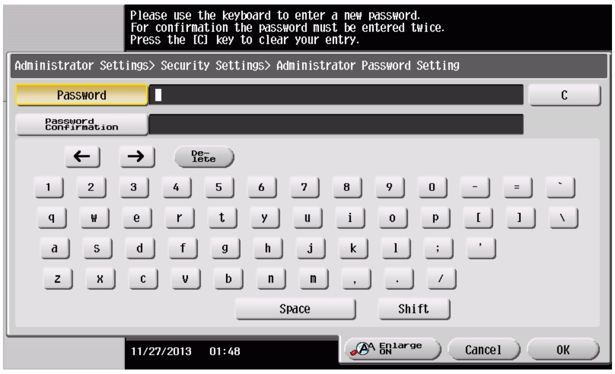
4 Touch [OK].

➔ If a wrong Administrator Password is entered, a message that tells that the Administrator Password does not match appears. Enter the correct Administrator Password.

➔ If the Enhanced Security Mode is set to [ON], entry of a wrong password is counted as unauthorized access. If a wrong Administrator Password is entered a predetermined number of times (once to three times) or more set by the administrator of the machine, a message appears saying that the machine accepts no more Administrator Passwords because of unauthorized access for any subsequent entry of the Administrator Password. The machine is then set into an access lock state. To cancel the access lock state, settings must be made by the Service Engineer; or, turn off, and then turn on, the main power switch of the machine. If the main power switch is turned off and on, the access lock state is canceled after the lapse of time set for [Release Time Settings]. When the main power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it

off. If there is no wait period between turning the main power switch off, then on again, the machine may not function properly.
Here is the sequence, through which the main power switch and sub power key are turned on and off:
Turn off the sub power key ►► Turn off the main power switch ►► Turn on the main power switch ►► Turn on the sub power key

5 Enter the new Administrator Password from the keyboard.
To prevent entry of a wrong password, enter the password again in [Password Confirmation].



Please use the keyboard to enter a new password.
For confirmation the password must be entered twice.
Press the [C] key to clear your entry.

Administrator Settings> Security Settings> Administrator Password Setting

11/27/2013 01:48

➔ Touch [C] to clear all characters.

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

➔ Touch [Shift] to show the upper case/symbol screen.

➔ Touch [Cancel] to go back to the Security Settings screen.

6 Touch [OK].

➔ If the entered Administrator Password does not meet 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, a message that tells that the Administrator Password does not match appears. Enter the correct Administrator Password.

2.7 Protecting Data in the HDD

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

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

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.

2.7.1 Setting the Encryption Key (encryption word)

✔ For the procedure to call the Security Settings screen on the display, see steps 1 and 2 of page 2-12.

✔ 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. Try to change the Encryption Key at regular intervals.

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

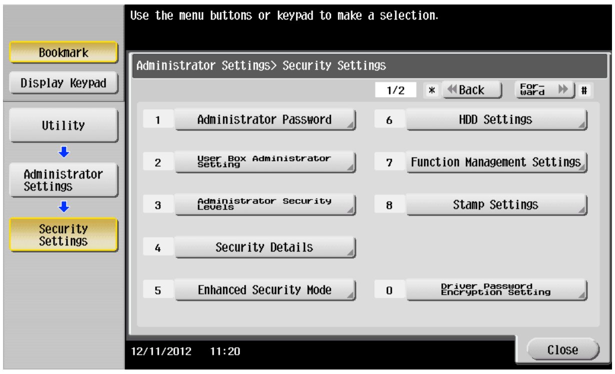
✔ If only the Encryption Key is to be set while the machine is being used without setting the Encryption Key, the Service Engineer must perform some setting procedures in advance. For details, contact your Service Representative.

✔ To edit/release the Encryption Key, see page 2-25. Do not release the Encryption Key when the Enhanced Security Mode is set to [ON]. Releasing the Encryption Key will cancel the Enhanced Security Mode.

✔ 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. For the functions whose settings are reset to the default values, see page 2-7.

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

2 Touch [HDD Settings].

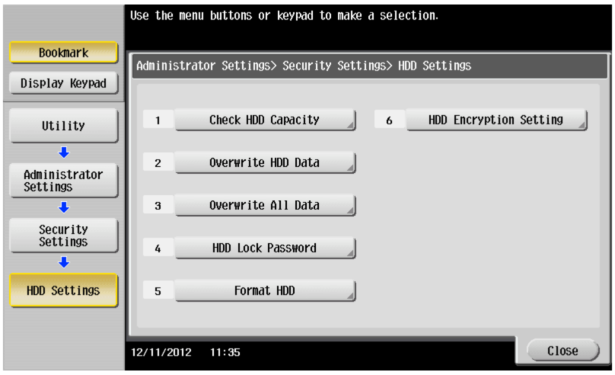


Use the menu buttons or keypad to make a selection.

Administrator Settings> Security Settings

12/11/2012 11:20

3 Touch [HDD Encryption Setting].

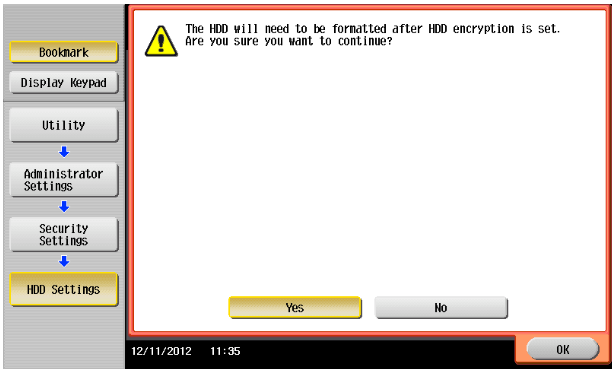


Use the menu buttons or keypad to make a selection.

Administrator Settings> Security Settings> HDD Settings

12/11/2012 11:35

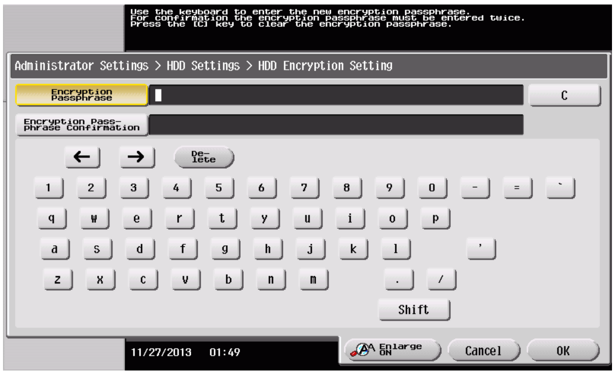
4 A confirmation message appears. Select [Yes] and touch [OK].



The HDD will need to be formatted after HDD encryption is set.
Are you sure you want to continue?

12/11/2012 11:35

5 Enter the new 20 characters Encryption Key from the keyboard.
To prevent entry of a wrong Encryption Key, enter the Encryption Key again in [Encryption Passphrase Confirmation].



Use the keyboard to enter the new encryption passphrase.
For confirmation the encryption passphrase must be entered twice.
Press the [C] key to clear the encryption passphrase.

Administrator Settings > HDD Settings > HDD Encryption Setting

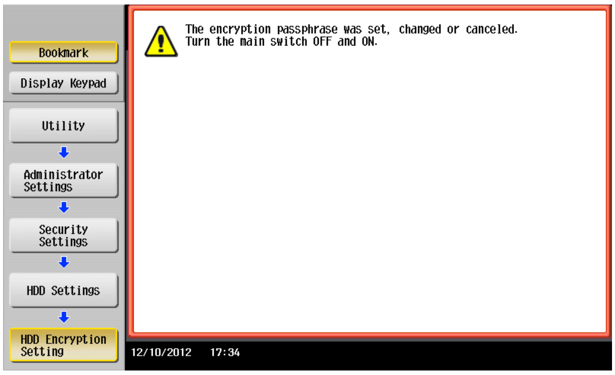
11/27/2013 01:49

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

6 Touch [OK].

- ➔ If the entered Encryption Key does not meet the Password Rules, a message that tells that the entered Encryption Key cannot be used appears. Enter the correct Encryption Key. For details of the Password Rules, see page 1-9.
- ➔ If the entered Encryption Key does not match, a message that tells that the Encryption Key does not match appears. Enter the correct Encryption Key.

7 Make sure that a message appears prompting you to turn OFF and then ON the main power switch. Now, turn OFF and then turn ON the main power switch.

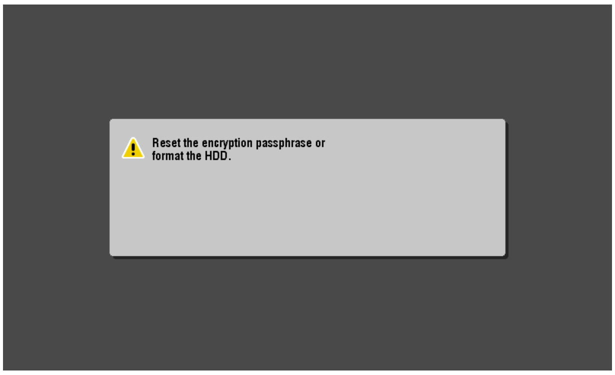


The encryption passphrase was set, changed or canceled.
Turn the main switch OFF and ON.

12/10/2012 17:34

→ When the main power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. if there is no wait period between turning the main power switch off, then on again, the machine may not function properly.
Here is the sequence, through which the main power switch and sub power key are turned on and off:
Turn off the sub power key ►► Turn off the main power switch ►► Turn on the main power switch ►► Turn on the sub power key

8 The following screen appears after the machine has been restarted.

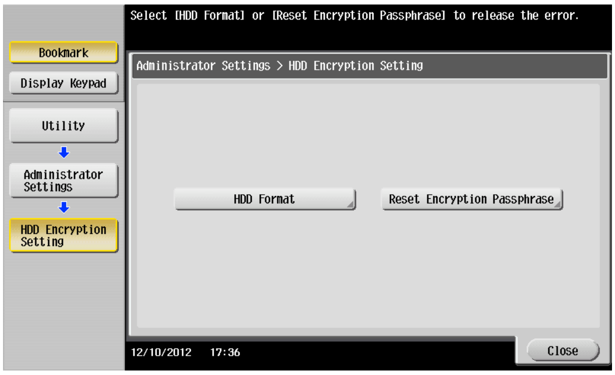


Reset the encryption passphrase or format the HDD.

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

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

10 Touch [HDD Format].

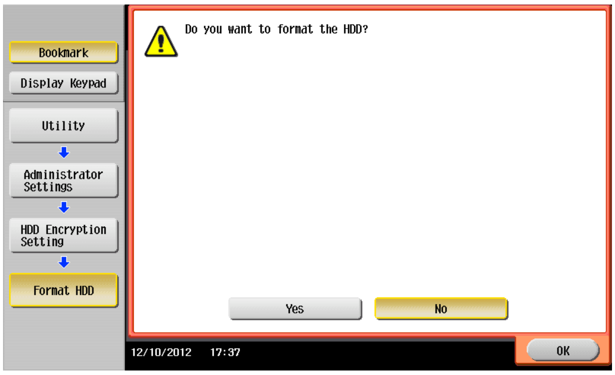


Select [HDD Format] or [Reset Encryption Passphrase] to release the error.

Administrator Settings > HDD Encryption Setting

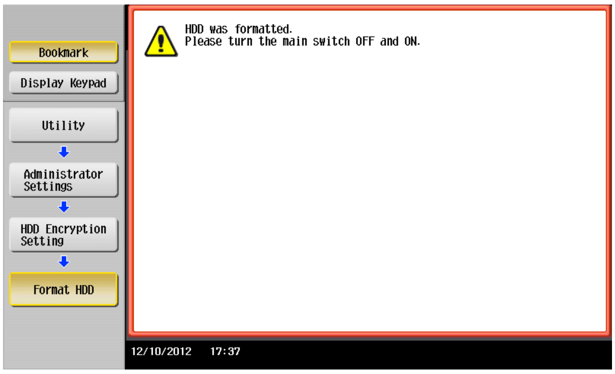
12/10/2012 17:36

11 A confirmation message appears. Select [Yes] and touch [OK].



Do you want to format the HDD?

12 Make sure that a message appears prompting you to turn OFF and then ON the main power switch. Now, turn OFF and then turn ON the main power switch.



HDD was formatted.
Please turn the main switch OFF and ON.

➔ When the main power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. if there is no wait period between turning the main power switch off, then on again, the machine may not function properly.
Here is the sequence, through which the main power switch and sub power key are turned on and off:
Turn off the sub power key ►► Turn off the main power switch ►► Turn on the main power switch ►► Turn on the sub power key

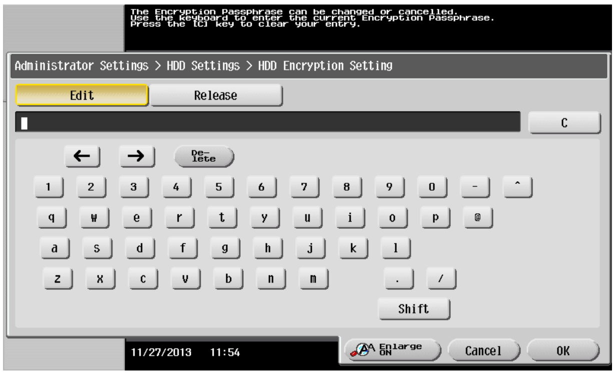
2.7.2 Changing the Encryption Key

✔ For the procedure to call the Encryption Key entry screen on the display, see steps 1 through 4 of page 2-21.

✔ 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 Encryption Key entry screen on the display from the control panel.

2 Enter the currently registered 20 characters Encryption Key from the keyboard.



The Encryption Passphrase can be changed or cancelled.
Use the keyboard to enter the current Encryption Passphrase.
Press the [C] key to clear your entry.

➔ Touch [C] to clear all characters.

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

➔ Touch [Shift] to show the upper case/symbol screen.

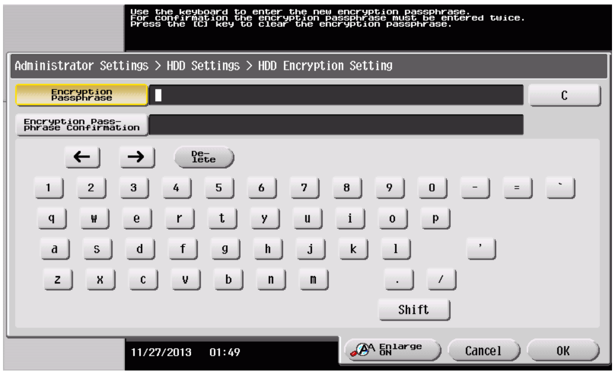
➔ Touch [Cancel] to go back to the HDD Settings screen.

3 Select [Edit] and touch [OK].

➔ If a wrong Encryption Key is entered, a message that tells that the Encryption Key does not match appears. Enter the correct Encryption Key.

➔ Releasing the Encryption Key by selecting [Release] will cancel the Enhanced Security Mode.

4 Enter the new 20 characters Encryption Key from the keyboard.
To prevent entry of a wrong Encryption Key, enter the Encryption Key again in [Encryption Passphrase Confirmation].



Use the keyboard to enter the new encryption passphrase.
For confirmation the encryption passphrase must be entered twice.
Press the [C] key to clear the encryption passphrase.

➔ Touch [C] to clear all characters.

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

➔ Touch [Shift] to show the upper case/symbol screen.

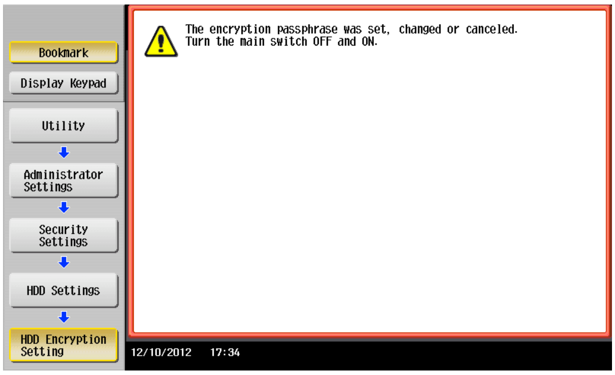
➔ Touch [Cancel] to go back to the HDD Settings screen.

5 Touch [OK].

➔ If the entered Encryption Key does not meet the Password Rules, a message that tells that the entered Encryption Key cannot be used appears. Enter the correct Encryption Key. For details of the Password Rules, see page 1-9.

➔ If the entered Encryption Key does not match, a message that tells that the Encryption Key does not match appears. Enter the correct Encryption Key.

6 Make sure that a message appears prompting you to turn OFF and then ON the main power switch. Now, turn OFF and then turn ON the main power switch.



The encryption passphrase was set, changed or canceled.
Turn the main switch OFF and ON.

12/10/2012 17:34

➔ When the main power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. if there is no wait period between turning the main power switch off, then on again, the machine may not function properly.
Here is the sequence, through which the main power switch and sub power key are turned on and off:
Turn off the sub power key ►► Turn off the main power switch ►► Turn on the main power switch ►► Turn on the sub power key

2.8 Overwrite All Data Function

When access to the machine by the administrator of the machine through the Administrator Settings is authenticated, the machine enables setting of the operation of the Overwrite All Data function.

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

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.

Setting the Overwrite All Data function

✔ Performing Overwrite All Data deletes the currently set external server. Set the external server again. For the procedure to set the external server, see page 2-14.

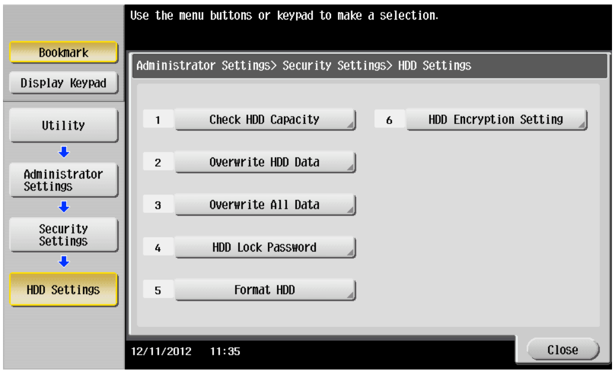
✔ Performing Overwrite All Data deletes the loadable driver installed in the machine, which calls for setting made by the Service Engineer. For details, contact your Service Representative.

✔ For the procedure to call the HDD Settings screen on the display, see steps 1 and 2 of page 2-21.

✔ 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 HDD Settings screen on the display from the control panel.

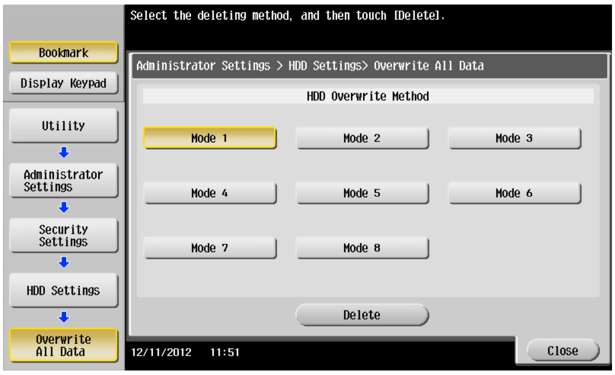
2 Touch [Overwrite All Data].



Use the menu buttons or keypad to make a selection.

Administrator Settings> Security Settings> HDD Settings

3 Select the desired mode and touch [Delete].

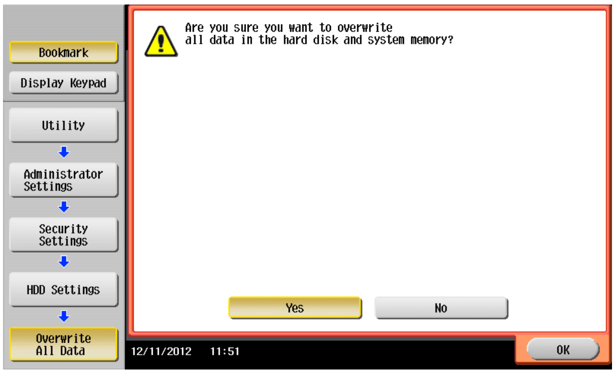


Select the deleting method, and then touch [Delete].

Administrator Settings > HDD Settings> Overwrite All Data

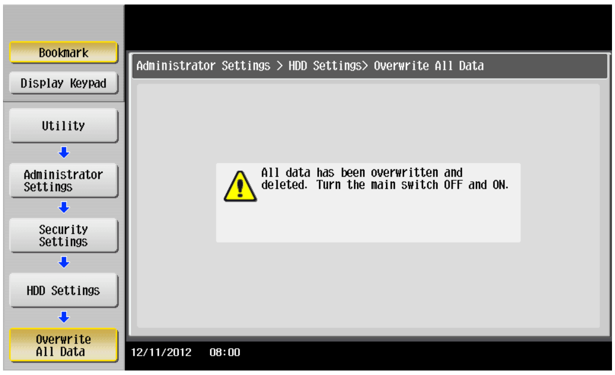
HDD Overwrite Method

4 A confirmation message appears. Select [Yes] and touch [OK].



Are you sure you want to overwrite all data in the hard disk and system memory?

5 Make sure that a message appears prompting you to turn OFF and then ON the main power switch. Now, turn OFF and then turn ON the main power switch.



Administrator Settings > HDD Settings> Overwrite All Data

All data has been overwritten and deleted. Turn the main switch OFF and ON.

➔ Check that all data has been overwritten and erased properly. Data is not erased properly if an error occurs during the procedure. For details, contact your Service Representative.

➔ When the main power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. if there is no wait period between turning the main power switch off, then on again, the machine may not function properly.
Here is the sequence, through which the main power switch and sub power key are turned on and off:
Turn off the sub power key ►► Turn off the main power switch ►► Turn on the main power switch ►► Turn on the sub power key

➔ After the main power switch has been turned on, quickly turn it off and give the machine to the Service Engineer. If the Overwrite All Data function is executed by mistake, contact the Service Engineer. For details, contact your Service Representative.

2.9 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

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

Setting the S/MIME Communication

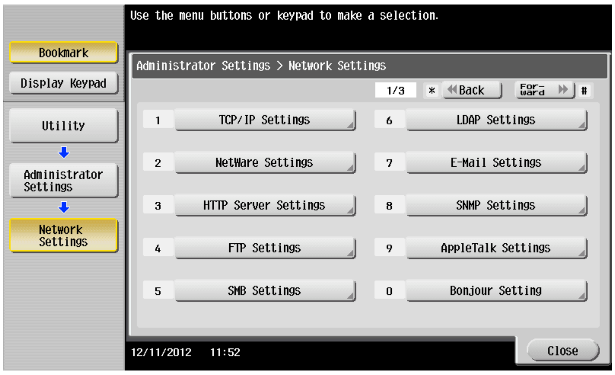
✔ For the procedure to call the Administrator Settings on the display, see page 2-2.

✔ 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].

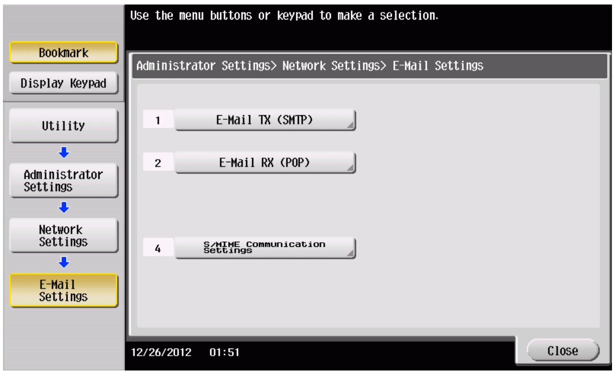
3 Touch [E-Mail Settings].



Use the menu buttons or keypad to make a selection.

Administrator Settings > Network Settings

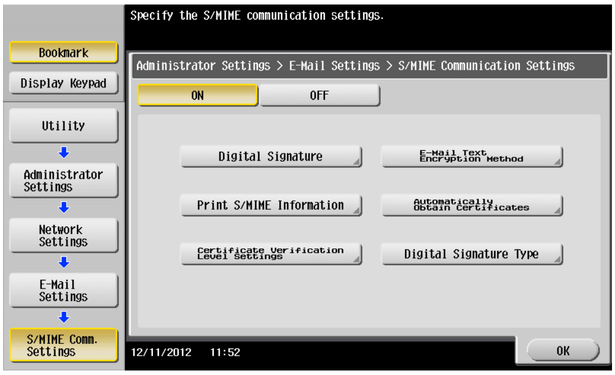
4 Touch [S/MIME Communication Settings].



Use the menu buttons or keypad to make a selection.

Administrator Settings> Network Settings> E-Mail Settings

5 Select [ON] and [E-Mail Text Encryption Method].



Specify the S/MIME communication settings.

Bookmark
Display Keypad
Utility
Administrator Settings
Network Settings
E-Mail Settings
S/MIME Comm. Settings

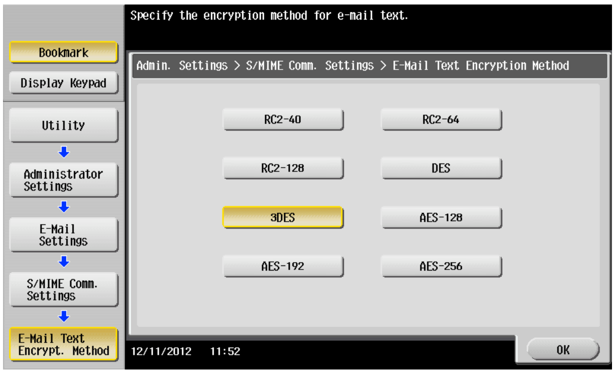
Administrator Settings > E-Mail Settings > S/MIME Communication Settings

ON OFF

Digital Signature
E-Mail Text Encryption Method
Print S/MIME Information
Automatically Obtain Certificates
Certificate Verification Level Settings
Digital Signature Type

12/11/2012 11:52
OK

6 Select encryption method and touch [OK].



Specify the encryption method for e-mail text.

Bookmark
Display Keypad
Utility
Administrator Settings
E-Mail Settings
S/MIME Comm. Settings
E-Mail Text Encrypt. Method

Admin. Settings > S/MIME Comm. Settings > E-Mail Text Encryption Method

RC2-40 RC2-64
RC2-128 DES
3DES AES-128
AES-192 AES-256

12/11/2012 11:52
OK

➔ 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.

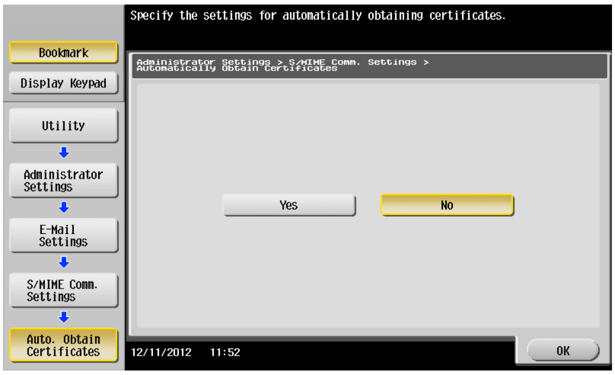
Name	Encryption algorithm	Encryption key length
[3DES]	3 key triple DES	168 bits
[AES-128]	AES	128 bits
[AES-192]	AES	192 bits
[AES-256]	AES	256 bits

➔ The Enhanced Security Mode is canceled, if the setting is changed to [RC2] or [DES] when the Enhanced Security Mode is [ON].

7 Touch [OK].

8 Select [Automatically Obtain Certificates].

9 Select [No] and touch [OK].



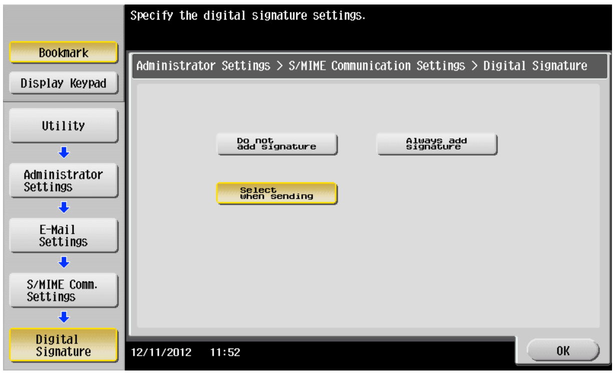
Specify the settings for automatically obtaining certificates.

Administrator Settings > S/MIME Comm. Settings > Automatically Obtain Certificates

12/11/2012 11:52

10 Touch [Digital Signature].

11 Select [Always add signature] or [Select when sending] and touch [OK].



Specify the digital signature settings.

Administrator Settings > S/MIME Communication Settings > Digital Signature

12/11/2012 11:52

12 Touch [OK].

2.10 PC-Fax RX 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 operation of the PC-Fax RX Setting Function. This function enables received fax documents to be saved in user boxes on the hard disk installed in the machine. Memory RX User Boxes or any other user boxes specified are used as saving destination user boxes.

NOTICE

If the PC-Fax RX Setting is made, the TSI User Box Setting function cannot be used.

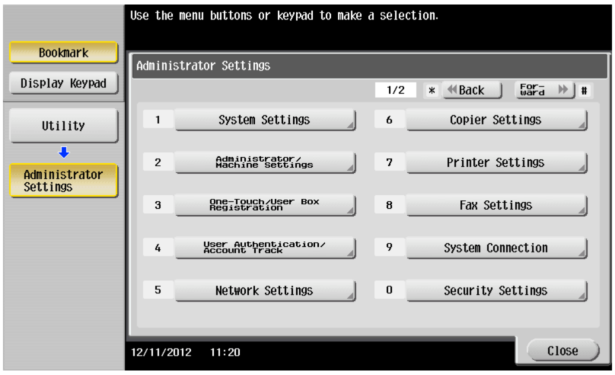
PC-Fax RX Setting

✔ 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 [Fax Settings].

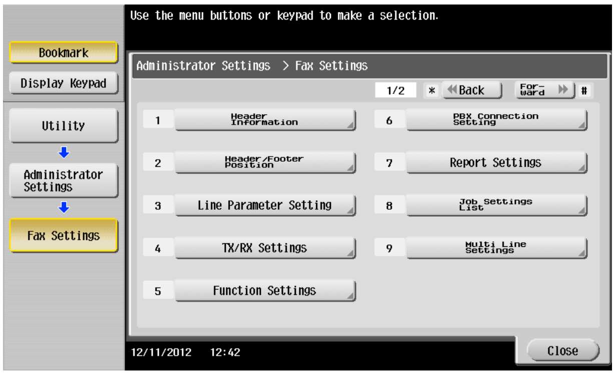


Use the menu buttons or keypad to make a selection.

Administrator Settings

12/11/2012 11:20

3 Touch [Function Settings].

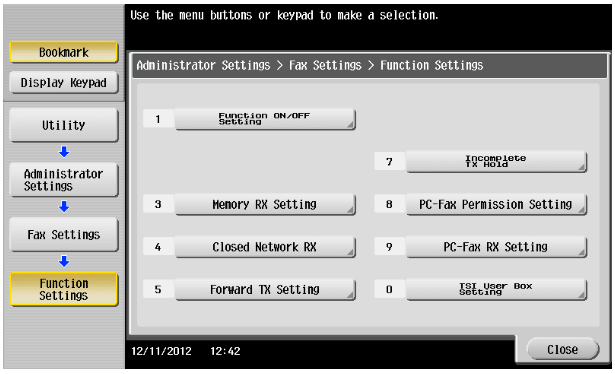


Use the menu buttons or keypad to make a selection.

Administrator Settings > Fax Settings

12/11/2012 12:42

4 Touch [PC-Fax RX Setting].

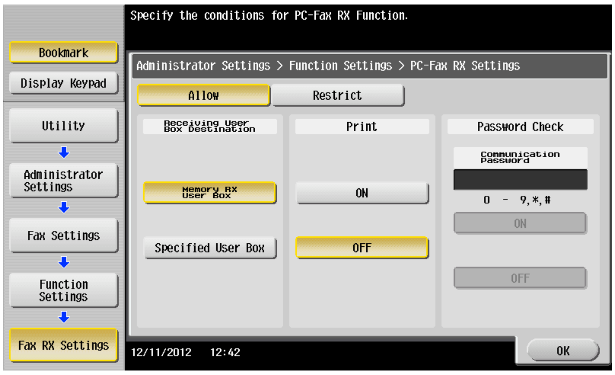


Use the menu buttons or keypad to make a selection.

Administrator Settings > Fax Settings > Function Settings

12/11/2012 12:42

5 Make the necessary settings.



Specify the conditions for PC-Fax RX Function.

Administrator Settings > Function Settings > PC-Fax RX Settings

- ➔ When [Specified User Box] is selected, the data is stored at the box whose number is assigned with F code Sub address.
- ➔ FAX input data is saved to the box as TIFF.
- ➔ When a user deleted [Specified User Box] specified at Receiving User Box Destination, the received data will be saved at print or forced memory inbox according to the conditions set for FAX receiving. Also when a new box is assigned with the same box number after [Specified User Box] specified at Receiving User Box Destination is deleted, the data will be saved at the newly assigned inbox, therefore you should be careful with the number assigned.

6 Touch [OK].

2.11 TSI User Box 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 operation of the TSI User Box Setting Function. This function automatically sorts documents received with fax IDs (TSIs) of the transmitters into other devices or boxes of the machine set up for each transmitter.

TSI User Box Setting

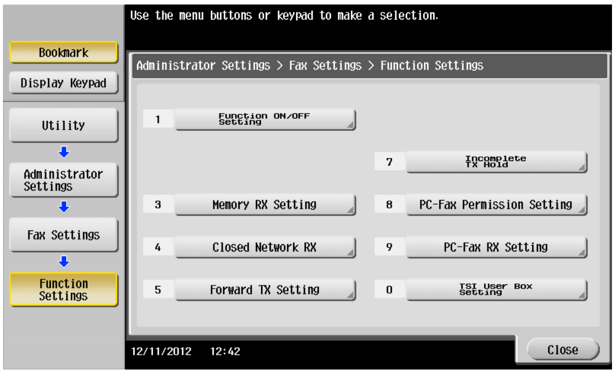
✔ For the procedure to call the Function Settings screen on the display, see step 1 through 3 of page 2-32.

✔ 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.

✔ When saving high confidential document, do not make box save via FAX.

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

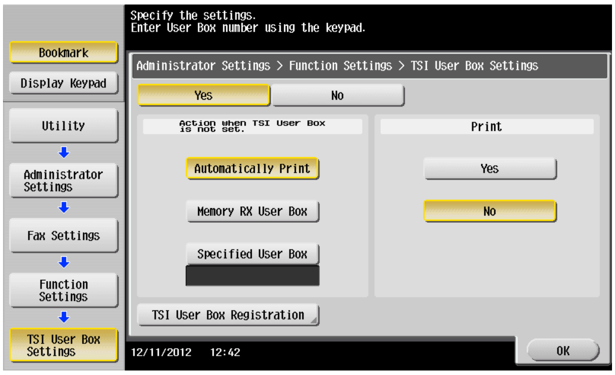
2 Touch [TSI User Box Setting].



Use the menu buttons or keypad to make a selection.

Administrator Settings > Fax Settings > Function Settings

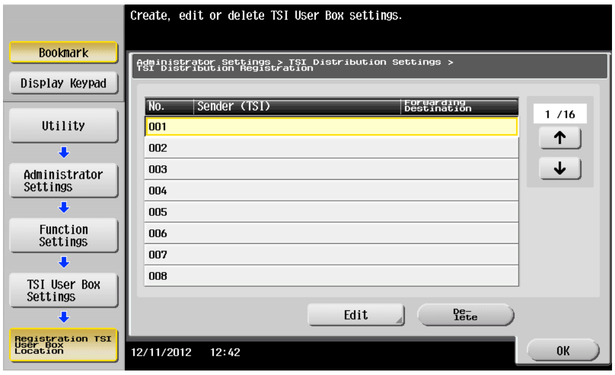
3 Select [Yes] and touch [TSI User Box Registration].



Specify the settings.
Enter User Box number using the keypad.

Administrator Settings > Function Settings > TSI User Box Settings

4 Select the number to be set and touch [Edit].



Create, edit or delete TSI User Box settings.

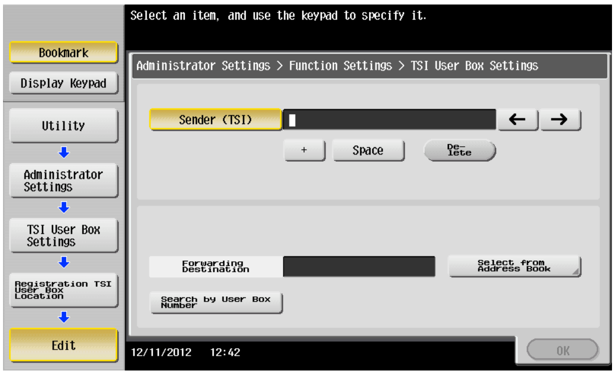
Administrator Settings > TSI Distribution Settings > TSI Distribution Registration

No.	Sender (TSI)	Forwarding Destination
001		
002		
003		
004		
005		
006		
007		
008		

➔ You can register up to 128 where the received data is distributed.

➔ To delete the registered one, select the number and touch [Delete].

5 Make the necessary settings, and touch [OK].



Select an item, and use the keypad to specify it.

Administrator Settings > Function Settings > TSI User Box Settings

12/11/2012 12:42

➔ Confidential inbox or terminal box cannot be set as the distribution target.

➔ When [Box] specified to save TSI is not available, the data will be saved at print or forced memory inbox according to the condition set for [Action when TSI User Box is not set]. Also when a new box is assigned with the same box number after [Box] set for the TSI is deleted, the data will be stored at the newly assigned inbox, therefore you should be careful with the number assigned.

6 Touch [OK].

2.12 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.

2.12.1 Setting the IP Address

✔ For the procedure to call the Network Settings screen on the display, see steps 1 and 2 of page 2-29.

✔ 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 [TCP/IP Settings].

3 Touch [IPv4 Settings].

4 Touch [Manual Input].

5 Select [IP Address] and set the IP Address.

➔ If [Auto Input] is selected for IP Application Method in step 4, select the means of acquiring the IP Address automatically from among DHCP Settings, BOOTP Settings, ARP/PING Settings, AUTO IP Settings, and the like.

6 Touch [OK].

7 Touch [OK].

➔ If a message appears that prompts you to turn OFF and ON the main power switch, turn OFF and ON the main power switch. When the main power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. If there is no wait period between turning the main power switch off, then on again, the machine may not function properly.
Here is the sequence, through which the main power switch and sub power key are turned on and off:
Turn off the sub power key ►► Turn off the main power switch ►► Turn on the main power switch ►► Turn on the sub power key

2.12.2 Registering the DNS Server

✔ For the procedure to call the TCP/IP Settings screen on the display, see steps 1 and 2 of page 2-36.

✔ 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 TCP/IP Settings screen on the display from the control panel.

2 Make the necessary settings for the DNS Server.

➔ If [Enable] is selected from the DNS Server Auto Obtain and DNS Domain Name Auto Retrieval, the DNS Server Address and DNS Domain Name are automatically acquired.

3 Touch [OK].

➔ If a message appears that prompts you to turn OFF and ON the main power switch, turn OFF and ON the main power switch. When the main power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. If there is no wait period between turning the main power switch off, then on again, the machine may not function properly.
Here is the sequence, through which the main power switch and sub power key are turned on and off:
Turn off the sub power key ►► Turn off the main power switch ►► Turn on the main power switch ►► Turn on the sub power key

2.13 NetWare Setting Function

When access to the machine by the administrator of the machine through the Administrator Settings is authenticated, the machine enables registration as the Print Server.

Making the NetWare Setting

✔ For the procedure to call the Network Settings screen on the display, see steps 1 and 2 of page 2-29.

✔ 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 [NetWare Settings].

3 Make the necessary settings.

4 Touch [OK].

➔ If a message appears that prompts you to turn OFF and ON the main power switch, turn OFF and ON the main power switch. When the main power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. If there is no wait period between turning the main power switch off, then on again, the machine may not function properly.
Here is the sequence, through which the main power switch and sub power key are turned on and off:
Turn off the sub power key ►► Turn off the main power switch ►► Turn on the main power switch ►► Turn on the sub power key

2.14 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 and 2 of page 2-29.

✔ 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 Make the necessary settings.

5 Touch [OK].

6 Touch [Close].

➔ If a message appears that prompts you to turn OFF and ON the main power switch, turn OFF and ON the main power switch. When the main power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. If there is no wait period between turning the main power switch off, then on again, the machine may not function properly.
Here is the sequence, through which the main power switch and sub power key are turned on and off:
Turn off the sub power key ►► Turn off the main power switch ►► Turn on the main power switch ►► Turn on the sub power key

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.

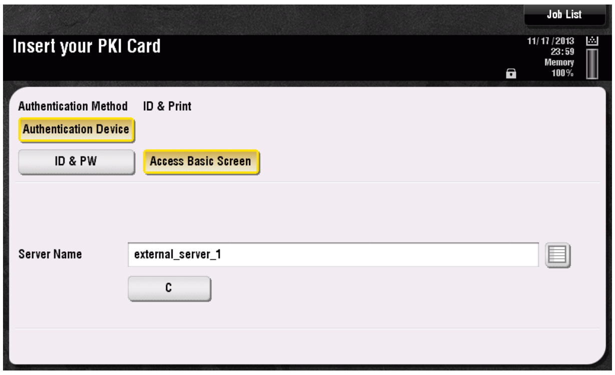
If a document is saved in the PKI Encrypted Document User Box of this machine, the print data of the user in question saved in the PKI Encrypted Document User Box of this machine can be automatically printed after the authentication by means of the IC card on the control panel is successful. Because 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.



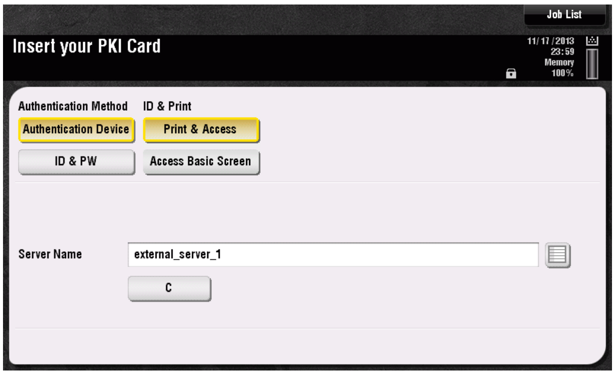
Insert your PKI Card

Authentication Method: Authentication Device

ID & Print: Access Basic Screen

Server Name: external_server_1

➔ The following screen appears 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.



Insert your PKI Card

Authentication Method: Authentication Device

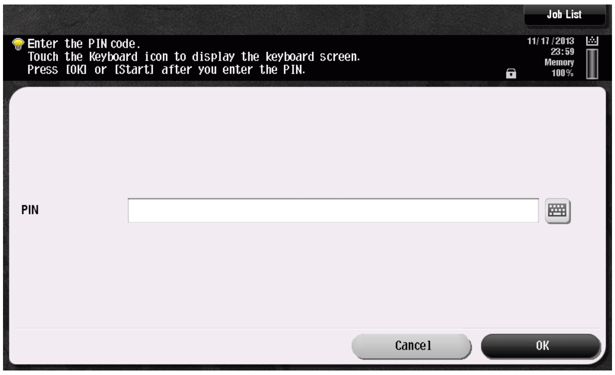
ID & Print: Print & Access

Server Name: external_server_1

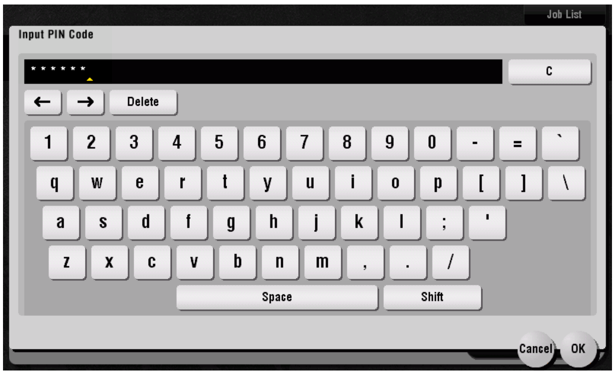
Login Method	Description
[Print & Access]	The user operation mode screen is called to the screen after the PKI Encrypted document of the corresponding user is printed.
[Access Basic Screen]	Only the ordinary login procedure is applicable and no PKI Encrypted document are printed.

➔ 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 keyboard icon in the [PIN] field.


Enter the PIN code.
Touch the Keyboard icon to display the keyboard screen.
Press [OK] or [Start] after you enter the PIN.

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



- ➔ Touch [C] to clear all characters.
- ➔ Touch [Delete] 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.

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

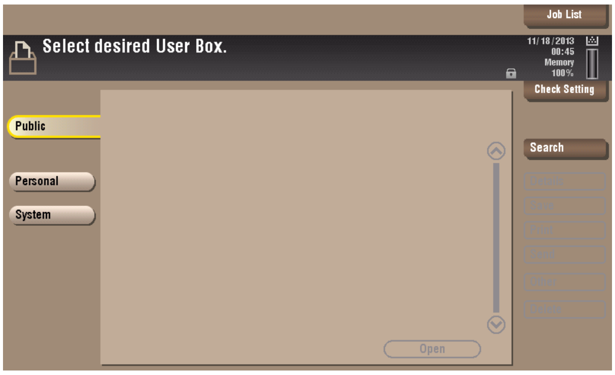
✔ For the logon procedure, see page 3-2.

✔ 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 [User Box].

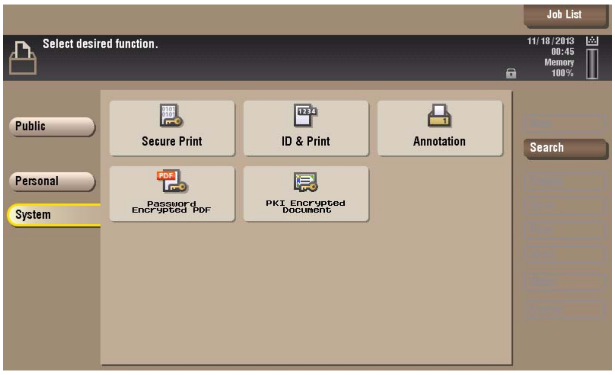
3 Touch [System].



Select desired User Box.

11/18/2013 00:45 Memory 100%

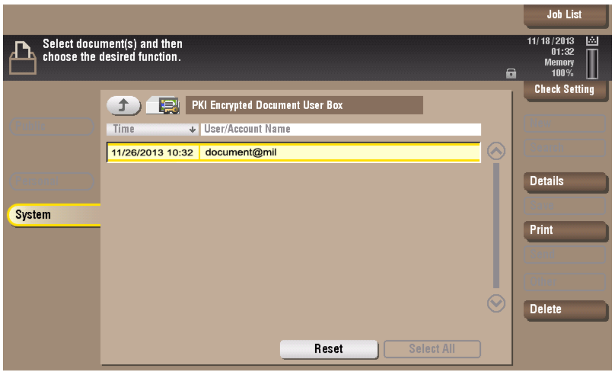
4 Touch [PKI Encrypted Document].



Select desired function.

11/18/2013 00:45 Memory 100%

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



Select document(s) and then choose the desired function.

11/18/2013 01:32 Memory 100%

PKI Encrypted Document User Box

Time	User/Account Name
11/26/2013 10:32	document@mil

➔ 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

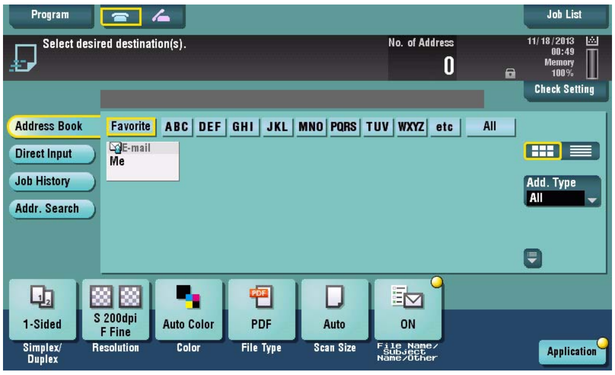
✔ For the logon procedure, see page 3-2.

✔ 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.

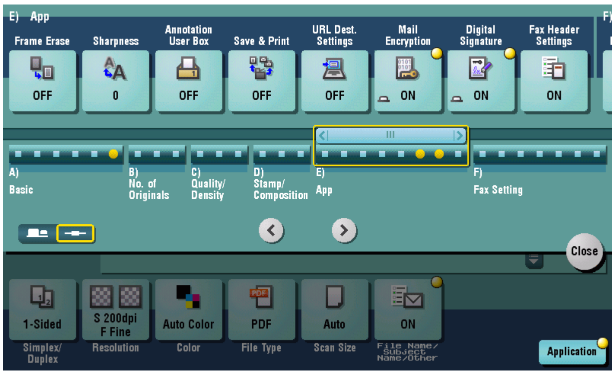
1 Using the IC card, log on to the machine.

2 Touch [Menu] ▸▸ [Scan/Fax].

3 Touch [Application].

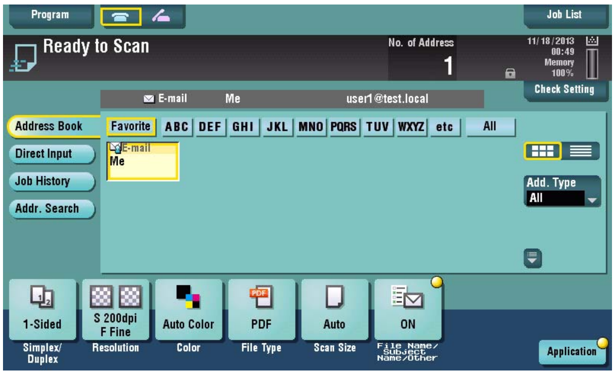


4 Select [Mail Encryption] and [Digital Signature].



5 Touch [Close].

6 Touch [Me].



7 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

© 2014 KONICA MINOLTA, INC.