

bizhub C253/C203

for PKI Card System

User's Guide [Security Operations]



Contents

1 Security

1.1	Introduction	1-2
	Compliance with the ISO15408 Standard	1-2
	Operating Precautions.....	1-2
	INSTALLATION CHECKLIST	1-3
1.2	Security Functions	1-4
1.2.1	Check Count Clear Conditions.....	1-4
1.3	Data to be Protected	1-5
1.4	Precautions for Operation Control	1-6
	Roles and Requirements of the Administrator.....	1-6
	Password Usage Requirements	1-6
	Operation and control of the machine.....	1-6
	Network Connection Requirements for the Machine	1-7
	Machine Maintenance Control.....	1-7
	Implementing digital signature properly	1-7
	Operating conditions for the IC card and IC card reader	1-7
	IC card owner requirements	1-7
1.5	Miscellaneous	1-8
	Password Rules	1-8
	Precautions for Use of Various Types of Applications	1-8
	Types of Data Cleared by Overwrite All Data Function	1-8
	Items cleared by HDD Format	1-8

2 Administrator Operations

2.1	Accessing the Administrator Settings	2-2
2.1.1	Accessing the Administrator Settings	2-2
	<Setting can be made only from the control panel>	2-3
2.1.2	Accessing the User Mode	2-5
	<Setting can be made only from the control panel>	2-5
2.2	Preventing Unauthorized Access	2-7
2.2.1	Setting Prohibited Functions When Authentication Error.....	2-7
	<Setting can be made only from the control panel>	2-8
2.3	Setting the External Server	2-10
2.3.1	Setting the External Server	2-10
	<Setting can be made only from the control panel>	2-10
2.4	System Auto Reset Function	2-13
2.4.1	Setting the System Auto Reset function.....	2-13
	<Setting can be made only from the control panel>	2-13
2.5	Changing the Administrator Password	2-15
2.5.1	Changing the Administrator Password.....	2-15
	<Setting can be made only from the control panel>	2-15
2.6	Protecting Data in the HDD	2-18
2.6.1	Setting the HDD Lock Password.....	2-18
	<Setting can be made only from the control panel>	2-19
2.6.2	Changing the HDD Lock Password.....	2-21
	<Setting can be made only from the control panel>	2-21
2.6.3	Setting the Encryption Key (encryption word)	2-24
	<Setting can be made only from the control panel>	2-24
2.6.4	Changing the Encryption Key	2-30
	<Setting can be made only from the control panel>	2-30
2.7	Overwrite All Data Function	2-33
2.7.1	Setting the Overwrite All Data function	2-33
	<Setting can be made only from the control panel>	2-34

2.8	S/MIME Communication Setting Function	2-36
2.8.1	Setting the S/MIME Communication	2-36
	<Setting can be made only from the control panel>	2-36
2.9	TCP/IP Setting Function	2-40
2.9.1	Setting the IP Address	2-40
	<Setting can be made only from the control panel>	2-40
2.9.2	Registering the DNS Server.....	2-41
	<Setting can be made only from the control panel>	2-41
2.10	NetWare Setting Function	2-42
2.10.1	Making the NetWare Setting.....	2-42
	<Setting can be made only from the control panel>	2-42
2.11	SMB Setting Function	2-43
2.11.1	Setting the NetBIOS Name.....	2-43
	<Setting can be made only from the control panel>	2-43
2.12	E-Mail Setting Function	2-44
2.12.1	Setting the SMTP Server (E-Mail Server).....	2-44
	<Setting can be made only from the control panel>	2-44

3 User Operations

3.1	User Authentication Function	3-2
3.1.1	User authentication using the IC card	3-2
	<Setting can be made only from the control panel>	3-3
3.2	Encrypted Document Function	3-5
3.2.1	Accessing the Encrypted document	3-5
	<Setting can be made only from the control panel>	3-5
3.3	Scan to Me Function	3-8
3.3.1	Scan to Me procedure	3-8
	<Setting can be made only from the control panel>	3-8



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 C253/C203 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 C253/bizhub C203 PKI Card System Control Software (MFP Controller: A02E0Y0-0100-GN0-U6).

Compliance with the ISO15408 Standard

The security functions offered by the bizhub C253/C203 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 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.

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.

INSTALLATION CHECKLIST

This Installation Checklist contains items that are to be checked 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
	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.	<input type="checkbox"/>
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.	<input type="checkbox"/>
	Set CE Authentication to [ON] and set the CE Password.	<input type="checkbox"/>
	Check that CS Remote Care is set to RAM Clear Set, Internet ISW Setting to OFF, and HDD to Installed.	<input type="checkbox"/>
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.	<input type="checkbox"/>
	Check that the HDD Lock Password or Encryption Key, or both, have been set by the Administrator of the machine.	<input type="checkbox"/>
	Check that External Server has been set by the Administrator of the machine.	<input type="checkbox"/>
	Check that Prohibited Functions When Authentication Error has been set to [Mode2] by the Administrator of the machine.	<input type="checkbox"/>
	Check that PageScope Web Connection has been set to [OFF] by the Administrator of the machine.	<input type="checkbox"/>
	Check that Access Setting of OpenAPI has been set to [Restrict] by the Administrator of the machine.	<input type="checkbox"/>
	Check that TCP Socket has been set to [OFF] by the Administrator of the machine.	<input type="checkbox"/>
	Check that FTP Server has been set to [OFF] by the Administrator of the machine.	<input type="checkbox"/>
	Check that Write Setting of SNMP v1/v2c Settings has been set to [Invalid] and SNMP v3(IP) has been set to [OFF] by the Administrator of the machine.	<input type="checkbox"/>
	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.	<input type="checkbox"/>
	Explain to the administrator that the settings for the security functions for this machine have been specified.	<input type="checkbox"/>

To make sure that the machine is used properly, make each setting according to the above checklist. Also, make the necessary settings according to the above checklist whenever the machine is initialized by HDD Format or Initialization to thereby make sure that the machine is in the correct operating condition.

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			
Service Representative		-	

1.2 Security Functions

A password that can be set must meet the requirements of the Password Rules. The machine does not accept setting of an easily decipherable password. For details of the Password Rules, see "[Password Rules](#)" on page 1-8.

If a wrong password is entered, during password authentication, a predetermined number of times (once to five times) set by the Administrator of the machine or more, 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 use of the machine.

Setting the HDD Lock Password provides the following security function. That is, even if the HDD is illegally replaced with another, the HDD authentication function prohibits access to the HDD, when the HDD Lock Password is yet to be set or there is a mismatch in the passwords. In addition, should the HDD be removed unawares, the HDD Lock Password locks the HDD protecting data contained in the HDD. Furthermore, by mounting the optional Security Kit SC-503 and setting the Encryption Key, the data stored in the HDD is encrypted, thereby protecting the data in the HDD. Note, however, that the HDD Lock Password and Encryption Key do 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 NVRAM to factory settings, preventing leak of data. For details of items to be cleared by Overwrite All Data function, see "[Types of Data Cleared by Overwrite All Data Function](#)" on page 1-8.

1.2.1 Check Count Clear Conditions

The following are the conditions for clearing or resetting the check count of the number of wrong entries when [Mode2] is set for Prohibited Functions When Authentication Error.

<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 stored 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 stored 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 stored 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 of a job in the queue
- Image files other than Encrypted document
- Data files left in the data space used as image files
- 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.

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, HDD Lock 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, HDD Lock Password and Encryption Key.
- The Administrator should set the Administrator Password using eight digits. (Selectable from among a total of 92 characters)
- The Administrator must change the Administrator Password, HDD Lock 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, HDD Lock 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.

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 HDD Lock Password according to the environment, in which this machine is used. If the machine is mounted with the optional Security Kit SC-503, the Administrator should also set either the HDD Lock Password or Encryption Key, or both.
- The Administrator should enable Prohibited Functions When Authentication Error and control the operation of the machine for use in [Mode2].
- The Administrator should disable PageScope Web Connection and control the operation of the machine for use in the disable state.
 - To disable PageScope Web Connection, press the [Utility/Counter] key, and then [Administrator Settings] - [Network Settings] - [HTTP Server Settings] on the MFP control panel, and set "PSWC Settings" to "OFF."
- The Administrator should disable OpenAPI and control the operation of the machine for use in the disable state.
 - To disable OpenAPI, press the [Utility/Counter] key, and then [Administrator Settings] - [System Connection] - [OpenAPI Settings] on the MFP control panel, and set "Access Setting" to "Restrict."
- The Administrator should disable the TCP Socket and control the operation of the machine for use in the disable state.
 - To disable the TCP Socket, press the [Utility/Counter] key, and then [Administrator Settings] - [Network Settings] - [Forward] - [TCP Socket Settings] on the MFP control panel, and set "TCP Socket" to "OFF."
- The Administrator should disable the FTP Server and control the operation of the machine for use in the disable state.
 - To disable the FTP Server, press the [Utility/Counter] key, and then [Administrator Settings] - [Network Settings] - [FTP Settings] on the MFP control panel, and set "FTP Server Settings" to "OFF."

- The Administrator should disable Write Setting of SNMP v1/v2c and control the operation of the machine for use in the disable state.
- To disable Write Setting of SNMP v1/v2c, press the [Utility/Counter] key, and then [Administrator Settings] - [Network Settings] - [SNMP Settings] - [Forward] - [SNMP v1/v2c Settings] - [Forward] on the MFP control panel, and set "Write Setting" to "Invalid."
- The Administrator should disable SNMP v3 and control the operation of the machine for use in the disable state.
- To disable SNMP v3, press the [Utility/Counter] key, and then [Administrator Settings] - [Network Settings] - [SNMP Settings] on the MFP control panel, and set "SNMP v3(IP)" to "OFF."

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.

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.

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, ask your Service Representative.

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

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

Types of passwords	No. of digits	Characters
Administrator Password	0 to 8 digits	<ul style="list-style-type: none"> Numeric characters: 0 to 9 Alpha characters: upper and lower case letters Symbols: !, #, \$, %, &, ', (,), *, ,, -, ., /, :, ;, <, =, >, ?, @, [, \,], ^, _ ` {, , }, ~ Selectable from among a total of 92 characters
HDD Lock Password	20 digits	<ul style="list-style-type: none"> Numeric characters: 0 to 9 Alpha characters: upper and lower case letters Symbols: !, #, \$, %, &, ', * , +, -, ., /, =, <, @, ^, _ ` {, , }, ~ Selectable from among a total of 83 characters
Encryption Key		



Note

Be sure to set the Administrator Password using eight digits to keep the security status. For details of the Administrator Password Setting, see ["Changing the Administrator Password" on page 2-15](#).

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.

Types of Data Cleared by Overwrite All Data Function

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

Types of Data Cleared	Description
Encrypted document file	Deletes all Encrypted document files saved in Encrypted document User Box
Image files	<ul style="list-style-type: none"> Image files saved other than Encrypted document files Image files of jobs in job queue state
HDD Lock Password	Clears the currently set password
Encryption Key	Clears the currently set Encryption Key
Administrator Password	Clears the currently set password, resetting it to the factory setting
S/MIME certificate data	Deletes the currently set S/MIME certificate
External Server	Deletes the currently set External Server
Loadable driver	Deletes the currently set loadable driver

Items cleared by HDD Format

Following are the items that are cleared by HDD Format.

Types of Data Cleared	Description
Encrypted document file	Deletes all Encrypted document files saved in Encrypted document User Box
External Server	Deletes the External Server
Loadable driver	Deletes the loadable driver



Note

Performing HDD Format deletes the loadable driver installed in the machine, which calls for setting made by the Service Engineer. For details, ask your Service Representative.



2

Administrator Operations

2 Administrator Operations

2.1 Accessing the Administrator Settings

This machine implements authentication of the user of the Administrator Settings function through the 8-digit 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.

Two different methods are available for accessing Administrator Settings. In Administrator Settings, the setting for the machine system can be registered or changed. In User Mode, the same settings as the user authority can be made. For box setting operations, however, the same functions can be set as those of Administrator Settings. User Mode also allows jobs to be checked or deleted, which is not possible in Administrator Settings.

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.



Note

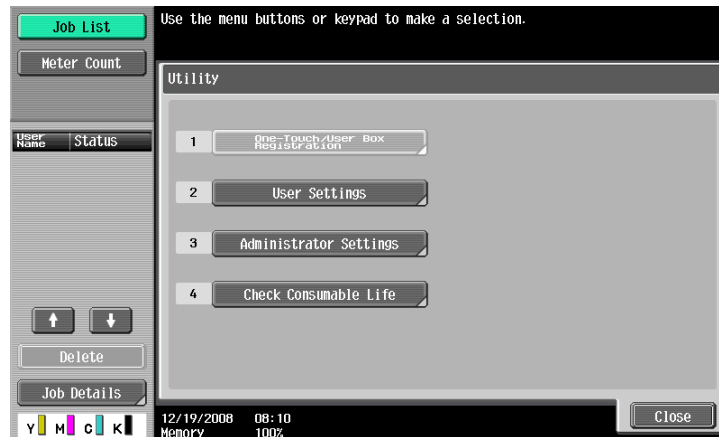
Make sure that none of the general users of the machine will know the Administrator Password.

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

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.

<Setting can be made only from the control panel>

- 1 Press the [Utility/Counter] key.
- 2 Touch [Administrator Settings].



- ? Is it possible to gain access to the Administrator Settings while a job is being executed?
 → The machine does not accept access to the Administrator Settings while a job is being executed. Wait until the execution of the job is completed before attempting to access the Administrator Settings again.

- 3 Enter the 8-digit Administrator Password from the keyboard and keypad.



- Press the [C] key 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].
 - ? What happens if a wrong Administrator Password is entered?
 - If a wrong Administrator Password is entered, a message appears saying that there is a mismatch in the Administrator Passwords and entry of the Administrator Password will be prohibited for five sec. Wait for some while before entering the correct Administrator Password.
 - If Prohibited Functions When Authentication Error is set to [Mode2], entry of a wrong password is counted as unauthorized access. If a wrong Administrator Password is entered a predetermined number of times (once to five times) set by the Administrator of the machine or more, 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 switch are turned on and off:
Turn off the sub power switch → Turn off the main power switch → Turn on the main power switch → Turn on the sub power switch
- 5 Press the [Utility/Counter] key to log off from the Administrator Settings.

2.1.2 Accessing the User Mode



Note

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.

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.

<Setting can be made only from the control panel>

- 1 Touch [ID & PW].



- 2 Touch [Password].



- 3 Enter the 8-digit Administrator Password from the keyboard and keypad.



- Press the [C] key 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].

- 5 Press [Access] or touch [Login].

? What happens if a wrong Administrator Password is entered?

- If a wrong Administrator Password has been entered, the machine gives a message that tells that authentication has not been successful. Enter the correct Administrator Password.
- If Prohibited Functions When Authentication Error is set to [Mode2], entry of a wrong password is counted as unauthorized access. If a wrong Administrator Password is entered a predetermined number of times (once to five times) set by the Administrator of the machine or more, 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 switch are turned on and off:
Turn off the sub power switch → Turn off the main power switch → Turn on the main power switch → Turn on the sub power switch

- 6 Press the [Access] key to log off from the User Mode.

2.2 Preventing Unauthorized Access

When access by the Administrator of the machine through the Administrator Settings via the control panel 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 [Mode2] is set, the check count can be selected from among once to five times. To prevent unauthorized access, operate the machine in [Mode2]. 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.



...

Note

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.

2.2.1 Setting Prohibited Functions When Authentication Error



...

Note

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.

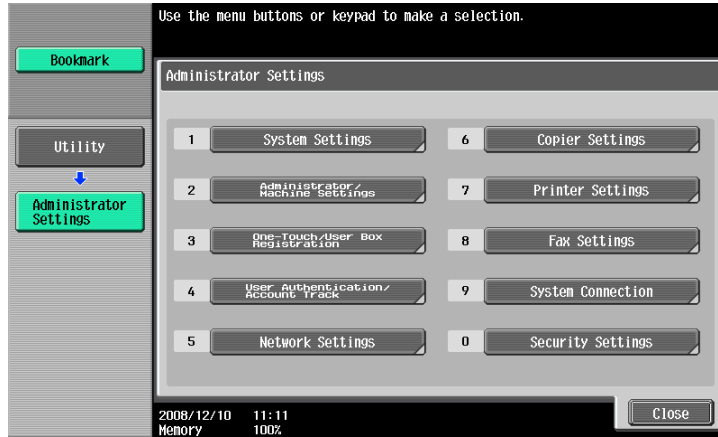
Release Time can be set to any value between 1 min. and 60 min. in 1-min. increments. An input data error message appears when any value falling outside the range of 1 to 60 min. is set. Enter the correct Release Time again.

<Setting can be made only from the control panel>

✓ For the procedure to call the Administrator Settings to the display, see "[Accessing the Administrator Settings](#)" on page 2-2.

1 Call the Administrator Settings to the screen from the control panel.

2 Touch [Security Settings].



3 Touch [Security Details].



4 Touch [Prohibited Functions When Authentication Error].



5 Touch [Mode 2].

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

6 Touch [Release Time Settings].**7** Press the [C] key and, from the keypad, enter the time, after the lapse of which the access lock state of the Administrator Settings is canceled.**8** Touch [OK].

2.3 Setting the External Server

When access to the Administrator of the machine by the Administrator Settings via the control panel 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.

2.3.1 Setting the External Server



Note

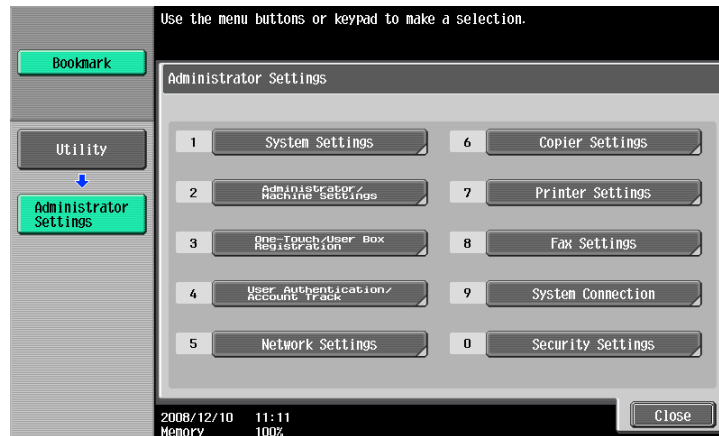
Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.

A Sever Name that already exists cannot be redundantly registered.

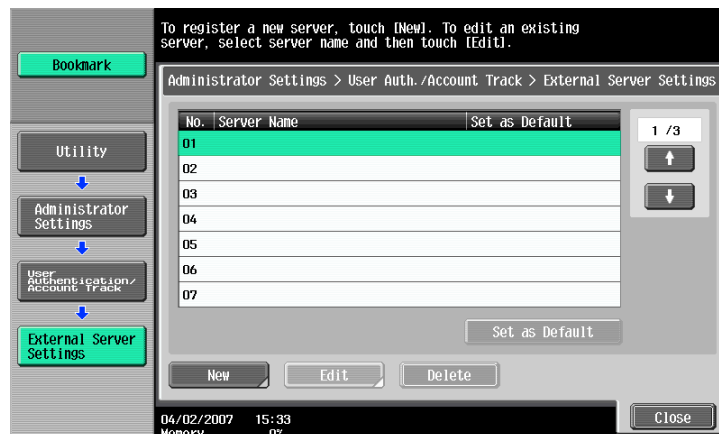
<Setting can be made only from the control panel>

- ✓ For the procedure to call the Administrator Settings to the display, see "[Accessing the Administrator Settings](#)" on page 2-2.

- 1 Call the Administrator Settings to the screen from the control panel.
- 2 Touch [User Authentication/Account Track].



- 3 Touch [External Sever Settings].
- 4 Touch the specific Sever Registration key, in which no sever has been registered.
- 5 Touch [New].



- ? What steps should be followed to change or delete a server previously registered?
 → To change or delete a previously registered server, touch [Edit] or [Delete].

6 Touch [Server Type].

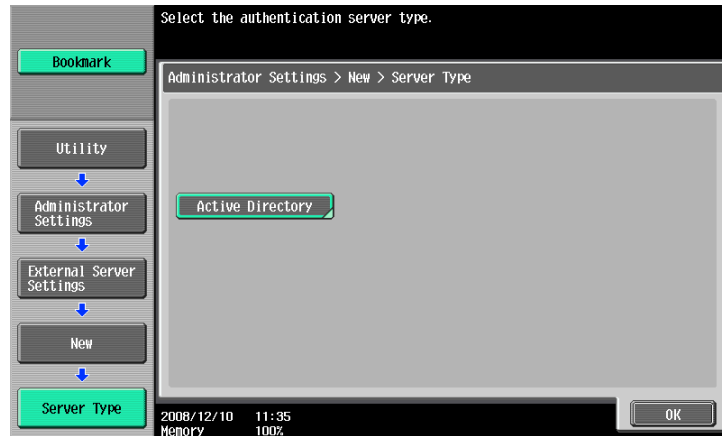


7 Touch [Active Directory].



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



9 Touch [OK].**10** Make the necessary settings.

? What happens if the Sever Name is yet to be entered?

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

11 Touch [OK].**12** Touch [Close].

? What steps should be performed if two or more External Servers have been registered?

→ If two or more External Servers have been registered, select any desired server and touch [Set as Default].

2.4 System Auto Reset Function

When access to the Administrator of the machine by the Administrator Settings via the control panel is authenticated, the machine enables setting of the operation of the System Auto Reset function.

If no operations are performed for a predetermined period of time during access to the Administrator Settings or user mode (during setting of User Authentication) from the control panel, the System Auto Reset function automatically causes the user to log off from the mode. Processing of a specific function, 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 function has been started, the System Auto Reset function does not cause 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.

2.4.1 Setting the System Auto Reset function



Note

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.

<Setting can be made only from the control panel>

✓ For the procedure to call the Administrator Settings to the display, see "[Accessing the Administrator Settings](#)" on page 2-2.

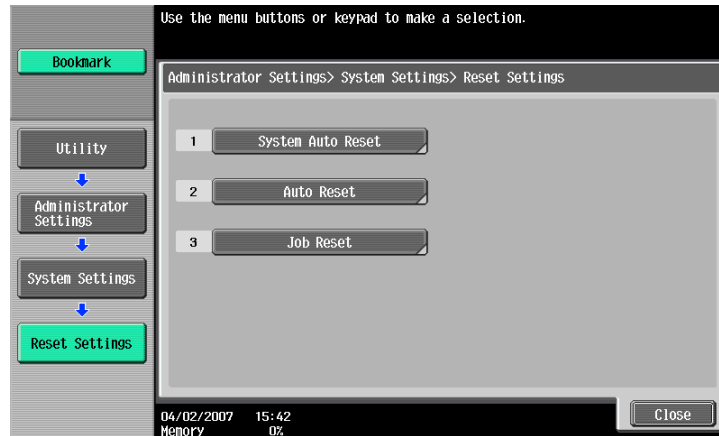
- 1 Call the Administrator Settings to the screen from the control panel.
- 2 Touch [System Settings].



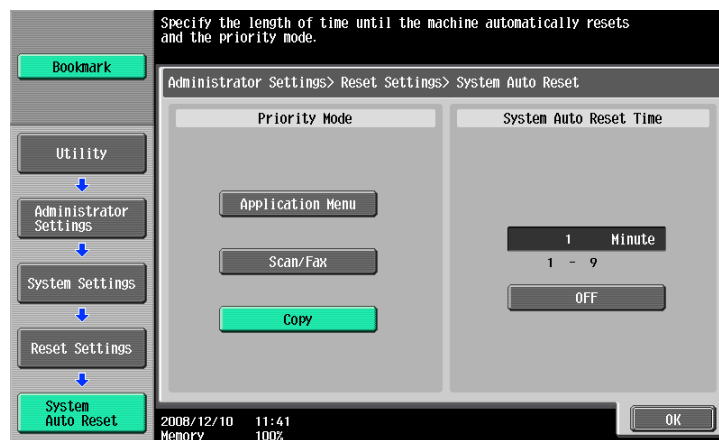
- 3 Touch [Reset Settings].



4 Touch [System Auto Reset].



5 Press the [C] key and enter the period of time (1 min. to 9 min.) after which System Auto Reset is activated from 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 again.
- 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.
- Press the [C] key to clear all characters.

6 Touch [OK].

2.5 Changing the Administrator Password

When access to the Administrator of the machine from the control panel by the Administrator Settings 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.



Note

Be sure to set the new Administrator Password using eight digits.

2.5.1 Changing the Administrator Password



Note

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.

<Setting can be made only from the control panel>

- ✓ For the procedure to call the Security Settings menu to the display, see steps 1 and 2 of "[Setting Prohibited Functions When Authentication Error](#)" on page 2-7.

- 1 Call the Security Settings to the screen from the control panel.
- 2 Touch [Administrator Password].



- 3 Enter the currently set 8-digit Administrator Password from the keyboard and keypad.



- Press the [C] key 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].

- ? What if an Administrator Password different from that is currently registered is mistakenly entered?
- If there is a mismatch between the currently registered Administrator Password and the Administrator Password entered, a message appears that tells that there is a mismatch in the Administrator Passwords. Enter the correct Administrator Password.
- If Prohibited Functions When Authentication Error is set to [Mode2], entry of a wrong password is counted as unauthorized access. If a wrong Administrator Password is entered a predetermined number of times (once to five times) set by the Administrator of the machine, the Utility screen appears and the machine is 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 switch are turned on and off:
 Turn off the sub power switch → Turn off the main power switch → Turn on the main power switch → Turn on the sub power switch

5 Enter the new 8-digit Administrator Password from the keyboard and keypad.



- Press the [C] key 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].

7 To prevent entry of a wrong Administrator Password, enter the new 8-digit Administrator Password once again.



- Press the [C] key 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.

8 Touch [OK].

? What happens if there is a mismatch in the Administrator Passwords?

→ If there is a mismatch in the Administrator Passwords, a message appears that tells that there is a mismatch in the Administrator Passwords. Perform steps 5 through 8 once again.

2.6 Protecting Data in the HDD

When access to the Administrator of the machine by the Administrator Settings is authenticated, the machine enables the operation for setting and changing the HDD Lock Password. It also enables the operation for setting and changing the Encryption Key when the optional Security Kit SC-503 is mounted.

Should the HDD be removed unawares, the HDD Lock Password locks the HDD protecting data contained in the HDD. Furthermore, by setting the Encryption Key, the data stored in the HDD is encrypted, thereby protecting the data in the HDD. The HDD Lock Password and Encryption Key entered are displayed as "*"."

To protect data in the HDD, be sure to set the HDD Lock Password or Encryption Key.



...

Note

Do not set any number that can easily be guessed from birthdays, employee identification numbers, and the like for the HDD Lock Password and Encryption Key. Try to change the password at regular intervals.

Make sure that nobody but the Administrator of the machine comes to know the HDD Lock Password or Encryption Key.

If only the Encryption Key is to be set while the machine is being used without setting the HDD Lock Password or Encryption Key, the Service Engineer must perform some setting procedures in advance. For more details, ask the Service Representative.

HDD Format should be performed before setting the Encryption Key. Performing HDD Format deletes the currently set External Server. Set the External Server again. For the procedure to set the External Server, see "[Setting the External Server](#)" on page 2-10.



...

Reminder

When the HDD Lock Password is set, HDD verification is carried out when the machine is started. If the HDD has been improperly replaced with another, or if the HDD Lock Password is yet to be set, a message appears that tells that there is a mismatch between the HDD and the HDD Lock Password. Further, the HDD has the following function. That is, if the HDD is illegally removed or replaced with another, detection of a wrong HDD Lock Password five consecutive times will lock the authentication function. Leak of data can thus be prevented.

When an Encryption Key (encryption word) is set using HDD Encryption Setting, an Encryption Key with a key length of 128 bits is generated using the SHA-1 algorithm. The generated encryption key is used to encrypt or decrypt data through AES encryption algorithm.

When the Encryption Key (encryption word) is set with the optional Security Kit SC-503 mounted on the machine, the encryption strength can be selected from among [Encryption Priority] or [Overwrite Priority]. For more details, see "[Setting the Encryption Key \(encryption word\)](#)" on page 2-24.

2.6.1 Setting the HDD Lock Password



...

Note

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 switch are turned on and off:

Turn off the sub power switch → Turn off the main power switch → Turn on the main power switch → Turn on the sub power switch

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.

<Setting can be made only from the control panel>

- ✓ For the procedure to call the Security Settings menu to the display, see steps 1 and 2 of "[Setting Prohibited Functions When Authentication Error](#)" on page 2-7.

- 1 Call the Security Settings to the screen from the control panel.
- 2 Touch [HDD Settings].



- 3 Touch [HDD Lock Password].



- 4 Enter the 20-digit HDD Lock Password from the keyboard and keypad.



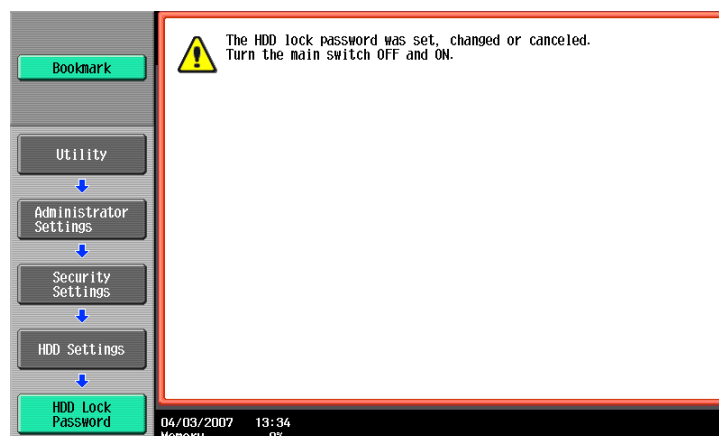
- Press the [C] key to clear all characters.
- Touch [Delete] to delete the last character entered.
- Touch [Shift] to show the upper case/symbol screen.
- Touch [Cancel] to go back to the HDD Settings screen.

- 5 Touch [OK].
- ? What happens if the HDD Lock Password entered does not meet the requirements of the Password Rules?
- If the HDD Lock Password entered does not comply with the Password Rules, a message appears that tells that the HDD Lock Password entered cannot be used. Enter the correct HDD Lock Password. For details of the Password Rules, see "[Password Rules](#)" on page 1-8.
- To change the HDD Lock Password, see "[Changing the HDD Lock Password](#)" on page 2-21.
- 6 To prevent entry of a wrong password, enter the 20-digit HDD Lock Password once again.



- Press the [C] key 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.

- 7 Touch [OK].
- ? What happens if there is a mismatch in the HDD Lock Passwords?
- If there is a mismatch in the HDD Lock Passwords, a message appears that tells that there is a mismatch in the HDD Lock Passwords. Perform steps 4 through 7 once again.
- 8 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.



Note

NEVER forget the HDD Lock Password set through the above procedure. The HDD Lock Password must be entered when changing canceling the HDD Lock Password.

2.6.2 Changing the HDD Lock Password



Note

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 switch are turned on and off:

Turn off the sub power switch → Turn off the main power switch → Turn on the main power switch → Turn on the sub power switch

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.

<Setting can be made only from the control panel>

- ✓ To call the HDD Lock Password entry screen to the display, see steps 1 through 3 of "[Setting the HDD Lock Password](#)" on page 2-18.

- 1 Call the HDD Lock Password entry screen to the display from the control panel.
- 2 Enter the currently registered 20-digit password from the keyboard and keypad.



- Press the [C] key 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 the [Edit] and touch [OK].

? What happens if there is a mismatch in the HDD Lock Passwords?

→ If there is a mismatch in the HDD Lock Passwords, a message appears that tells that there is a mismatch in the HDD Lock Passwords. Enter the correct password.

- 4 Enter the new 20-digit HDD Lock Password from the keyboard and keypad.



- Press the [C] key 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].

? What happens if the HDD Lock Password entered does not meet the requirements of the Password Rules?

- If the HDD Lock Password entered does not comply with the Password Rules, a message appears that tells that the HDD Lock Password entered cannot be used. Enter the correct HDD Lock Password. For details of the Password Rules, see ["Password Rules" on page 1-8](#).

- 6 To prevent entry of a wrong password, enter the 20-digit HDD Lock Password once again.



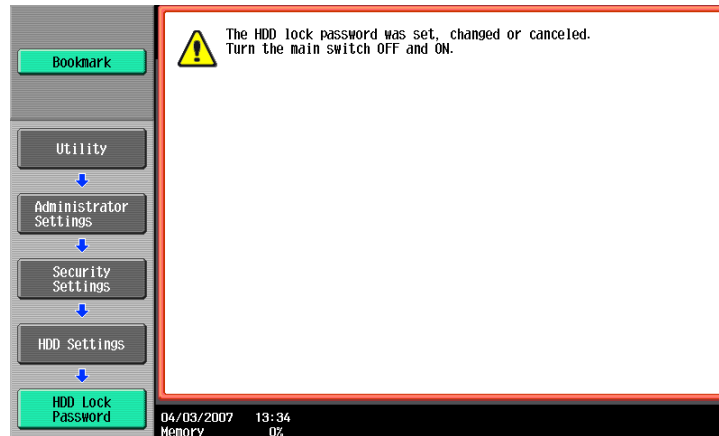
- Press the [C] key to clear all characters.
- Touch [Delete] to delete the last character entered.
- Touch [Shift] to show the upper case/symbol screen.
- Touch [Cancel] to go back to the HDD Settings screen.

- 7 Touch [OK].

? What happens if there is a mismatch in the HDD Lock Passwords?

- If there is a mismatch in the HDD Lock Passwords, a message appears that tells that there is a mismatch in the HDD Lock Passwords. Perform steps 4 through 7 once again.

- 8 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.

**Note**

NEVER forget the HDD Lock Password set through the above procedure. The HDD Lock Password must be entered when changing canceling the HDD Lock Password.

2.6.3 Setting the Encryption Key (encryption word)



Note

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 switch are turned on and off:

Turn off the sub power switch → Turn off the main power switch → Turn on the main power switch → Turn on the sub power switch

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.

<Setting can be made only from the control panel>

- ✓ For the procedure to call the HDD Settings menu to the display, see steps 1 and 2 of "[Setting the HDD Lock Password](#)" on page 2-18.

- 1 Call the HDD Settings to the screen from the control panel.
- 2 Touch [HDD Encryption Setting].



- 3 A message appears that confirms whether or not the setting of the Encryption Key is to be continued. Select [Yes] and touch [OK].



- 4 Enter the new 20-digit Encryption Key from the keyboard and keypad.



- Press the [C] key 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].

? What happens if the Encryption Key entered does not meet the requirements of the Password Rules?

→ If the Encryption Key entered does not comply with the Password Rules, a message appears that tells that the Encryption Key entered cannot be used. Enter the correct Encryption Key. For details of the Password Rules, see "[Password Rules](#)" on page 1-8.

→ To change the Encryption Key, see "[Changing the Encryption Key](#)" on page 2-30.

- 6 To prevent entry of a wrong Encryption Key, enter the 20-digit Encryption Key once again.



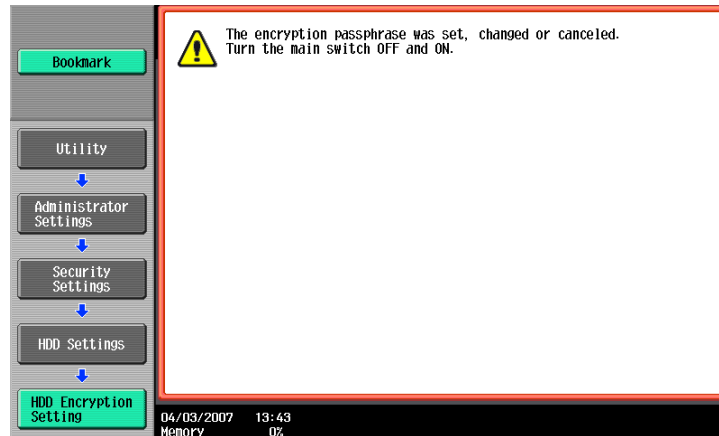
- Press the [C] key to clear all characters.
- Touch [Delete] to delete the last character entered.
- Touch [Shift] to show the upper case/symbol screen.
- Touch [Cancel] to go back to the HDD Settings screen.

- 7 Touch [OK].

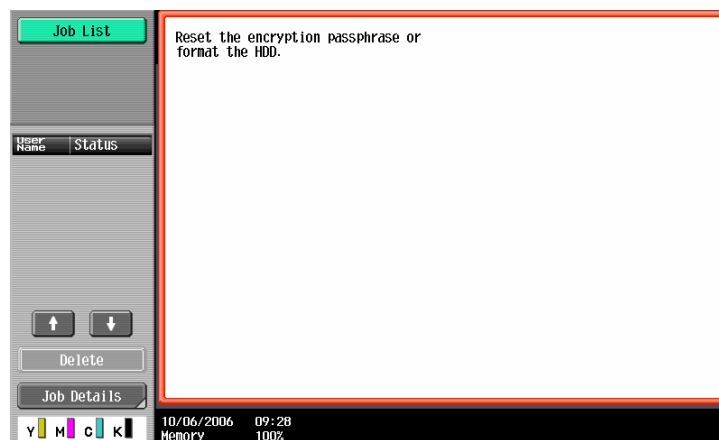
? What if there is a mismatch in the Encryption Keys?

→ If there is a mismatch in the Encryption Keys, a message appears that tells that there is a mismatch in the Encryption Keys. Perform steps 4 through 7 once again.

- 8 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.



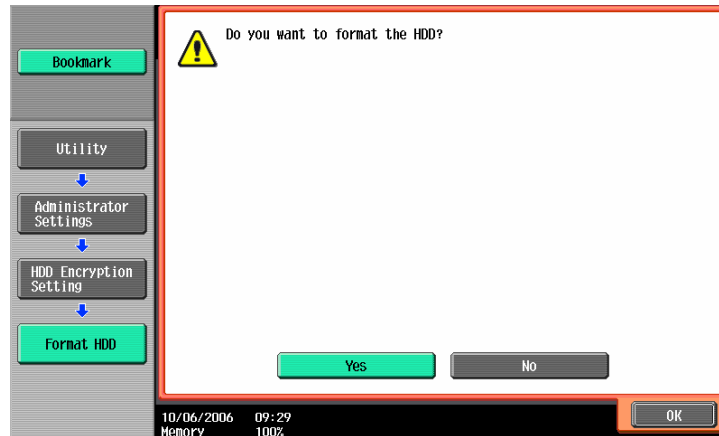
- 9 The following screen appears after the machine has been restarted.



- 10 Call the Administrator Settings to the screen from the control panel.
- For the procedure to call the Administrator Settings to the screen, see "[Accessing the Administrator Settings](#)" on page 2-2.
- 11 Touch [HDD Format].



- 12 A message will appear that confirms whether the HDD may be formatted or not. Select the [Yes] and touch [OK].



? What happens when HDD Format is executed?

- Executing HDD Format erases data in the HDD. It is recommended that important data 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. For the functions whose settings are reset to the default values, see ["Items cleared by HDD Format" on page 1-8](#).

- 13 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.



- To make the setting of [Encryption Priority] or [Overwrite Priority], go to step 14.

? What is the difference between Encryption Priority and Overwrite Priority?

- [Encryption Priority] refers to writing of data in HDD with an enhanced encryption strength. It is recommended that [Encryption Priority] be selected to achieve a greater effect of encryption.
- [Overwrite Priority] refers to writing of data in HDD through the standard encryption technique.
- [Encryption Priority] is the default setting.

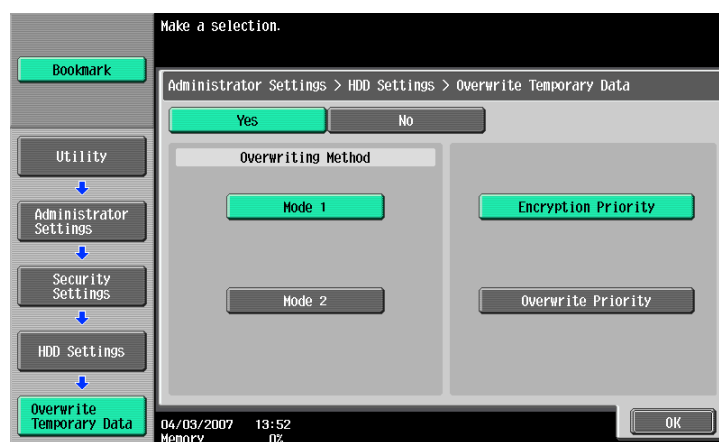
- 14 Call the HDD Settings menu to the screen from the control panel.

- For the procedure to call the HDD Settings menu to the display, see steps 1 and 2 of ["Setting the HDD Lock Password" on page 2-18](#).

15 Touch [Overwrite Temporary Data].



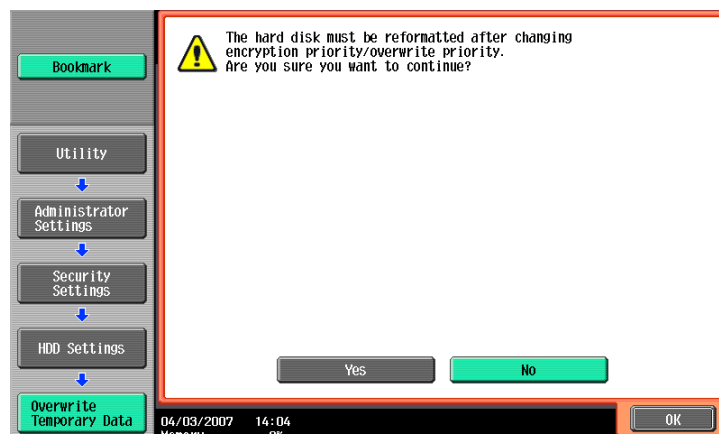
16 Touch [Encryption Priority] or [Overwrite Priority].



17 Touch [OK].

- If the setting has been changed in step 16, the screen shown in step 18 will appear. Perform HDD Format.

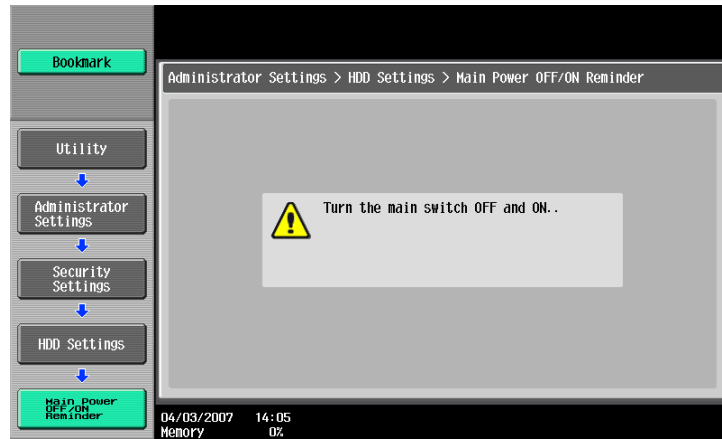
18 A message appears requesting confirmation of the execution of HDD format. Select [Yes] and touch [OK].



? What happens when HDD Format is executed?

- Executing HDD Format erases data in the HDD. It is recommended that important data 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. For the functions whose settings are reset to the default values, see ["Items cleared by HDD Format" on page 1-8.](#)

- 19 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.



2.6.4 Changing the Encryption Key



Note

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 switch are turned on and off:

Turn off the sub power switch → Turn off the main power switch → Turn on the main power switch → Turn on the sub power switch

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.

<Setting can be made only from the control panel>

- ✓ For the procedure to call the Encryption Key entry screen to the display, see steps 1 through 3 of "[Setting the Encryption Key \(encryption word\)](#)" on page 2-24.

- 1 Call the Encryption Key entry screen to the display.
- 2 Enter the currently registered 20-digit Encryption Key from the keyboard and keypad.



- Press the [C] key 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 the [Edit] and touch [OK].

? What if there is a mismatch in the Encryption Keys?

- If there is a mismatch in the Encryption Keys, a message appears that tells that there is a mismatch in the Encryption Keys. Enter the correct Encryption Key once again.

- 4 Enter the new 20-digit Encryption Key from the keyboard and keypad.



- Press the [C] key 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].

? What happens if the Encryption Key entered does not meet the requirements of the Password Rules?

- If the Encryption Key entered does not comply with the Password Rules, a message appears that tells that the Encryption Key entered cannot be used. Enter the correct Encryption Key. For details of the Password Rules, see "[Password Rules](#)" on page 1-8.

- 6 To prevent entry of a wrong Encryption Key, enter the 20-digit Encryption Key once again.



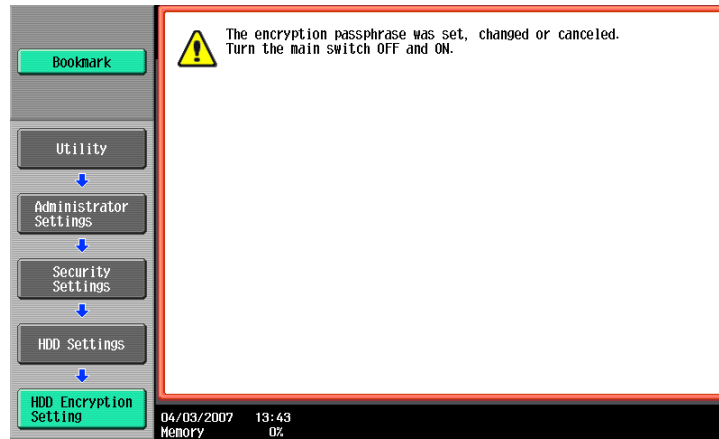
- Press the [C] key to clear all characters.
- Touch [Delete] to delete the last character entered.
- Touch [Shift] to show the upper case/symbol screen.
- Touch [Cancel] to go back to the HDD Settings screen.

- 7 Touch [OK].

? What if there is a mismatch in the Encryption Keys?

- If there is a mismatch in the Encryption Keys, a message appears that tells that there is a mismatch in the Encryption Keys. Perform steps 4 through 7 once again.

- 8 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.



2.7 Overwrite All Data Function

When access to the Administrator Settings by the Administrator of the machine via the control panel 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 stored in all spaces of the HDD. The function also resets all passwords saved in the NVRAM to factory settings, preventing leak of data. For details of items that are cleared by the Overwrite All Data function, see "[Types of Data Cleared by Overwrite All Data Function](#)" on page 1-8.

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.

2.7.1 Setting the Overwrite All Data function



Note

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 switch are turned on and off:

Turn off the sub power switch → Turn off the main power switch → Turn on the main power switch → Turn on the sub power switch

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.

Performing Overwrite All Data deletes the currently set External Server. Set the External Server again. For the procedure to set the External Server, see "[Setting the External Server](#)" on page 2-10.

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

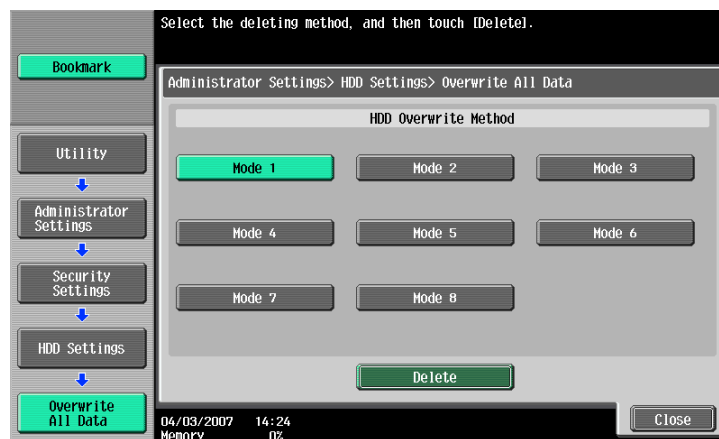
<Setting can be made only from the control panel>

- ✓ For the procedure to call the HDD Settings menu to the display, see steps 1 and 2 of "[Setting the HDD Lock Password](#)" on page 2-18.

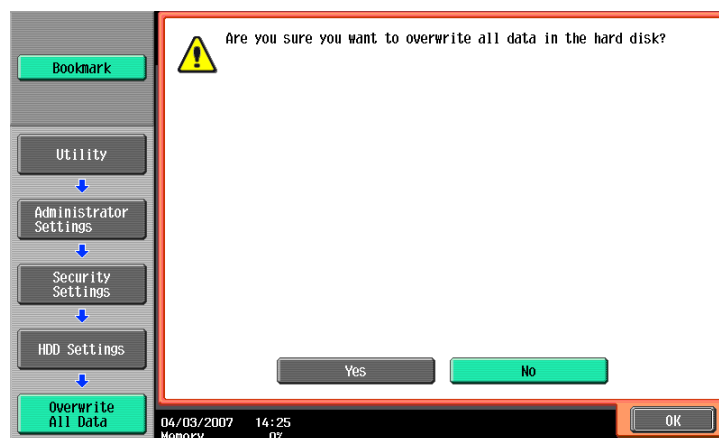
- 1 Call the HDD Settings to the screen from the control panel.
- 2 Touch [Overwrite All Data].



- 3 Select the desired mode and touch [Delete].



- 4 A message appears that prompts you to confirm whether you want to overwrite all data. Select [Yes] and touch [OK].



- 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.

**Note**

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 more details, consult the Service Representative.

2.8 S/MIME Communication Setting Function

When access to the Administrator of the machine by 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.



Note

Be sure to set [Always add signature] or [Select when sending] for Digital Signature.

2.8.1 Setting the S/MIME Communication



Note

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

For encryption strength, 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 strength that is the strongest of all compliant with the currently used mail software.



Detail

Each encryption strength code represents the following.

Name: encryption algorithm: encryption key length

3DES: 3 key triple DES: 168 bits

AES-128: AES: 128bit

AES-192: AES: 192bit

AES-256: AES: 256bit

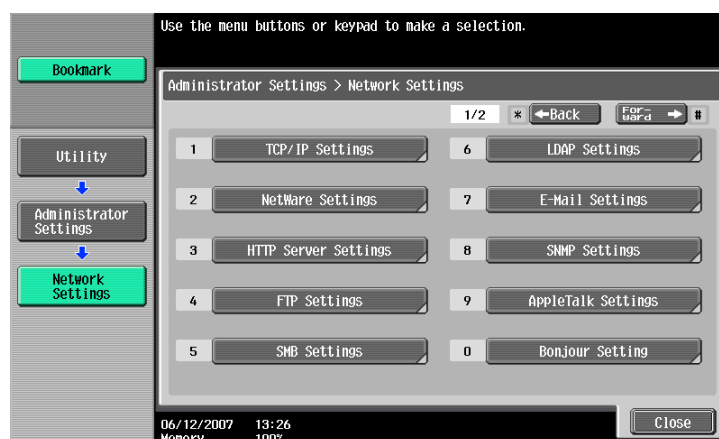
<Setting can be made only from the control panel>

- ✓ For the procedure to call the Administrator Settings to the display, see "[Accessing the Administrator Settings](#)" on page 2-2.

1 Call the Administrator Settings to the screen from the control panel.

2 Touch [Network Settings].

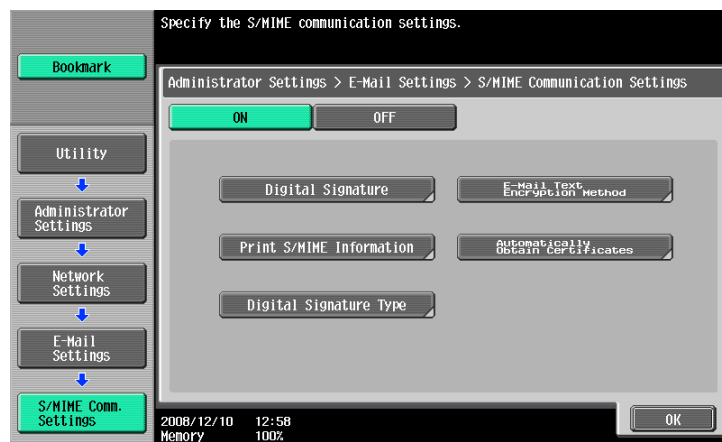
3 Touch [E-Mail Settings].



- 4 Touch [S/MIME Communication Settings].



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



- 6 Select encryption strength and touch [OK].

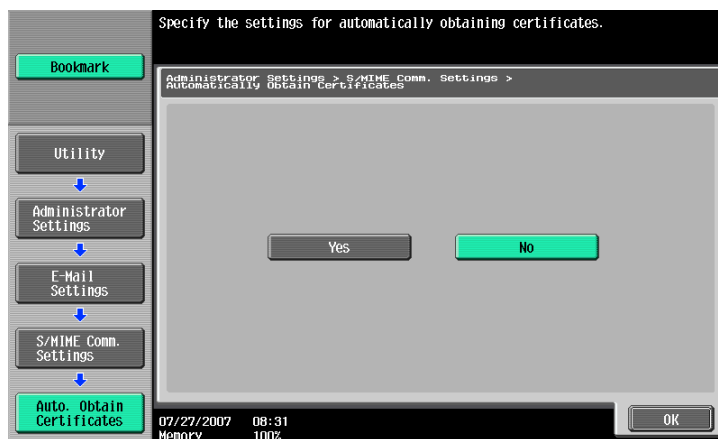


- 7 Touch [OK].

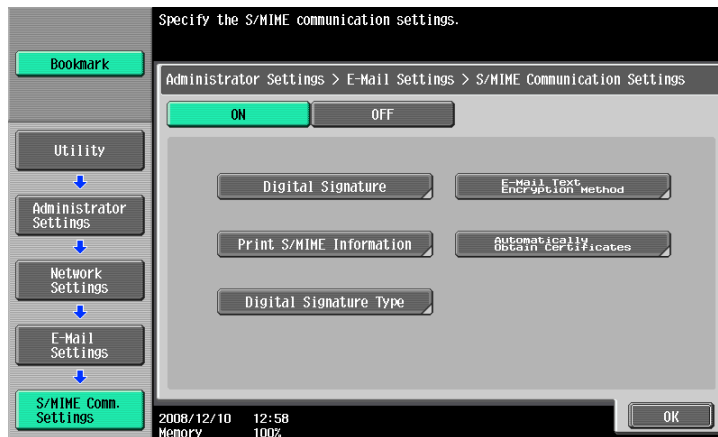
8 Select [Automatically Obtain Certificates].



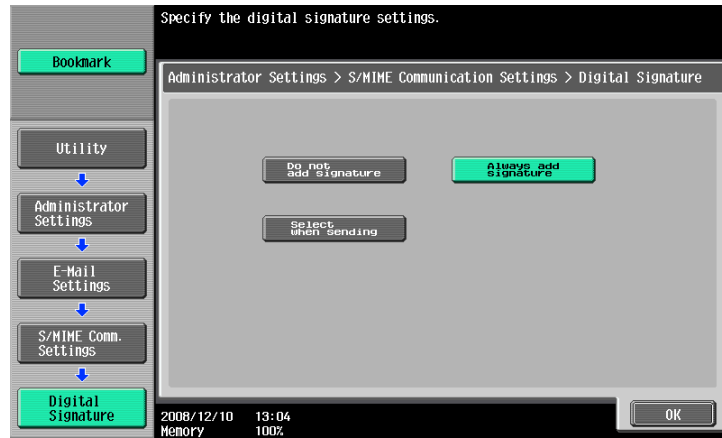
9 Select [NO] and touch [OK].



10 Select [Digital Signature].



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



- 12 Touch [OK].

2.9 TCP/IP Setting Function

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

2.9.1 Setting the IP Address



...

Note

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.

<Setting can be made only from the control panel>

- ✓ For the procedure to call the Network Settings menu to the display, see steps 1 and 2 of "[Setting the S/MIME Communication](#)" on page 2-36.
- 1** Call the Network Settings to the screen from the control panel.
- 2** Touch [TCP/IP Settings].
- 3** Touch [IPv4 Setting].
- 4** Touch [Manual Input].
- 5** Select [IP Address] and set the IP Address.
 - If [Auto Input] has been 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].

2.9.2 Registering the DNS Server



Note

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.

<Setting can be made only from the control panel>

- ✓ For the procedure to call the TCP/IP settings screen to the display, see steps 1 through 3 of "[Setting the IP Address](#)" on page 2-40.

- 1 Call the TCP/IP settings screen to the display from the control panel.
- 2 Make the various settings for the DNS Server.
 - If [Enable] is selected from the DNS Server Auto Obtain and DNS Domain Auto Obtain, the DNS Server Address and DNS Domain Name are automatically acquired.
- 3 Touch [OK].

2.10 NetWare Setting Function

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

2.10.1 Making the NetWare Setting



...

Note

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.

<Setting can be made only from the control panel>

- ✓ For the procedure to call the Network Settings menu to the display, see steps 1 and 2 of "[Setting the S/MIME Communication](#)" on page 2-36.

- 1 Call the Network Settings to the screen from the control panel.
- 2 Touch [NetWare Settings].
- 3 Make the necessary settings.
- 4 Touch [OK].

2.11 SMB Setting Function

When access to the Administrator of the machine by the Administrator Settings is authenticated, the machine enables setting of the NetBIOS Name.

2.11.1 Setting the NetBIOS Name



...

Note

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.

<Setting can be made only from the control panel>

- ✓ For the procedure to call the Network Settings menu to the display, see steps 1 and 2 of "[Setting the S/MIME Communication](#)" on page 2-36.

- 1 Call the Network Settings to the screen from the control panel.
- 2 Touch [SMB Settings].
- 3 Touch [Print Settings].
- 4 Touch [NetBIOS Name].
- 5 Make the necessary settings.
- 6 Touch [OK].

2.12 E-Mail Setting Function

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

2.12.1 Setting the SMTP Server (E-Mail Server)

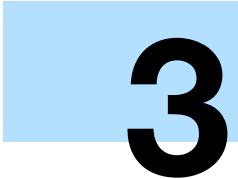
**Note**

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.

<Setting can be made only from the control panel>

- ✓ For the procedure to call the Network Settings menu to the display, see steps 1 and 2 of "[Setting the S/MIME Communication](#)" on page 2-36.

- 1 Call the Network Settings to the screen from the control panel.
- 2 Touch [E-Mail Settings].
- 3 Touch [E-Mail TX (SMTP)].
- 4 Make the necessary settings.
- 5 Touch [OK].



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 stored in the PKI Encrypted Document User Box of this machine, the print data of the user in question stored 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.



Detail

Contact the Administrator of the machine if the server is not registered.

3.1.1 User authentication using the IC card

If a document is stored in the PKI Encrypted Document User Box, select any desired login method.

<For control panel>

Login Method	Description
[Begin Printing]	Prints only the PKI Encrypted document of the corresponding user. The user operation mode screen is not called to the screen.
[Print & Login]	The user operation mode screen is called to the screen after the PKI Encrypted document of the corresponding user is printed.
[Access] or [Login]	If [Access] or [Login] is selected, only the ordinary login procedure is applicable and no PKI Encrypted document are printed.



Note

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.

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.



Reminder

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 [Login] 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 "[Accessing the Encrypted document](#)" on page 3-5.

The number of consecutive failure count for the locking depends on the setting made on the IC card side.

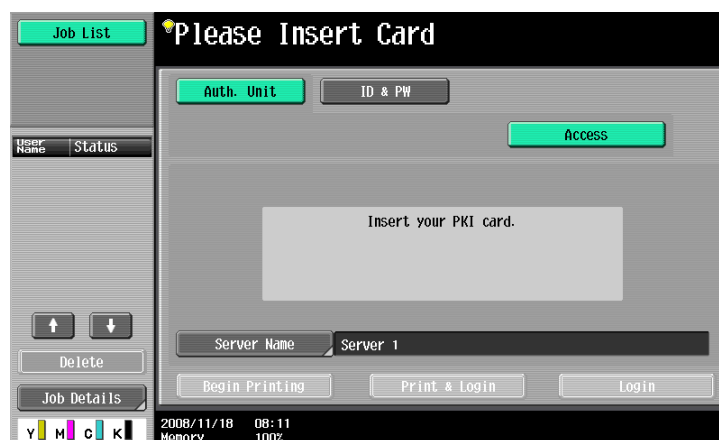
If authentication fails, the permissible authentication failure count appears.

<Setting can be made only from the control panel>

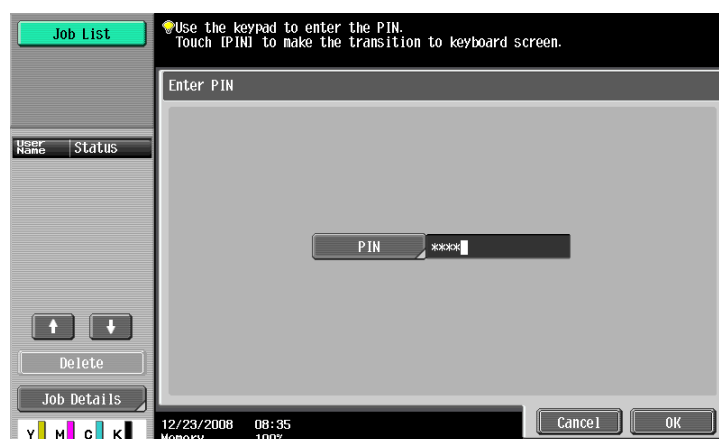
- 1 Insert the IC card into the IC card reader connected to the machine.



- The following screen appears if any document is stored in the PKI Encrypted Document User Box.



- 2 Make sure that the IC card is recognized, press [Access] or touch [Login]. If a document is stored in the PKI Encrypted Document User Box, select any desired login method.
- 3 Enter the PIN code registered in the IC card from the 10-key pad. If the PIN code includes any character other than numerals, touch [PINCODE].



- Touch [Cancel] to go back to the screen shown in step 2.
- Go to step 5 if the PIN code consists only of numerals.

- 4 Enter the PIN code from the keyboard or 10-key pad and touch [OK].



- Press the [C] key 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 3.
- 5 Touch [OK].
- 6 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 stored in the machine. The PKI encrypted document stored in the machine can be decrypted only by an encrypted IC card, which makes this function just right for printing highly confidential documents.

3.2.1 Accessing the Encrypted document



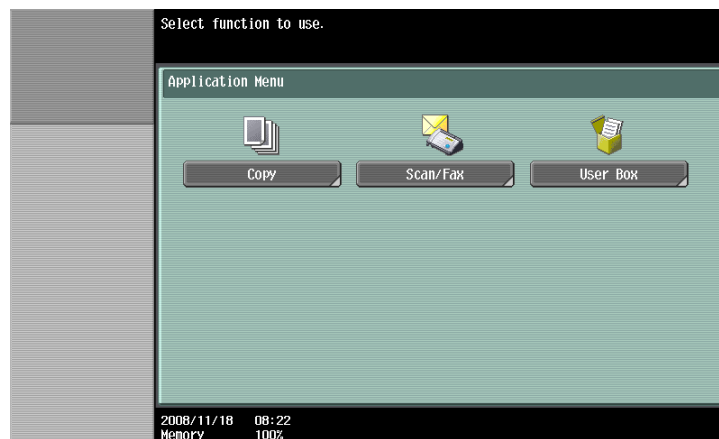
Note

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.

<Setting can be made only from the control panel>

✓ For the logon procedure, see "[User authentication using the IC card](#)" on page 3-2.

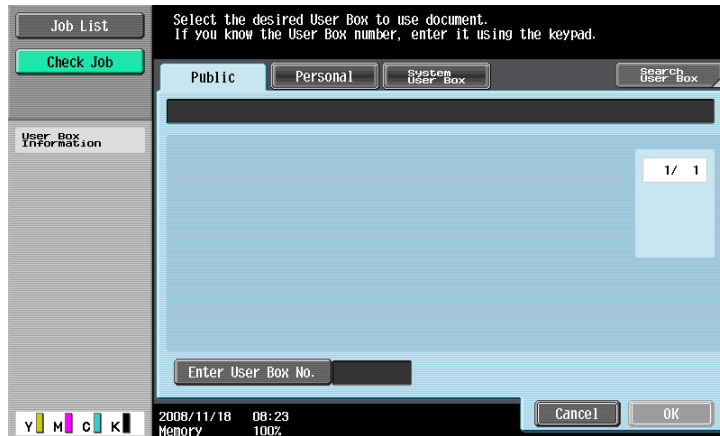
- 1 Using the IC card, log on to the machine.
- 2 Press the [Box] key.
- 3 Touch [Use Box].



- 4 Touch [Use Document].



- 5 Touch [System User Box] tab.



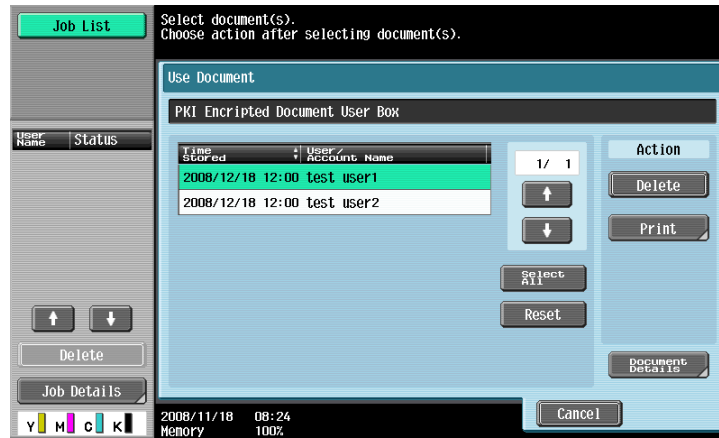
- 6 Select [Encrypted document User Box] and touch [OK].



- 7 Select [PKI Encrypted Document User Box] and touch [OK].



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



- To Delete PKI Encrypted Document, select [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.



Note

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

3.3.1 Scan to Me procedure



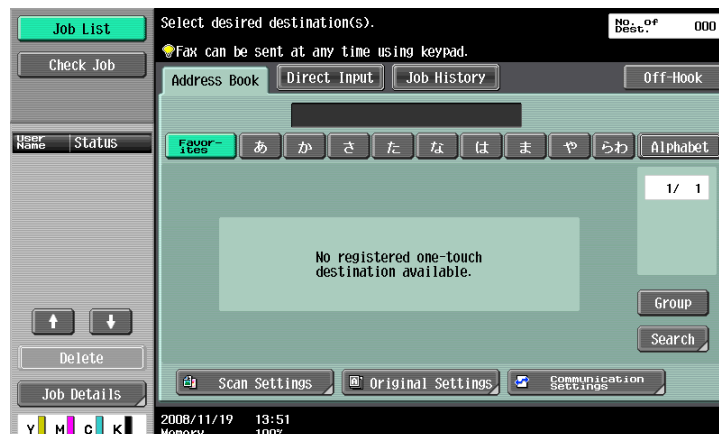
Note

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.

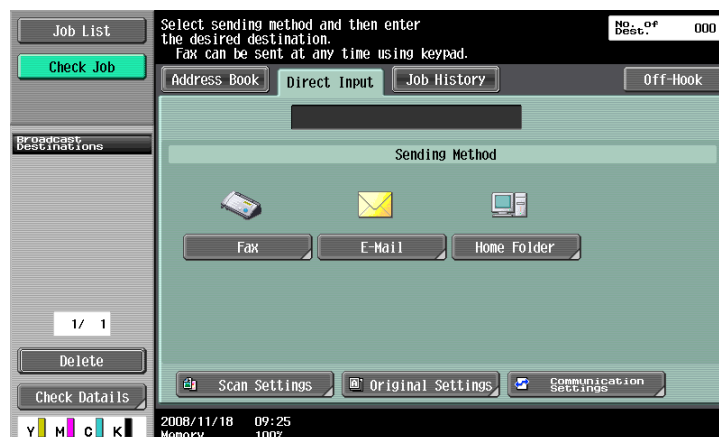
<Setting can be made only from the control panel>

- ✓ For the logon procedure, see "[User authentication using the IC card](#)" on page 3-2.

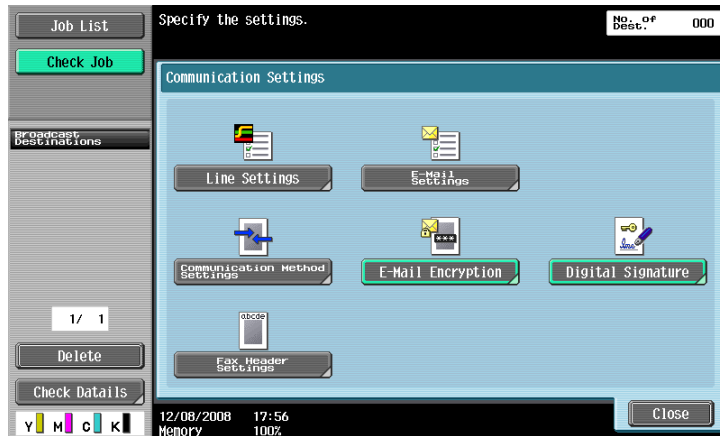
- 1 Using the IC card, log on to the machine.
- 2 Press the [Fax/Scan] key.
- 3 Touch [Direct Input] tab.



- 4 Touch [Communication Settings].



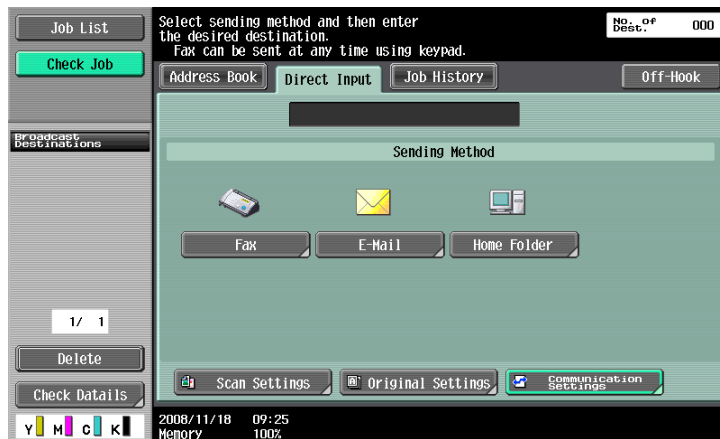
- 5 Select [E-Mail Encryption] and [Digital Signature].



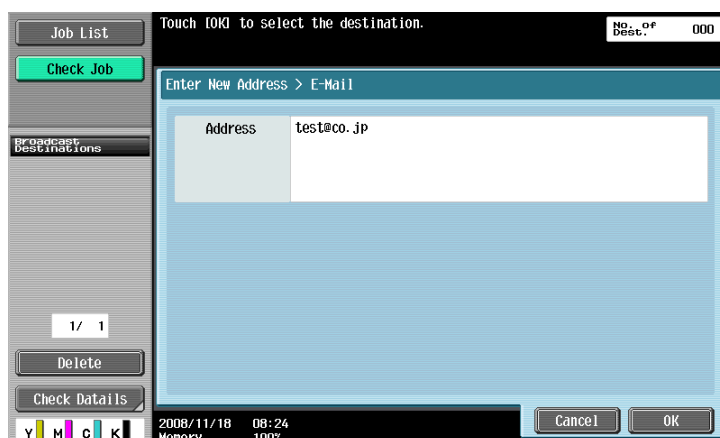
- If [E-Mail Encryption] and [Digital Signature] are selected after the destination has been set, the set destination is canceled, making it necessary to set the destination once again.

- 6 Touch [Close].

- 7 Touch [E-mail].



- 8 Check that the destination is your e-mail address and then touch [OK].



- 9 Touch [START].



Note

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>

Copyright