Océ User's Guide

VarioLink 3622/4222/5022

[Security Operations]

2009.01
Ver. 1.06

Océ-Technologies B.V.

Copyright

Océ-Technologies B.V. makes no representation or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose.
Further, Océ-Technologies B.V. reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation to notify any person of such revision or changes.

Contents

1 Security

2 Administrator Operations

3 User Operations

4 Application Software

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 VarioLink 3622/4222/5022 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. 1.06) describes bizhub 501/421/361/ineo 501/421/361/VarioLink 3622/4222/5022 Multi Function Peripheral Control Software (A0R50Y0-0100-G00-11, BIOS control controller: A0R50Y0-1D00-G00-10).

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 VarioLink 3622/4222/5022 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.

The Web Connection functions can be used only if the setting is made to accept "Cookie."

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 and its Checksum, BIOS and its 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 upgrade of the MFP controller Firmware is necessary and perform the Firmware upgrade. Explain to the Administrator of the machine that upgrade of the BIOS Firmware is necessary and perform the Firmware upgrade.	□
	Set CE Authentication to [ON] and set the CE Password.	□
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 data has been backed up by the Administrator of the machine using the HDD Backup Utility if necessary.	□
	Check that Release Time Settings has been set to 5 min. or more by the Administrator of the machine.	□
	Check that the HDD Lock Password , has been set by the Administrator of the machine.	□
	Check that the Flash Memory Lock Password has been set by the Administrator of the machine.	
	Check that User Authentication has been set to [ON (MFP)] or [ON (External Server)] (Active Directory only) by the Administrator of the machine.	□
	Check that the self-signed certificate for SSL communications has been registered by the Administrator of the machine.	□
	Check that data has been restored by the Administrator of the machine using the HDD Backup Utility if necessary.	□
	Let the Administrator of the machine set Enhanced Security Mode to [ON].	□
	The languages, in which the contents of the User's Guide Security Operations have been evaluated, are Japanese and 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				
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 **"Enhancing the Security Function" on page 2-9**.

Setting the Enhanced Security Mode to [ON] will enhance the authentication function. Access control is then provided through password authentication for any access to the Administrator Settings, User Authentication mode, Account Track mode, User Box, a User Box data file and a Secure Print Document file. Access is thereby granted only to the authenticated user.

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 1-9**.

If a wrong password is entered, during password authentication, a predetermined number of times (once to three 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 used of the machine.

To cancel the password entry operation prohibited condition, the Administrator must perform the Release Setting. When the Administrator performs the Release Setting for the operation prohibited condition, a sound operation control in utmost security is achieved under the control of the Administrator.

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. Setting the Flash Memory Lock Password provides the following security function. That is, even if the flash memory is illegally replaced with another, the flash memory authentication function prohibits access to the flash memory when the Flash Memory Lock Password is not set or there is a mismatch in the passwords. In addition, should the flash memory be removed unawares, the Flash Memory Lock Password locks the flash memory protecting data contained in the flash memory. Furthermore, by mounting the optional Security Kit SC-505 and setting the Image Data Encryption Passphrase, the image data stored in the HDD is encrypted, thereby protecting the image data in the HDD. Note, however, that the HDD Lock Password, Flash Memory Lock Password, and Image Data Encryption Passphrase cannot prevent the HDD and flash memory from being physically removed.

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 and flash memory 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 1-11**.

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 at the time of authentication by the Enhanced Security Mode.

<Administrator Settings>

- Authentication of Administrator Settings is successful.

<User Authentication Mode>

- User Authentication mode is successful.
- Release of Prohibited Functions When Authentication Error is executed.

<Account Track Mode>

- Account Track mode is successful.
- Release of Prohibited Functions When Authentication Error is executed.

<Secure Print Document>

- Authentication of Secure Print Document is successful.
- Release of Prohibited Functions When Authentication Error is executed.

<Box>

- Authentication of User Box is successful.
- Authentication for execution of change of User Box Name and User Box Password is successful.
- Release of Prohibited Functions When Authentication Error is executed.

<SNMP Password (auth-Password, priv-Password)>

- Authentication of SNMP is successful.
- Release of Prohibited Functions When Authentication Error is executed.

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.

- Image files stored by Secure Print
- Image files stored in Personal User Box, Public User Box and Group User Box

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.

- Image files stored by Secure Print
- Image files stored in Personal User Box, Public User Box and Group User Box
- Image files of a job in the queue
- Image files other than Secure Print file and User Box file
- Data files left in the data space used as image files
- Temporary data files generated during print image file processing
- Destination recipient data (e-mail address, telephone number)

This machine offers specific functions as data protection methods: the SSL function that ensures confidentiality of images transmitted and received over the network and the S/MIME function that is used for encrypting image files.

When transmitting and receiving highly confidential image data among different pieces of IT equipment within an office LAN, the machine carries out communications with the correct destination via encrypted and reliable paths, assuming an office environment that responds to most stringent security requirements.

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, Image Data Encryption Passphrase, Flash Memory Lock Password, auth-Password and priv-Password appropriately so that they may not be leaked. These passwords should not be ones that can be easily guessed. The user, on the other hand, should control the User Box Password, Secure Print Password, and User Password appropriately so that they may not be leaked. Again, these passwords should not be ones that can be easily guessed. For the Public User Box shared among a number of users, the User Box Password should be appropriately controlled so that it may not be leaked to anyone who is not the user of the Public User Box.

<To Achieve Effective Security>

- Make absolutely sure that only the Administrator knows the Administrator Password, HDD Lock Password, Image Data Encryption Passphrase, Flash Memory Lock Password, auth-Password and priv-Password.
- The Administrator must change the Administrator Password, HDD Lock Password, Image Data Encryption Passphrase, Flash Memory Lock Password, auth-Password and priv-Password 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, Account Password, HDD Lock Password, Image Data Encryption Passphrase, Flash Memory Lock Password, auth-Password and priv-Password. Do not set any number that consists of 7 digits or less.
- If a User Password or User Box Password has been changed, the Administrator should have the corresponding user change the password as soon as possible.
- The Administrator should change the Account Password set for each account at regular intervals and, should one be changed, he or she should immediately inform users who implement Account Track of the new Account Password.
- If the Administrator Password has been changed by the Service Engineer, the Administrator should change the Administrator Password as soon as possible.
- The Administrator should have users ensure that the User Authentication, Secure Print Document, and User Box are known only by the user concerned.
- The Administrator should have users who implement Account Authentication ensure that the Account Password set for the account is known by the users implementing Account Authentication only.
- The Administrator should make sure that only the users who share a Public User Box and Group User Box know the password set for it.
- The Administrator should have users change the passwords set for the User Authentication and User Box at regular intervals.
- The Administrator should make sure that any user does not set any number that can easily be guessed from birthdays, employee identification numbers, and the like for the passwords set for the User Authentication, Secure Print Document, and User Box.

Network Connection Requirements for the Machine

Packets being transmitted over the LAN installed in the office, in which the machine is installed, should be protected from unauthorized manipulation. 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.
- Configure the LAN installed in the office, in which the machine is installed, by using a switching hub and other devices to ensure that the packets are protected from unauthorized manipulation.
- Provide an appropriate network control at all times to make sure that no other copying machine is connected without prior notice to the office LAN to which this machine is connected.

User information control server control requirements

The server administrator is required to apply patches and control accounts for the user information control server connected to the LAN within the office, in which this machine is installed, to ensure operation control that achieves appropriate access control.

Security function operation setting operating requirements

The Administrator should make sure of correct operation control so that the machine is used with the Enhanced Security Mode set to [ON].

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 Secure Print Document file, User Box, and User Box file.
- The Administrator of the machine should set the HDD Lock Password and Flash Memory Lock Password according to the environment in which this machine is used. If the optional Security Kit SC-505 is mounted on the machine, the Administrator should also set the Image Data Encryption Passphrase.

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.

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 User Password, Administrator Password, Account Password, User Box Password, Secure Print Password, HDD Lock Password, Flash Memory Lock Password, and Image Data Encryption Passphrase. For the Administrator Password, HDD Lock Password, Flash Memory Lock Password, and Image Data Encryption Passphrase, 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	8 digits	• 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	• Numeric characters: 0 to 9 • Alpha characters: upper and lower case letters • Symbols: !, #, $, %, &, ', *, +, -, ., /, =, <, @, ^, _, `, {, |, }, ~, ? Selectable from among a total of 84characters *Selectable from among a total of 83 characters as HDD Lock Password. "?" is not selectable.
Flash Memory Lock Password		
Image Data Encryption Passphrase		
User Password	8 digits or more	• Numeric characters: 0 to 9 • Alpha characters: upper and lower case letters • Symbols: !, #, $, %, &, ', (,), *, ,, -, ., /, :, ;, <, =, >, ?, @, [, \,], ^, _, `, {, |, }, ~, ", +, SPACE Selectable from among a total of 95 characters
Account Password	8 digits	
User Box Password		
Secure Print Password		
SNMP Password • auth-Password • priv-Password	8 digits or more	• Numeric characters: 0 to 9 • Alpha characters: upper and lower case letters • Symbols: !, #, $, %, &, ', (,), *, ,, -, ., /, :, ;, <, =, >, ?, @, [,], ^, _, `, {, |, }, ~, ", + Selectable from among a total of 93 characters

Detail

Note that use of the characters "","" "+," and "space" may be partly limited.

Precautions for Use of Various Types of Applications

When Web Connection or an application of various other types is used, the password control function of the application stores the password that has been entered in your PC. If you want the password not stored, disable the password control function of the application.
When using the Web Connection or an application of various other types, use one that shows "*" or "●" for the password entered.

Internet Explorer or other type of web browser, "SSL v3" or "TLS v1" should be used, not "SSL v2," for the SSL setting.

Encrypting communications

The following are the cryptographic algorithms of key exchange and communications encryption systems supported in generation of encryption keys.

- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA

Note

No algorithms can be selected during generation of encryption keys. SSL v3 is automatically selected for the SSL setting according to the application and browser. Do not therefore change the setting manually to SSL v2.

Use the following browsers to ensure SSL encryption communication with appropriate strength. Use of any of the following browsers achieves SSL encryption communication that ensures confidentiality of the image data transmitted and received.

Windows 98, Me, NT4.0, 2000, XP, Server2003

- Recommended is Microsoft "Internet Explorer 6" or later.
  If "Internet Explorer 5.x" is used, Microsoft XML parser "MSXML 3.x" or later must be installed.
- Recommended is Netscape Navigator 7.02 or later.
- Recommended is Mozilla Firefox 1.0 or later.

Macintosh MacOS 8.x, 9.x, MacOS X

- Recommended is Netscape Navigator 7.02 or later.
- Recommended is Mozilla Firefox 1.0 or later.

Linux

- Recommended is Netscape Navigator 7.02 or later.
- Recommended is Mozilla Firefox 1.0 or later.

SSL encryption communication with confidentiality properly maintained can be achieved in image data transmitted and received in any of the following applications.

- Box Operator
- HDD TWAIN
- Direct Print
- HDD Backup Utility

Detail

SSL encryption communication is not applicable to transmission of Secure Print in Direct Print.

IPP printing

IPP (Internet Printing Protocol) is a function that allows Secure Print Documents and image data stored in boxes to be printed via the Internet by using the HTTP (HyperText Transfer Protocol) of the TCP/IP Protocol. IPPS (IPP over SSL/TLS) is the type of IPP that performs the SSL encryption communication.

<IPP setting on Windows Vista>

Windows Vista, which offers enhanced security functions, gives a certificate error message if the SSL certificate is one that is not issued by a certification body. In such cases, it becomes necessary to register with Windows Vista the certificate of this machine as that issued by a reliable party for the computer account.

First, register Host Name and IP address of this machine in the DNS server in advance. Then, in TCP/IP Settings of Web Connection, set the DNS Host Name and DNS Default Domain Name registered with the DNS server.

It should also be noted that, for the certificate to be imported, a certificate for SSL encryption communication should be registered in Web Connection and exported in advance as the certificate including the public key.

1. From "Continue to this website," call the Web Connection window to the screen.
2. Click "Certificate Error" to display the certificate. Then, click "Install Certificate" to install the certificate.
3. Display the physical stores. Then, deploy the certificate, which has earlier been exported, in "Local Computer" of "Trusted Root Certification Authorities" to thereby import the certificate.

<IPPS printing settings in Windows Vista>

Through additional printer setting, type "https://Host Name.Domain Name/ipp."

For [Host Name] and [Domain Name], specify the names set with the DNS server.

<Installing printer driver>

To perform IPP printing, the printer driver must be installed. From "Add Printer Wizard," select "Connect to a printer on the Internet or on your intranet" and type the URL of this machine in the following format in the "URL" field.

http:// <IP address of this machine> /ipp
E.g.: If the machine IP address is 192.168.1.20
Type http://192.168.1.20/ipp

To set IPPS printing:
Type https:// <IP address of the machine> /ipp.

Detail
The printer, for which the settings have been made, can be used in the same manner as the ordinary local printer.

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
User registration data	Deletes all user-related data that has been registered
Box registration data/file	Deletes all User Box-related information and files saved in User Box
Secure Print ID/Password/file	Deletes all Secure Print Document-related information and files saved
Image files	• Image files saved other than Secure Print Document files, ID & Print files and User Box files • Image files of jobs in job queue state
Destination recipient data files	Deletes all destination recipient data including e-mail addresses and telephone numbers
HDD Lock Password	Clears the currently set password
Flash Memory Lock Password	Clears the currently set password
Image Data Encryption Passphrase	Clears the currently set Image Data Encryption Passphrase
Administrator Password	Clears the currently set password, resetting it to the factory setting
SNMP Password	Clears the currently set password, resetting it to the factory setting (MAC address)
Account registration data	Deletes all account track-related data that has been registered
S/MIME certificate data	Deletes the currently set S/MIME certificate
SSL certificate	Deletes the currently set SSL certificate
Network Setting	Clears the currently set network settings (DNS Server setting, IP Address setting, SMTP Server setting, NetWare Setting, NetBIOS setting and AppleTalk Printer Name setting), resetting it to the factory setting

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 settings for the machine system and network 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.

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

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.

While you are logging onto the Admin Mode using Web Connection, any operations from the machine’s control panel are disabled.

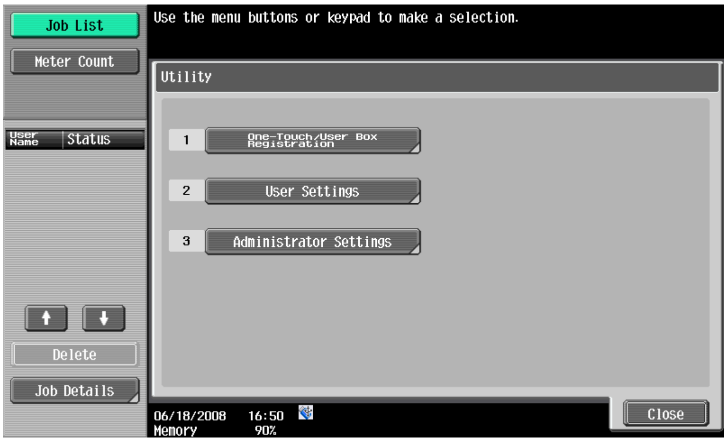
When accessing the Administrator Settings from the control panel, if you have already logged on to the Administrator Settings using Web Connection, the machine displays a message that tells not to turn off the power because of the remote operation being performed and rejects any operation on the control panel. Wait until the message disappears before attempting to access the Administrator Settings once again.

When accessing the Administrator Settings from the control panel, if [Export to the device] operation is being executed using the Data Administrator, the machine displays a message that tells not to turn off the power because of the remote operation being performed and rejects any operation on the control panel. Wait until the message disappears before attempting to access the Administrator Settings once again.

<From the Control Panel>

1 Press the [Utility/Counter] key.

2 Touch [Administrator Settings].

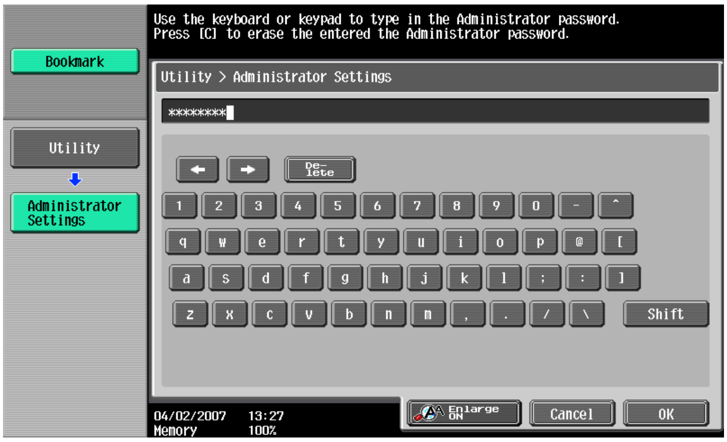


Use the menu buttons or keypad to make a selection.

? 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.



Use the keyboard or keypad to type in the Administrator password.
Press [C] to erase the entered the Administrator password.

Utility > Administrator Settings

****

- 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 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) 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

The Administrator must first make User Authentication settings before he or she can access User Mode. For details of the User Authentication, see "Setting the Authentication Method" on page 2-19.

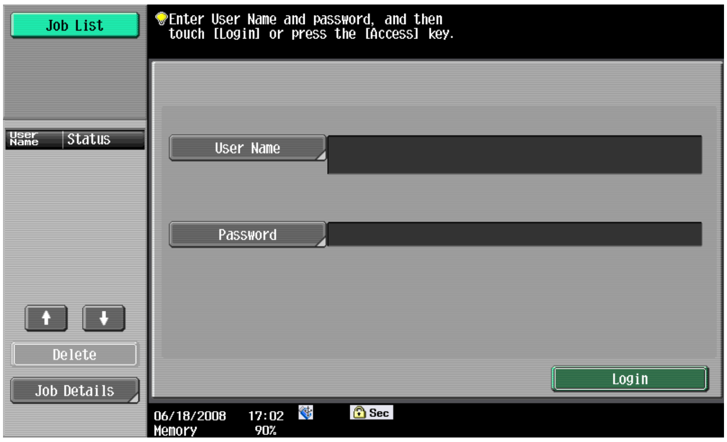
Make sure that none of the general users of the machine will know the Administrator Password.

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.

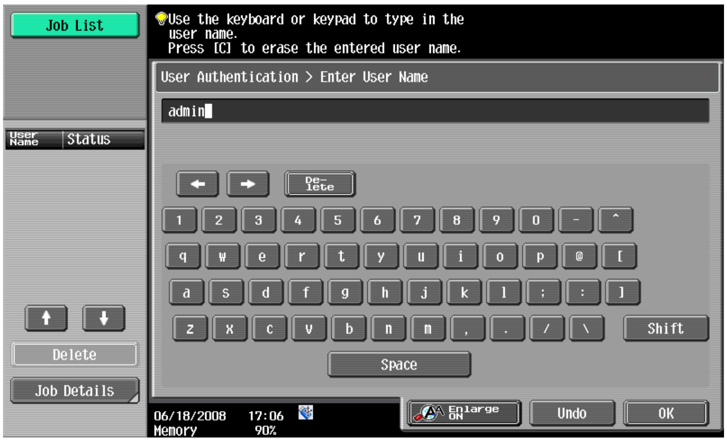
<From the Control Panel>

1 Touch [User Name].



Enter User Name and password, and then touch [Login] or press the [Access] key.

2 Type "admin" in User Name.



Use the keyboard or keypad to type in the user name.
Press [C] to erase the entered user name.

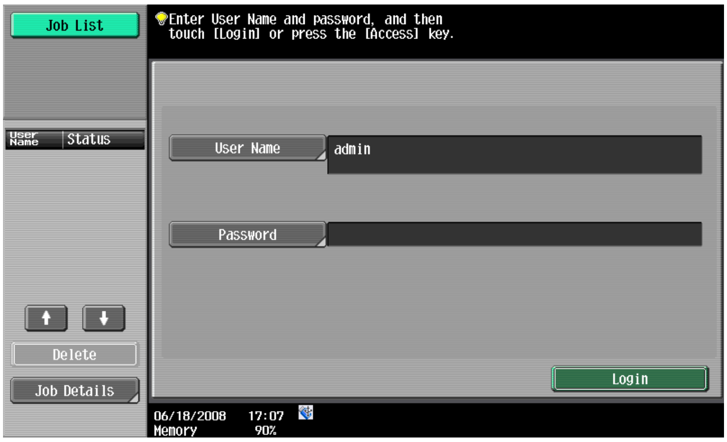
User Authentication > Enter User Name

admin

- Press the [C] key 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.

3 Touch [OK].

4 Touch [Password].

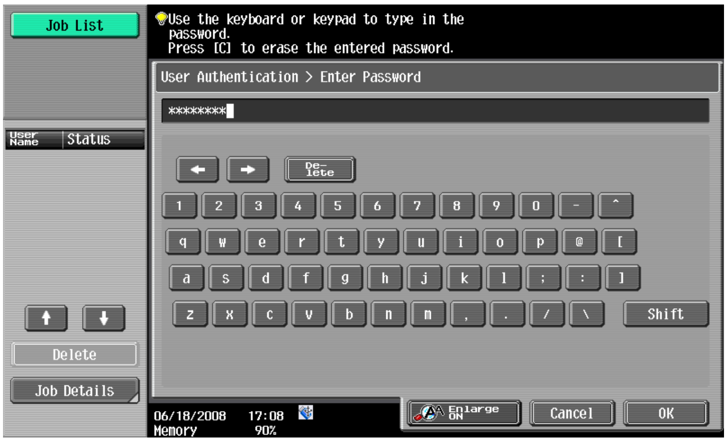


Enter User Name and password, and then touch [Login] or press the [Access] key.

User Name: admin

Password:

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



Use the keyboard or keypad to type in the password.
Press [C] to erase the entered password.

User Authentication > Enter Password

****

- 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 4.

6 Touch [OK].

7 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 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) 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

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

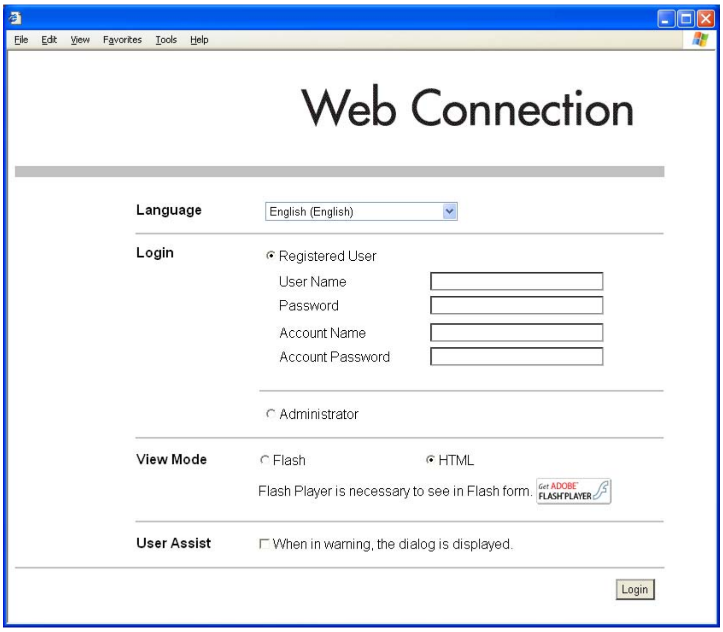
<From Web Connection>

1 Start the Web browser.

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

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

4 Click the Administrator radio button and [Login].



Web Connection

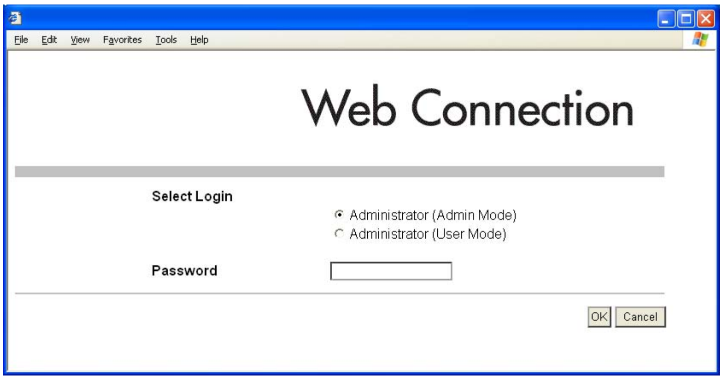
Language: English (English)

Login
● Registered User
User Name
Password
Account Name
Account Password
○ Administrator

View Mode: ○ Flash ● HTML
Flash Player is necessary to see in Flash form. Get ADOBE FLASH PLAYER

User Assist: □ When in warning, the dialog is displayed.

5 Select "Administrator (Admin Mode)" or "Administrator (User Mode)" and enter the 8-digit Administrator Password in the "Password" box.



Web Connection

Select Login
● Administrator (Admin Mode)
○ Administrator (User Mode)

Password

- Administrator (Admin Mode) is a mode, in which settings of the machine can be registered or changed. In this mode, system and network settings can be made.
- Administrator (User Mode) is a mode, in which the same settings as the user authority can be made. For box setting operations, however, the same functions can be set as those of Admin Mode. User Mode also allows jobs to be checked or deleted, which is not possible in Admin Mode.

? What is the Administrator Password used for accessing the Admin Mode via the Web Connection?

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

6 Click the [OK].

? 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. In this case, click [OK] and enter the correct Administrator Password in the "Password" box.

➔ 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) 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

? What if you fail to log on to the Admin Mode?

➔ If you have already logged on to the Admin Mode from the control panel or using Web Connection, the machine displays a message that tells that another administrator has previously logged on and rejects any attempt to log on to the Admin Mode using the Web Connection. Click [OK] and wait for some while before attempting to access the Admin Mode once again.

➔ If [Export to the device] operation is being executed using the Data Administrator, the machine displays a message that tells you cannot log on to the mode because of the remote operation being performed and rejects any attempts to the Admin Mode via the Web Connection. Click [OK] and wait for some while before attempting to access the Admin Mode once again.

? Is it possible to gain access to the Admin Mode while a job is being executed?

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

7 Click the [Logout].

8 Click the [OK].

This allows you to log off from the Admin Mode.

✎...

Note

If you have logged on to the Admin Mode using the Web Connection and if you close the web browser without clicking [Logout], the touch panel of the machine remains locked for 70 sec.

2.2 Enhancing the Security 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 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, User Authentication, Account Track, SNMP authentication, all Secure Print Documents, and all User Boxes. A function is also set that determines whether each password meets predetermined requirements. The security function is thus enhanced in the Enhanced Security Mode.

In advance, HD-509, provided as option, must be loaded and the following settings must first be made before the Enhanced Security Mode is set to [ON].

Note
When a service engineer initializes network, make the settings of the network functions including SSL certificate re-registration and set the Enhanced Security Mode to [ON] again.

Settings to be Made in Advance	Description
Administrator Password	An 8-digit password that meets the Password Rules. The factory setting is "12345678."
User Authentication	Set to either [ON (MFP)] or [ON (External Server)] (Active Directory).
HDD Lock Password	Set the 20-digit HDD Lock Password.
Flash Memory Lock Password	Set the 20-digit Flash Memory Lock Password.
Release Time Settings	Set the release time to 5 min. or more.
Certificate for SSL	Register the self-signed certificate for SSL communications.
Management Function Choice	Calls for setting made by the Service Engineer. For details, ask your Service Representative.
CE Password	
CE Authentication	
HDD	
Operation Ban Release Time	

Detail
Image Data Encryption Passphrase cannot be deleted after enhancing security function. You need to reset the Security mode to delete the key.

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

Function Name	Factory Setting	When Enhanced Security Mode is set to [ON]
Password Rules	Invalid	Enable (not to be changed)
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.
Security Print Access	Mode 1	Mode 2 (not to be changed) * In association with Prohibit Functions When Authentication Error the method is changed from authentication using Secure Print ID and password (Mode 1) to that using the password with the secure document first narrowed down by Secure Print ID (Mode 2).
Public User Access	Restrict	Restrict (not to be changed)
User List	OFF	OFF (not to be changed)
Print Without Authentication	Restrict	Restrict (not to be changed)
User Box Admin. Setting	Restrict	Restrict (not to be changed)
SSL	OFF	ON (not to be changed)
FTP Server	ON	OFF (not to be changed)
SNMPv1/v2c	Read/Write enabled	Only Read is enabled (not to be changed)

Function Name	Factory Setting	When Enhanced Security Mode is set to [ON]
SNMP v3 Security Level and auth/priv-password	auth/priv-password	The security level can be selected from among [auth-password] and [auth/priv-password]. An 8-digit-or-more auth-password and priv-password can both be set.
Print Data Capture	Allow	Restrict (not to be changed)
Network Setting Clear	Enabled	Restrict
Administrator Password Change Via Network	Enabled	Restrict (not to be changed)
Release Time settings	5 min.	The setting value should be 5 min. or more (no value less than 5 can be set)
Change by the user of destination data previously registered (Address Book and Program)	Allow	Restrict (not to be changed)
System auto reset	1 min.	1 to 9 min Changing in to [NO use] is not allowed

✎...

Reminder

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

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.

Types of Data Cleared	Description
Enhanced Security Mode	Set to [OFF]
User Authentication	Set to [OFF]
Account Track Authentication	Set to [OFF]
Public User Access	Set to [Restrict]
User List	Set to [OFF]
Print Without Authentication	Set to [Restrict]
User registration data	Deletes all user-related data that has been registered
Account Track registration data	Deletes all account track-related data that has been registered
Box registration data/file	Deletes all User Box-related information and files saved in User Box
Secure Print ID/Password/file	Deletes all Secure Print Document-related information and files saved
Destination recipient data files	Deletes all destination recipient data including e-mail addresses and telephone numbers

2.2.2 Setting the Enhanced Security Mode

✎...

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

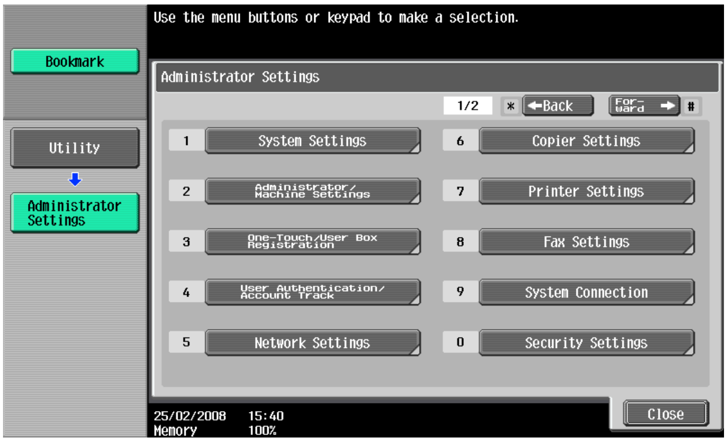
Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.

<Setting can be made only from the control panel>

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

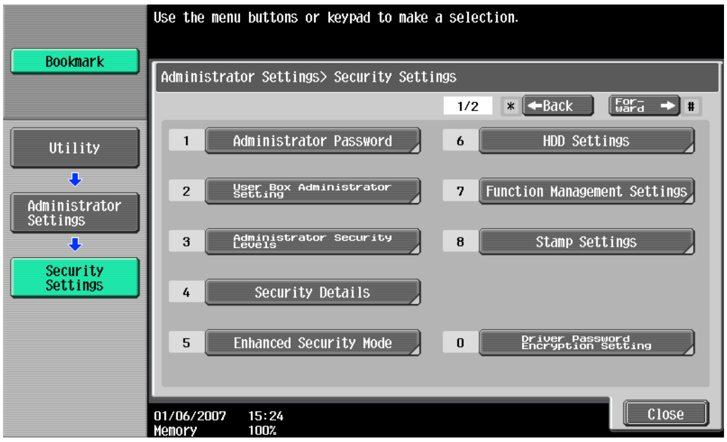
1 Call the Administrator Settings to the screen from the control panel.

2 Touch [Security Settings].



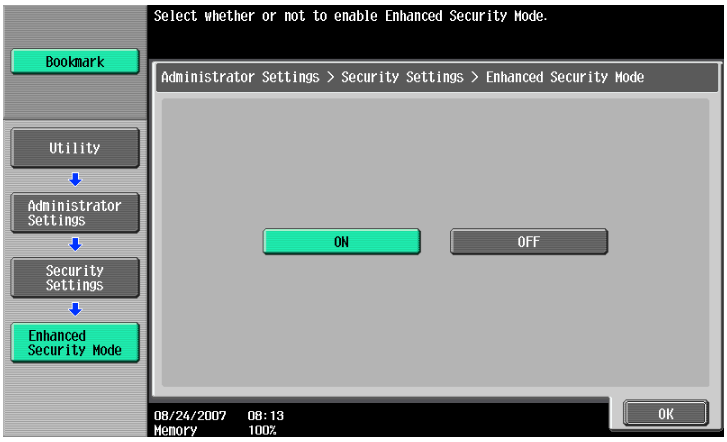
Use the menu buttons or keypad to make a selection.

3 Touch [Enhanced Security Mode].



Use the menu buttons or keypad to make a selection.

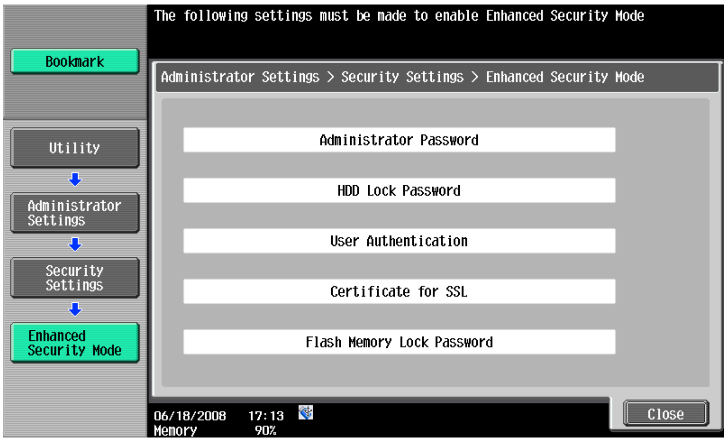
4 Select [ON] to enable the Enhanced Security Mode and touch [OK].



Select whether or not to enable Enhanced Security Mode.

Administrator Settings > Security Settings > Enhanced Security Mode

– 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

Administrator Password

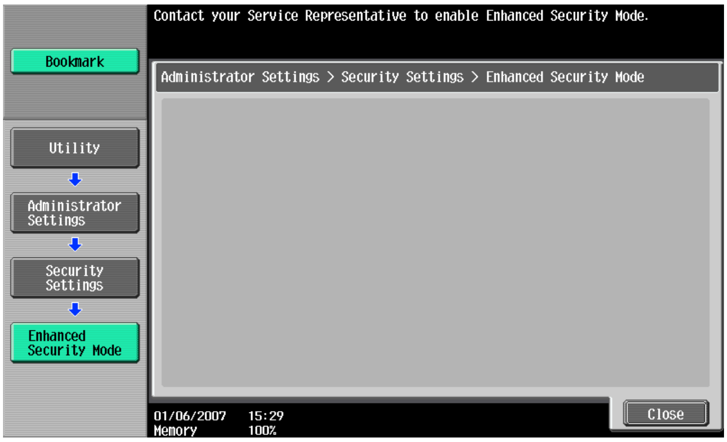
HDD Lock Password

User Authentication

Certificate for SSL

Flash Memory Lock Password

– The following screen appears if the previously required settings are yet to be made by the Service Engineer. Consult the Service Representative.



Contact your Service Representative to enable Enhanced Security Mode.

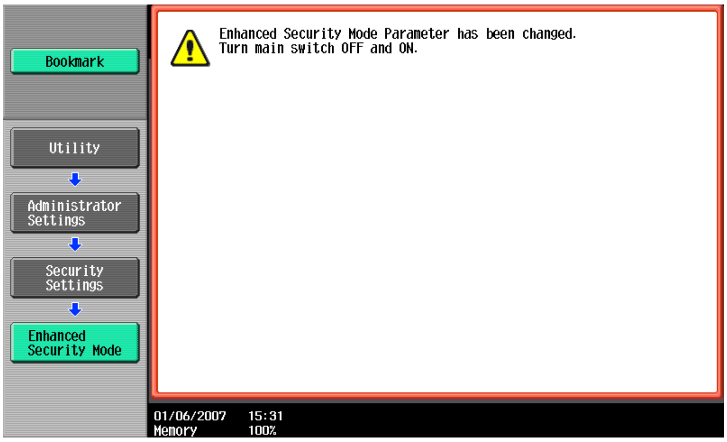
Administrator Settings > Security Settings > Enhanced Security Mode

? What is the factory setting for the Enhanced Security Mode?

→ 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.

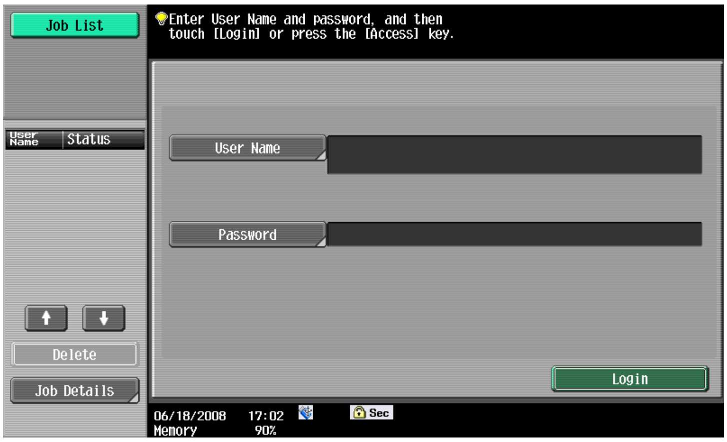
5 Touch [OK].

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.


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

01/06/2007 15:31
Memory 100%

If the Enhanced Security Mode is properly set to [ON], the following icon appears at the center of the User Authentication screen, indicating that the machine is in the Enhanced Security Mode.Icon doesn't appear when debug function with serial port is ON at Service mode. If Icon is not displayed, contact to a service counter.


Enter User Name and password, and then touch [Login] or press the [Access] key.

06/18/2008 17:02
Memory 90%

2.3 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, User Authentication, Account Track, SNMP authentication, Secure Print authentication, and User Box authentication 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], it is prohibited to change the setting from [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.

✎...

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.

2.3.1 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.

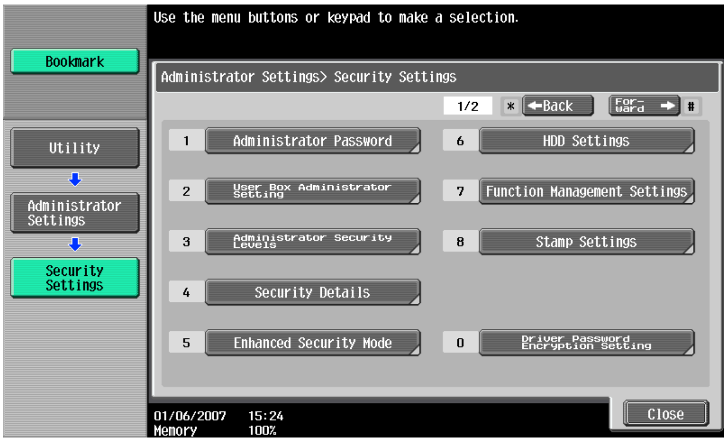
In the Enhanced Security Mode, Release Time less than 5 min. cannot be set.

<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 the Enhanced Security Mode" on page 2-11**.

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

2 Touch [Security Details].

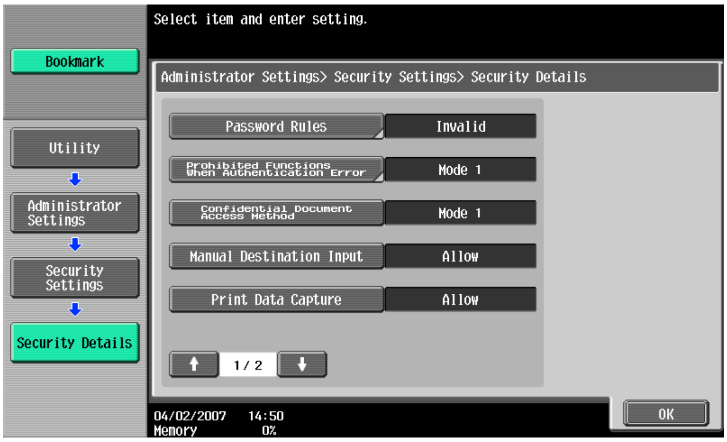


Use the menu buttons or keypad to make a selection.

Administrator Settings> Security Settings

01/06/2007 15:24
Memory 100%

3 Touch [Prohibited Functions When Authentication Error].



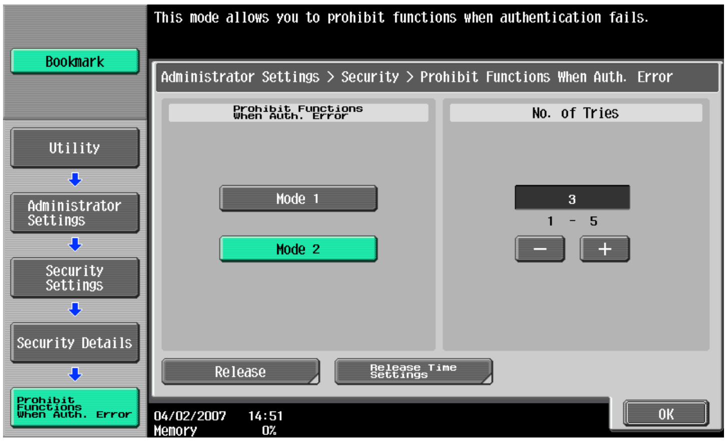
Select item and enter setting.

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
Print Data Capture	Allow

04/02/2007 14:50
Memory 0%

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

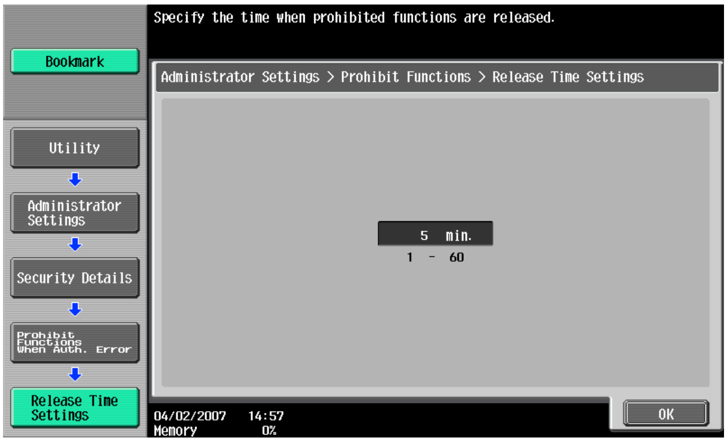
No. of Tries: 3 (1 - 5)

04/02/2007 14:51
Memory 0%

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

5 Touch [Release Time Settings].

6 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.



Specify the time when prohibited functions are released.

Administrator Settings > Prohibit Functions > Release Time Settings

5 min.

1 - 60

04/02/2007 14:57
Memory 0%

7 Touch [OK].

2.4 Canceling the Operation Prohibited State

When access to the Administrator of the machine by the Administrator Settings via the control panel is authenticated, the machine enables the operation of Release Setting performed for canceling the state of Prohibited Functions When Authentication Error (access lock state) as a result of unauthorized access.

Release Setting clears the unauthorized access check count for all User Authentication, Account Track, SNMP authentication, all Secure Print authentication, and all User Box authentication, resetting it to zero.

Perform the following procedure to cancel the password entry prohibited state.

- Administrator Settings: The operation prohibited state is canceled by the Service Engineer, or after the lapse of a predetermined period of time after the main power switch is turned off and on
- User/Account authentication: Release
- Secure Print authentication: Release
- User Box authentication: Release
- SNMP authentication: Release

2.4.1 Performing Release Setting

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

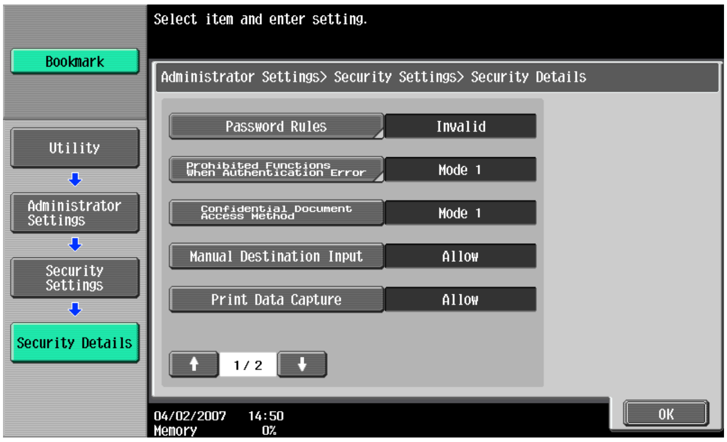
Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.

<Setting can be made only from the control panel>

✔ For the procedure to call the Security Details menu to the display, see steps 1 and 2 of **"Setting Prohibited Functions When Authentication Error" on page 2-14**.

1 Call the Security Details to the screen from the control panel.

2 Touch [Prohibited Functions When Authentication Error].



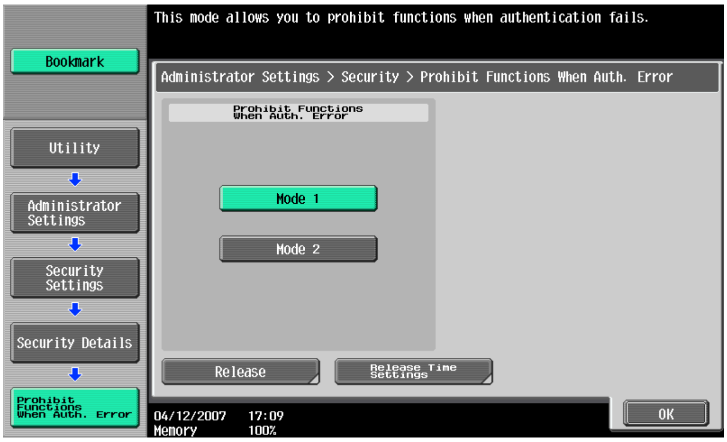
Select item and enter setting.

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
Print Data Capture	Allow

04/02/2007 14:50
Memory 0%

3 Touch [Release].

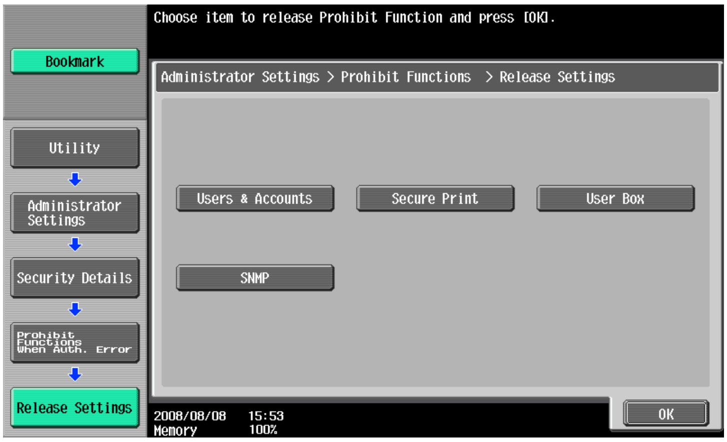


This mode allows you to prohibit functions when authentication fails.

Administrator Settings > Security > Prohibit Functions When Auth. Error

04/12/2007 17:09
Memory 100%

4 Select the function, for which Prohibit Function as a result of unauthorized access is to be released.



Choose item to release Prohibit Function and press [OK].

Administrator Settings > Prohibit Functions > Release Settings

2008/08/08 15:53
Memory 100%

5 Touch [OK].

This clears the unauthorized access check count of the specific function selected in step 4.

2.5 Setting the Authentication Method

When access to the Administrator of the machine by the Administrator Settings via the control panel is authenticated, the machine enables setting of the authentication method for User Authentication and for Account Track.

The User Authentication method may be [ON (MFP)] that uses the authentication system the machine has, [ON (External Server)] that uses a user information control system of the external server, or [OFF].

If the Enhanced Security Mode is set to [ON], the authentication method should be operated by either [ON (MFP)] or [ON (External Server)] (Active Directory).

The Account Track authentication method may be set to [ON] or [OFF]. If [ON] is selected, two or more users may be classified into different groups for control.

It is also possible to synchronize User Authentication with Account Track. Selecting "Synchronize" for "Synchronize User Authentication & Account Track" allows the machine to be used only through User Authentication.

Detail

*Changing the Account Track setting erases all user and account information data that has previously been registered. This changes all Personal User Boxes owned by the users who are deleted and all Group User Boxes owned by the accounts that are deleted to Public User Boxes. If the password set for a particular box before this change does not meet the requirements of the Password Rules, however, no access can be made to the Public User Box, to which that specific box was changed. In this case, the Administrator must first newly set a password that meets the requirements of the Password Rules. For details of the Password Rules, see **"Password Rules" on page 1-9**.*

Note

If [ON (External Server)] is selected for the authentication method, be sure to select [Active Directory] in the External Server Settings.

2.5.1 Setting the Authentication Method

Note

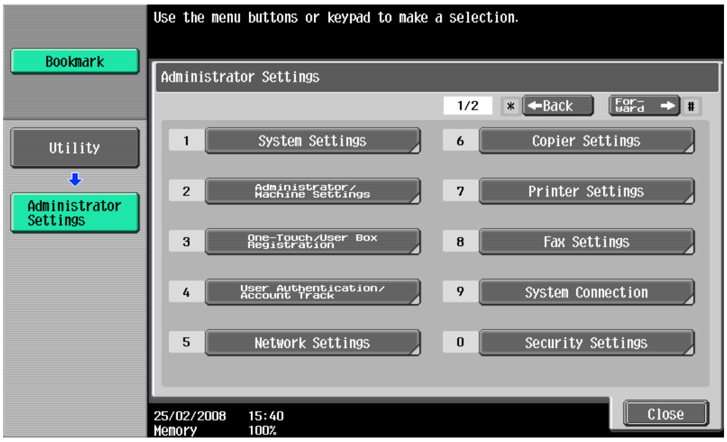
Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.

<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**.

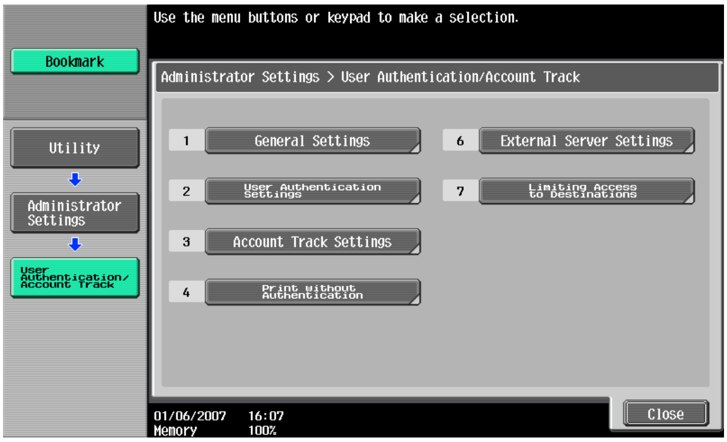
1 Call the Administrator Settings to the screen from the control panel.

2 Touch [User Authentication/Account Track].



Use the menu buttons or keypad to make a selection.

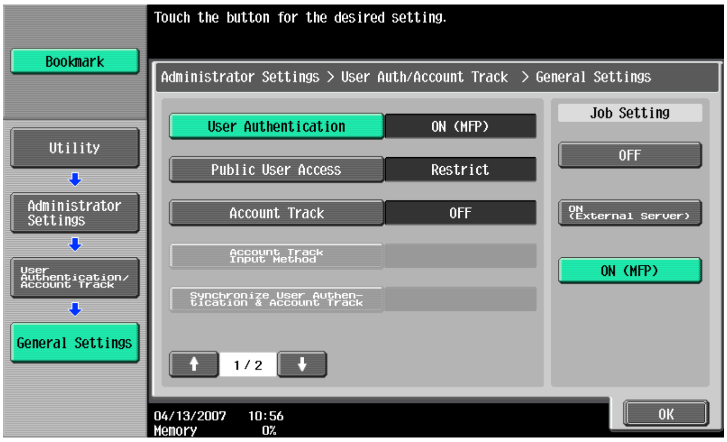
3 Touch [General Settings].


Use the menu buttons or keypad to make a selection.

Administrator Settings > User Authentication/Account Track

01/06/2007 16:07
Memory 100%
Bookmark
Utility
Administrator Settings
User Authentication/Account Track
1 General Settings
2 User Authentication Settings
3 Account Track Settings
4 Print without Authentication
6 External Server Settings
7 Limiting Access to Destinations
Close

4 Select [User Authentication] and touch [ON (MFP)] or [ON (External Server)].


Touch the button for the desired setting.

Administrator Settings > User Auth/Account Track > General Settings

User Authentication ON (MFP)
Public User Access Restrict
Account Track OFF

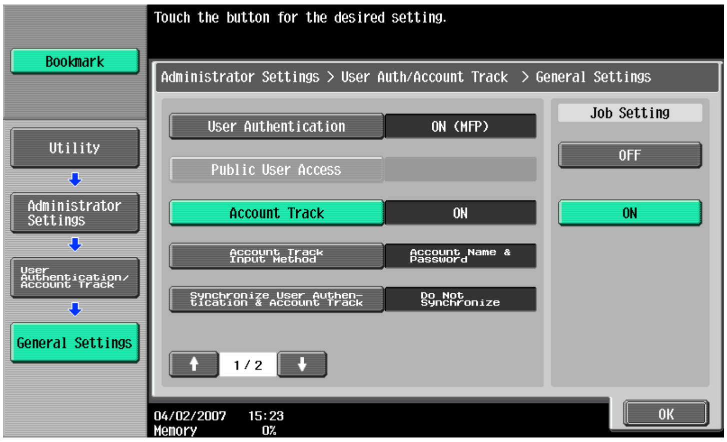
04/13/2007 10:56
Memory 0%
Bookmark
Utility
Administrator Settings
User Authentication/Account Track
General Settings
Account Track Input Method
Synchronize User Authentication & Account Track
1 / 2
Job Setting
OFF
ON (External Server)
ON (MFP)
OK

? What steps must be performed to use the External Server?

➔ To use the External Server, the External Server must be registered in advance.

➔ For how to make the External Server Settings, see "Setting the External Server" on page 2-22.

5 Select [Account Track] and touch [ON].


Touch the button for the desired setting.

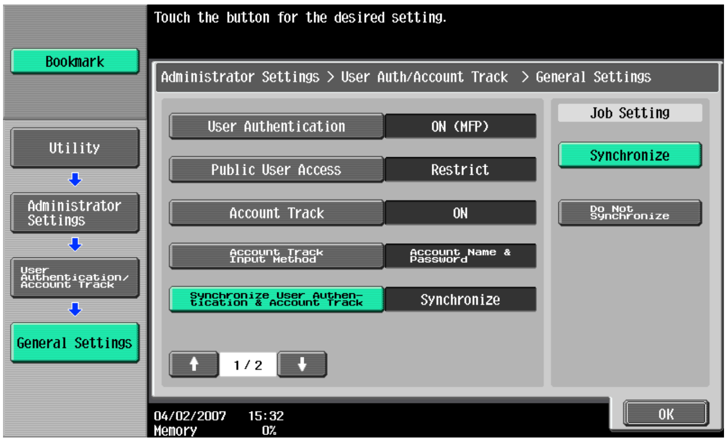
Administrator Settings > User Auth/Account Track > General Settings

User Authentication ON (MFP)
Public User Access
Account Track ON
Account Track Input Method Account Name & Password
Synchronize User Authentication & Account Track Do Not Synchronize

04/02/2007 15:23
Memory 0%

– If the Account Track is not to be used, go to step 7.

6 Select [Synchronize User Authentication & Account Track] and touch [Synchronize].



Touch the button for the desired setting.

Administrator Settings > User Auth/Account Track > General Settings

User Authentication: ON (MFP)

Public User Access: Restrict

Account Track: ON

Account Track Input Method: Account Name & Password

Synchronize User Authentication & Account Track: Synchronize

Job Setting: Synchronize

04/02/2007 15:32
Memory 0%

– To separate the User Authentication from Account Track authentication screens, select [Do not Synchronize].

7 Touch [OK].

8 A message appears that prompts you to clear the use control data. Now, select [Yes] and touch [OK].

2.5.2 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.

If [ON (External Server)] is selected for the authentication method, the External Server must be registered in the machine in advance.

A Sever Name that already exists cannot be redundantly registered.

<Setting can be made only from the control panel>

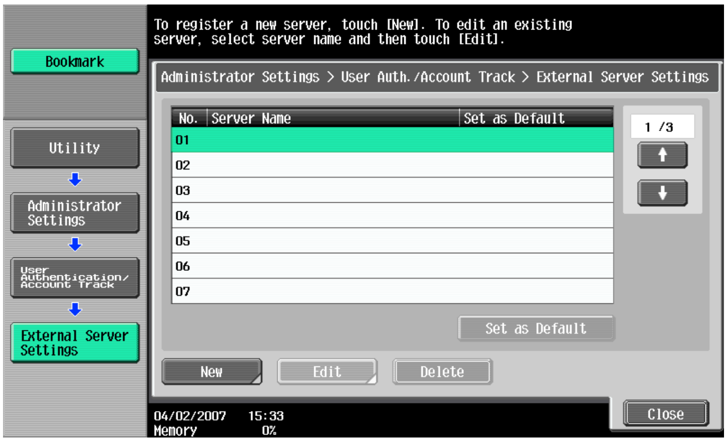
✔ For the procedure to call the User Authentication/Account Track screen to the display, see steps 1 and 2 of **"Setting the Authentication Method" on page 2-19**.

1 Call the User Authentication/Account Track screen to the display from the control panel.

2 Touch [External Sever Settings].

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

4 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

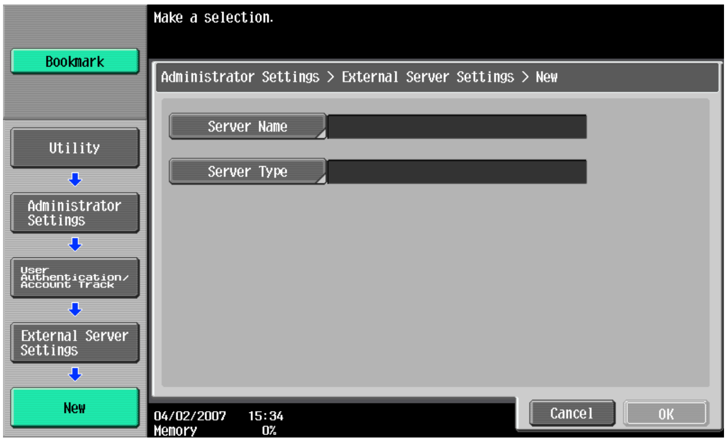
No.	Server Name	Set as Default
01		
02		
03		
04		
05		
06		
07		

04/02/2007 15:33
Memory 0%

? 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].

5 Touch [Server Type].

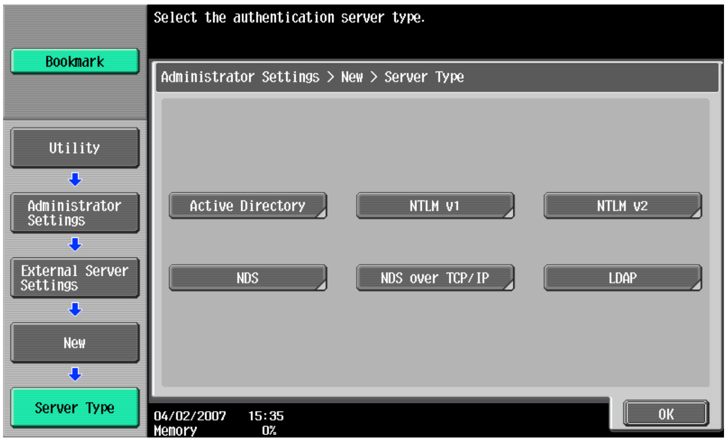


Make a selection.

Administrator Settings > External Server Settings > New

04/02/2007 15:34
Memory 0%

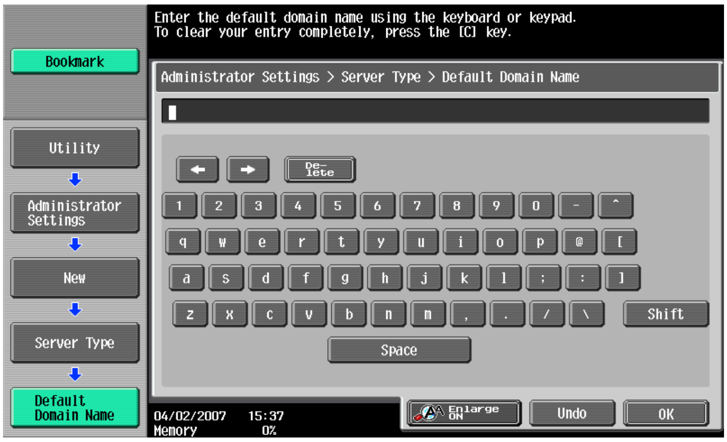
6 Touch [Active Directory].


Select the authentication server type.

Administrator Settings > New > Server Type

04/02/2007 15:35
Memory 0%

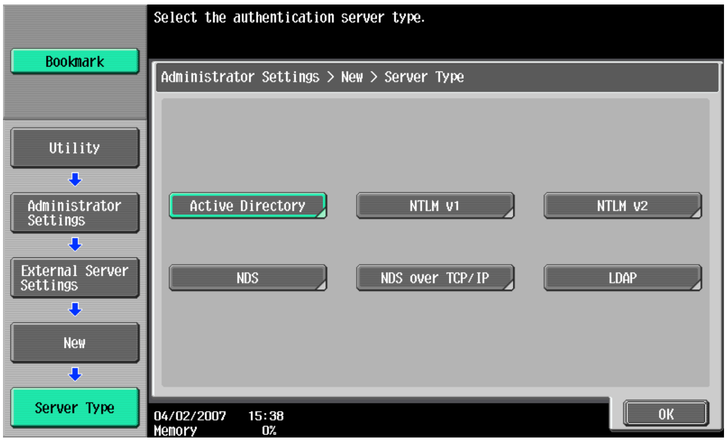
7 From the keyboard and keypad, enter the Domain Name and touch [OK].


Enter the default domain name using the keyboard or keypad.
To clear your entry completely, press the [C] key.

Administrator Settings > Server Type > Default Domain Name

04/02/2007 15:37
Memory 0%

8 Touch [OK].


Select the authentication server type.

Administrator Settings > New > Server Type

04/02/2007 15:38
Memory 0%

9 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.

10 Touch [OK].

11 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].

2.6 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.

2.6.1 Setting the System Auto Reset function

✎...

Note

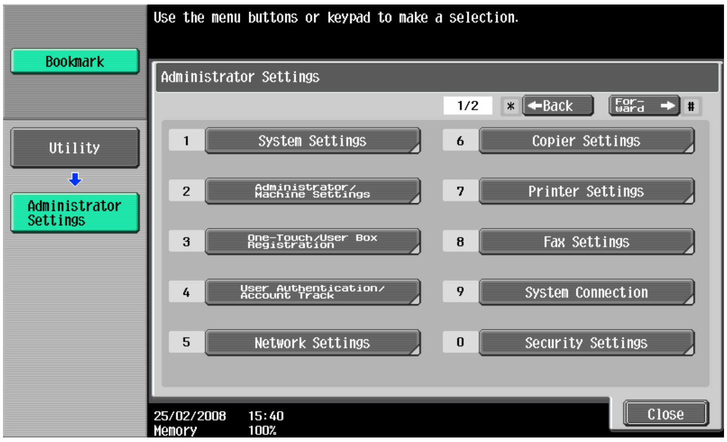
Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.

<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.

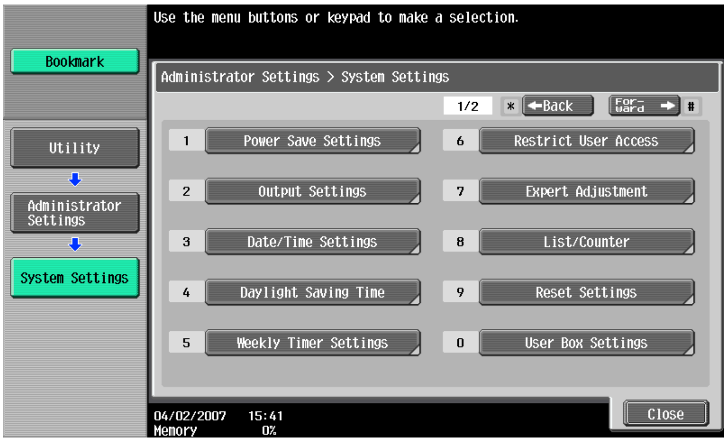
2 Touch [System Settings].



Use the menu buttons or keypad to make a selection.

Administrator Settings

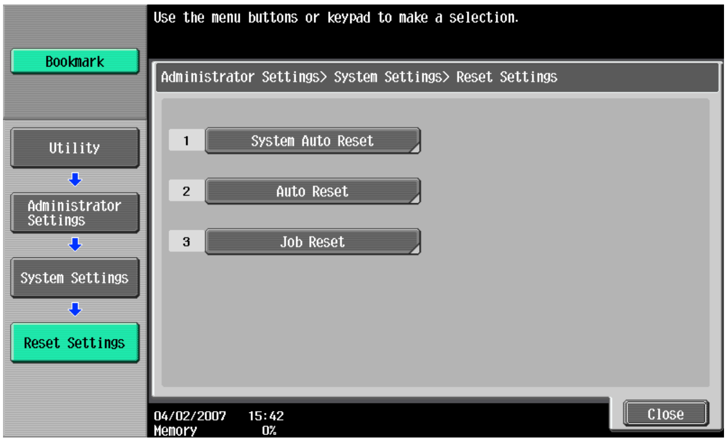
3 Touch [Reset Settings].



Use the menu buttons or keypad to make a selection.

Administrator Settings > System Settings

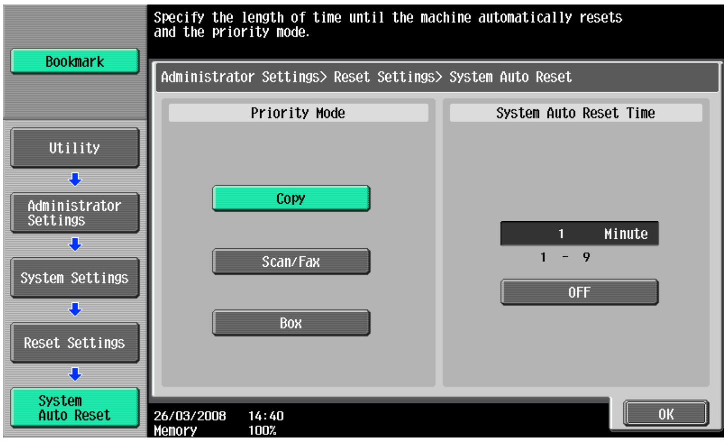
4 Touch [System Auto Reset].



Use the menu buttons or keypad to make a selection.

Administrator Settings> System Settings> Reset Settings

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.



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

Administrator Settings> Reset Settings> System Auto Reset

Priority Mode: Copy

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

- 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].

2.7 User Setting Function

When access to the Administrator of the machine by the Administrator Settings is authenticated, the machine enables registration of the users who can use the machine. It also enables operations for deleting a user and changing a User Password. In Web Connection, import/export of the user registration information is enabled, allowing the backup data of the user registration information to be saved or the saved backup data to be restored.

User Registration allows the User Name, User Password, and other user information to be registered for enabling access to, or operation of, the machine. Up to 1,000 different users can be registered. User Registration allows identification and authentication of each individual user, thereby preventing unauthorized use of the machine. A User Password may consist of 8 to 64 digits. The password entered is displayed as "*" or "●."

Detail

If [ON (External Server)] (Active Directory) is set for the authentication method, it is not possible to make user registration or change a User Password from the control panel. To register or change a user, make the settings on the server side. If Data Administrator is used for registering user information, however, the user name must match that registered in the External Server. Further, a User Password can be set, but is not to be used for authentication.

If [ON (External Server)] (Active Directory) is set for the authentication method and if a user not registered with this machine is authenticated through user authentication, that particular user name is automatically registered in the machine.

If [ON (External Server)] (Active Directory) is set for the authentication method and if a user registered with this machine is authenticated through user authentication, that particular user name, along with the External Server name, is automatically registered in the machine. No two User Names registered in an External Server may be alike.

If the user authentication method is changed between [ON (MFP)] and [ON (External Server)], the user information registered under the previous authentication method cannot be used under the new authentication method.

*If the user authentication method is to be changed, be sure first to delete all user information used under the old authentication method and then change the user authentication method as necessary. If a previously registered user is deleted, the Personal User Box owned by that specific user is changed to Public User Box. If the password set for a particular box before this change does not meet the requirements of the Password Rules, however, no access can be made to the Public User Box, to which that specific box was changed. In this case, the Administrator must first newly set a password that meets the requirements of the Password Rules. For details of the Password Rules, see **"Password Rules" on page 1-9**.*

Note

*If synchronization with Account Track has been set, the account should be registered in advance. For how to make the Account Track Registration, see **"Account Track Setting Function" on page 2-34**.*

2.7.1 Making user 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.

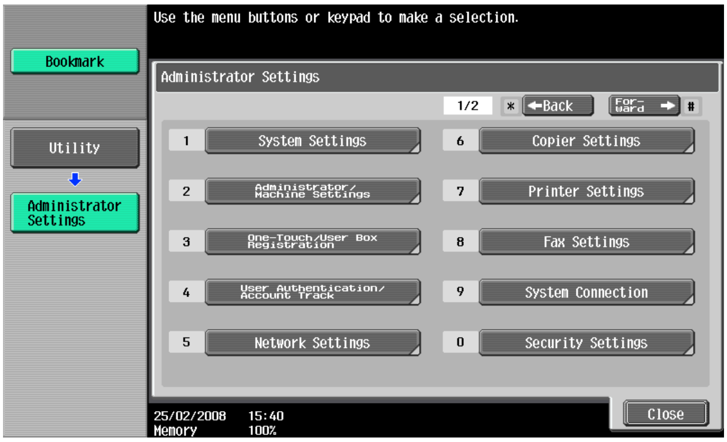
A User Name that already exists cannot be redundantly registered.

<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.

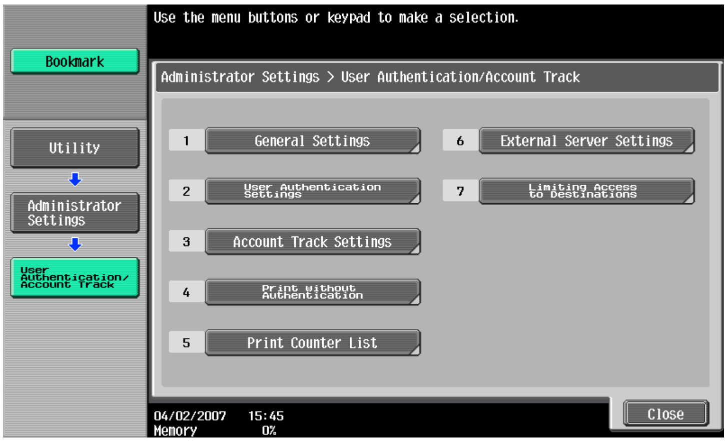
2 Touch [User Authentication/Account Track].



Use the menu buttons or keypad to make a selection.

Administrator Settings

3 Touch [User Authentication Settings].

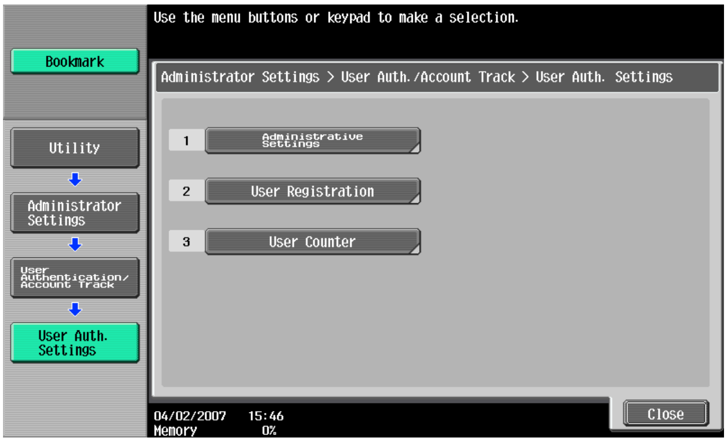


Use the menu buttons or keypad to make a selection.

Administrator Settings > User Authentication/Account Track

Bookmark
Utility
Administrator Settings
User Authentication/Account Track
1 General Settings
2 User Authentication Settings
3 Account Track Settings
4 Print without Authentication
5 Print Counter List
6 External Server Settings
7 Limiting Access to Destinations
04/02/2007 15:45
Memory 0%
Close

4 Touch [User Registration].

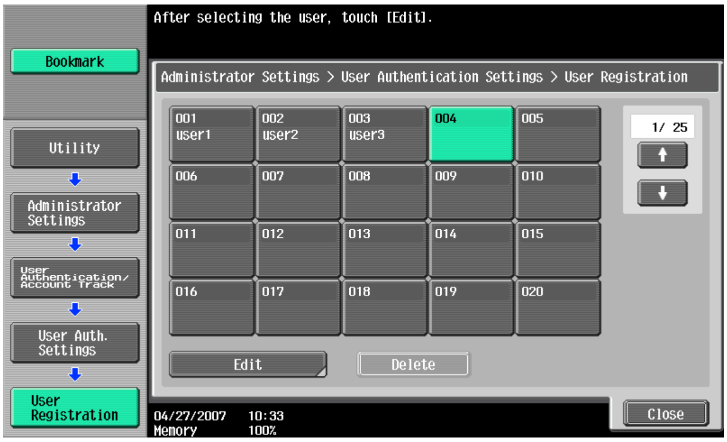


Use the menu buttons or keypad to make a selection.

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

04/02/2007 15:46
Memory 0%

5 Select a specific User Registration key, in which no user has been registered, and touch [Edit].



After selecting the user, touch [Edit].

Administrator Settings > User Authentication Settings > User Registration

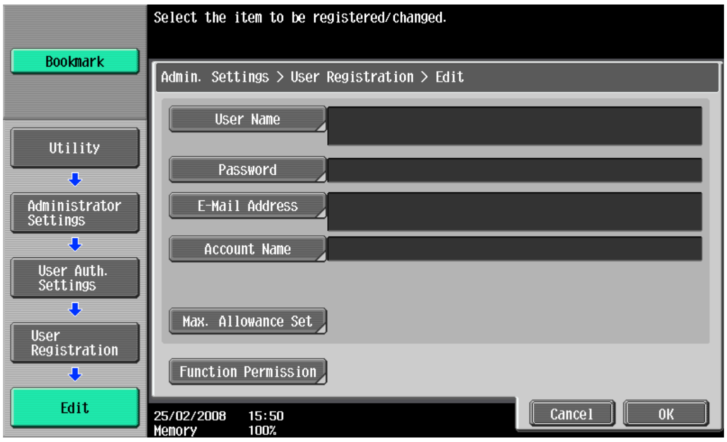
04/27/2007 10:33
Memory 100%

? What steps should be taken to delete a previously registered user or change a User Password?

➔ To delete a previously registered user or change a User Password, touch the corresponding User Registration key.

➔ To change a User Password, perform steps 6 through 8.

6 Touch [Password].

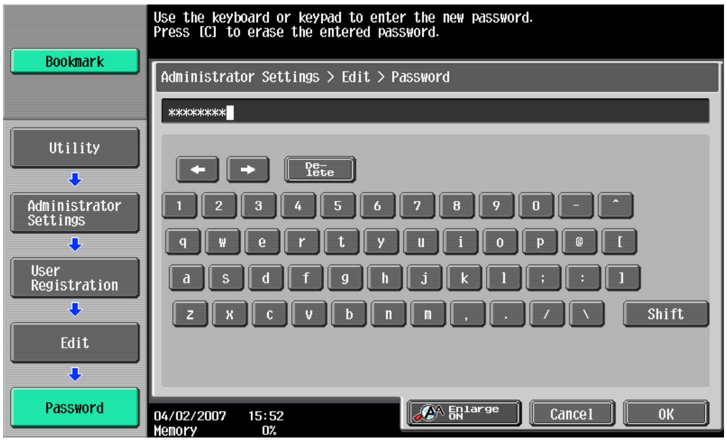


Select the item to be registered/changed.

Admin. Settings > User Registration > Edit

25/02/2008 15:50
Memory 100%

7 From the keyboard and keypad, enter a new User Password that may consist of 8 or more digits.



Use the keyboard or keypad to enter the new password.
Press [C] to erase the entered password.

Administrator Settings > Edit > Password

****

04/02/2007 15:52
Memory 0%

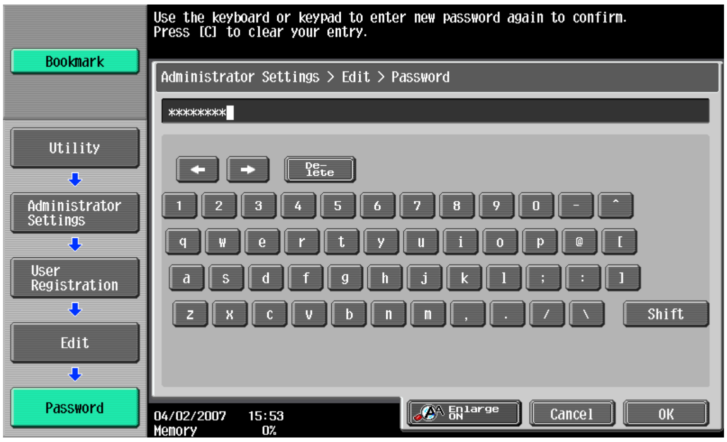
- Press the [C] key to clear all characters.
- Touch [Delete] to delete the last character entered.
- Touch [Shift] to show the upper case/symbol screen.
- Touch [Cancel] to go back to the screen shown in step 6.

8 Touch [OK].

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

➔ If the User Password entered does not comply with the Password Rules, a message appears that tells that the User Password entered cannot be used. Enter the correct User Password. For details of the Password Rules, see **"Password Rules" on page 1-9**.

9 To prevent entry of a wrong password, enter the User Password that consists of 8 to 64 digits again.



Use the keyboard or keypad to enter new password again to confirm.
Press [C] to clear your entry.

Administrator Settings > Edit > Password

****

04/02/2007 15:53
Memory 0%

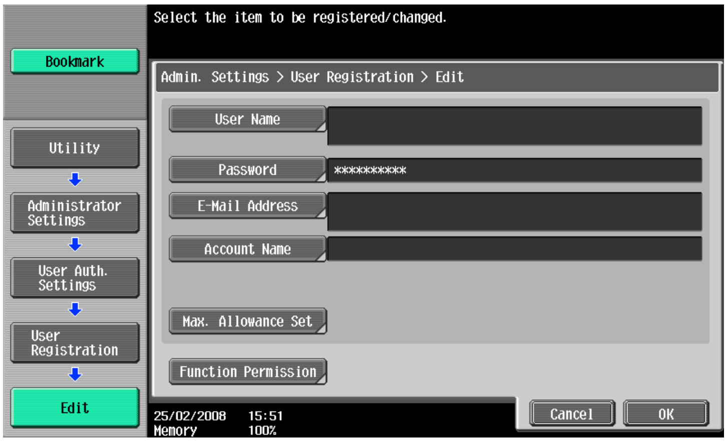
- Press the [C] key to clear all characters.
- Touch [Delete] to delete the last character entered.
- Touch [Shift] to show the upper case/symbol screen.
- Touch [Cancel] to go back to the screen shown in step 6.

10 Touch [OK].

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

➔ If there is a mismatch in the User Passwords, a message appears that tells that there is a mismatch in the User Passwords. Perform steps 7 through 10 once again.

11 Touch [Account Name].



Select the item to be registered/changed.

Admin. Settings > User Registration > Edit

User Name:

Password: **********

E-Mail Address:

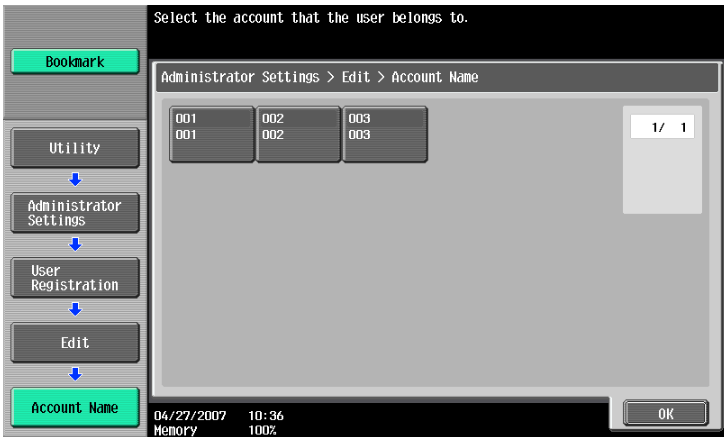
Account Name:

? What happens if Account Track has not been set or synchronization with Account Track has not been set for the authentication method?

➔ If Account Name is not registered, Account Track becomes necessary even with "Synchronize" set for "Synchronize User Authentication & Account Track." Account Track is, however, necessary only for the first time. Once any account is authenticated, that particular account is registered for Account Name. The machine can thereafter be used only through User Authentication.
It should be noted that this function is valid only through operation from the control panel of the machine. In operation from Web Connection or application software, if Account Name is not registered, User Authentication and Account Track are necessary each time, even with "Synchronize" set for "Synchronize User Authentication & Account Track."

➔ [Account Name] is not displayed if Account Track has not been set or synchronization with Account Track has not been set for the authentication method.

12 Select the arbitrary Account.



Select the account that the user belongs to.

Administrator Settings > Edit > Account Name

13 Touch [OK].

14 Make the necessary settings.

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

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

15 Touch [OK].

✎...

Reminder

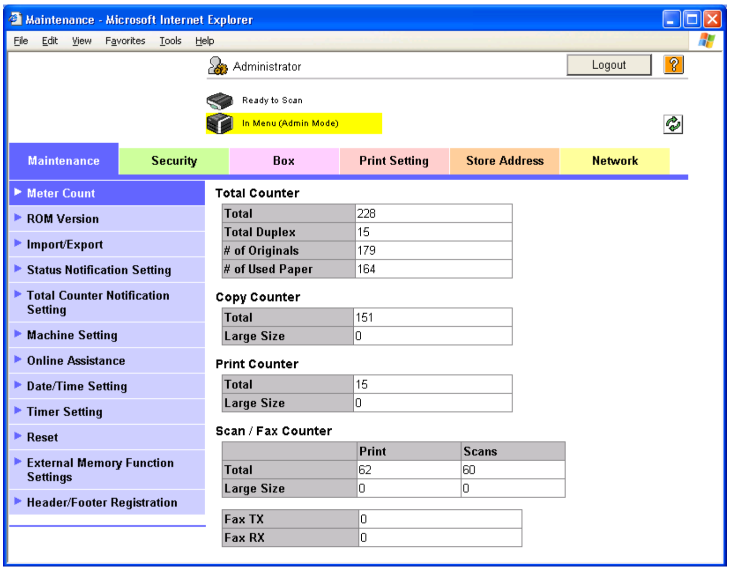
*To delete a previously registered user, touch [Delete] in step 5. Check the contents of registration on the confirmation screen and select [Yes] and touch [OK] if the previously registered user is to be deleted. Note that, if a previously registered user is deleted, the Personal User Box owned by that specific user is changed to Public User Box. If the password set for a particular box before this change does not meet the requirements of the Password Rules, however, no access can be made to the Public User Box, to which that specific box was changed. In this case, the Administrator must first newly set a password that meets the requirements of the Password Rules. For details of the Password Rules, see **"Password Rules" on page 1-9**.*

<From Web Connection>

✔ For the procedure to access the Admin Mode, see "Accessing the Administrator Settings" on page 2-2.

1 Start Web Connection and access the Admin Mode.

2 Click the [Security] tab and the [User Registration] menu.



Total Counter

Total	228
Total Duplex	15
# of Originals	179
# of Used Paper	164

Copy Counter

Total	151
Large Size	0

Print Counter

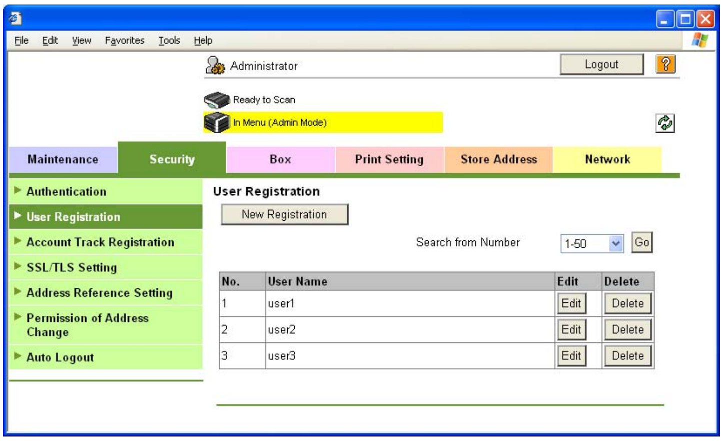
Total	15
Large Size	0

Scan / Fax Counter

	Print	Scans
Total	62	60
Large Size	0	0

Fax TX	0
Fax RX	0

3 Click the [New Registration].

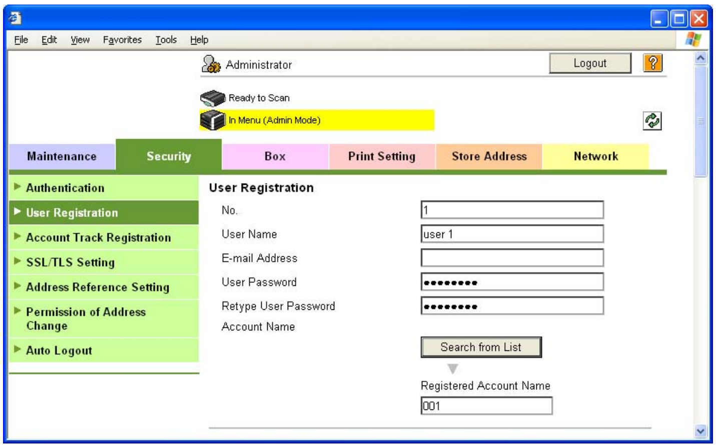


User Registration

No.	User Name	Edit	Delete
1	user1	Edit	Delete
2	user2	Edit	Delete
3	user3	Edit	Delete

– To change a User Password, click the [Edit] and select the "User Password is changed." check box. Then, enter the new User Password.

4 Make the necessary settings.



User Registration

No.	1
User Name	user 1
E-mail Address	
User Password	••••••••
Retype User Password	••••••••
Account Name	

Registered Account Name: 001

– Click the [Cancel] to go back to the previous screen.

? Are there any precautions to be used when making settings?

→ Any number that has previously been registered cannot be registered.

→ The User Password to be registered must the requirements of the Password Rules. For details of the Password Rules, see **"Password Rules" on page 1-9**.

? What happens if Account Track has not been set or synchronization with Account Track has not been set for the authentication method?

→ [Account Name] is not displayed if Account Track has not been set or synchronization with Account Track has not been set for the authentication method.

5 Click the [OK].

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

→ If the User Password entered does not comply with the Password Rules, a message appears that tells that the User Password entered cannot be used. Click [OK] to go back to the screen of step 3. Perform steps 3 through 5 once again. For details of the Password Rules, see **"Password Rules" on page 1-9**.

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

→ If there is a mismatch in the User Passwords, a message appears that tells that there is a mismatch in the User Passwords. Enter the correct User Password.

6 Check the message that tells that the setting has been completed. Then, click [OK].

✎...

Reminder

To delete a previously registered user, touch the [Delete] in step 3. Check the contents of registration on the confirmation screen and touch [OK] if the previously registered user is to be deleted. Note that, if a previously registered user is deleted, the Personal User Box owned by that specific user is changed to Public User Box. If the password set for a particular box before this change does not meet the requirements of the Password Rules, however, no access can be made to the Public User Box, to which that specific box was changed. In this case, the Administrator must first newly set a password that meets the requirements of the Password Rules. For details of the Password Rules, see ***"Password Rules" on page 1-9****.*

2.8 Account Track Setting Function

When access to the Administrator of the machine by the Administrator Settings is authenticated, the machine enables registration of accounts, for which use of the machine is restricted. It also enables operations for deleting a account and changing a Account Password. In Web Connection, import/export of the account registration information is enabled, allowing the backup data of the account registration information to be saved or the saved backup data to be restored.

Account Track Registration allows the Account Name, Account Password, and other account information to be registered for enabling access to, or operation of, the machine. Up to 1,000 different users or accounts can be registered. A Account Password may consist of 8 digits. The password entered is displayed as "*" or "●."

2.8.1 Making account 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.

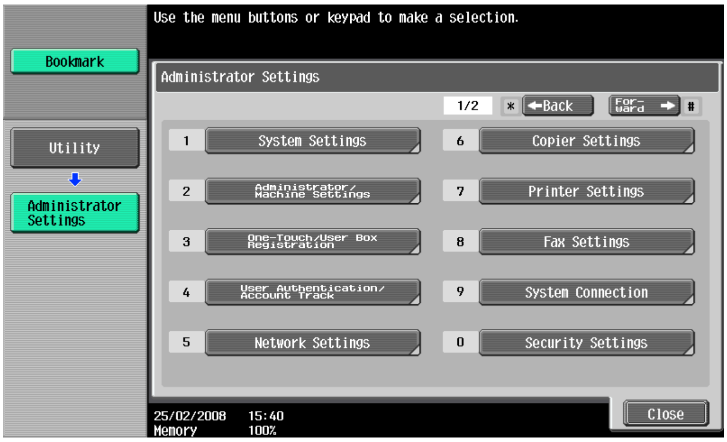
A Account Name that already exists cannot be redundantly registered.

<From the Control Panel>

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

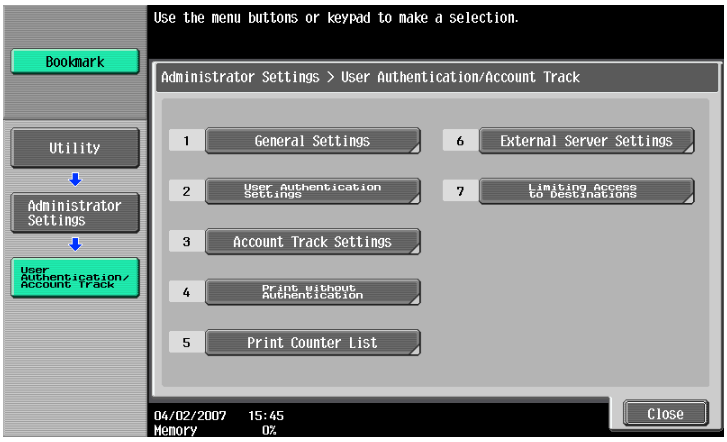
1 Call the Administrator Settings to the screen from the control panel.

2 Touch [User Authentication/Account Track].



Use the menu buttons or keypad to make a selection.

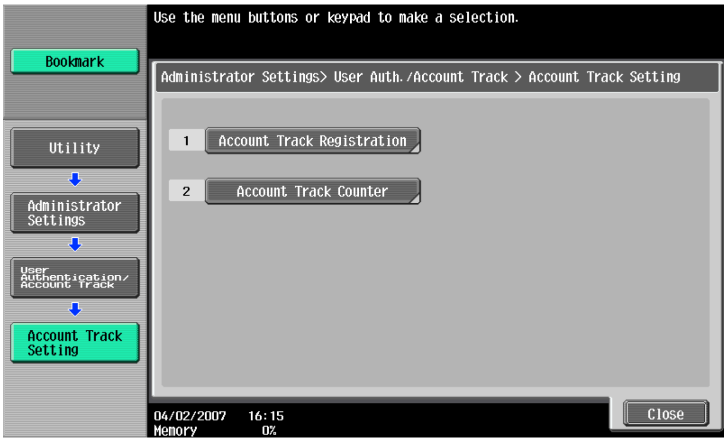
3 Touch [Account Track Settings].



Use the menu buttons or keypad to make a selection.

Bookmark
Utility
Administrator Settings
User Authentication/Account Track
Administrator Settings > User Authentication/Account Track
1 General Settings
2 User Authentication Settings
3 Account Track Settings
4 Print without Authentication
5 Print Counter List
6 External Server Settings
7 Limiting Access to Destinations
04/02/2007 15:45
Memory 0%
Close

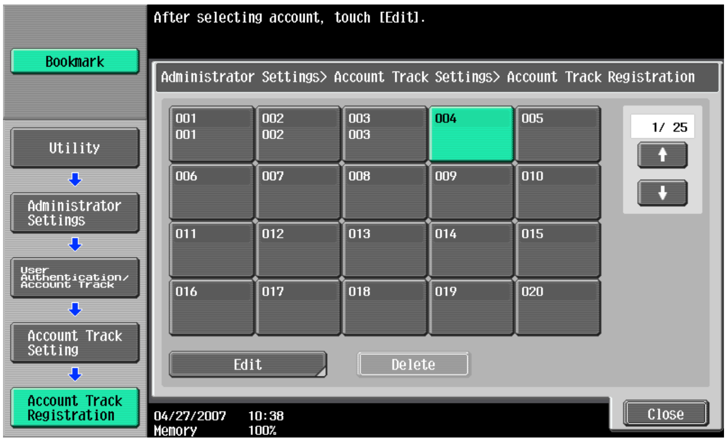
4 Touch [Account Track Registration].


Use the menu buttons or keypad to make a selection.

Administrator Settings> User Auth./Account Track > Account Track Setting

04/02/2007 16:15
Memory 0%

5 Select a specific Account Registration key, in which no account has been registered, and touch [Edit].


After selecting account, touch [Edit].

Administrator Settings> Account Track Settings> Account Track Registration

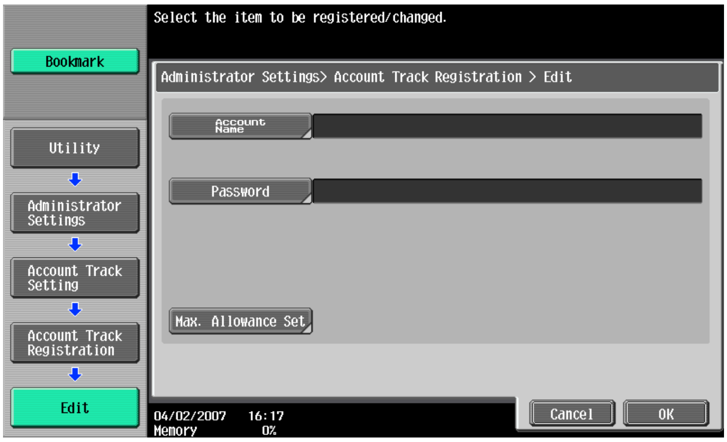
04/27/2007 10:38
Memory 100%

? What steps should be taken to delete a previously registered account or change a Account Password?

➔ To delete a previously registered account or change a Account Password, touch the corresponding Account Track Registration key.

➔ To change a Account Password, perform steps 6 through 8.

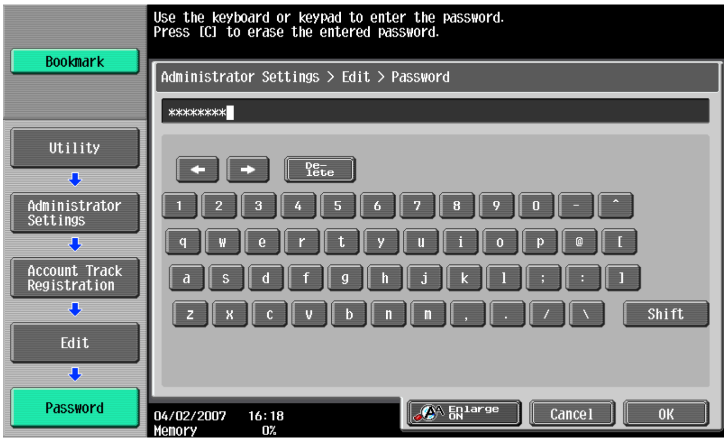
6 Touch [Password].


Select the item to be registered/changed.

Administrator Settings> Account Track Registration > Edit

04/02/2007 16:17
Memory 0%

7 From the keyboard and keypad, enter a new Account Password that may consist of 8 digits.



Use the keyboard or keypad to enter the password.
Press [C] to erase the entered password.

Administrator Settings > Edit > Password

****

04/02/2007 16:18
Memory 0%

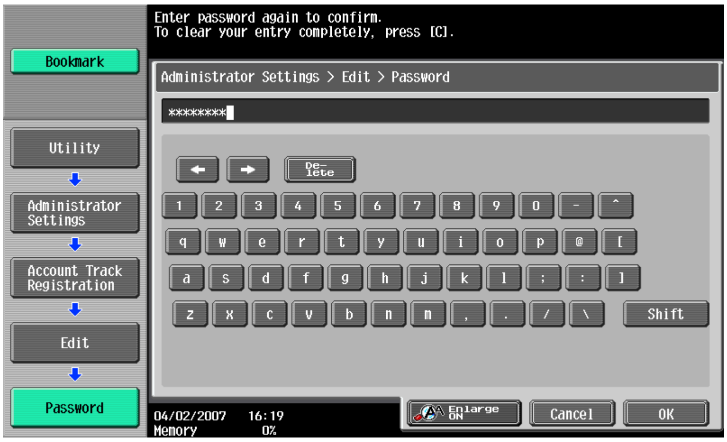
- Press the [C] key to clear all characters.
- Touch [Delete] to delete the last character entered.
- Touch [Shift] to show the upper case/symbol screen.
- Touch [Cancel] to go back to the screen shown in step 6.

8 Touch [OK].

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

➔ If the Account Password entered does not comply with the Password Rules, a message appears that tells that the Account Password entered cannot be used. Enter the correct Account Password. For details of the Password Rules, see **"Password Rules" on page 1-9**.

9 To prevent entry of a wrong password, enter the Account Password that consists of 8 digits again.



Enter password again to confirm.
To clear your entry completely, press [C].

Administrator Settings > Edit > Password

****

04/02/2007 16:19
Memory 0%

- 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 6.

10 Touch [OK].

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

➔ If there is a mismatch in the Account Passwords, a message appears that tells that there is a mismatch in the Account Passwords. Perform steps 7 through 10 once again.

11 Make the necessary settings.

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

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

12 Touch [OK].

✎...

Reminder

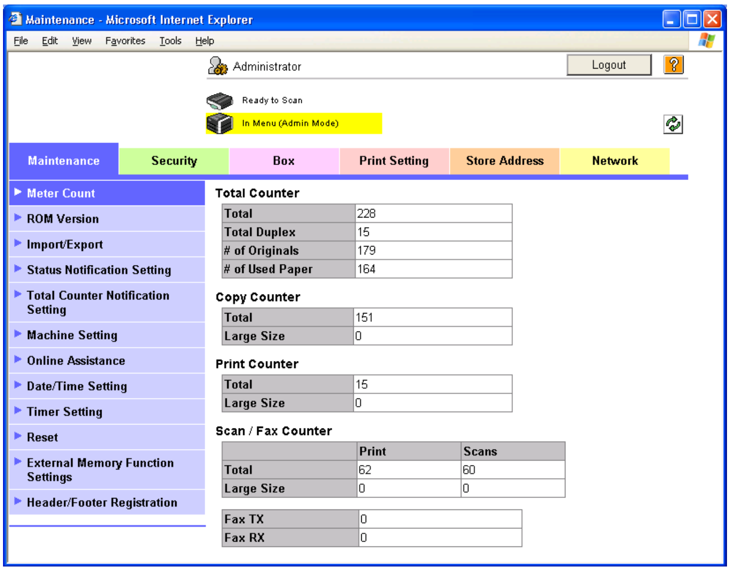
To delete a previously registered account, touch [Delete] in step 5. Check the contents of registration on the confirmation screen and select [Yes] and touch [OK] if the previously registered account is to be deleted. Note that, if a previously registered account is deleted, the Group User Box owned by that specific account is changed to Public User Box. If the password set for a particular box before this change does not meet the requirements of the Password Rules, however, no access can be made to the Public User Box, to which that specific box was changed. In this case, the Administrator must first newly set a password that meets the requirements of the Password Rules. For details of the Password Rules, see ***"Password Rules" on page 1-9****.*

<From Web Connection>

✔ For the procedure to access the Admin Mode, see "Accessing the Administrator Settings" on page 2-2.

1 Start Web Connection and access the Admin Mode.

2 Click the [Security] tab and the [Account Track Registration] menu.



Total Counter

Total	228
Total Duplex	15
# of Originals	179
# of Used Paper	164

Copy Counter

Total	151
Large Size	0

Print Counter

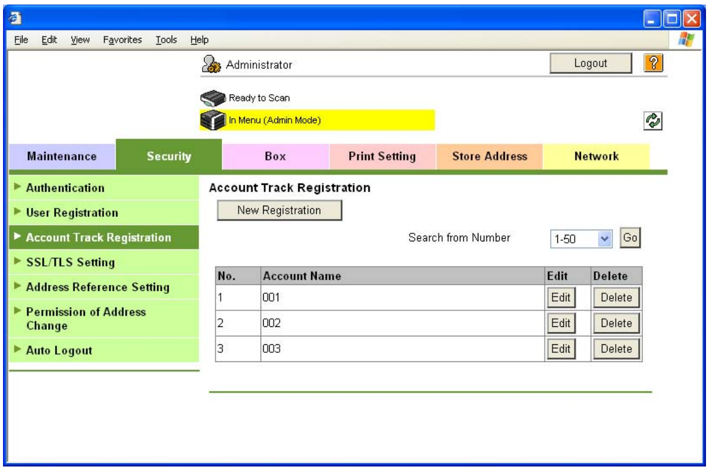
Total	15
Large Size	0

Scan / Fax Counter

	Print	Scans
Total	62	60
Large Size	0	0

Fax TX	0
Fax RX	0

3 Click the [New Registration].

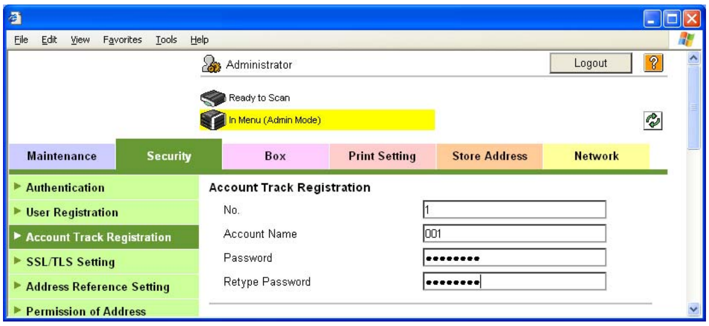


Account Track Registration

No.	Account Name	Edit	Delete
1	001	Edit	Delete
2	002	Edit	Delete
3	003	Edit	Delete

– To change a Account Password, click the [Edit] and select the "Password is changed." check box. Then, enter the new Account Password.

4 Make the necessary settings.



Account Track Registration

No.	1
Account Name	001
Password	••••••••
Retype Password	••••••••

– Click the [Cancel] to go back to the previous screen.

? Are there any precautions to be used when making settings?

→ Any number that has previously been registered cannot be registered.

→ The Account Password to be registered must the requirements of the Password Rules. For details of the Password Rules, see **"Password Rules" on page 1-9**.

5 Click the [OK].

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

→ If the Account Password entered does not comply with the Password Rules, a message appears that tells that the Account Password entered cannot be used. Click [OK] to go back to the screen of step 3. Perform steps 3 through 5 once again. For details of the Password Rules, see **"Password Rules" on page 1-9**.

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

→ If there is a mismatch in the Account Passwords, a message appears that tells that there is a mismatch in the Account Passwords. Enter the correct Account Password.

6 Check the message that tells that the setting has been completed. Then, click [OK].

✎...

Reminder

To delete a previously registered account, touch the [Delete] in step 3. Check the contents of registration on the confirmation screen and touch [OK] if the previously registered account is to be deleted. Note that, if a previously registered account is deleted, the Group User Box owned by that specific account is changed to Public User Box. If the password set for a particular box before this change does not meet the requirements of the Password Rules, however, no access can be made to the Public User Box, to which that specific box was changed. In this case, the Administrator must first newly set a password that meets the requirements of the Password Rules. For details of the Password Rules, see ***"Password Rules" on page 1-9****.*

2.9 User Box Function

When access to the Administrator of the machine by the Administrator Settings is authenticated, the machine enables the User Box. It also allows the User Box Password and user and account attributes to be changed.

User Box prepares a User Box in the HDD as a space for saving image files. The Administrator of the machine is allowed to register a Public User Box that is shared among registered users. Up to 1,000 personal, public and Group User Boxes can be registered. A User Box Password may consist of 8 digits. The password entered is displayed as "*" or "●."

The term "user attributes" is a generic name used to refer to Owner Change and User Box Type.

The term "account attributes" is a generic name used to refer to Owner Change and Account Box Type.

Note

If [ON (External Server)] (Active Directory) is set for the authentication method, the same Personal User Box name as that registered with the machine can be created and registered along with the External Server name. No two Personal User Box names registered in an External Server may be alike.

Reminder

If a job is executed in the copy, fax, or scan mode by specifying a User Box number that has not been registered, the Personal User Box owned by the user who logged on through User Authentication is automatically registered.

2.9.1 Setting the User Box

Note

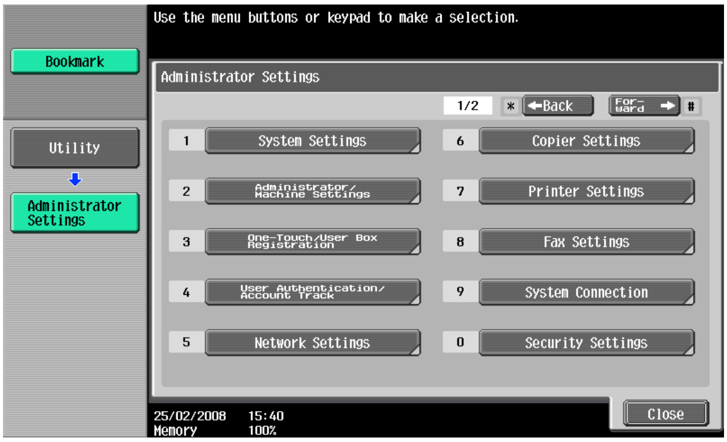
Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.

<From the Control Panel>

✔ For the procedure to access the Administrator Settings, see **"Accessing the Administrator Settings" on page 2-2**.

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

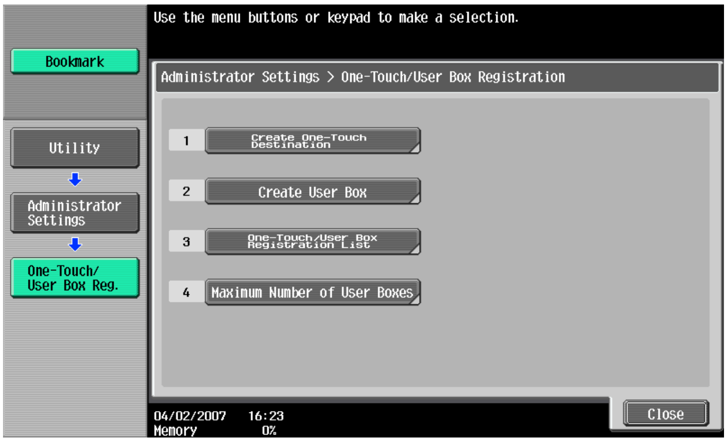
2 Touch [One-Touch/User Box Registration].



Use the menu buttons or keypad to make a selection.

Administrator Settings

3 Touch [Create User Box].



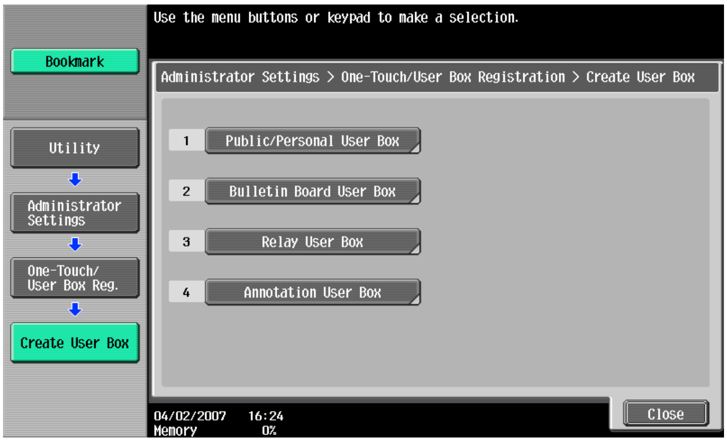
Use the menu buttons or keypad to make a selection.

Administrator Settings > One-Touch/User Box Registration

04/02/2007 16:23
Memory 0%

Bookmark
Utility
Administrator Settings
One-Touch/ User Box Reg.
1 Create One-Touch Destination
2 Create User Box
3 One-Touch/User Box Registration List
4 Maximum Number of User Boxes
Close

4 Touch [Public/Personal User Box].

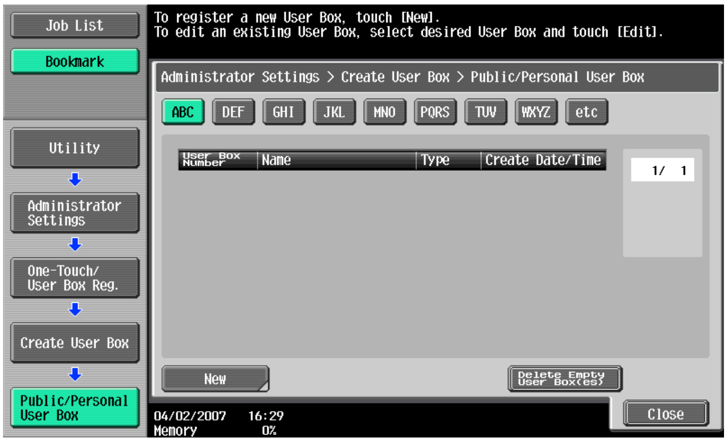


Use the menu buttons or keypad to make a selection.

Administrator Settings > One-Touch/User Box Registration > Create User Box

04/02/2007 16:24
Memory 0%

5 Touch [New].



To register a new User Box, touch [New].
To edit an existing User Box, select desired User Box and touch [Edit].

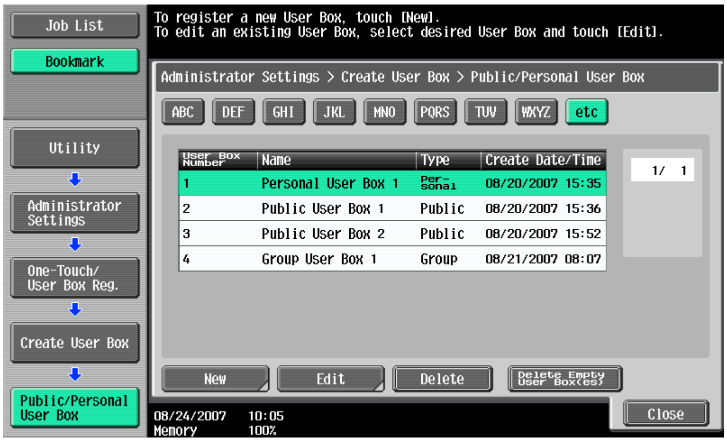
Administrator Settings > Create User Box > Public/Personal User Box

User Box Number	Name	Type	Create Date/Time

1/ 1

04/02/2007 16:29
Memory 0%

– To change the setting of a User Box, touch the corresponding User Box key.



To register a new User Box, touch [New].
To edit an existing User Box, select desired User Box and touch [Edit].

Administrator Settings > Create User Box > Public/Personal User Box

User Box Number	Name	Type	Create Date/Time
1	Personal User Box 1	Personal	08/20/2007 15:35
2	Public User Box 1	Public	08/20/2007 15:36
3	Public User Box 2	Public	08/20/2007 15:52
4	Group User Box 1	Group	08/21/2007 08:07

08/24/2007 10:05
Memory 100%

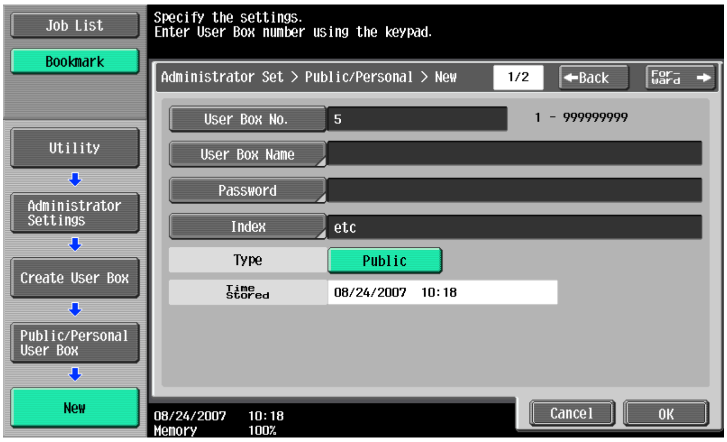
? What steps should be taken to delete a previously registered User Box or change a User Box Password, user attributes and account attributes?

→ To change the User Box Password, user attributes and account attributes, touch [Edit].

→ For a Personal User Box, the User Box Type and owner can be set or changed. For the change procedure, see **"Changing the user attributes and account attributes" on page 2-46**.

→ To delete a User Box, touch [Delete]. A message will then appear for confirming whether or not the specified User Box can be surely deleted. Select [Yes] and touch [OK] to delete the specified User Box.

6 Touch [Password].



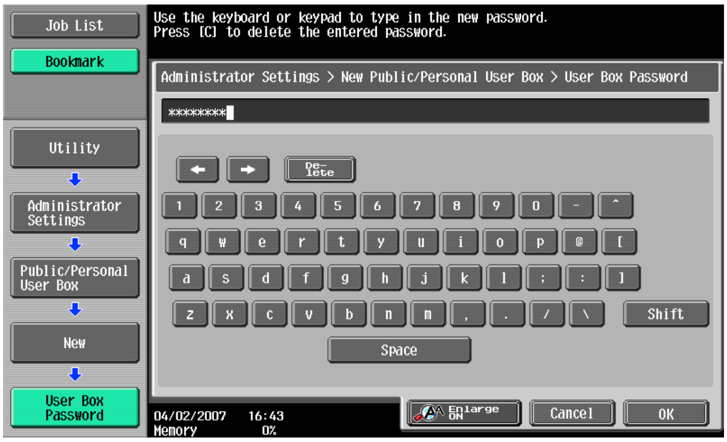
Specify the settings.
Enter User Box number using the keypad.

Administrator Set > Public/Personal > New

User Box No.: 5 (1 – 999999999)
User Box Name:
Password:
Index: etc
Type: Public
Time Stored: 08/24/2007 10:18

08/24/2007 10:18
Memory 100%

7 Enter the new 8-digit User Box Password from the keyboard and keypad.



Use the keyboard or keypad to type in the new password.
Press [C] to delete the entered password.

Administrator Settings > New Public/Personal User Box > User Box Password

****

04/02/2007 16:43
Memory 0%

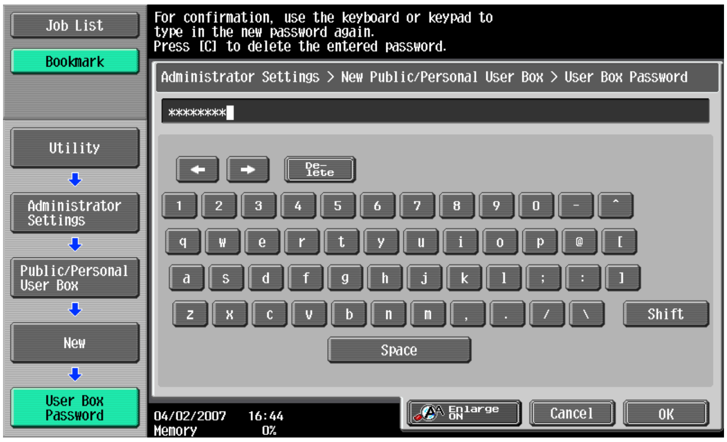
– Press the [C] key to clear all characters.
– Touch [Delete] to delete the last character entered.
– Touch [Shift] to show the upper case/symbol screen.
– Touch [Cancel] to go back to the screen shown in step 6.

8 Touch [OK].

? What happens if the User Box Password entered does not meet the requirements of the Password Rules?

➔ If the User Box Password entered does not comply with the requirements of the Password Rules, a message appears that tells that the User Box Password entered cannot be used. Enter the correct User Box Password. For details of the Password Rules, see **"Password Rules" on page 1-9**.

9 To prevent entry of a wrong password, enter the 8-digit User Box Password again.



For confirmation, use the keyboard or keypad to type in the new password again.
Press [C] to delete the entered password.

Administrator Settings > New Public/Personal User Box > User Box Password

****

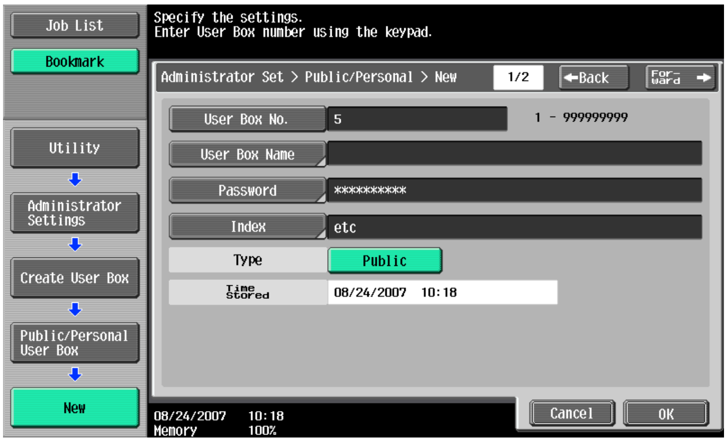
– Press the [C] key to clear all characters.
– Touch [Delete] to delete the last character entered.
– Touch [Shift] to show the upper case/symbol screen.
– Touch [Cancel] to go back to the screen shown in step 6.

10 Touch [OK].

? What happens if there is a mismatch in the User Box Passwords?

➔ If there is a mismatch in the User Box Passwords, a message appears that tells that there is a mismatch in the User Box Passwords. Perform steps 6 through 10 once again.

11 Make the necessary settings.



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

Administrator Set > Public/Personal > New

User Box No.: 5 (1 - 999999999)
User Box Name:
Password: **********
Index: etc
Type: Public
Time Stored: 08/24/2007 10:18

? What if a User Box No. is duplicated?

➔ A User Box No. that has been registered cannot be registered anew.

? What if no Name has been entered?

➔ If no Name has been registered, [OK] cannot be touched. Be sure to register the Name.

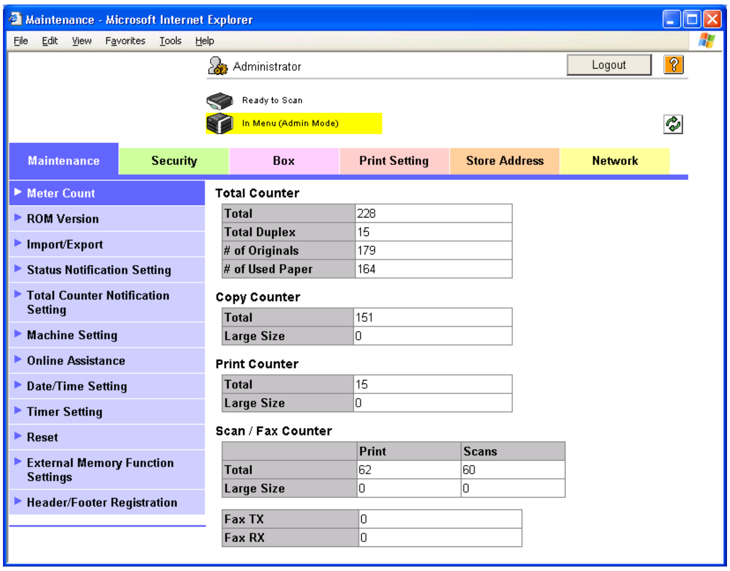
12 Touch [OK].

<From Web Connection>

✔ For the procedure to access the Admin Mode, see "Accessing the Administrator Settings" on page 2-2.

1 Start Web Connection and access the Admin Mode.

2 Click the [Box] tab and the [Create User Box] menu.



Total Counter

Total	228
Total Duplex	15
# of Originals	179
# of Used Paper	164

Copy Counter

Total	151
Large Size	0

Print Counter

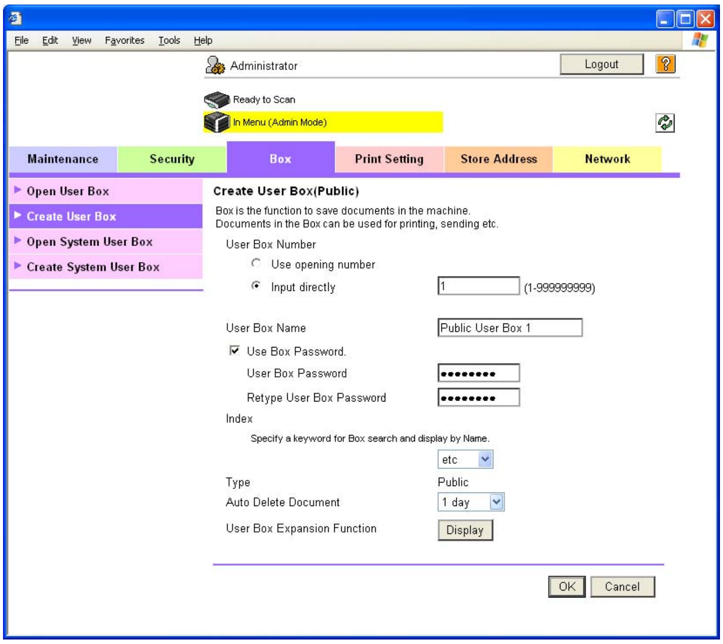
Total	15
Large Size	0

Scan / Fax Counter

	Print	Scans
Total	62	60
Large Size	0	0

Fax TX	0
Fax RX	0

3 Make the necessary settings.



Create User Box(Public)

Box is the function to save documents in the machine.
Documents in the Box can be used for printing, sending etc.

User Box Number
○ Use opening number
● Input directly 1 (1-999999999)

User Box Name: Public User Box 1

☑ Use Box Password.

User Box Password: ••••••••

Retype User Box Password: ••••••••

Index
Specify a keyword for Box search and display by Name.
etc

Type: Public

Auto Delete Document: 1 day

User Box Expansion Function: Display

? Are there any precautions to be used when making settings?

➔ Be sure to enter the User Box Number., User Box Name, User Box Password, and Retype User Box Password.

➔ A User Box Number that has been registered cannot be registered anew.

4 Click the [OK].

? What happens if the User Box Password entered does not meet the requirements of the Password Rules?

➔ If the User Box Password entered does not comply with the Password Rules, a message appears that tells that the User Box Passwords entered cannot be used. Click [OK] to go back to the screen of step 3. Perform steps 3 through 4 once again. For details of the Password Rules, see **"Password Rules" on page 1-9**.

? What happens if there is a mismatch in the User Box Passwords?

→ If there is a mismatch in the User Box Passwords, a message appears that tells that there is a mismatch in the User Box Passwords. Enter the correct User Box Password.

? What steps should be performed to change the user attributes, account attributes and User Box Password?

→ For the procedure to change the user attributes, account attributes and User Box Password, see **"Changing the user attributes and account attributes" on page 2-46**.

5 Check the message that tells that the setting has been completed. Then, click [OK].

2.9.2 Changing the user attributes and account attributes

The Administrator of the machine can change the box type of the box previously registered. For the Personal User Box, the owner user can be changed, and for the Group User Box, the owner account can be changed.

✎...

Note

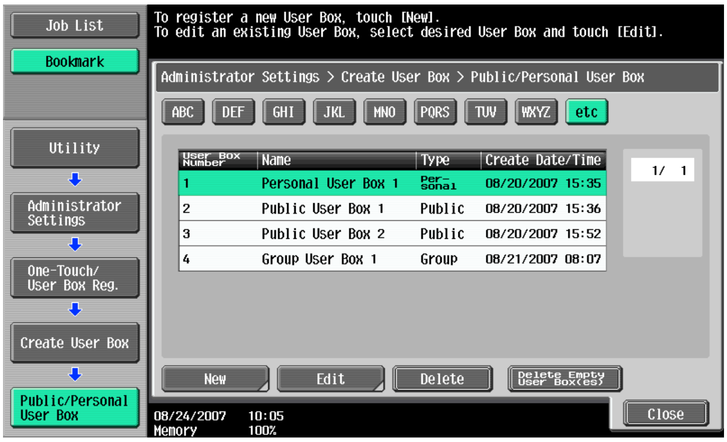
Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.

<From the Control Panel>

✔ For the procedure to call the User Box setting screen to the display, see steps 1 through 4 of **"Setting the User Box" on page 2-40**.

1 Call the User Box setting screen to the display from the control panel.

2 Select the desired User Box key and touch [Edit].



To register a new User Box, touch [New].
To edit an existing User Box, select desired User Box and touch [Edit].

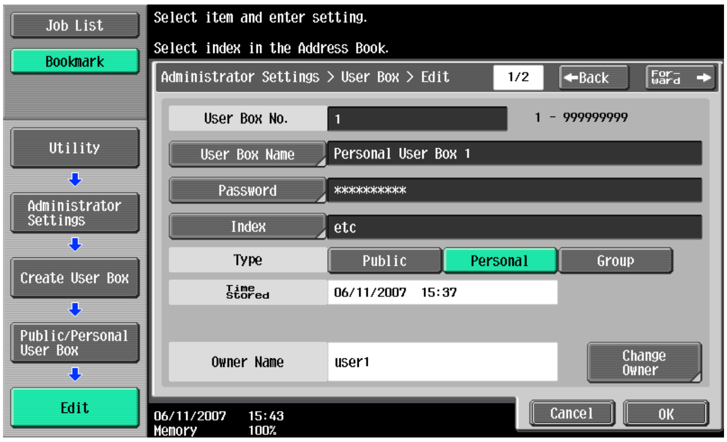
Administrator Settings > Create User Box > Public/Personal User Box

User Box Number	Name	Type	Create Date/Time
1	Personal User Box 1	Per-sonal	08/20/2007 15:35
2	Public User Box 1	Public	08/20/2007 15:36
3	Public User Box 2	Public	08/20/2007 15:52
4	Group User Box 1	Group	08/21/2007 08:07

08/24/2007 10:05
Memory 100%

– If the User Box Type has been changed, go to step 3. If the User Box Password has been changed, go to step 7.
– To change the owner user or owner account, perform steps 4 to 6.

3 Select the User Box Type.



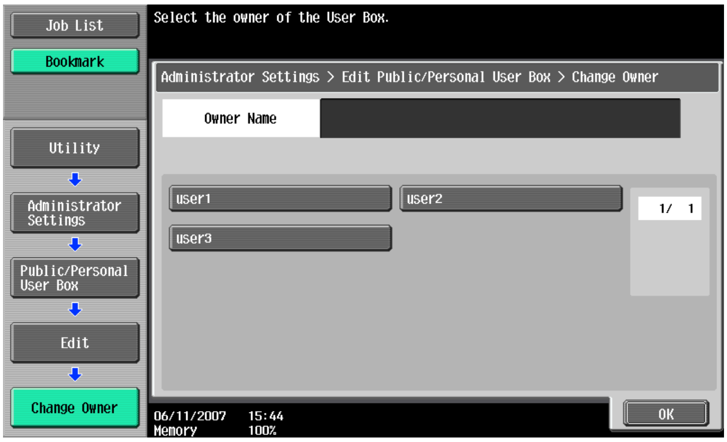
Select item and enter setting.
Select index in the Address Book.

Administrator Settings > User Box > Edit

User Box No. 1 (1 - 999999999)
User Box Name: Personal User Box 1
Password: **********
Index: etc
Type: Public / Personal / Group
Time Stored: 06/11/2007 15:37
Owner Name: user1

06/11/2007 15:43
Memory 100%

- [Change Owner] appears if the Box Type has been changed to [Personal]. Select the desired user name of the owner.



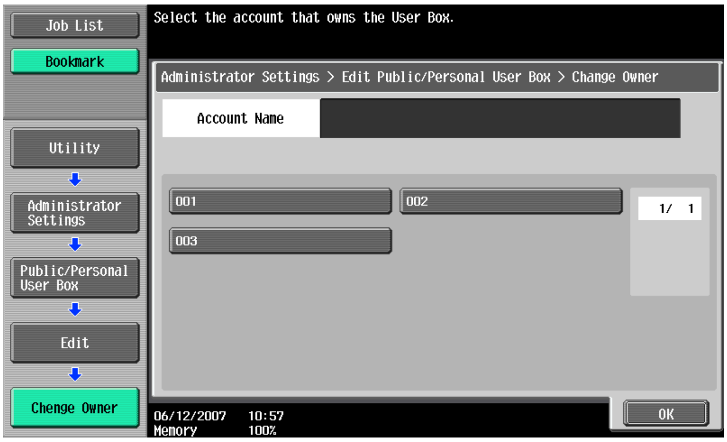
Select the owner of the User Box.

Administrator Settings > Edit Public/Personal User Box > Change Owner

Owner Name

06/11/2007 15:44
Memory 100%

- [Change Account Name] appears if the Box Type has been changed to [Group]. Select the desired account name of the owner.



Select the account that owns the User Box.

Administrator Settings > Edit Public/Personal User Box > Change Owner

Account Name

06/12/2007 10:57
Memory 100%

? What happens when the User Box Type is changed?

→ Changing the User Box Type clears the User Box Password. Perform steps 7 through 11 to set the User Box Password.

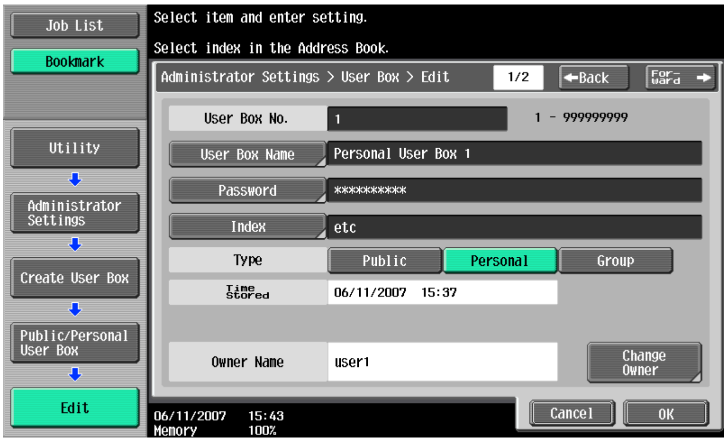
→ If the User Box Type has been changed to [Public], set a User Box Password that meets the requirements of the Password Rules. For details of the Password Rules, see **"Password Rules" on page 1-9**.

? What happens if the box type is changed to [Public]?

→ Changing the box type to [Public] nullifies the setting of the owner user or owner account.

→ Public User Box cannot be changed to Personal User Box or Group User Box.

4 Touch [Change Owner] if the box type is [Personal] and touch [Change Account Name] if the box type is [Group].



Select item and enter setting.
Select index in the Address Book.

Administrator Settings > User Box > Edit

User Box No. 1 1 - 999999999

User Box Name: Personal User Box 1

Password: **********

Index: etc

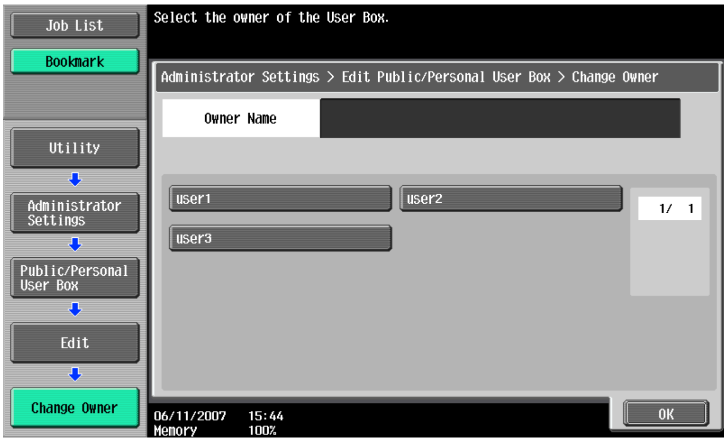
Type: Public Personal Group

Time Stored: 06/11/2007 15:37

Owner Name: user1

06/11/2007 15:43
Memory 100%

5 For [Change Owner], select the desired user.



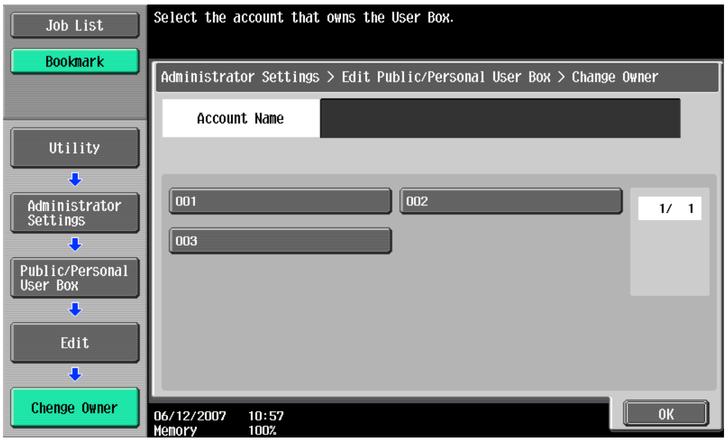
Select the owner of the User Box.

Administrator Settings > Edit Public/Personal User Box > Change Owner

Owner Name

06/11/2007 15:44
Memory 100%

– For [Change Account Name], select the desired user.



Select the account that owns the User Box.

Administrator Settings > Edit Public/Personal User Box > Change Owner

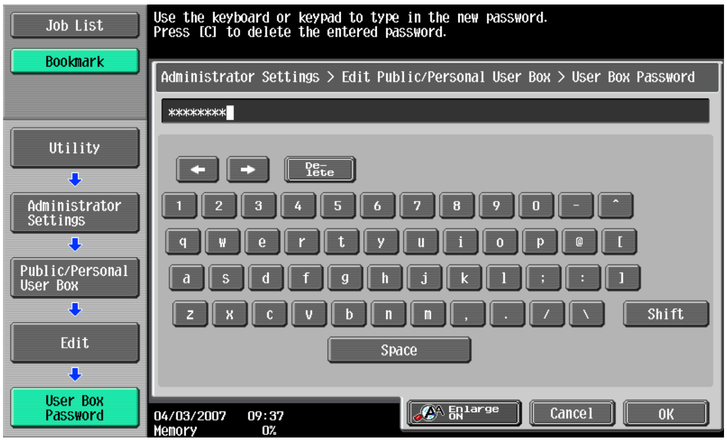
Account Name

06/12/2007 10:57
Memory 100%

6 Touch [OK].

7 Touch [Password].

8 Enter the new 8-digit User Box Password from the keyboard and keypad.



Use the keyboard or keypad to type in the new password.
Press [C] to delete the entered password.

Administrator Settings > Edit Public/Personal User Box > User Box Password

****

04/03/2007 09:37
Memory 0%

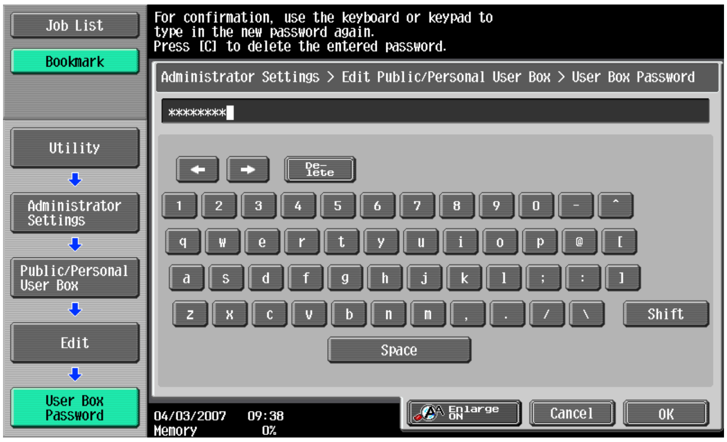
– Press the [C] key to clear all characters.
– Touch [Delete] to delete the last character entered.
– Touch [Shift] to show the upper case/symbol screen.
– Touch [Cancel] to go back to the screen shown in step 3.

9 Touch [OK].

? What happens if the User Box Password entered does not meet the requirements of the Password Rules when [Public] is set for the box type?

➔ If the User Box Password entered does not comply with the Password Rules with [Public] set for the box type, a message appears that tells that the User Box Password entered cannot be used. For details of the Password Rules, see **"Password Rules" on page 1-9**.

10 To prevent entry of a wrong password, enter the 8-digit User Box Password again.



For confirmation, use the keyboard or keypad to type in the new password again.
Press [C] to delete the entered password.

Administrator Settings > Edit Public/Personal User Box > User Box Password

****

04/03/2007 09:38
Memory 0%

– 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.

11 Touch [OK].

? What happens if there is a mismatch in the User Box Passwords?

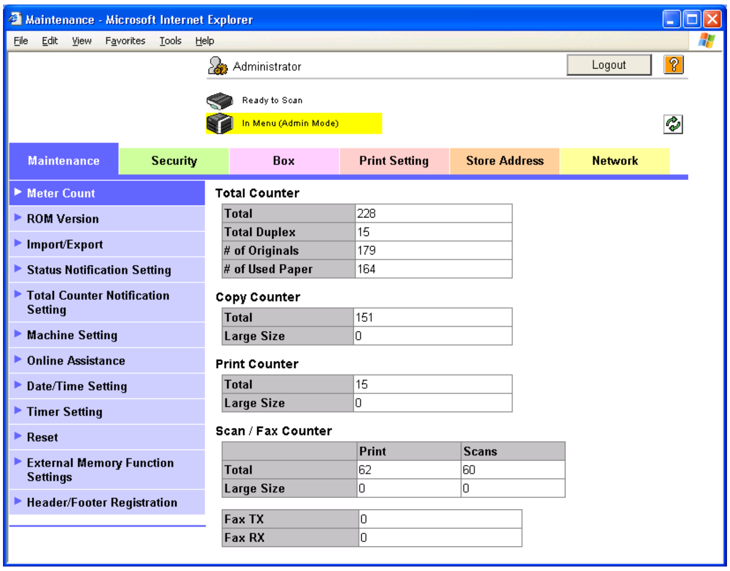
➔ If there is a mismatch in the User Box Passwords, a message appears that tells that there is a mismatch in the User Box Passwords. Perform steps 8 through 11 once again.

<From Web Connection>

✔ For the procedure to access the Admin Mode, see "Accessing the Administrator Settings" on page 2-2.

1 Start Web Connection and access the Admin Mode.

2 Click the [Box] tab and the [Open User Box] menu.



Total Counter

Total	228
Total Duplex	15
# of Originals	179
# of Used Paper	164

Copy Counter

Total	151
Large Size	0

Print Counter

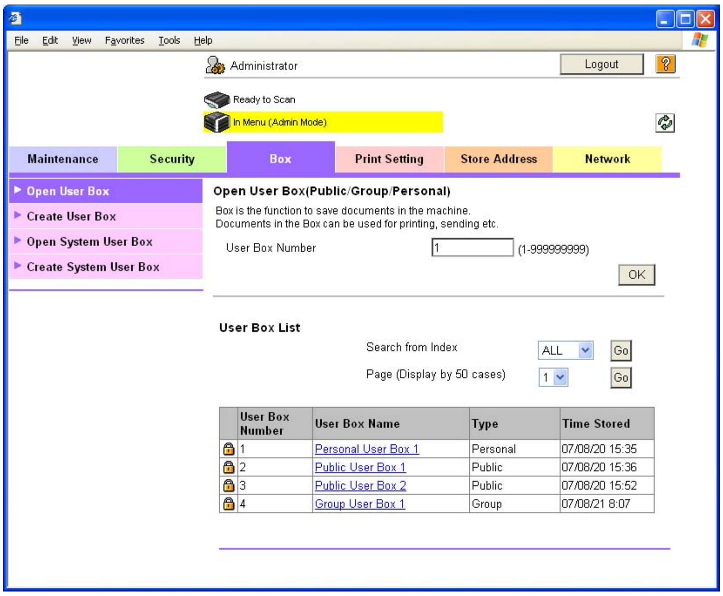
Total	15
Large Size	0

Scan / Fax Counter

	Print	Scans
Total	62	60
Large Size	0	0

Fax TX	0
Fax RX	0

3 Enter any given User Box Number and click [OK].



Open User Box(Public/Group/Personal)

Box is the function to save documents in the machine.
Documents in the Box can be used for printing, sending etc.

User Box Number 1 (1-999999999)

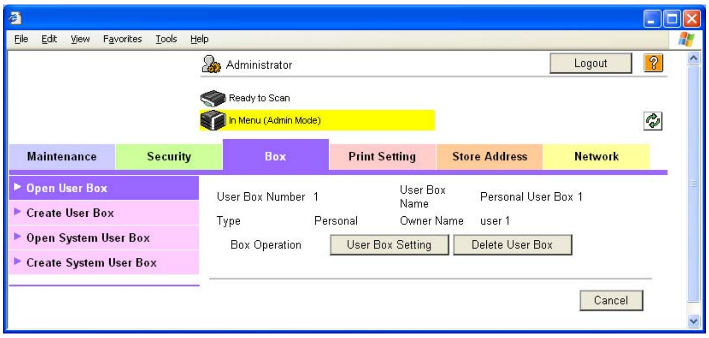
User Box List

Search from Index ALL

Page (Display by 50 cases) 1

User Box Number	User Box Name	Type	Time Stored
1	Personal User Box 1	Personal	07/08/20 15:35
2	Public User Box 1	Public	07/08/20 15:36
3	Public User Box 2	Public	07/08/20 15:52
4	Group User Box 1	Group	07/08/21 8:07

4 Click the [User Box Setting].



User Box Number 1 User Box Name Personal User Box 1

Type Personal Owner Name user 1

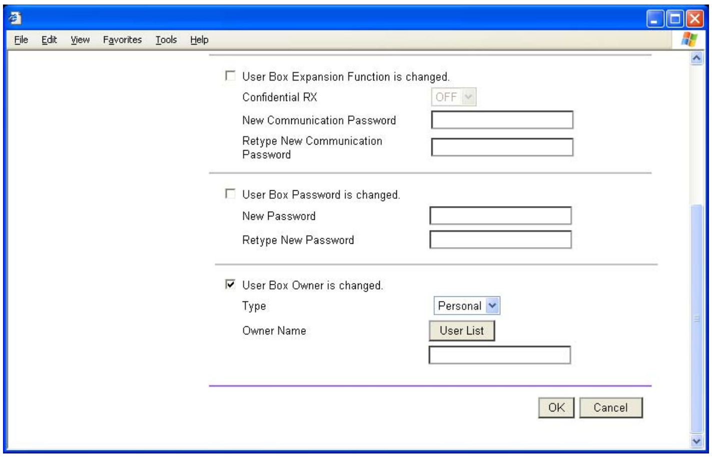
Box Operation

– Go to step 5 if the selected User Box Type is [Personal] or [Group], and go to step 6 if the selected User Box Type is [Public].

? What steps should be performed to delete a User Box?

➔ To delete a User Box, click [Delete User Box]. A message will then appear for confirming whether the specific User Box can definitely be deleted. Click [OK] to delete the specified User Box.

5 Click the "User Box Owner is changed." check box and change the user attributes of the box.



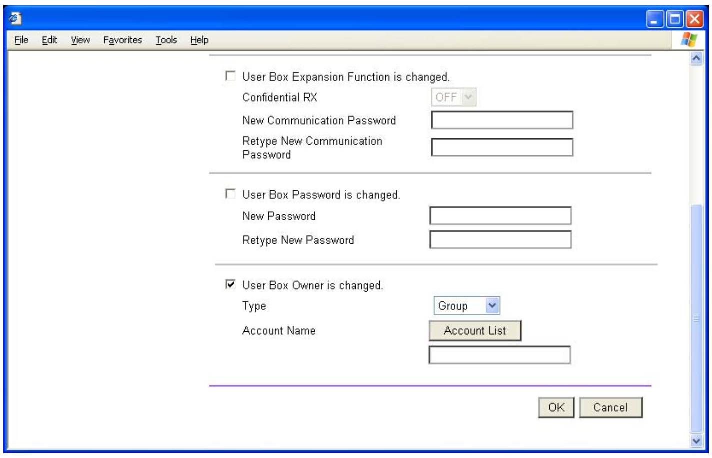
□ User Box Expansion Function is changed.
Confidential RX OFF
New Communication Password
Retype New Communication Password

□ User Box Password is changed.
New Password
Retype New Password

☑ User Box Owner is changed.
Type Personal
Owner Name User List

OK Cancel

– Clicking User List allows a account to be selected from among those registered in Account List.
– User Name can be directly entered in the Owner Name box.
– The following screen appears if the account attributes are to be changed.



□ User Box Expansion Function is changed.
Confidential RX OFF
New Communication Password
Retype New Communication Password

□ User Box Password is changed.
New Password
Retype New Password

☑ User Box Owner is changed.
Type Group
Account Name Account List

OK Cancel

– Click [Account List] to select a specific user from the registered User List.
– An account name may be directly entered in the Account Name box.

? What happens if User Box Owner is changed. is clicked?

➔ If the "User Box Owner is changed." check box is clicked, it clears the User Box Password. Be sure to set the User Box Password again.

➔ If the "User Box Owner is changed." check box is not clicked, the changes made will not be validated. If the changes need to be made, make sure that the "User Box Owner is changed." check box has been clicked.

? What steps can be taken to change the User Box Type?

➔ To change the User Box Type, click the Type pull-down menu and select the desired box type.

? What precautions should be used when entering the Owner Name?

➔ Enter the User Name that has been registered through User Registration for the Owner Name.

? What precautions should be account when entering the Account Name?

➔ Enter the Account Name that has been registered through Account Registration for the Account Name.

6 Click the "User Box Password is changed." check box and enter the User Box Password.

? What precautions should be used when entering the User Box Password?

➔ If the User Box Type has been set to [Public], enter a User Box Password that meets the requirements of the Password Rules in the "New Password" box. For details of the Password Rules, see **"Password Rules" on page 1-9**.

➔ In the "Retype New Password" box, enter the same User Box Password as that entered in the "New Password" box.

7 Click the [OK].

? What happens if the User Box Password entered does not meet the requirements of the Password Rules when Public is set for User Box Type?

➔ If the User Box Password entered does not meet the requirements of the Password Rules when [Public] is set for User Box Type, a message appears that tells that the User Box Password entered cannot be used. Click [OK] to go back to the screen of step 4. Perform steps 4 through 7 once again. For details of the Password Rules, see **"Password Rules" on page 1-9**.

? What happens if there is a mismatch in the User Box Passwords?

➔ If there is a mismatch in the User Box Password between that entered in "New Password" and that entered in "Retype New Password," a message appears that tells that there is a mismatch in the User Box Password. Enter the correct User Box Password.

? What if no Owner Name, or a wrong one, has been entered?

➔ If no Owner Name is entered, a message appears that tells that no Owner Names have been entered. Enter the correct Owner Name.

➔ If a user name not registered with the machine is entered in the "Owner Name" box, a message appears that tells that the Owner Name entered in the box is illegal. Click [OK] to go back to the screen of step 3. Perform steps 3 through 7 once again.

? What if no Account Name, or a wrong one, has been entered?

➔ If no Account Name is entered, a message appears that tells that no Account Names have been entered. Enter the correct Account Name.

➔ If a user name not registered with the machine is entered in the "Account Name" box, a message appears that tells that the Account Name entered in the box is illegal. Click [OK] to go back to the screen of step 3. Perform steps 3 through 7 once again.

2.10 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.

2.10.1 Changing the Administrator Password

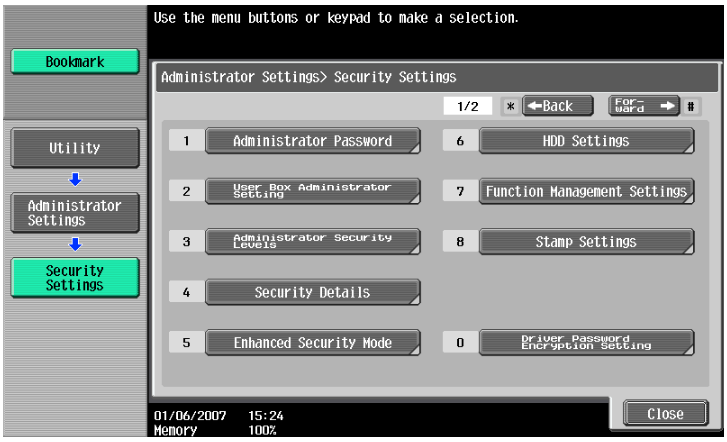
Note
Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.

<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 the Enhanced Security Mode" on page 2-11**.

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

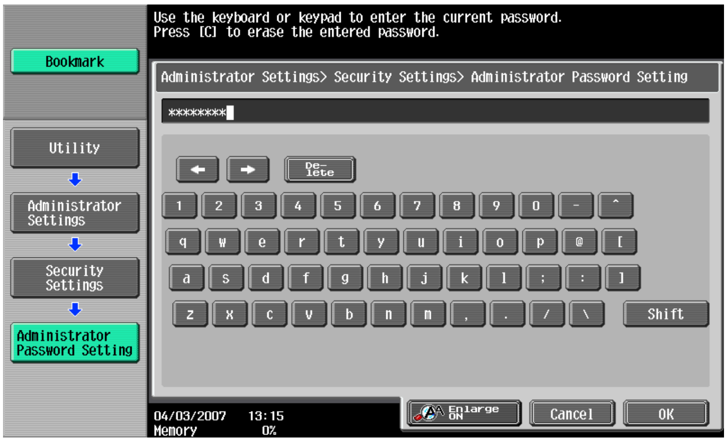
2 Touch [Administrator Password].



Use the menu buttons or keypad to make a selection.

Administrator Settings> Security Settings

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



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

Administrator Settings> Security Settings> Administrator Password Setting

****

- 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.

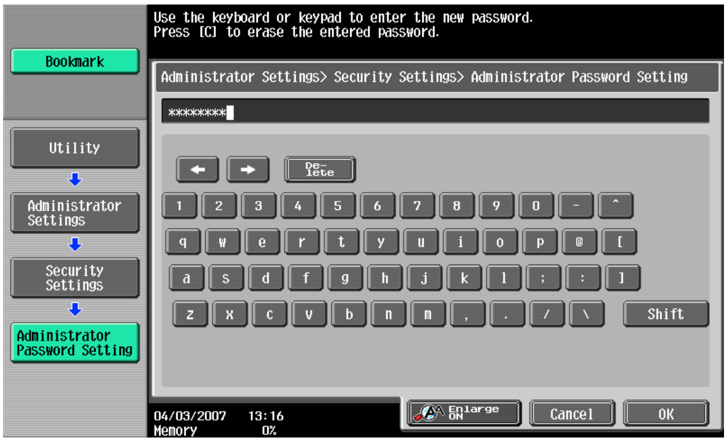
4 Touch [OK].

? 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 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) 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.



Use the keyboard or keypad to enter the new password.
Press [C] to erase the entered password.

Administrator Settings> Security Settings> Administrator Password Setting

****

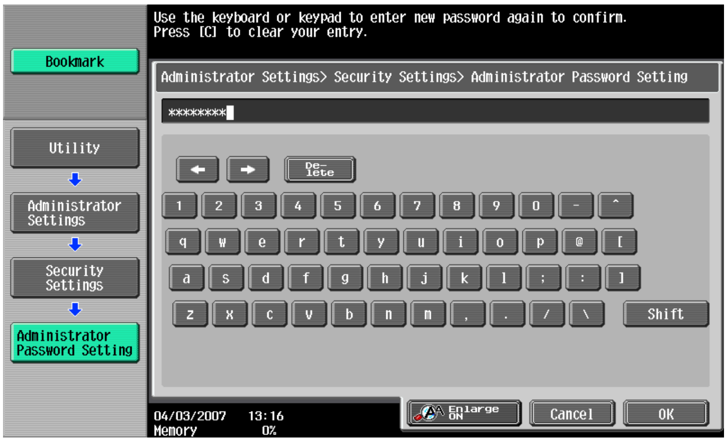
– Press the [C] key to clear all characters.
– Touch [Delete] to delete the last character entered.
– Touch [Shift] to show the upper case/symbol screen.
– Touch [Cancel] to go back to the Security Settings screen.

6 Touch [OK].

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

➔ If the Administrator Password entered does not comply with the Password Rules, a message appears that tells that the Administrator Password entered cannot be used. Enter the correct Administrator Password. For details of the Password Rules, see **"Password Rules" on page 1-9**.

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



Use the keyboard or keypad to enter new password again to confirm.
Press [C] to clear your entry.

Administrator Settings> Security Settings> Administrator Password Setting

****

04/03/2007 13:16
Memory 0%

- 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.

2.11 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 Image Data Encryption Passphrase when the optional Security Kit SC-505 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 Image Data Encryption Passphrase, encrypt the image data which is registered by secure print or the image data which is saved in the user boxes and protect the data. The HDD Lock Password and Image Data Encryption Passphrase entered are displayed as "*."

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 Image Data Encryption Passphrase. 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 Image Data Encryption Passphrase.

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

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

2.11.1 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

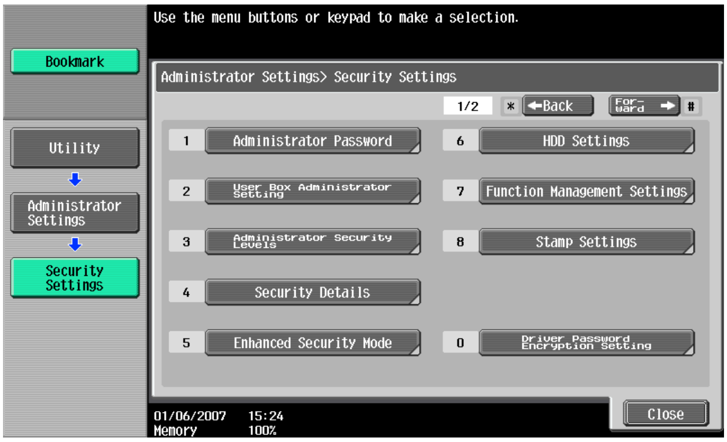
Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.

<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 the Enhanced Security Mode" on page 2-11**.

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

2 Touch [HDD Settings].

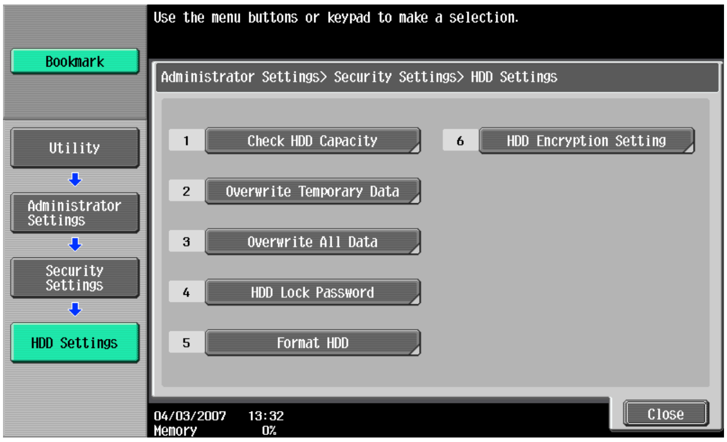


Use the menu buttons or keypad to make a selection.

Administrator Settings> Security Settings

01/06/2007 15:24
Memory 100%

3 Touch [HDD Lock Password].

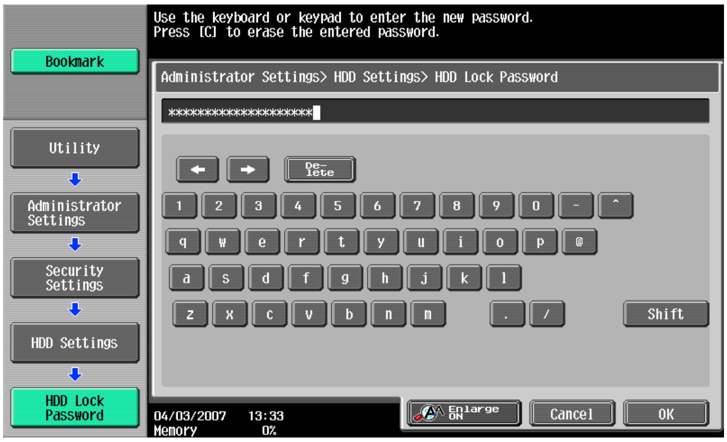


Use the menu buttons or keypad to make a selection.

Administrator Settings> Security Settings> HDD Settings

04/03/2007 13:32
Memory 0%

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



Use the keyboard or keypad to enter the new password.
Press [C] to erase the entered password.

Administrator Settings> HDD Settings> HDD Lock Password

****

04/03/2007 13:33
Memory 0%

- 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.

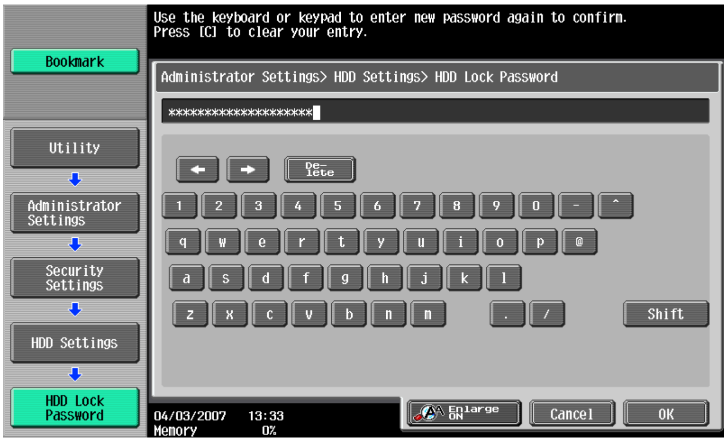
5 Touch [OK].

? 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 1-9**.

➔ To change the HDD Lock Password, see **"Changing the HDD Lock Password" on page 2-59**.

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



Use the keyboard or keypad to enter new password again to confirm.
Press [C] to clear your entry.

Administrator Settings> HDD Settings> HDD Lock Password

****

04/03/2007 13:33
Memory 0%

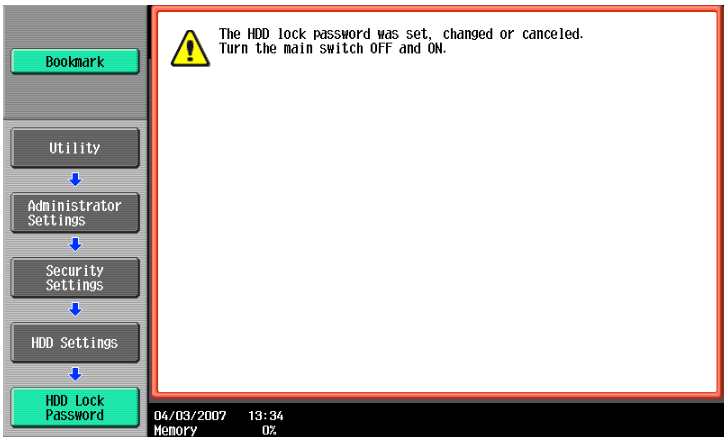
– Press the [C] key to clear all characters.
– Touch [Delete] to delete the last character entered.
– Touch [Shift] to show the upper case/symbol screen.
– Touch [Cancel] to go back to the HDD Settings screen.

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. Perform steps 4 and 5 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.



The HDD lock password was set, changed or canceled.
Turn the main switch OFF and ON.

04/03/2007 13:34
Memory 0%

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.

2.11.2 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

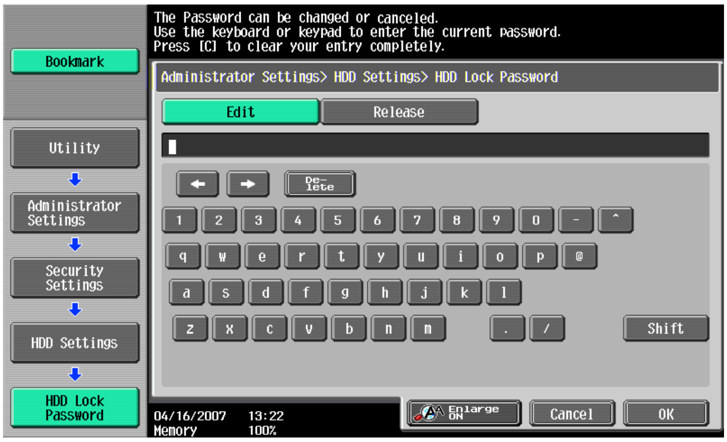
Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.

<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 2-56**.

1 Call the HDD Lock Password entry screen to the display from the control panel.

2 Enter the currently registered 20-digit HDD Lock Password from the keyboard and keypad.



The Password can be changed or canceled.
Use the keyboard or keypad to enter the current password.
Press [C] to clear your entry completely.

Administrator Settings> HDD Settings> HDD Lock Password

04/16/2007 13:22
Memory 100%

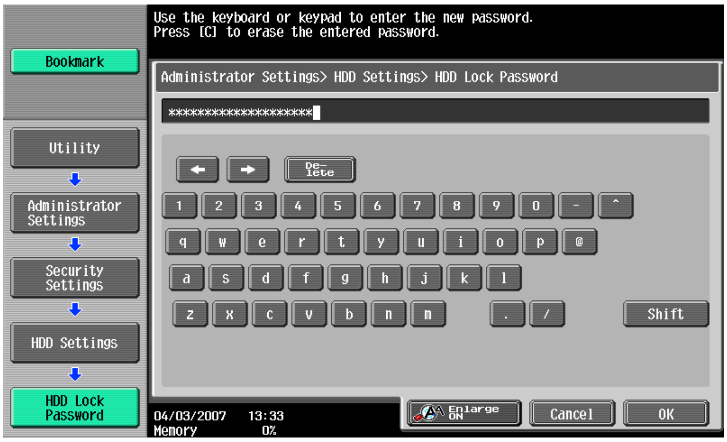
- Press the [C] key to clear all characters.
- Touch [Delete] to delete the last character entered.
- Touch [Shift] to show the upper case/symbol screen.
- Touch [Cancel] to go back to the HDD Settings screen.

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



Use the keyboard or keypad to enter the new password.
Press [C] to erase the entered password.

Administrator Settings> HDD Settings> HDD Lock Password

****

04/03/2007 13:33
Memory 0%

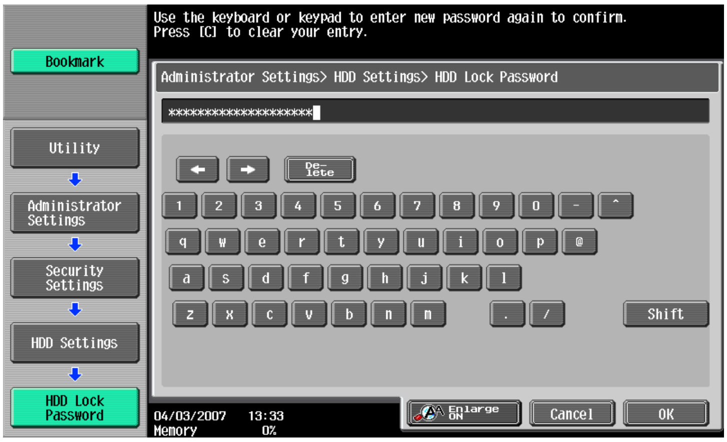
- Press the [C] key to clear all characters.
- Touch [Delete] to delete the last character entered.
- Touch [Shift] to show the upper case/symbol screen.
- Touch [Cancel] to go back to the HDD Settings screen.

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 1-9**.

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



Use the keyboard or keypad to enter new password again to confirm.
Press [C] to clear your entry.

Administrator Settings> HDD Settings> HDD Lock Password

****

04/03/2007 13:33
Memory 0%

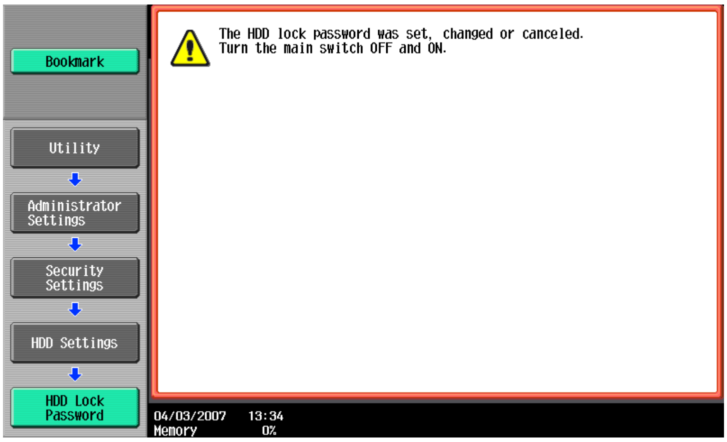
- Press the [C] key to clear all characters.
- Touch [Delete] to delete the last character entered.
- Touch [Shift] to show the upper case/symbol screen.
- Touch [Cancel] to go back to the HDD Settings screen.

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.



The HDD lock password was set, changed or canceled.
Turn the main switch OFF and ON.

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.

2.11.3 Setting the Image Data Encryption Passphrase

✎...

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.

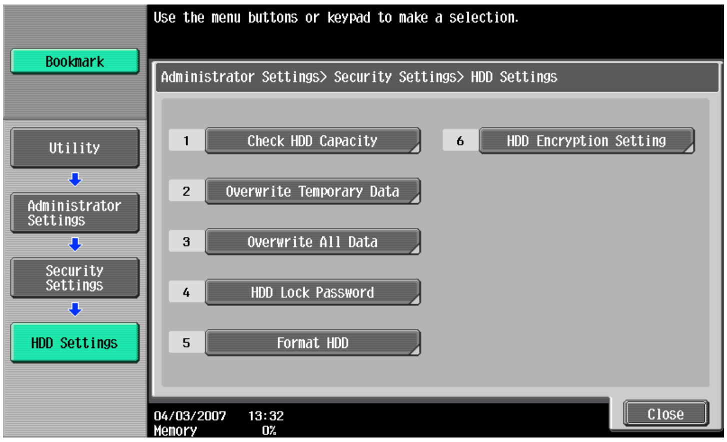
Image Data Encryption Passphrase cannot be deleted when the Enhanced Security Mode is set to ON. To delete the Image Data Encryption Passphrase, the Enhanced Security Mode must be turned OFF temporarily.
Image Data Encryption Passphrase can be set or changed when the Enhanced Security Mode is set to ON.

<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 2-56**.

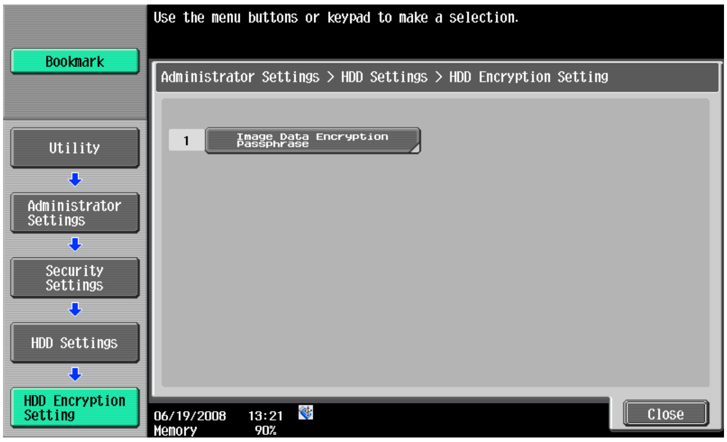
1 Call the HDD Settings to the screen from the control panel.

2 When Touch [HDD Encryption Setting], [Image Data Encryption Passphrase] appears.



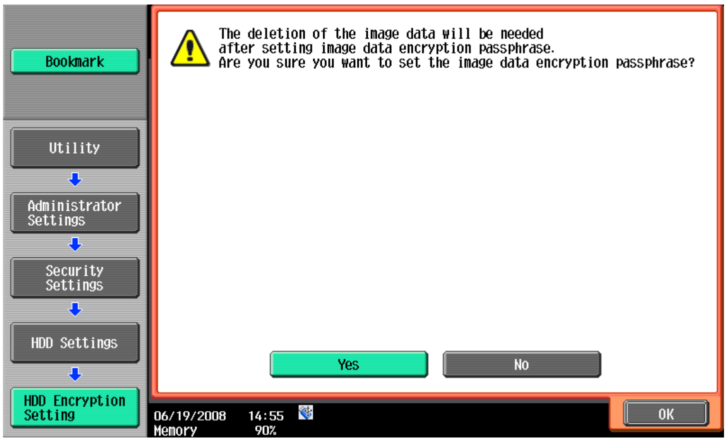
Use the menu buttons or keypad to make a selection.

3 Touch [Image Data Encryption Passphrase].



Use the menu buttons or keypad to make a selection.

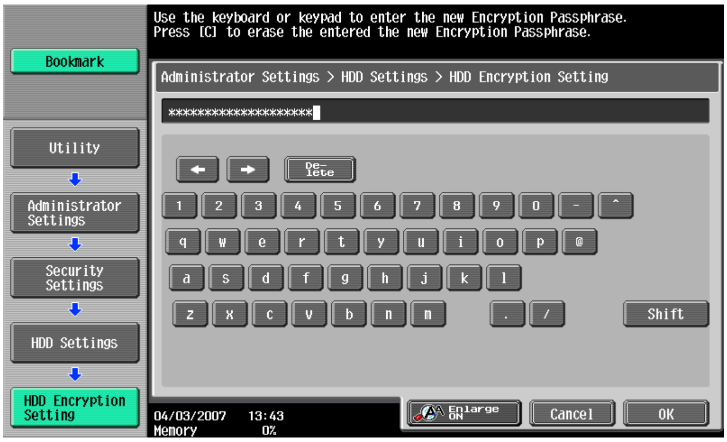
4 A message appears that confirms whether or not the setting of the Image Data Encryption Passphrase is to be continued. Select [Yes] and touch [OK].



The deletion of the image data will be needed
after setting image data encryption passphrase.
Are you sure you want to set the image data encryption passphrase?

06/19/2008 14:55
Memory 90%

5 Enter the new 20-digit Image Data Encryption Passphrase from the keyboard and keypad.



Use the keyboard or keypad to enter the new Encryption Passphrase.
Press [C] to erase the entered the new Encryption Passphrase.

Administrator Settings > HDD Settings > HDD Encryption Setting

****

04/03/2007 13:43
Memory 0%

– 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.

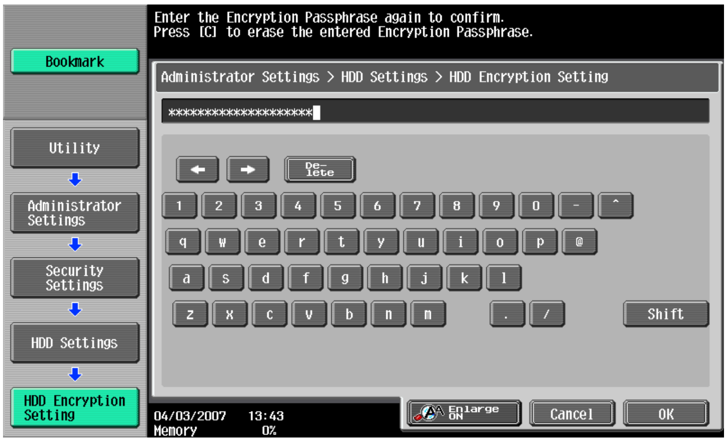
6 Touch [OK].

? What happens if the Image Data Encryption Passphrase entered does not meet the requirements of the Password Rules?

➔ If the Image Data Encryption Passphrase entered does not comply with the Password Rules, a message appears that tells that the Image Data Encryption Passphrase entered cannot be used. Enter the correct Image Data Encryption Passphrase. For details of the Password Rules, see **"Password Rules" on page 1-9**.

➔ To change the Image Data Encryption Passphrase, see **"Changing the Image Data Encryption Passphrase" on page 2-67**.

7 To prevent entry of a wrong Image Data Encryption Passphrase, enter the 20-digit Image Data Encryption Passphrase once again.



Enter the Encryption Passphrase again to confirm.
Press [C] to erase the entered Encryption Passphrase.

Administrator Settings > HDD Settings > HDD Encryption Setting

****

04/03/2007 13:43
Memory 0%

- 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.

8 Touch [OK].

? What if there is a mismatch in the Image Data Encryption Passphrases?

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

9 Select the image data formatting method.

- HDD Format

  Outline: Image data is deleted logically.

  Date migration condition: Abbreviated address, Group address, Program address, Box information, User registration, Group registration, Program memory are migrated, however, Audit log, Job history, Fax journal and encrypted PDF file are deleted.

  Image data deletion condition: As it is the logical deletion, remaining information of the data remains at HDD.

  Execution time: Around 30 seconds.

  Operation method: Go to step 10 when HDD format is selected.

- Overwrite image data

  Outline: Image data currently set is deleted.

  Data migration condition: All data excepting image data is migrated.

  Image data deletion condition: When Primary data overwrite function is ON, Image data is overwritten according to the setting condition of the Overwrite Primary data. When the function is OFF, remaining data remains at HDD.

  Execution time: The time depends on the amount of image.

  Operation method: Go to step 13, when Overwrite Image data is selected.

- Overwrite All data

  Outline: HDD partitions that store image data are overwritten according to the set mode.

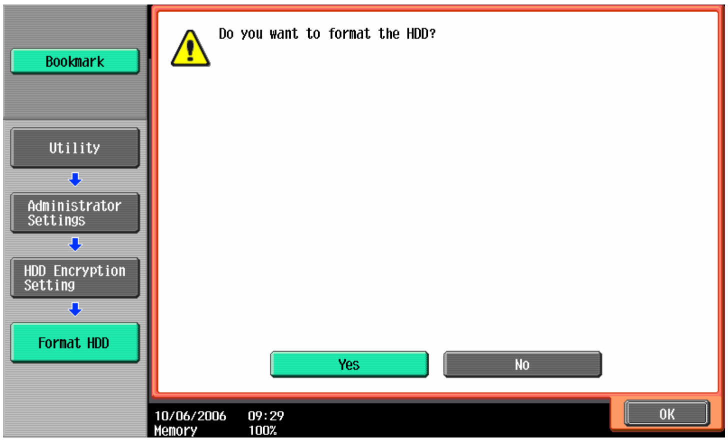
  Data migration condition: Abbreviated address, Group address, Program address, Box information, User registration, Group registration, Program memory are migrated, however, Audit log, Job history, Fax journal and encrypted PDF file are deleted.

  Image data delete condition: All image data including remaining one is deleted.

  Execution time: Execution time varies between 1 hour or less and 4 hours according to the mode set.

  Operation method: Go to step 16 when Overwrite All data is selected.

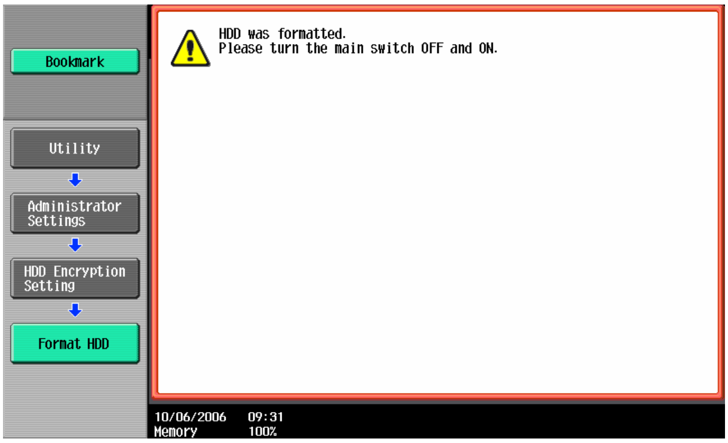
10 A message will appear that confirms whether the HDD may be formatted or not.
Select the [Yes] and touch [OK].



Do you want to format the HDD?

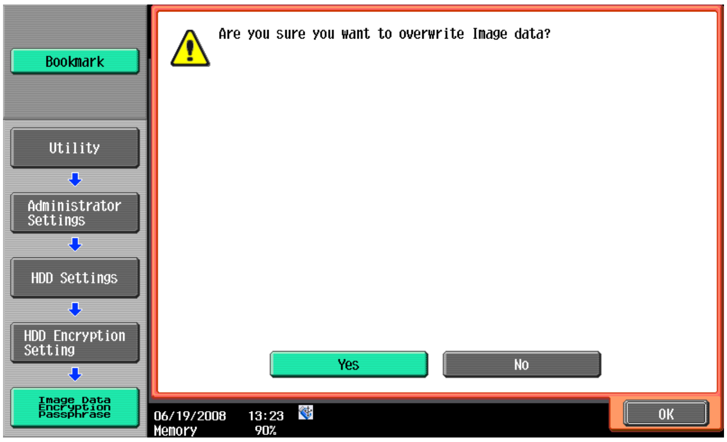
11 "Now formatting HDD. Please wait." message appears.

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.

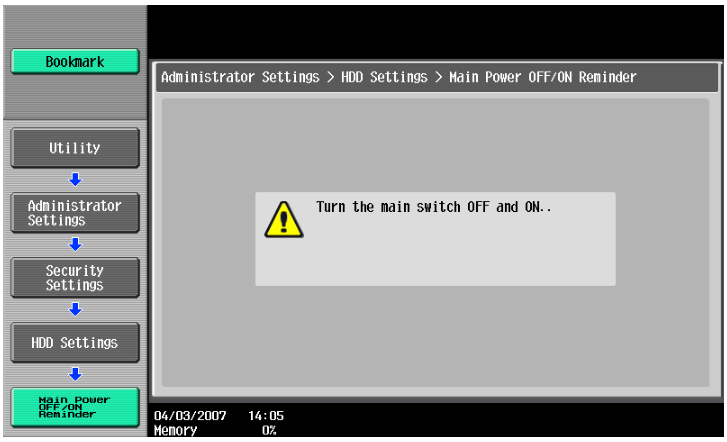
13 A message appears asking whether you want to overwrite image data. Select [YES] and touch [OK].



Are you sure you want to overwrite Image data?

14 "All data is being overwritten and cleared. Please wait." message appears.

15 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.

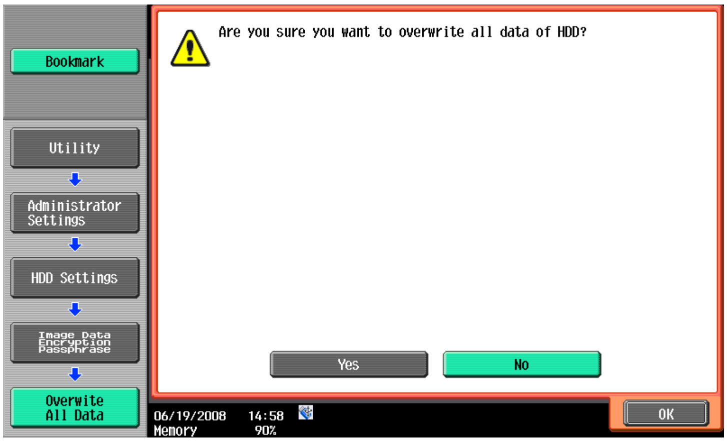


Administrator Settings > HDD Settings > Main Power OFF/ON Reminder

Turn the main switch OFF and ON..

16 Select the desired mode and touch [Delete].
The overwrite method can be chosen from eight different modes of [Mode 1] to [Mode 8]. Overwrite All Data takes about 1 hour in [Mode 1] at the minimum and about 4 hours in [Mode 8] at the maximum. For the overwrite methods of [Mode 1] to [Mode 8], see **"Setting the Overwrite All Data function" on page 2-78**.

17 A message appears asking whether you want to overwrite all data. Select [YES] and touch [OK].



Are you sure you want to overwrite all data of HDD?

18 "All data is being overwritten and cleared. Please wait." message appears.

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.

2.11.4 Changing the Image Data Encryption Passphrase

Note

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

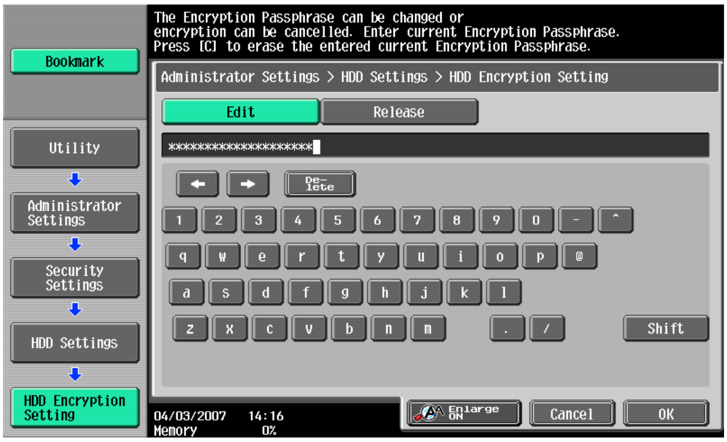
Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.

<Setting can be made only from the control panel>

✔ For the procedure to call the Image Data Encryption Passphrase entry screen to the display, see steps 1 through 3 of **"Setting the Image Data Encryption Passphrase" on page 2-62**.

1 Call the Image Data Encryption Passphrase entry screen to the display.

2 Enter the currently registered 20-digit Image Data Encryption Passphrase from the keyboard and keypad.



The Encryption Passphrase can be changed or encryption can be cancelled. Enter current Encryption Passphrase. Press [C] to erase the entered current Encryption Passphrase.

Administrator Settings > HDD Settings > HDD Encryption Setting

****

04/03/2007 14:16
Memory 0%

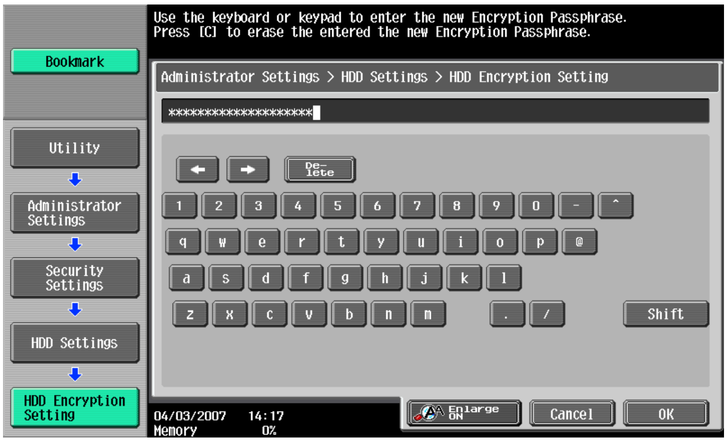
- Press the [C] key to clear all characters.
- Touch [Delete] to delete the last character entered.
- Touch [Shift] to show the upper case/symbol screen.
- Touch [Cancel] to go back to the HDD Settings screen.

3 Select the [Edit] and touch [OK].

? What if there is a mismatch in the Image Data Encryption Passphrase?

➔ If there is a mismatch in the Image Data Encryption Passphrase, a message appears that tells that there is a mismatch in the Image Data Encryption Passphrase. Enter the correct Image Data Encryption Passphrase once again.

4 Enter the new 20-digit Image Data Encryption Passphrase from the keyboard and keypad.



Use the keyboard or keypad to enter the new Encryption Passphrase.
Press [C] to erase the entered the new Encryption Passphrase.

Administrator Settings > HDD Settings > HDD Encryption Setting

****

04/03/2007 14:17
Memory 0%

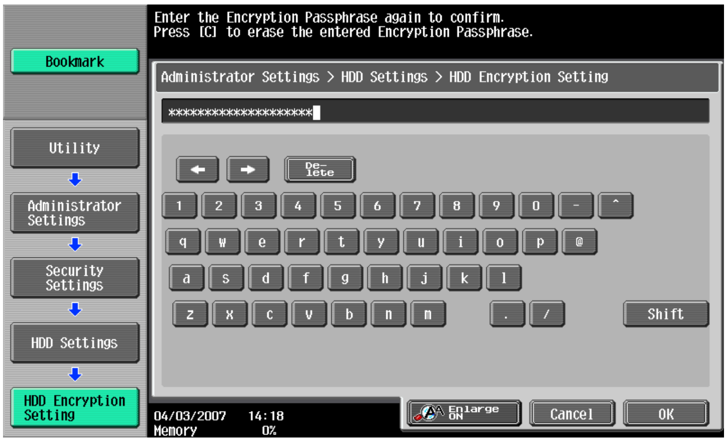
- Press the [C] key to clear all characters.
- Touch [Delete] to delete the last character entered.
- Touch [Shift] to show the upper case/symbol screen.
- Touch [Cancel] to go back to the HDD Settings screen.

5 Touch [OK].

? What happens if the Image Data Encryption Passphrase entered does not meet the requirements of the Password Rules?

➔ If the Image Data Encryption Passphrase entered does not comply with the Password Rules, a message appears that tells that the Image Data Encryption Passphrase entered cannot be used. Enter the correct Image Data Encryption Passphrase. For details of the Password Rules, see **"Password Rules" on page 1-9**.

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



Enter the Encryption Passphrase again to confirm.
Press [C] to erase the entered Encryption Passphrase.

Administrator Settings > HDD Settings > HDD Encryption Setting

****

04/03/2007 14:18
Memory 0%

- 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 Image Data Encryption Passphrase?

➔ If there is a mismatch in the Image Data Encryption Passphrase, a message appears that tells that there is a mismatch in the Image Data Encryption Passphrase. Perform steps 4 through 7 once again.

8 Select the image data formatting method.

- HDD Format

  Outline: Image data is deleted logically.

  Date migration condition: Abbreviated address, Group address, Program address, Box information, User registration, Group registration, Program memory are migrated, however, Audit log, Job history, Fax journal and encrypted PDF file are deleted.

  Image data deletion condition: As it is the logical deletion, remaining information of the data remains at HDD.

  Execution time: Around 30 seconds.

  Operation method: Go to step 9 when HDD format is selected.

- Overwrite image data

  Outline: Image data currently set is deleted.

  Data migration condition: All data excepting image data is migrated.

  Image data deletion condition: When Primary data overwrite function is ON, Image data is overwritten according to the setting condition of the Overwrite Primary data. When the function is OFF, remaining data remains at HDD.

  Execution time: The time depends on the amount of image.

  Operation method: Go to step 12, when Overwrite Image data is selected.

- Overwrite All data

  Outline: HDD partitions that store image data are overwritten according to the set mode.

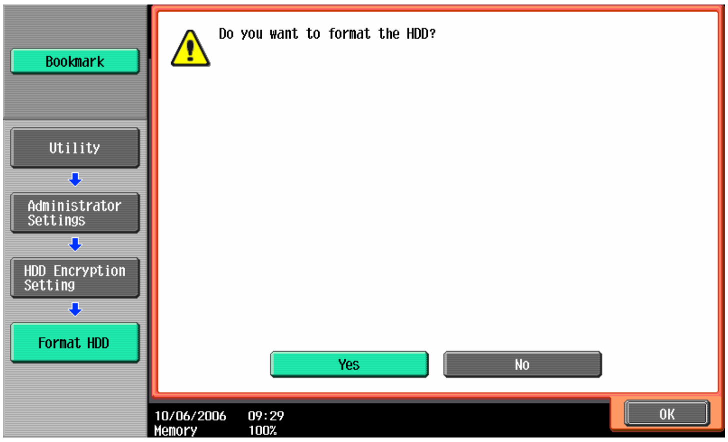
  Data migration condition: Abbreviated address, Group address, Program address, Box information, User registration, Group registration, Program memory are migrated, however, Audit log, Job history, Fax journal and encrypted PDF file are deleted.

  Image data delete condition: All image data including remaining one is deleted.

  Execution time: Execution time varies between 1 hour or less and 4 hours according to the mode set.

  Operation method: Go to step 15 when Overwrite All data is selected.

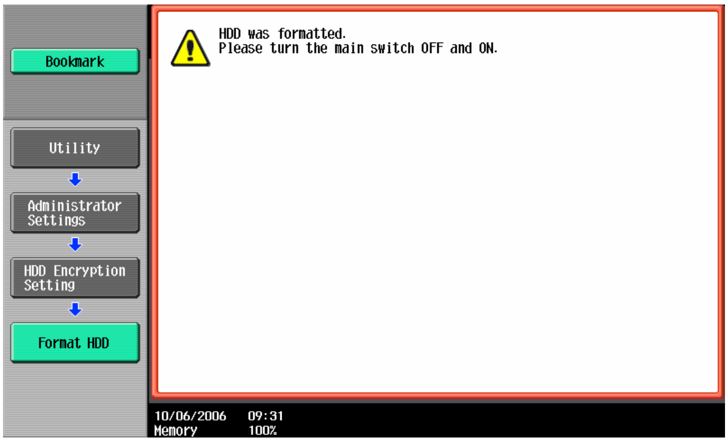
9 A message will appear that confirms whether the HDD may be formatted or not.
Select the [Yes] and touch [OK].



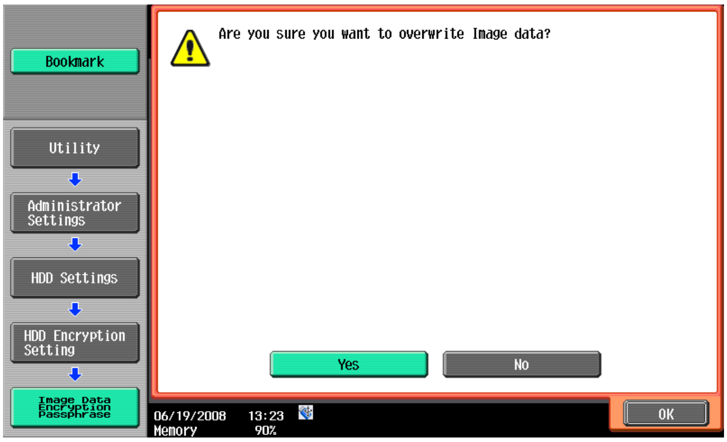
Do you want to format the HDD?

10 "Now formatting HDD. Please wait." message appears.

11 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.

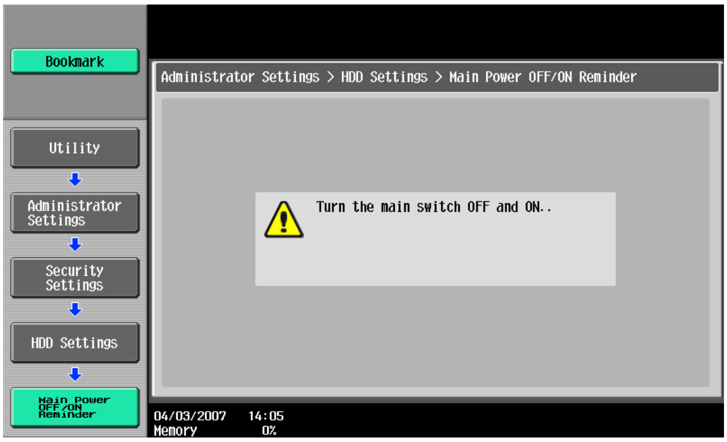

HDD was formatted.
Please turn the main switch OFF and ON.

12 A message appears asking whether you want to overwrite image data. Select [YES] and touch [OK].


Are you sure you want to overwrite Image data?

13 "All data is being overwritten and cleared. Please wait." message appears.

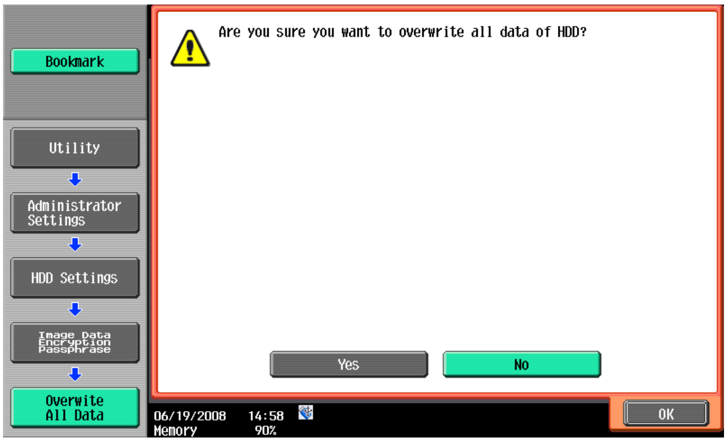
14 Make sure that a message appears prompting you to turn OFF and then ON the main power switch. Now, turn OFF and then turn ON the main power switch.


Administrator Settings > HDD Settings > Main Power OFF/ON Reminder

Turn the main switch OFF and ON..

15 Select the desired mode and touch [Delete].
The overwrite method can be chosen from eight different modes of [Mode 1] to [Mode 8]. Overwrite All Data takes about 1 hour in [Mode 1] at the minimum and about 4 hours in [Mode 8] at the maximum. For the overwrite methods of [Mode 1] to [Mode 8], see **"Setting the Overwrite All Data function" on page 2-78**.

16 A message appears asking whether you want to overwrite all data. Select [YES] and touch [OK].



Are you sure you want to overwrite all data of HDD?

17 "All data is being overwritten and cleared. Please wait." message appears.

18 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.

2.12 Protecting Data Stored in the Flash Memory

The administrator settings in this machine allow setting or changing the Flash Memory Lock Password that is used to authenticate the Administrator of the machine.

Should the flash memory be removed unawares, the Flash Memory Lock Password locks the flash memory protecting data contained in it. The Flash Memory Lock Password entered is displayed as "*."

✎...

Note

Set unique password for Flash Memory Lock Password. Do not set any number that can easily guessed from birthdays, employee identification numbers, and the like for Flash Memory Lock Password. Change the Flash Memory Lock Password at regular intervals.

Make sure that nobody but the Administrator of the machine comes to know the Flash Memory Lock Password.

✎...

Note

When the Flash Memory Lock Password is set, flash memory verification is carried out when the machine is started. If the flash memory is illegally replaced with another and the flash memory cannot be unlocked by the Flash Memory Lock Password, the machine sounds an alert and stops booting while displaying an hourglass icon on the control panel. If the flash memory does not have the Flash Memory Lock Password setting, the control panel displays Service Call "SC-D303", a message that tells there is a mismatch between the flash memory and the Flash Memory Lock Password.

The flash memory has the following function. Even if the flash memory is illegally removed or replaced with another, detection of a wrong Flash Memory Password five consecutive times will lock the authentication function. Leak of data can thus be prevented.

2.12.1 Setting the Flash Memory Lock Password

✎...

Note

When the main power switch is turned OFF and ON, wait at least 10 seconds to turn it ON again after turning it OFF. If there is no interval between turning the main power switch OFF and ON, 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.

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

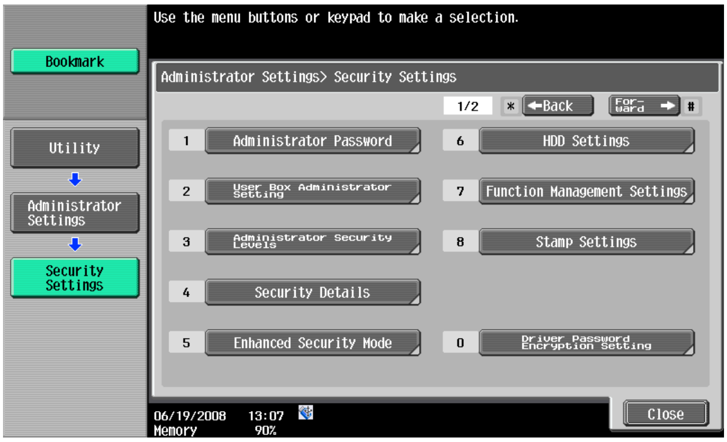
Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.

<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 the Enhanced Security Mode" on page 2-11**.

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

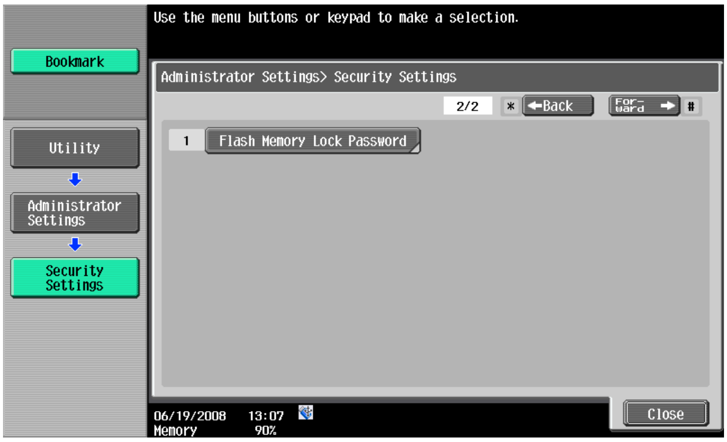
2 Touch [Forward].



Use the menu buttons or keypad to make a selection.

Administrator Settings> Security Settings

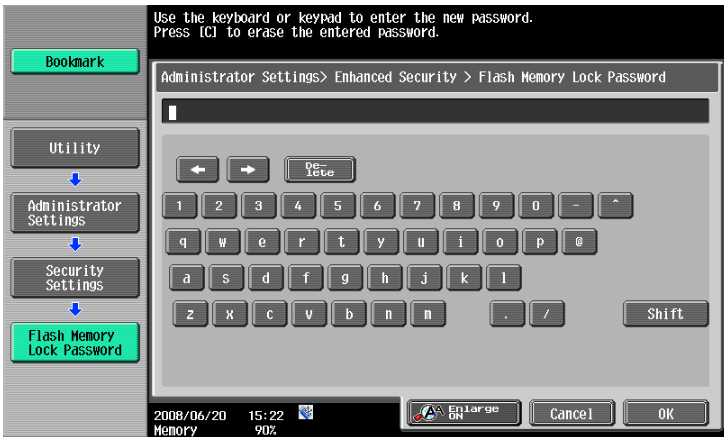
3 Touch [Flash Memory Lock Password].



Use the menu buttons or keypad to make a selection.

Administrator Settings> Security Settings

4 Enter the 20-digit Flash Memory Lock Password from the keyboard and key pad.



Use the keyboard or keypad to enter the new password.
Press [C] to erase the entered password.

Administrator Settings> Enhanced Security > Flash Memory Lock Password

- 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.

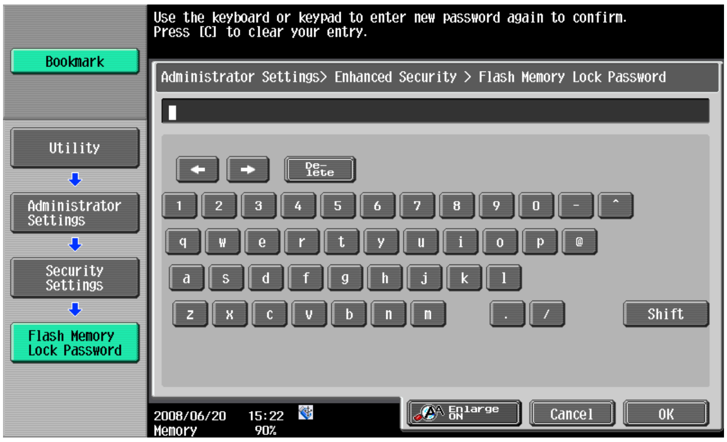
5 Touch [OK].

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

➔ If the Flash Memory Password entered does not comply with the Password Rules, a message appears saying that the Flash Memory Password entered cannot be used. Enter the correct Flash Memory Lock Password. For details of the Password Rules, see **"Password Rules" on page 1-9**.

➔ To change the Flash Memory Lock Password, see **"Changing the Flash Memory Lock Password" on page 2-75**

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



Use the keyboard or keypad to enter new password again to confirm.
Press [C] to clear your entry.

Administrator Settings> Enhanced Security > Flash Memory Lock Password

2008/06/20 15:22
Memory 90%

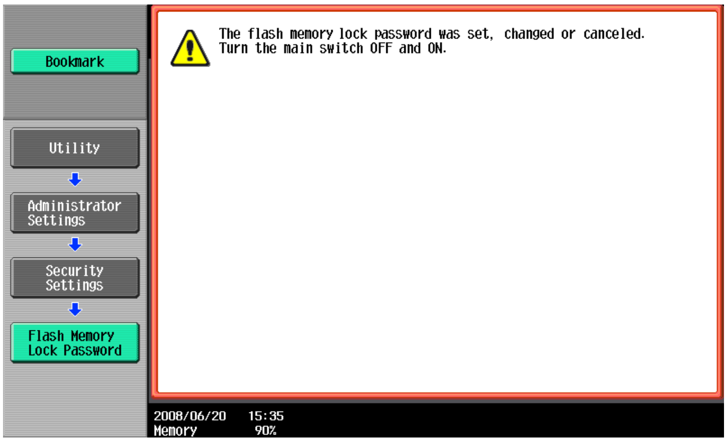
- Press the [C] key to clear all characters.
- Touch [Delete] to delete the last character entered.
- Touch [Shift] to show the upper case/symbol screen.
- Touch [Cancel] to go back to the Security Settings screen.

7 Touch [OK].

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

➔ If there is a mismatch in the Flash Memory Lock Passwords, a message appears saying that there is a mismatch in the Flash Memory Lock Passwords. Perform steps 4 to 6 once again.

8 Make sure that a message appears promoting you to turn OFF and ON the main power switch. Turn OFF and ON the main power switch.



The flash memory lock password was set, changed or canceled.
Turn the main switch OFF and ON.

2008/06/20 15:35
Memory 90%

Note

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

2.12.2 Changing the Flash Memory Lock 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.

✎...

Note

When the main power switch is turned OFF and ON, wait at least 10 seconds to turn it ON again after turning it OFF. If there is no interval between turning the main power switch OFF and ON, 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.

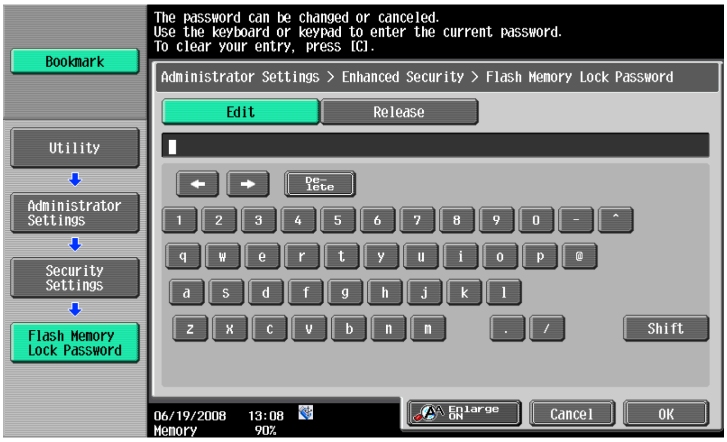
Turn off the sub power switch → Turn off the main power switch → Turn on the main power switch → Turn on the sub power switch.

<Setting can be made only from the control panel>

✔ To call the Flash Memory Lock Password entry screen to the display, see steps 1 through 3 of **"Setting the Flash Memory Lock Password" on page 2-72**.

1 Call the Flash Memory Lock Password entry screen to the display from the control panel.

2 Enter the 20-digit Flash Memory Lock Password from the keyboard and key pad.



The password can be changed or canceled.
Use the keyboard or keypad to enter the current password.
To clear your entry, press [C].

Administrator Settings > Enhanced Security > Flash Memory Lock Password

06/19/2008 13:08
Memory 90%

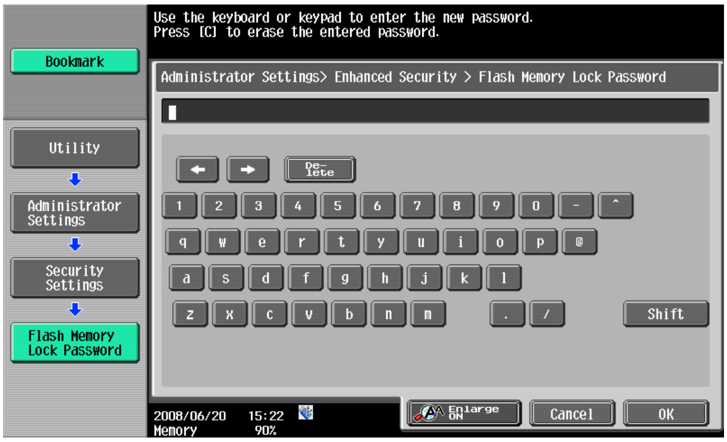
- Press the [C] key to clear all characters.
- Touch [Delete] to delete the last character entered.
- Touch [Shift] to show the upper case/symbol screen.
- Touch [Cancel] to go back to the Security Settings screen.

3 Select [Edit] and touch [OK].

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

→ If the Flash Memory Password entered does not comply with the Password Rules, a message appears saying that the Flash Memory Password entered cannot be used. Enter the correct Flash Memory Lock Password. For details of the Password Rules.

4 Enter the 20-digit new Flash Memory Lock Password from the keyboard and key pad.



Use the keyboard or keypad to enter the new password.
Press [C] to erase the entered password.

Administrator Settings> Enhanced Security > Flash Memory Lock Password

2008/06/20 15:22
Memory 90%

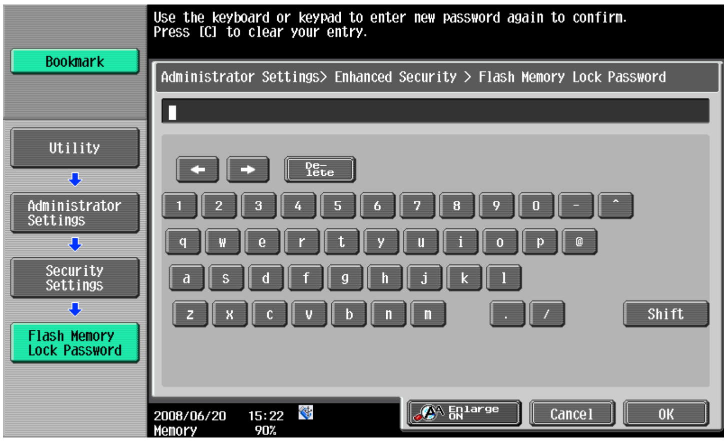
- Press the [C] key to clear all characters.
- Touch [Delete] to delete the last character entered.
- Touch [Shift] to show the upper case/symbol screen.
- Touch [Cancel] to go back to the Security Settings screen.

5 Touch [OK].

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

→ If the Flash Memory Password entered does not comply with the Password Rules, a message appears saying that the Flash Memory Password entered cannot be used. Enter the correct Flash Memory Lock Password. For details of the Password Rules, see **"Password Rules" on page 1-9**.

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



Use the keyboard or keypad to enter new password again to confirm.
Press [C] to clear your entry.

Administrator Settings> Enhanced Security > Flash Memory Lock Password

2008/06/20 15:22
Memory 90%

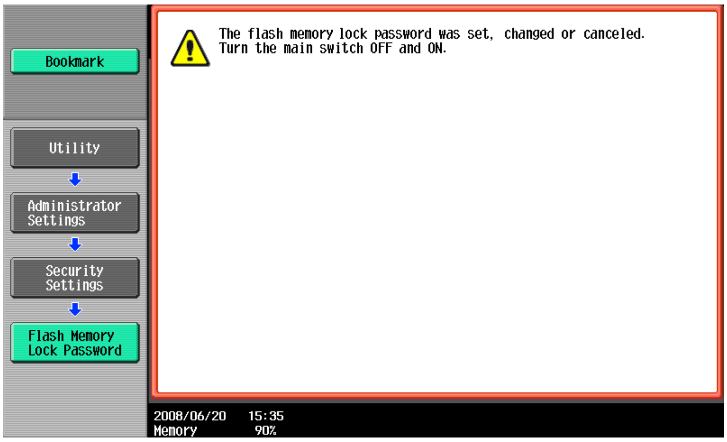
- Press the [C] key to clear all characters.
- Touch [Delete] to delete the last character entered.
- Touch [Shift] to show the upper case/symbol screen.
- Touch [Cancel] to go back to the Security Settings screen.

7 Touch [OK].

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

→ If there is a mismatch in the Flash Memory Lock Passwords, a message appears saying that there is a mismatch in the Flash Memory Lock Passwords. Perform steps 4 to 6 once again.

8 Make sure that a message appears promoting you to turn OFF and ON the main power switch. Turn OFF and ON the main power switch.



The flash memory lock password was set, changed or canceled.
Turn the main switch OFF and ON.

Note

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

2.13 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 and all user settings saved in the flash memory 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 1-11**.

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 4 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.

2.13.1 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

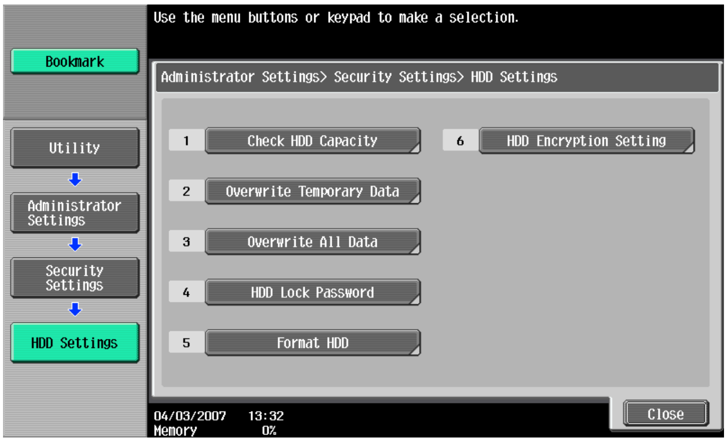
Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.

<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 2-56**.

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

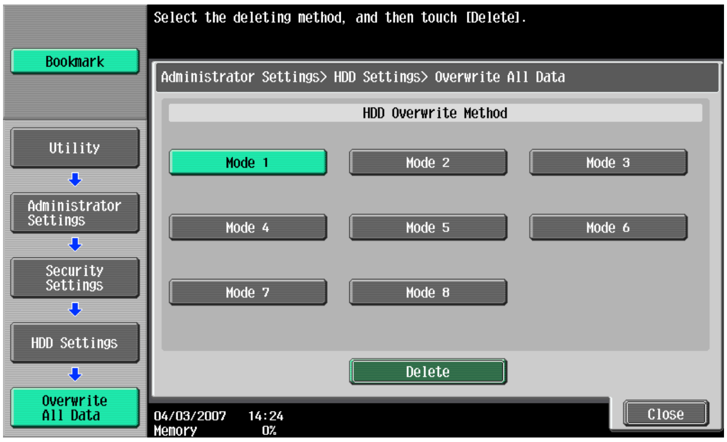
2 Touch [Overwrite All Data].



Use the menu buttons or keypad to make a selection.

Administrator Settings> Security Settings> HDD Settings

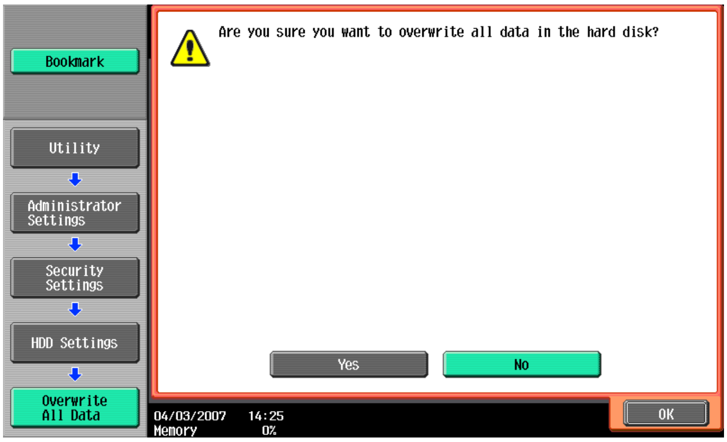
3 Select the desired mode and touch [Delete].



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

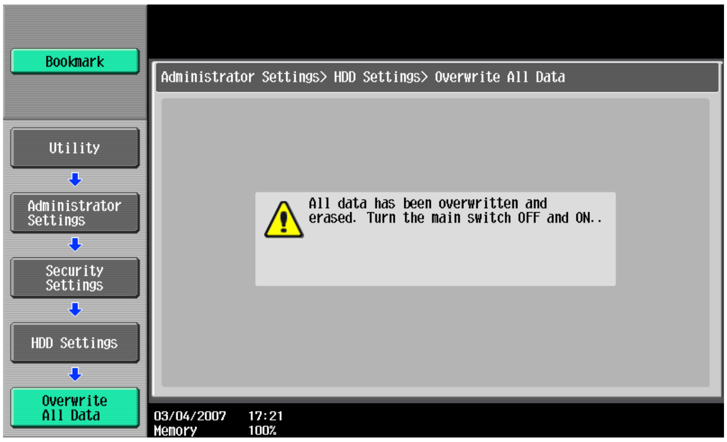
Administrator Settings> HDD Settings> Overwrite All Data

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



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

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 erased. Turn the main switch OFF and ON..

✎...

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.

2.14 SSL Setting Function

When access to the Administrator of the machine by the Administrator Settings is authenticated, the machine enables the setting of encryption of image data transmitted and received between the PC and the machine.

2.14.1 Setting the SSL

Note

Do not leave the machine with the Admin 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 Admin Mode.

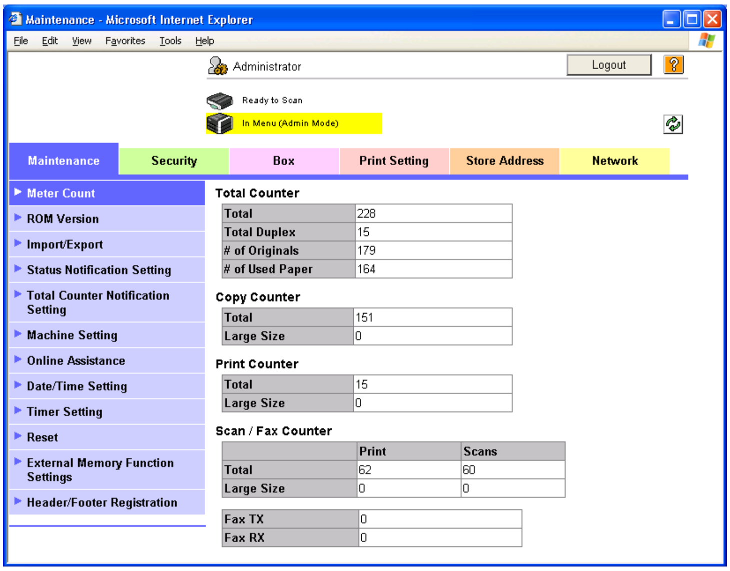
For encryption strength, select the strong "DES, RC4-40, RC4-128, 3DES-168, or AES- 256."

<Setting can be made only from Web Connection>

✔ For the procedure to call the Admin Mode to the display, see **"Accessing the Administrator Settings" on page 2-2**.

1 Start Web Connection and access the Admin Mode.

2 Click the [Security] tab and the [SSL/TLS Setting] menu.



Total Counter

Total	228
Total Duplex	15
# of Originals	179
# of Used Paper	164

Copy Counter

Total	151
Large Size	0

Print Counter

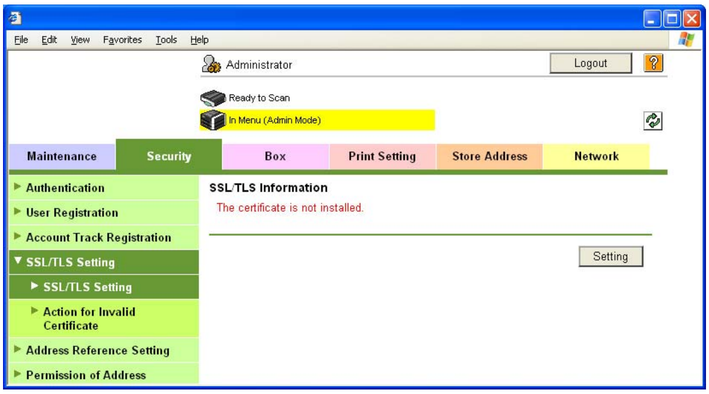
Total	15
Large Size	0

Scan / Fax Counter

	Print	Scans
Total	62	60
Large Size	0	0

Fax TX	0
Fax RX	0

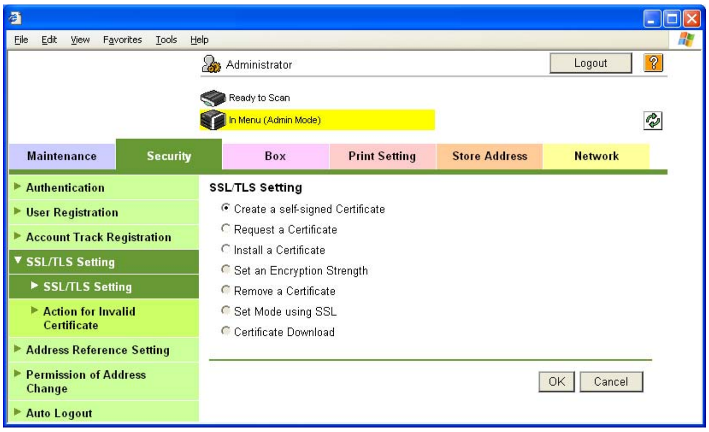
3 Click the [Setting] menu.



SSL/TLS Information

The certificate is not installed.

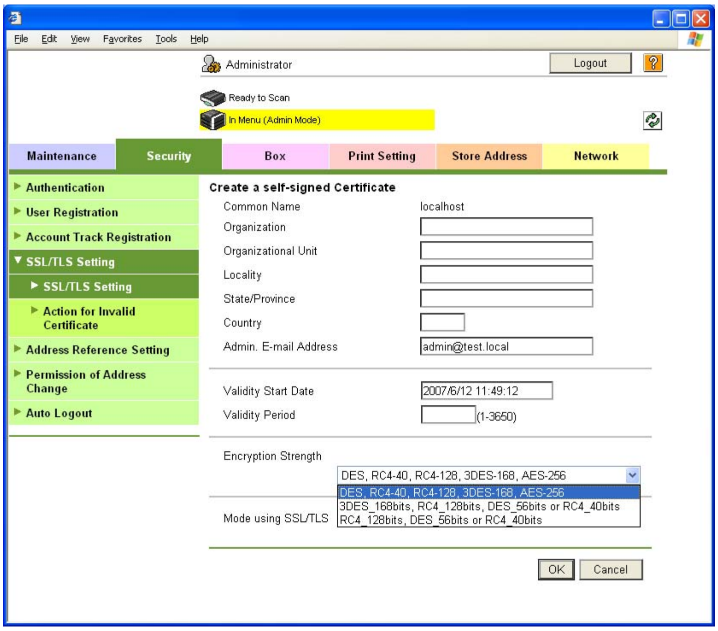
4 Select [Create a self-signed Certificate] and click [OK].



SSL/TLS Setting

- ● Create a self-signed Certificate
- ○ Request a Certificate
- ○ Install a Certificate
- ○ Set an Encryption Strength
- ○ Remove a Certificate
- ○ Set Mode using SSL
- ○ Certificate Download

5 Select the Encryption Strength.

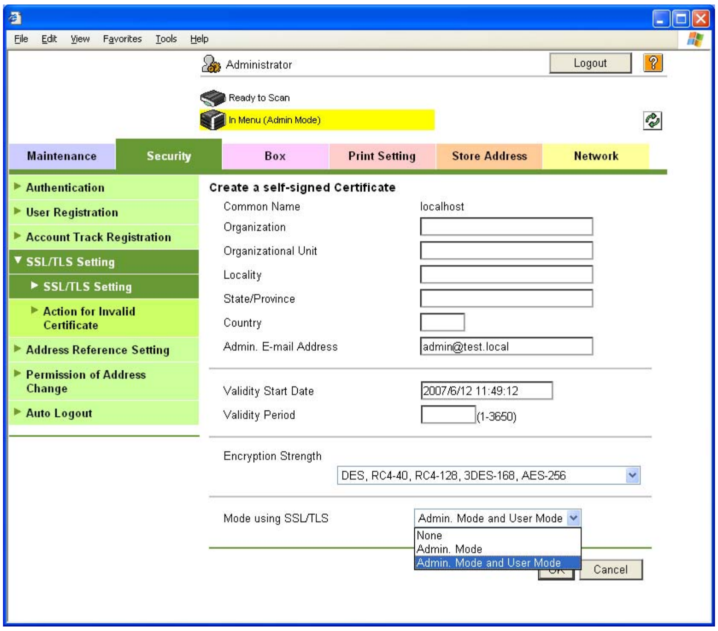


Create a self-signed Certificate

Common Name	localhost
Organization	
Organizational Unit	
Locality	
State/Province	
Country	
Admin. E-mail Address	admin@test.local
Validity Start Date	2007/6/12 11:49:12
Validity Period	(1-3650)
Encryption Strength	DES, RC4-40, RC4-128, 3DES-168, AES-256
Mode using SSL/TLS	

Encryption Strength options:
- DES, RC4-40, RC4-128, 3DES-168, AES-256
- 3DES_168bits, RC4_128bits, DES_56bits or RC4_40bits
- RC4_128bits, DES_56bits or RC4_40bits

6 Select "Admin. Mode and User Mode" for "Mode using SSL/TLS."

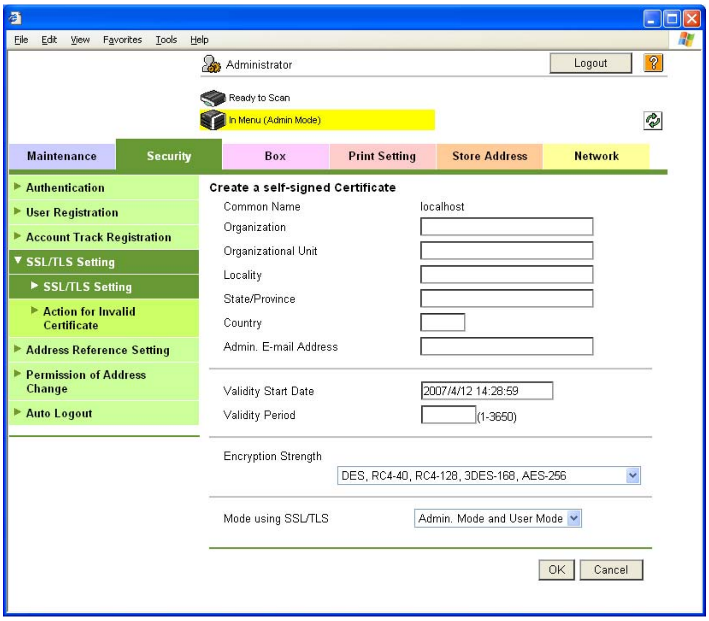


Create a self-signed Certificate

Common Name	localhost
Organization	
Organizational Unit	
Locality	
State/Province	
Country	
Admin. E-mail Address	admin@test.local
Validity Start Date	2007/6/12 11:49:12
Validity Period	(1-3650)
Encryption Strength	DES, RC4-40, RC4-128, 3DES-168, AES-256
Mode using SSL/TLS	Admin. Mode and User Mode

Mode using SSL/TLS options:
- None
- Admin. Mode
- Admin. Mode and User Mode

7 Make the necessary settings.



Create a self-signed Certificate

Common Name localhost

Organization

Organizational Unit

Locality

State/Province

Country

Admin. E-mail Address

Validity Start Date 2007/4/12 14:28:59

Validity Period (1-3650)

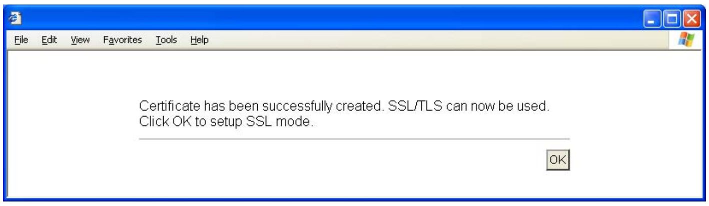
Encryption Strength DES, RC4-40, RC4-128, 3DES-168, AES-256

Mode using SSL/TLS Admin. Mode and User Mode

? What if data entered for each item does not meet the requirements?

→ If data entered for each item does not meet the requirements, a message appears that tells that the data entered is wrong.

8 Click the [OK].
The certificate can now be registered.



Certificate has been successfully created. SSL/TLS can now be used.
Click OK to setup SSL mode.

– The key length set for the public key of the server generated in SSL certificate setting is 1024 bits.

2.14.2 Changing the Encryption Strength Setting

✎...

Note

Do not leave the machine with the Admin 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 Admin Mode.

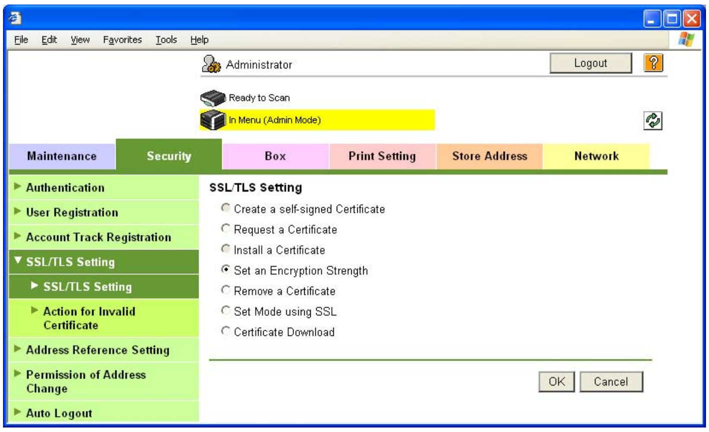
For encryption strength, select the strong "DES, RC4-40, RC4-128, 3DES-168, or AES- 256."

<Setting can be made only from Web Connection>

✔ For call the SSL/TLS Setting menu to the display, see steps 1 through 3 of **"Setting the SSL" on page 2-81**.

1 Start Web Connection and call the SSL/TLS Setting menu to the display.

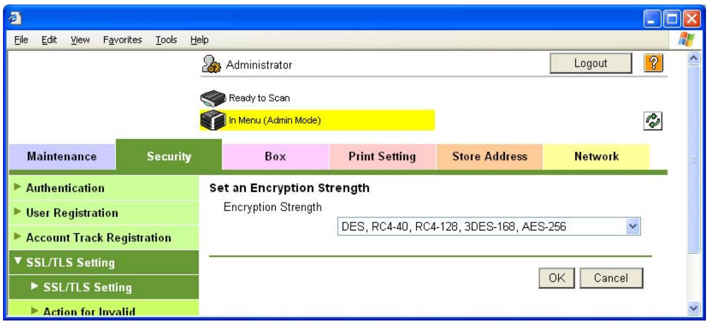
2 Select [Set an Encryption Strength] and click the [OK].



SSL/TLS Setting

○ Create a self-signed Certificate
○ Request a Certificate
○ Install a Certificate
● Set an Encryption Strength
○ Remove a Certificate
○ Set Mode using SSL
○ Certificate Download

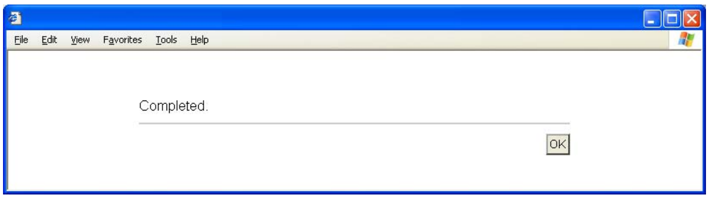
3 Select Encryption Strength and click [OK].



Set an Encryption Strength

Encryption Strength: DES, RC4-40, RC4-128, 3DES-168, AES-256

4 Click the [OK].



Completed.

2.14.3 Changing the Mode Using SSL

✎...

Note

Do not leave the machine with the Admin 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 Admin Mode.

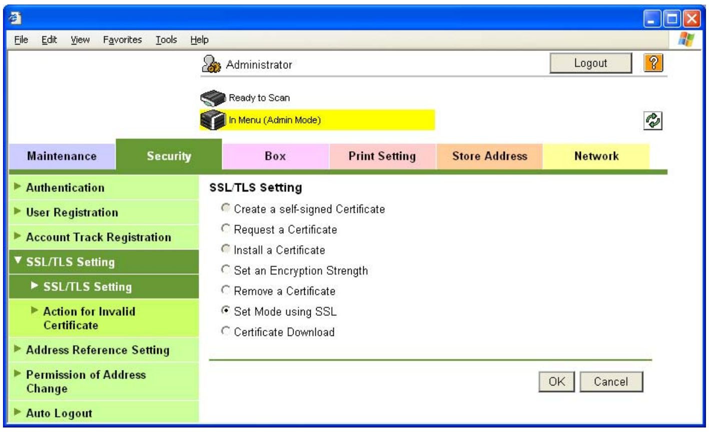
Select "Admin. Mode and User Mode" for "Mode using SSL/TLS."

<Setting can be made only from Web Connection>

✔ For call the SSL/TLS Setting menu to the display, see steps 1 through 3 of **"Setting the SSL" on page 2-81**.

1 Start Web Connection and call the SSL/TLS Setting menu to the display.

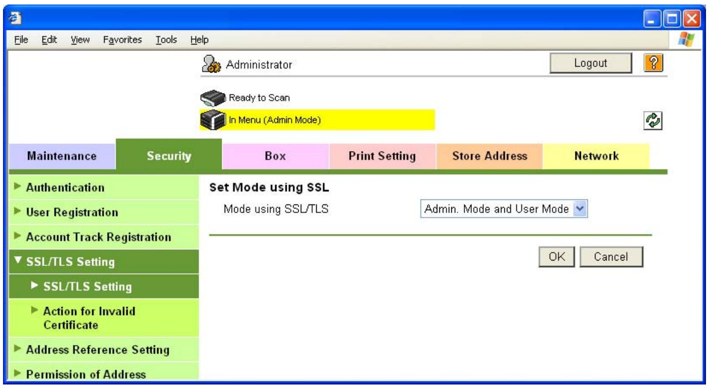
2 Select [Set Mode using SSL] and click the [OK].



SSL/TLS Setting

○ Create a self-signed Certificate
○ Request a Certificate
○ Install a Certificate
○ Set an Encryption Strength
○ Remove a Certificate
● Set Mode using SSL
○ Certificate Download

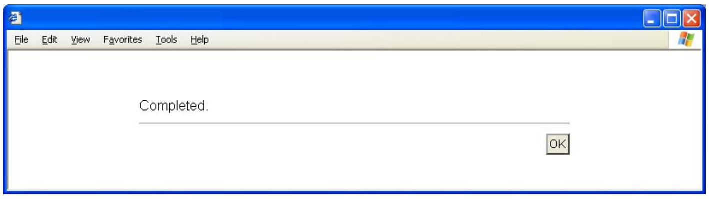
3 Select Mode using SSL/TLS and click [OK].



Set Mode using SSL

Mode using SSL/TLS: Admin. Mode and User Mode

4 Click the [OK].



Completed.

2.14.4 Removing a Certificate

✎...

Note

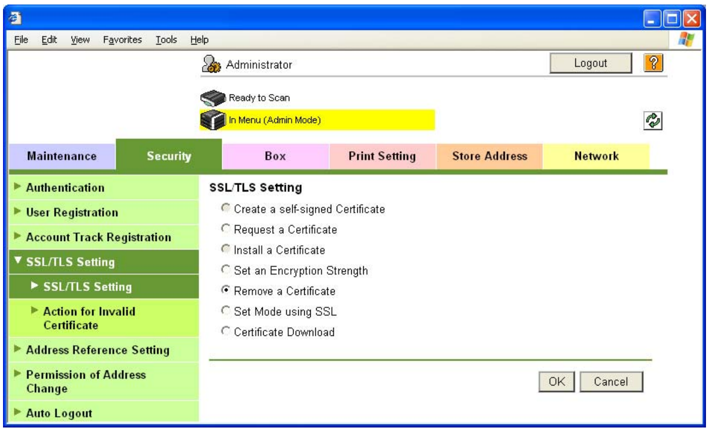
Do not leave the machine with the Admin Mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin Mode.

<Setting can be made only from Web Connection>

✔ For call the SSL/TLS Setting menu to the display, see steps 1 through 3 of **"Setting the SSL" on page 2-81**.

1 Start Web Connection and call the SSL/TLS Setting menu to the display.

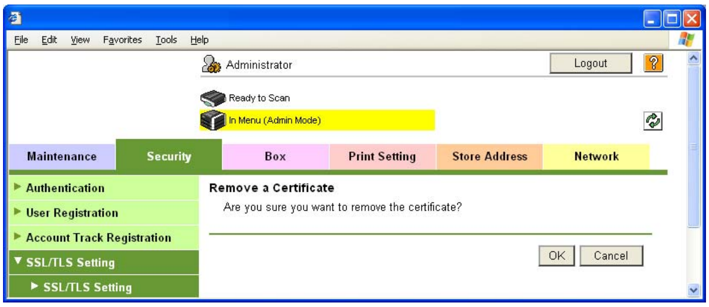
2 Select [Remove a Certificate] and click the [OK].



SSL/TLS Setting

○ Create a self-signed Certificate
○ Request a Certificate
○ Install a Certificate
○ Set an Encryption Strength
● Remove a Certificate
○ Set Mode using SSL
○ Certificate Download

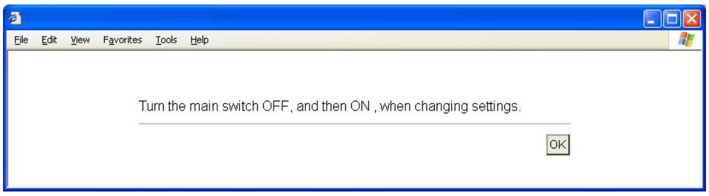
3 Click the [OK].



Remove a Certificate

Are you sure you want to remove the certificate?

4 Click [OK] and restart the machine.



Turn the main switch OFF, and then ON , when changing settings.

– No certificates can be removed if Enhanced Security Mode is set to [ON].

2.15 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.

2.15.1 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.

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

*[NO] should be selected for [Automatically Obtain Certificates], so that no certificates are registered through automatic acquisition. For registration of certificates, see **"Registering the certificate" on page 2-92**.*

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

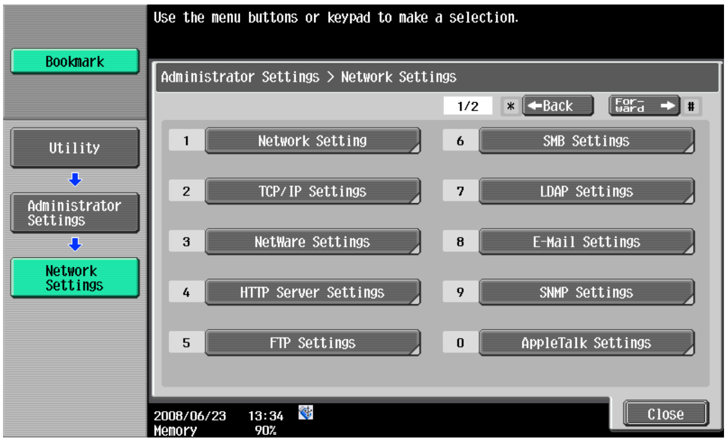
<From the Control Panel>

✔ 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].

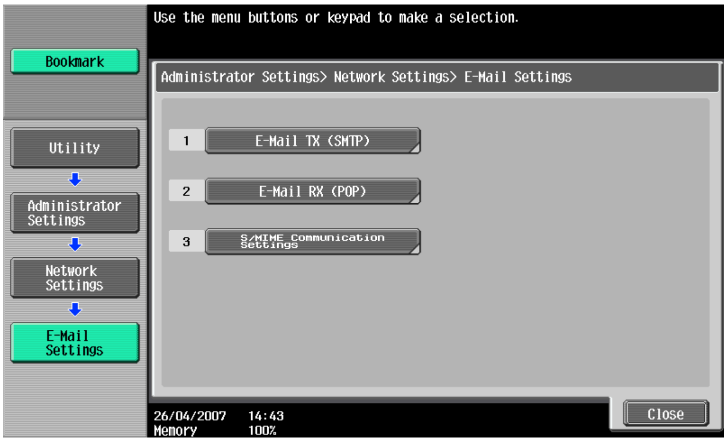
3 Touch [E-Mail Settings].



Use the menu buttons or keypad to make a selection.

Administrator Settings > Network Settings

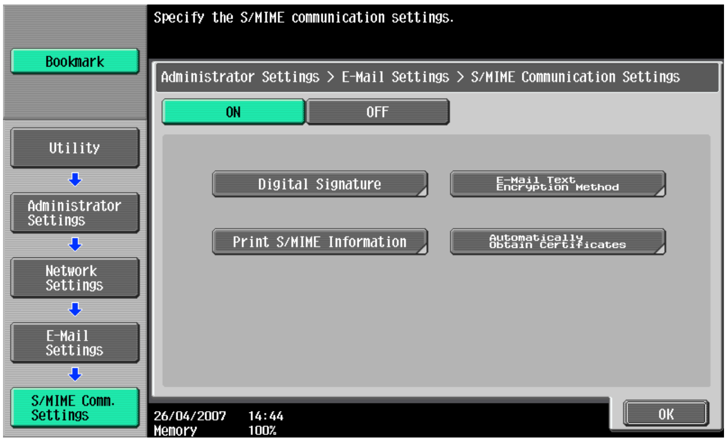
4 Touch [S/MIME Communication Settings].



Use the menu buttons or keypad to make a selection.

Administrator Settings> Network Settings> E-Mail Settings

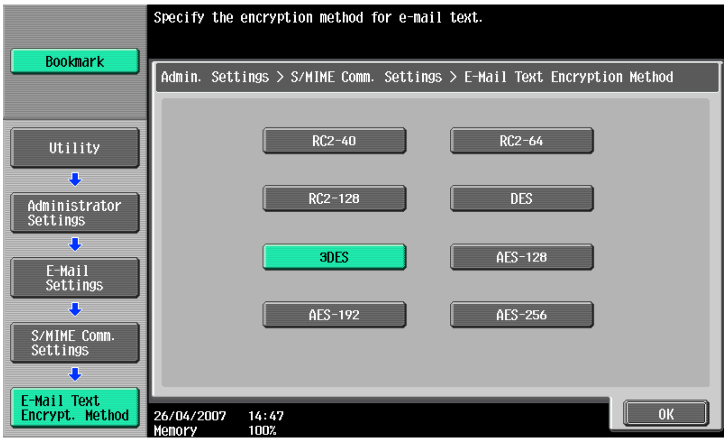
5 Select [ON] and [E-Mail Text Encryption Method].



Specify the S/MIME communication settings.

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

6 Select encryption strength and touch [OK].

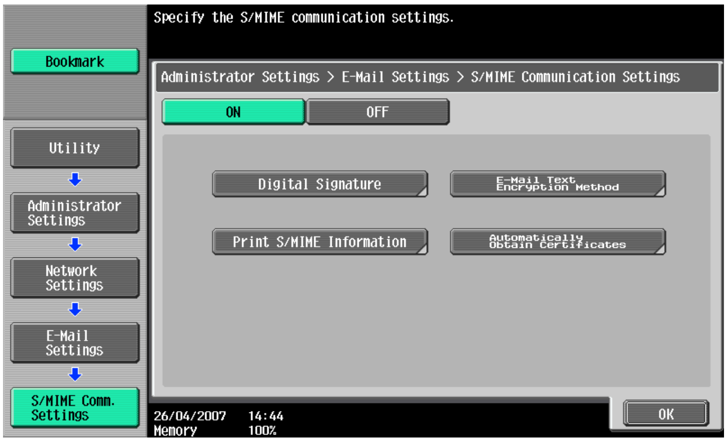


Specify the encryption method for e-mail text.

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

7 Touch [OK].

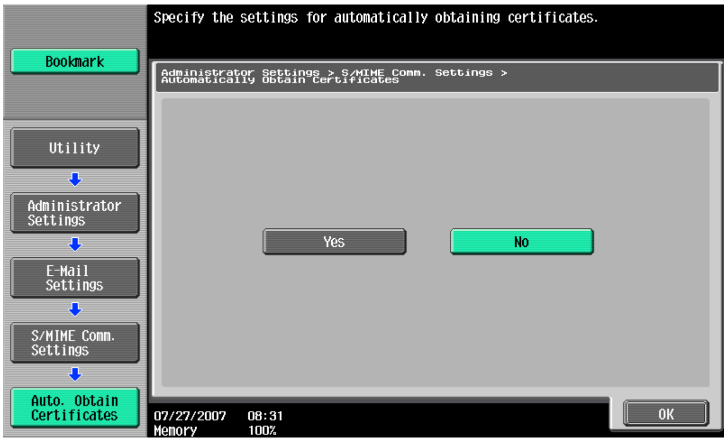
8 Select [Automatically Obtain Certificates].



Specify the S/MIME communication settings.

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

9 Select [NO] and touch [OK].



Specify the settings for automatically obtaining certificates.

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

✎...

Note

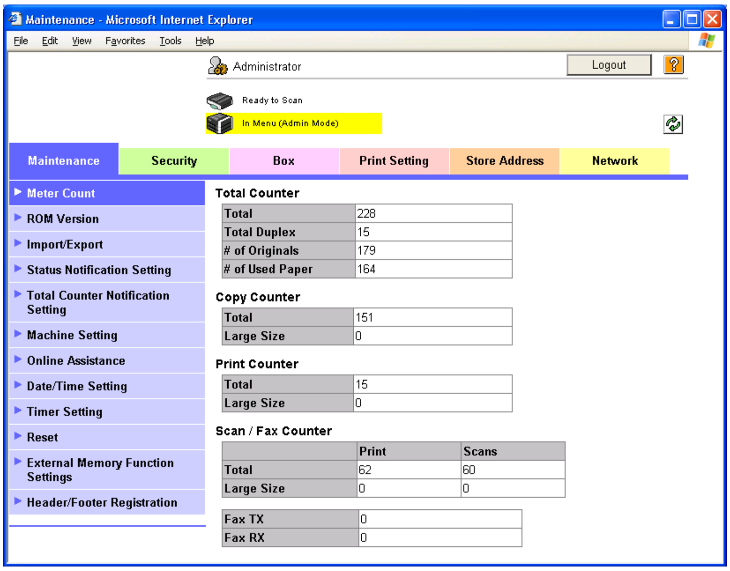
To ensure that correct certificate is registered, do not register certificates through [Automatically Obtain Certificates]. For registration of certificates, see ***"Registering the certificate" on page 2-92****.*

<From Web Connection>

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

1 Start Web Connection and access the Admin Mode.

2 Click the [Network] tab.



Total Counter

Total	228
Total Duplex	15
# of Originals	179
# of Used Paper	164

Copy Counter

Total	151
Large Size	0

Print Counter

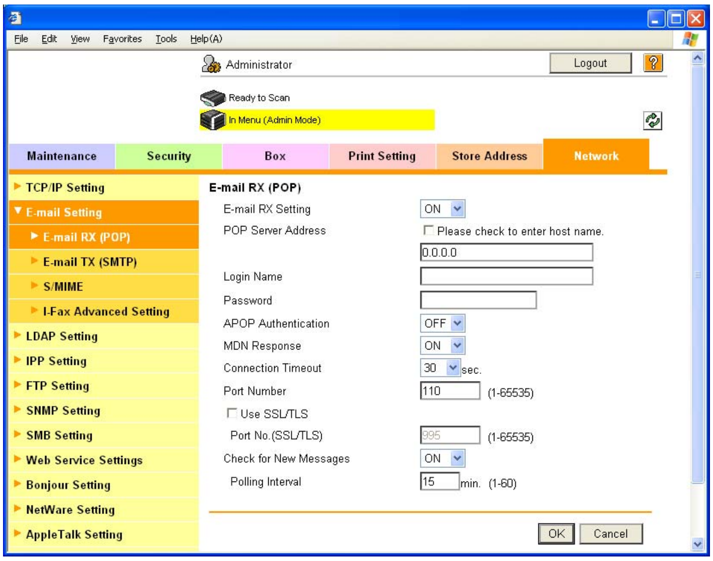
Total	15
Large Size	0

Scan / Fax Counter

	Print	Scans
Total	62	60
Large Size	0	0

Fax TX	0
Fax RX	0

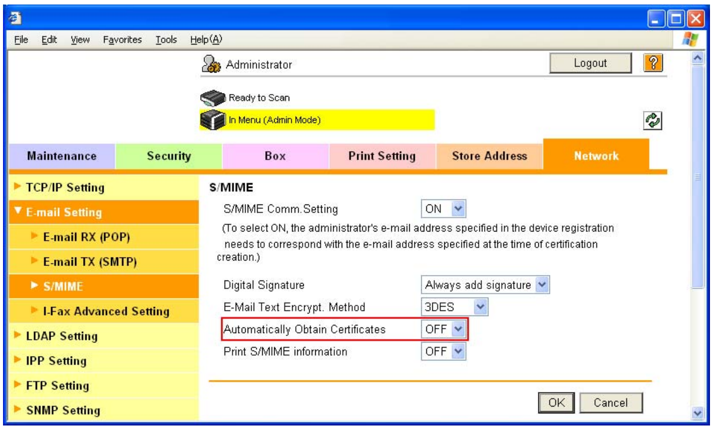
3 Click the [S/MIME] of the [E-mail Setting] menu.



E-mail RX (POP)

E-mail RX Setting	ON
POP Server Address	□ Please check to enter host name. 0.0.0.0
Login Name	
Password	
APOP Authentication	OFF
MDN Response	ON
Connection Timeout	30 sec.
Port Number	110 (1-65535)
□ Use SSL/TLS	
Port No.(SSL/TLS)	995 (1-65535)
Check for New Messages	ON
Polling Interval	15 min. (1-60)

4 Make a necessary settings.



S/MIME

S/MIME Comm.Setting: ON

(To select ON, the administrator's e-mail address specified in the device registration needs to correspond with the e-mail address specified at the time of certification creation.)

Digital Signature: Always add signature

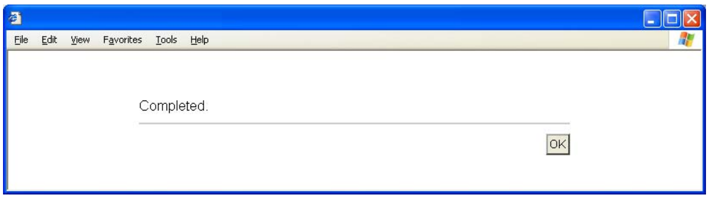
E-Mail Text Encrypt. Method: 3DES

Automatically Obtain Certificates: OFF

Print S/MIME information: OFF

5 Click the [OK].

6 Click the [OK].



Completed.

2.15.2 Registering the certificate

Note

Do not leave the machine with the Admin 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 Admin Mode.

To register an authorized certificate, do not register one using [Automatically Obtain Certificates] of [S/MIME Communication Setting] in Administrator Settings.

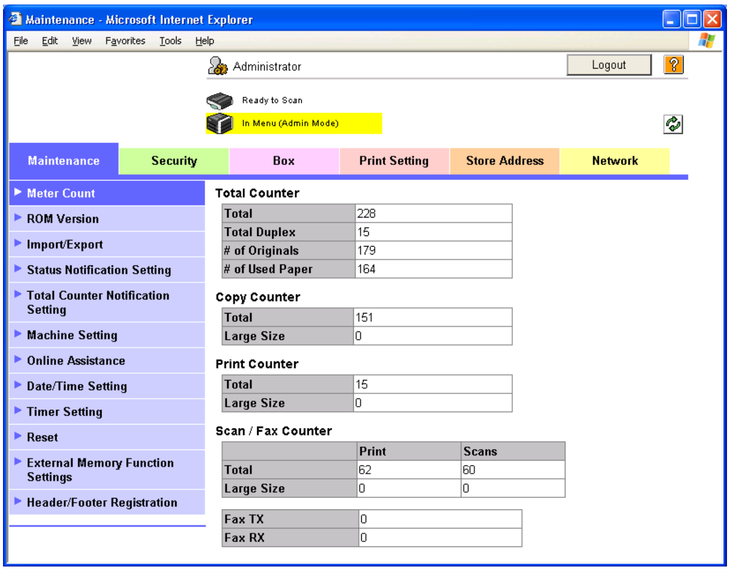
Set 1024 bits or more for the key length of the RSA public key for the certificate of each destination.

<From Web Connection>

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

1 Start Web Connection and access the Admin Mode.

2 Click the [Address Book] menu of the [Store Address] tab.



Total Counter

Total	228
Total Duplex	15
# of Originals	179
# of Used Paper	164

Copy Counter

Total	151
Large Size	0

Print Counter

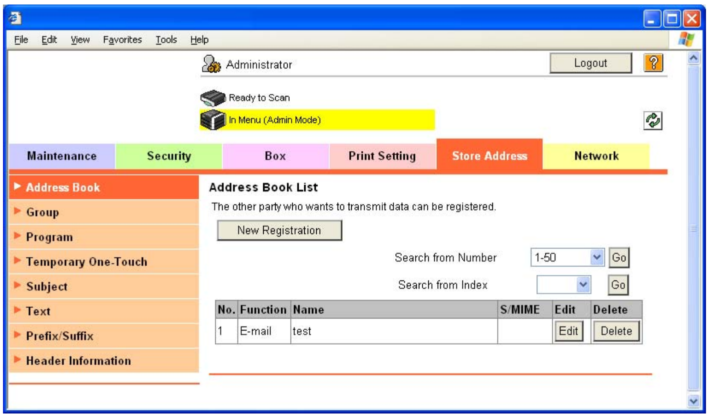
Total	15
Large Size	0

Scan / Fax Counter

	Print	Scans
Total	62	60
Large Size	0	0

Fax TX	0
Fax RX	0

3 Click the [New Registration].



Address Book List

The other party who wants to transmit data can be registered.

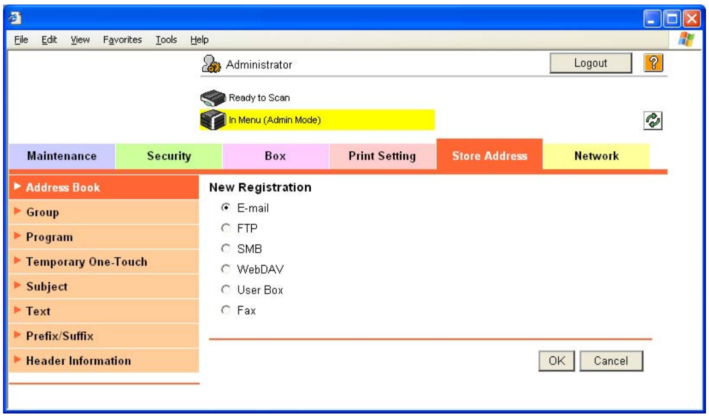
Search from Number 1-50

Search from Index

No.	Function	Name	S/MIME	Edit	Delete
1	E-mail	test		Edit	Delete

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

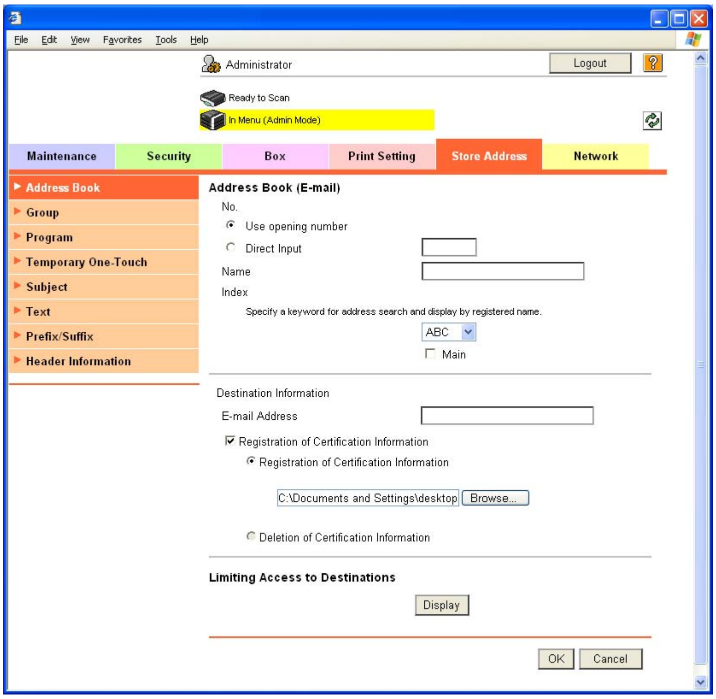
4 Select the [E-mail] and click the [OK].



New Registration

● E-mail
○ FTP
○ SMB
○ WebDAV
○ User Box
○ Fax

5 Click to select [Registration of Certification Information] and, through [Browse], set the certificate information. If certificate information is to be deleted, select [Deletion of Certification Information].



Address Book (E-mail)

No.
● Use opening number
○ Direct Input
Name
Index
Specify a keyword for address search and display by registered name.
ABC
□ Main

Destination Information
E-mail Address
☑ Registration of Certification Information
● Registration of Certification Information
C:\Documents and Settings\desktop
○ Deletion of Certification Information

Limiting Access to Destinations

6 Make a necessary settings.

? Are there any precautions to be used when making settings?

➔ Any number that has previously been registered cannot be registered.

➔ If Name and E-mail Address have not been registered, a message appears that tells that Name and E-mail Address are yet to be entered. Enter the correct Name and E-mail Address.

7 Click the [OK].

2.16 SNMP Setting Function

When access to the Administrator of the machine by the Administrator Settings is authenticated, the machine enables changing of the SNMP v3 Write User Password (auth-password, priv-password) required for accessing the MIB object over the network using the SNMP from the PC. In Web Connection, import/export of the Device Setting is enabled, allowing the setting for Security Level of SNMP v3 Setting to be saved or the saved backup data to be restored.

Each of the auth-password and priv-password can consist of 8 to 32 digits. The password entered for the authentication purpose appears as "*" or "●" on the display.

2.16.1 Changing the auth-password and priv-password

✎...

Note

For tightening security, set priv-password without fail.

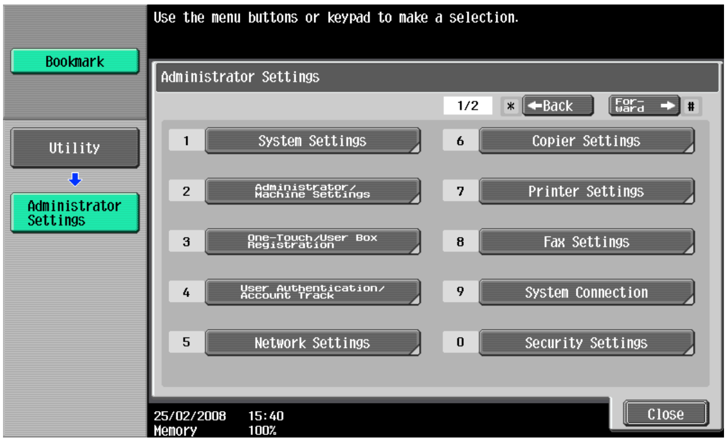
Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.

<From the Control Panel>

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

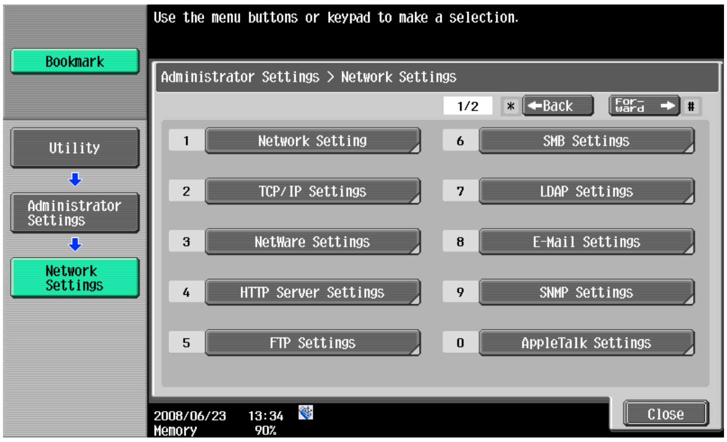
1 Call the Administrator Settings to the screen from the control panel.

2 Touch [Network Settings].



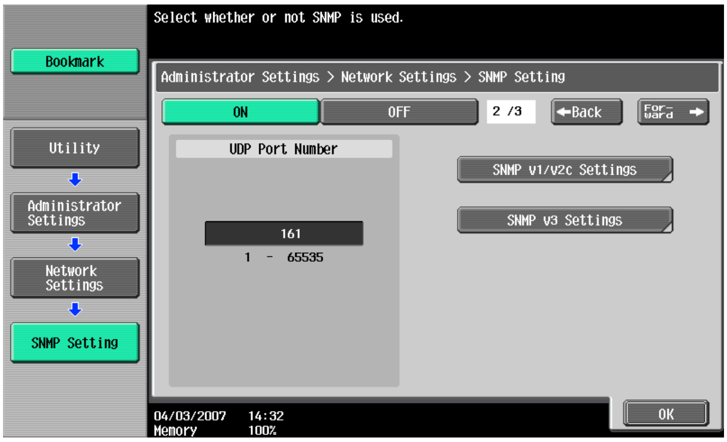
Use the menu buttons or keypad to make a selection.

3 Touch [SNMP Settings].



Use the menu buttons or keypad to make a selection.

4 Touch [Forward→] to show the [2/3] and touch [SNMP v3 Settings].



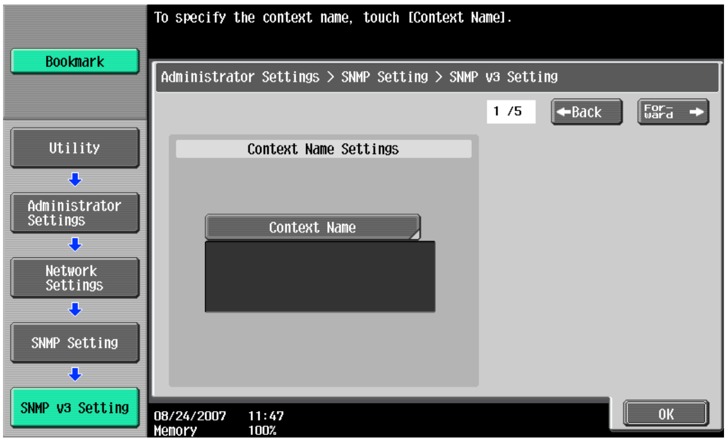
Select whether or not SNMP is used.

Administrator Settings > Network Settings > SNMP Setting

UDP Port Number: 161 (1 - 65535)

04/03/2007 14:32
Memory 100%

5 Touch [Forward→] to show the [4/5] SNMPv3/Write Settings screen.



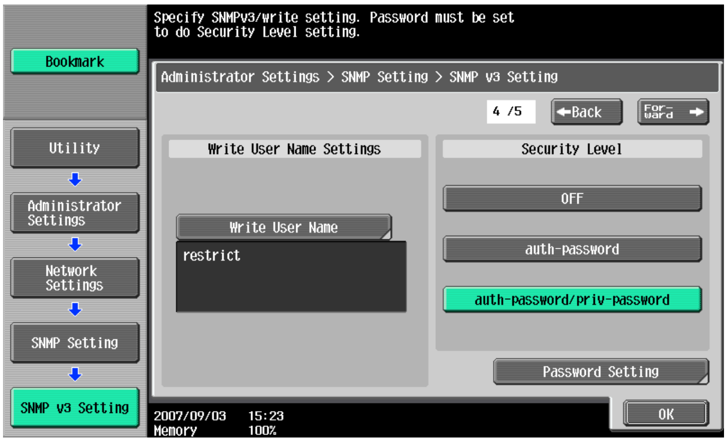
To specify the context name, touch [Context Name].

Administrator Settings > SNMP Setting > SNMP v3 Setting

Context Name Settings

08/24/2007 11:47
Memory 100%

6 Select [auth-password] or [auth-password/priv-password] of Security Level and touch [Password Setting].



Specify SNMPv3/write setting. Password must be set to do Security Level setting.

Administrator Settings > SNMP Setting > SNMP v3 Setting

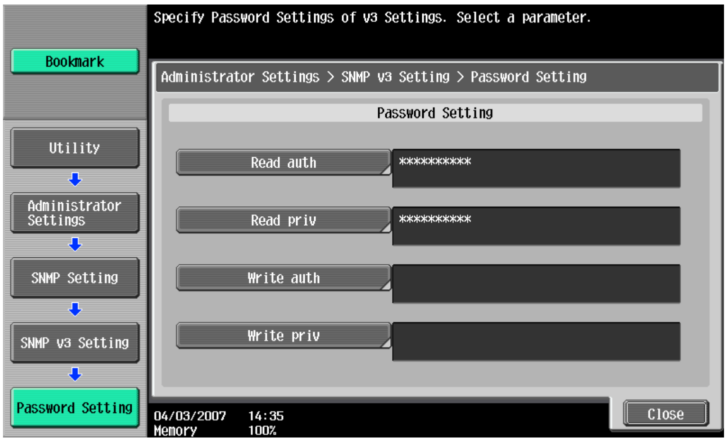
Write User Name Settings

Write User Name: restrict

Security Level: auth-password/priv-password

2007/09/03 15:23
Memory 100%

7 Touch [Write auth].



Specify Password Settings of v3 Settings. Select a parameter.

Administrator Settings > SNMP v3 Setting > Password Setting

Password Setting

Read auth ***********

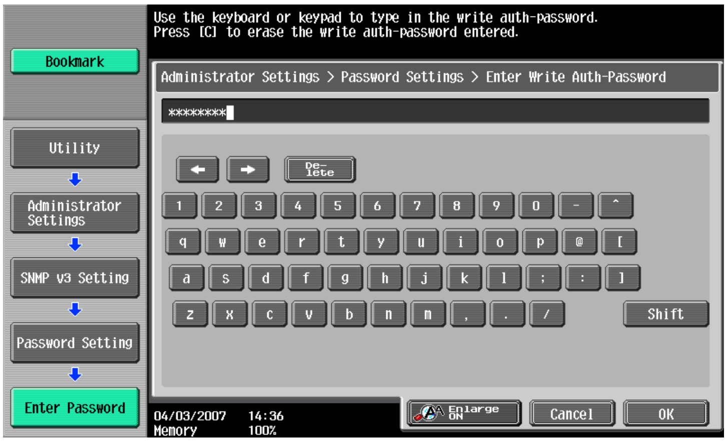
Read priv ***********

Write auth

Write priv

04/03/2007 14:35
Memory 100%

8 Enter the new 8-digit-or-more auth-password from the keyboard and keypad.



Use the keyboard or keypad to type in the write auth-password.
Press [C] to erase the write auth-password entered.

Administrator Settings > Password Settings > Enter Write Auth-Password

****

04/03/2007 14:36
Memory 100%

- 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 previous screen.

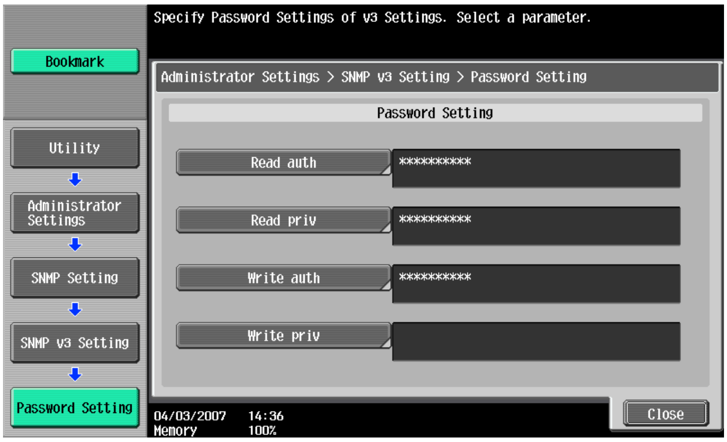
9 Touch [OK].

- Go to step 10 if [auth-password/priv-password] has been selected in step 6.

? What happens if the auth-password entered does not meet the requirements of the Password Rules?

➔ If the auth-password entered does not comply with the Password Rules, a message appears that tells that the auth-password entered cannot be used. Enter the correct auth-password. For details of the Password Rules, see **"Password Rules" on page 1-9**.

10 Touch [Write priv].



Specify Password Settings of v3 Settings. Select a parameter.

Administrator Settings > SNMP v3 Setting > Password Setting

Password Setting

Read auth ***********

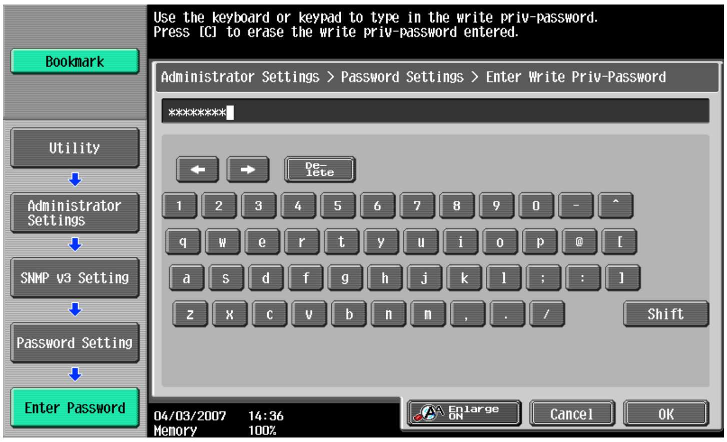
Read priv ***********

Write auth ***********

Write priv

04/03/2007 14:36
Memory 100%

11 Enter the new 8-digit-or-more priv-password from the keyboard and keypad.



Use the keyboard or keypad to type in the write priv-password.
Press [C] to erase the write priv-password entered.

Administrator Settings > Password Settings > Enter Write Priv-Password

****

04/03/2007 14:36
Memory 100%

- 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 previous screen.

12 Touch [OK].

? What happens if the priv-password entered does not meet the requirements of the Password Rules?

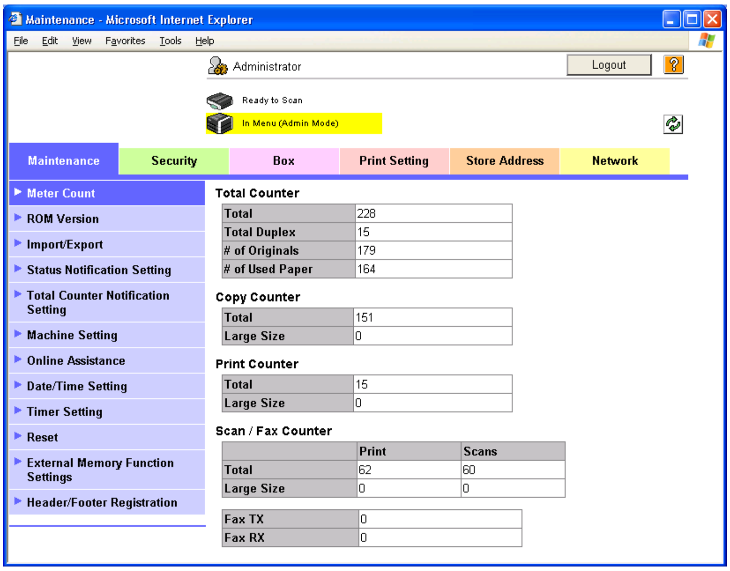
➔ If the priv-password entered does not comply with the Password Rules, a message appears that tells that the priv-password entered cannot be used. Enter the correct priv-password. For details of the Password Rules, see **"Password Rules" on page 1-9**.

<From Web Connection>

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

1 Start Web Connection and access the Admin Mode.

2 Click the [Network] tab.



Total Counter

Total	228
Total Duplex	15
# of Originals	179
# of Used Paper	164

Copy Counter

Total	151
Large Size	0

Print Counter

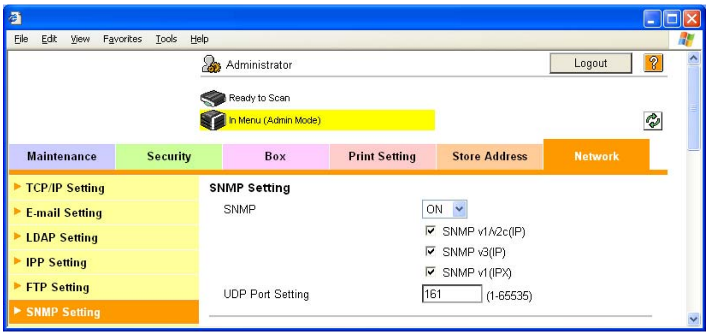
Total	15
Large Size	0

Scan / Fax Counter

	Print	Scans
Total	62	60
Large Size	0	0

Fax TX	0
Fax RX	0

3 Click the [SNMP Setting] menu.



SNMP Setting

SNMP: ON

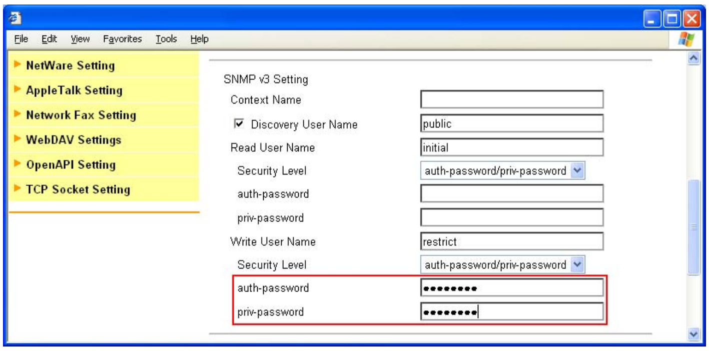
☑ SNMP v1/v2c(IP)

☑ SNMP v3(IP)

☑ SNMP v1(IPX)

UDP Port Setting: 161 (1-65535)

4 Enter the auth-password and priv-password in the boxes marked by the rectangle, that is, the Write side SNMP v3 Setting.



SNMP v3 Setting

Context Name:

☑ Discovery User Name: public

Read User Name: initial

Security Level: auth-password/priv-password

auth-password:

priv-password:

Write User Name: restrict

Security Level: auth-password/priv-password

auth-password: ••••••••

priv-password: ••••••••

5 Click the [OK].

? What happens if the auth-password and priv-password entered does not meet the requirements of the Password Rules?

➔ If the auth-password and priv-password entered does not comply with the Password Rules, a message appears that tells that the auth-password and priv-password entered cannot be used. Enter the correct auth-password and priv-password. For details of the Password Rules, see **"Password Rules" on page 1-9**.

2.16.2 SNMP access authentication function

If the settings of the Administrator mode are to be changed using SNMP from the PC, the user attempting to gain access is authenticated to be the Administrator of the machine by using the Write User Name and SNMP Password (auth-password, priv-password) of the SNMP v3 Write settings made in this machine.

Operation of the network setting function and the SNMP password change function of the security control functions that can be used over the network using SNMP is granted to the Administrator who is identified by a matching SNMP password for the Write User Name.

The entry of a wrong SNMP password (auth-password, priv-password) is counted as unauthorized access, if the Enhanced Security Mode is set to [ON]. If a wrong SNMP password (auth-password, priv-password) is entered a predetermined number of times (once to three times) set by the Administrator of the machine or more, the machine is set into an access lock state, rejecting any more logon attempts. To reset the access lock state, the Administrator of the machine should perform the procedure for resetting the operation prohibited state.

Detail

If [auth-password] has been selected for Security Level, hashing is used for the authentication information (auth-password) to be transmitted. The machine uses HMAC-MD5 for hashing.
If [auth-password/priv-password] has been selected for Security Level, the authentication information (auth-password/priv-password) and data (object ID that specifies the object to be changed, value to be set, etc.) to be transmitted are used for hashing and encryption. The machine uses CBC-DES for encryption.

For accessing the MIB, use the MIB browser corresponding to the above encryption algorithm.

2.16.3 SNMP v3 setting function

The Administrator who has been authenticated through SNMP access authentication from the PC is allowed to operate the SNMP password change function.

The entry of a wrong SNMP password (auth-password, priv-password) is counted as unauthorized access, if the Enhanced Security Mode is set to [ON]. If a wrong SNMP password (auth-password, priv-password) is entered a predetermined number of times (once to three times) set by the Administrator of the machine or more, the machine is set into an access lock state, rejecting any more logon attempts. To reset the access lock state, the Administrator of the machine should perform the procedure for resetting the operation prohibited state.

For the auth-password and priv-password, enter the password that meets the requirements of the Password Rules. For details of the Password Rules, see **"Password Rules" on page 1-9**.

To change the setting, specify the corresponding object ID. See the table below for the setting items.

Setting Item	Object ID
Write User Name	1.3.6.1.4.1.18334.1.1.2.1.5.6.4.2.1.2.2
Security Level	1.3.6.1.4.1.18334.1.1.2.1.5.6.4.2.1.3.2
auth-password	1.3.6.1.4.1.18334.1.1.2.1.5.6.4.2.1.4.2
priv-password	1.3.6.1.4.1.18334.1.1.2.1.5.6.4.2.1.5.2

2.16.4 SNMP network setting function

The Administrator who has been authenticated through SNMP access authentication from the PC is allowed to operate the network setting function. To change the setting, specify the corresponding object ID. See the table below for the setting items.

Setting Item		Object ID
IP address setting	IP Address	1.3.6.1.4.1.18334.1.1.2.1.5.7.1.1.1.3.1
	BOOT Protocol use setting	1.3.6.1.4.1.18334.1.1.2.1.5.7.1.1.1.6.1
	BOOT Protocol Type	1.3.6.1.4.1.18334.1.1.2.1.5.7.1.1.1.7.1
DNS server address setting		1.3.6.1.4.1.18334.1.1.2.1.5.7.1.2.1.3.1.1
SMTP server address setting		1.3.6.1.4.1.18334.1.1.2.1.5.7.13.1.1.3.1
NetWare setting	Print Server Name	1.3.6.1.4.1.18334.1.1.2.1.5.8.3.1.3.1.1
	Printer Name	1.3.6.1.4.1.18334.1.1.2.1.5.8.5.1.3.1.1
AppleTalk Printer Name Setting		1.3.6.1.4.1.18334.1.1.2.1.5.9.2.1.3.1.1
NetBIOS setting		1.3.6.1.4.1.18334.1.1.2.1.5.10.1.1.4.1

2.17 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.

2.17.1 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.

<From the Control Panel>

✔ For the procedure to call the Network Settings menu to the display, see steps 1 and 2 of **"Changing the auth-password and priv-password" on page 2-94**.

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

2 Touch [TCP/IP Settings].

3 Touch [IP Settings].

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].

<From Web Connection>

✔ For the procedure to call the Network menu to the display, see steps 1 and 2 of **"Changing the auth-password and priv-password" on page 2-94**.

1 Start the Web Connection and call the Network menu to the display.

2 Click the [TCP/IP Setting] menu.

3 Select [Manual Setting] from the IP Address Setting Method pull-down menu.

4 Enter the IP Address in the "IP Address" box.

– If [Auto Setting] is selected from the IP Address Setting Method pull-down menu in step 3, select the means with which to acquire the IP Address automatically, including DHCP, BOOTP, ARP/PING, and AUTOIP setting.

5 Click the [OK].

6 Click the [OK].

7 Click the [Logout].

2.17.2 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.

<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 2-102**.

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].

<From Web Connection>

✔ For the procedure to call the TCP/IP setting menu to the display, see steps 1 and 2 of **"Setting the IP Address" on page 2-102**.

1 Start the Web Connection and call the TCP/IP Setting menu to the display.

2 Enter the address in the DNS Server box.

– If [Enable] is selected from the DNS Server Auto Obtain and DNS Domain Auto Obtain pull-down menus, the DNS Server Address and DNS Domain Name are automatically acquired.

3 Make the necessary settings.

4 Click the [OK].

5 Click the [OK].

6 Click the [Logout].

2.18 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.

2.18.1 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.

<From the Control Panel>

✔ For the procedure to call the Network Settings menu to the display, see steps 1 and 2 of **"Changing the auth-password and priv-password" on page 2-94**.

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

2 Touch [NetWare Settings].

3 Make the necessary settings.

4 Touch [OK].

<From Web Connection>

✔ For the procedure to call the Network menu to the display, see steps 1 and 2 of **"Changing the auth-password and priv-password" on page 2-94**.

1 Start the Web Connection and call the Network menu to the display.

2 Click the [NetWare Setting] menu.

3 Make the necessary settings.

4 Click the [OK].

5 Click the [OK].

6 Click the [Logout].

2.19 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.

2.19.1 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.

<From the Control Panel>

✔ For the procedure to call the Network Settings menu to the display, see steps 1 and 2 of **"Changing the auth-password and priv-password" on page 2-94**.

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].

<From Web Connection>

✔ For the procedure to call the Network menu to the display, see steps 1 and 2 of **"Changing the auth-password and priv-password" on page 2-94**.

1 Start the Web Connection and call the Network menu to the display.

2 Click the [SMB Setting] menu.

3 Click the [Print Setting] menu.

4 Enter the NetBIOS Name in the "NetBIOS Name" box.

5 Click the [OK].

6 Click the [OK].

7 Click the [Logout].

2.20 AppleTalk Setting Function

When access to the Administrator of the machine by the Administrator Settings is authenticated, the machine enables making of the AppleTalk Settings.

2.20.1 Making the AppleTalk 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.

<From the Control Panel>

✔ For the procedure to call the Network Settings menu to the display, see steps 1 and 2 of **"Changing the auth-password and priv-password" on page 2-94**.

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

2 Touch [AppleTalk Settings].

3 Make the necessary settings.

4 Touch [OK].

<From Web Connection>

✔ For the procedure to call the Network menu to the display, see steps 1 and 2 of **"Changing the auth-password and priv-password" on page 2-94**.

1 Start the Web Connection and call the Network menu to the display.

2 Click the [AppleTalk Setting] menu.

3 Make the necessary settings.

4 Click the [OK].

5 Click the [OK].

6 Click the [Logout].

2.21 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).

2.21.1 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.

<From the Control Panel>

✔ For the procedure to call the Network Settings menu to the display, see steps 1 and 2 of **"Changing the auth-password and priv-password" on page 2-94**.

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].

<From Web Connection>

✔ For the procedure to call the Network menu to the display, see steps 1 and 2 of **"Changing the auth-password and priv-password" on page 2-94**.

1 Start the Web Connection and call the Network menu to the display.

2 Click the [E-mail Setting] menu.

3 Click the [E-mail TX (SMTP)] menu.

4 Make the necessary settings.

5 Click the [OK].

6 Click the [OK].

7 Click the [Logout].

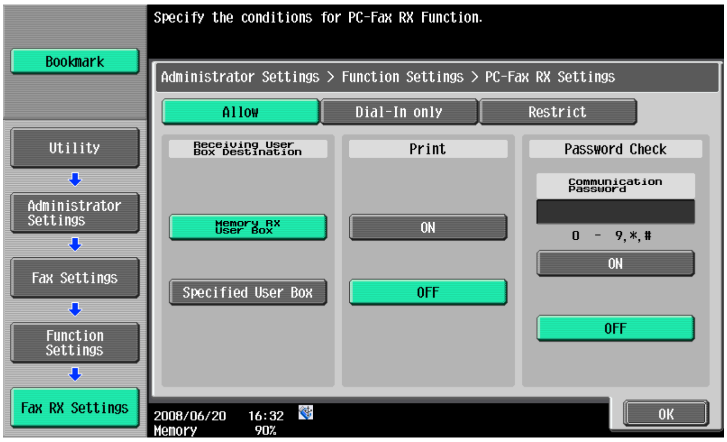
2.22 Setting PC-FAX receiving

You can set whether or not to use PC-FAX receive function when the optional hard disk is mounted.

2.22.1 Setting PC-FAX receive

<From the Control Panel>

When the function to be used, set the following contents.



Specify the conditions for PC-Fax RX Function.

Item	Explanation
Receiving User Box Destination	Received data is output or input to forced memory inbox or specified box. [Specified User Box] is selected, the data is stored at the box whose number is assigned with F code Sub address.
Print	It is set whether or not to print after receiving data.
Password Check	It can set password check/communication password (within 8 digits).

Detail

When Dial-in is set ON, [Dial-in only] is appeared after [Allow]. PC-FAX receiving setting cam be made only when the data is received with dial-in number.

FAX input data is saved to the box as TIFF.

When a user [Specified User Box] set at when data is sent out, 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] is deleted, the data will be saved at the newly assigned inbox, Therefore you should be careful with the number assigned.

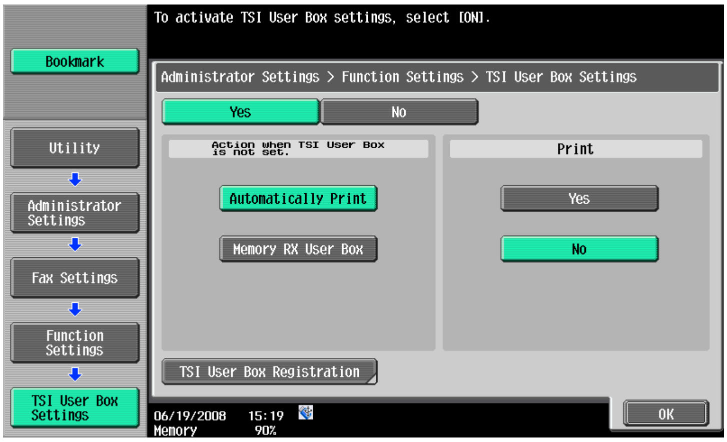
2.23 Setting TSI distribution

When the optional hard disk is mounted, TSI distribution function will be available.

2.23.1 Setting TSI distribution

<From the Control Panel>

When the optional hard disk is mounted, you can set whether or not to use TSI distribution system.



To activate TSI User Box settings, select [ON].

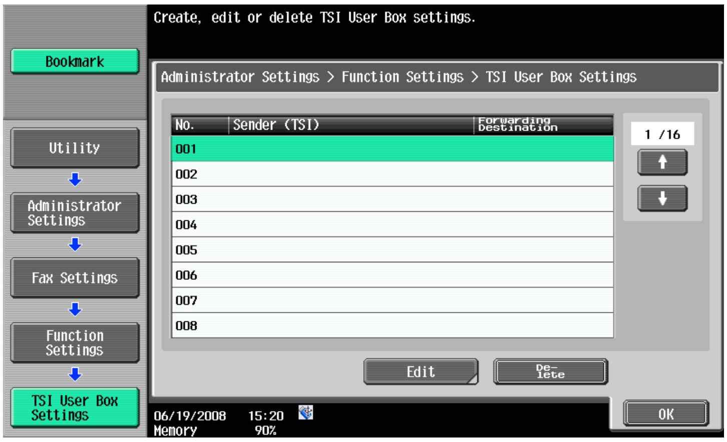
Administrator Settings > Function Settings > TSI User Box Settings

Item	Explanation
Action when TSI User Box is not set	Setting when applicable boxes do not exist [Automatically Print]: Received data will be printed out [Memory RX User Box]: Data will be saved to forced memory inbox
Print	Setting whether or not to print after receiving data
TSI User Box Registration	To register where the TSI is distributed to.

2.23.2 Setting TSI distribution and register TSI distribution

<From the Control Panel>

You can register up to 128 where the received data is distributed. Select the number to be set and press [Edit].



Create, edit or delete TSI User Box settings.

Administrator Settings > Function Settings > TSI User Box Settings

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

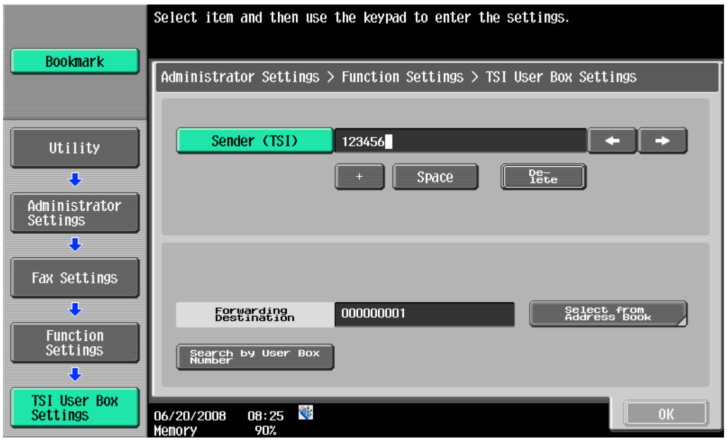
Reminder

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

2.23.3 Setting TSI distribution and register TSI distribution

<From the Control Panel>

Received fax can be distributed to other machine or box of this machine. Fax ID of sender is entered at [Sender (TSI)] and the place the data to be distributed to is set at [Forwarding Destination]. To distribute to other machine, specify the place at [Select from Address Book]. To distribute to the box of this machine, specify it at [Search by User Box Number].



Select item and then use the keypad to enter the settings.

Administrator Settings > Function Settings > TSI User Box Settings

Sender (TSI): 123456

Forwarding Destination: 000000001

06/20/2008 08:25
Memory 90%

Detail

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

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

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 box, Therefore you should be careful with the number assigned.

3 User Operations

3 User Operations

3.1 User Authentication Function

When [ON (MFP)] or [ON (External Server)] (Active Directory) is set for Authentication Method of the Administrator Settings, the User Authentication function implements authentication of the user of this machine before he or she actually uses it through the User Password that consists of 8 to 64 digits. During the authentication procedure, the User 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.

✎...

Note

*Before operating the machine, the user him/herself should change the User Password from that registered by the Administrator of the machine. For details of changing the User Password, see **"Performing Change Password" on page 3-9**. For more details of User Name and User Password, ask the Administrator of the machine.*

If the User Password is changed by the Administrator of the machine during operation of this machine, the user him/herself should immediately change the User Password.

3.1.1 Performing user authentication

If a document is stored in the ID & Print User Box, select any desired login method.

✎...

Note

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

Make absolutely sure that your User Password is not known by any other users.

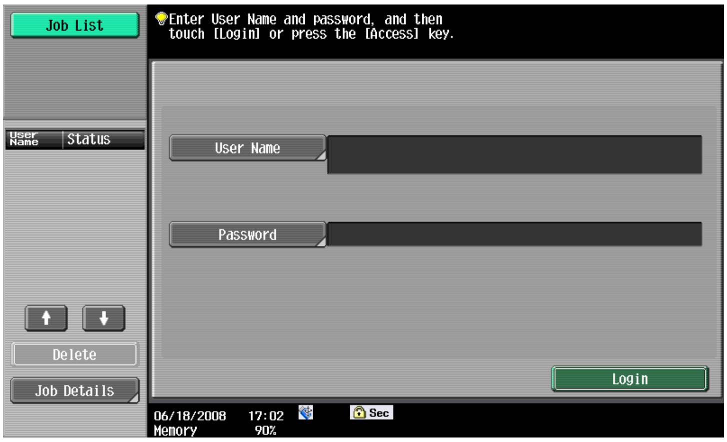
✎...

Reminder

If any User Name not registered with this machine is authenticated through User Authentication when [ON (External Server)] (Active Directory) is set for Authentication Method, the User Name is automatically registered with this machine.

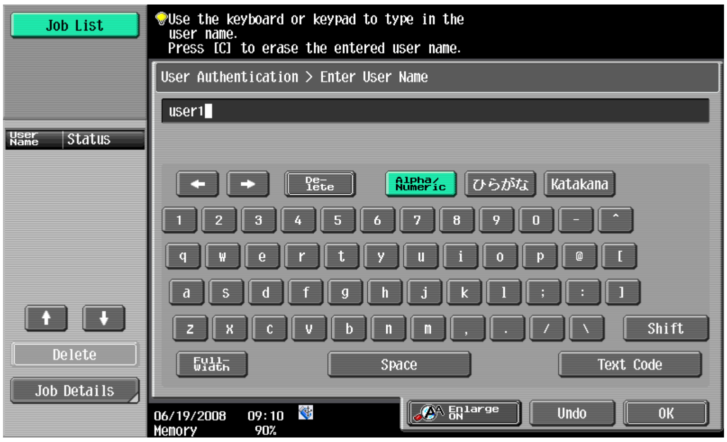
<From the Control Panel>

1 Touch [User Name].



Enter User Name and password, and then touch [Login] or press the [Access] key.

2 Enter the User Name from the keyboard and keypad.



Use the keyboard or keypad to type in the user name.
Press [C] to erase the entered user name.

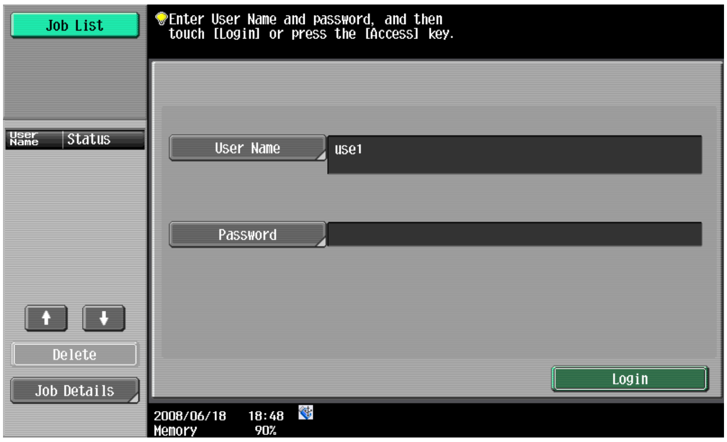
User Authentication > Enter User Name

user1

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

3 Touch [OK].

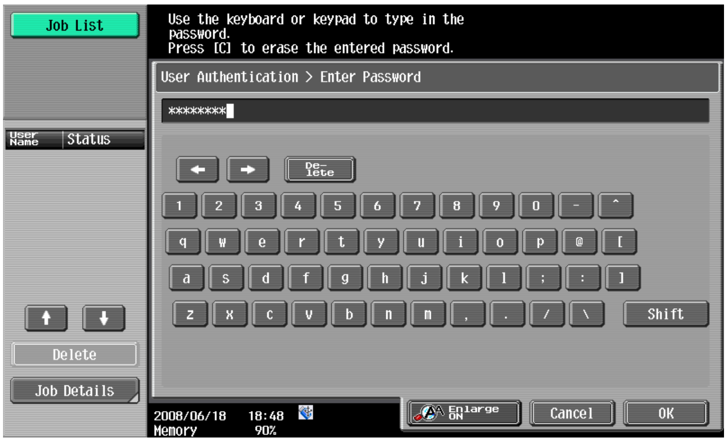
4 Touch [Password].



Enter User Name and password, and then touch [Login] or press the [Access] key.

User Name: use1

5 Enter the 8-to-64-digit User Password from the keyboard or keypad.



Use the keyboard or keypad to type in the password.
Press [C] to erase the entered password.

User Authentication > Enter Password

****

– 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 4.

6 Touch [OK].

7 Press [Access] or touch [Login].

– Go to step 15 if User Authentication only has been set, or "Synchronize" has been set for Synchronize User Authentication & Account Track.

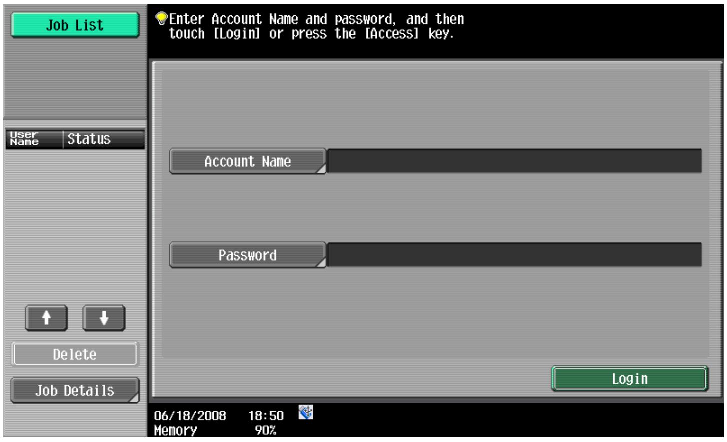
? What if a wrong User Name or User Password is entered?

→ If a wrong User Name is entered, a message appears that tells that authentication has not been successful. The machine then prohibits entry for User Authentication for 5 sec. and then causes the screen of step 1 to reappear. Perform User Authentication once again.

→ If there is a mismatch of User Password relative to the registered User Name, a message appears that tells that authentication has not been successful. The machine then prohibits entry of User Name and User Password for 5 sec. and then causes the screen of step 4 to reappear. Enter the correct User Password.

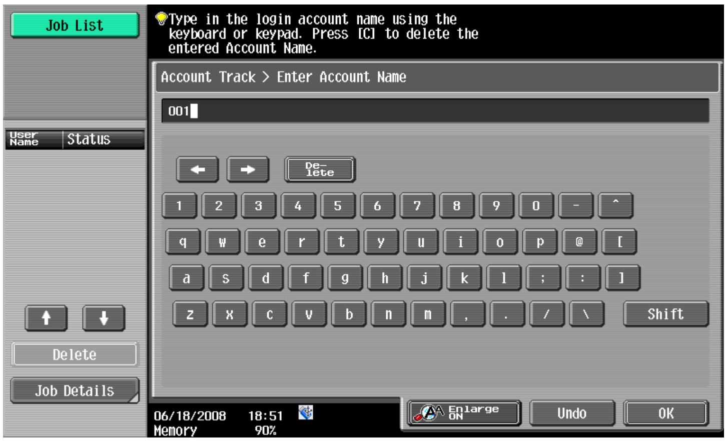
→ If the Enhanced Security Mode is set to [ON], the entry of a wrong User Password is counted as unauthorized access. If a wrong User Password for the corresponding User Name entered is entered a predetermined number of times (once to three times) set by the Administrator of the machine or more, a message appears that tells that authentication has not been successful for any subsequent operation for authentication. The machine is then set into an access lock state, rejecting any more logon attempts. To cancel the access lock state, the Administrator of the machine must perform the Release Setting. Contact the Administrator of the machine.

8 Touch [Account Name].



Enter Account Name and password, and then touch [Login] or press the [Access] key.

9 Enter the Account Name from the keyboard and keypad.


Type in the login account name using the keyboard or keypad. Press [C] to delete the entered Account Name.

Account Track > Enter Account Name

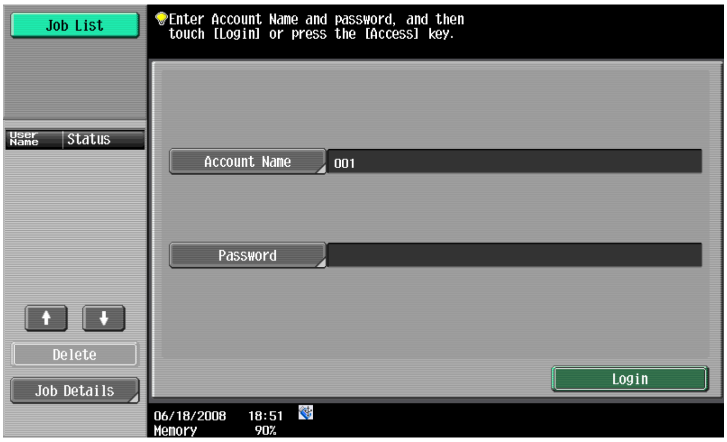
001

06/18/2008 18:51 Memory 90%

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

10 Touch [OK].

11 Touch [Password].

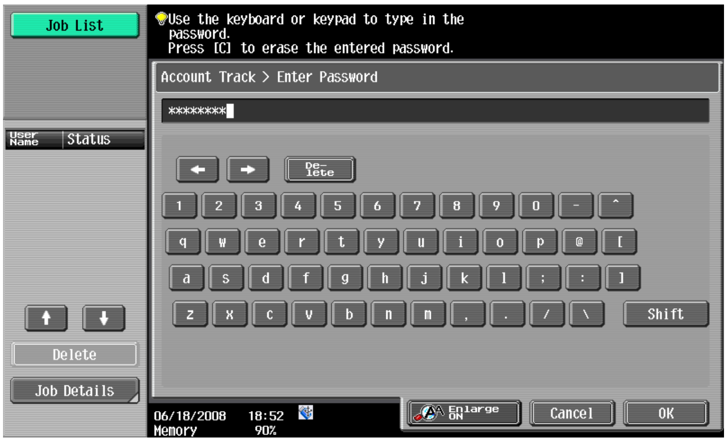

Enter Account Name and password, and then touch [Login] or press the [Access] key.

Account Name 001

Password

06/18/2008 18:51 Memory 90%

12 Enter the 8-digit Account Password from the keyboard or keypad.


Use the keyboard or keypad to type in the password.
Press [C] to erase the entered password.

Account Track > Enter Password

****

06/18/2008 18:52 Memory 90%

- 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 11.

13 Touch [OK].

14 Press [Access] or touch [Login].

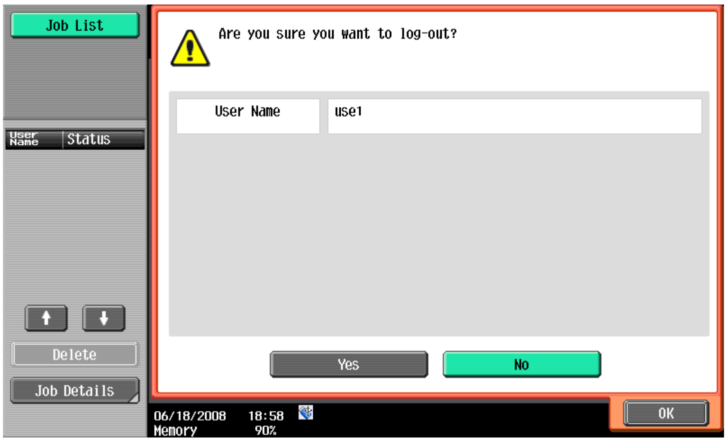
? What if a wrong Account Name or Account Password is entered?

➔ If a wrong Account Name is entered, a message appears that tells that authentication has not been successful. The machine then prohibits entry for Account authentication for 5 sec. and then causes the screen of step 1 to reappear. Perform Account authentication once again.

➔ If there is a mismatch of Account Password relative to the registered Account Name, a message appears that tells that authentication has not been successful. The machine then prohibits entry of Account Name and Account Password for 5 sec. and then causes the screen of step 11 to reappear. Enter the correct Account Password.

➔ If the Enhanced Security Mode is set to [ON], the entry of a wrong Account Password is counted as unauthorized access. If a wrong Account Password for the corresponding Account Name entered is entered a predetermined number of times (once to three times) set by the Administrator of the machine or more, a message appears that tells that authentication has not been successful for any subsequent operation for authentication. The machine is then set into an access lock state, rejecting any more logon attempts. To cancel the access lock state, the Administrator of the machine must perform the Release Setting. Contact the Administrator of the machine.

15 Pressing the [Access] key will show the following screen.
Select [Yes] and touch [OK] to log off from the user operation mode.

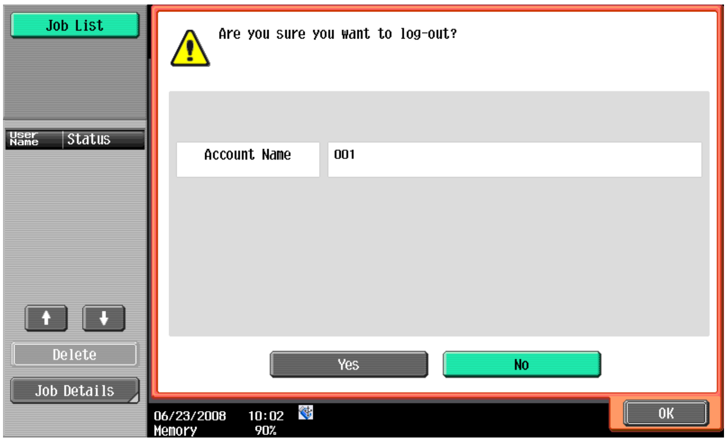


Are you sure you want to log-out?

User Name: use1

06/18/2008 18:58
Memory 90%

– The following screen appears if Account Track has been set.



Are you sure you want to log-out?

Account Name: 001

06/23/2008 10:02
Memory 90%

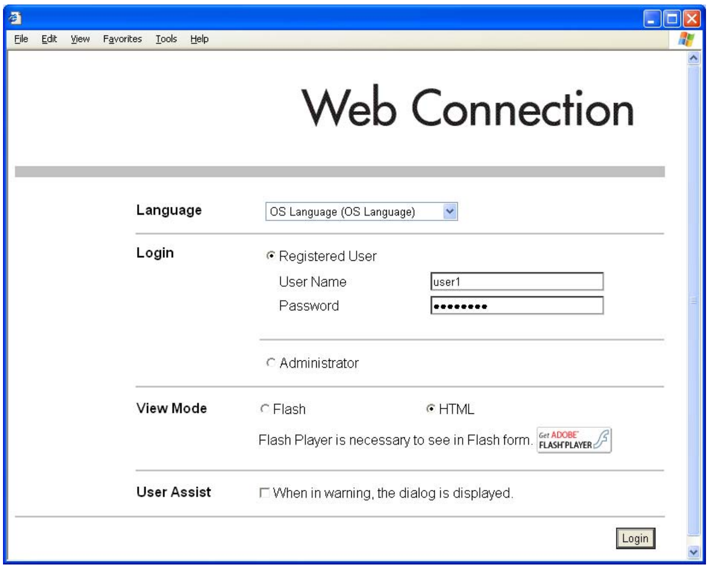
<From Web Connection>

1 Start the Web browser.

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

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

4 Click the Registered User radio button and enter the User Name and User Password.



Web Connection

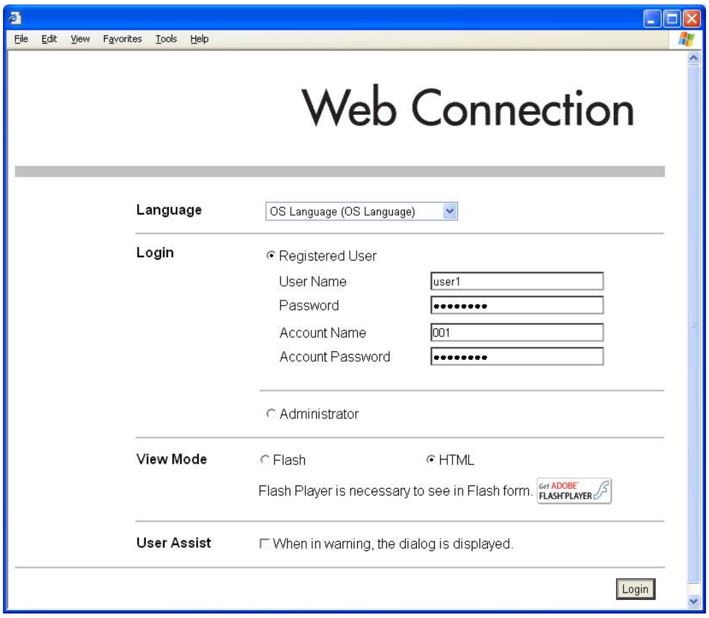
Language: OS Language (OS Language)

Login: ● Registered User
User Name: user1
Password: ••••••••
○ Administrator

View Mode: ○ Flash ● HTML
Flash Player is necessary to see in Flash form.

User Assist: □ When in warning, the dialog is displayed.

- If Account Track has been set, enter the User Name, User Password, Account Name, and Account Password.



Web Connection

Language: OS Language (OS Language)

Login: ● Registered User
User Name: user1
Password: ••••••••
Account Name: 001
Account Password: ••••••••
○ Administrator

View Mode: ○ Flash ● HTML
Flash Player is necessary to see in Flash form.

User Assist: □ When in warning, the dialog is displayed.

- If "Synchronize" has been set for Synchronize User Authentication & Account Track, successful authentication results from simply entering the User Name and User Password.

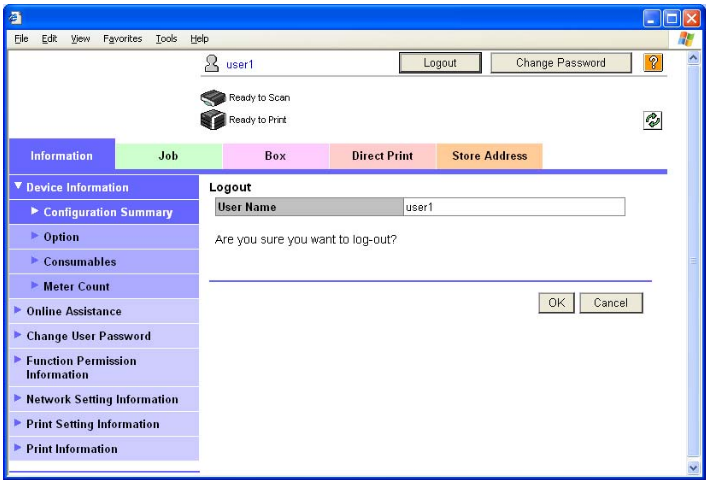
5 Click the [Login].

? What if a wrong User Name or User Password is entered?

→ If there is a mismatch of User/Account Password relative to the registered User/Account Name, a message appears that tells that authentication has not been successful. Click [OK] to go back to the screen of step 4. Enter the correct User/Account Name and User/Account Password.

→ If the Enhanced Security Mode is set to [ON], the entry of a wrong User/Account Password is counted as unauthorized access. If a wrong User/Account Password for the corresponding User/Account Name entered is entered a predetermined number of times (once to three times) set by the Administrator of the machine or more, a message appears that tells that authentication has not been successful for any subsequent operation for authentication. The machine is then set into an access lock state, rejecting any more logon attempts. To cancel the access lock state, the Administrator of the machine must perform the Release Setting. Contact the Administrator of the machine.

6 Clicking [Logout] will show the following screen.
Click [OK] to log off from the user operation mode.



Logout

User Name	user1

Are you sure you want to log-out?

3.2 Change Password Function

When [ON (MFP)] is set for Authentication Method of User Authentication, the machine permits each of all users who have been authenticated through User Authentication to change his or her User Password.

The User Password entered is displayed as "*" or "●."

3.2.1 Performing Change Password

✎...

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.

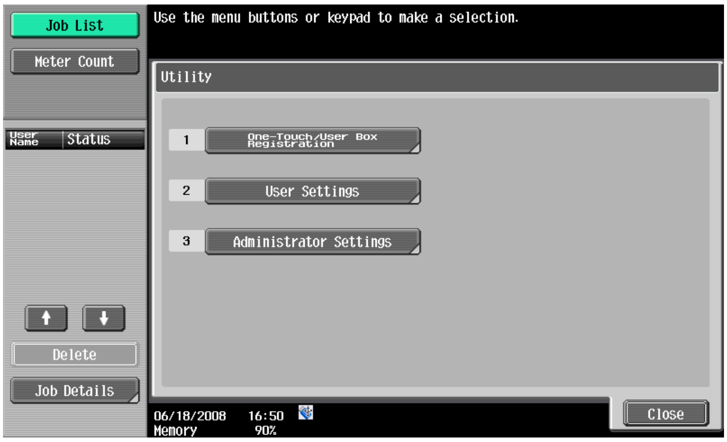
<From the Control Panel>

✔ For the logon procedure, see **"Performing user authentication" on page 3-2**.

1 Log on to the user operation mode through User Authentication from the control panel.

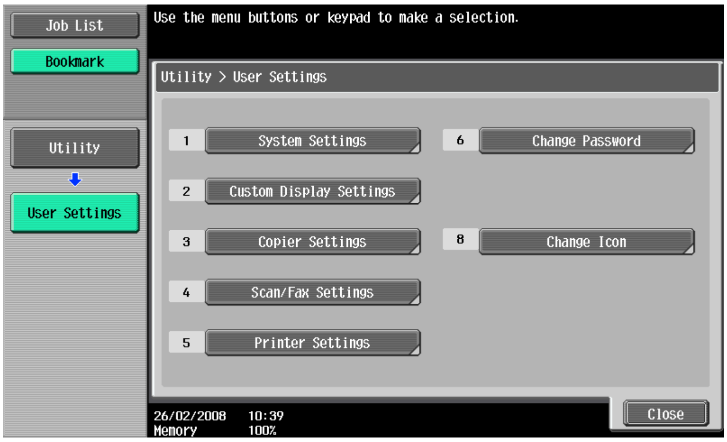
2 Press the [Utility/Counter] key.

3 Touch [User Settings].



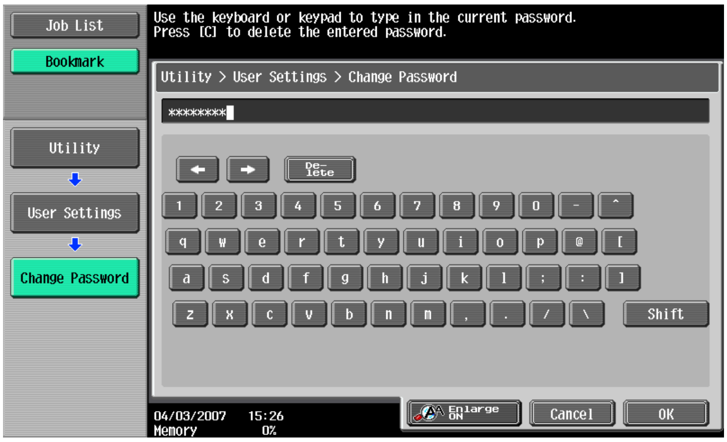
Use the menu buttons or keypad to make a selection.

4 Touch [Change Password].



Use the menu buttons or keypad to make a selection.

5 Enter the currently registered 8-digit-or-more User Password from the keyboard and keypad.



Use the keyboard or keypad to type in the current password.
Press [C] to delete the entered password.

Utility > User Settings > Change Password

****

04/03/2007 15:26
Memory 0%

- 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 previous screen.

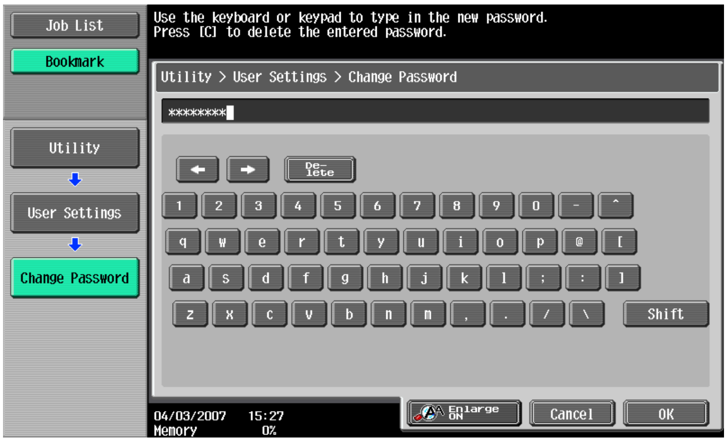
6 Touch [OK].

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

→ If there is a mismatch in the User Passwords, a message appears that tells that there is a mismatch in the User Passwords. Enter the correct User Password.

→ If the Enhanced Security Mode is set to [ON], the entry of a wrong User Password is counted as unauthorized access. If the current password is mistakenly entered a predetermined number of times (once to three times) set by the Administrator of the machine, the user authentication screen will reappear. A message then appears that tells that authentication has not been successful for any subsequent operation for authentication. The machine is now set into an access lock state, rejecting any more logon attempts. To cancel the access lock state, the Administrator of the machine must perform the Release Setting. Contact the Administrator of the machine.

7 From the keyboard or keypad, enter the new User Password that can consist of 8 to 64 digits.



Use the keyboard or keypad to type in the new password.
Press [C] to delete the entered password.

Utility > User Settings > Change Password

****

04/03/2007 15:27
Memory 0%

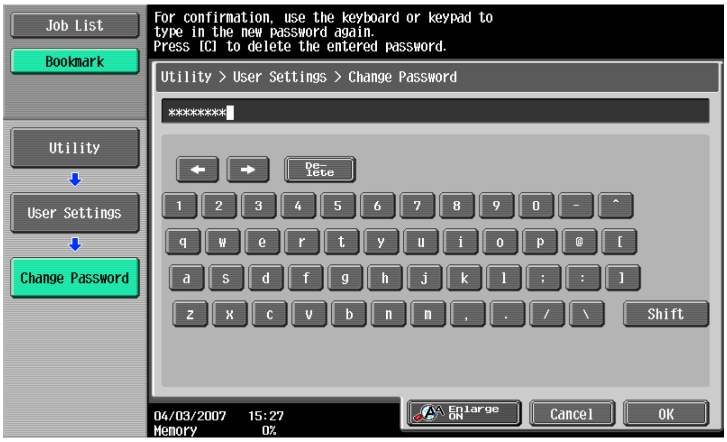
- Press the [C] key to clear all characters.
- Touch [Delete] to delete the last character entered.
- Touch [Shift] to show the upper case/symbol screen.
- Touch [Cancel] to go back to the screen shown in step 4.

8 Touch [OK].

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

→ If the User Password entered does not comply with the Password Rules, a message appears that tells that the User Password entered cannot be used. Enter the correct User Password. For details of the Password Rules, see **"Password Rules" on page 1-9**.

9 To prevent entry of a wrong password, enter the 8-to-64-digit User Password again.



For confirmation, use the keyboard or keypad to type in the new password again.
Press [C] to delete the entered password.

Utility > User Settings > Change Password

****

04/03/2007 15:27
Memory 0%

– 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 4.

10 Touch [OK].

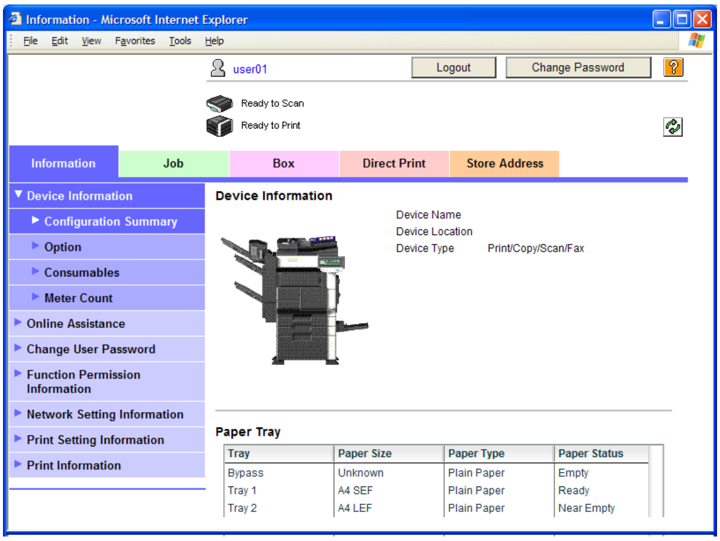
? What happens if there is a mismatch in the User Passwords?
➔ If there is a mismatch in the User Passwords, a message appears that tells that there is a mismatch in the User Passwords. Perform steps 7 through 10 once again.

<From Web Connection>

✔ For the logon procedure, see "Performing user authentication" on page 3-2.

1 Log on to the user operation mode through User Authentication from the Web Connection.

2 Click the [Change User Password] menu of the [Information] tab or [Change Password].



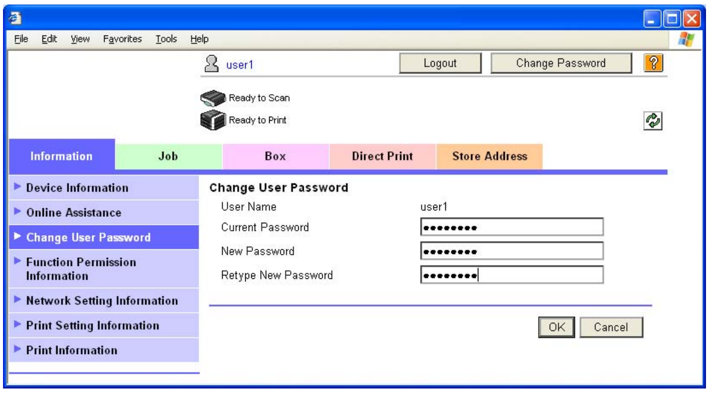
Device Information

Device Name
Device Location
Device Type Print/Copy/Scan/Fax

Paper Tray

Tray	Paper Size	Paper Type	Paper Status
Bypass	Unknown	Plain Paper	Empty
Tray 1	A4 SEF	Plain Paper	Ready
Tray 2	A4 LEF	Plain Paper	Near Empty

3 Enter the currently registered User Password and a new User Password. Then, to make sure that you have entered the correct new password, enter the new User Password once again.



Change User Password

User Name	user1
Current Password	••••••••
New Password	••••••••
Retype New Password	••••••••

4 Click the [OK].

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

→ If there is a mismatch in the password between the currently registered User Password and the User Password typed in the "Current Password" box, a message appears that tells there is a mismatch in the User Password. Click [OK] to go back to the user authentication screen. Then, perform steps 1 through 5 again.

? What happens if the User Password entered in the New Password box fails to meet the requirements of the Password Rules?

→ If the User Password entered in the "New Password" box fails to meet the requirements of the Password Rules, a message appears that tells that the User Password entered cannot be used, as it fails to meet the requirements of the Password Rules. Click [OK] to go back to the screen of step 3. Perform steps 3 and 4 once again. For details of the Password Rules, see "Password Rules" on page 1-9.

? What happens if there is a mismatch in the password between that entered in New Password and that entered in Retype New Password?

→ If there is a mismatch in the password between that entered in the "New Password" box and that entered in the "Retype New Password" box, a message appears that tells that there is a mismatch in the User Password. Enter the correct User Password.

5 Click the [OK].

3.3 Secure Print Document Function

The Secure Print Document function allows a Secure Print Document specified by a corresponding password from the PC to be used in the condition registered in the machine.

To access a Secure Print Document file, authentication is performed through an 8-digit password that verifies an authenticated user of the Secure Print Document file. The password entered is displayed as "*." When the Enhanced Security Mode is set to [ON], the number of times in which authentication fails is counted.

✎...

Note

When the Enhanced Security Mode is set to [ON], go through User Authentication by entering the User Name and User Password registered in the machine through the printer driver of the PC. The password entered is displayed as "." If the User Password does not correspond to the User Name entered, the Secure Print Job is discarded without being registered. Entry of a wrong User Password is counted as unauthorized access. If a wrong User Password is entered a predetermined number of times (once to three times) set by the Administrator of the machine or more, the subsequent authentication operation is an access lock state and it is not possible to transmit the print job. As a result, the access lock state disables user authentication attempts from the control panel or Web Connection. To cancel the access lock state, the Administrator of the machine must perform the Release Setting. Contact the Administrator of the machine.*

Enter the Secure Print ID and password through the printer driver on the PC side. The password entered is displayed as "."*

*The Secure Print password must be the one consisting of 8 digits and meeting the Password Rules requirements. Any Secure Print Document, the password for which does not meet the Password Rules requirements, will not be registered in the machine. For details of the Password Rules, see **"Password Rules" on page 1-9**.*

3.3.1 Accessing the Secure Print 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.

For the Secure Print ID, enter the one that has been set on the printer driver side.

If a wrong Secure Print ID is entered, the target Secure Print Document will not be displayed. Enter the correct Secure Print ID.

For the Secure Print Password, enter the 8-digit one set on the printer driver side.

The machine rejects any Secure Print Password that consists of less than 8 digits.

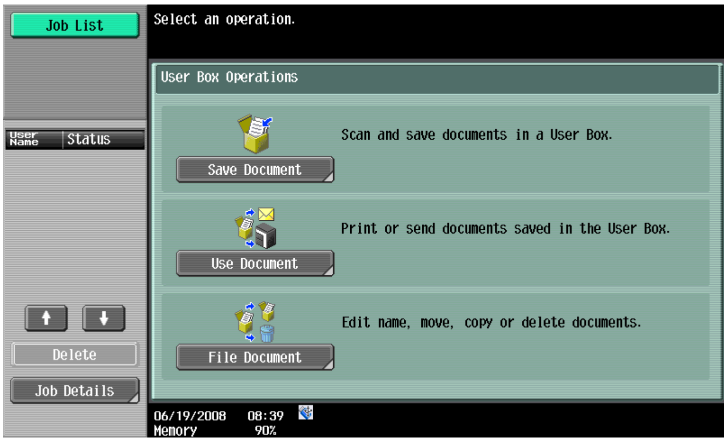
<Setting can be made only from the control panel>

✔ For the logon procedure, see "Performing user authentication" on page 3-2.

1 Log on to the user operation mode through User Authentication from the control panel.

2 Press the [Box] key.

3 Touch [Use Document].



Select an operation.

User Box Operations

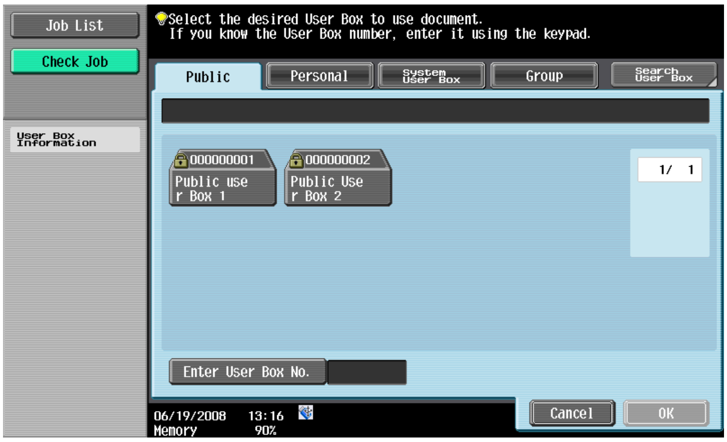
Scan and save documents in a User Box.

Print or send documents saved in the User Box.

Edit name, move, copy or delete documents.

06/19/2008 08:39
Memory 90%

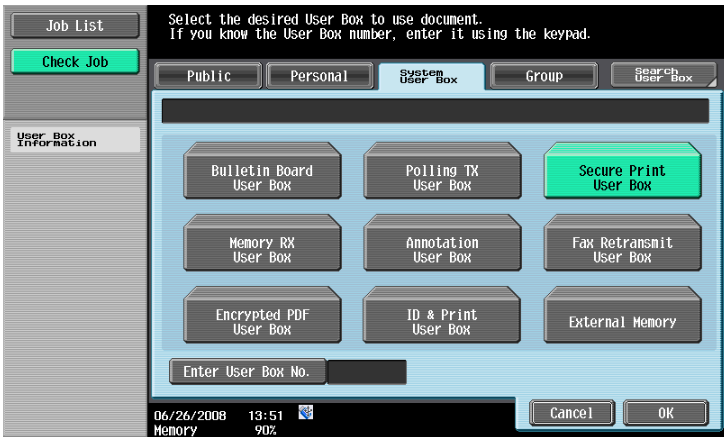
4 Touch [System User Box] tab.



Select the desired User Box to use document.
If you know the User Box number, enter it using the keypad.

06/19/2008 13:16
Memory 90%

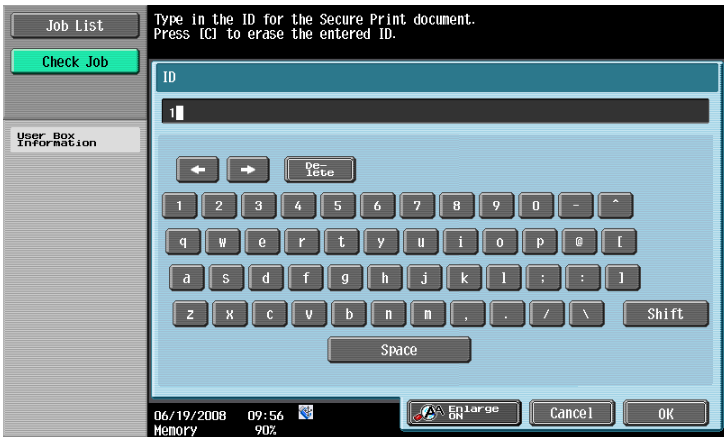
5 Select [Secure Print User Box] and touch [OK].



Select the desired User Box to use document.
If you know the User Box number, enter it using the keypad.

06/26/2008 13:51
Memory 90%

6 Enter the Secure Print ID that consists of up to 16 digits from the keyboard and keypad.



Type in the ID for the Secure Print document.
Press [C] to erase the entered ID.

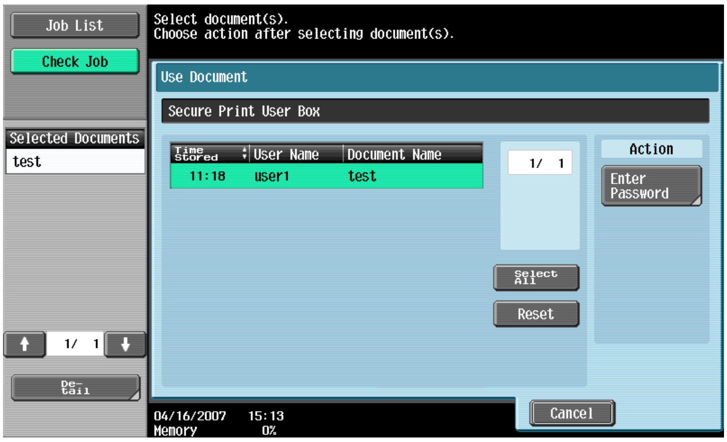
ID: 1

06/19/2008 09:56
Memory 90%

- 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 5.

7 Touch [OK].

8 Select the desired Secure Print Document and touch [Enter Password].



Select document(s).
Choose action after selecting document(s).

Use Document

Secure Print User Box

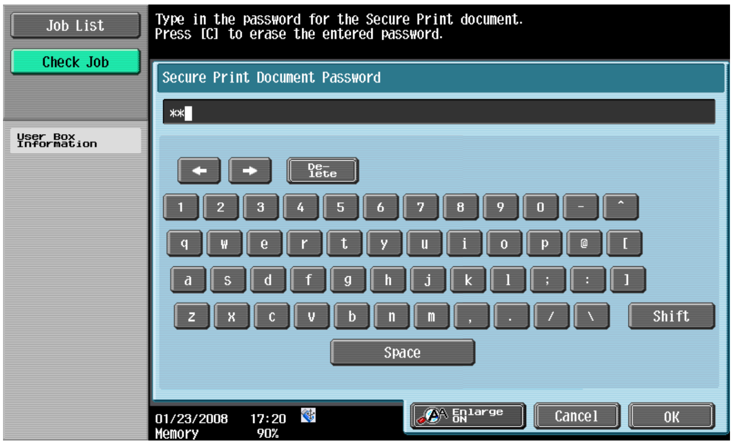
Selected Documents: test

Time Stored	User Name	Document Name
11:18	user1	test

04/16/2007 15:13
Memory 0%

- Two or more Secure Print Documents can be selected at the same time.
- Touching [Select All] will select all Secure Print Documents having the same ID shown in the list.

9 Enter the 8-digit Secure Print Password from the keyboard and keypad.



Type in the password for the Secure Print document.
Press [C] to erase the entered password.

Secure Print Document Password: **

01/23/2008 17:20
Memory 90%

- 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 8.

10 Touch [OK].

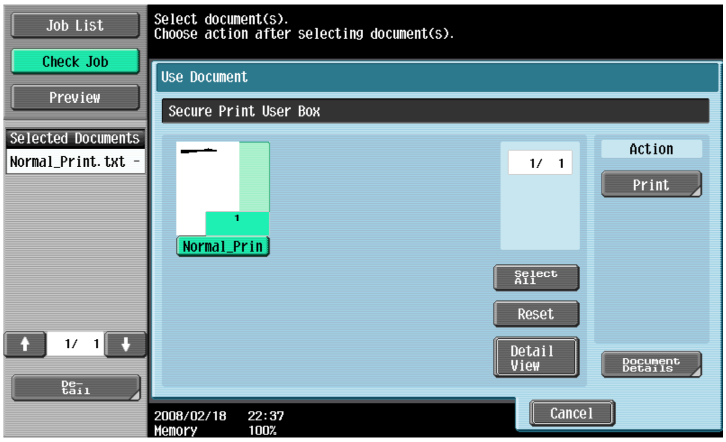
? What if there is a mismatch of the Secure Print Password relative to the Secure Print ID?

➔ If there is a mismatch of the Secure Print Password relative to the Secure Print ID, a message appears that tells that authentication has not been successful. The machine then prohibits entry of the Secure Print Password for 5 sec. Enter the correct Secure Print Password.

➔ If two or more Secure Print Documents have been selected in step 8, the machine counts as unauthorized access any Secure Print Document, the Secure Print Password of which is a mismatch.

➔ If the Enhanced Security Mode is set to [ON], entry of a wrong Secure Print Password is counted as unauthorized access. If a wrong Secure Print Password is entered a predetermined number of times (once to three times) set by the Administrator of the machine or more, a message appears that tells that authentication has not been successful for any subsequent operation for authentication. The machine is then set into an access lock state, disabling access to the Secure Print Document. To cancel the access lock state, the Administrator of the machine must perform the Release Setting. Contact the Administrator of the machine.

11 Select the target Secure Print Document and touch [Print].



Select document(s).
Choose action after selecting document(s).

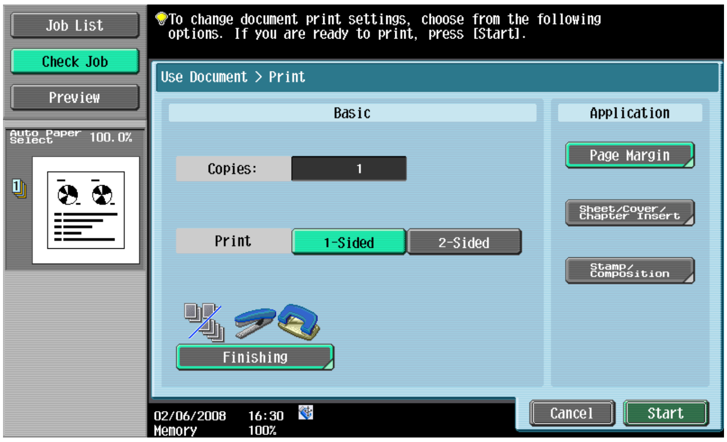
Use Document

Secure Print User Box

Selected Documents
Normal_Print.txt

2008/02/18 22:37
Memory 100%

12 Check the details of the document and press the [Start] key or touch [Start].



To change document print settings, choose from the following options. If you are ready to print, press [Start].

Use Document > Print

Copies: 1

Print: 1-Sided

Auto Paper Select 100.0%

02/06/2008 16:30
Memory 100%

– Touch [Cancel] to go back to the screen shown in step 11.

✎...

Reminder

If two or more Secure Print Documents, each having an identical Secure Print ID and Secure Print Password, have been registered, multiple Secure Print Documents can be printed at once.

3.4 User Box Function

For all users who have been authenticated through User/Account Authentication, the machine enables the operation of registering and changing the User Box. It also enables the operation of acquiring or printing image files saved in the User Box and sending of S/MIME encrypted image files.

User Box creates a User Box in the HDD as a space for storing an image file. User Box is available in three different types: Personal User Box which only the user who has logged on through User Authentication can use; Public User Box that is shared among two or more users who have previously registered; and Group User Box that can be used by the user who has logged on through Account Authentication. Up to 1,000 User Boxes can be registered.

A user who accesses the Personal User Box or Public User Box or Group User Box is authenticated through an 8-digit User Box Password. The 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.

Reminder
If a job is executed in the copy, fax, scan, or printer mode by specifying a User Box number that has not been registered, the Personal User Box owned by the user who logged on through User Authentication is automatically registered.

If Account Track has not been enabled, Group User Box cannot be created.

3.4.1 Setting the User Box

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 the User Box type is changed after a User Box Password has been set, it clears the User Box Password. Set the User Box Password once again.

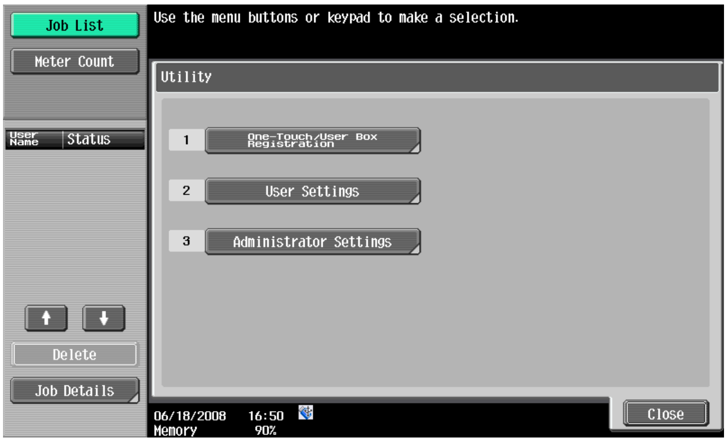
<From the Control Panel>

✔ For the logon procedure, see **"Performing user authentication" on page 3-2**.

1 Log on to the user operation mode through User Authentication from the control panel.

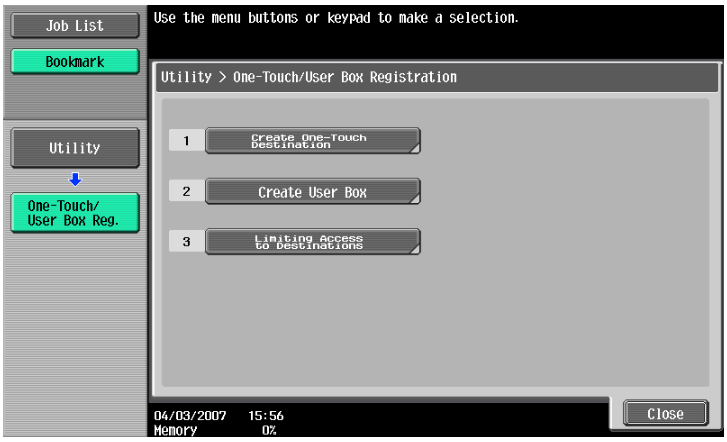
2 Press the [Utility/Counter] key.

3 Touch [One-Touch/User Box Registration].



Use the menu buttons or keypad to make a selection.

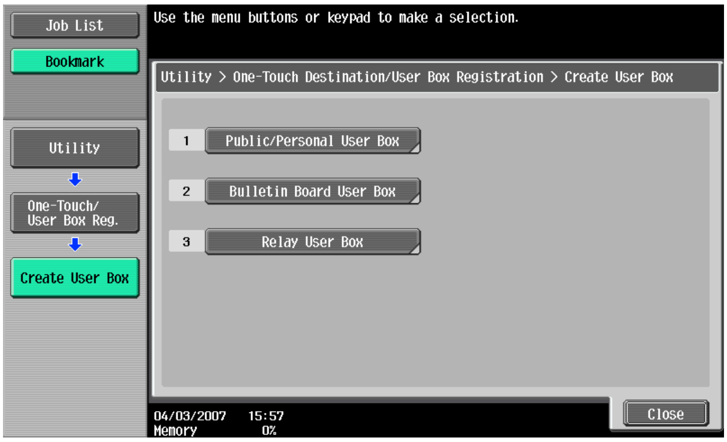
4 Touch [Create User Box].


Use the menu buttons or keypad to make a selection.

Utility > One-Touch/User Box Registration

04/03/2007 15:56
Memory 0%

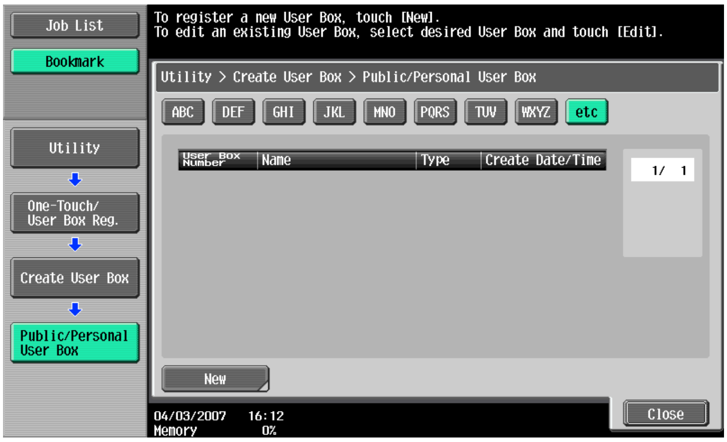
5 Touch [Public/Personal User Box].


Use the menu buttons or keypad to make a selection.

Utility > One-Touch Destination/User Box Registration > Create User Box

04/03/2007 15:57
Memory 0%

6 Touch [New].


To register a new User Box, touch [New].
To edit an existing User Box, select desired User Box and touch [Edit].

Utility > Create User Box > Public/Personal User Box

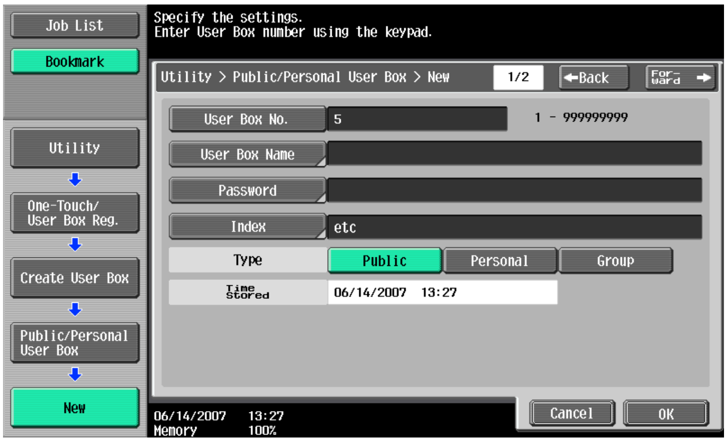
User Box Number	Name	Type	Create Date/Time

04/03/2007 16:12
Memory 0%

? What steps should be performed to change the User Box setting?

→ For the procedure to change the User Box setting, see **"Changing the User Box Password and user attributes and account attributes" on page 3-23**.

7 Touch [Public] or [Personal] or [Group] to select the User Box type.



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

Utility > Public/Personal User Box > New

User Box No.: 5 (1 - 999999999)
User Box Name:
Password:
Index: etc
Type: Public
Time Stored: 06/14/2007 13:27

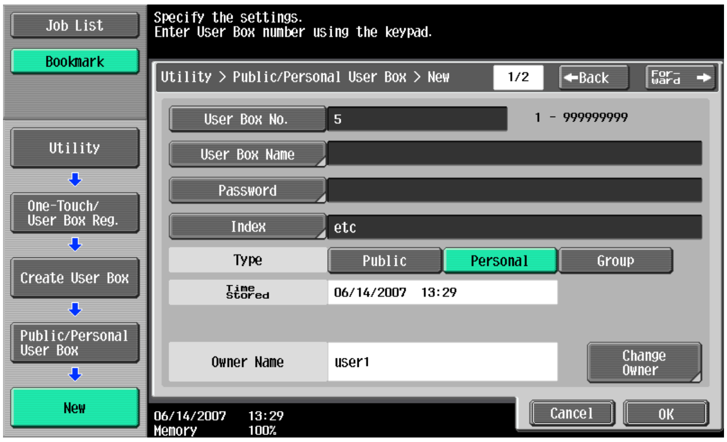
06/14/2007 13:27
Memory 100%

? What steps should be performed to change the Owner Name of the User Box?

→ When [Personal] is selected, [Change Owner] is displayed. Then, select the owner user.

→ When [Group] is selected, [Change Account Name] is displayed. Then, select the account.

8 Touch [Password].



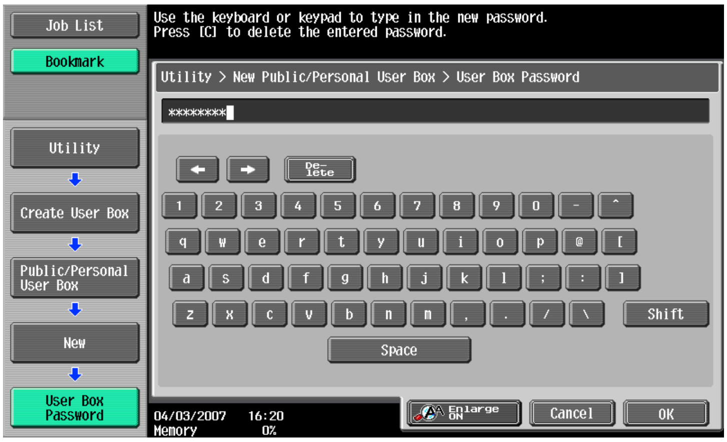
Specify the settings.
Enter User Box number using the keypad.

Utility > Public/Personal User Box > New

User Box No.: 5 (1 - 999999999)
User Box Name:
Password:
Index: etc
Type: Personal
Time Stored: 06/14/2007 13:29
Owner Name: user1

06/14/2007 13:29
Memory 100%

9 Enter the new 8-digit User Box Password from the keyboard and keypad.



Use the keyboard or keypad to type in the new password.
Press [C] to delete the entered password.

Utility > New Public/Personal User Box > User Box Password

****

04/03/2007 16:20
Memory 0%

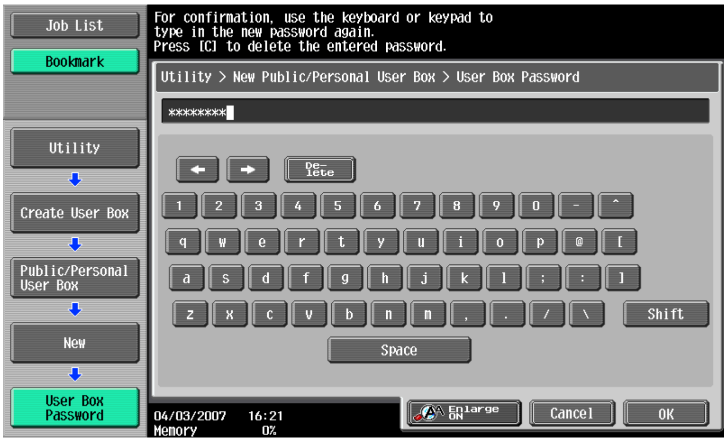
– Press the [C] key to clear all characters.
– Touch [Delete] to delete the last character entered.
– Touch [Shift] to show the upper case/symbol screen.
– Touch [Cancel] to go back to the screen shown in step 8.

10 Touch [OK].

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

➔ If the User Box Password entered does not meet the requirements of the Password Rules with [Public] selected for User Box Type, a message appears that tells that the User Box Password that has been entered cannot be used. Enter the correct User Box Password. For details of the Password Rules, see **"Password Rules" on page 1-9**.

11 To prevent entry of a wrong password, enter the 8-digit User Box Password again.



For confirmation, use the keyboard or keypad to type in the new password again.
Press [C] to delete the entered password.

Utility > New Public/Personal User Box > User Box Password

****

04/03/2007 16:21
Memory 0%

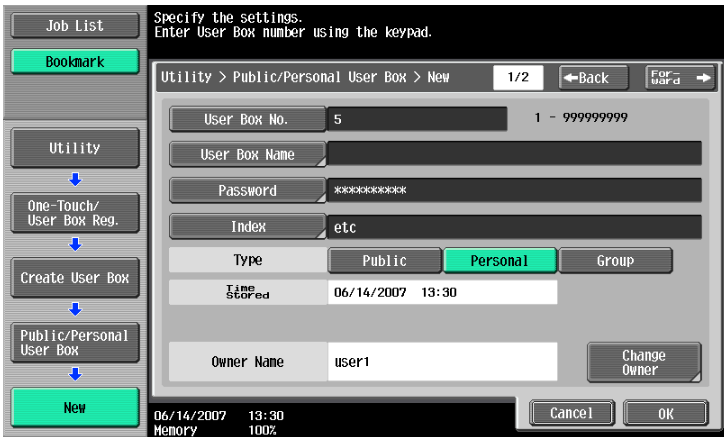
– Press the [C] key to clear all characters.
– Touch [Delete] to delete the last character entered.
– Touch [Shift] to show the upper case/symbol screen.
– Touch [Cancel] to go back to the screen shown in step 8.

12 Touch [OK].

? What happens if there is a mismatch in the User Box Passwords?

➔ If there is a mismatch in the User Box Passwords, a message appears that tells that there is a mismatch in the User Box Passwords. Perform steps 9 through 11 once again.

13 Make the necessary settings.



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

Utility > Public/Personal User Box > New 1/2

User Box No.: 5 (1 - 999999999)
User Box Name:
Password: **********
Index: etc
Type: Public Personal Group
Time Stored: 06/14/2007 13:30
Owner Name: user1

06/14/2007 13:30
Memory 100%

? What if a User Box No. is duplicated?

➔ A User Box No. that has been registered cannot be registered anew.

? What if no Name has been entered?

➔ If no Name has been registered, [OK] cannot be touched. Be sure to register the Name.

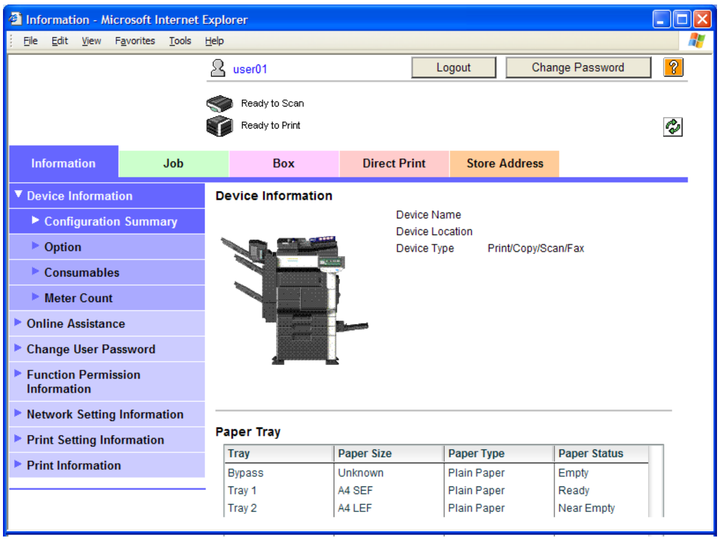
14 Touch [OK].

<From Web Connection>

✔ For the logon procedure, see **"Performing user authentication" on page 3-2**.

1 Log on to the user operation mode through User Authentication from the Web Connection.

2 Click the [Box] tab and the [Create User Box] menu.



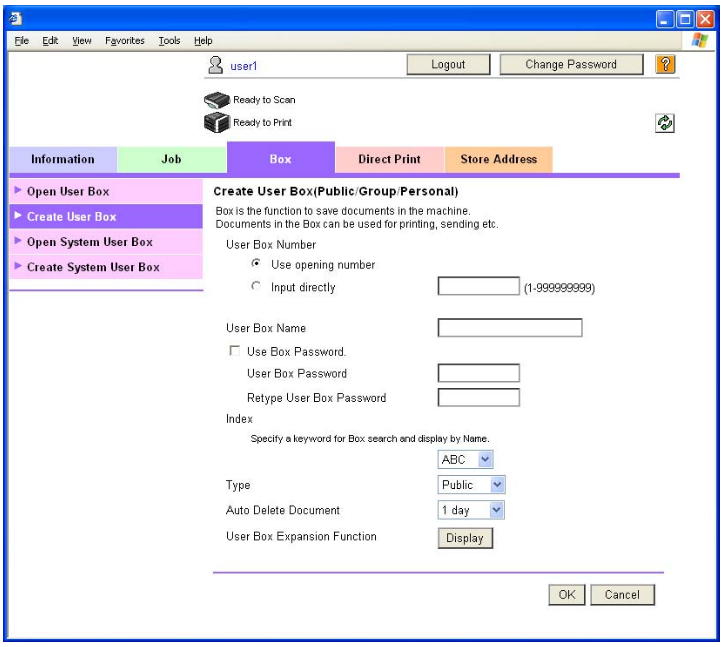
Device Information

Device Name
Device Location
Device Type Print/Copy/Scan/Fax

Paper Tray

Tray	Paper Size	Paper Type	Paper Status
Bypass	Unknown	Plain Paper	Empty
Tray 1	A4 SEF	Plain Paper	Ready
Tray 2	A4 LEF	Plain Paper	Near Empty

3 Make the necessary settings.



Create User Box(Public/Group/Personal)

Box is the function to save documents in the machine.
Documents in the Box can be used for printing, sending etc.

User Box Number
● Use opening number
○ Input directly (1-999999999)

User Box Name

□ Use Box Password.
User Box Password
Retype User Box Password

Index
Specify a keyword for Box search and display by Name.
ABC

Type: Public
Auto Delete Document: 1 day
User Box Expansion Function: Display

? Are there any precautions to be used when making settings?

→ Be sure to enter the User Box Number, User Box Name, User Box Password, and Retype User Box Password.

→ A User Box Number that has been registered cannot be registered anew.

→ If [Personal] is selected from the User Box Type pull-down menu, click [User List] and select the user from the registered user list, or enter the User Name of the owner of the User Box in the "Owner Name" box.

→ If [Group] is selected from the User Box Type pull-down menu, click [Account List] and select the user from the registered user list, or enter the Account Name of the owner of the User Box in the "Account Name" box.

4 Click the [OK].

? What happens if the User Box Password entered does not meet the requirements of the Password Rules?

➔ If the User Box Password entered does not meet the requirements of the Password Rules with [Public] selected for User Box Type, a message appears that tells that the User Box Password that has been entered cannot be used. Click [OK] to go back to the screen of step 3. Perform steps 3 through 4 once again. For details of the Password Rules, see **"Password Rules" on page 1-9**.

? What happens if there is a mismatch in the User Box Passwords?

➔ If there is a mismatch in the password between that entered in the "User Box Password" box and that entered in the "Retype User Box Password" box, a message appears that tells that there is a mismatch in the User Box Password. Enter the correct User Box Password.

? What if no Owner Name, or a wrong one, has been entered?

➔ If no Owner Name is entered, a message appears that tells that no Owner Names have been entered. Enter the correct Owner Name.

➔ If a user name not registered with the machine is entered in the "Owner Name" box, a message appears that tells that the Owner Name entered in the box is illegal. Click [OK] to go back to the screen of step 3. Perform steps 3 through 4 once again.

? What if no Account Name, or a wrong one, has been entered?

➔ If no Account Name is entered, a message appears that tells that no Account Names have been entered. Enter the correct Account Name.

➔ If a user name not registered with the machine is entered in the "Account Name" box, a message appears that tells that the Account Name entered in the box is illegal. Click [OK] to go back to the screen of step 3. Perform steps 3 through 4 once again.

? What steps should be performed to change the User Box setting?

➔ For the procedure to change the User Box setting, see **"Changing the User Box Password and user attributes and account attributes" on page 3-23**.

5 Check the message that tells that the setting has been completed. Then, click [OK].

3.4.2 Changing the User Box Password and user attributes and account attributes

✎...

Note

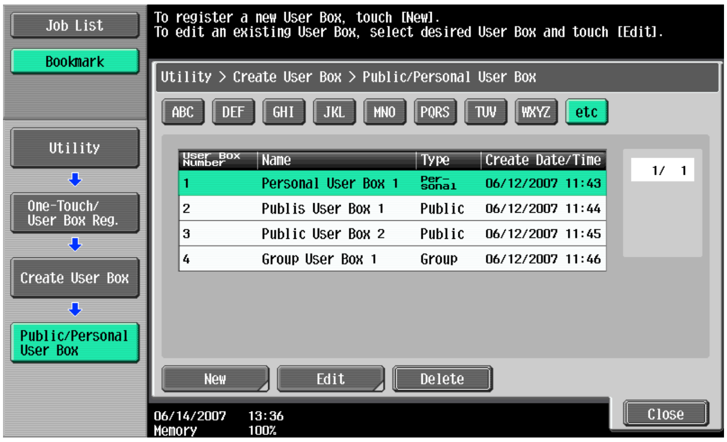
Do not leave the machine while you are in the user operation mode. If it is absolutely necessary to leave the machine, be sure first to log off from the user operation mode.

<From the Control Panel>

✔ For the procedure to call the User Box screen to the display, see steps 1 through 5 of **"Setting the User Box" on page 3-17**.

1 Call the User Box screen to the display from the control panel.

2 Select the target User Box and touch [Edit].



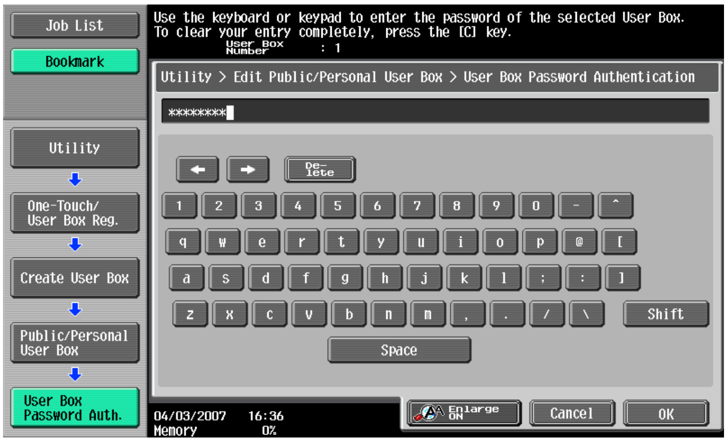
To register a new User Box, touch [New].
To edit an existing User Box, select desired User Box and touch [Edit].

Utility > Create User Box > Public/Personal User Box

User Box Number	Name	Type	Create Date/Time
1	Personal User Box 1	Per-sonal	06/12/2007 11:43
2	Publis User Box 1	Public	06/12/2007 11:44
3	Public User Box 2	Public	06/12/2007 11:45
4	Group User Box 1	Group	06/12/2007 11:46

06/14/2007 13:36
Memory 100%

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



Use the keyboard or keypad to enter the password of the selected User Box.
To clear your entry completely, press the [C] key.
User Box Number : 1

Utility > Edit Public/Personal User Box > User Box Password Authentication

****

04/03/2007 16:36
Memory 0%

- 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].

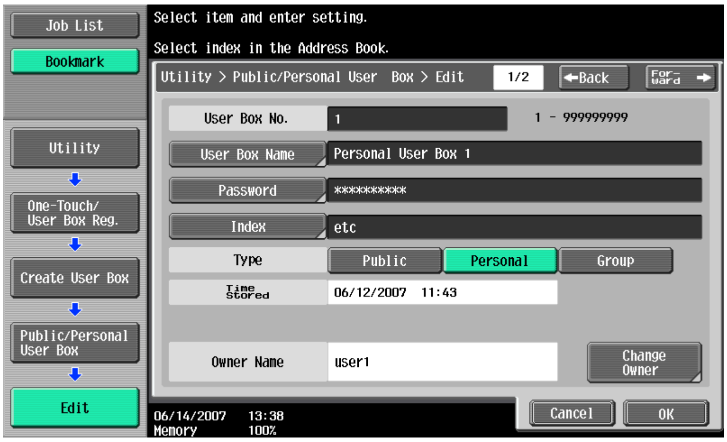
- If the User Box Type has been changed, go to step 5. If the User Box Password has been changed, go to step 9.
- To change the owner user or owner account, perform steps 6 to 8.

? What happens if there is a mismatch in the User Box Password?

➔ If there is a mismatch between the currently registered User Box Password and the User Box Password entered, a message appears that tells that there is a mismatch in the User Box Password and the screen of step 2 reappears. Perform steps 2 through 4 once again.

➔ If the Enhanced Security Mode is set to [ON], entry of a wrong User Box Password is counted as unauthorized access. If a wrong User Box Password is entered a predetermined number of times (once to three times) set by the Administrator of the machine, the screen of step 2 reappears and the machine is set into an access lock state. To cancel the access lock state, the Administrator of the machine must perform the Release Setting. Contact the Administrator of the machine.

5 Select the User Box Type.



Select item and enter setting.

Select index in the Address Book.

Utility > Public/Personal User Box > Edit 1/2

User Box No. 1 1 - 999999999

User Box Name Personal User Box 1

Password **********

Index etc

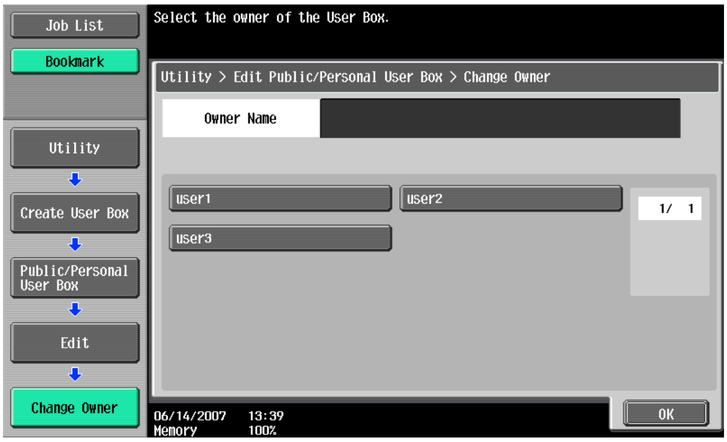
Type Public Personal Group

Time Stored 06/12/2007 11:43

Owner Name user1

06/14/2007 13:38 Memory 100%

– [Change Owner] appears if the Box Type has been changed to [Personal]. Select the desired user name of the owner.



Select the owner of the User Box.

Utility > Edit Public/Personal User Box > Change Owner

Owner Name

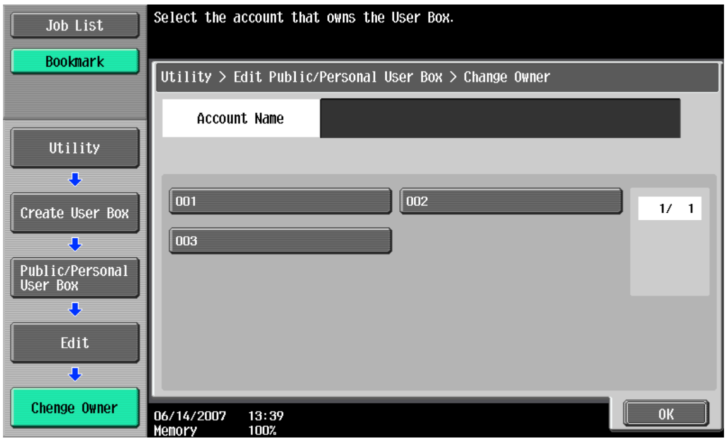
user1 user2

user3

1/ 1

06/14/2007 13:39 Memory 100%

– [Change Account Name] appears if the Box Type has been changed to [Group]. Select the desired account name of the owner.



Select the account that owns the User Box.

Utility > Edit Public/Personal User Box > Change Owner

Account Name

001 002

003

1/ 1

06/14/2007 13:39 Memory 100%

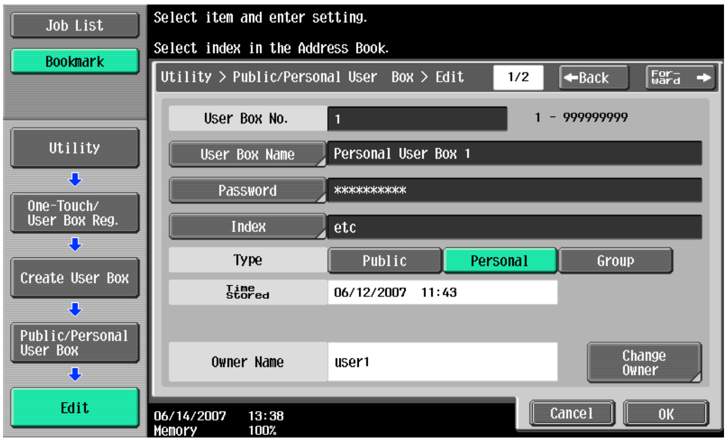
? What happens when the User Box Type is changed?

➔ Changing the User Box Type clears the User Box Password. Perform steps 9 through 15 to set the User Box Password.

? What happens if the User Box Password entered does not meet the requirements of the Password Rules when [Public] is set for the box type?

➔ If the User Box Password entered does not comply with the Password Rules with [Public] set for the box type, a message appears that tells that the User Box Password entered cannot be used. For details of the Password Rules, see "Password Rules" on page 1-9.

6 Touch [Change Owner] if the box type is [Personal] and touch [Change Account Name] if the box type is [Group].



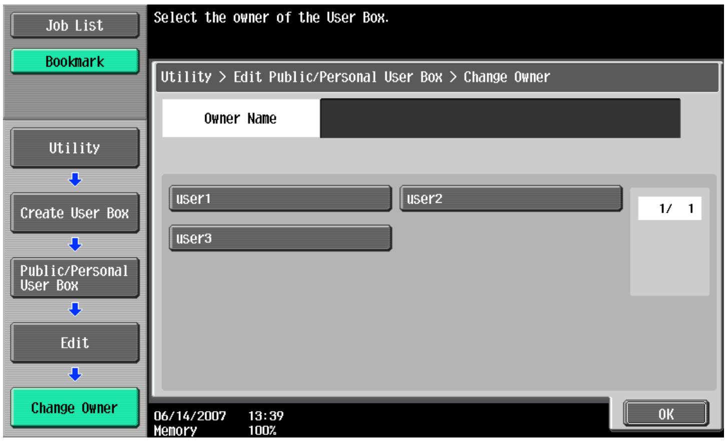
Select item and enter setting.

Select index in the Address Book.

Utility > Public/Personal User Box > Edit 1/2

User Box No.	1	1 - 999999999
User Box Name	Personal User Box 1	
Password	**********	
Index	etc	
Type	Public / Personal / Group	
Time Stored	06/12/2007 11:43	
Owner Name	user1	

7 For [Change Owner], select the desired user.



Select the owner of the User Box.

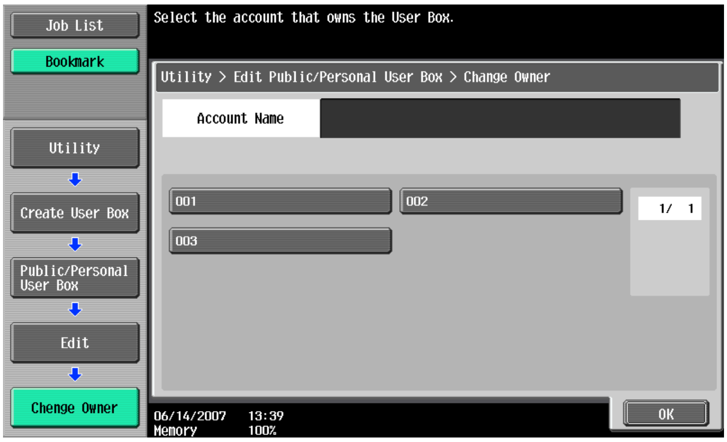
Utility > Edit Public/Personal User Box > Change Owner

Owner Name

user1 user2
user3

1/ 1

– For [Change Account Name], select the desired user.



Select the account that owns the User Box.

Utility > Edit Public/Personal User Box > Change Owner

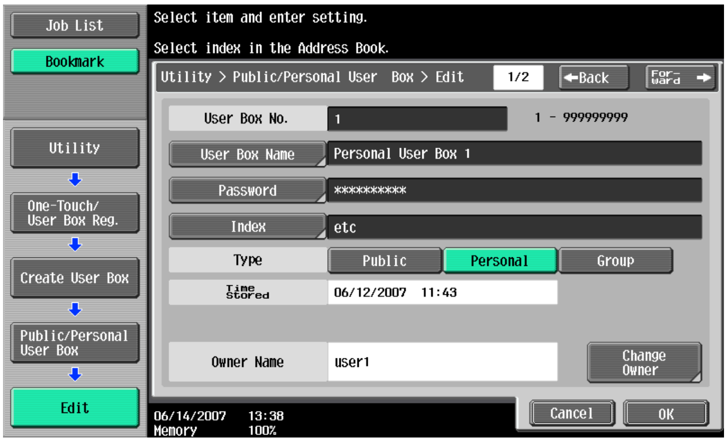
Account Name

001 002
003

1/ 1

8 Touch [OK].

9 Touch [Password].



Select item and enter setting.
Select index in the Address Book.

Utility > Public/Personal User Box > Edit 1/2

User Box No. 1 1 - 999999999

User Box Name: Personal User Box 1

Password: **********

Index: etc

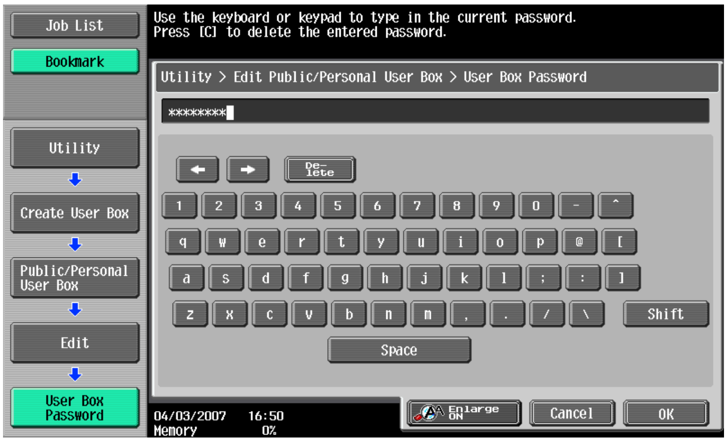
Type: Public / Personal / Group

Time Stored: 06/12/2007 11:43

Owner Name: user1

06/14/2007 13:38
Memory 100%

10 Enter the currently set 8-digit User Box Password from the keyboard or keypad.



Use the keyboard or keypad to type in the current password.
Press [C] to delete the entered password.

Utility > Edit Public/Personal User Box > User Box Password

****

04/03/2007 16:50
Memory 0%

- 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 9.

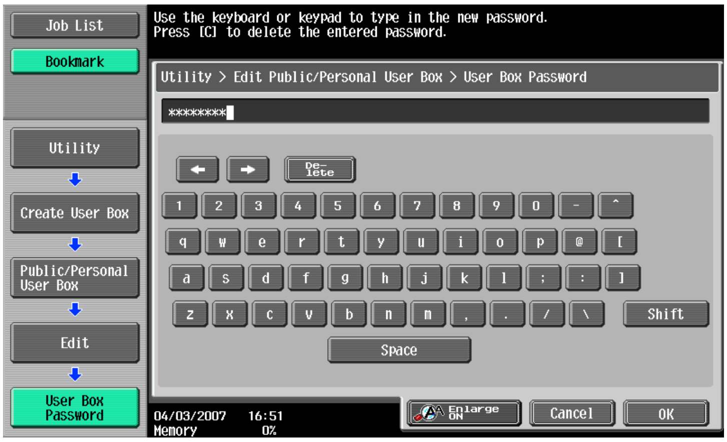
11 Touch [OK].

? What happens if the User Box Password entered does not meet the requirements of the Password Rules?

➔ If the User Box Password entered does not match the current password, a message appears that tells that the User Box Password entered is wrong. Enter the correct User Box Password.

➔ If the Enhanced Security Mode is set to [ON], entry of a wrong User Box Password is counted as unauthorized access. If a wrong User Box Password is entered a predetermined number of times (once to three times) set by the Administrator of the machine, the screen of step 2 reappears and the machine is set into an access lock state. To cancel the access lock state, the Administrator of the machine must perform the Release Setting. Contact the Administrator of the machine.

12 Enter the new 8-digit User Box Password from the keyboard and keypad.



Use the keyboard or keypad to type in the new password.
Press [C] to delete the entered password.

Utility > Edit Public/Personal User Box > User Box Password

****

04/03/2007 16:51
Memory 0%

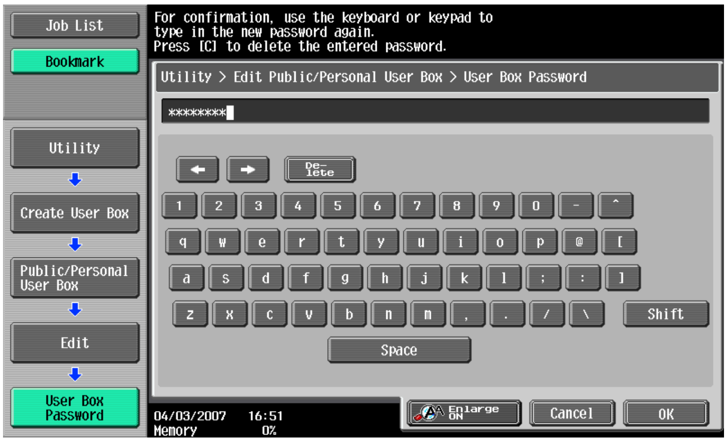
- Press the [C] key to clear all characters.
- Touch [Delete] to delete the last character entered.
- Touch [Shift] to show the upper case/symbol screen.
- Touch [Cancel] to go back to the screen shown in step 9.

13 Touch [OK].

? What precautions should be used when User Box Type is set to Public?

➔ If the User Box Password entered does not meet the requirements of the Password Rules with [Public] set for User Box Type, a message appears that tells that the User Box Password entered cannot be used. Enter the correct User Box Password. For details of the Password Rules, see **"Password Rules" on page 1-9**.

14 To prevent entry of a wrong password, enter the 8-digit User Box Password again.



For confirmation, use the keyboard or keypad to type in the new password again.
Press [C] to delete the entered password.

Utility > Edit Public/Personal User Box > User Box Password

****

04/03/2007 16:51
Memory 0%

- 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 9.

15 Touch [OK].

? What happens if there is a mismatch in the User Box Passwords?

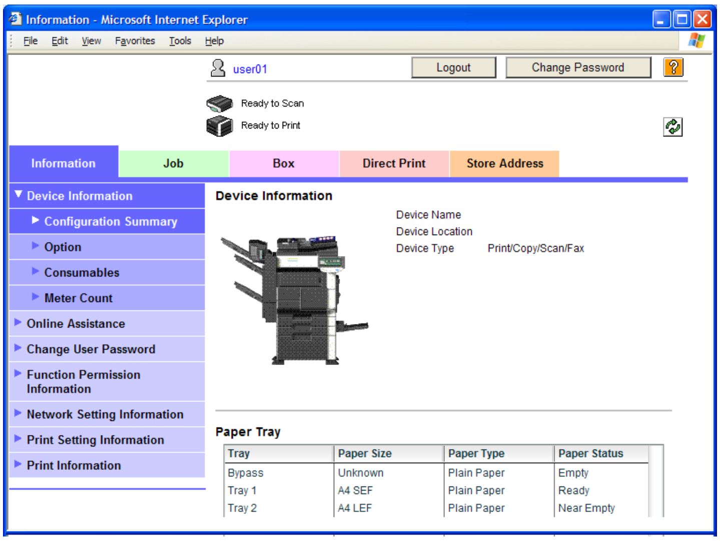
➔ If there is a mismatch in the User Box Passwords, a message appears that tells that there is a mismatch in the User Box Passwords. Perform steps 12 through 15 once again.

<From Web Connection>

✔ For the logon procedure, see "Performing user authentication" on page 3-2.

1 Log on to the user operation mode through User Authentication from the Web Connection.

2 Click the [Box] tab and the [Open User Box] menu.



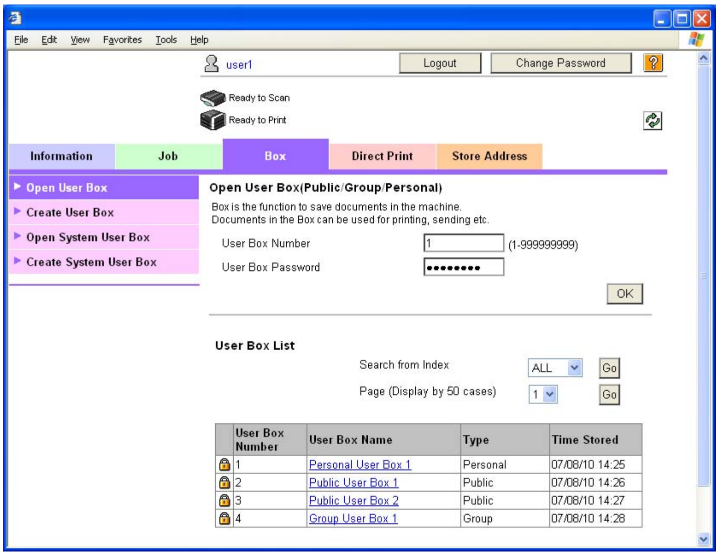
Device Information

Device Name
Device Location
Device Type Print/Copy/Scan/Fax

Paper Tray

Tray	Paper Size	Paper Type	Paper Status
Bypass	Unknown	Plain Paper	Empty
Tray 1	A4 SEF	Plain Paper	Ready
Tray 2	A4 LEF	Plain Paper	Near Empty

3 Enter the User Box Number and User Box Password of the target User Box and click [OK].



Open User Box(Public/Group/Personal)

Box is the function to save documents in the machine.
Documents in the Box can be used for printing, sending etc.

User Box Number 1 (1-999999999)

User Box Password ••••••••

User Box List

Search from Index ALL

Page (Display by 50 cases) 1

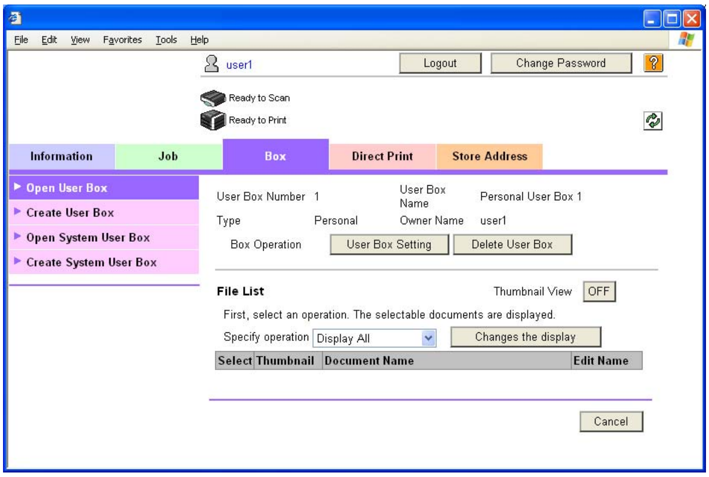
	User Box Number	User Box Name	Type	Time Stored
🔒	1	Personal User Box 1	Personal	07/08/10 14:25
🔒	2	Public User Box 1	Public	07/08/10 14:26
🔒	3	Public User Box 2	Public	07/08/10 14:27
🔒	4	Group User Box 1	Group	07/08/10 14:28

? What if there is a mismatch between the User Box Number and User Box Password?

→ If there is a mismatch between the User Box Number and User Box Password, a message appears that tells that authentication has not been successful. Click [OK] and perform step 3 once again.

→ If the Enhanced Security Mode is set to [ON], entry of a wrong User Box Password is counted as unauthorized access. If a wrong User Box Password is entered a predetermined number of times (once to three times) set by the Administrator of the machine, a message appears that tells that authentication has not been successful for any subsequent operation for authentication. The machine is then set into an access lock state. To cancel the access lock state, the Administrator of the machine must perform the Release Setting. Contact the Administrator of the machine.

4 Click the [User Box Setting].



User Box Number 1 User Box Name Personal User Box 1

Type Personal Owner Name user1

Box Operation

File List Thumbnail View OFF

First, select an operation. The selectable documents are displayed.

Specify operation Display All

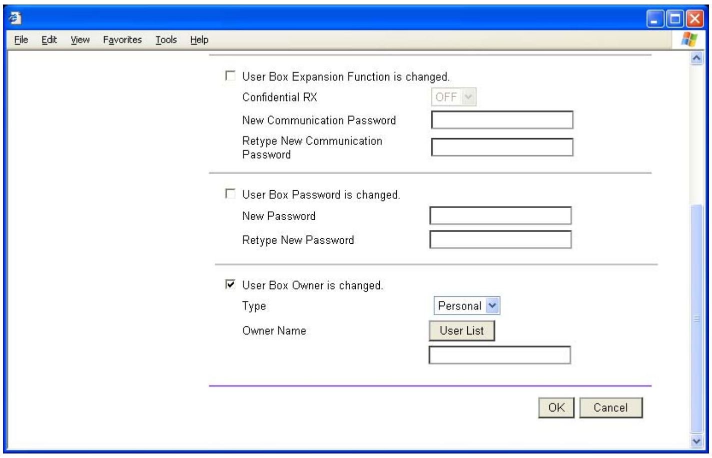
Select	Thumbnail	Document Name	Edit Name

- Go to step 5 if the selected User Box Type is [Personal] or [Group], and go to step 6 if the selected User Box Type is [Public].

? What steps should be performed to delete a User Box?

→ To delete a User Box, click [Delete User Box]. A message will then appear for confirming whether the specific User Box can definitely be deleted. Click [OK] to delete the specified User Box.

5 Click the "User Box Owner is changed." check box and change the user attributes of the box.

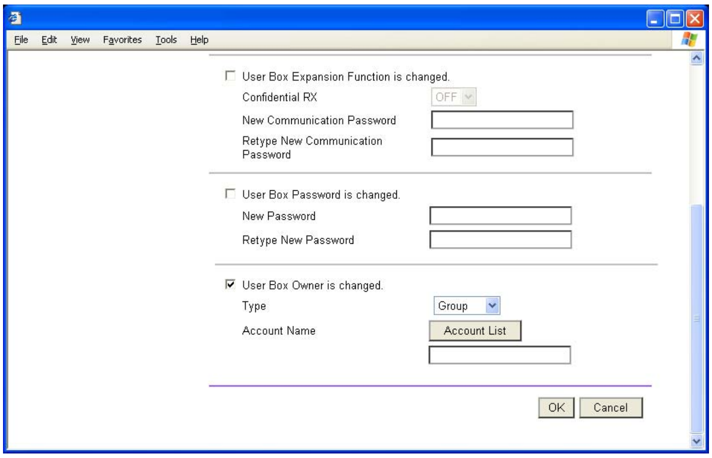


□ User Box Expansion Function is changed.
Confidential RX OFF
New Communication Password
Retype New Communication Password

□ User Box Password is changed.
New Password
Retype New Password

☑ User Box Owner is changed.
Type Personal
Owner Name

- Click [User List] to select a specific user from the registered User List.
- A user name may be directly entered in the Owner Name box.
- The following screen appears if the account attributes are to be changed.



□ User Box Expansion Function is changed.
Confidential RX OFF
New Communication Password
Retype New Communication Password

□ User Box Password is changed.
New Password
Retype New Password

☑ User Box Owner is changed.
Type Group
Account Name

- Click [Account List] to select a specific user from the registered User List.
- An account name may be directly entered in the Account Name box.

? What happens if User Box Owner is changed. is clicked?

→ If the "User Box Owner is changed." check box is clicked, it clears the User Box Password. Be sure to set the User Box Password again.

→ If the "User Box Owner is changed." check box is not clicked, the changes made will not be validated. If the changes need to be made, make sure that the "User Box Owner is changed." check box has been clicked.

? What steps can be taken to change the User Box Type?

→ To change the User Box Type, click the User Box Type pull-down menu and select the desired User Box Type.

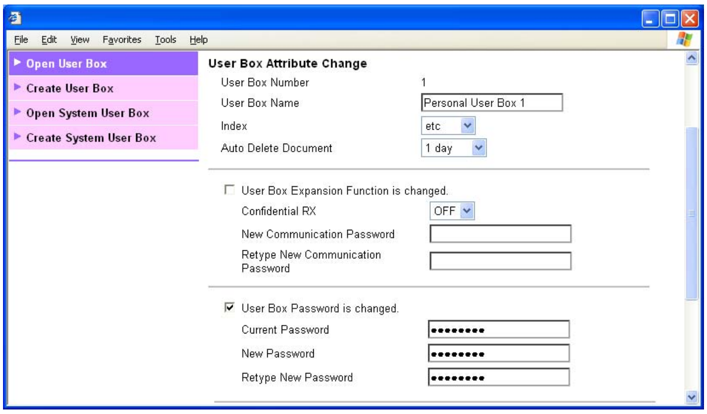
? What precautions should be used when entering the Owner Name?

→ Enter the User Name that has been registered through User Registration for the Owner Name.

? What precautions should be used when entering the Account Name?

→ Enter the Account Name that has been registered through Account Track Registration for the Account Name.

6 Click the "User Box Password is changed." check box and enter the User Box Password.



User Box Attribute Change

User Box Number 1

User Box Name Personal User Box 1

Index etc

Auto Delete Document 1 day

□ User Box Expansion Function is changed.

Confidential RX OFF

New Communication Password

Retype New Communication Password

☑ User Box Password is changed.

Current Password ●●●●●●●●

New Password ●●●●●●●●

Retype New Password ●●●●●●●●

? What precautions should be used when entering the User Box Password?

→ In the "Current Password" box, enter the currently set User Box Password.

→ If the User Box Type has been set to [Public], enter a User Box Password that meets the requirements of the Password Rules in the "New Password" box. For details of the Password Rules, see **"Password Rules" on page 1-9**.

→ Enter the same User Box Password as that entered in the "New Password" box in the "Retype New Password" box.

7 Click the [OK].

? What if there is a mismatch in the Current User Box Passwords?

→ If there is a mismatch in the Current User Box Passwords, a message appears that tells that there is a mismatch in the Current User Box Passwords. Click [OK] to go back to the screen of step 3. Perform steps 3 through 7 once again.

? What happens if the New User Box Password entered does not meet the requirements of the Password Rules with [Public] selected for the box type?

→ If the User Box Password entered in the "New Password" box does not meet the requirements of the Password Rules with [Public] selected for the box type, a message appears that tells that the User Box Password that has been entered cannot be used. Click [OK] to go back to the screen of step 3. Perform steps 3 through 7 once again. For details of the Password Rules, see **"Password Rules" on page 1-9**.

? What happens if there is a mismatch in the New User Box Password and the Retype New User Box Password?

→ If there is a mismatch in the password between that entered in the "New Password" box and that entered in the "Retype New Password" box, a message appears that tells that there is a mismatch in the User Box Password. Enter the correct User Box Password.

? What if no Owner Name, or a wrong one, has been entered?

➔ If no Owner Name is entered, a message appears that tells that no Owner Names have been entered. Enter the correct Owner Name.

➔ If a user name not registered with the machine is entered in the "Owner Name" box, a message appears that tells that the Owner Name entered in the box is illegal. Click [OK] to go back to the screen of step 3. Perform steps 3 through 7 once again.

? What if no Account Name, or a wrong one, has been entered?

➔ If no Account Name is entered, a message appears that tells that no Account Names have been entered. Enter the correct Account Name.

➔ If a account name not registered with the machine is entered in the "Account Name" box, a message appears that tells that the Account Name entered in the box is illegal. Click [OK] to go back to the screen of step 3. Perform steps 3 through 7 once again.

8 Click the [OK].

3.4.3 Accessing the User Box and User Box file

<For control panel>

Operation Menu Type	Functions that can be Performed
Save Document	Read new document
Use Document	Print, Send (fax, e-mail, file)
File Document	Delete, Move, Copy, and Edit Name for files

Different functions can be performed on different types of files stored in the User Boxes.
See the table given below for the relation between the file type and functions that can be performed.

<For Web Connection>

File Type	Functions that can be Performed
Copy job files	Print, Move/Copy, Delete
Print job files	Print, Move/Copy, Delete
Scan job files	Print, Move/Copy, Delete, Send to other device, Download to PC
Fax job files	Print, Move/Copy, Delete, Send to other device, Download to PC

✎...

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.

✎...

Reminder

If the destination is to be specified using the corresponding one-touch key for executing [Fax] or [Fax TX] from the control panel, always check that the destination is correct to make sure that the data is sent to the correct destination.

If the destination is to be specified through direct input for executing [Fax] or [Fax TX] from the control panel, always check that the destination is correct to make sure that the data is sent to the correct destination.

<From the Control Panel>

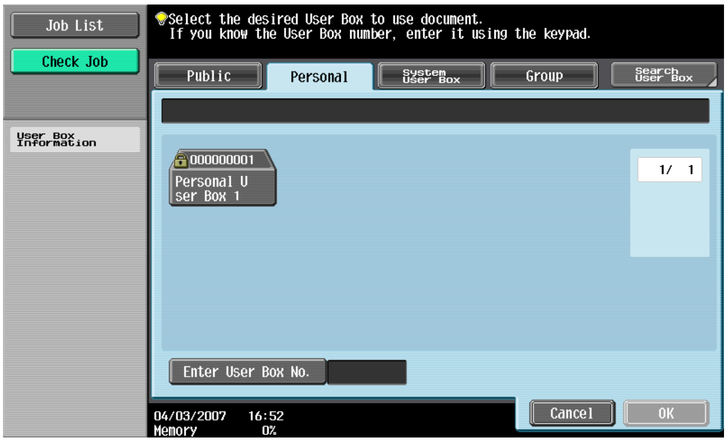
✔ For the logon procedure, see **"Performing user authentication" on page 3-2**.

1 Log on to the user operation mode through User Authentication from the control panel.

2 Press the [Box] key.

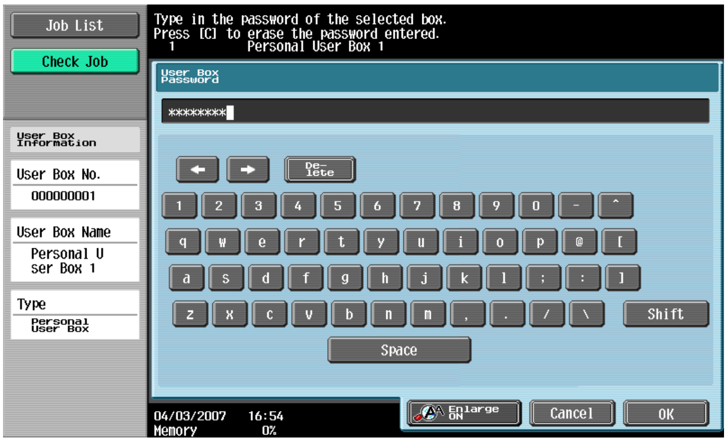
3 Select the operation menu.

4 Select the any arbitrary User Box and touch [OK].



Select the desired User Box to use document.
If you know the User Box number, enter it using the keypad.

5 Enter the 8-digit User Box Password from the keyboard and keypad.



Type in the password of the selected box.
Press [C] to erase the password entered.
1 Personal User Box 1

User Box Password: ********

User Box No.: 000000001

User Box Name: Personal User Box 1

Type: Personal User Box

– 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 4.

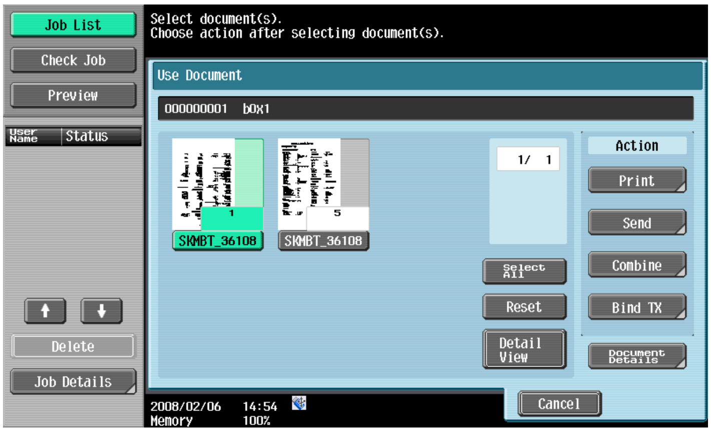
6 Touch [OK].

? What if there is a mismatch in the User Box Passwords?

→ If there is a mismatch in the User Box Passwords, a message appears that tells that authentication has not been successful. The machine then prohibits entry of the User Box Password for 5 sec. Enter the correct User Box Password.

→ If the Enhanced Security Mode is set to [ON], entry of a wrong User Box Password is counted as unauthorized access. If a wrong User Box Password is entered a predetermined number of times (once to three times) set by the Administrator of the machine or more, a message appears that tells that authentication has not been successful for any subsequent operation for authentication. The machine is then set into an access lock state, rejecting any more logon attempts. To cancel the access lock state, the Administrator of the machine must perform the Release Setting. Contact the Administrator of the machine.

7 Select any arbitrary file.



Select document(s).
Choose action after selecting document(s).

Use Document

000000001 b0x1

8 Select the desired function from Print setting, Bind setting, TX setting and binding TX.

- Selecting [Delete] will delete the specified file.

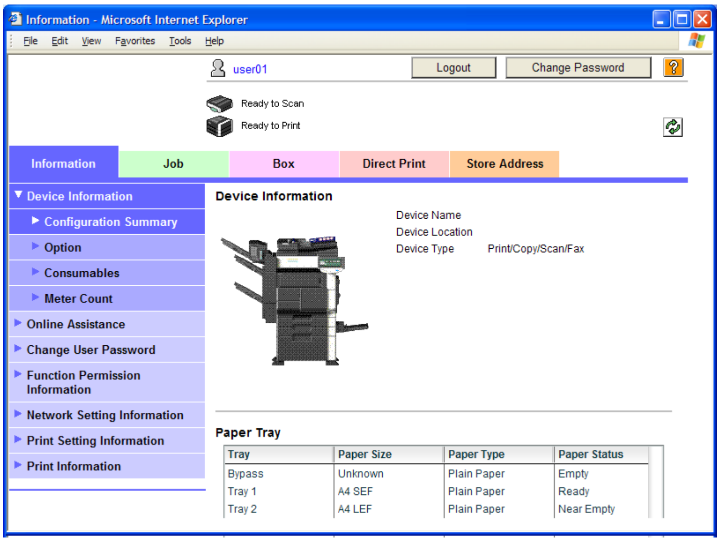
9 Press the [Start] key or touch [Start].

<From Web Connection>

✔ For the logon procedure, see "Performing user authentication" on page 3-2.

1 Log on to the user operation mode through User Authentication from the Web Connection.

2 Click the [Box] tab and the [Open User Box] menu.



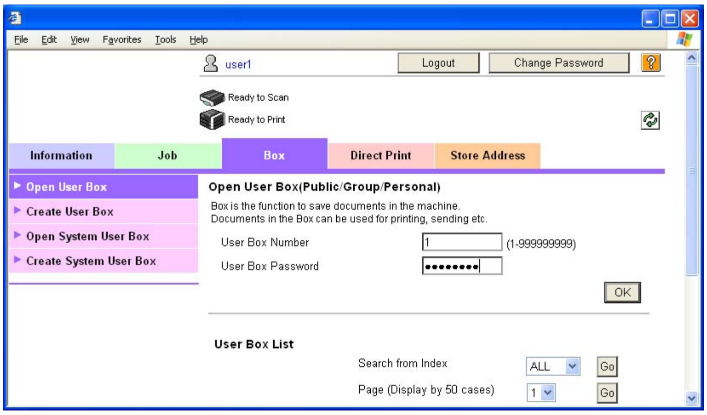
Device Information

Device Name
Device Location
Device Type Print/Copy/Scan/Fax

Paper Tray

Tray	Paper Size	Paper Type	Paper Status
Bypass	Unknown	Plain Paper	Empty
Tray 1	A4 SEF	Plain Paper	Ready
Tray 2	A4 LEF	Plain Paper	Near Empty

3 Enter the User Box Number and User Box Password of the target User Box and click [OK].



Open User Box(Public/Group/Personal)

Box is the function to save documents in the machine.
Documents in the Box can be used for printing, sending etc.

User Box Number 1 (1-999999999)

User Box Password ••••••••

User Box List

Search from Index ALL

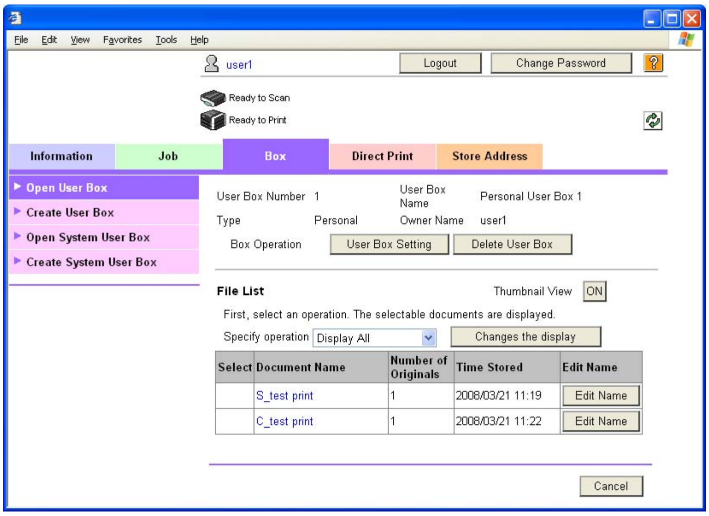
Page (Display by 50 cases) 1

? What if there is a mismatch between the User Box Number and the User Box Password?

→ If there is a mismatch between the User Box Number and the User Box Password, a message appears that tells that authentication has not been successful. Click [OK] and perform step 3 once again.

→ If the Enhanced Security Mode is set to [ON], entry of a wrong User Box Password is counted as unauthorized access. If a wrong User Box Password is entered a predetermined number of times (once to three times) set by the Administrator of the machine or more, a message appears that tells that authentication has not been successful for any subsequent operation for authentication. The machine is then set into an access lock state, rejecting any more logon attempts. To cancel the access lock state, the Administrator of the machine must perform the Release Setting. Contact the Administrator of the machine.

4 Select the desired operation from the pull-down menu and click [Changes the display].



User Box Number 1 User Box Name Personal User Box 1

Type Personal Owner Name user1

Box Operation

File List Thumbnail View ON

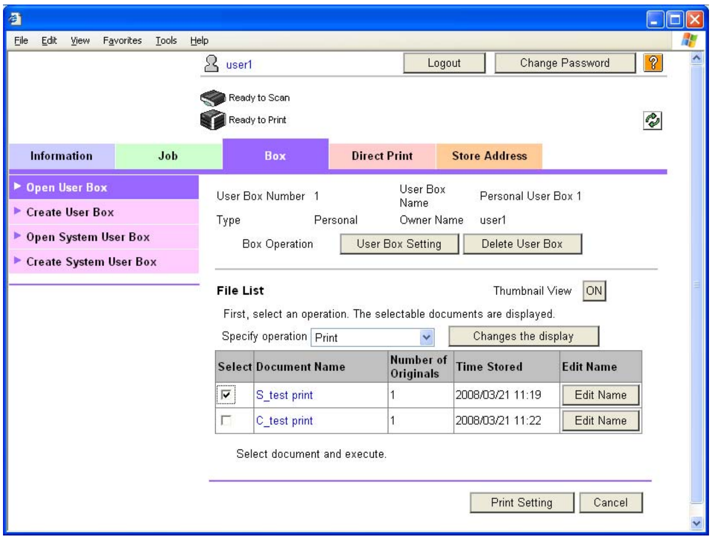
First, select an operation. The selectable documents are displayed.

Specify operation Display All

Select	Document Name	Number of Originals	Time Stored	Edit Name
	S_test print	1	2008/03/21 11:19	Edit Name
	C_test print	1	2008/03/21 11:22	Edit Name

– Selecting the [Delete] in step 4 will cause a message to appear that confirms whether the specified file can be deleted or not. Click [OK] to delete the specified file.

5 Select the document and perform the intended function.



User Box Number 1 User Box Name Personal User Box 1

Type Personal Owner Name user1

Box Operation

File List Thumbnail View ON

First, select an operation. The selectable documents are displayed.

Specify operation Print

Select	Document Name	Number of Originals	Time Stored	Edit Name
☑	S_test print	1	2008/03/21 11:19	Edit Name
☐	C_test print	1	2008/03/21 11:22	Edit Name

Select document and execute.

3.4.4 Sending S/MIME box files

✎...

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.

To select [E-Mail Encryption], the Administrator of the machine must make the S/MIME settings in advance.

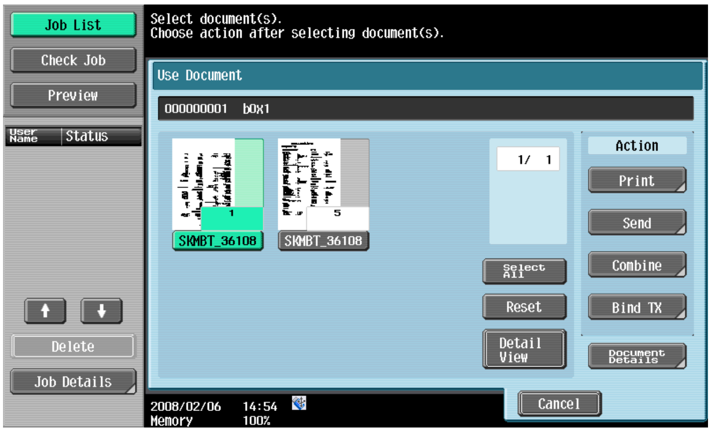
To select the destination, the Administrator of the machine must register the certificate with the destination in advance.

<From the Control Panel>

✔ For the procedure to call the Use Document screen to the display, see steps 1 through 6 of **"Accessing the User Box and User Box file" on page 3-32**.

1 Call the Use Document screen to the display from the control panel.

2 Select the file to be sent and click [Send].

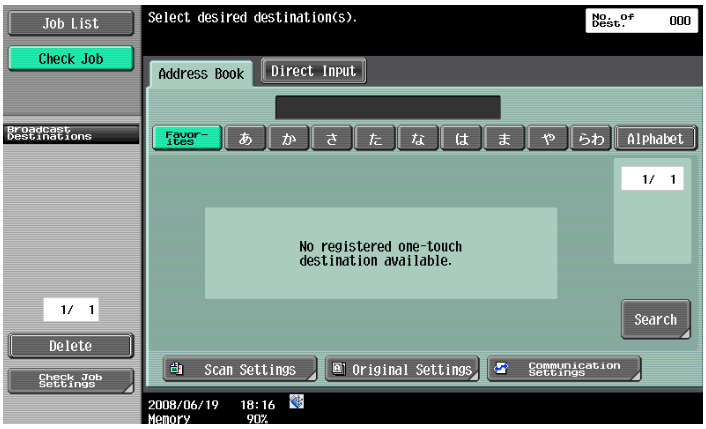


Select document(s).
Choose action after selecting document(s).

Use Document

000000001 box1

3 Select [Communication Settings].

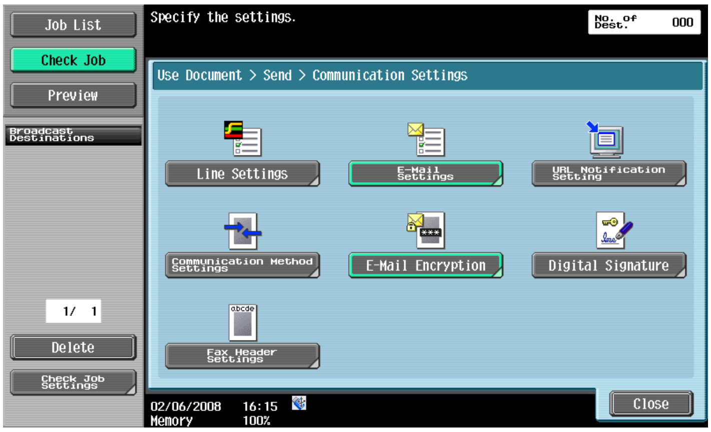


Select desired destination(s).

No. of Dest. 000

No registered one-touch destination available.

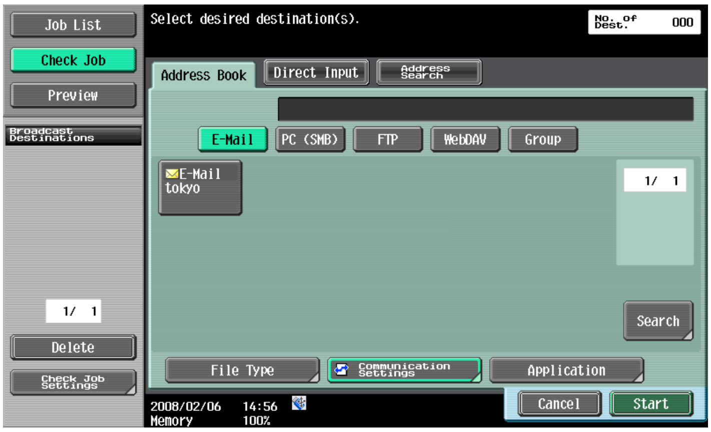
4 Select [E-Mail Encryption] and touch [Close].



? What happens if [E-Mail Encryption] is selected after the destination has been set?

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

5 Select the destination and touch [Start] or press the Start key.



3.5 Outline of document save

What Document save can do

When the data is saved at box mode, it directly specifies the box that the document will be saved. The document to be saved is regarded same as the scan save.

<Public User Box/Personal User Box/Group User Box>

- Printed or scanned documents using this machine are saved.
- It can save the document whose printing is instructed through a computer under the network.
- Personal User Box or Group User Box are available to limit the people who can use the box according to the status of user authentication or group administration.

<Annotation User Box>

- When you want to add the image of date/time and filing number to the saved data for printing or sending, you save the data to this Annotation User Box. Press [System User Box] tab and then [Annotation User Box] to select the box.

<External Memory>

- Scanned data can be directly stored to the external memory that is connected to the external memory machine. Confirm that the external memory is set to the USB connector of this machine, and press [External Memory] of [System User Box] tab.

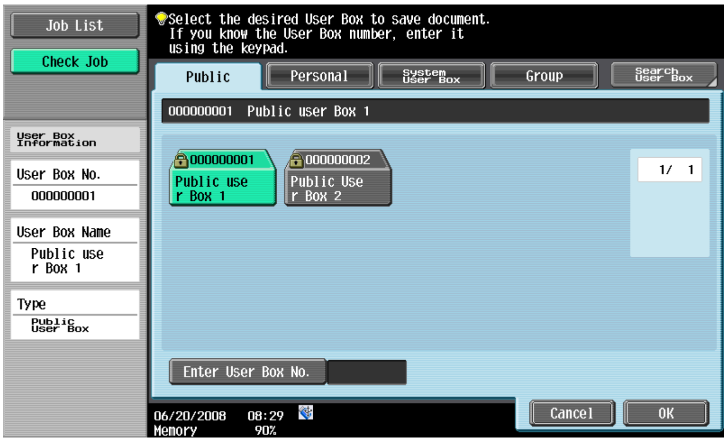
Detail

Document save to external memory is set OFF at factory setting (cannot be saved). It is set OFF also when User authentication is set. When you want to utilize this function, change the setting accordingly at Administrator Set.

Initial screen of Document save

<Public user box/Personal user box/Group use box>

- When you select [Public]/[Personal]/[Group] tab, list of boxes the data can be stored will appear. Select the desired box.



Select the desired User Box to save document.
If you know the User Box number, enter it
using the keypad.

000000001 Public user Box 1

User Box Information

User Box No.
000000001

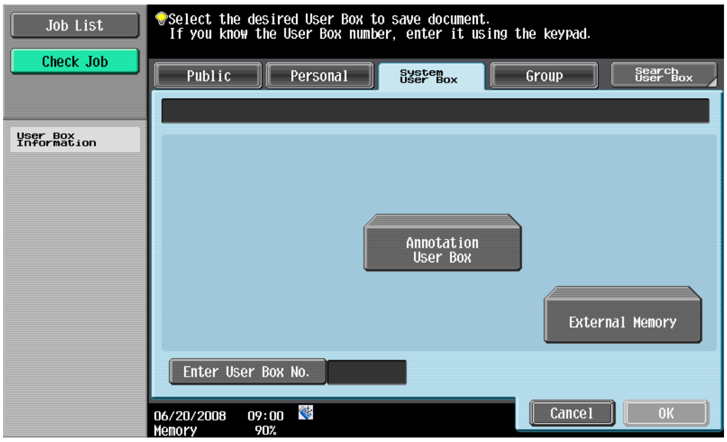
User Box Name
Public use
r Box 1

Type
Public
User Box

06/20/2008 08:29
Memory 90%

<System Box>

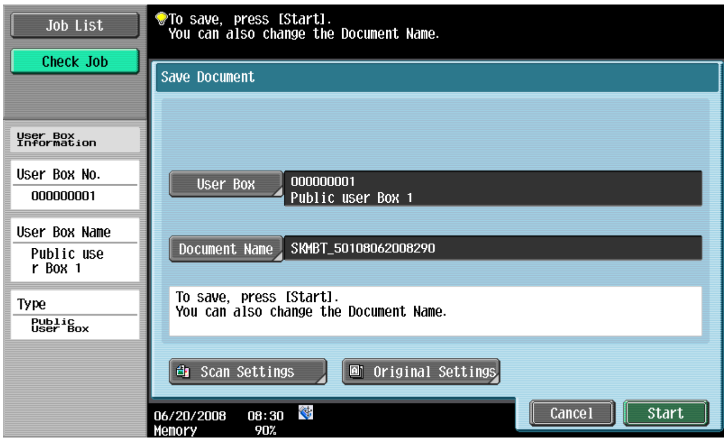
- When [System User Box] tab is selected, list of boxes the data can be stored will appear. Select the desired box.
  When you select [Annotation User Box], more specific box can be selected.



Select the desired User Box to save document.
If you know the User Box number, enter it using the keypad.

06/20/2008 09:00
Memory 90%

Document save screen



To save, press [Start].
You can also change the Document Name.

Save Document

User Box No.: 000000001

User Box Name: Public user Box 1

Type: Public User Box

User Box: 000000001 Public user Box 1

Document Name: SKMBT_50108062008290

To save, press [Start].
You can also change the Document Name.

06/20/2008 08:30
Memory 90%

Item	Explanation
User Box	Public User Box/Personal User Box/Group Use Box and Annotation User Box, the save box can be changed. Press [Save box] to select the desired box.
Document Name	Keyboard to enter the document name is displayed. Enter the name on the panel.
Scan Settings	Details of scan reading conditions can be set.
Original Settings	Details such as original paper type or setting direction can be set.

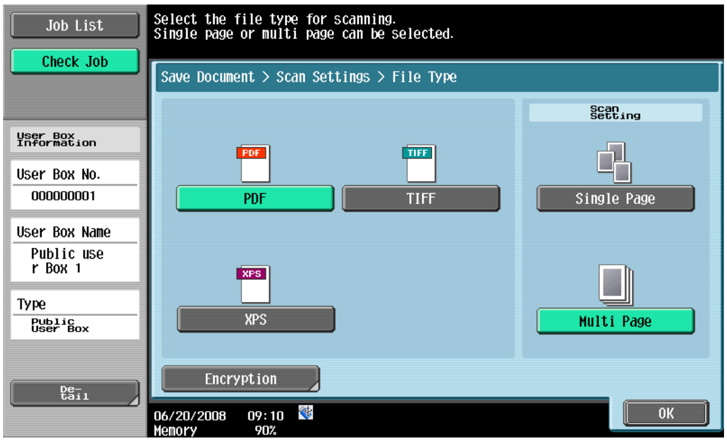
✎...

Note

In case the external memory is used, the place the document is save cannot be changed.

File style

To select the file style to save the scanned data.



Select the file type for scanning.
Single page or multi page can be selected.

Save Document > Scan Settings > File Type

User Box Information
User Box No.
000000001
User Box Name
Public user Box 1
Type
Public User Box

06/20/2008 09:10
Memory 90%

<File style>

- The selectable file style is as follows

Item	Explanation
PDF	Save as PDF
TIFF	Save as TIFF
XPS	Save as XPS

Reminder
Even if the file style has already been selected at box save, you need to specify the file style when downloading data.

When the data is stored at XPS, the optional hard disk is necessary

<Setting page>

- Data can be specified in bulk at save.

Item	Explanation
Single Page	File is created by saving the data per page at download.
Multi Page	File is created by saving whole scanned data.

Reminder
Even if the [Single Page] is selected at box save, you need to specify the page when downloading data.

4 Application Software

4 Application Software

4.1 Data Administrator

Data Administrator is an application for management purpose that allows the authentication, destination and network functions of the machine to be edited or registered from a PC connected over the network.

It allows the authentication, destination and network setting list to be downloaded in your PC, the data in the list to be edited on the PC, and then the data to be written in the machine.

A destination list of file formats including XML, CSV, TAB, LDIF, and Lotus Notes Structured Text can be downloaded. A destination list can also be downloaded by searching through or browsing destinations using the LDAP protocol for a directory server such as Active Directory.

Select [Authentication Settings/Address Settings] to edit or register the authentication or destination function of the machine, and select [Administrator settings] to edit or register the network function of 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.

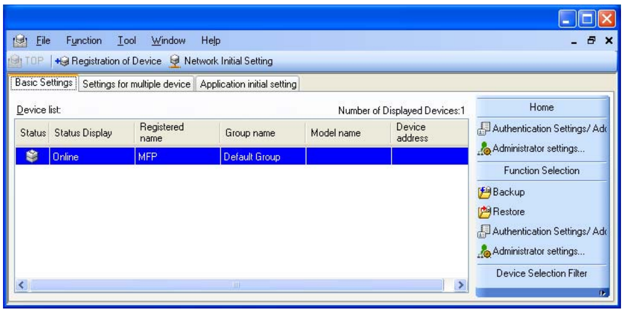
Do not leave the site while you are gaining access to the machine through Data Administrator. If it is absolutely necessary to leave the site, be sure first to log off from the Data Administrator.

4.1.1 Gaining access from Data Administrator

<From the PC>

1 Start the Data Administrator.

2 Select this machine from Device List and click [Authentication Settings/Address Settings] or [Administrator settings].


File
Function
Tool
Window
Help
TOP
Registration of Device
Network Initial Setting
Basic Settings
Settings for multiple device
Application initial setting
Home
Authentication Settings/ Adc
Administrator settings...
Function Selection
Backup
Restore
Authentication Settings/ Adc
Administrator settings...
Device Selection Filter

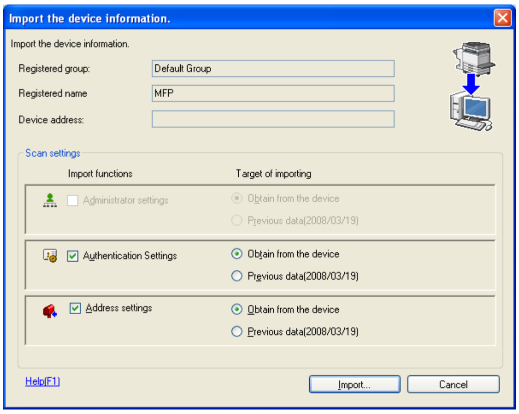
Device list:

Number of Displayed Devices:1

Status	Status Display	Registered name	Group name	Model name	Device address
	Online	MFP	Default Group		

3 Check the settings on the "Import device information" screen and click [Import].

- The following screen appears if [Authentication Settings/Address Settings] has been selected in step 2.



Import the device information.

Import the device information.

Registered group: Default Group

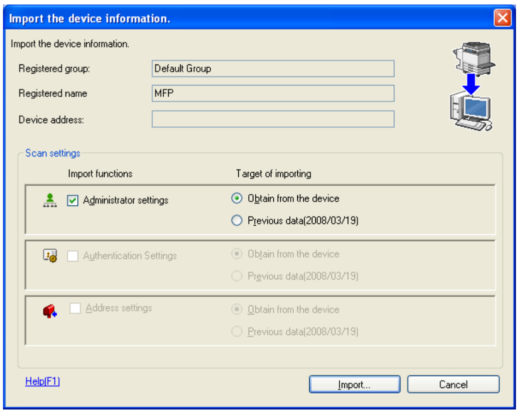
Registered name: MFP

Device address:

Scan settings

Import functions	Target of importing
□ Administrator settings	● Obtain from the device ○ Previous data(2008/03/19)
☑ Authentication Settings	● Obtain from the device ○ Previous data(2008/03/19)
☑ Address settings	● Obtain from the device ○ Previous data(2008/03/19)

- The following screen appears if [Administrator settings] has been selected in step 2.



Import the device information.

Import the device information.

Registered group: Default Group

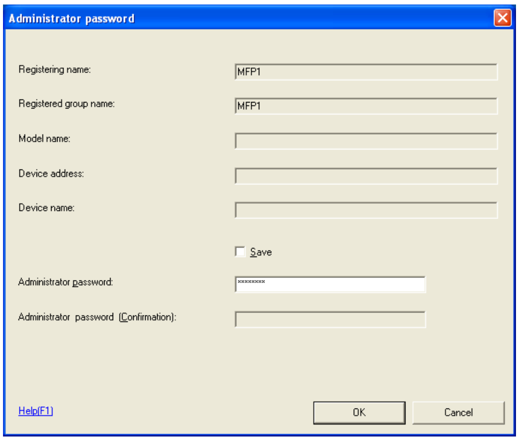
Registered name: MFP

Device address:

Scan settings

Import functions	Target of importing
☑ Administrator settings	● Obtain from the device ○ Previous data(2008/03/19)
□ Authentication Settings	● Obtain from the device ○ Previous data(2008/03/19)
□ Address settings	● Obtain from the device ○ Previous data(2008/03/19)

4 Type the 8-digit Administrator Password registered in the machine and click [OK].



Administrator password

Registering name: MFP1

Registered group name: MFP1

Model name:

Device address:

Device name:

□ Save

Administrator password: ********

Administrator password (Confirmation):

- If the "Save" check box is selected, enter the 8-digit Administrator Password once again to make sure that the Administrator Password has been entered correctly.

? 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 passwords and entry of the Administrator Password will be prohibited for five sec. Wait for some while before entering the correct Administrator Password.

➔ If a wrong Administrator Password is entered for confirmation, a message appears that tells that there is a mismatch in the Administrator Password. 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) 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 Check the data displayed on the SSL certificate check screen and click [Yes].

✎...

Reminder
If the "Save" check box has been selected, the Administrator Password entered is stored in the PC being used. If you do not want the Administrator Password stored, clear the "Save" check box.

4.1.2 Setting the user authentication method

✎...

Reminder

To change the user authentication method from "Device authentication" to "Network server authentication," it is necessary first to register the domain name of Active Directory on the machine side.

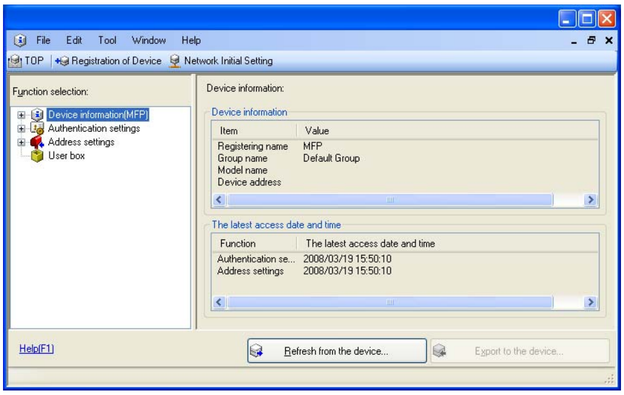
If "Network server authentication" is selected, "Active Directory" must invariably be selected.

<From the PC>

✔ For the procedure to access the machine, see steps 1 through 5 of **"Gaining access from Data Administrator" on page 4-2**.

1 Access the machine through [Authentication Settings/Address Settings] mode of Data Administrator.

2 Click the [Authentication settings].



Device information:

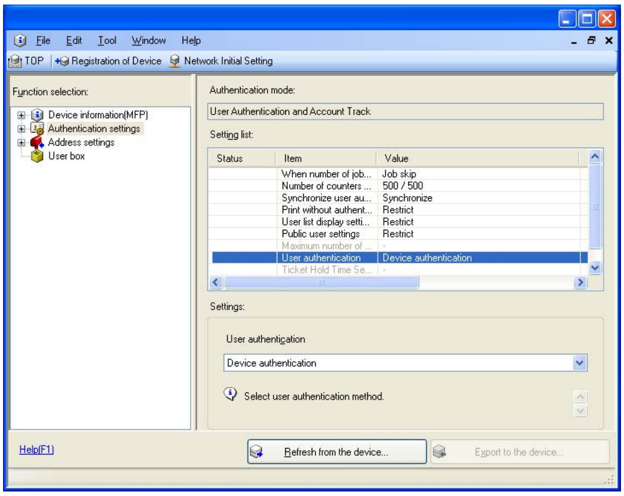
Device information

Item	Value
Registering name	MFP
Group name	Default Group
Model name	
Device address	

The latest access date and time

Function	The latest access date and time
Authentication se...	2008/03/19 15:50:10
Address settings	2008/03/19 15:50:10

3 Click the [User authentication].



Authentication mode:

User Authentication and Account Track

Setting list:

Status	Item	Value
	When number of job...	Job skip
	Number of counters ...	500 / 500
	Synchronize user au...	Synchronize
	Print without authent...	Restrict
	User list display setti...	Restrict
	Public user settings	Restrict
	Maximum number of ...	-
	User authentication	Device authentication
	Ticket Hold Time Se...	-

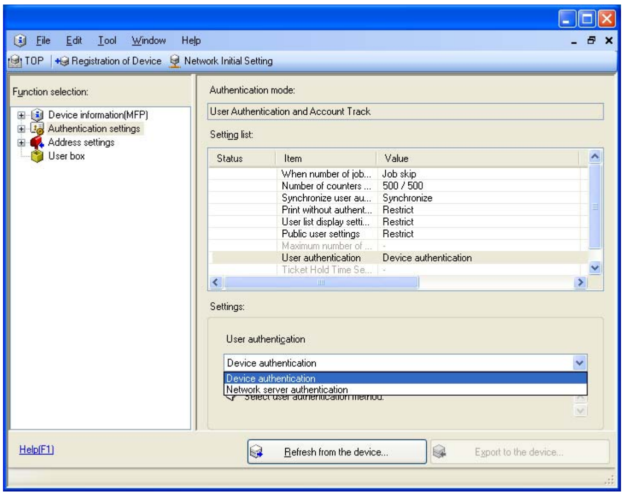
Settings:

User authentication

Device authentication

Select user authentication method.

4 From the pull-down menu of User authentication, select the user authentication method.



Authentication mode: User Authentication and Account Track

Setting list:

Status	Item	Value
	When number of job...	Job skip
	Number of counters ...	500 / 500
	Synchronize user au...	Synchronize
	Print without authent...	Restrict
	User list display setti...	Restrict
	Public user settings	Restrict
	Maximum number of ...	-
	User authentication	Device authentication
	Ticket Hold Time Se...	-

Settings:

User authentication

Device authentication

Device authentication
Network server authentication

Select user authentication method.

5 Click the [Export to the device].

Note

If you have already logged on to the Administrator Settings via the control panel or using Web Connection, the machine displays a message that tells that the write operation has not been successful because of a device lock error. Click [OK] and wait for some while before attempting to execute [Export to the device] again.

If there is a job being executed or a reserved job (timer TX, fax redial waiting, etc.) in the machine, the machine displays a message that tells that the write operation has not been successful because of a device lock error. Click [OK] and wait for some while before attempting to execute [Export to the device] again.

4.1.3 Changing the authentication mode

✎...

Note

*Changing the Account Track setting erases all user and account information data that has previously been registered. This changes all Personal User Boxes owned by the users who are deleted and all Group User Boxes owned by the accounts that are deleted to Public User Boxes. If the password set for a particular box before this change does not meet the requirements of the Password Rules, however, no access can be made to the Public User Box, to which that specific box was changed. In this case, the Administrator must first newly set a password that meets the requirements of the Password Rules. For details of the Password Rules, see **"Password Rules" on page 1-9**.*

If you have already logged on to the Administrator Settings via the control panel or using Web Connection, the machine displays a message that tells that the write operation has not been successful because of a device lock error. Click [OK] and wait for some while before attempting to execute [Export to the device] again.

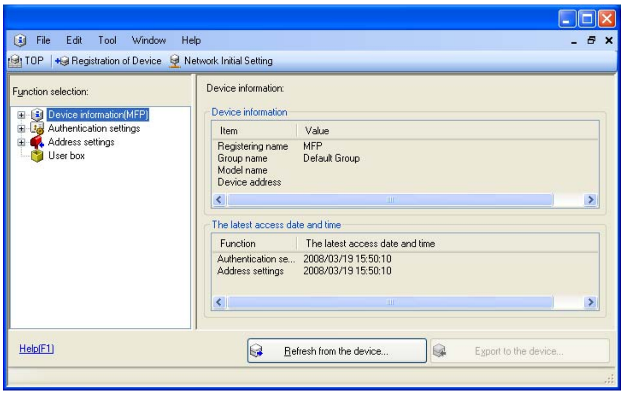
If there is a job being executed or a reserved job (timer TX, fax redial waiting, etc.) in the machine, the machine displays a message that tells that the write operation has not been successful because of a device lock error. Click [OK] and wait for some while before attempting to execute [Export to the device] again.

<From the PC>

✔ For the procedure to access the machine, see steps 1 through 5 of **"Gaining access from Data Administrator" on page 4-2**.

1 Access the machine through [Authentication Settings/Address Settings] mode of Data Administrator.

2 Click the [Authentication settings].



Device information:

Device information

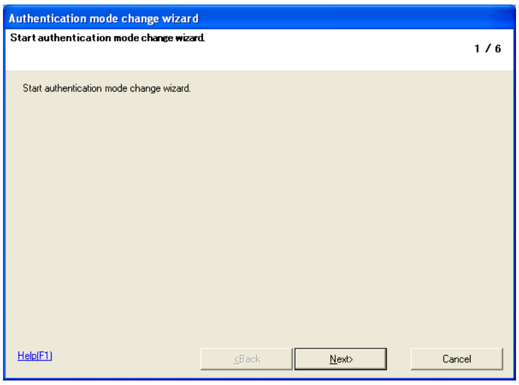
Item	Value
Registering name	MFP
Group name	Default Group
Model name	
Device address	

The latest access date and time

Function	The latest access date and time
Authentication se...	2008/03/19 15:50:10
Address settings	2008/03/19 15:50:10

3 From [Edit] on the tool bar, select [Authentication] and click [Change authentication mode].

4 Click the [Next].

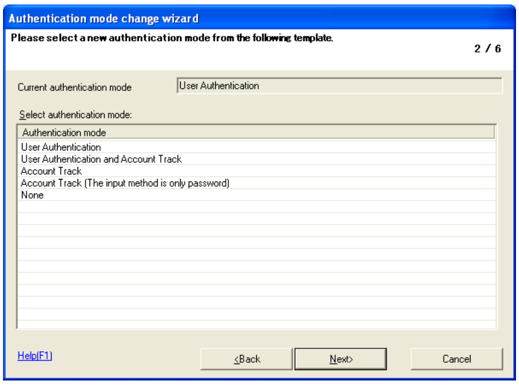


Start authentication mode change wizard.

1 / 6

Start authentication mode change wizard.

5 Select the specific [Authentication mode] to be changed and click [Next].


Authentication mode change wizard

Please select a new authentication mode from the following template.

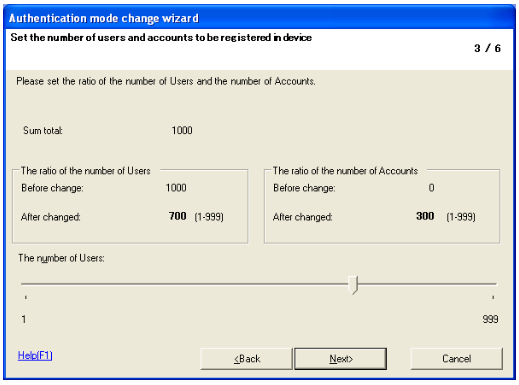
2 / 6

Current authentication mode: User Authentication

Select authentication mode:

Authentication mode
User Authentication
User Authentication and Account Track
Account Track
Account Track (The input method is only password)
None

– If [User Authentication and Account Track] has been selected, set [The ratio of the number of Users] and [The ratio of the number of Accounts].


Authentication mode change wizard

Set the number of users and accounts to be registered in device

3 / 6

Please set the ratio of the number of Users and the number of Accounts.

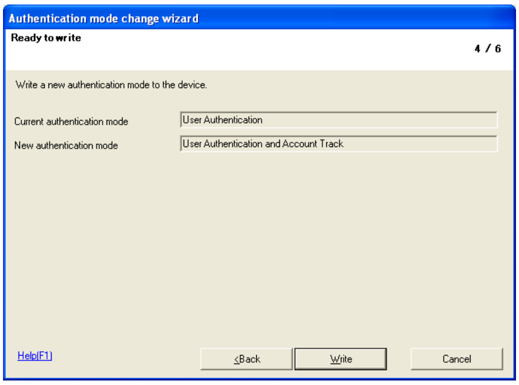
Sum total: 1000

The ratio of the number of Users
Before change: 1000
After changed: 700 (1-999)

The ratio of the number of Accounts
Before change: 0
After changed: 300 (1-999)

The number of Users:

6 Verify the new authentication mode and click [Write].


Authentication mode change wizard

Ready to write

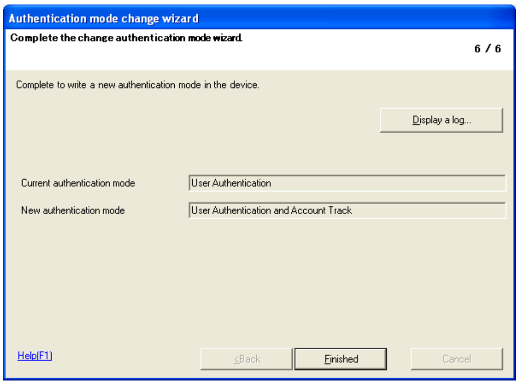
4 / 6

Write a new authentication mode to the device.

Current authentication mode: User Authentication

New authentication mode: User Authentication and Account Track

7 Click the [Finished].


Authentication mode change wizard

Complete the change authentication mode wizard.

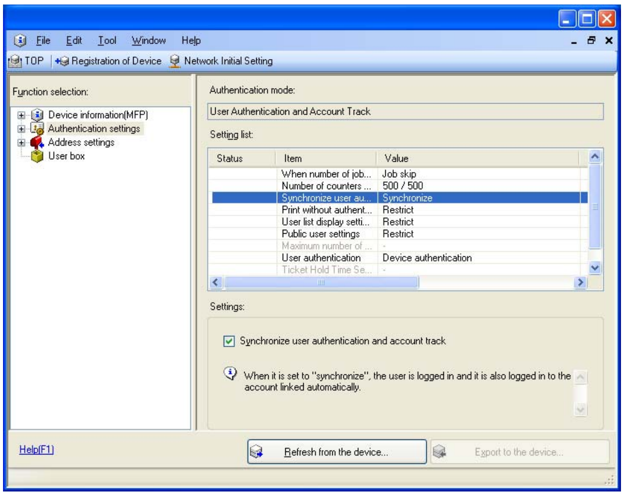
6 / 6

Complete to write a new authentication mode in the device.

Current authentication mode: User Authentication

New authentication mode: User Authentication and Account Track

– If [User Authentication and Account Track] has been selected in step 5, [Synchronize] is set for "Synchronize user authentication and account track." If you want user authentication not synchronized with account track, click to deselect [Synchronize user authentication and account track] and execute [Export to the device] once again.



Authentication mode:

User Authentication and Account Track

Setting list:

Status	Item	Value
	When number of job...	Job skip
	Number of counters ...	500 / 500
	Synchronize user au...	Synchronize
	Print without authent...	Restrict
	User list display setti...	Restrict
	Public user settings	Restrict
	Maximum number of ...	-
	User authentication	Device authentication
	Ticket Hold Time Se...	-

Settings:

☑ Synchronize user authentication and account track

When it is set to "synchronize", the user is logged in and it is also logged in to the account linked automatically.

4.1.4 Making the user settings

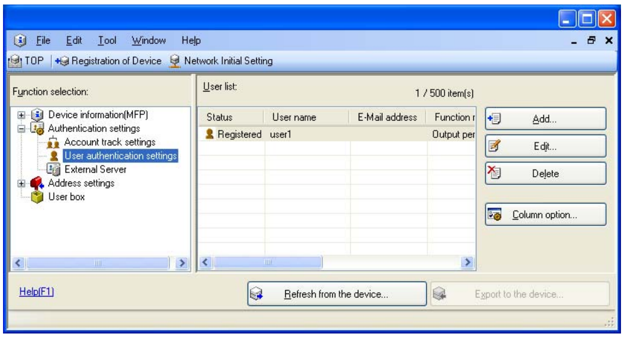
<From the PC>

✔ For the procedure to access the machine, see steps 1 through 5 of **"Gaining access from Data Administrator" on page 4-2**.

1 Access the machine through [Authentication Settings/Address Settings] mode of Data Administrator.

2 Click the Authentication settings expand button.

3 Click the [User authentication settings].



User list: 1 / 500 item(s)

Status	User name	E-Mail address	Function r
Registered	user1		Output per

4 Select the desired function.

- To register the user, click [Add].
- To change data registered for the user, click [Edit].
- To delete the user, click [Delete].

? What precautions should be used when registering a user or changing registered data of a user?

➔ If the User Password does not meet the requirements of the Password Rules, a message appears that this particular User Password cannot be used. Click [OK] and enter the correct User Password. For details of the Password Rules, see **"Password Rules" on page 1-9**.

➔ If the User Name has not been entered, a message appears that tells that the User Name is yet to be entered. Click [OK] and enter the User Name.

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

5 Click the [OK].

6 Click the [Export to the device].

✎...

Note

If you have already logged on to the Administrator Settings via the control panel or using Web Connection, the machine displays a message that tells that the write operation has not been successful because of a device lock error. Click [OK] and wait for some while before attempting to execute [Export to the device] again.

If there is a job being executed or a reserved job (timer TX, fax redial waiting, etc.) in the machine, the machine displays a message that tells that the write operation has not been successful because of a device lock error. Click [OK] and wait for some while before attempting to execute [Export to the device] again.

✎...

Reminder

*If [Delete] is selected in step 4, a screen appears that prompts you to confirm the execution of deletion. Click [Yes] to delete the user. Note that, if a previously registered user is deleted, the Personal User Box owned by that specific user is changed to Public User Box. If the password set for a particular box before this change does not meet the requirements of the Password Rules, however, no access can be made to the Public User Box, to which that specific box was changed. In this case, the Administrator must first newly set a password that meets the requirements of the Password Rules. For details of the Password Rules, see **"Password Rules" on page 1-9**.*

4.1.5 Making the account settings

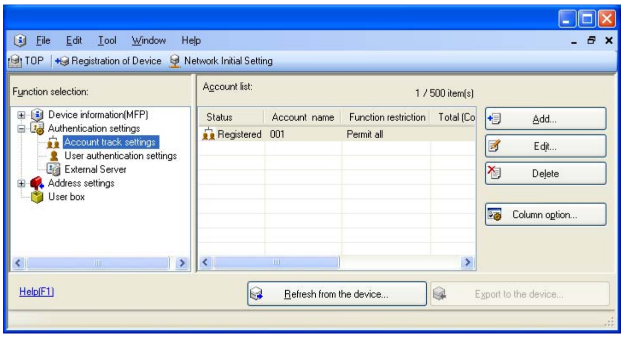
<From the PC>

✔ For the procedure to access the machine, see steps 1 through 5 of **"Gaining access from Data Administrator" on page 4-2**.

1 Access the machine through [Authentication Settings/Address Settings] mode of Data Administrator.

2 Click the Authentication settings expand button.

3 Click the [Account track settings].



Status	Account name	Function restriction	Total (Co
Registered	001	Permit all	

4 Select the desired function.

– To register the account, click [Add].
– To change data registered for the account, click [Edit].
– To delete the account, click [Delete].

? What precautions should be used when registering a account or changing registered data of a account?

➔ If the Account Password does not meet the requirements of the Password Rules, a message appears that this particular Account Password cannot be used. Click [OK] and enter the correct Account Password. For details of the Password Rules, see **"Password Rules" on page 1-9**.

➔ If the Account Name has not been entered, a message appears that tells that the User Name is yet to be entered. Click [OK] and enter the Account Name.

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

5 Click the [OK].

6 Click the [Export to the device].

✎...

Note

If you have already logged on to the Administrator Settings via the control panel or using Web Connection, the machine displays a message that tells that the write operation has not been successful because of a device lock error. Click [OK] and wait for some while before attempting to execute [Export to the device] again.

If there is a job being executed or a reserved job (timer TX, fax redial waiting, etc.) in the machine, the machine displays a message that tells that the write operation has not been successful because of a device lock error. Click [OK] and wait for some while before attempting to execute [Export to the device] again.

✎...

Reminder

*If [Delete] is selected in step 4, a screen appears that prompts you to confirm the execution of deletion. Click [Yes] to delete the account. Note that, if a previously registered account is deleted, the Group User Box owned by that specific account is changed to Public User Box. If the password set for a particular box before this change does not meet the requirements of the Password Rules, however, no access can be made to the Public User Box, to which that specific box was changed. In this case, the Administrator must first newly set a password that meets the requirements of the Password Rules. For details of the Password Rules, see **"Password Rules" on page 1-9**.*

4.1.6 Registering the certificate

✎...

Note

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

If the abbreviated name and E-mail address have not been entered, an input error message appears. Then, click [OK] and enter the abbreviated name and E-mail address.

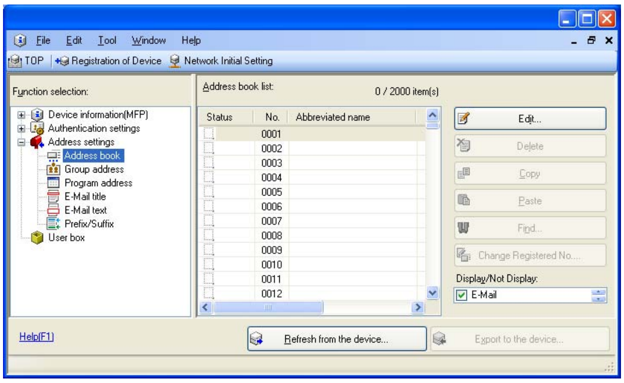
<From the PC>

✔ For the procedure to access the machine, see steps 1 through 5 of **"Gaining access from Data Administrator" on page 4-2**.

1 Access the machine through [Authentication Settings/Address Settings] mode of Data Administrator.

2 Click the Address settings expand button.

3 Click the [Address book].

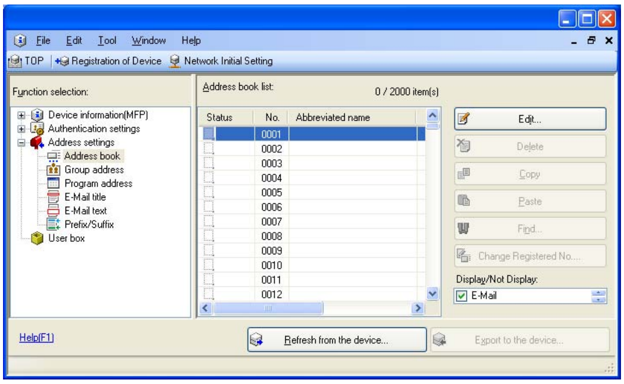


Address book list: 0 / 2000 item(s)

Status	No.	Abbreviated name
□	0001	
□	0002	
□	0003	
□	0004	
□	0005	
□	0006	
□	0007	
□	0008	
□	0009	
□	0010	
□	0011	
□	0012	

Display/Not Display: ☑ E-Mail

4 Select the number to be registered and click [Edit].

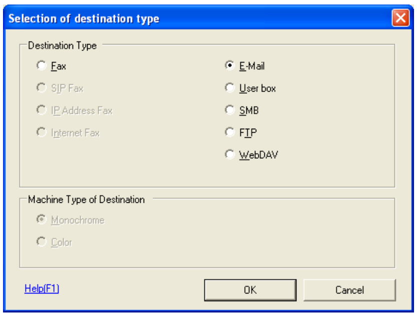


Address book list: 0 / 2000 item(s)

Status	No.	Abbreviated name
□	0001	
□	0002	
□	0003	
□	0004	
□	0005	
□	0006	
□	0007	
□	0008	
□	0009	
□	0010	
□	0011	
□	0012	

Display/Not Display: ☑ E-Mail

5 Select the [E-Mail] and Click the [OK].


Selection of destination type

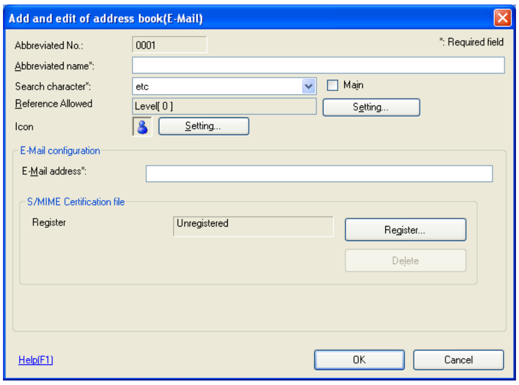
Destination Type

○ Fax ● E-Mail
○ SIP Fax ○ User box
○ IP Address Fax ○ SMB
○ Internet Fax ○ FTP
○ WebDAV

Machine Type of Destination

● Monochrome
○ Color

6 Click [Register] of S/MIME Certification file and select the certificate to be registered.



Add and edit of address book(E-Mail)

*: Required field

Abbreviated No.: 0001

Abbreviated name*:

Search character*: etc □ Main

Reference Allowed: Level[0] Setting...

Icon Setting...

E-Mail configuration

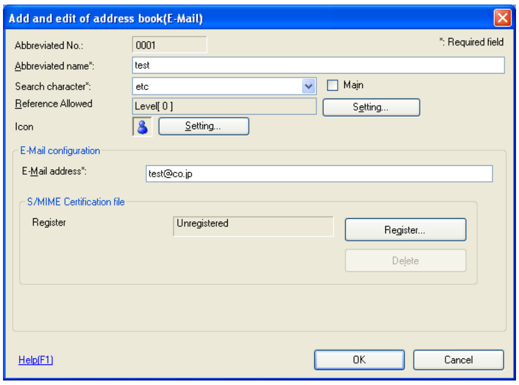
E-Mail address*:

S/MIME Certification file

Register: Unregistered Register... Delete

Help(F1) OK Cancel

7 Make the necessary settings.



Add and edit of address book(E-Mail)

*: Required field

Abbreviated No.: 0001

Abbreviated name*: test

Search character*: etc □ Main

Reference Allowed: Level[0] Setting...

Icon Setting...

E-Mail configuration

E-Mail address*: test@co.jp

S/MIME Certification file

Register: Unregistered Register... Delete

Help(F1) OK Cancel

8 Click the [OK].

9 Click the [Export to the device].

✎...

Note

If you have already logged on to the Administrator Settings via the control panel or using Web Connection, the machine displays a message that tells that the write operation has not been successful because of a device lock error. Click [OK] and wait for some while before attempting to execute [Export to the device] again.

If there is a job being executed or a reserved job (timer TX, fax redial waiting, etc.) in the machine, the machine displays a message that tells that the write operation has not been successful because of a device lock error. Click [OK] and wait for some while before attempting to execute [Export to the device] again.

4.2 Box Operator

Box Operator is application software used exclusively for changing the name of scan or fax data stored in a User Box, downloading or deleting such scan or fax data, creating a User Box, changing the properties (user attributes) of a User Box, and performing other tasks. It allows a network-connected PC to gain access to the HDD of the machine for accomplishing these tasks.

When an attempt is made to gain access to the machine through Box Operator, the user is authenticated to be an authorized user by using an 8-to-64-digit User Password and an 8-digit User Box Password. During the authentication procedure, the password entered appears as "*." When the Enhanced Security Mode is set to [ON], the number of times in which authentication fails is counted.

Note

Do not leave the site while you are gaining access to the machine through Box Operator. If it is absolutely necessary to leave the site, be sure first to log off from the Box Operator.

4.2.1 Accessing User Box

Reminder

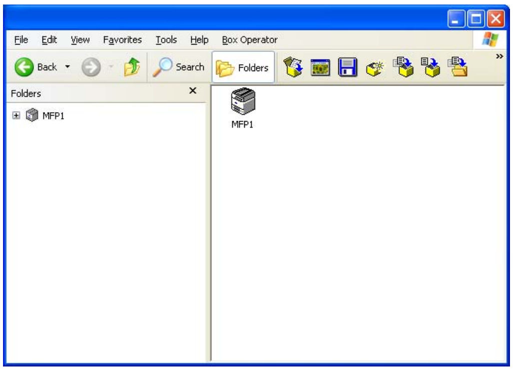
If the "Save logon user name" check box has been selected, the User Password entered is stored in the PC being used. If you do not want the User Password stored, clear the "Save logon user name" check box.

If the "Save box password until disconnected" check box has been selected, the User Box Password entered is stored in the PC being used. If you do not want the User Box Password stored, clear the "Save box password until disconnected" check box.

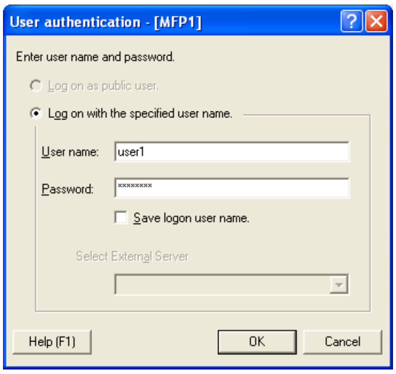
<From the PC>

1 Start the Box Operator.

2 Double-click this machine.



3 Type the User Name and the 8-to-64-digit User Password.



User authentication - [MFP1]

Enter user name and password.

○ Log on as public user.

● Log on with the specified user name.

User name: user1

Password: ********

□ Save logon user name.

Select External Server

? What steps must be performed if ON (External Server) is set for the authentication method?

➔ If [ON (External Server)] is set for the authentication method, select the desired external server.

4 Click the [OK].

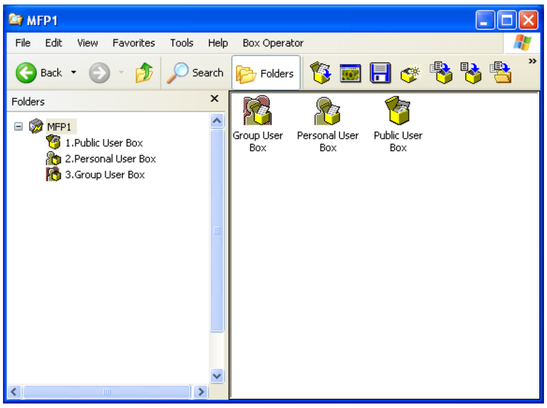
? What happens if a wrong User Password is entered?

→ If the User Password entered does not correspond to the registered User Name, a message appears that tells that authentication has not been successful. Click [OK] and then enter the correct User Password.

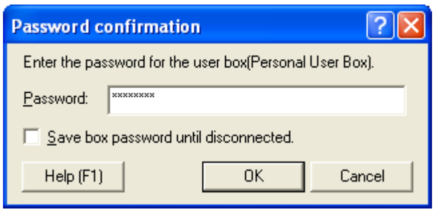
→ If the Enhanced Security Mode is set to [ON], the entry of a wrong User Password is counted as unauthorized access. If a wrong User Password is entered a predetermined number of times (once to three times) set by the Administrator of the machine or more, a message appears that tells that authentication has not been successful for any subsequent operation for authentication. The machine is then set into an access lock state, rejecting any more logon attempts. To cancel the access lock state, the Administrator of the machine must perform the Release Setting. Contact the Administrator of the machine.

→ If [ON (External Server)] (Active Directory) is set for the authentication method and if user authentication is successful, the User Name not registered in the machine is automatically registered.

5 Click or double-click the desired User Box icon.



6 Type the 8-digit User Box Password.


Password confirmation

Enter the password for the user box(Personal User Box).

Password: ********

□ Save box password until disconnected.

7 Click the [OK].

– To delete a User Box, select the specific User Box icon and, from the [File] menu, select [Delete]. A message will then appear that prompts you to confirm that you want to delete the User Box. Click [Yes] and enter the User Box Password corresponding to the specific User Box. This deletes the User Box.

? What happens if a wrong User Box Password is entered?

→ If there is a mismatch in the User Box Password, a message appears that tells that authentication has not been successful. Click [OK] and then enter the correct User Box Password.

→ If the Enhanced Security Mode is set to [ON], the entry of a wrong User Box Password is counted as unauthorized access. If a wrong User Box Password is entered a predetermined number of times (once to three times) set by the Administrator of the machine or more, a message appears that tells that authentication has not been successful for any subsequent operation for authentication. The machine is then set into an access lock state, rejecting any more logon attempts. To cancel the access lock state, the Administrator of the machine must perform the Release Setting. Contact the Administrator of the machine.

4.2.2 Creating a User Box

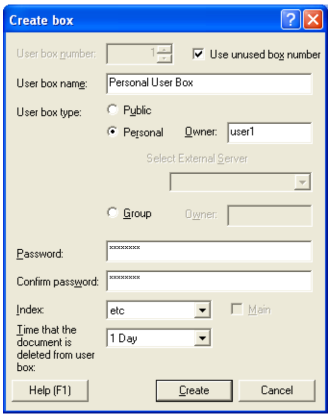
<From the PC>

✔ For the procedure to access the User Box, see steps 1 through 7 of **"Accessing User Box" on page 4-14**.

1 Access the User Box through Box Operator.

2 From the [Box Operator] menu, select [Create User Box]. Or, click .

3 Make the necessary settings.



Create box

User box number: 1 ☑ Use unused box number

User box name: Personal User Box

User box type: ○ Public

● Personal Owner: user1

Select External Server

○ Group Owner:

Password: *********

Confirm password: *********

Index: etc □ Main

Time that the document is deleted from user box: 1 Day

- Do not fail to enter data in the "User Box name," "Password," and "Confirm password" boxes.
- A Use unused box number that already exists cannot be registered redundantly.
- If [Private] is selected for User Box Type, enter the User Name of the user who owns the User Box in the "Owner" box.
- If [Group] is selected for the User Box Type, enter the name of the account that owns the box in the "Owner" box.

? What happens if the Automatic check box is selected?

→ If the "Automatic" check box is selected, the User Box No. is automatically assigned.

? What happens if Public is selected for User Box Type?

→ If "Public" is selected for User Box Type, set the User Box Password that meets the requirements of the Password Rules. For details of the Password Rules, see **"Password Rules" on page 1-9**.

4 Click the [Create].

✎...

Note

If the User Box Password entered does not meet the requirements of the Password Rules, a message appears that the User Box Password that has been entered cannot be used. Click [OK] and enter the correct User Box Password. For details of the Password Rules, see ***"Password Rules" on page 1-9****.*

If there is a mismatch in the User Box Password between that entered in the "Password" box and that entered in the "Confirm password" box, a message appears that tells that there is a mismatch in the User Box Password. Enter the correct User Box Password.

If the Owner Name is not entered with "Private" selected for User Box Type, a message appears that warns that the Owner Name is yet to be entered. Enter the correct Owner Name.

If the Account Name is not entered with "Group" selected for User Box Type, a message appears that warns that the Account Name is yet to be entered. Enter the correct Account Name.

If a user name not registered with the machine is entered in the "Owner Name" box, a message appears that tells that the Owner Name entered in the box is illegal. Click [OK] and enter the correct Owner Name.

If a account name not registered with the machine is entered in the "Account Name" box, a message appears that tells that the Account Name entered in the box is illegal. Click [OK] and enter the correct Account Name.

✎...

Reminder

For the procedure to change the User Box Password and properties (user attributes, account attributes), see ***"Changing User Box properties (user attributes, account attributes)" on page 4-18****.*

4.2.3 Changing User Box properties (user attributes, account attributes)

✎...

Reminder

If the "Save box password until disconnected" check box has been selected, the User Box Password entered is stored in the PC being used. If you do not want the User Box Password stored, clear the "Save box password until disconnected" check box.

<From the PC>

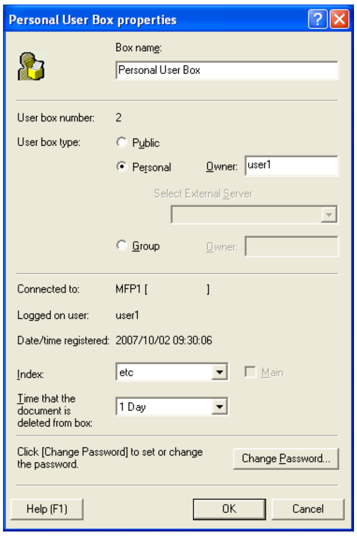
✔ For the procedure to access the User Box, see steps 1 through 7 of **"Accessing User Box" on page 4-14**.

1 Access the User Box through Box Operator.

2 Select the icon of the desired User Box.

3 From the [File] menu, select [Property], or right-click to select [Property].

4 Make the necessary settings.



Personal User Box properties

Box name: Personal User Box

User box number: 2

User box type: ○ Public

● Personal Owner: user1

Select External Server

○ Group Owner:

Connected to: MFP1 [ ]

Logged on user: user1

Date/time registered: 2007/10/02 09:30:06

Index: etc □ Main

Time that the document is deleted from box: 1 Day

Click [Change Password] to set or change the password. Change Password...

Help (F1) OK Cancel

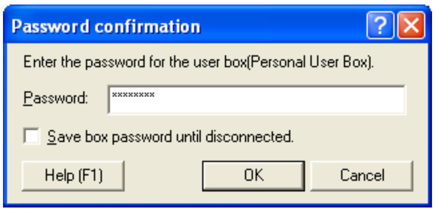
– To set the User Box Password, perform steps 7 through 9.

? What steps should be performed to change the owner of the User Box?

→ To change the owner of the User Box, enter the user name that has been registered with this machine as a user for a Personal User Box and that has been registered with this machine as an account for a Group User Box.

→ If Public is to be set for User Box Type, a password that meets the requirements of the Password Rules must be entered in the "New Password" box. For details of the Password Rules, see **"Password Rules" on page 1-9**.

5 Click the [OK].



Password confirmation

Enter the password for the user box[Personal User Box].

Password: ********

□ Save box password until disconnected.

Help (F1) OK Cancel

– If a User Box Password has been set, the password confirmation screen appears. Then, enter the currently set 8-digit User Box Password and click [OK].

? What precautions should be used when User Box Type is changed from Personal or Group to Public?

➔ If User Box Type is changed from "Personal" or "Group" to "Public" and if the User Box Password set for the Personal or Group User Box before this change does not meet the requirements of the Password Rules, a message appears that tells that the User Box Password is illegal.

? What happens if a wrong User Box Password is entered?

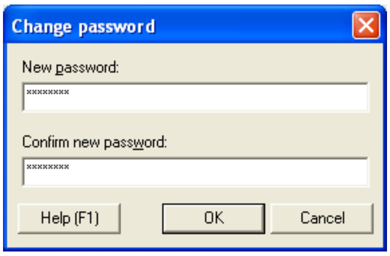
➔ If a wrong User Box Password is entered, a message appears that tells that the User Box Password entered is wrong. Click [OK] and then enter the correct User Box Password.

➔ If the Enhanced Security Mode is set to [ON], the entry of a wrong User Box Password is counted as unauthorized access. If a wrong User Box Password is entered a predetermined number of times (once to three times) set by the Administrator of the machine or more, a message appears that tells that authentication has not been successful for any subsequent operation for authentication. The machine is then set into an access lock state, rejecting any more logon attempts. To cancel the access lock state, the Administrator of the machine must perform the Release Setting. Contact the Administrator of the machine.

6 Select [Property] from the [File] menu or right-click to select [Property].

7 Click the [Change Password].

8 Enter the User Box Password.



New password: ********

Confirm new password: ********

? What precautions should be used when entering the User Box Password in each of the different password boxes?

➔ If Public is to be set for User Box Type, a password that meets the requirements of the Password Rules must be entered in the "New Password" box. For details of the Password Rules, see **"Password Rules" on page 1-9**.

➔ In the "Confirm new password" box, enter the same User Box Password as that entered in the "New password" box.

9 Click the [OK].

? What steps should be performed to change the owner of the User Box?

➔ When the owner of the User Box is to be changed, enter the User Name registered in the machine as an authorized user of the machine in the Owner Name.

Note

When [OK] is clicked, the password confirmation screen of step 5 appears. Enter the 8-digit User Box Password, which was set before the change of the password, and click [OK].

*If the User Box Password entered does not meet the requirements of the Password Rules with "Public" selected for User Box Type, a message appears that tells that the User Box Password entered cannot be used. Click [OK] and perform steps 8 and 9 again. For details of the Password Rules, see **"Password Rules" on page 1-9**.*

If the Enhanced Security Mode is set to [ON], the entry of a wrong User Box Password is counted as unauthorized access. If a wrong User Box Password is entered a predetermined number of times (once to three times) set by the Administrator of the machine or more, a message appears that tells that authentication has not been successful for any subsequent operation for authentication. The machine is then set into an access lock state, rejecting any more logon attempts. To cancel the access lock state, the Administrator of the machine must perform the Release Setting. Contact the Administrator of the machine.

4.2.4 Accessing the User Box file

Different functions can be operated depending on the file format.

Study the following table for the relationship between the file format and operable functions.

File format	Operable functions
PDF	Icon display, thumbnail display, detail display, opening in a specific application, file acquisition, file name change, file deletion, copy to another User Box, move to another User Box, copy to another Folder, move to another Folder
TIFF	Icon display, thumbnail display, detail display, opening in a specific application, opening in Box Operator viewer, file acquisition, file name change, file deletion, copy to another User Box, move to another User Box, copy to another Folder, move to another Folder

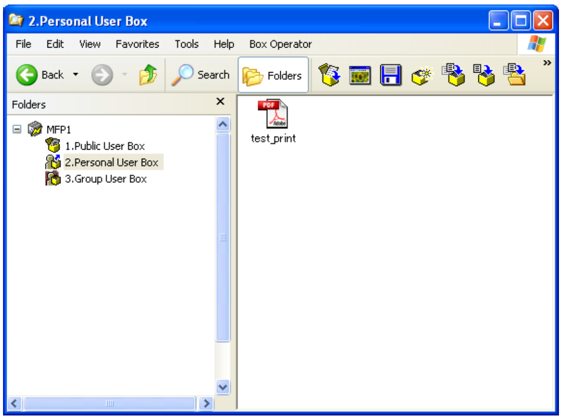
Reminder
The file saved in the User Box may be saved in your PC from Box Operator through drag-&-drop.

<From the PC>

✔ For the procedure to access the User Box, see steps 1 through 4 of **"Accessing User Box" on page 4-14**.

1 Access the User Box through Box Operator.

2 Select any desired file.



3 Select the desired function.

4.3 HDD TWAIN driver

The HDD TWAIN driver, which is to be installed in the PC of a general user, is a TWAIN driver used exclusively for allowing the HDD of this machine to be recognized as a TWAIN device.

The HDD TWAIN driver is a utility function for downloading document data stored in the User Box in the scan or fax mode in the image processing application of the PC.

When an attempt is made to gain access to the machine through the HDD TWAIN driver, the user is authenticated to be an authorized user by using an 8-to-64-digit User Password and an 8-digit User Box Password. During the authentication procedure, the User Password entered for the authentication purpose appears as "*" on the display. When the Enhanced Security Mode is set to [ON], the number of times in which authentication fails is counted.

Note
Do not leave the site while you are gaining access to the machine through the HDD TWAIN driver. If it is absolutely necessary to leave the site, be sure first to log off from the HDD TWAIN driver.

Reminder
If [ON (External Server)] (Active Directory) is set for the authentication method and if user authentication is successful, the User Name not registered in the machine is automatically registered.

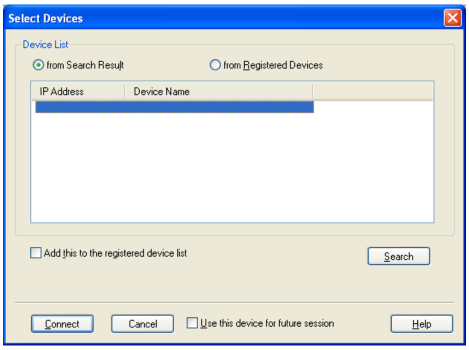
4.3.1 Accessing from the HDD TWAIN driver

<From the PC>

1 Start the image processing application.

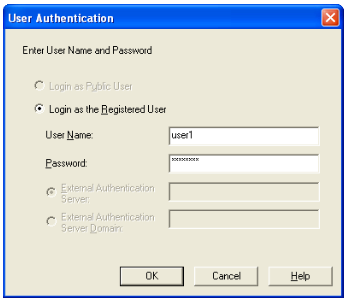
2 From the [File] menu, click [Read], and then select [Generic HDD TWAIN Ver.3].

3 Select this machine and click [Connect].



Select Devices
Device List
● from Search Result
○ from Registered Devices
IP Address
Device Name
□ Add this to the registered device list
Search
Connect
Cancel
□ Use this device for future session
Help

4 Select the "Login as the Registered User" radio button and enter the User Name and the 8-to-64-digit User Password.



User Authentication

Enter User Name and Password

○ Login as Public User

● Login as the Registered User

User Name: user1

Password: ********

External Authentication Server:
External Authentication Server Domain:
OK
Cancel
Help

? What steps must be performed if ON (External Server) is set for the authentication method?
→ If [ON (External Server)] is set for the authentication method, enter the desired external server.

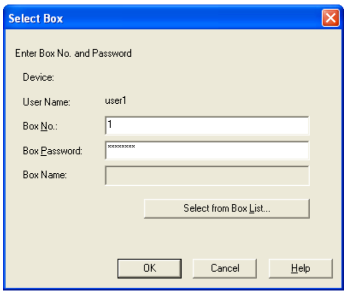
5 Click the [OK].

? What happens if a wrong User Password is entered?

→ If a wrong User Password is entered for the corresponding User Name registered, a message appears that tells that authentication has not been successful. Enter the correct User Name and User Password.

→ If the Enhanced Security Mode is set to [ON], the entry of a wrong User Password is counted as unauthorized access. If a wrong User Password is entered a predetermined number of times (once to three times) set by the Administrator of the machine or more, a message appears that tells that authentication has not been successful for any subsequent operation for authentication. The machine is then set into an access lock state, rejecting any more logon attempts. To cancel the access lock state, the Administrator of the machine must perform the Release Setting. Contact the Administrator of the machine.

6 Enter the desired User Box No. and 8-digit User Box Password.



Select Box

Enter Box No. and Password

Device:

User Name: user1

Box No.: 1

Box Password: ********

Box Name:

7 Click the [OK].

? What happens if there is a mismatch between the User Box No. and User Box Password?

→ If there is a mismatch between the User Box No. and User Box Password, a message appears that tells that authentication has not been successful. Click [OK] and perform step 6 once again.

→ If the Enhanced Security Mode is set to [ON], the entry of a wrong User Password is counted as unauthorized access. If a wrong User Password is entered a predetermined number of times (once to three times) set by the Administrator of the machine or more, a message appears that tells that authentication has not been successful for any subsequent operation for authentication. The machine is then set into an access lock state, rejecting any more logon attempts. To cancel the access lock state, the Administrator of the machine must perform the Release Setting. Contact the Administrator of the machine.

8 Select the desired document data and click [Read].

4.4 Direct Print

Direct Print is an application that allows a PDF file or a TIFF file to be directly transmitted to, and printed on, the printer.

It permits printing of data through drag and drop to the desktop icon and using the context (right-click) menu of Windows, and automatic printing of data using a hot folder. The application also allows two or more different print job setups to be registered.

When data is to be printed through Direct Print, the user is authenticated to be an authorized user by using an 8-to-64-digit User Password or Account Password. When the Enhanced Security Mode is set to [ON], the number of times in which authentication fails is counted.

✎...

Note

If the "Edit Authentication/Account Track for each drag-and-drop printing" check box is not selected on the Direct Print main screen, no authentication screen appears for drag-and-drop printing. Select the "Edit Authentication/Account Track for each drag-and-drop printing" check box when using Direct Print.

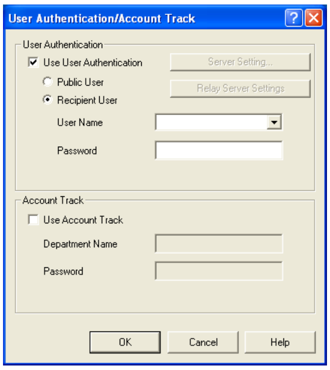
4.4.1 Printing through Direct Print

<From the PC>

1 Drag and drop the desired file to the Direct Print shortcut.

– Right-click the desired file. Direct Print can be selected from the menu that will then be displayed.

2 Select the "Use User Authentication" check box and the "Recipient User" radio button.



User Authentication/Account Track

User Authentication

☑ Use User Authentication

○ Public User

● Recipient User

User Name

Password

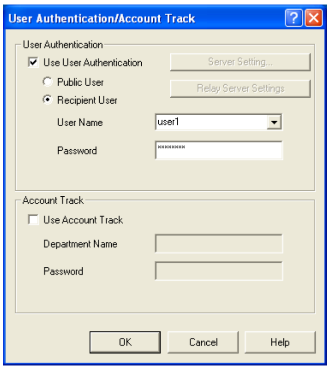
Account Track

□ Use Account Track

Department Name

Password

3 Enter the User Name and the 8-to-64-digit User Password that have been registered in the machine.



User Authentication/Account Track

User Authentication

☑ Use User Authentication

○ Public User

● Recipient User

User Name user1

Password ********

Account Track

□ Use Account Track

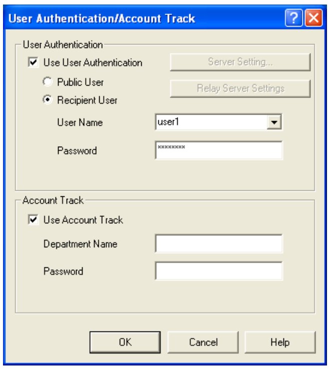
Department Name

Password

? What steps must be performed if ON (External Server) is set for the authentication method?

→ If [ON (External Server)] is set for the authentication method, select the desired external server.

4 To enable Account Track, click the [Use Account Track] check box.


User Authentication/Account Track

User Authentication

☑ Use User Authentication

○ Public User

● Recipient User

User Name: user1

Password: ********

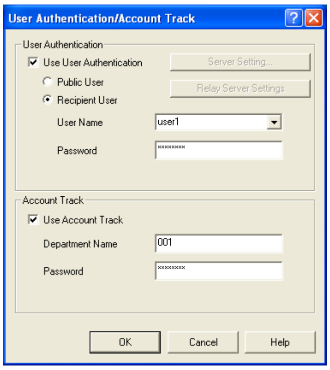
Account Track

☑ Use Account Track

Department Name:

Password:

5 Enter the Account Name and 8-to-64-digit Account Password registered with the machine.


User Authentication/Account Track

User Authentication

☑ Use User Authentication

○ Public User

● Recipient User

User Name: user1

Password: ********

Account Track

☑ Use Account Track

Department Name: 001

Password: ********

6 Click the [OK].

Note

If there is a mismatch between the User Password and Account Password entered and the User Name and Account Password registered, the specified file is erased as an error from the machine without being printed.

If the Enhanced Security Mode is set to [ON], the entry of a wrong User Password or Account Password is counted as unauthorized access. If a wrong User Password or Account Password is entered a predetermined number of times (once to three times) set by the Administrator of the machine or more, the machine is then set into an access lock state, rejecting any more logon attempts. To cancel the access lock state, the Administrator of the machine must perform the Release Setting. Contact the Administrator of the machine.

4.5 HDD Backup Utility

The HDD Backup Utility, which is to be installed in the PC of the Administrator of the machine, is application software used exclusively for accessing the HDD in this machine.

The HDD Backup Utility functions performed by the Administrator of the machine allow the image data saved in the HDD of the machine to be backed up and restored. It is not possible to open directly the backup data.

To gain access to the machine from the HDD Backup Utility, the user is authenticated to be an authorized Administrator by using an 8-digit Administrator Password. The Administrator Password entered during the authentication procedure is displayed as "*." When the Enhanced Security mode is set to [ON], the number of times in which authentication fails is counted.

✎...

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 Technical Representative.

4.5.1 Backup

✎...

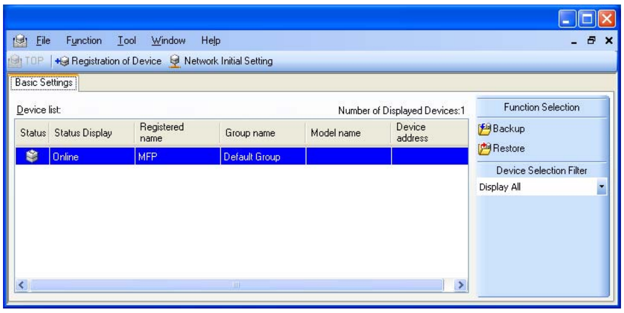
Reminder

If the "Save the administrator password" check box is selected, the Administrator Password entered is stored in the PC being used. If you do not want the Administrator Password stored, clear the "Save the administrator password" check box.

<From the PC>

1 Start the HDD Backup Utility.

2 Select this machine and click [Backup].

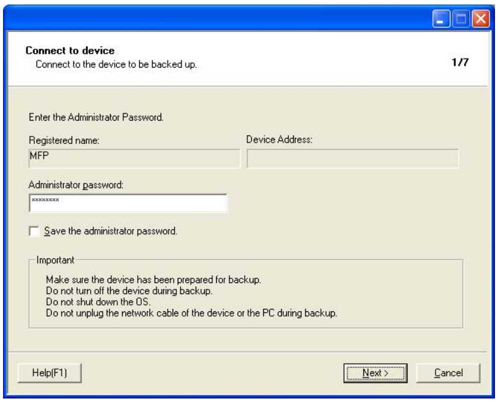


Device list:

Number of Displayed Devices:1

Status	Status Display	Registered name	Group name	Model name	Device address
	Online	MFP	Default Group		

3 Enter the 8-digit Administrator Password registered in the machine in the "Administrator password" box.



Connect to device

Connect to the device to be backed up. 1/7

Enter the Administrator Password.

Registered name: MFP

Device Address:

Administrator password: ********

□ Save the administrator password.

Important

Make sure the device has been prepared for backup.
Do not turn off the device during backup.
Do not shut down the OS.
Do not unplug the network cable of the device or the PC during backup.

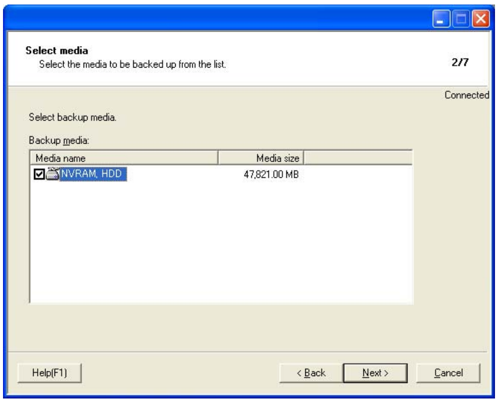
4 Click the [Next].

? 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 passwords. 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) 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 From "Backup media," select the check box of the desired media and click [Next].



Select media
Select the media to be backed up from the list.
2/7

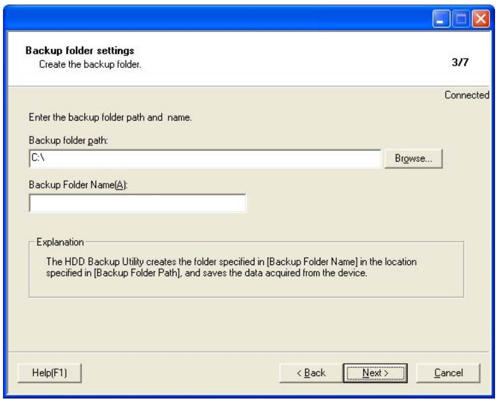
Connected

Select backup media.

Backup media:

Media name	Media size
☑ NVRAM, HDD	47,821.00 MB

6 Click [Browse] and specify the destination, in which the backup folder is to be saved.



Backup folder settings
Create the backup folder.
3/7

Connected

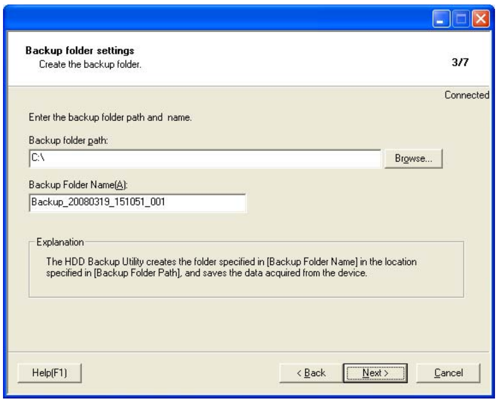
Enter the backup folder path and name.

Backup folder path: C:\

Backup Folder Name(A):

Explanation
The HDD Backup Utility creates the folder specified in [Backup Folder Name] in the location specified in [Backup Folder Path], and saves the data acquired from the device.

7 Type a backup folder name that consists of one to 50 characters in the "Backup folder name" text box and click [Next].



Backup folder settings
Create the backup folder.
3/7

Connected

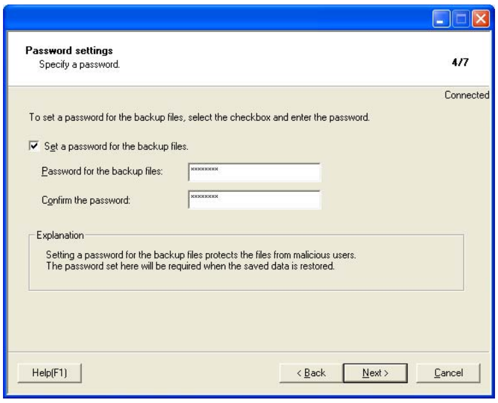
Enter the backup folder path and name.

Backup folder path: C:\

Backup Folder Name(A): Backup_20080319_151051_001

Explanation
The HDD Backup Utility creates the folder specified in [Backup Folder Name] in the location specified in [Backup Folder Path], and saves the data acquired from the device.

8 To set a password for the backup file, select the corresponding check box and type a password that consists of one to 64 digits in the "Password for the backup files" and "Confirm the password" boxes and then click [Next].



Password settings
Specify a password.
4/7

Connected

To set a password for the backup files, select the checkbox and enter the password.

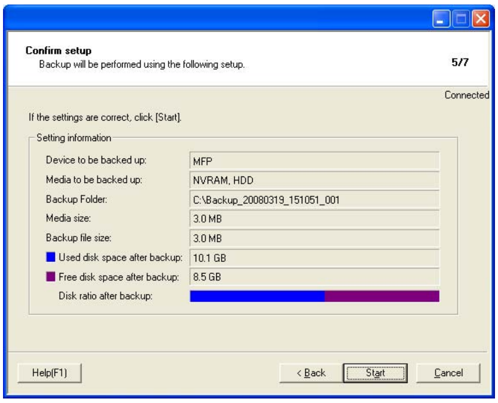
☑ Set a password for the backup files.

Password for the backup files: ********

Confirm the password: ********

Explanation
Setting a password for the backup files protects the files from malicious users.
The password set here will be required when the saved data is restored.

9 Check the data that has been set and click [Start].



Confirm setup
Backup will be performed using the following setup.
5/7

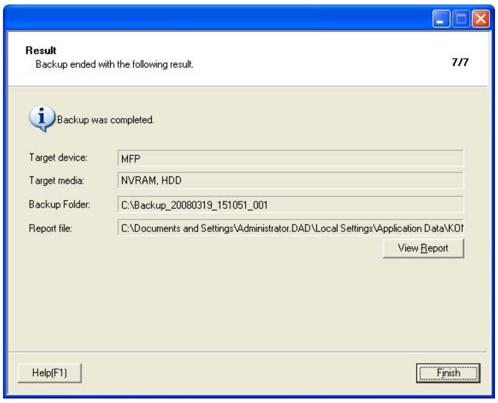
Connected

If the settings are correct, click [Start].

Setting information

Device to be backed up:	MFP
Media to be backed up:	NVRAM, HDD
Backup Folder:	C:\Backup_20080319_151051_001
Media size:	3.0 MB
Backup file size:	3.0 MB
🟦 Used disk space after backup:	10.1 GB
🟪 Free disk space after backup:	8.5 GB
Disk ratio after backup:	

10 Make sure that the backup procedure has been completed. Then, click [Finish].



Result

Backup ended with the following result.

7/7

Backup was completed.

Target device:	MFP
Target media:	NVRAM, HDD
Backup Folder:	C:\Backup_20080319_151051_001
Report file:	C:\Documents and Settings\Administrator.DAD\Local Settings\Application Data\KOI

Reminder

In Backup, none of the following settings are backed up: Administrator Password, CE Password, HDD Lock Password, Flash Memory Lock Password, Image Data Encryption Passphrase, and CE Lock Release Time.

Security settings other than the above are all backed up. Pay attention to which settings are backed up and which are not when restoring data. Especially, be sure not to forget the settings made to security related data such as auth-password and priv-password during back up.

Note that the Enhanced Security Mode is turned OFF when restoring data that are backed up under the condition where the Enhanced Security Mode is set to OFF.

In backup, Image Data Encryption Passphrase cannot be backed up. If Image Data Encryption Passphrase is changed during backup, a warning message appears saying that there is a mismatch in the Image Data Encryption Passphrases when the machine is started after restoration. To reset the warning message, the Image Data Encryption Passphrase set during backup must be set on the machine again. Be sure not to forget the Image Data Encryption Passphrase set during backup.

4.5.2 Restore

...

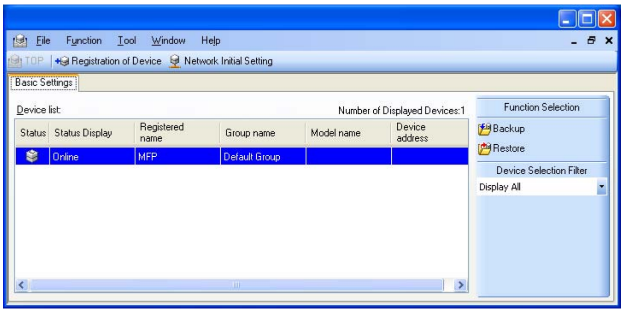
Reminder

If the "Save the administrator password" check box is selected, the Administrator Password entered is stored in the PC being used. If you do not want the Administrator Password stored, clear the "Save the administrator password" check box.

<From the PC>

1 Start the HDD Backup Utility.

2 Select this machine and click [Restore].

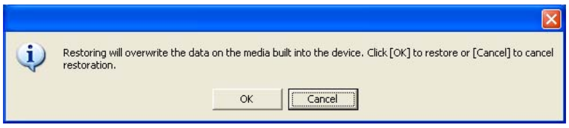


Device list:

Number of Displayed Devices:1

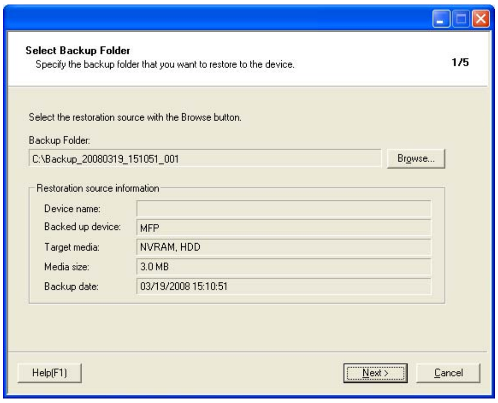
Status	Status Display	Registered name	Group name	Model name	Device address
	Online	MFP	Default Group		

3 Click the [OK].



Restoring will overwrite the data on the media built into the device. Click [OK] to restore or [Cancel] to cancel restoration.

4 Click [Browse] and specify the destination, in which the backup file is to be saved.



Select Backup Folder

Specify the backup folder that you want to restore to the device.

1/5

Select the restoration source with the Browse button.

Backup Folder: C:\Backup_20080319_151051_001

Restoration source information

Device name:

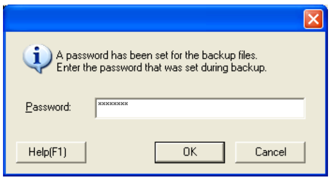
Backed up device: MFP

Target media: NVRAM, HDD

Media size: 3.0 MB

Backup date: 03/19/2008 15:10:51

– If a password has been set for the backup data, type the password that consists of one to 64 digits set during Backup and click [OK].

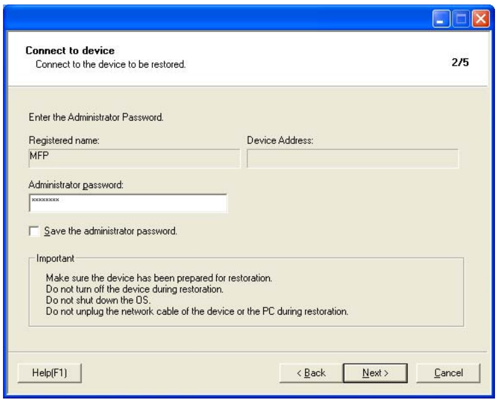


A password has been set for the backup files.
Enter the password that was set during backup.

Password: ********

5 Click the [Next].

6 Type the 8-digit Administrator Password registered in the machine in the "Administrator Password" box.



Connect to device
Connect to the device to be restored. 2/5

Enter the Administrator Password.

Registered name: MFP

Device Address:

Administrator password: ********

□ Save the administrator password.

Important

Make sure the device has been prepared for restoration.
Do not turn off the device during restoration.
Do not shut down the OS.
Do not unplug the network cable of the device or the PC during restoration.

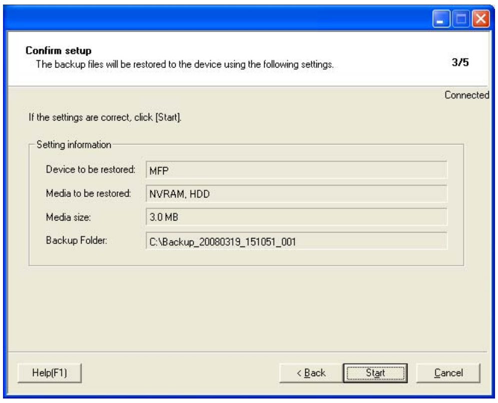
7 Click the [Next].

? 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 passwords. 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) 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

8 Check the data that has been set and click [Start].



Confirm setup
The backup files will be restored to the device using the following settings. 3/5

Connected

If the settings are correct, click [Start].

Setting information

Device to be restored: MFP

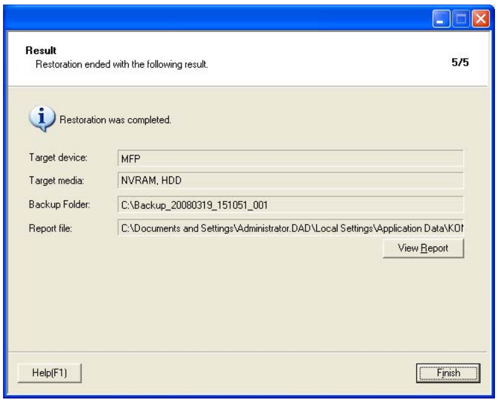
Media to be restored: NVRAM, HDD

Media size: 3.0 MB

Backup Folder: C:\Backup_20080319_151051_001

9 Click the [OK].

Make sure that Restore procedure has been completed and then click [Finish].



Result

Restoration ended with the following result.

5/5

Restoration was completed.

Target device: MFP

Target media: NVRAM, HDD

Backup Folder: C:\Backup_20080319_151051_001

Report file: C:\Documents and Settings\Administrator.DAD\Local Settings\Application Data\KOI

✎...

Reminder

Restore doesn't backup Administrator Password, CE Password, HDD Lock Password, Flash Memory Lock Password, Image Data Encryption Passphrase, and CE Lock Release Time. But please note that all other security data is backed up at restore. Especially data related security such as auth-password or priv-password, make sure to keep the back up information.

Encryption key is not backed up at restore. Therefore warning will be given for discordance of Encryption key at the time of restart after restore when the encryption word is changed. You need to set the back up encryption word again to reset the warning. Make sure to keep the back up information.