KONICA MINOLTA

The essentials of imaging

bizhub PRO 920

User's Guide

Security

- Security Functions
- Enhanced Security Mode
- Protect and Delete Data After Use
- User Authentication in Enhanced Security Mode
- HDD Store Function in Enhanced Security Mode
- Administrator Security Functions

bizhub PRO 920

Security

User's Guide

The Control Software version is as follows.

(This software consists of Image control program and Controller control program.)

Image control program (Image Control I1) version: 10-0000 or later
Controller control program (IP Control P) version: 10-0000 or later

About the Firmware version display function:

The bizhub PRO 920 Control Software (Image control program / Controller control program) version mentioned above can be confirmed by using the service representative (CE) service mode firmware version display function.

When you display the firmware version, the Image control program and Controller control program versions will be displayed as follows.

Image control program (Image Control I1) version:
2 digits + 4 zeros following the hyphen (Ex: 10-0000)
Controller control program (IP Control P) version:
2 digits + 4 zeros following the hyphen (Ex: 10-0000)

Please keep this in mind when checking the software version.

ACKNOWLEDGEMENTS:

- KONICA MINOLTA, KONICA MINOLTA Logo and the essentials of imaging are registered trademarks or trademarks of KONICA MINOLTA HOLDINGS, INC.
- bizhub PRO is a registered trademark or trademark of KONICA MINOLTA BUSINESS TECHNOLOGIES, INC.

Copyright © 2005 KONICA MINOLTA BUSINESS TECHNOLOGIES, Inc.

EXEMPTION

- No part of this manual may be used or duplicated without permission.
- Manufacturer and Sales Company will have no liability for any influences caused by using the printing system and this User’s Guide.
- The information written in this User’s Guide is subject to change without prior notice.

Composition of User's Guide

This machine is provided with the following user's guides as printed matters.

***bizhub PRO 920 User's Guide - Copier**

This guide describes an outline of the machine and copy operations.

Please refer to this guide for safety information, turning on/off the machine, paper supply, dealing with machine trouble such as paper jam, and copy operation available on the machine.

*** bizhub PRO 920 User's Guide - POD Administrator's Reference**

This guide provides you with detailed information about the machine management and how to customize the machine according to your daily use.

Please refer to this guide for a setup and management of the machine including copy paper setting, tray setting, and a network setup.

*** bizhub PRO 920 User's Guide - Network Scanner**

This guide describes the operation of the network scanner function equipped for the machine as standard.

Please refer to this guide for full information on storing data (Scan to HDD, Scan to E-Mail, Scan to FTP, Scan to SMB) or reading data.

*** bizhub PRO 920 User's Guide - Security <This book>**

This guide describes the security functions.

Please refer to this guide for how to use the Enhanced Security mode, and for detailed machine operation in Enhanced Security mode.

To operate safely, be sure to read “Section 1 Safety Information” in “bizhub PRO 920 User's Guide - Copier” before using the machine.

Contents

1 Security Functions

The bizhub PRO 920 device has two security modes.

Normal mode

Use this mode if the machine is used by a single person and there is a low possibility of illicit access and operations. This is the default mode when shipped from the factory. To use regular mode, please see the use's guide for each individual machine.

Enhanced Security mode

Use this mode if the machine is connected to a local area network, or to external networks through a telephone line or other means. An Administrator manages the device according to this user's guide, so that users can have a safe operating environment.

Your administrator is the only one who can turn the Enhanced Security mode ON and OFF, and make other changes, and your service representative will designate an administrator.

To turn the Enhanced Security mode ON, the service representative should set a CE authentication password and Administrator password for the device.

If IC-203 is not installed, you cannot set the Enhanced Security Mode to ON.

The Enhanced Security mode cannot be turned ON when the Machine NIC is activated. Please contact your service representative when using the Enhanced Security mode.

Enhanced Security mode is recommended to prevent data from being accessed or tampered with.

Environments in which Enhanced Security mode is recommended

- The device is connected to an local network, the Internet through a firewall, or the external telephone line for maintenance.
- The device is monitored by a telephone line or a network.

Creating a secure environment

For security, we recommend that supervisors and an administrator use Enhanced Security mode and establish an environment as follows.

- Where to set up the device
  Set up the device in a place where only designated personnel can operate it.
- User training
  The administrator must provide training and information to users to maintain the security of the device. Users should keep passwords set up by the administrator, and a password that they set up on their own in a secure place.
  The administrator is supposed to give the instructions for releasing the authentication function to a user when creating a Box for that user, therefore the user should perform to release the authentication function when machine operation is completed.
- Qualifications to be an administrator
  A supervisor must select a reliable person who has adequate knowledge, technical ability, and experience as an administrator, to whom to delegate administration of the device.
- Guarantee of service representative (CE)
  A supervisor or an administrator can use Enhanced Security mode after confirming that a service contract was signed with the service representative (CE).
  Clearly state in the service contract that the service representative will not engage in any fraudulent actions.
- Secure LAN
  We recommend that you use an apparatus such as WEP code (802.11×) to prevent tapping during communication when setting up a local area network.

2 Enhanced Security Mode

2.1 Description of Enhanced Security mode

The following items will have enhanced security.

- Protect and delete used data in memory and on the HDD
  There are two kinds of image data that will be saved in memory and on the HDD: AHA compressed data and uncompressed data (TIFF and PDF formats). Memory and HDD areas containing the AHA compressed data is freed up when data is deleted. However in normal mode data is not completely deleted so it could be read through illicit means. In the Enhanced Security mode, data will be completely cleared before freeing up image areas.
  Regardless of the data type (compressed or uncompressed), the image area in memory and on the HDD where the data has been saved will be freed up after it is completely overwritten by the data disrelated to the image data.
- Enhanced password
  The password is made up of 8 to 64 alphanumerical characters (case sensitive).
  If a wrong password is entered, attempts to re-try cannot be made for five seconds.
- Machine NIC setting
  When the Enhanced Security mode is ON, the Machine NIC cannot be used.
- Access to the Box with a password
  Set up a system that requires users to input an enhanced password as described above, to save data or to print data saved in the Box on the HDD.
  If an enhanced password is set up as above, security will be improved when saving scanned data in the Box. No one other than the machine manager can delete the Box or Personal Folder in which scanned data is saved, and changing the Box's attributes requires authentication with the enhanced password. In addition, authentication will be required to use scanned data saved in the Box.
- External access prohibited
  No access is allowed over telephone lines other than CS Remote Care.
- Create, save and analyze an audit log
  A history of security function operations will be created and saved. Date and time, information identifying the person who made the operation, details of the operation, and results of the operation will be saved, enabling analysis of unauthorized access. This log will be overwritten if the audit area is depleted.

- Administrator authentication
  A service representative will set up an authentication data for an administrator.
  The administrator must input a password to gain authorized access. Only one authentication string can be registered per machine.
- Administrator Setting mode
  If the Administrator Setting mode has been entered by successful administrator authentication, the setting change of various machine functions will be available on the machine.
  Be sure to exit the Administrator Setting mode if you leave in front of the machine while using the Administrator Setting mode.

2.2 Data protected by Enhanced Security mode

Data protected by Enhanced Security mode (for users) is as follows.

- Data saved in the Personal Folder (with a password)

The following data administered by the administrator will also receive enhanced protection.

- User data
- Data controlling the machine

Data that is not protected in Enhanced Security mode

When the machine is connected to PCs on a local network, passwords input in PCs are not subject to Enhanced Security mode.

To turn Enhanced Security mode ON/OFF

The administrator can turn Enhanced Security mode ON/OFF.

If Enhanced Security mode is OFF, data can potentially be accessed, so be careful.

If data is accessed in Enhanced Security mode, the administrator may not notice until he/she analyzes the audit log. Be careful when the administrator is absent for a long time.

2.3 Display when Enhanced Security mode is ON

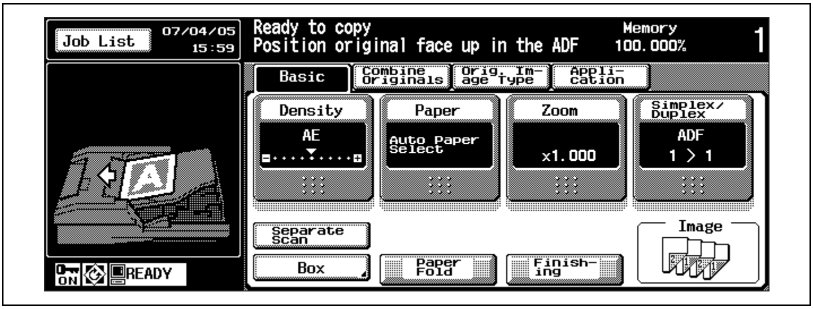
The Administrator can turn Enhanced Security mode ON/OFF.

Detail

To turn Enhanced Security mode ON/OFF, see Security Administrator Operation on page 44.

When Enhanced Security mode is ON, the enhanced security icon [ON] will appear on the Copy/Box/Scanner Basic Screens.

Copy Basic Screen



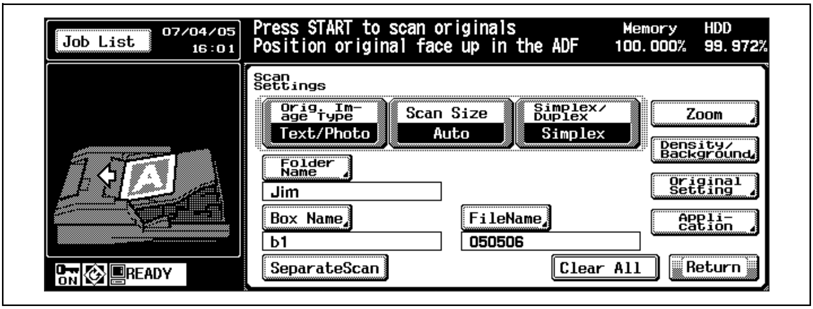
07/04/05 15:59

Ready to copy
Position original face up in the ADF

Memory 100.000% 1

Density: AE
Paper: Auto Paper Select
Zoom: x1.000
Simplex/Duplex: ADF 1 > 1

Box Basic Screen



07/04/05 16:01

Press START to scan originals
Position original face up in the ADF

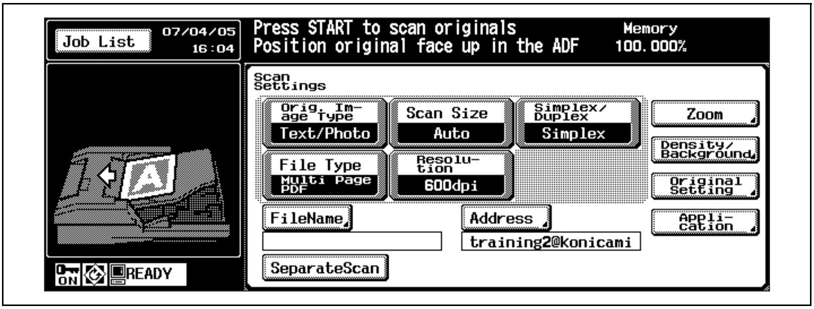
Memory 100.000% HDD 99.972%

Scan Settings

Orig. Image Type: Text/Photo
Scan Size: Auto
Simplex/Duplex: Simplex

Folder Name: Jim
Box Name: b1
FileName: 050506

Scanner Basic Screen



Job List 07/04/05 16:04

Press START to scan originals
Position original face up in the ADF

Memory 100.000%

Scan Settings

Orig. Image Type: Text/Photo

Scan Size: Auto

Simplex/Duplex: Simplex

File Type: Multi Page PDF

Resolution: 600dpi

Address: training2@konicami

Check the Enhanced Security icon on each Basic Screen to see if Enhanced Security mode is ON or OFF.

3 Protect and Delete Data After Use

Data from each mode (copy / scan / printer) will be temporarily saved in memory or on the HDD, and it will be deleted unless it is moved to a Box.

Data is compressed using a special method, so it cannot be decompressed externally.

When deleting compressed data, a part of it will be destroyed or overwritten to prevent decompression.

- Data saved temporarily in memory will be overwritten by unavailable data (NA) when the job is interrupted or ended.
- Data saved in several areas of memory will be overwritten simultaneously.
- Data in the Box will be overwritten when a delete order is issued.
- If data is sent externally, it will be overwritten when the transmission is complete.
- If the administrator issues a delete order for each Box, it will be overwritten.

4 User Authentication in Enhanced Security Mode

4.1 Description of user authentication

In Enhanced Security mode, setting up password conditions will be tougher to improve security. The administrator should set up a user name and password required for user authentication, as this is an administrator operation.

User Name: 1 to 64 alphanumerical characters
Password: 8 to 64 alphanumerical characters (case sensitive)

If a wrong password is entered, attempts to re-try cannot be made for five seconds.

✎...

Reminder
Do not use your name, birthday, employee number, etc. for a password that others can easily figure out.

If a password set in normal mode is fewer than 8 characters or more than 64 characters, you cannot use it in Enhanced Security mode.
If this happens, contact the administrator to turn OFF Enhanced Security mode, and set a new password following the above conditions.

Even after a successful access has been made, authentication with user name and password will be required under the following conditions.

- The main power switch is turned off.
- The sub power switch is turned off.
- The [Access] on the control panel is pressed.
- The [Copy]/[Scan]/[Box] on the control panel is pressed, when the User/Account Authentication Connect is turned on.
- The [Job List] on the touch panel is touched, when the User/Account Authentication Connect is turned on.
- The auto reset function operates.

Detail

When a user accesses a Box for which a password has been set in the HDD, all authentication operations with password will be saved in an audit log.

Detail

Initially, the user authentication is not available on the machine. To activate this function, the distribution number for each section should be changed. For details, see the User's guide of POD Administrator's Reference.

4.2 To register a new user

Follow the procedure below to setup a new user name and password to be required for user authentication in Enhanced Security mode.

Detail

Passwords are case sensitive.

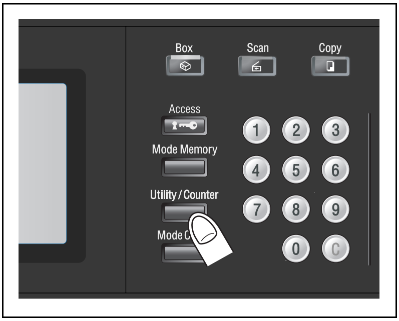
If a wrong password or fewer than 8 alphanumerical characters are entered and the [OK] is touched, the warning message "Password does not match" will appear, and no key will work for five seconds. Enter the right password after five seconds.

If authentication fails, the information will be saved in the audit log.

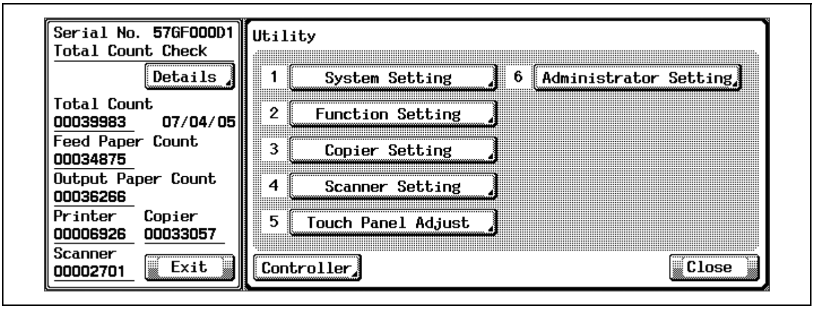
Procedure

1 Press [Utility/Counter] on the control panel.

The Utility Screen will be displayed.



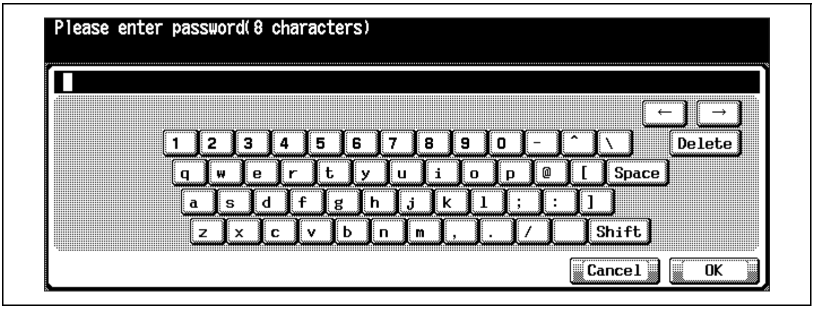
2 Touch [6 Administrator Setting].



Serial No. 57GF000D1
Total Count Check
Total Count 00039983 07/04/05
Feed Paper Count 00034875
Output Paper Count 00036266
Printer 00006926 Copier 00033057
Scanner 00002701

The Input Administrator Password Screen will be displayed.

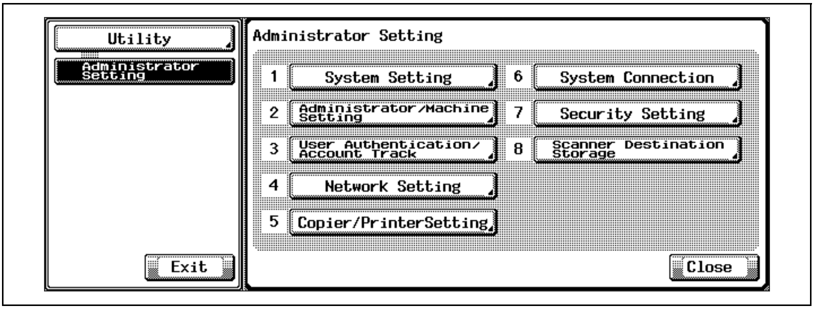
3 Enter the password.
Use the touch screen keypad to enter the 8-digit Administrator password, then touch [OK].



Please enter password(8 characters)

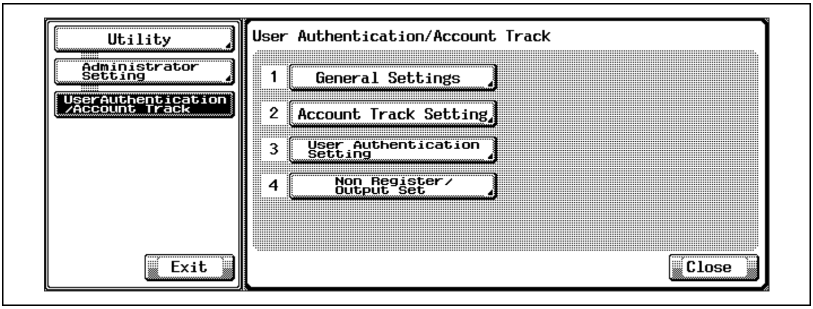
The Administrator Setting Screen will be displayed.

4 Touch [3 User Authentication/Account Track].



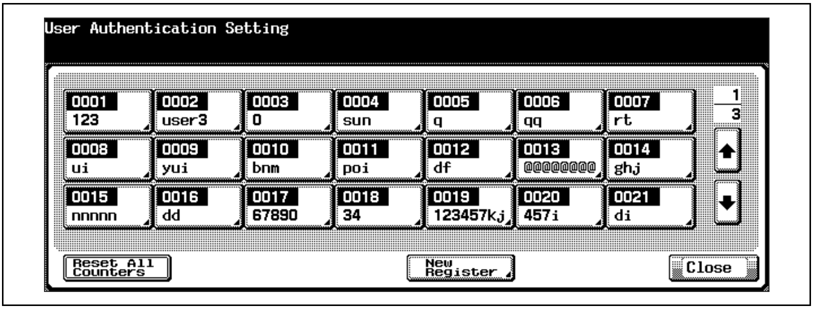
The User Authentication/Account Track Screen will be displayed.

5 Touch [3 User Authentication Setting].


Utility
Administrator Setting
UserAuthentication /Account Track
Exit
User Authentication/Account Track
1 General Settings
2 Account Track Setting
3 User Authentication Setting
4 Non Register/ Output Set
Close

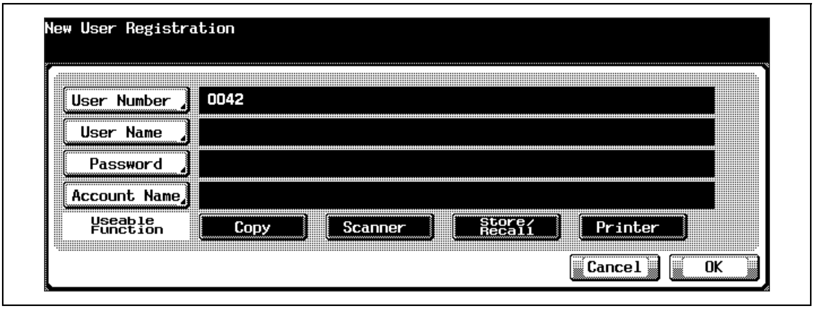
The User Authentication Setting Screen will be displayed.

6 Touch [New Register].



The New User Registration Screen will be displayed.

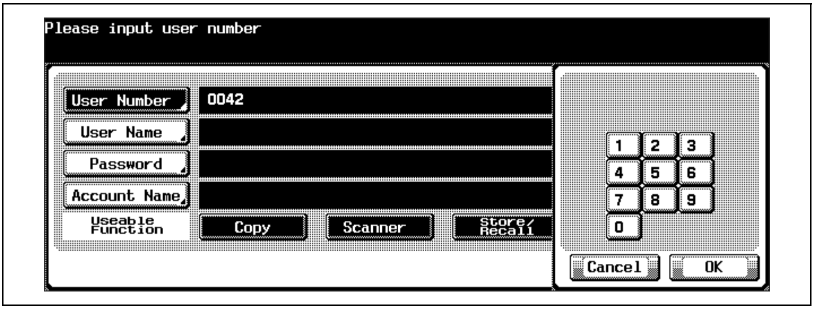
7 Touch [User Number], [User Name], [Password], or [Account Name] to display each subsequent screen, then make the desired setting.



New User Registration

User Number: 0042

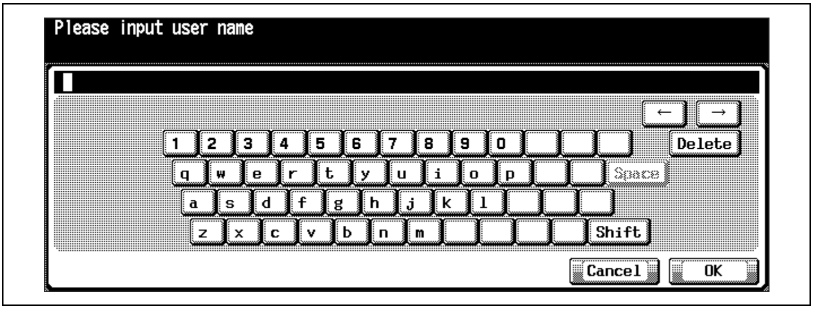
– To enter the User Number, touch [User Number] on the New User Registration Screen. Use the screen keypad on the popup menu to enter the desired user number. Touch [OK] to return to the New User Registration Screen.



Please input user number

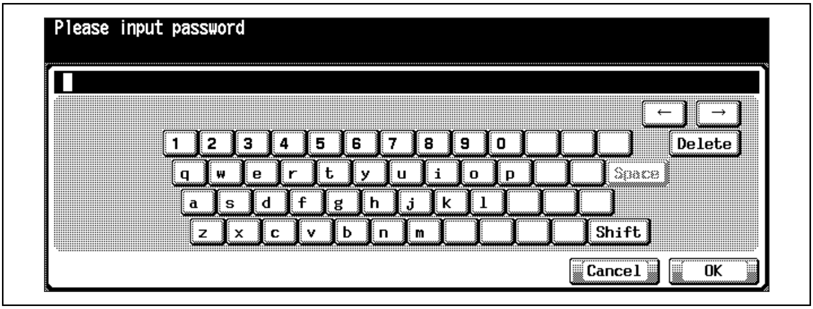
User Number: 0042

- To enter the User Name, touch [User Name] on the New User Registration Screen. Enter the desired user name from the screen keypad. Touch [OK] to return to the New User Registration Screen.



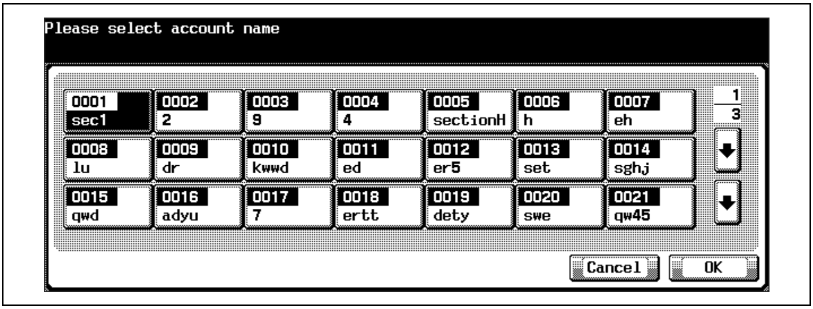
Please input user name

- To enter the Password, touch [Password] on the New User Registration Screen. Enter the desired password from the screen keypad. Touch [OK] to return to the New User Registration Screen.



Please input password

- To enter the account name, touch [Account Name] on the New User Registration Screen. Touch the desired account name key to highlight it. Touch [OK] to return to the New User Registration Screen.



Please select account name

0001 sec1	0002 2	0003 9	0004 4	0005 sectionH	0006 h	0007 eh
0008 lu	0009 dr	0010 kwwd	0011 ed	0012 er5	0013 set	0014 sghj
0015 qwd	0016 adyu	0017 7	0018 ertt	0019 dety	0020 swe	0021 qw45

8 Specify the usable function.
To prohibit a specific function, touch the key on the New User Registration Screen to release the highlight.

9 Touch [OK].
When settings are completed, touch [OK] on the New User Registration Screen.

The User Authentication Setting Screen will be restored.

4.3 To change a user data

Follow the procedure below to change a user data (user name and password) once registered.

Detail
Passwords are case sensitive.

If a wrong password or fewer than 8 alphanumerical characters are entered and the [OK] is touched, the warning message "Password does not match" will appear, and no key will work for five seconds. Enter the right password after five seconds.

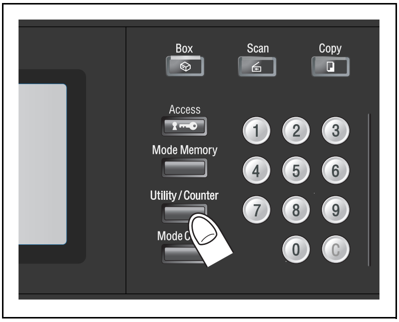
The current password cannot be used again.

If authentication fails, the information will be saved in the audit log.

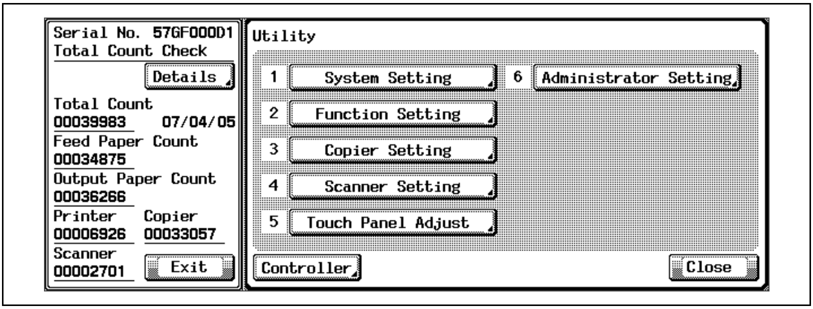
Procedure

1 Press [Utility/Counter] on the control panel.

The Utility Screen will be displayed.

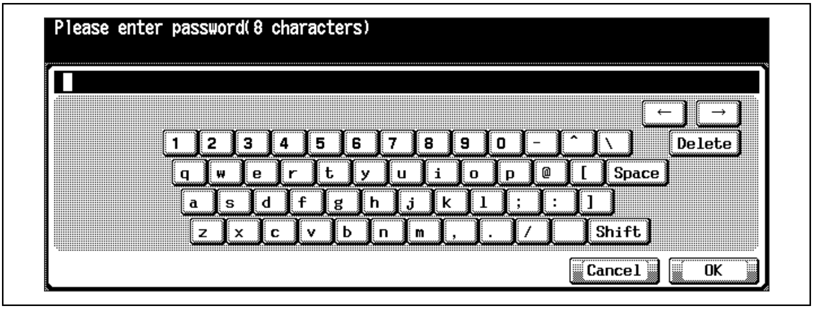


2 Touch [6 Administrator Setting].


Serial No. 57GF000D1
Total Count Check
Total Count 00039983 07/04/05
Feed Paper Count 00034875
Output Paper Count 00036266
Printer 00006926 Copier 00033057
Scanner 00002701

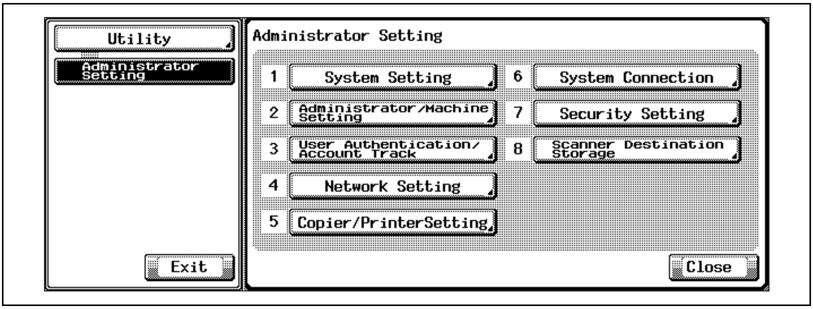
The Input Administrator Password Screen will be displayed.

3 Enter the password.
Use the touch screen keypad to enter the 8-digit Administrator password, then touch [OK].


Please enter password(8 characters)
← →
1 2 3 4 5 6 7 8 9 0 - ^ \ Delete
q w e r t y u i o p @ [Space
a s d f g h j k l ; :]
z x c v b n m , . / Shift
Cancel
OK

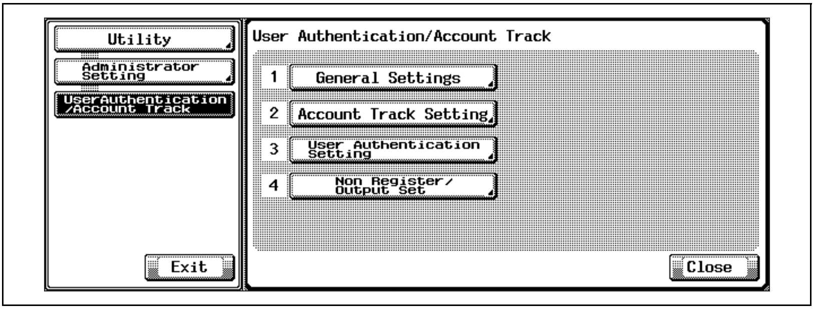
The Administrator Setting Screen will be displayed.

4 Touch [3 User Authentication/Account Track].



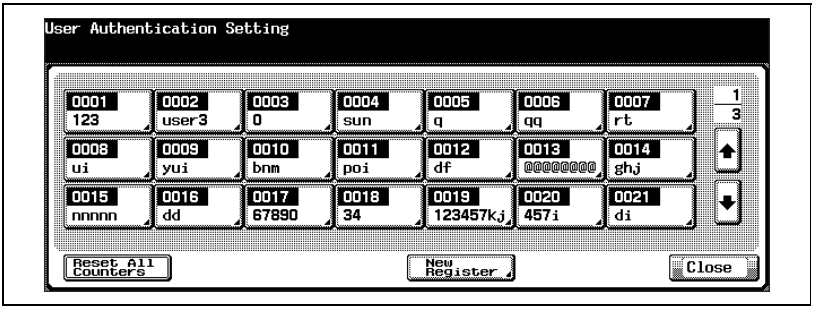
The User Authentication/Account Track Screen will be displayed.

5 Touch [3 User Authentication Setting].


Utility
Administrator Setting
UserAuthentication /Account Track
Exit
User Authentication/Account Track
1 General Settings
2 Account Track Setting
3 User Authentication Setting
4 Non Register/ Output Set
Close

The User Authentication Setting Screen will be displayed.

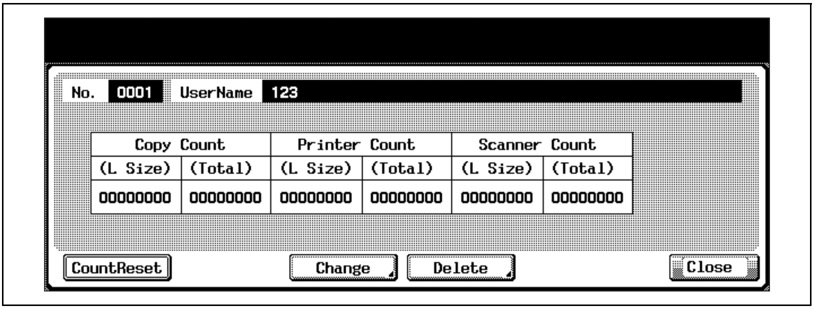
6 Touch the user name key to be changed.



0001 123	0002 user3	0003 0	0004 sun	0005 q	0006 qq	0007 rt
0008 ui	0009 yui	0010 bnm	0011 poi	0012 df	0013 @@@@@@@@	0014 ghj
0015 nnnnn	0016 dd	0017 67890	0018 34	0019 123457kj	0020 457i	0021 di

The User Count Screen will be displayed.

7 Touch [Change].

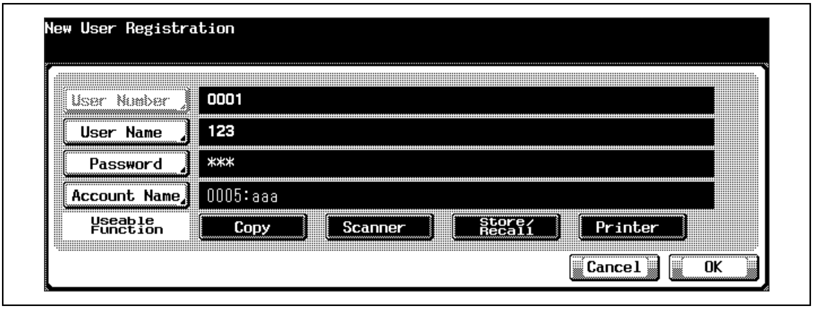


No. 0001 UserName 123

Copy Count		Printer Count		Scanner Count	
(L Size)	(Total)	(L Size)	(Total)	(L Size)	(Total)
00000000	00000000	00000000	00000000	00000000	00000000

The Change Registered User Data Screen will be displayed.

8 Touch [User Name], [Password] or [Account Name] to display each subsequent screen, then make the desired setting change.



New User Registration

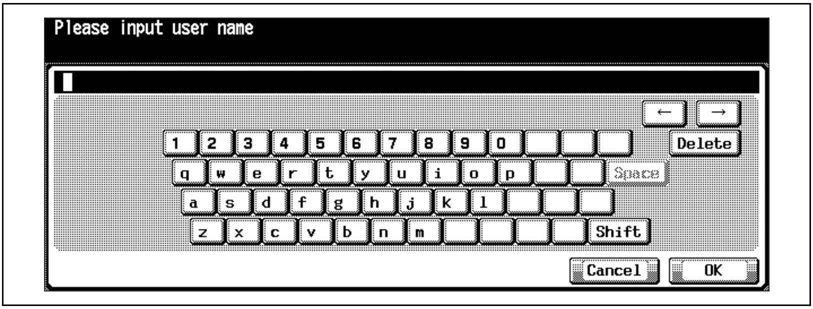
User Number: 0001

User Name: 123

Password: ***

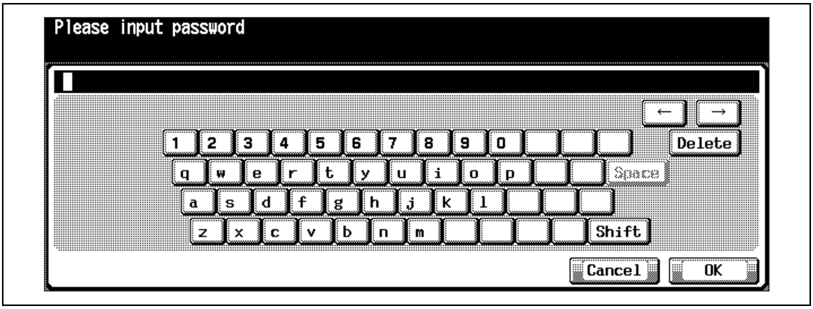
Account Name: 0005:aaa

- To change the user name, touch [User Name] on the User Registration Screen. Enter the desired user name from the screen keypad. Touch [OK] to return to the Change Registered User Data Screen.



Please input user name

- To change the Password, touch [Password] on the User Registration Screen. Enter the desired password from the screen keypad. Touch [OK] to return to the Change Registered User Data Screen.



Please input password

- To change the account name, touch [Account Name] on the User Registration Screen. Touch the desired section key to highlight it. Touch [OK] to return to the Change Registered User Data Screen.

9 Specify the usable function.
To prohibit a specific function, touch the key on the Change Registration User Data Screen to release the highlight.

10 Touch [OK].
When settings are completed, touch [OK] on the Change Registered User Data Screen.
The User Authentication Setting Screen will be restored.

4.4 To delete a user

Follow the procedure below to delete a user name, password, and also Personal Folder.

Detail
Passwords are case sensitive.

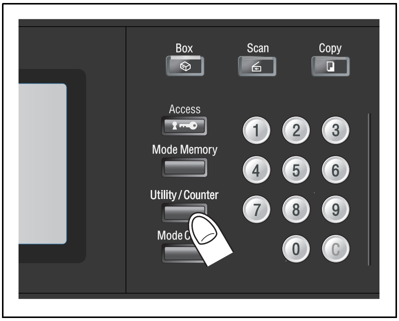
If a wrong password or fewer than 8 alphanumerical characters are entered and the [OK] is touched, the warning message "Password does not match" will appear, and no key will work for five seconds. Enter the right password after five seconds.

If authentication fails, the information will be saved in the audit log.

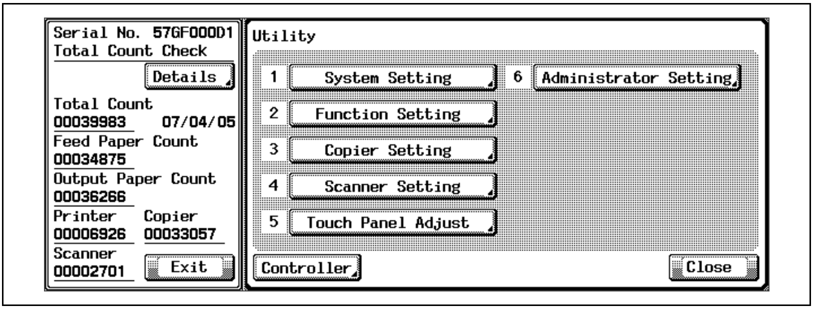
Procedure

1 Press [Utility/Counter] on the control panel.

The Utility Screen will be displayed.



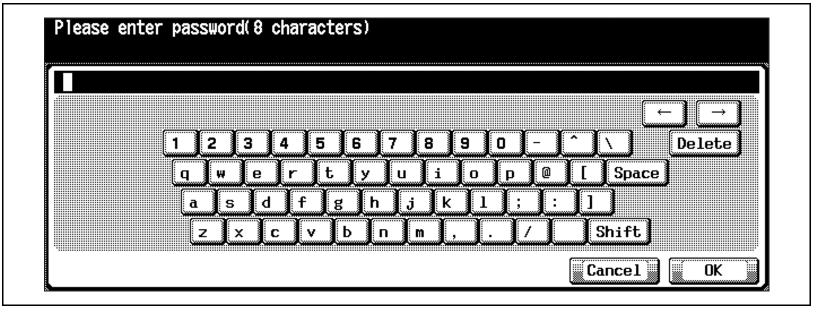
2 Touch [6 Administrator Setting].



Serial No. 57GF000D1
Total Count Check
Total Count
00039983 07/04/05
Feed Paper Count
00034875
Output Paper Count
00036266
Printer Copier
00006926 00033057
Scanner
00002701

The Input Administrator Password Screen will be displayed.

3 Enter the password.
Use the touch screen keypad to enter the 8-digit Administrator password, then touch [OK].

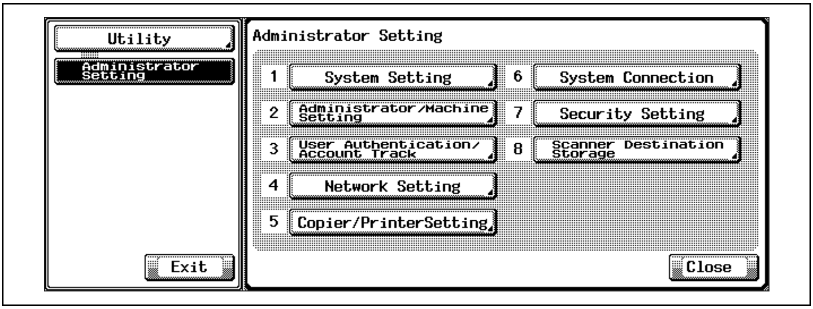


Please enter password(8 characters)

← →
1 2 3 4 5 6 7 8 9 0 - ^ \ Delete
q w e r t y u i o p @ [Space
a s d f g h j k l ; :]
z x c v b n m , . / Shift
Cancel
OK

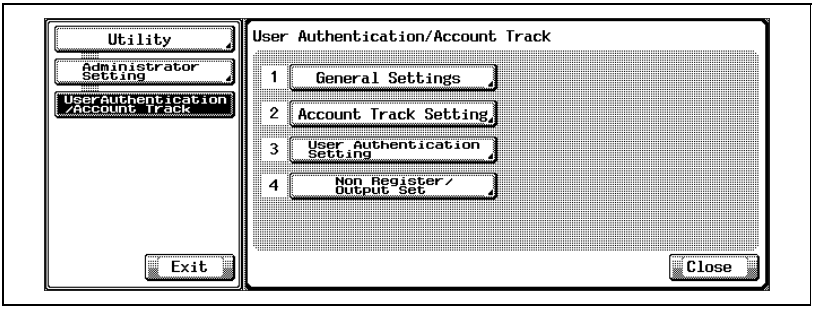
The Administrator Setting Screen will be displayed.

4 Touch [3 User Authentication/Account Track].



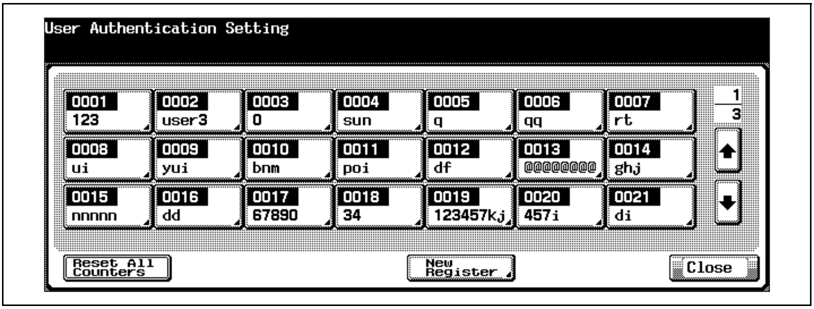
The User Authentication/Account Track Screen will be displayed.

5 Touch [3 User Authentication Setting].


Utility
Administrator Setting
UserAuthentication /Account Track
Exit
User Authentication/Account Track
1 General Settings
2 Account Track Setting
3 User Authentication Setting
4 Non Register/ Output Set
Close

The User Authentication Setting Screen will be displayed.

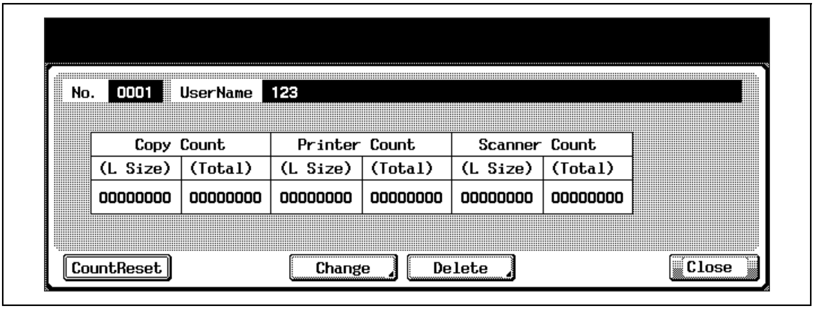
6 Touch the user name key to be deleted.


User Authentication Setting

0001 123	0002 user3	0003 0	0004 sun	0005 q	0006 qq	0007 rt
0008 ui	0009 yui	0010 bnm	0011 poi	0012 df	0013 @@@@@@@@	0014 ghj
0015 nnnnn	0016 dd	0017 67890	0018 34	0019 123457kj	0020 457i	0021 di

The User Count Screen will be displayed.

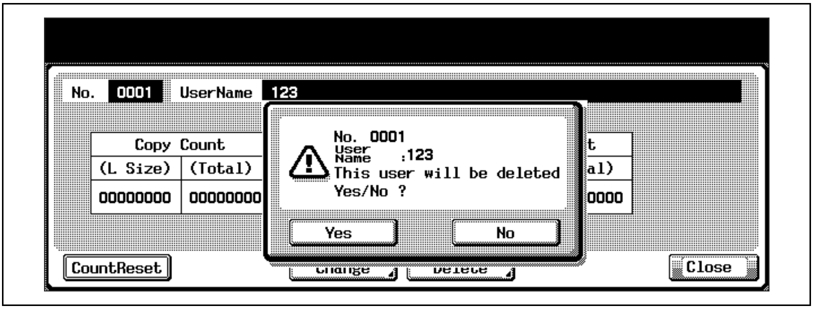
7 Touch [Delete].


No. 0001 UserName 123

Copy Count		Printer Count		Scanner Count	
(L Size)	(Total)	(L Size)	(Total)	(L Size)	(Total)
00000000	00000000	00000000	00000000	00000000	00000000

The popup menu will be displayed to confirm that the selected user will be deleted.

8 Touch [Yes].



No. 0001 UserName 123

Copy Count	
(L Size)	(Total)
00000000	00000000

No. 0001
User Name :123
This user will be deleted
Yes/No ?

The selected user name and password will be deleted. Also the personal folder that belongs to the user will be deleted together.

4.5 To change password by user

General users can change the password that has already been set for user authentication.
We recommend that a user himself/herself changes the password assigned by the administrator for security.

Detail
Passwords are case sensitive.

If a wrong password or fewer than 8 alphanumerical characters are entered and the [OK] is touched, the warning message "Password does not match" will appear, and no key will work for five seconds. Enter the right password after five seconds.

If authentication fails, the information will be saved in the audit log.

✎...
Reminder
Do not use your name, birthday, employee number, etc. for a password that others can easily figure out.

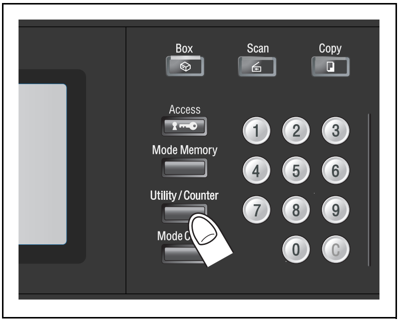
Detail
If password setup doesn't proceed successfully, the information will be saved in the audit log.

The password currently used cannot be entered as a new password.

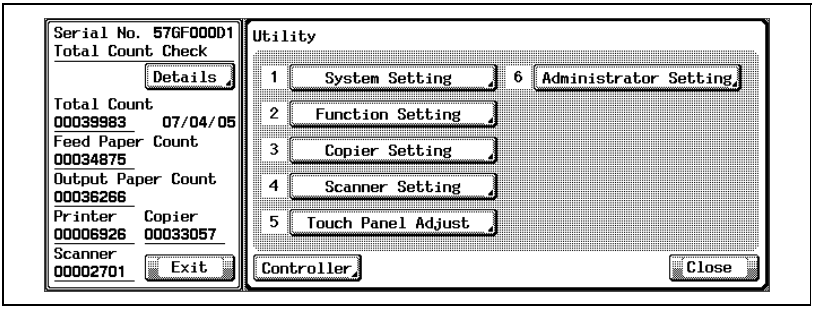
Procedure

1 Press [Utility/Counter] on the control panel.

The Utility Screen will be displayed.



2 Touch [1 System Setting].

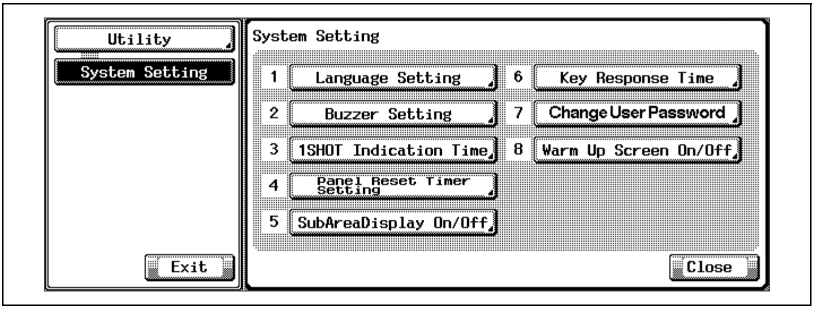


Serial No. 57GF000D1
Total Count Check

Total Count
00039983 07/04/05
Feed Paper Count
00034875
Output Paper Count
00036266
Printer 00006926 Copier 00033057
Scanner
00002701

The System Setting Screen will be displayed.

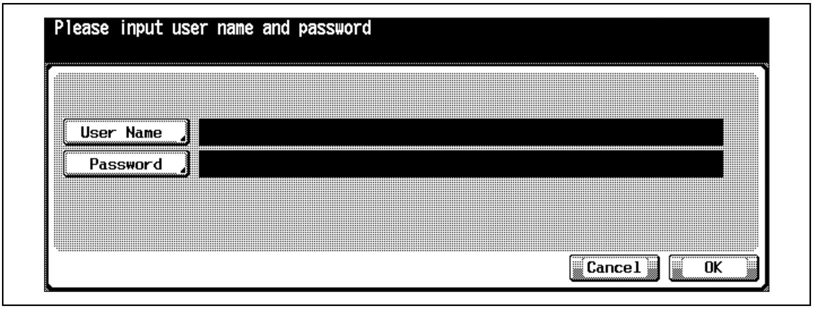
3 Touch [7 Change User Password].



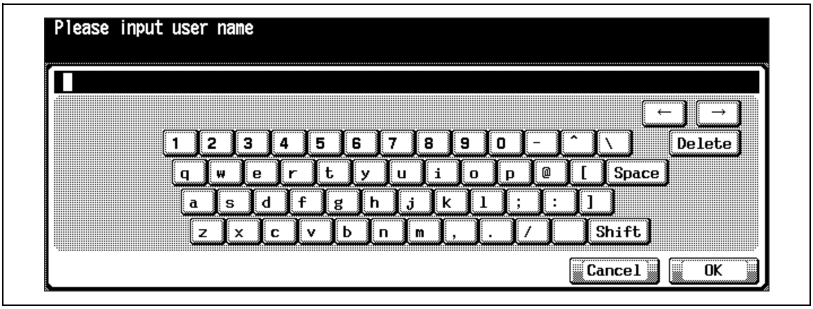
The User Authentication Screen will be displayed.

4 Enter your user name.

- Touch [User Name] to display the Input User Name Screen.


Please input user name and password

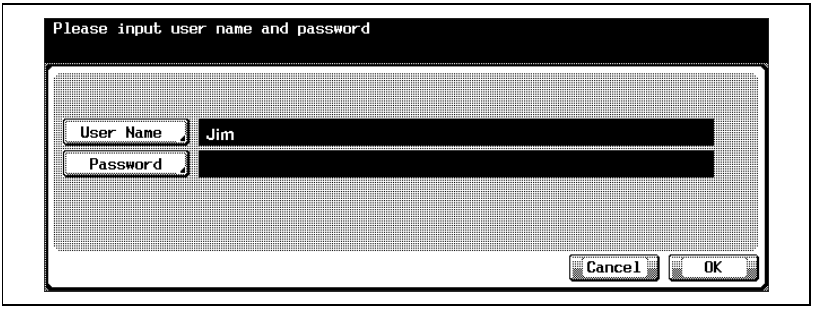
- Enter your user name, then touch [OK] to return to the User Authentication Screen.


Please input user name

The entered name will be displayed on the screen.

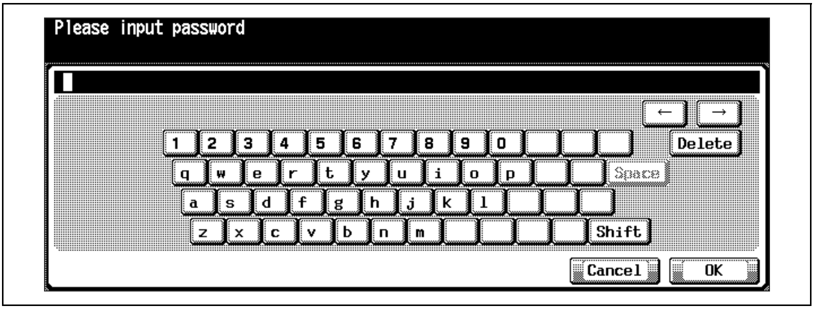
5 Enter your current password.

- Touch [Password] to display the Input User Password Screen.


Please input user name and password

User Name: Jim

– Enter your current password. The entered password will appear as asterisks (********) on the screen. Then touch [OK].

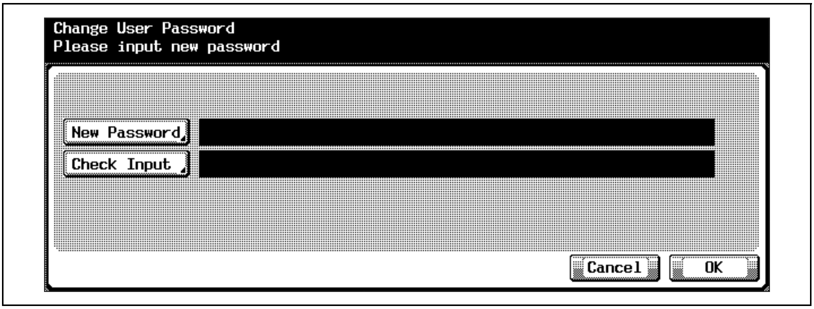


Please input password

The Change User Password Screen will be displayed.

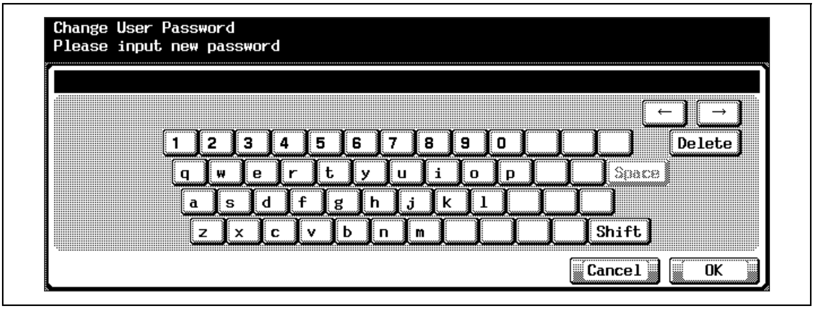
6 Enter your new password.

– Touch [New Password] to display the Input New Password Screen.



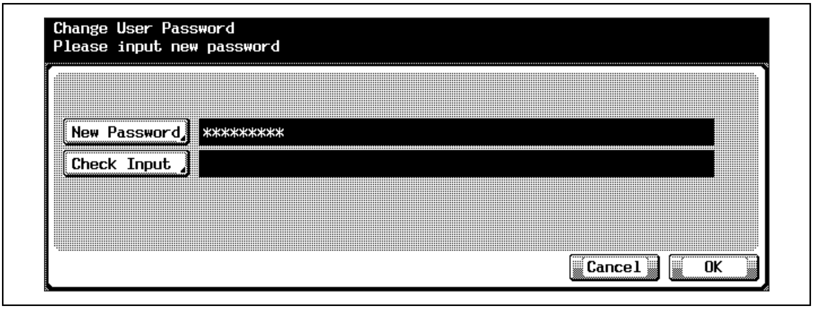
Change User Password
Please input new password

– Enter your new password, then touch [OK].



Change User Password
Please input new password

– Touch [Check Input] to display the Re-input New Password Screen.

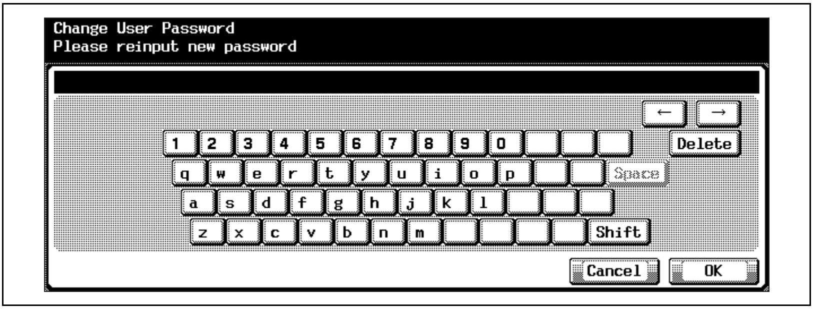


Change User Password
Please input new password

New Password **********

Check Input

– Enter your new password once more for confirmation, then touch [OK].



Change User Password
Please reinput new password

The Change User Password Screen will be restored.

7 Touch [OK].

The System Setting Screen will be restored.

5 HDD Store Function in Enhanced Security Mode

A Box built on the HDD is used to store the scanned data. To prevent the data from being accessed or tampered with, we recommend using the Box with a password specified.
Never fail to use the Enhanced Security mode when storing any secret document.
If the Enhanced Security mode is turned off temporarily for some reason, the administrator should tell that to all users.
For details to store and output the scanned data in a Box, see the User's guide of Network Scanner.

5.1 Store the data in a Box while Copying

The following is a detailed explanation of how to store the data in a Box and output in Enhanced Security mode for which a user name and password have been set.

Detail

Passwords are case sensitive.

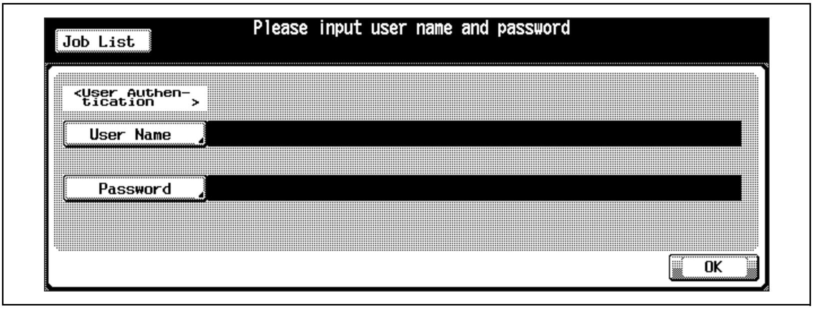
If a wrong password or fewer than 8 alphanumerical characters are entered and the [OK] is touched, the warning message "Password does not match" will appear, and no key will work for five seconds. Enter the right password after five seconds.

If authentication fails, the information will be saved in the audit log.

Procedure

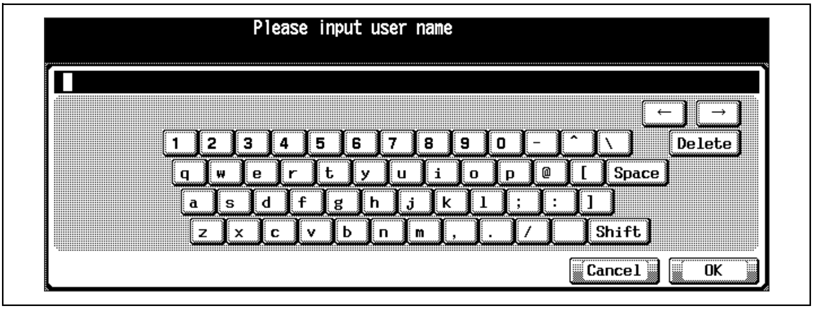
1 Enter your user name and user password on the User Authentication Screen.

- Touch [User Name] to display the Input User Name Screen.



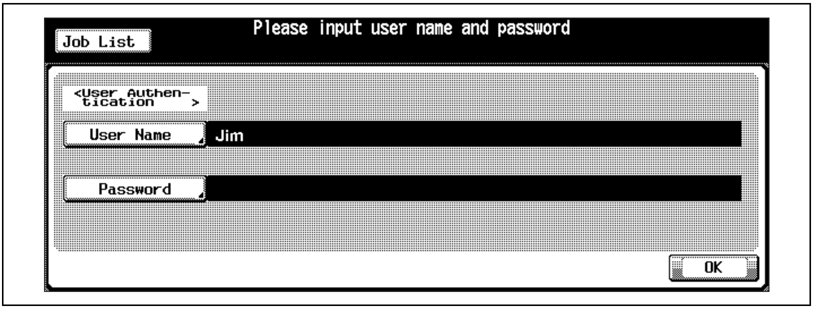
Please input user name and password

- Enter your user name, then touch [OK] to return to the User Authentication Screen.



Please input user name

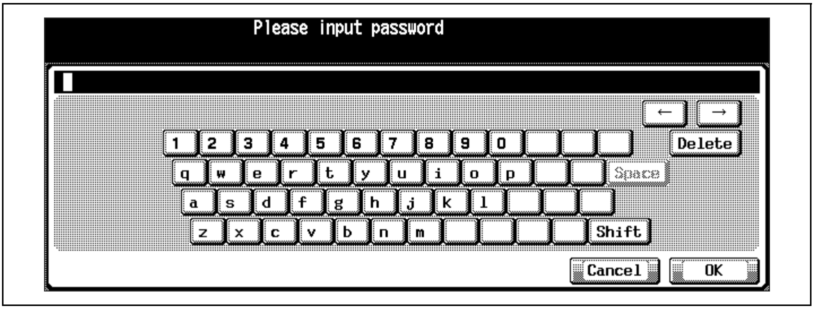
- Touch [Password] to display the Input User Password Screen.



Please input user name and password

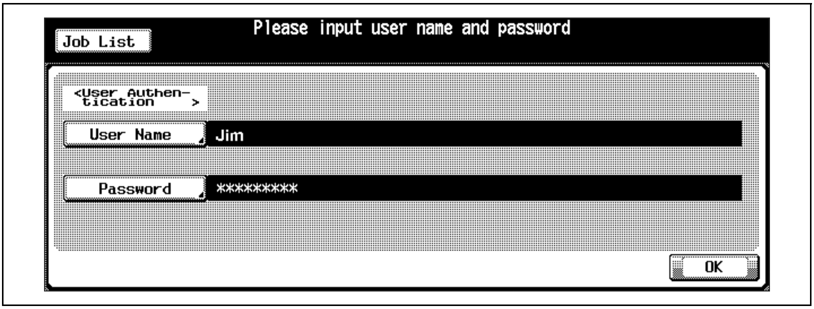
User Name: Jim

– Enter your user passwor, then touch [OK] to return to the User Authentication Screen



Please input password

2 Touch [OK] on the User Authentication Screen.



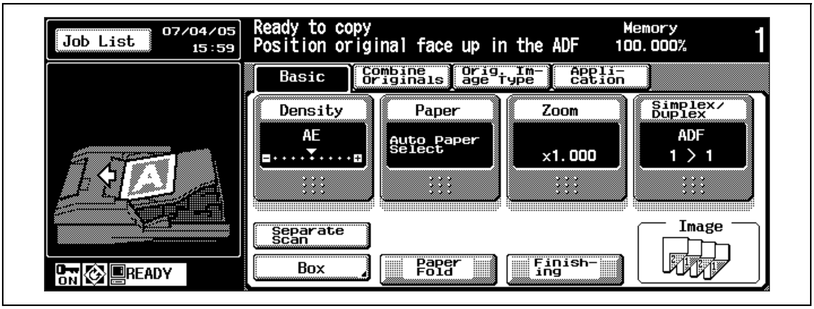
Please input user name and password

User Name Jim

Password **********

The Copy Basic Screen will be displayed.

3 Touch [Box] on the Copy Basic Screen.



07/04/05 15:59

Ready to copy
Position original face up in the ADF

Memory 100.000%

Density AE

Paper Auto Paper Select

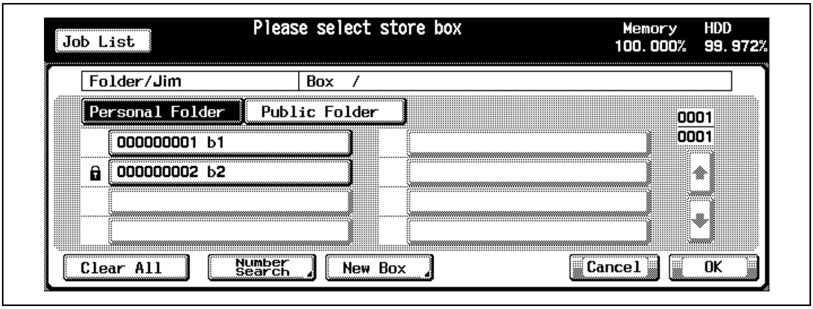
Zoom x1.000

Simplex/Duplex ADF 1 > 1

READY

The Store Box Selection Screen will be displayed.

4 Select the desired personal Box, then touch [OK].



Please select store box

Memory 100.000% HDD 99.972%

Folder/Jim | Box /

000000001 b1

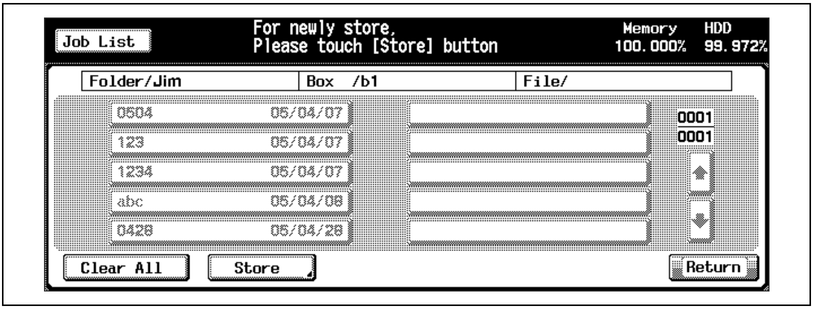
000000002 b2

0001
0001

– Enter the password if selected Box requires one.

The Personel File Screen will be displayed.

5 Touch [Store].



For newly store,
Please touch [Store] button

Memory 100.000% HDD 99.972%

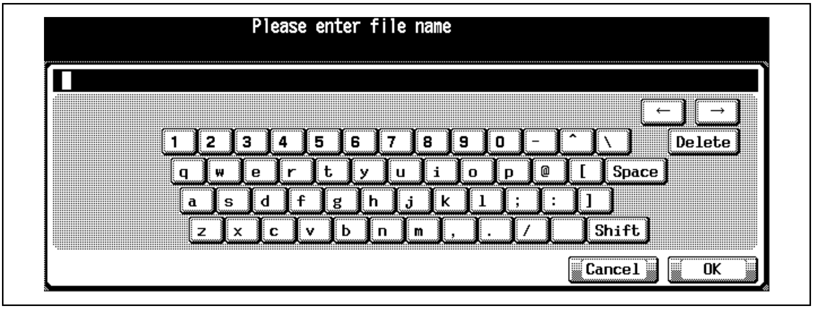
Folder/Jim | Box /b1 | File/

0504	05/04/07
123	05/04/07
1234	05/04/07
abc	05/04/08
0428	05/04/28

0001
0001

The Input File Name Screen will be displayed.

6 Enter the file name, then touch [OK].



Please enter file name

The Basic Screen will be restored.

7 Press [Start] on the control panel to scan.

After scanning all the originals, the machine automatically starts to print and store the data in a Box.

Scan
Copy
Reset
Interrupt
Proof Copy
Stop
Start
1
2
3
4
5
6
7
8
9
0
C
Data
Main Power

8 When operation is completed, press [Access] on the control panel.

The User Authentication Screen will be displayed to prohibit the machine operation without entering a user name and password.

5.2 Store scanned data in a Box

The following is a detailed explanation of how to store scanned data in a Box in Enhanced Security mode.

Detail
Passwords are case sensitive.

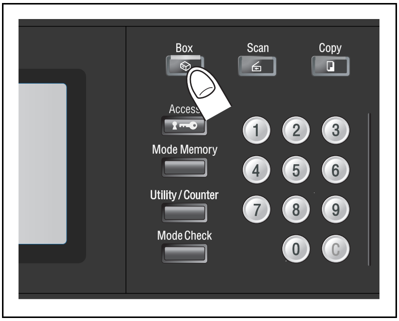
If a wrong password or fewer than 8 alphanumerical characters are entered and the [OK] is touched, the warning message "Password does not match" will appear, and no key will work for five seconds. Enter the right password after five seconds.

If authentication fails, the information will be saved in the audit log.

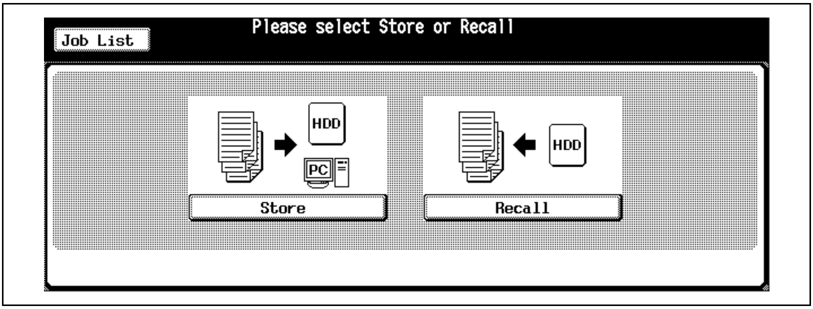
Procedure

1 Press [Box] on the control panel.

The Image Data Store/Recall Screen will be displayed.



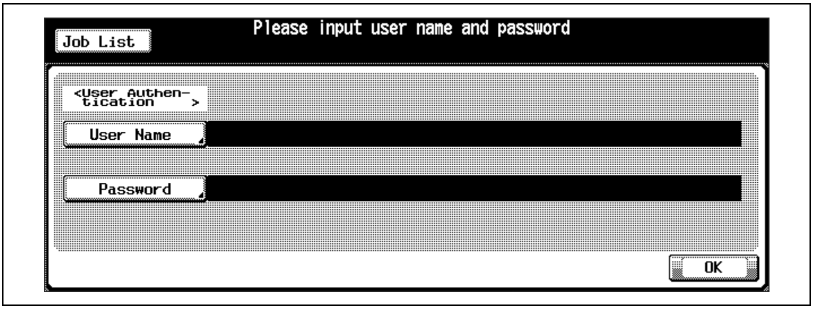
2 Touch [Store].



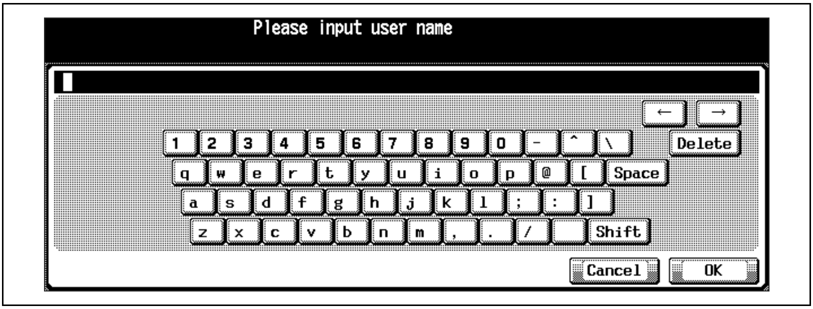
The User Authentication Screen will be displayed.

3 Enter your user name and user password on the User Authentication Screen.

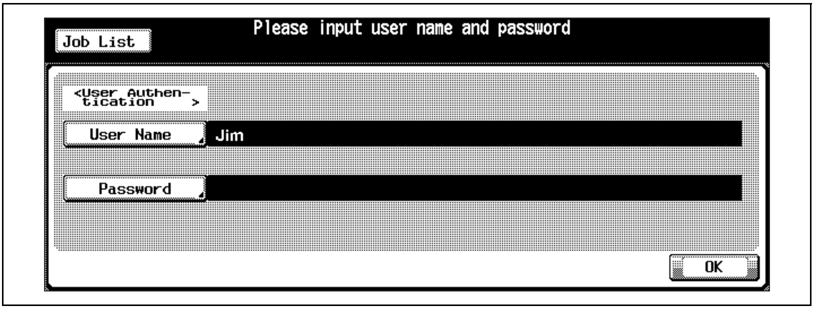
- Touch [User Name] to display the Input User Name Screen.



- Enter your user name, then touch [OK] to return to the User Authentication Screen.



- Touch [Password] to display the Input User Password Screen.

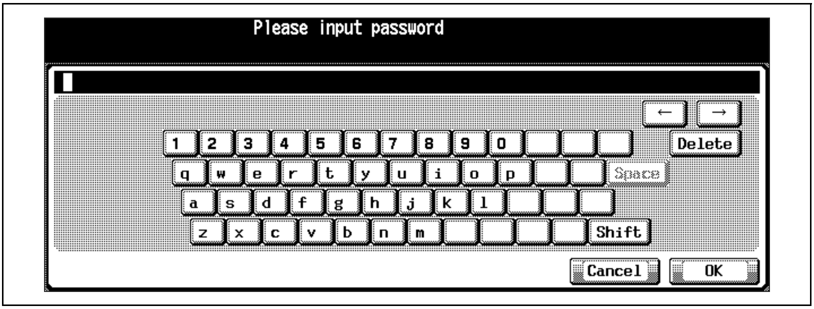


Please input user name and password

User Name Jim

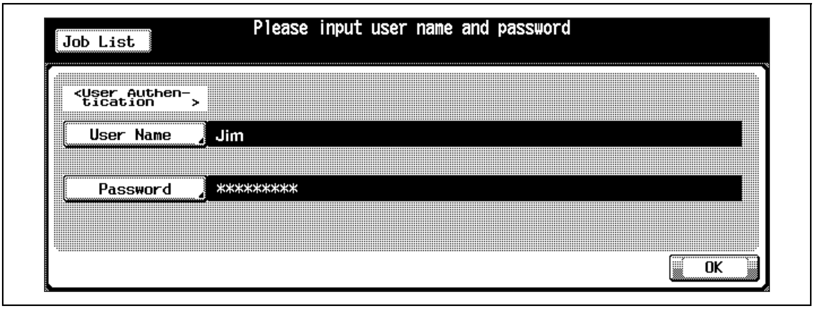
Password

- Enter your user password, then touch [OK] to return to the User Authentication Screen.



Please input password

4 Touch [OK] on the User Authentication Screen.



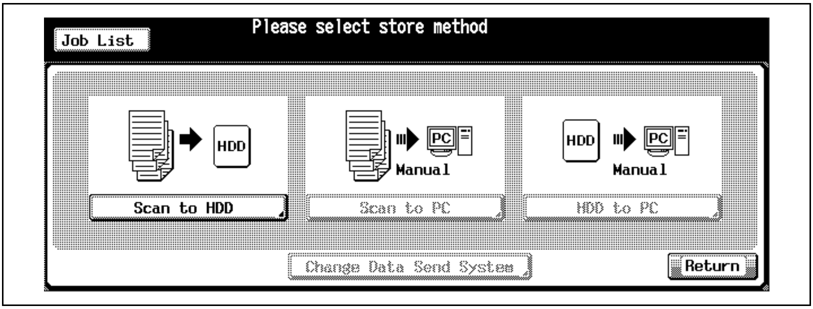
Please input user name and password

User Name Jim

Password *********

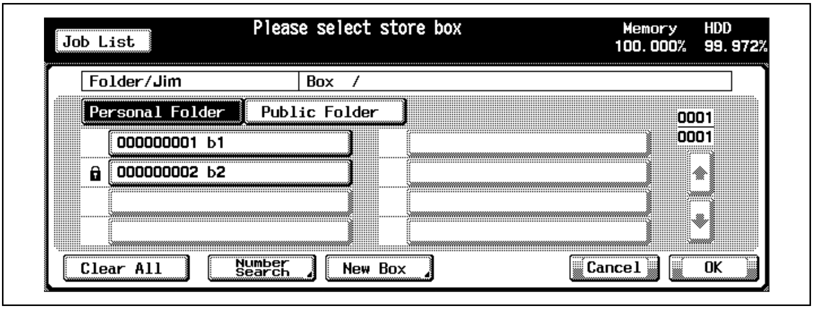
The Image Data Store Site Selection Screen will be displayed.

5 Touch [Scan to HDD].


Please select store method

The HDD Box List Screen will be displayed.

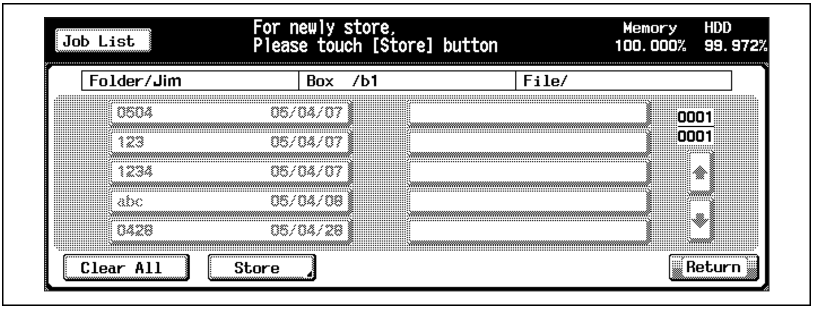
6 Select the desired personal Box, then touch [OK].


Please select store box
Memory 100.000%
HDD 99.972%
Folder/Jim
Box /

– Enter the password if selected Box requires one.

The Personal File Screen will be displayed.

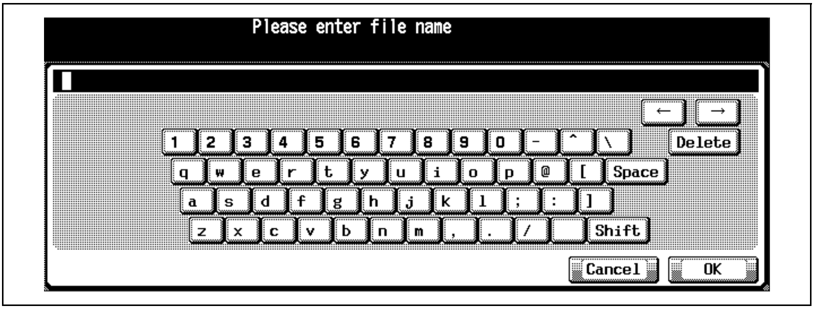
7 Touch [Store].


For newly store,
Please touch [Store] button
Memory 100.000%
HDD 99.972%
Folder/Jim
Box /b1
File/

0504	05/04/07
123	05/04/07
1234	05/04/07
abc	05/04/08
0428	05/04/28

The Input File Name Screen will be displayed.

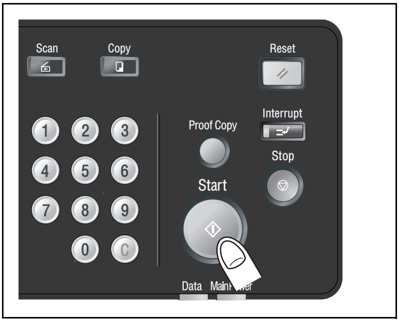
8 Enter the file name, then touch [OK].


Please enter file name

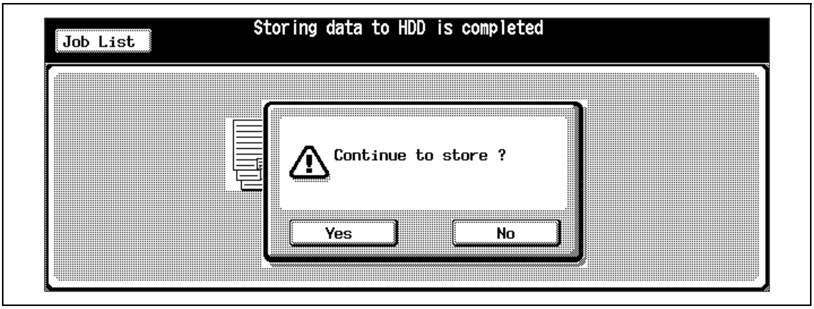
The Box Basic Screen will be displayed.

9 Press [Start] on the control panel to scan and store the image data.

The popup menu to confirm whether to continue or close it will be displayed.



10 Touch [Yes] or [No].


Storing data to HDD is completed

Continue to store ?

- To continue to store the next image data, touch [Yes]. The Input File Name Screen will be restored.
- To close, touch [No]. The User Authentication Screen will be displayed.

11 When operation is completed, press [Access] on the control panel.

The User Authentication Screen will be displayed to prohibit the machine operation without entering a user name and password.

5.3 Recall/Delete data in a Box

The following is a detailed explanation of how to recall or delete the data stored in a Box.

Detail

Passwords are case sensitive.

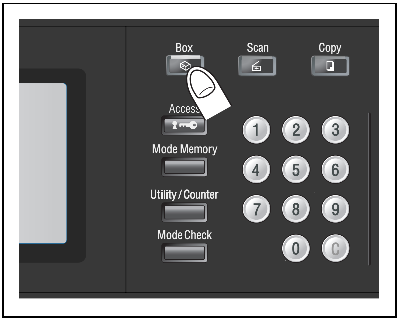
If a wrong password or fewer than 8 alphanumerical characters are entered and the [OK] is touched, the warning message "Password does not match" will appear, and no key will work for five seconds. Enter the right password after five seconds.

If authentication fails, the information will be saved in the audit log.

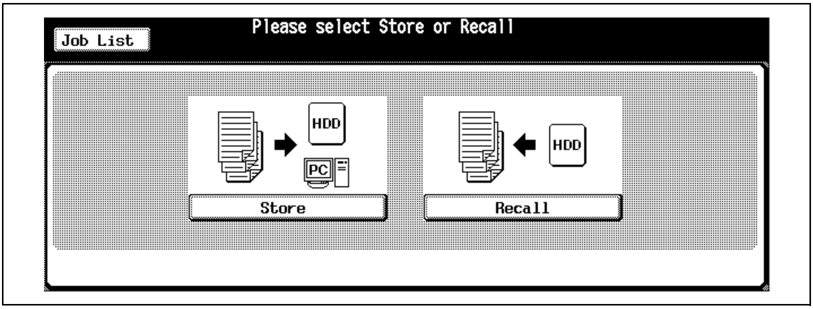
Procedure

1 Press [Box] on the control panel.

The Image Data Store/Recall Screen will be displayed.



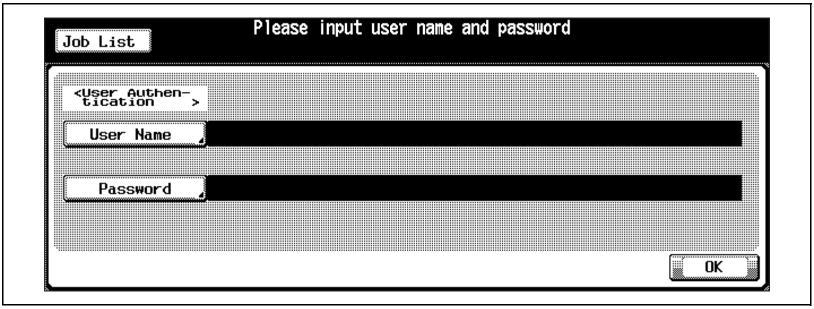
2 Touch [Recall].


Please select Store or Recall

The User Authentication Screen will be displayed.

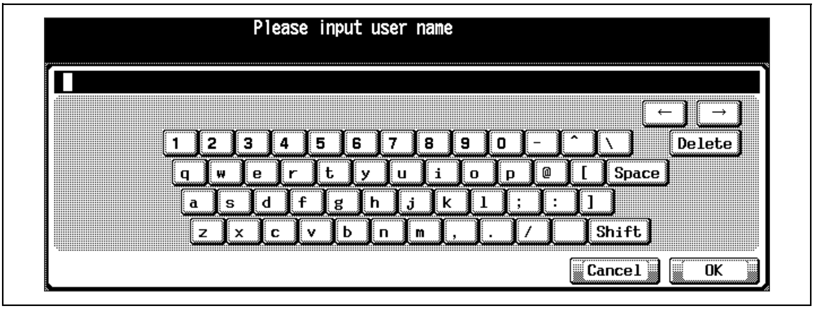
3 Enter your user name and user password on the User Authentication Screen.

– Touch [User Name] to display the Input User Name Screen.



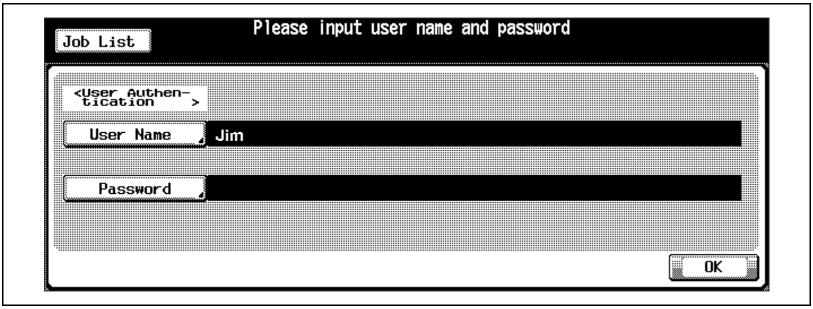
Please input user name and password

– Enter your user name, then touch [OK] to return to the User Authentication Screen.



Please input user name

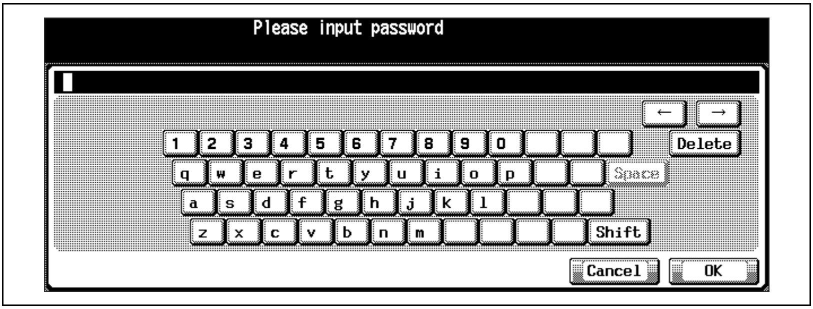
– Touch [Password] to display the Input User Password Screen.



Please input user name and password

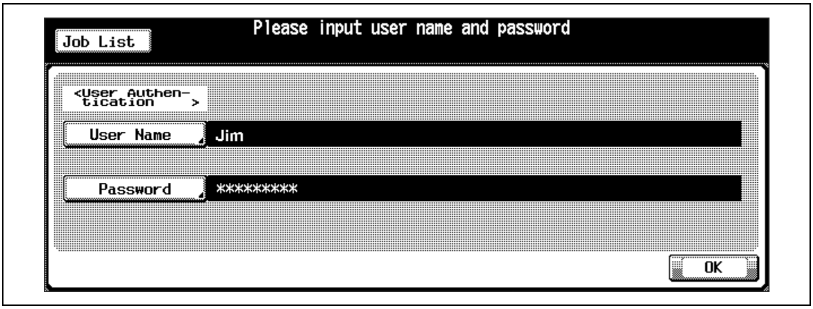
User Name: Jim

– Enter your user password, then touch [OK] to return to the User Authentication Screen.



Please input password

4 Touch [OK] on the User Authentication Screen.



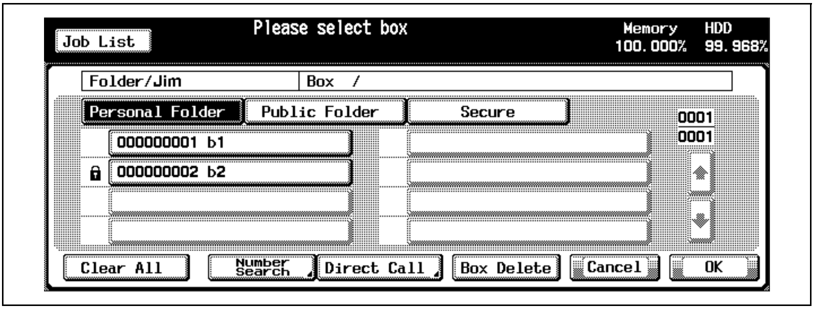
Please input user name and password

User Name: Jim

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

The Recall Box Selection Screen will be displayed.

5 Select the desired personal Box.



Please select box

Memory 100.000% HDD 99.968%

Folder/Jim | Box /

000000001 b1

000000002 b2

0001
0001

Enter the password if selected Box requires one.

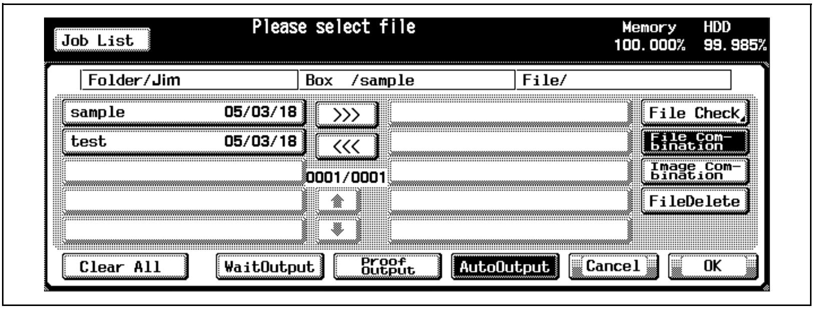
6 Touch [OK].

The Personal Box File Selection Screen will be displayed.
Proceed to step 7 if recalls the image data file.

Proceed to step 8 if deletes the image data file.

7 Recall the image data.

- Touch the desired file key, then touch [>>>]. To output the image data, touch [Wait Output], [Proof Output], or [Auto Output], as desired, and then touch [OK].



Please select file

Memory 100.000% HDD 99.985%

Folder/Jim | Box /sample | File/

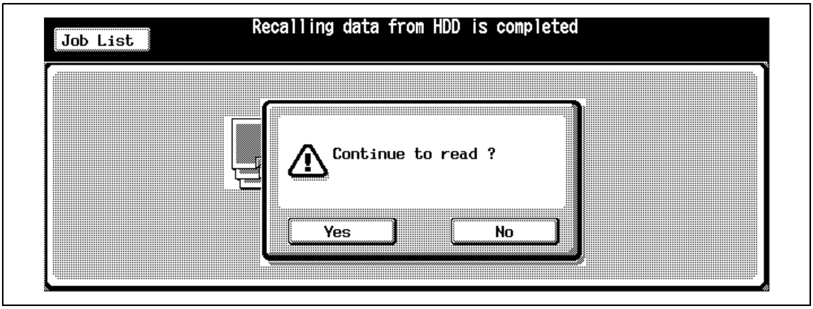
sample 05/03/18

test 05/03/18

0001/0001

- Enter the desired print quantity from touch panel keypad on the Input Print Quantity Screen.

- After outputting, the popup menu to confirm whether to continue or close it will be displayed. To continue to recall the next image data, touch [Yes]. The Personal Box File Selection Screen will be restored. To close, touch [No]. The Image Data Store/Recall Screen will be displayed.

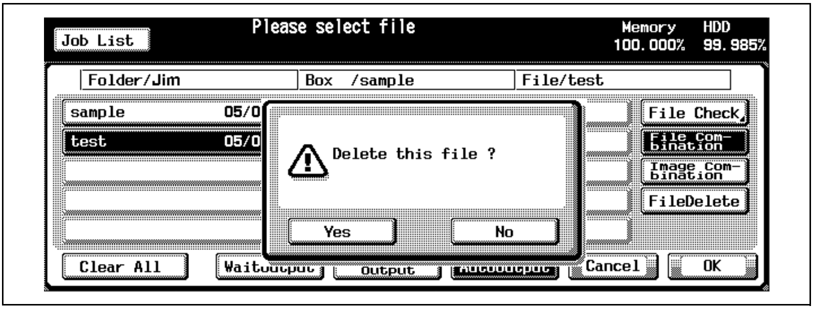


Recalling data from HDD is completed

Continue to read ?

8 Delete the image data.

- Touch the desired file key, then touch [File Delete]. The popup menu to confirm will be displayed. Touch [Yes] to delete the selected file. Touch [No] to display the Image Data Store/Recall Screen.



Please select file

Memory 100.000% HDD 99.985%

Folder/Jim Box /sample File/test

sample 05/0

test 05/0

Delete this file ?

9 When operation is completed, press [Access] on the control panel.

The User Authentication Screen will be displayed to prohibit the machine operation without entering a user name and password.

5.4 Output data in the Secure Box

Secure printing using a PC:

To set up data output using the secure printing function on PC, a secure folder with a specific password must be prepared. Enter the secure folder name made up of max. 8 alphanumerical characters.

Detail

Passwords are case sensitive.

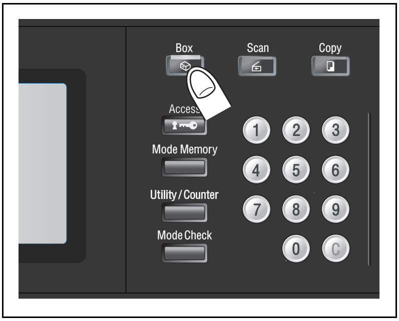
If a wrong password or fewer than 8 alphanumerical characters are entered and the [OK] is touched, the warning message "Password does not match" will appear, and no key will work for five seconds. Enter the right password after five seconds.

If authentication fails, the information will be saved in the audit log.

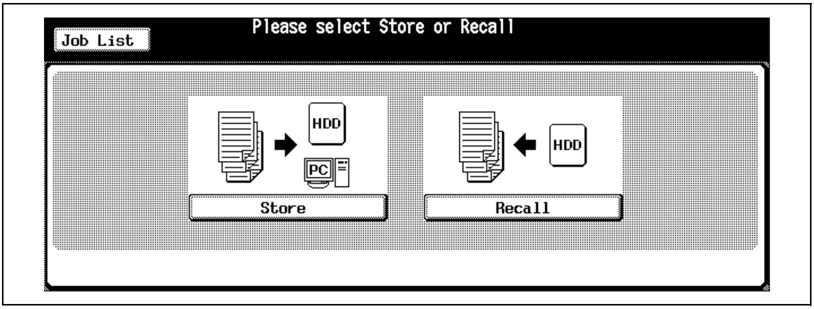
Outputting secure printing using a PC: printing on the machine:

1 Press [Box] on the control panel.

The Image Data Store/Recall Screen will be displayed.



2 Touch [Recall].

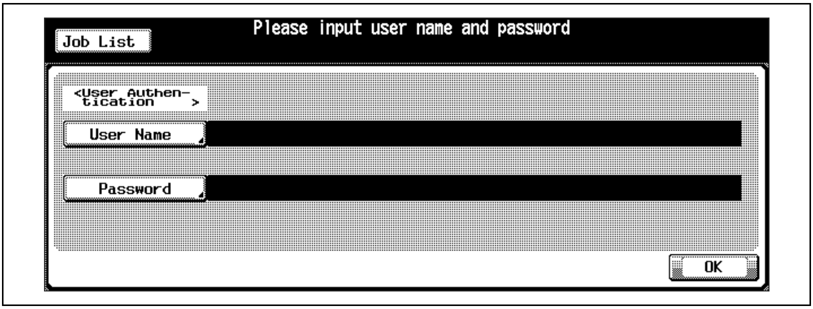


Please select Store or Recall

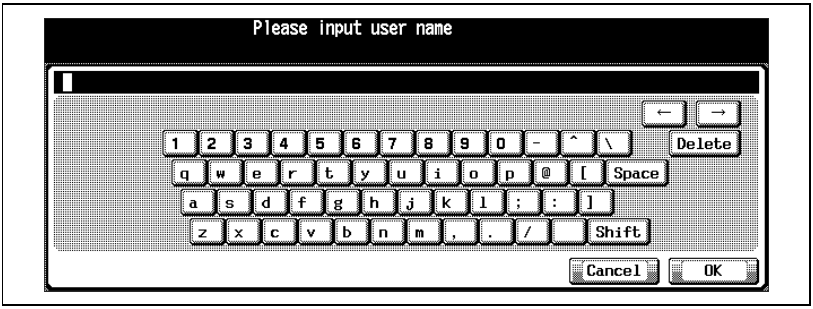
The User Authentication Screen will be displayed.

3 Enter your user name and user password on the User Authentication Screen.

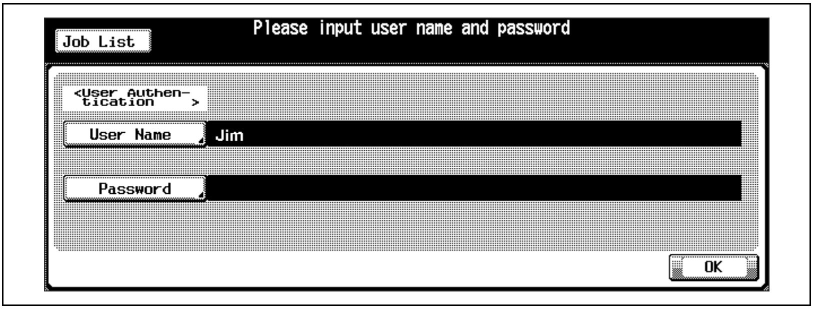
- Touch [User Name] to display the Input User Name Screen.



- Enter your user name, then touch [OK] to return to the User Authentication Screen.

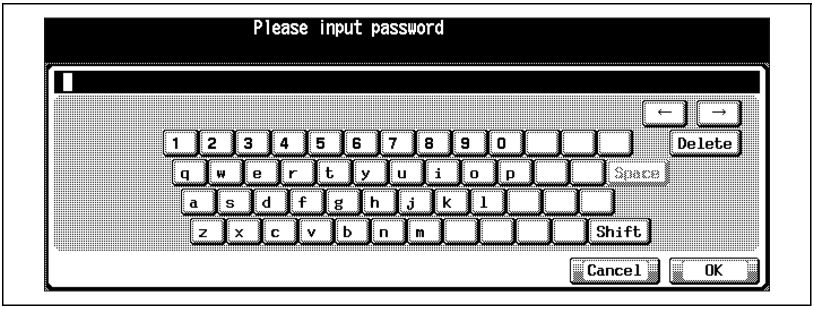


- Touch [Password] to display the Input User Password Screen.

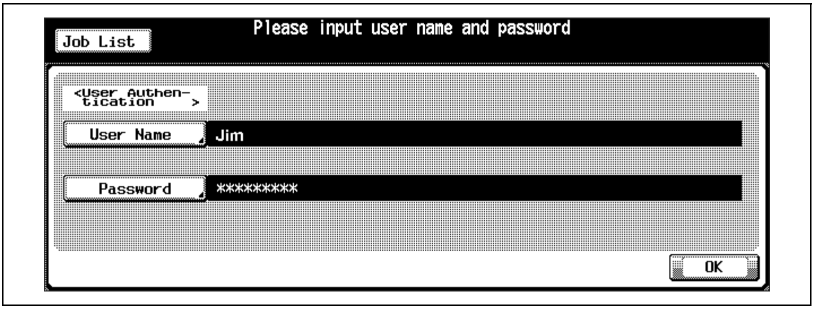


User Name Jim

– Enter your user password, then touch [OK] to return to the User Authentication Screen.



4 Touch [OK] on the User Authentication Screen.

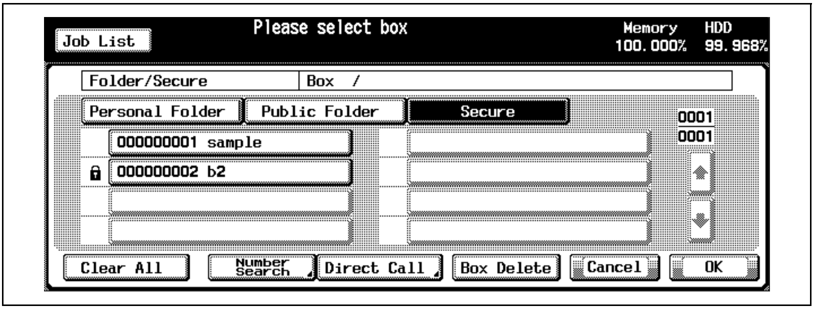


User Name Jim

Password **********

The Recall Box Selection Screen will be displayed.

5 Touch [Secure] to display the Secure Box List Screen.



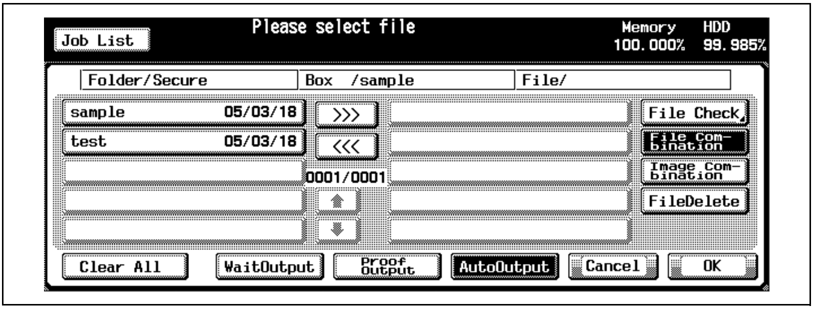
6 Select the desired secure box.

7 Enter the secure password setup in secure printing.

8 Touch [OK].

The Secure File List Screen will be displayed.

9 Select the desired secure file.
Touch the desired secure file key, then touch [>>>].



Please select file

Memory 100.000% HDD 99.985%

Folder/Secure | Box /sample | File/

sample	05/03/18
test	05/03/18

0001/0001

10 Secure printing will start.
Touch [Wait Output], [Proof Output], or [Auto Output], as desired.

6 Administrator Security Functions

To do so, an 8-digit CE authentication password and Administrator password must be set for the machine. Ask your authorized service representative to set up an Administrator password. To change this password, the administrator himself should operate the procedure described in the User's Guide of POD Administrator's reference.
To protect data in the machine from access and tampering, it is recommended to designate an administrator and use Enhanced Security mode.

6.1 Turn Enhanced Security mode ON/OFF

The following is an explanation of how to turn Enhanced Security mode On/Off.

Detail
Passwords are case sensitive.

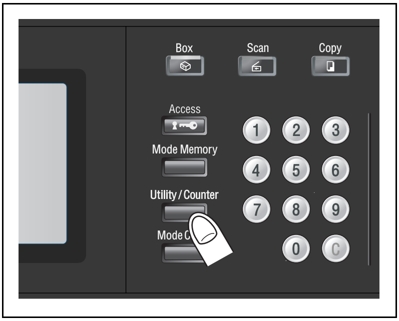
If a wrong password or fewer than 8 alphanumerical characters are entered and the [OK] is touched, the warning message "Password does not match" will appear, and no key will work for five seconds. Enter the right password after five seconds.

If authentication fails, the information will be saved in the audit log.

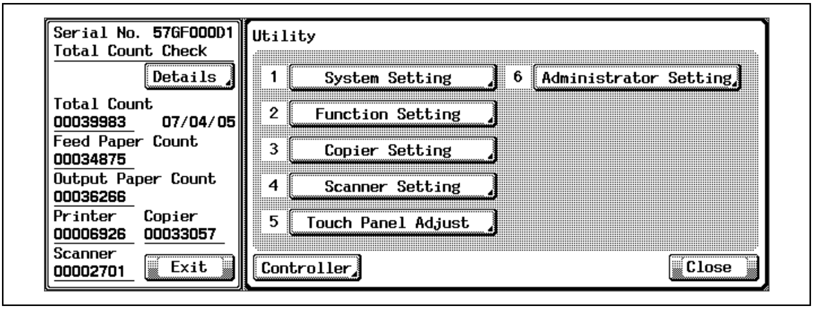
Procedure

1 Press [Utility/Counter] on the control panel.

The Utility Screen will be displayed.

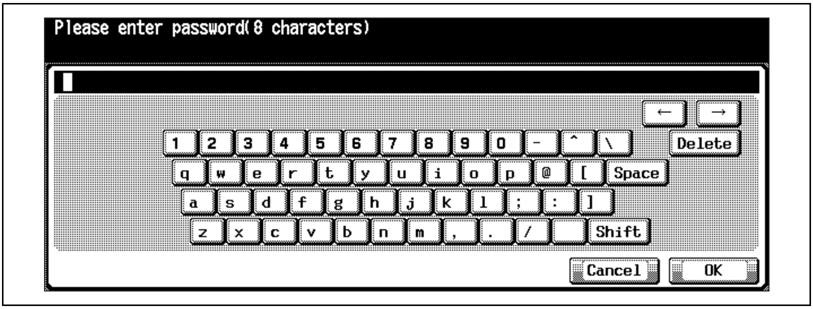


2 Touch [6 Administrator Setting].


Serial No. 57GF000D1
Total Count Check
Total Count
00039983 07/04/05
Feed Paper Count
00034875
Output Paper Count
00036266
Printer 00006926
Copier 00033057
Scanner 00002701

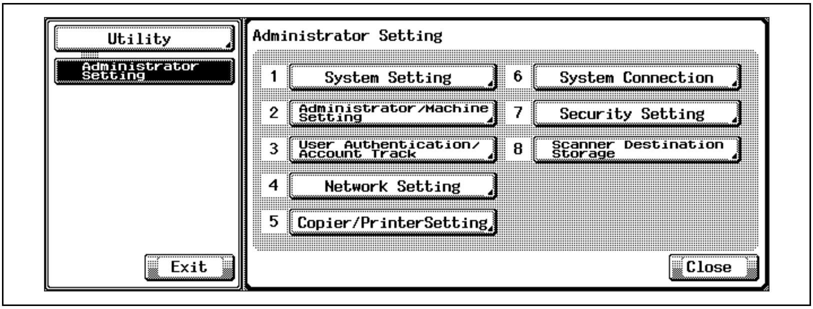
The Input Administrator Password Screen will be displayed.

3 Enter the password.
Use the touch panel keypad to enter the 8-digit Administrator password, then touch [OK].


Please enter password(8 characters)
← →
1 2 3 4 5 6 7 8 9 0 - ^ \ Delete
q w e r t y u i o p @ [Space
a s d f g h j k l ; :]
z x c v b n m , . / Shift
Cancel
OK

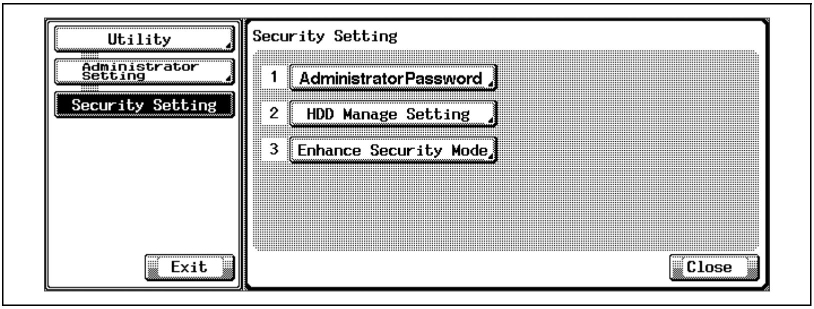
The Administrator Setting Screen will be displayed.

4 Touch [7 Security Setting].

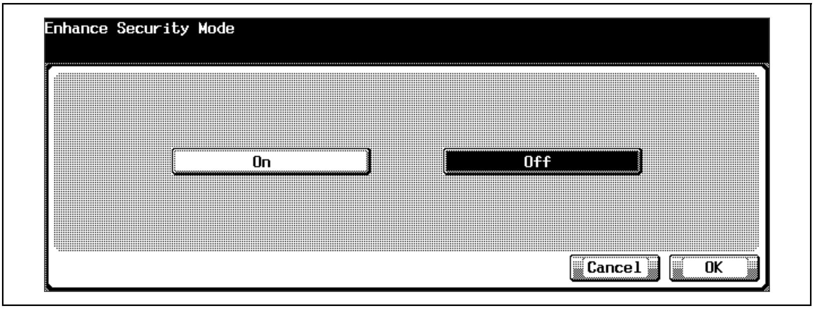


The Security Setting Screen will be displayed.

5 Touch [3 Enhance Security Mode].

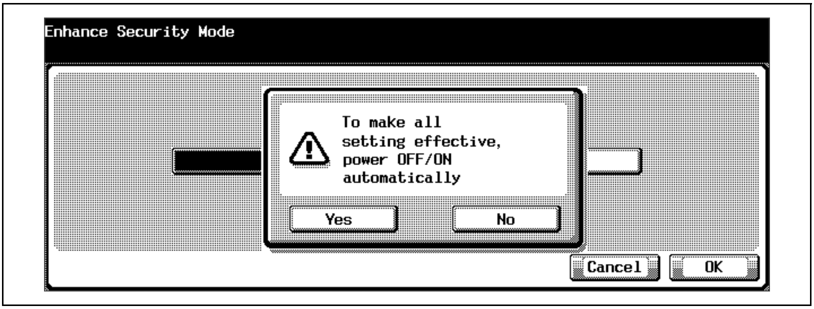


6 Turn Enhanced Security mode ON or OFF.
If you want to turn Enhanced Security mode ON, touch [On] to highlight it. If you want to turn it OFF, touch [Off] to highlight it. Touch [OK].



The Restart Confirmation popup screen will appear.

7 Touch [Yes].



To make all setting effective, power OFF/ON automatically

The machine will restart and the new setting will be activated.

6.2 HDD lock password

While the Enhanced Security mode is turned ON, a lock password (8 to 32 alphanumerical characters, case sensitive) can be set up on the HDD to protect the data stored on it.

If the HDD itself is externally accessed, the data readout will not be available until the correct lock password is entered.

...

Reminder

Do not use your name, birthday, employee number, etc. for a password that others can easily figure out.

Detail

The HDD lock password functions only when the Enhanced Security mode is ON. When turned OFF, the message “Please set Enhanced Security mode” will be displayed.

Detail

Passwords are case sensitive.

If a wrong password or fewer than 8 alphanumerical characters are entered and the [OK] is touched, the warning message “Password does not match” will appear, and no key will work for five seconds. Enter the right password after five seconds.

If authentication fails, the information will be saved in the audit log.

Detail

The main body serial number will be printed at the upper left on the Utility Screen and the upper right corner of the audit log. For details, see the next section “Print audit log” and page 57 for the sample log.

If authentication is succeeded, touch New Password to enter the new password. The key will not be active until authentication is succeeded.

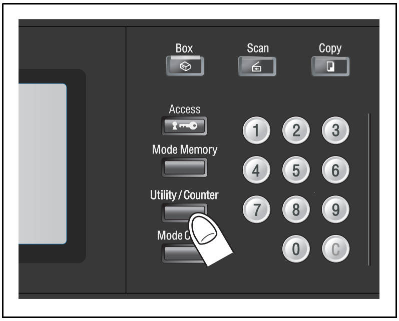
If authentication fails, the information will be saved in the audit log.

The current password cannot be used again as a new password.

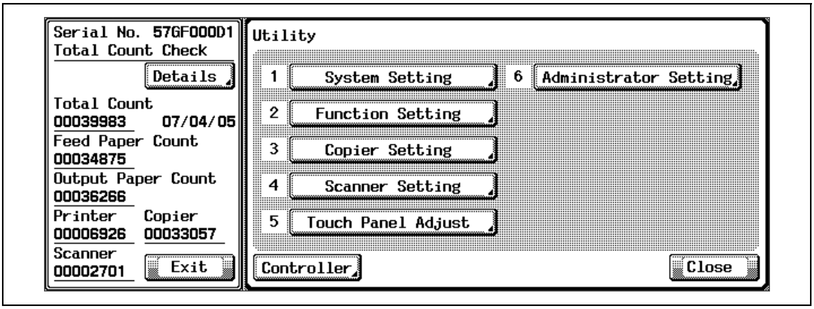
Procedure

1 Press [Utility/Counter] on the control panel.

The Utility Screen will be displayed.



2 Touch [6 Administrator Setting].



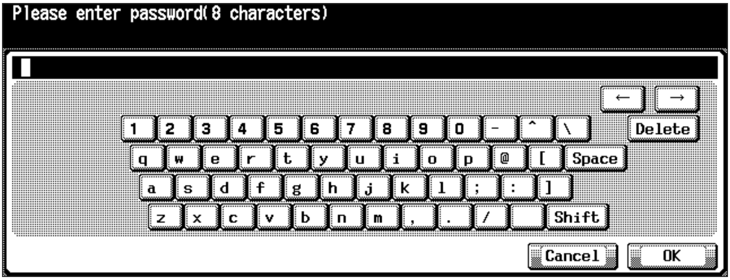
Serial No. 57GF000D1
Total Count Check

Total Count
00039983 07/04/05
Feed Paper Count
00034875
Output Paper Count
00036266
Printer 00006926
Copier 00033057
Scanner 00002701

Utility

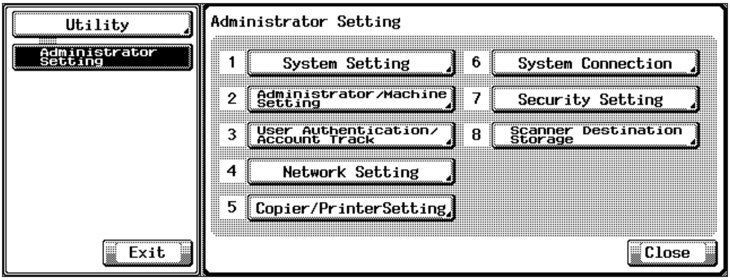
The Input Administrator Password Screen will be displayed.

3 Enter the password.
Use the touch panel keypad to enter the 8-digit administrator password, then touch [OK].


Please enter password(8 characters)

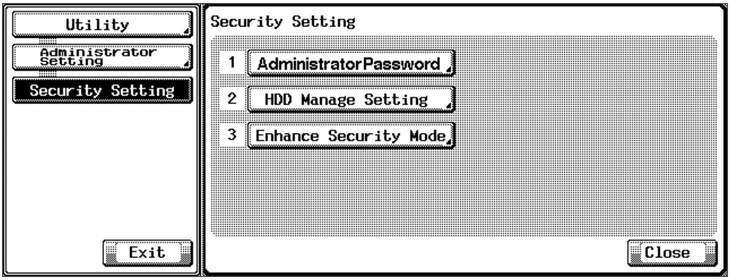
The Administrator Setting Screen will be displayed.

4 Touch [7 Security Setting].


Administrator Setting

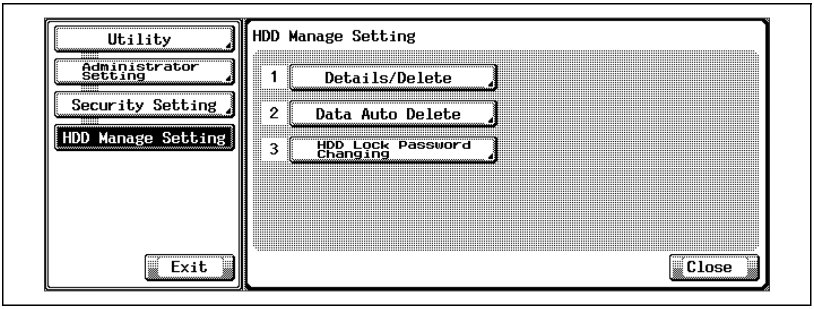
The Security Setting Screen will be displayed.

5 Touch [2 HDD Manage Setting].


Security Setting

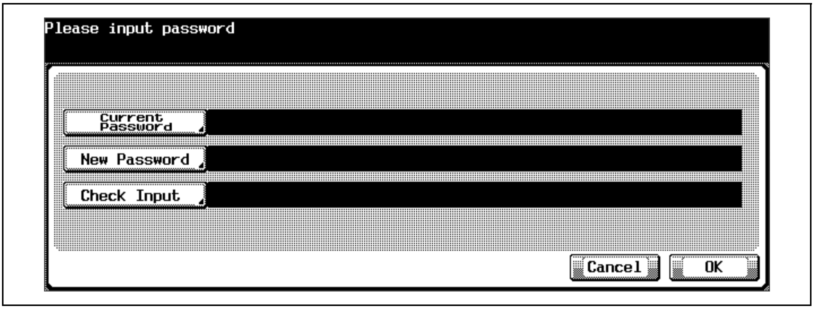
The HDD Manage Setting Screen will be displayed.

6 Touch [3 HDD Lock Password Changing].

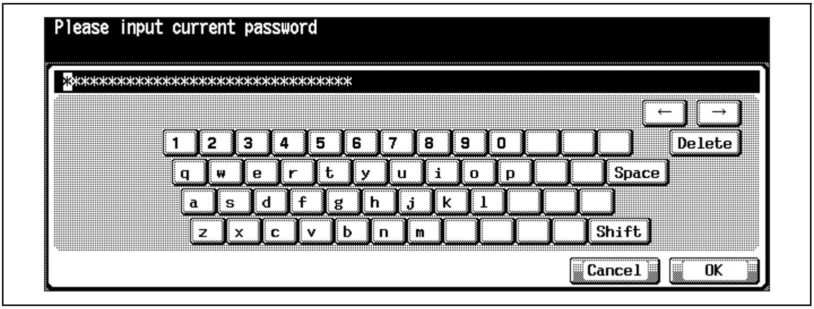


The HDD Lock Password Changing Screen will be displayed.

7 Enter current password.
Touch [Current Password] to display the Input Current Password Screen.

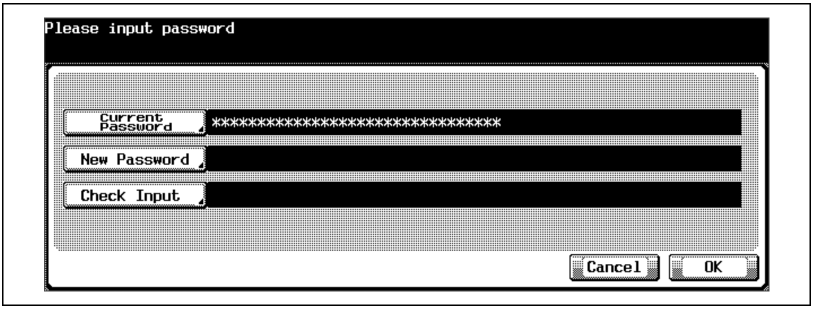


- Enter current password (The first password: 9-digit alphanumeric serial number of the main body). The entered password will appear as asterisks on the screen. Then, touch [OK].

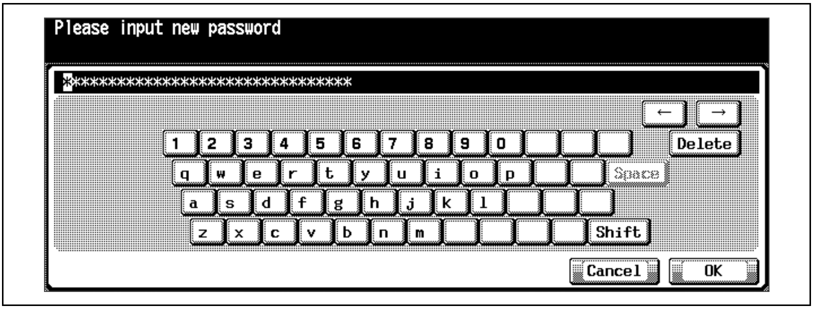


The Change HDD Lock Password Screen will be restored.

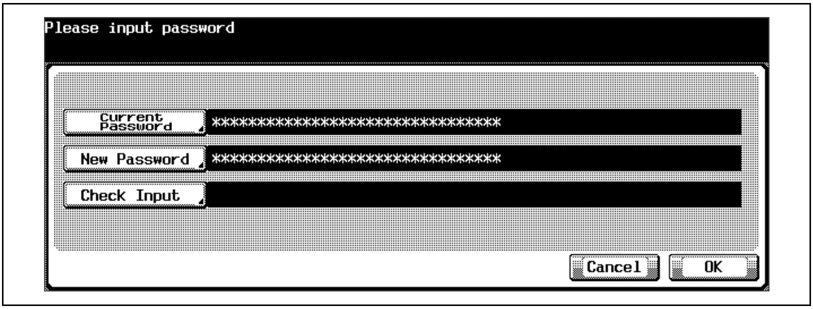
8 Enter new password.
Touch [New Password] to display the Input New Password Screen.



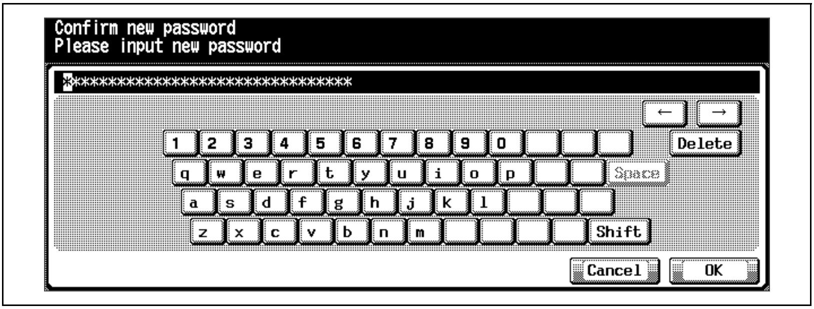
– Enter new password. The entered new password will appear as asterisks on the screen. Then, touch[OK].



– Touch [Check Input] to display the Re-input New Password Screen.



– Enter new password once more for confirmation, then touch [OK].



Confirm new password
Please input new password

****

The Change HDD Lock Password Screen will be restored.

6.3 Print audit log

An audit log will be automatically created when the data saved in the machine have been accessed.

All the audit log data can be output as follows.

Detail
Passwords are case sensitive.

If a wrong password or fewer than 8 alphanumerical characters are entered and the [OK] is touched, the warning message "Password does not match" will appear, and no key will work for five seconds. Enter the right password after five seconds.

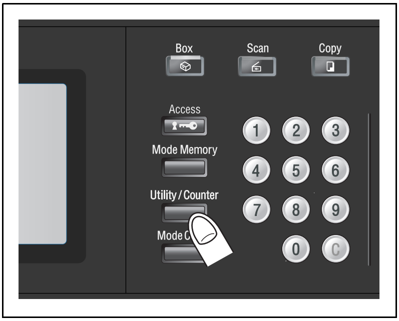
If authentication fails, the information will be saved in the audit log.

Detail
To stop printing, press [Stop] on the control panel, then touch [Cancel] on the confirmation popup screen.

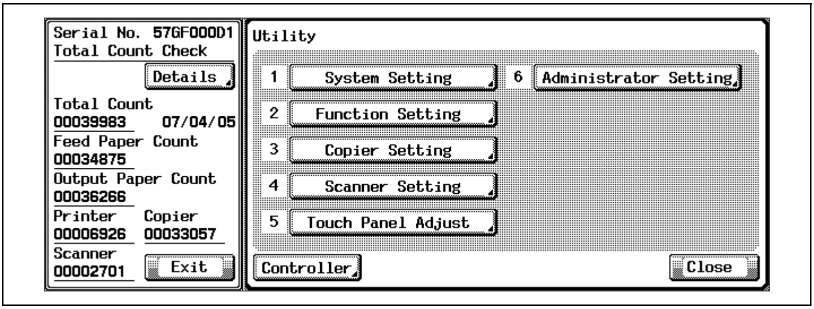
Procedure

1 Press [Utility/Counter] on the control panel.

The Utility Screen will be displayed.



2 Touch [6 Administrator Setting].

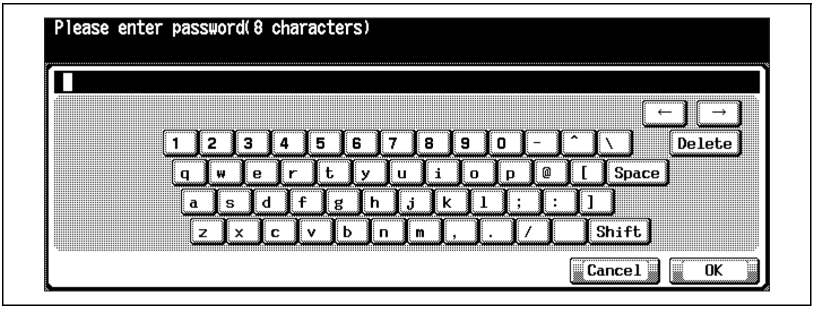


Serial No. 57GF000D1
Total Count Check

Total Count
00039983 07/04/05
Feed Paper Count
00034875
Output Paper Count
00036266
Printer 00006926 Copier 00033057
Scanner 00002701

The Input Administrator Password Screen will be displayed.

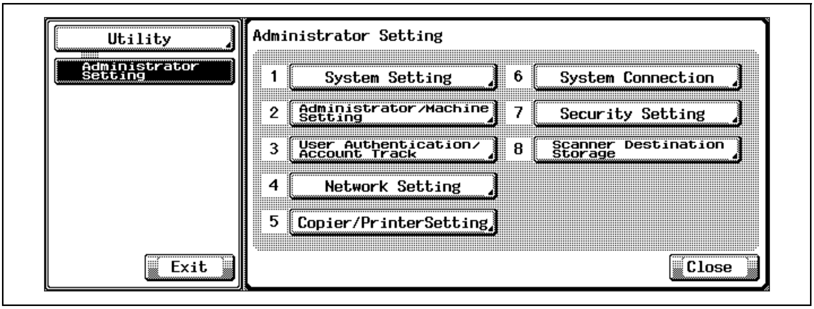
3 Enter the password.
Use the touch panel keypad to enter the 8-digit administrator password, then touch [OK].



Please enter password(8 characters)

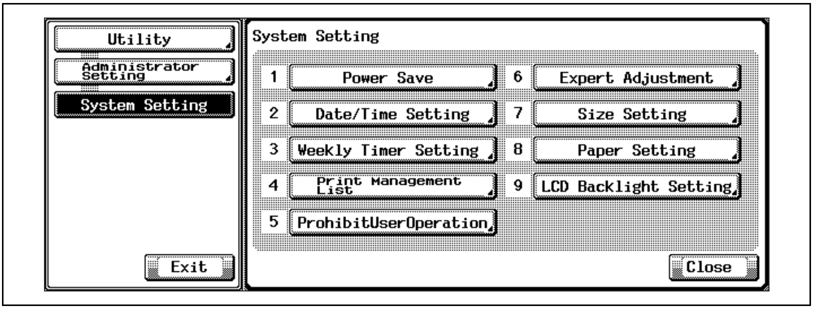
The Administrator Setting Screen will be displayed.

4 Touch [1 System Setting].



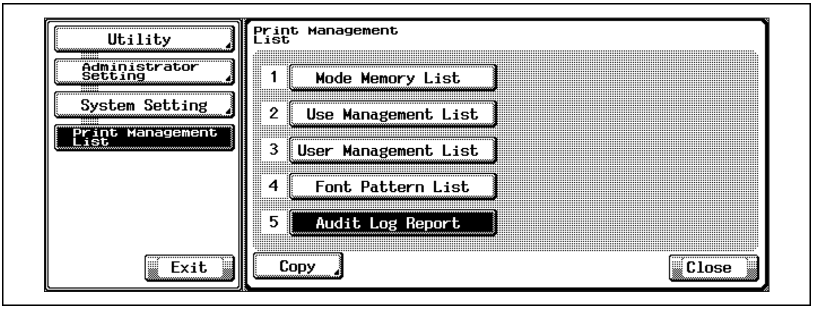
The System Setting Screen will be displayed.

5 Touch [4 Print Management List].



The Print Management List Screen will be displayed.

6 Touch [5 Audit Log Report], then touch [COPY].

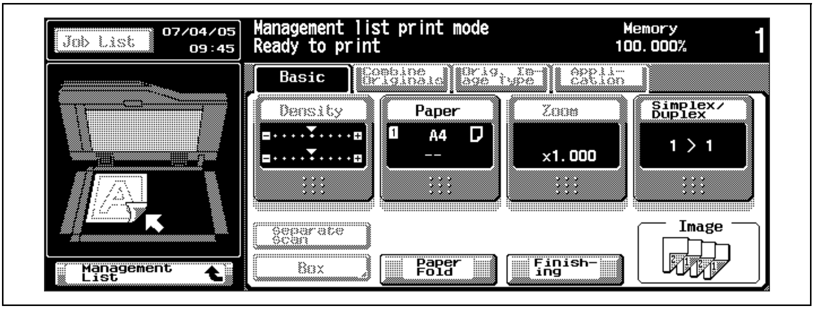


The Print Management List Screen will be displayed.

7 Press [Start] on the control panel.

Scan
Copy
Reset
Interrupt
Proof Copy
Stop
Start
1
2
3
4
5
6
7
8
9
0
C
Data
Main Power

8 Touch [Management List] to restore the Print Management List Screen.


Job List 07/04/05 09:45

Management list print mode
Ready to print

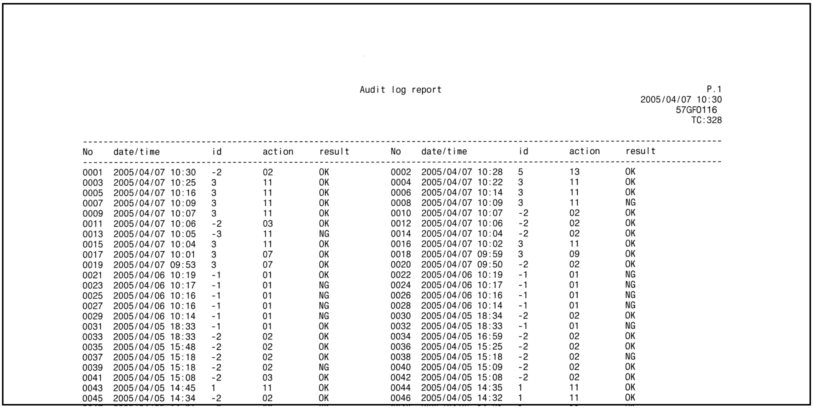
Memory 100.000%

1

6.4 Analyze audit log

Audit logs need to be analyzed by the administrator regularly (once per month) or when unauthorized access and tampering of data saved in the machine in Enhanced Security mode is noticed.

The machine is supposed to store up to 750 logs per month.
If more than 750 logs are assumed to be stored in a month, carry out the analysis in a shorter period before the unanalyzed logs reach that number.



```
                                         Audit log report                                     P.1
                                                                                 2005/04/07 10:30
                                                                                        57GF0116
                                                                                           TC:328
-------------------------------------------------------------------------------------------------
No    date/time          id      action    result      No    date/time          id      action    result
-------------------------------------------------------------------------------------------------
0001  2005/04/07 10:30   -2      02        OK          0002  2005/04/07 10:28   5       13        OK
0003  2005/04/07 10:25   3       11        OK          0004  2005/04/07 10:22   3       11        OK
0005  2005/04/07 10:16   3       11        OK          0006  2005/04/07 10:14   3       11        OK
0007  2005/04/07 10:09   3       11        OK          0008  2005/04/07 10:09   3       11        NG
0009  2005/04/07 10:07   3       11        OK          0010  2005/04/07 10:07   -2      02        OK
0011  2005/04/07 10:06   -2      03        OK          0012  2005/04/07 10:06   -2      02        OK
0013  2005/04/07 10:05   -3      11        NG          0014  2005/04/07 10:04   -2      02        OK
0015  2005/04/07 10:04   3       11        OK          0016  2005/04/07 10:02   3       11        OK
0017  2005/04/07 10:01   3       07        OK          0018  2005/04/07 09:59   3       09        OK
0019  2005/04/07 09:53   3       07        OK          0020  2005/04/07 09:50   -2      02        OK
0021  2005/04/06 10:19   -1      01        OK          0022  2005/04/06 10:19   -1      01        NG
0023  2005/04/06 10:17   -1      01        NG          0024  2005/04/06 10:17   -1      01        NG
0025  2005/04/06 10:16   -1      01        NG          0026  2005/04/06 10:16   -1      01        NG
0027  2005/04/06 10:16   -1      01        NG          0028  2005/04/06 10:14   -1      01        NG
0029  2005/04/06 10:14   -1      01        NG          0030  2005/04/05 18:34   -2      02        OK
0031  2005/04/05 18:33   -1      01        OK          0032  2005/04/05 18:33   -1      01        NG
0033  2005/04/05 18:33   -2      02        OK          0034  2005/04/05 16:59   -2      02        OK
0035  2005/04/05 15:48   -2      02        OK          0036  2005/04/05 15:25   -2      02        OK
0037  2005/04/05 15:18   -2      02        OK          0038  2005/04/05 15:18   -2      02        NG
0039  2005/04/05 15:18   -2      02        NG          0040  2005/04/05 15:09   -2      02        OK
0041  2005/04/05 15:08   -2      03        OK          0042  2005/04/05 15:08   -2      02        OK
0043  2005/04/05 14:45   1       11        OK          0044  2005/04/05 14:35   1       11        OK
0045  2005/04/05 14:34   -2      02        OK          0046  2005/04/05 14:32   1       11        OK
```

Audit Log Information

The audit log contains the following information.

1. date/time: date and time when an operation was made that results in the creation of a log entry.
2. id: the person who made the operation or who is subject to security protection can be specified.
   "-1": Operation by CE (service representative).
   "-2": Operation by the administrator.
   "-3": Operation by the unregistered user.
   Other integer: Indicates subjects for security protection, and the following action IDs narrow down the subject for protection.
   User ID (1 to 1000 numerical symbols)
   Secure User ID (1 to 99999 numerical symbols)
3. action: Used to specify the operation.
   Check details of operation that action indicates in the following table.
4. result: Result of an operation.
   For password authentication, success or failure will be indicated as OK and NG.
   For operations without password authentication, all log entries will be indicated as OK.

6.5 Table of items saved in audit log

No.	Operation	ID	Stored action	Result
1	CE authentication	CE ID	01	OK/NG
2	Administrator authentication	Administrator ID	02	OK/NG
3	Set/change Enhanced Security mode	Administrator ID	03	OK
4	Print audit log	Administrator ID	04	OK
5	Change/register CE password	CE ID	05	OK
6	Change/register Administrator password	CE ID/ Administrator ID	06	OK
7	Create user by Administrator	User ID	07	OK
8	Change/register user password by Administrator	User ID	08	OK
9	Delete user by Administrator	User ID	09	OK
10	Change attributes of user by Administrator	User ID	10	OK
11	Password authentication for user	User ID / Unregistered user ID	11	OK/NG
12	Change attributes of user by user (user password, etc.)	User ID	12	OK
13	Access to file (document data readout)	User ID	13	OK
14	Delete file (document data deletion)	User ID	14	OK
16	Password authentication for secure printing	Secure user ID / Unregistered user ID	16	OK/NG
17	Access to secure print file	Secure user ID	17	OK
18	Delete secure print file	Secure user ID	18	OK
19	Change HDD lock password	Administrator ID	19	OK

The purpose of analyzing the audit log is to understand the following and implement countermeasures:

Whether or not data was accessed or tampered with
Subject of attack
Details of attack
Results of attack

Specify unauthorized actions: password authentication

If logs have NG as the result of password authentication (action: 01, 02, 11, 16), items protected by passwords may have been attacked.

- Failed password authentication (NG) log entries specify who made the operation, and show if unauthorized actions were made when password authentication failed.
- Even if password authentication succeeded (OK), it shows whether a legitimate user created the action. You need to check carefully when successful authentication occurs after series of failures especially during times other than normal operating hours.

Specify unauthorized actions: actions other than password authentication under security

All operation results other than password authentication will be indicated as successful (OK), so determine if there were any unauthorized actions by ID and action.

- Since you cannot specify what was attacked only with an ID, you need to see the action and the table on the previous page to determine whether unauthorized actions were made on a personal box or secure box.
- Check the time, and see if the user who operated the specific subject made any unauthorized actions.

(Example)
If a document saved in a box was printed using fraudulent authorization, the following audit log entry will be created.

1. Password authentication for the box:
   Action = 11
   ID = Box that authentication was made
   Result = OK/NG
2. Access to the document in the box:
   Action = 13
   ID = Box that authentication was made

Check the date and time the above operation occurred, and see if the operation on the document in the personal box or secure box was made by a legitimate box user.

Actions to take if unauthorized operations are found

- If it’s found that a password has been leaked after analyzing the audit log, change the password immediately.
- It’s possible that a password may have been tampered with and legitimate users cannot access a box. The administrator must contact the user to confirm the situation, and if that’s the case, the administrator must change the password and delete the data saved in the box.
- If you cannot find documents that should be in a box or if you find a document with changed content, unauthorized actions may have occurred. Similar countermeasures are needed.

7 Index

KONICA MINOLTA

www.konicaminolta.com

Copyright
2005 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC.

57GN97070

2005.7
Printed in China