KONICA MINOLTA

The essentials of imaging

bizhub PRO 1200/1051

User's Guide

Security

1 Security Functions
2 Protect and Delete Data After Use
3 User Authentication in Security Strengthen Mode
4 HDD Store Function in Security Strengthen Mode
5 Administrator Security Functions
6 Index

bizhub PRO 1200/1051

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:

A0G60Y0-00I1-G00-10
A0G60Y0-00I1-G00-15
A0G60Y0-00I1-G00-20
A0G60Y0-00I1-G00-30

Controller control program (IC Control P) version:

A0G6011-00P1-G00-10
A0G6011-00P1-G00-20

About the Rom version display function:

The bizhub PRO 1200/1051 Control Software (Image control program / Controller control program) version mentioned above can be confirmed by using the service representative (CE) service mode ROM version display function.

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

A0G60Y0-00I1-G00-**
Image control program (Image Control I1) version:
G00-2 digits (Ex: G00-**)
A0G6011-00P1-G00-**
Controller control program (IC Control P) version:
G00-2 digits (Ex: G00-**)

Please keep this in mind when checking the software version.

FEDERAL OR STATE STATUTES MAY PROHIBIT THE COPYING OF CERTAIN DOCUMENTS OR INFORMATION, RESULTING IN FINES OR IMPRISONMENT FOR VIOLATORS.

Composition of User’s Guide

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

User's Guide - Copier (Printed matters), (User’s Guide CD)

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.

User's Guide - POD Administrator's Reference (Printed matters), (User’s Guide CD)

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 registration of copy paper, tray setting, and a network setup.

User's Guide - Security <This book> (Printed matters), (User’s Guide CD)

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.

User's Guide - Network Scanner (Printed matters), (User’s Guide CD)

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 reading data or storing data (Scan to HDD, Scan to E-Mail, Scan to FTP, Scan to SMB).

Trademarks/Copyrights (User’s Guide CD)

This guide describes trademarks, licenses and copyrights concerning this machine.

Be sure to read this guide before using the machine.

User's Guide - Printer (User’s Guide CD)

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

Please refer to this guide for how to use PCL driver, Adobe PS driver, and PageScope Web Connection in user mode.

User's Guide - Printer (PostScript3 Plug-in Driver) (User's Guide CD)

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

Please refer to this guide for how to use Plug-in driver in user mode.

Operation Quick Guide (Printed matters)

The descriptions given in this guide are excerpts from the operation section of frequently used functions.

Please refer to this guide for quick comprehension of various features available on the machine.

To operate safely, be sure to read "Section 1: Precautions for Installation and Use" in User's Guide - Copier before using the machine.

Contents

1 Security Functions

1.1 Modes 1
1.2 Environment 2
1.3 Overview of Security Strengthen Mode 3
1.4 Data protected by Security Strengthen mode 5

2 Protect and Delete Data After Use

3 User Authentication in Security Strengthen Mode

3.1 Description of user authentication 7
3.2 To register a new user 8
3.3 To change a user data 14
3.4 To delete a user 19
3.5 To change password by user 23

4 HDD Store Function in Security Strengthen Mode

4.1 Store the data in a Box while Copying 27
4.2 Store scanned data in a Box 33
4.3 Recall/Delete data in a Box 39
4.4 Output data in the Secure Box 44

5 Administrator Security Functions

5.1 Turn Security Strengthen mode ON/OFF 49
5.2 HDD lock password 55
5.3 Delete Temporary Data 59
5.4 Delete All Data 63
5.5 Print audit log 67
5.6 Analyze audit log 70
5.7 Table of items saved in audit log 71

6 Index

1 Security Functions

1.1 Modes

The bizhub PRO 1200/1051 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 user's guide for each individual machine.

Security Strengthen 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 Security Strengthen mode ON and OFF, and make other changes, and your service representative will designate an administrator.

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

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

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

Ask your administrator if the Security Strengthen mode is turned ON.

1.2 Environment

Environments in which Security Strengthen 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 Security Strengthen 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. Also, select a place security locked at night, and available to be monitored by an administrator in the daytime.
- 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 Security Strengthen 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.

1.3 Overview of Security Strengthen Mode

Protect and delete used data in memory and on the HDD

There are three kinds of image data that will be saved in memory and on the HDD: AHA compressed data and uncompressed data (TIFF, PDF and PS 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 Security functions, 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 unrelated 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 Security Strengthen 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 administrator 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.

1.4 Data protected by Security Strengthen mode

Data protected by Security Strengthen 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 Security Strengthen mode

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

To turn Security Strengthen mode ON/OFF

The administrator can turn Security Strengthen mode ON/OFF.

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

If data is accessed in Security Strengthen 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 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.

3 User Authentication in Security Strengthen Mode

3.1 Description of user authentication

In Security Strengthen 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 Security Strengthen mode.
If this happens, contact the administrator to turn OFF Security Functions, 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] key on the control panel is pressed.
- The [Copy]/[Scan]/[STORE]/[RECALL] tab 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 Account Distribute Number should be changed. For details, refer to the User's Guide - POD Administrator's Reference.

3.2 To register a new user

Follow the procedure below to setup a new user name and password to be required for user authentication in Security Strengthen 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 "Incorrect password Please wait for a while" will appear, and no key will work for five seconds. Enter the right password after five seconds.

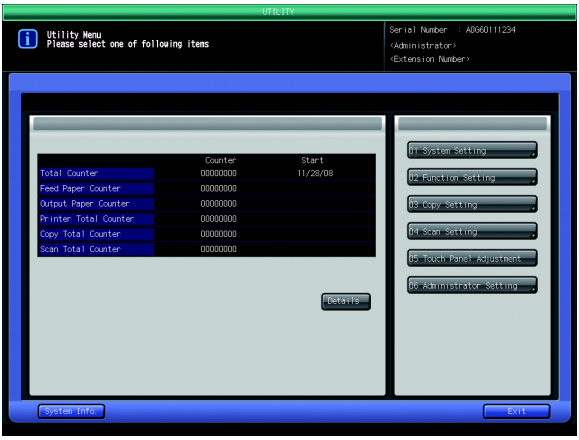
If authentication fails, the information will be saved in the audit log.

Procedure

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

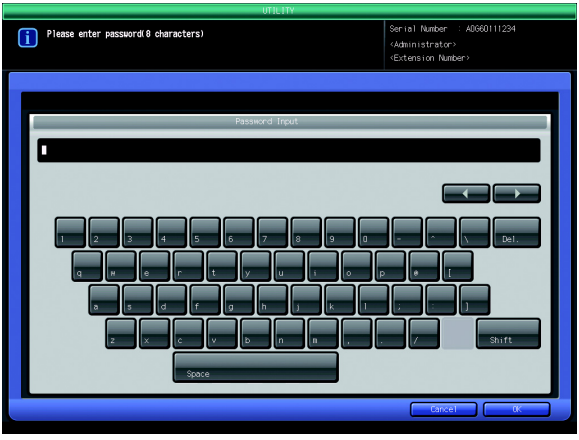
The Utility Screen will be displayed.

2 Touch [06 Administrator Setting].



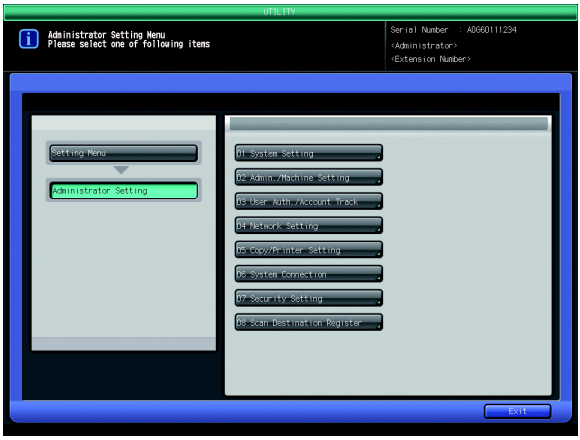
The Input Administrator Password Screen will be displayed.

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



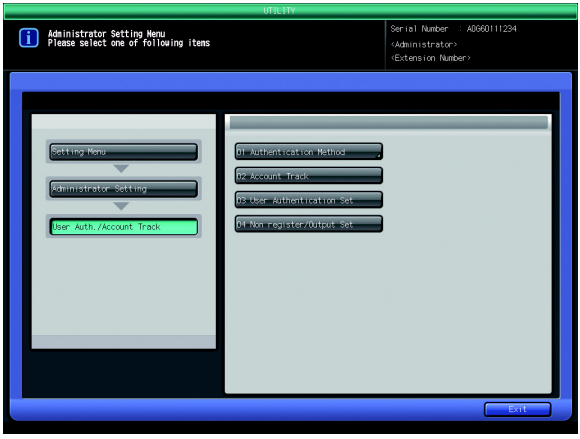
The Administrator Setting Screen will be displayed.

4 Touch [03 User Auth./Account Track].



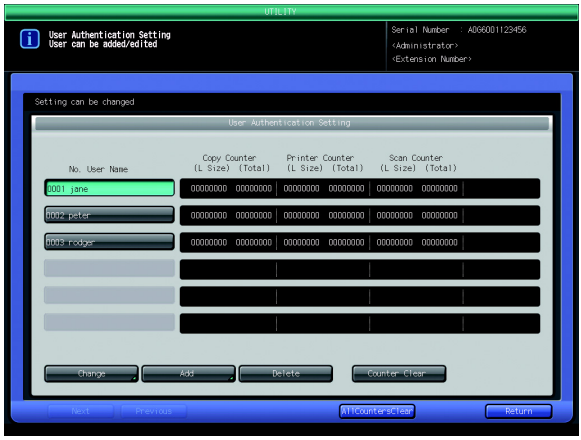
The User Authentication/Account Track Screen will be displayed.

5 Touch [03 User Authentication Set].



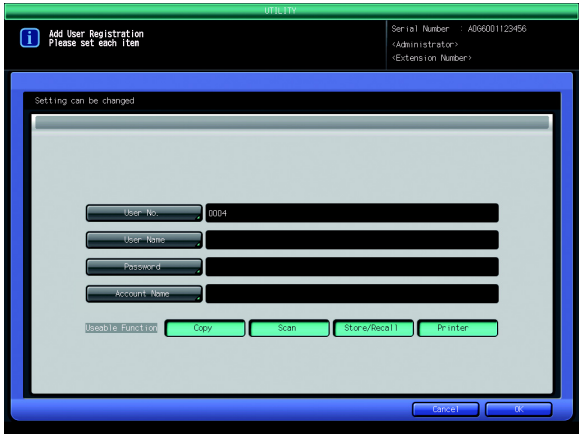
The User Authentication Setting Screen will be displayed.

6 Touch [Add].



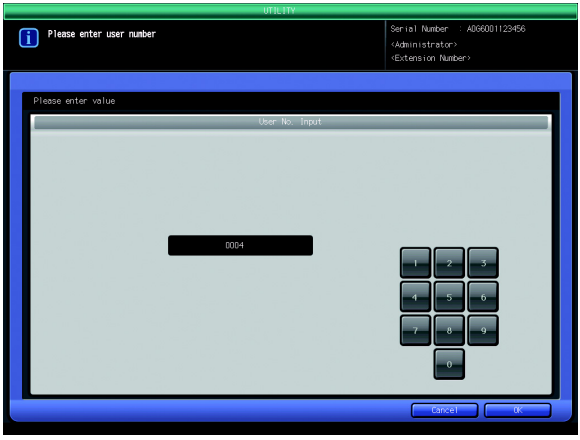
The New User Registration Screen will be displayed.

7 Touch [User No.], [User Name], [Password], or [Account Name] to display each subsequent screen, then make the desired setting.



– When the Synchronize User/Account Track of Authentication Method is selected [ON], the Account Name is available.

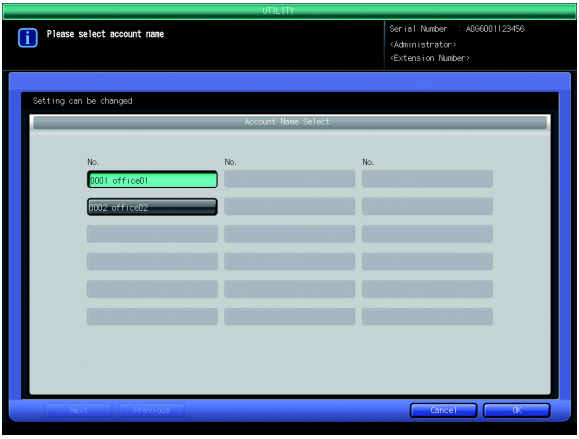
– To enter the User Number, touch [User No.] on the New User Registration Screen. Use the screen keypad on the popup menu to enter the desired user number. Touch [OK] to return to the New User Registration Screen.



– 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.

– 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.

– 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.



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

The User Authentication Setting Screen will be restored.

3.3 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 "Incorrect password Please wait for a while" will appear, and no key will work for five seconds. Enter the right password after five seconds.

The current password cannot be used again.

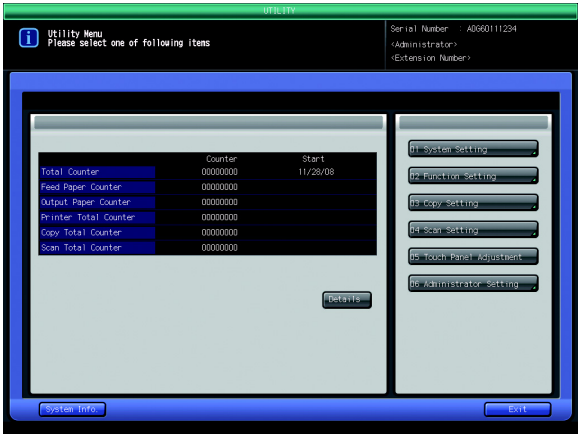
If authentication fails, the information will be saved in the audit log.

Procedure

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

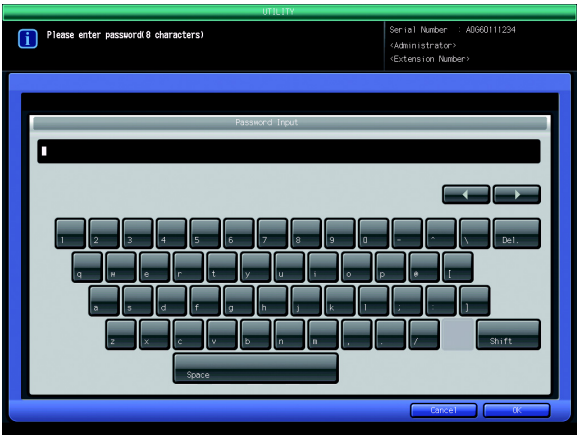
The Utility Screen will be displayed.

2 Touch [06 Administrator Setting].



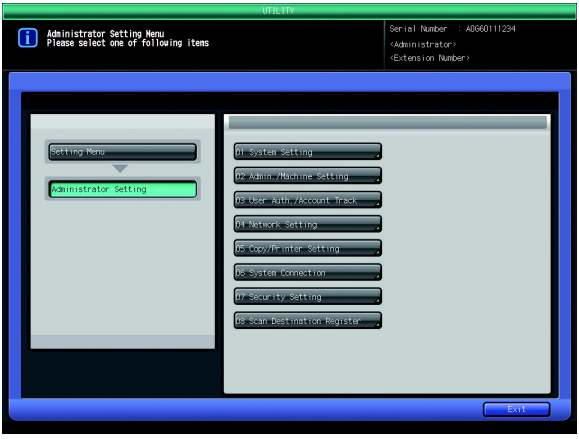
The Input Administrator Password Screen will be displayed.

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



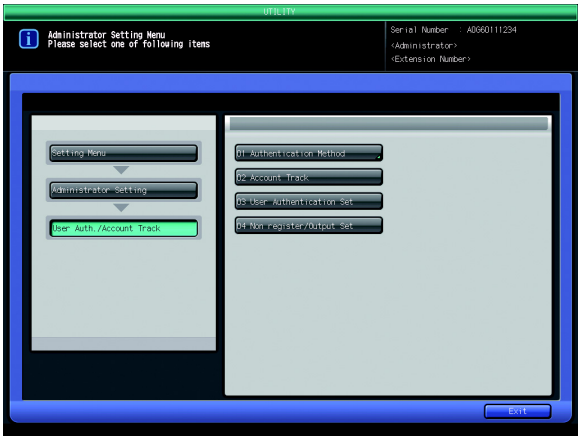
The Administrator Setting Screen will be displayed.

4 Touch [03 User Auth./Account Track].



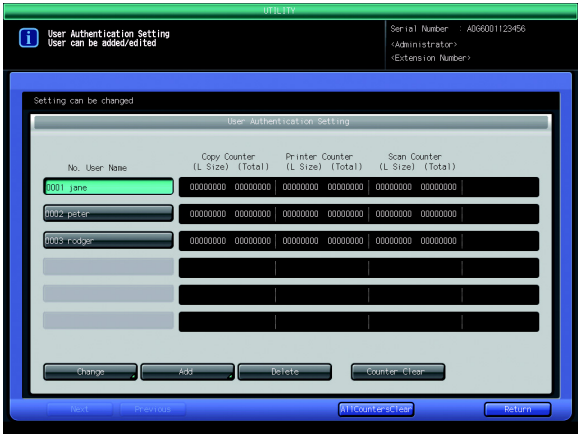
The User Authentication/Account Track Screen will be displayed.

5 Touch [03 User Authentication Set].



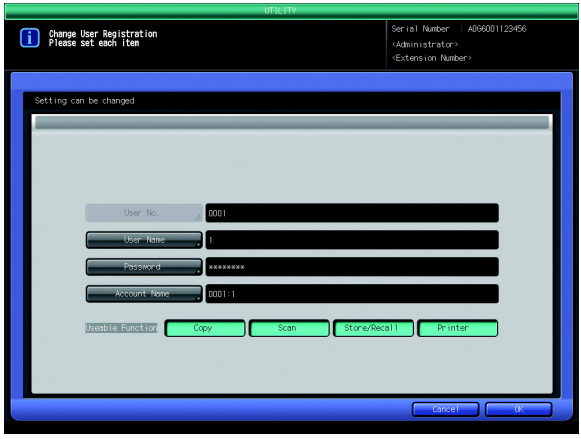
The User Authentication Setting Screen will be displayed.

6 Touch the user name key to be changed, then touch [Change].



The Change Registered User Data Screen will be displayed.

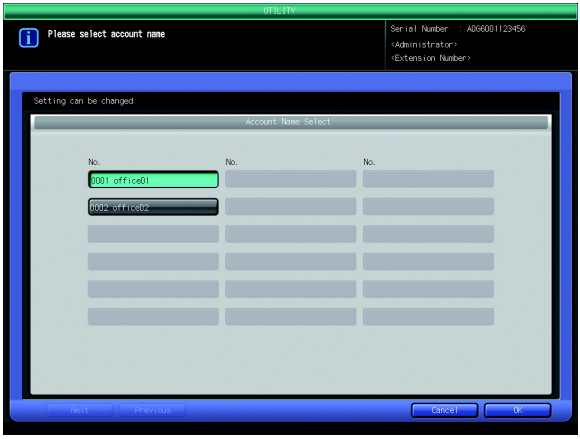
7 Touch [User Name], [Password] or [Account Name] to display each subsequent screen, then make the desired setting change.



– 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.

– 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.

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



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

3.4 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 "Incorrect password Please wait for a while" will appear, and no key will work for five seconds. Enter the right password after five seconds.

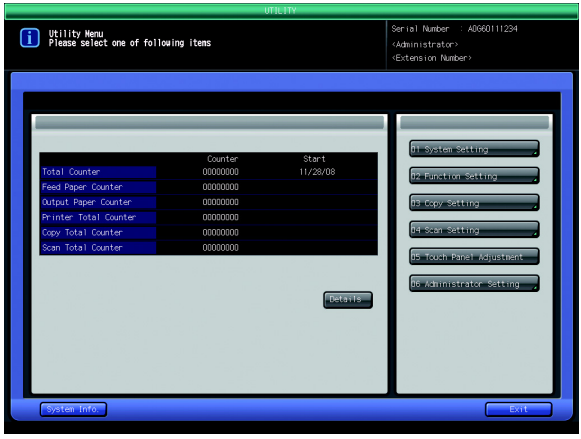
If authentication fails, the information will be saved in the audit log.

Procedure

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

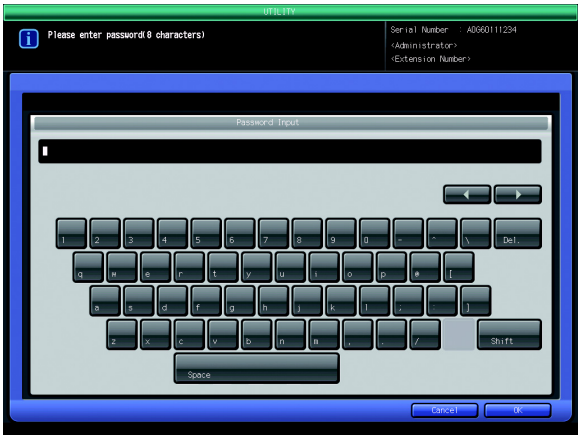
The Utility Screen will be displayed.

2 Touch [06 Administrator Setting].



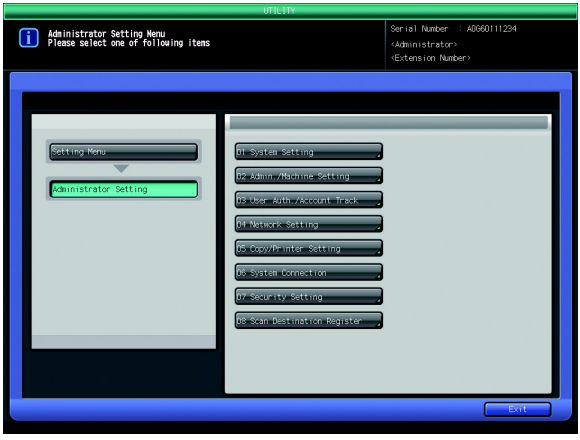
The Input Administrator Password Screen will be displayed.

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



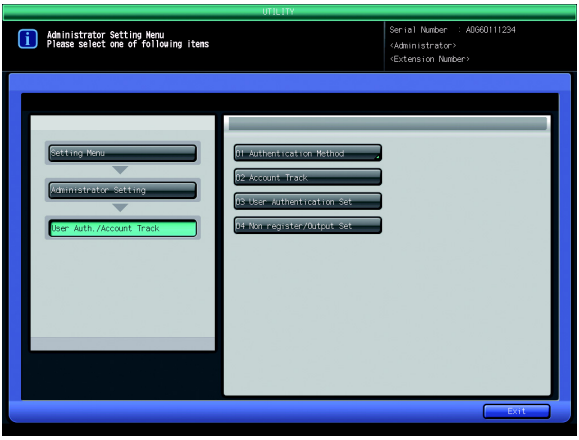
The Administrator Setting Screen will be displayed.

4 Touch [03 User Auth./Account Track].



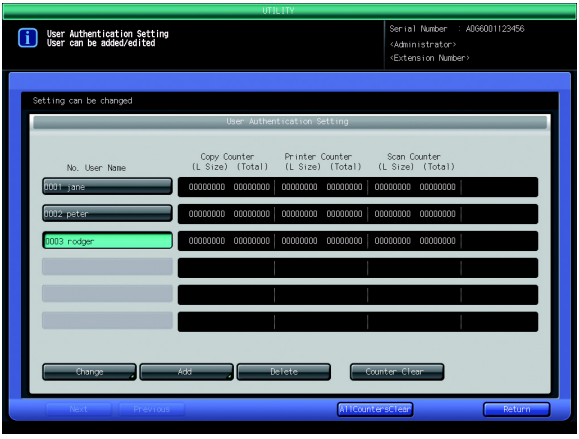
The User Authentication/Account Track Screen will be displayed.

5 Touch [03 User Authentication Set].



The User Authentication Setting Screen will be displayed.

6 Touch the user name key to be deleted.

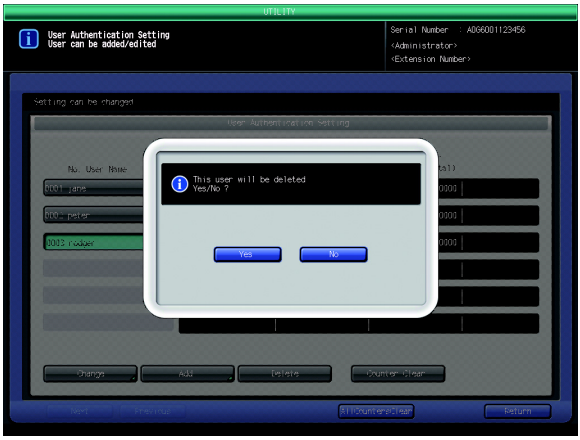


The selected key will be highlighted.

7 Touch [Delete].

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

8 Touch [Yes].



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

3.5 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 "Incorrect password Please wait for a while" 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 does not proceed successfully, the information will be saved in the audit log.

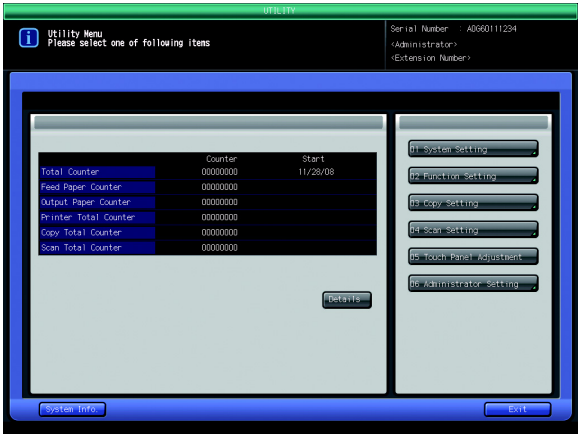
The password currently used cannot be entered as a new password.

Procedure

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

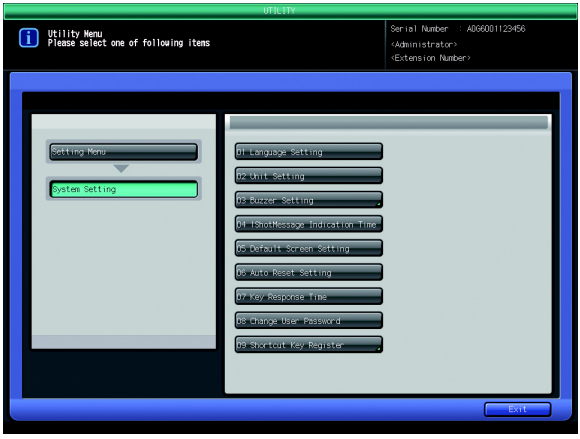
The Utility Screen will be displayed.

2 Touch [01 System Setting].



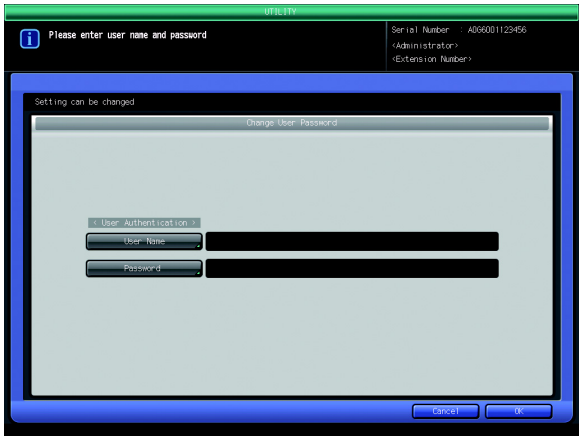
The System Setting Screen will be displayed.

3 Touch [08 Change User Password].



The User Authentication Screen will be displayed.

4 Touch [User Name], then enter your user name.

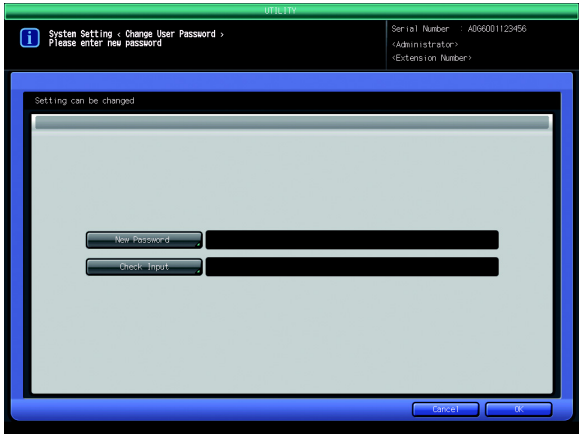


The entered name will be displayed on the screen.

5 Touch [password], then enter your current password.

– The entered password will appear as asterisks(********) on screen. When user authentication is completed successfully, the Change User Password Screen will be displayed.

6 Touch [New Password], enter your new password, then touch [OK].



7 Enter the new password again for confirmation.

– Touch [Check Input], then enter your new password once more. Touch [OK].

8 Touch [OK].

The System Setting Screen will be restored.

9 Touch [Exit].

The Copy Screen will be restored.

4 HDD Store Function in Security Strengthen 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 Security Strengthen mode when storing any secret document.
If the Security Strengthen 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.

4.1 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 Security Strengthen mode for which a user name and password have been set.

Detail

Passwords are case sensitive.

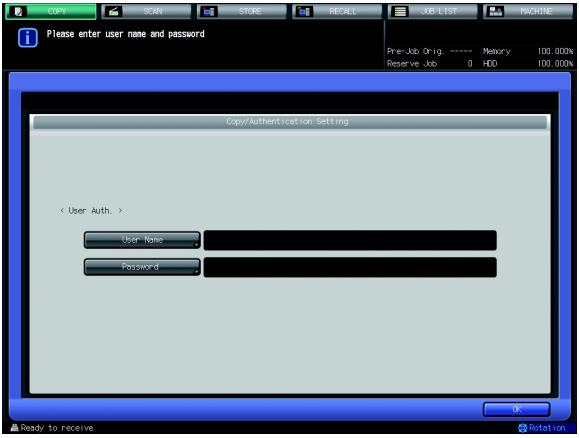
If a wrong password or fewer than 8 alphanumerical characters are entered and the [OK] is touched, the warning message "Incorrect password Please wait for a while" will appear, and no key will work for five seconds. Enter the right password after five seconds.

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

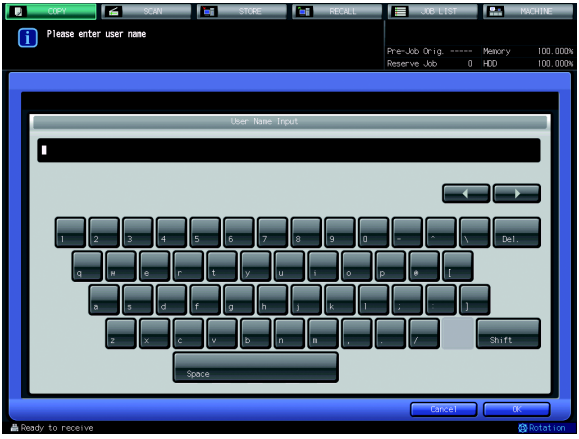
Procedure

1 On the User Authentication Screen, touch [User Name] and [Password] to enter your user name and password.

– 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.

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

2 Touch [OK].

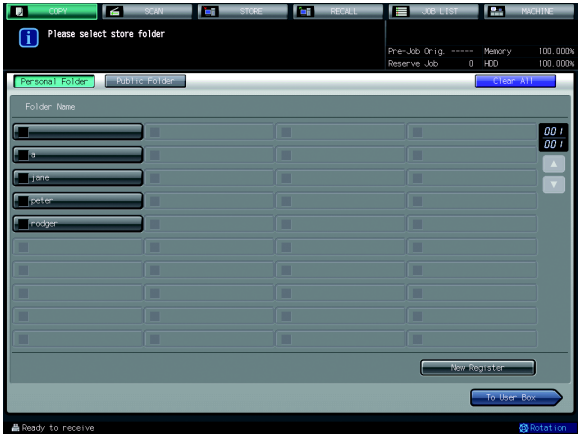
The Copy Screen will be displayed.
Position the original.

3 Touch [Output Setting] on the Copy Screen.

4 Touch [HDD Store] on the Output Setting Screen.

The HDD Folder List Screen will be displayed.

5 Select the desired personal Folder, then touch [To User Box].



The Personal Box Screen will be displayed.

6 Select the desired personal Box.

– Enter the password if selected Box requires one.

The Personal File Screen will be displayed.

7 Touch [New File Store].

The Input File Name Screen will be displayed.

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

9 Touch [OK].

The Copy Screen will be displayed.

10 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.

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.

4.2 Store scanned data in a Box

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

Detail

Passwords are case sensitive.

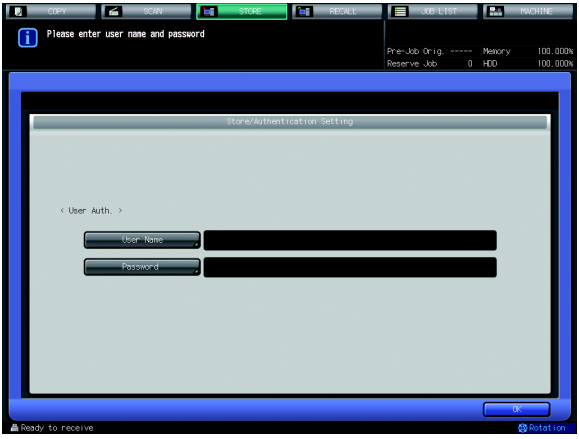
If a wrong password or fewer than 8 alphanumerical characters are entered and the [OK] is touched, the warning message "Password does not match" will appear, and no key will work for five seconds. Enter the right password after five seconds.

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

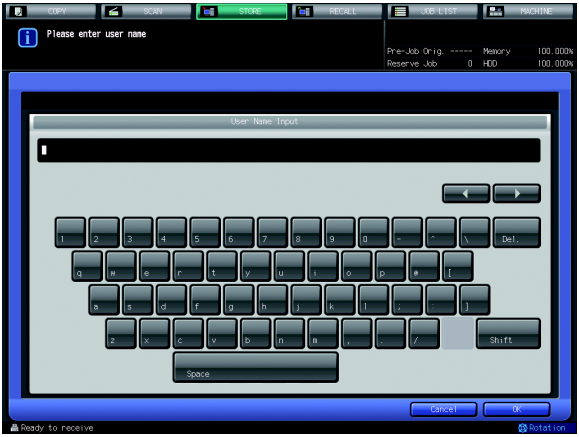
Procedure

1 Touch [STORE] tab, then touch [User Name] and [Password] on the User Authentication Screen to enter your user name and password.

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



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



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

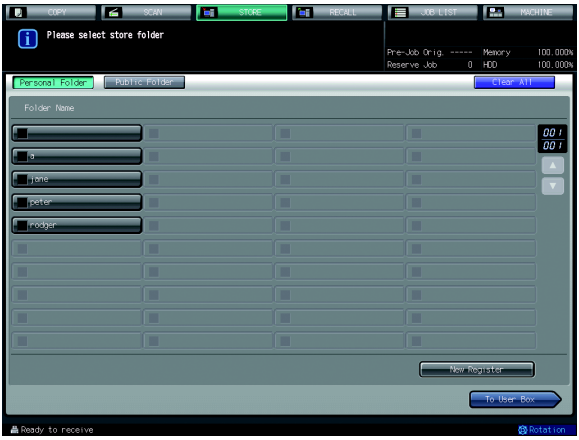
2 Touch [OK].

The Store Screen will be displayed.

3 Touch [Scan to HDD].

The personal Folder List Screen will be displayed.

4 Select the desired personal Folder, then touch [To User Box].



The Personal Box Screen will be displayed.

5 Select the desired personal Box.

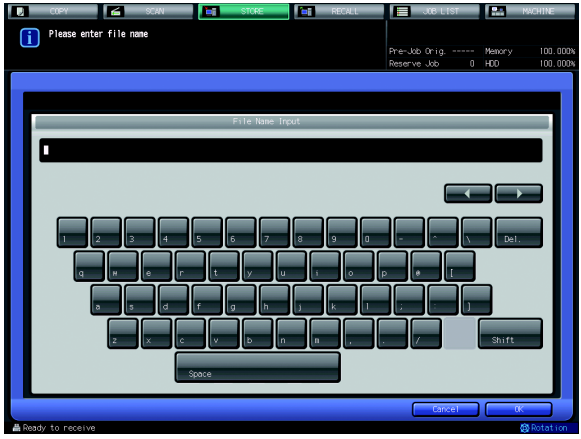
– Enter the password if selected Box requires one.

The Store Personal File Screen will be displayed.

6 Touch [New File Store].

The Input File Name Screen will be displayed.

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



The Scan Screen will be displayed.

8 Make the desired setting, then press [Start] on the control panel to scan and store the image data.

9 Touch the desired key on the popup screen.

Touch [Yes] to continue the scanning job, or touch [No] to complete the job.

10 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.

4.3 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 "Incorrect password Please wait for a while" will appear, and no key will work for five seconds. Enter the right password after five seconds.

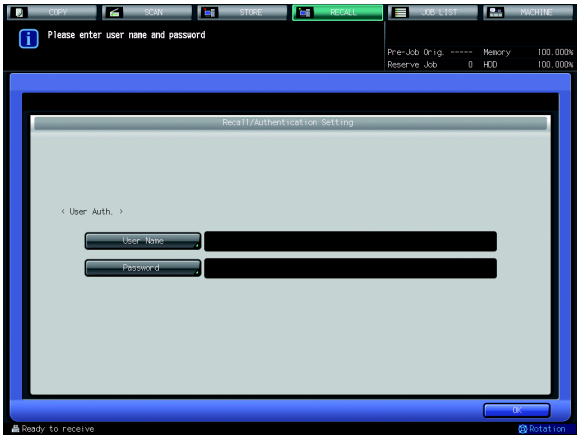
If authentication fails, the information will be saved in the audit log.

The blank page will not be output even when selecting the blank page for page range in Insert Sheet, Booklet, or Chapter job. The blank page can be set to output. Contact your service representative, if desired.

Procedure

1 Touch [RECALL] tab, then touch [User Name] and [Password] on the User Authentication Screen to enter your user name and password.

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



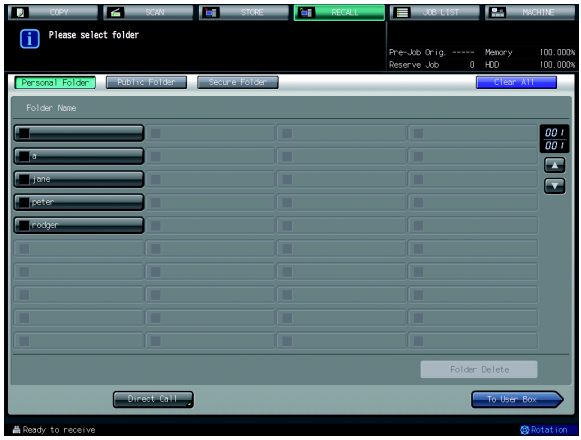
– Enter your user name, then touch [OK] to return to the User Authentication Screen.

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

2 Touch [OK].

The Recall Screen will be displayed.

3 Select the desired folder, then touch [To User Box].



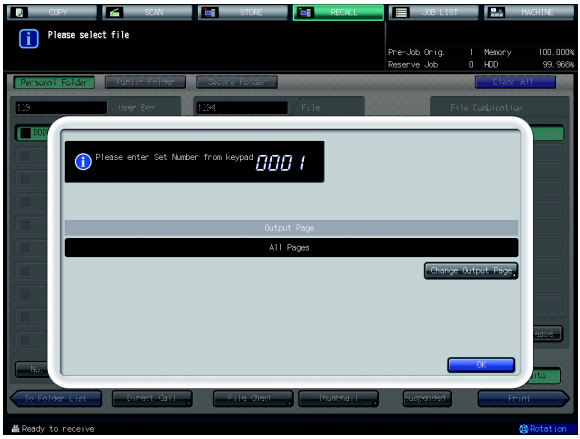
The HDD Box List Screen will be displayed.

4 Select the desired personal Box.

Enter the password if selected Box requires one.
The File Selection Screen will be displayed.

5 Recall the image data.

– Touch the desired file key, then touch [>>]. To output the image data, touch [Wait], [Proof], [Proof(1st Sheet)] or [Auto], as desired, and then touch [Print].
The [Proof(1st Sheet)] key does not appear on the screen by default, but can be available in the Utility mode.



– Enter the desired print quantity from touch panel keypad, then touch [OK].

– Specify the output page of the image data.
Touch [Change Output Page].
To output desired page(s), touch [Page Select], then enter the page number from control panel keypad.
Use “, (comma)” between pages, or “- (hyphen)” for consecutive pages.
To output all pages, touch [All Pages].
Touch [OK] to output.
– Touch the desired key on the popup screen.
Touch [Yes] to complete the job, or touch [No] to cancel the job.

6 Delete the image data.

– Touch the desired file key, then touch [File Delete]. The popup menu to confirm will be displayed. Touch [Yes].

The selected file will be deleted, and return to the File Selection Screen.

7 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.

4.4 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 "Incorrect password Please wait for a while" 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.

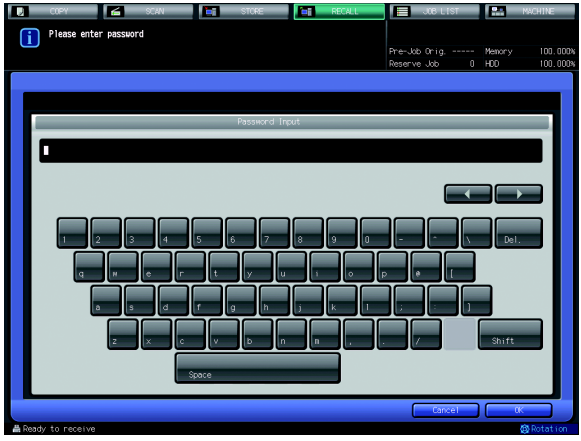
The blank page will not be output even when selecting the blank page for page range in Insert Sheet, Booklet, or Chapter job. The blank page can be set to output. Contact your service representative, if desired.

Outputting secure printing on the machine:

1 Touch [RECALL] tab, then touch [User Name] and [Password] on the User Authentication Screen to enter your user name and password.

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



2 Touch [OK].

The Recall Screen will be displayed.

3 Touch [Secure Folder] to display the Secure Box List Screen.

4 Select the desired secure box, then touch [OK].

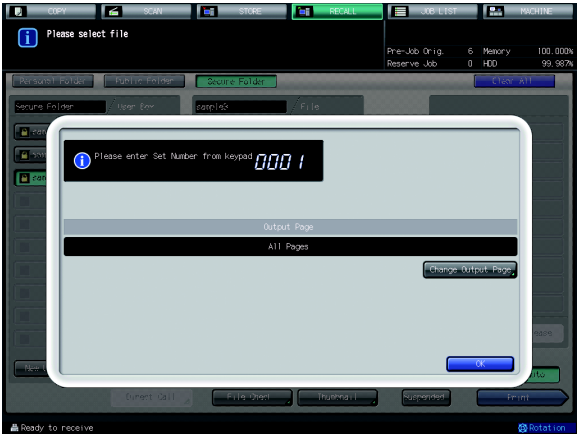
5 Enter the secure password setup in secure printing.
Touch [OK].

The Secure File List Screen will be displayed.

6 Select the desired secure file.

7 Touch [Wait], [Proof], [Proof(1st Sheet)], or [Auto] as desired, then touch [OK].

– The [Proof(1st Sheet)] key does not appear on the screen by default, but can be available in the Utility mode.
– Enter the desired print quantity from touch panel keypad.



– Specify the output page of the image data.
Touch [Change Output Page].
To output desired page(s), touch [Page Select], then enter the page number from the keypad.
Use “, (comma)” between pages, or “- (hyphen)” for consecutive pages.
To output all pages, touch [All Pages].
Touch [OK] to output.

– To continue the output, touch [Yes] on the popup screen. Or, touch [No] to complete it.

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 Administrator Security Functions

The administrator turns Security Strengthen mode ON/OFF.
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 - POD Administrator's Reference.
To protect data in the machine from access and tampering, it is recommended to designate an administrator and use Security Strengthen mode.

5.1 Turn Security Strengthen mode ON/OFF

The following is an explanation of how to turn Security Strengthen 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 "Incorrect password Please wait for a while" will appear, and no key will work for five seconds. Enter the right password after five seconds.

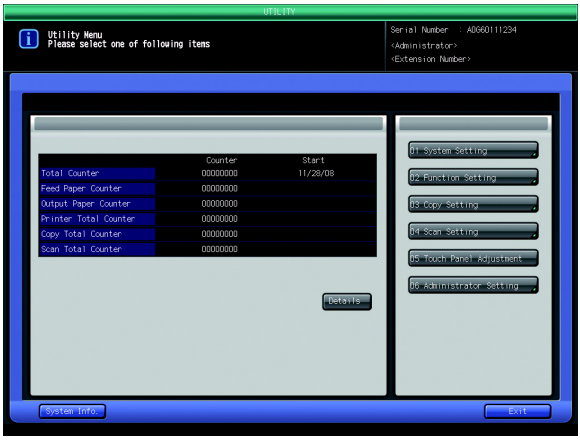
If authentication fails, the information will be saved in the audit log.

Procedure

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

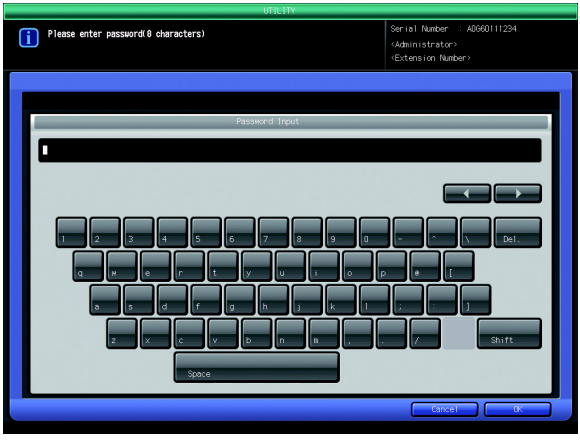
The Utility Screen will be displayed.

2 Touch [06 Administrator Setting].



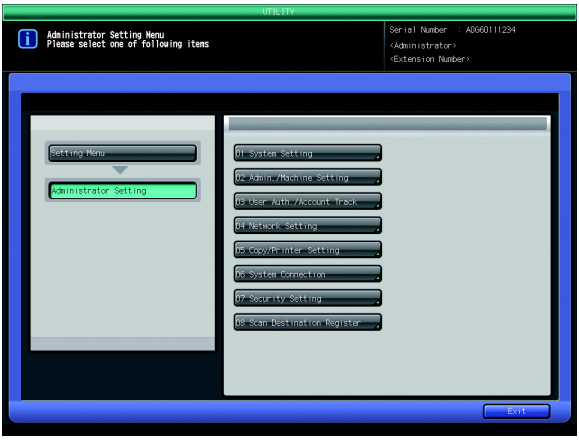
The Input Administrator Password Screen will be displayed.

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

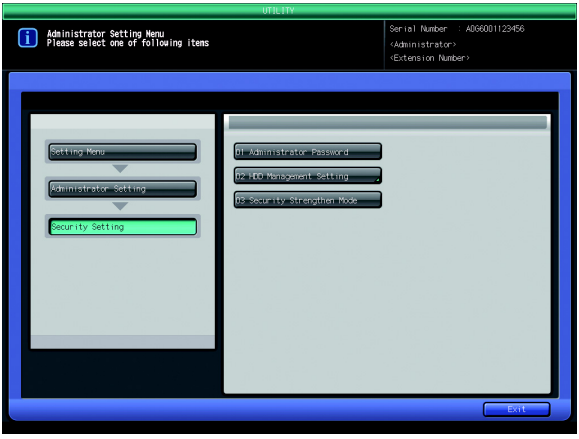


The Administrator Setting Screen will be displayed.

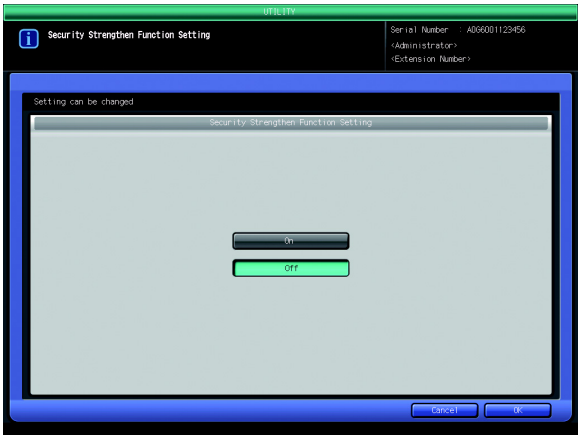
4 Touch [07 Security Setting].



5 Touch [03 Security Strengthen Mode].



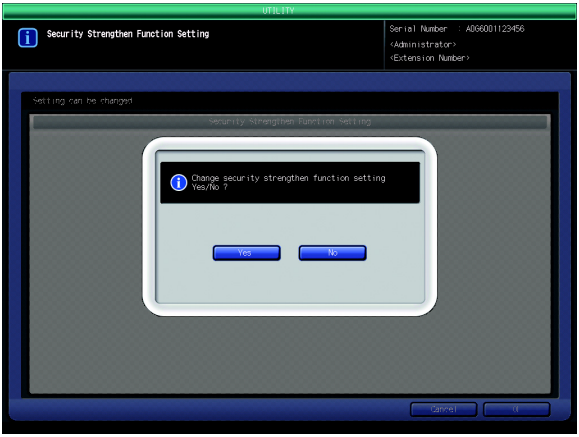
6 Turn Security Strengthen mode ON or OFF.
To turn Security Strengthen mode ON, touch [On].
To turn Security Strengthen mode OFF, touch [Off].

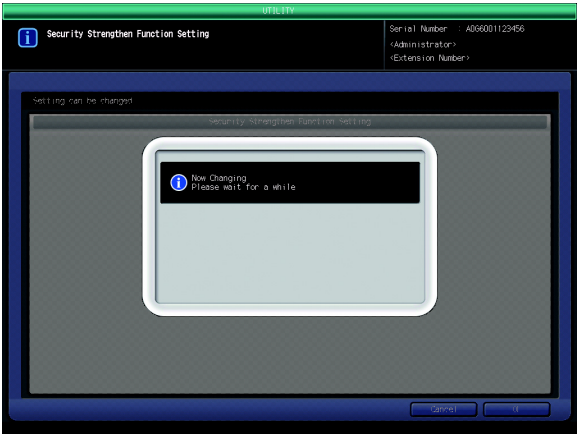


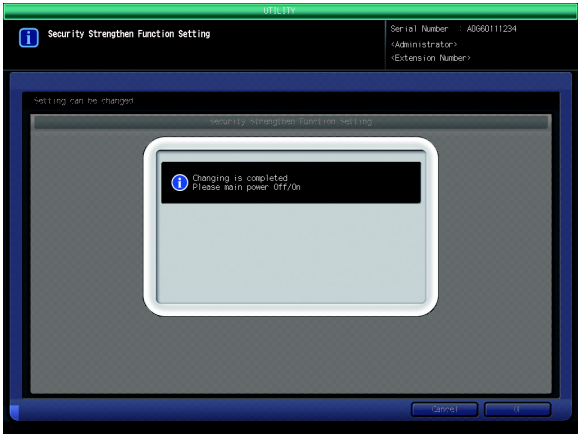
The Specify Completion popup screen will appear.

7 Touch [OK].

A popup message will be displayed to confirm that you are turning the Security Strengthen mode ON/OFF.
Touch [Yes].


UTILITY
Security Strengthen Function Setting
Serial Number : A06G001123456
<Administrator>
<Extension Number>
Setting can be changed
Security Strengthen Function Setting
Change security strengthen function setting
Yes/No ?
Yes
No
Cancel
OK


UTILITY
Security Strengthen Function Setting
Serial Number : A06G001123456
<Administrator>
<Extension Number>
Setting can be changed
Security Strengthen Function Setting
Now Changing
Please wait for a while
Cancel
OK



8 Turn OFF the sub power switch, then turn OFF the main power switch.

– While the message “Cooling in progress After cooling, Power off automatically” is displaying, do not turn OFF the main power.

9 Wait about 10 seconds.

10 Turn ON the main power switch and sub power switch.

5.2 HDD lock password

While the Security Strengthen 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.

Note

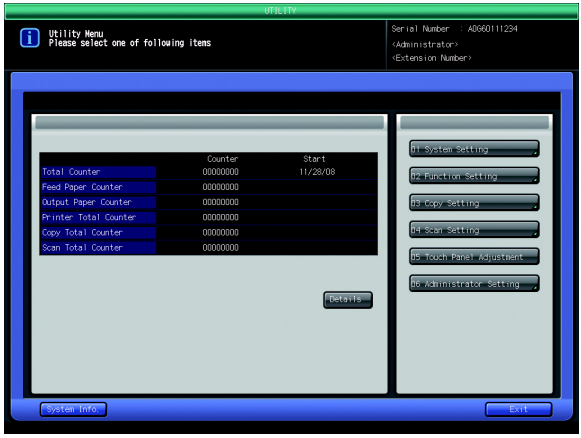
The HDD lock password functions only when the Security Strengthen mode is ON. When turned OFF, the message "Please set Security Strengthen mode" will be displayed.

Procedure

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

The Utility Screen will be displayed.

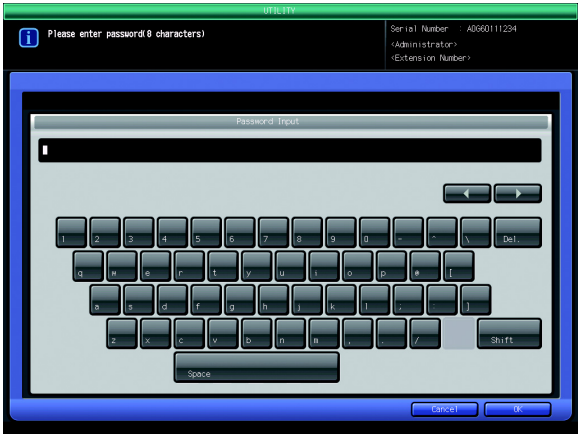
2 Touch [06 Administrator Setting].



The Input Administrator Password Screen will be displayed.

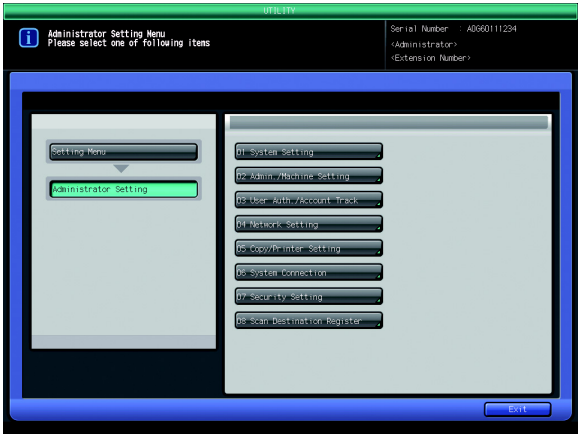
3 Enter the password.
Use the touch panel keypad to enter the 8-digit administrator password, then touch [OK].

- Passwords are case sensitive.
- If a wrong password or fewer than 8 alphanumerical characters are entered and the [OK] is touched, the warning message “Incorrect password Please wait for a while” 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.



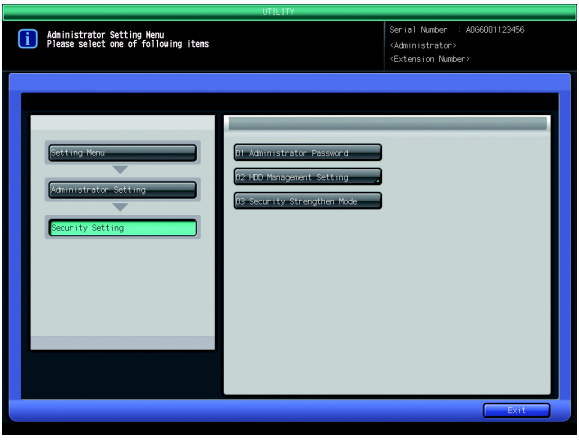
The Administrator Setting Screen will be displayed.

4 Touch [07 Security Setting].



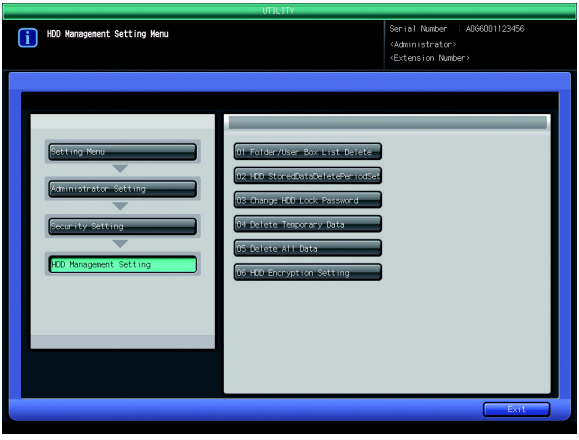
The Security Setting Screen will be displayed.

5 Touch [02 HDD Management Setting].



The HDD Management Setting Screen will be displayed.

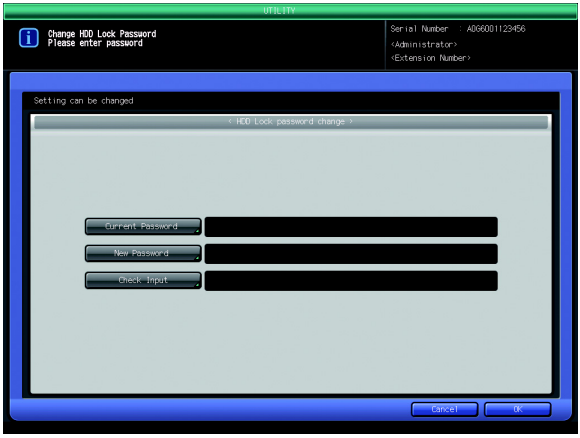
6 Touch [03 Change HDD Lock Password].



The Change HDD Lock Password Screen will be displayed.

7 Touch [Current Password] to enter the password currently used, then touch [OK].
The first password: 9-digit alphanumeric serial number of the main body.

8 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 60 for the sample log.



9 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.
- Touch [OK] to return to the previous screen.

10 Touch [Check Input] to re-enter the same password as above.
Touch [OK] to return to the previous screen.

11 Touch [OK].

5.3 Delete Temporary Data

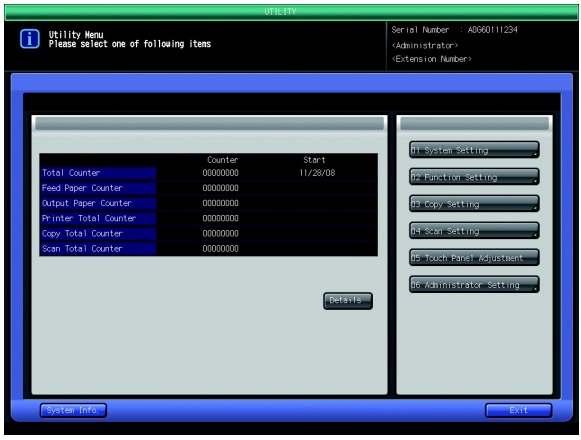
Use this function to select whether or not to erase the temporary data on HDD or DRAM in order to prevent them from being reused. When erasing the data, also select one of the two erase modes provided on the screen.

Procedure

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

The Utility Screen will be displayed.

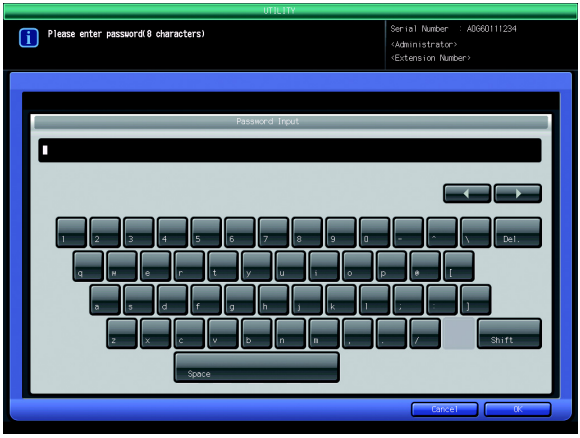
2 Touch [06 Administrator Setting].



The Input Administrator Password Screen will be displayed.

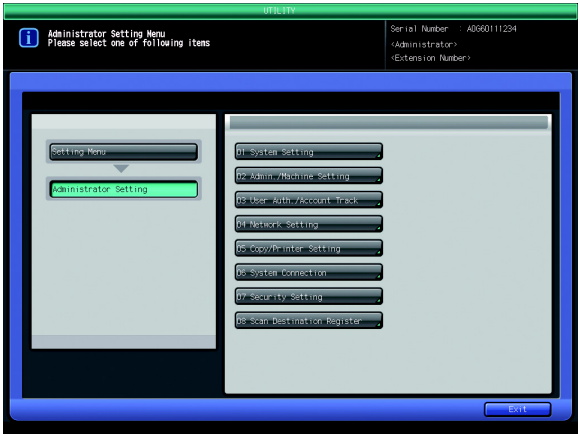
3 Enter the password.
Use the touch panel keypad to enter the 8-digit administrator password, then touch [OK].

- Passwords are case sensitive.
- If a wrong password or fewer than 8 alphanumerical characters are entered and the [OK] is touched, the warning message “Incorrect password Please wait for a while” 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.



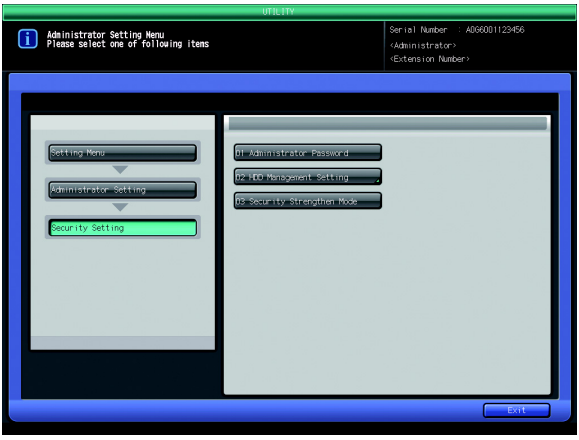
The Administrator Setting Screen will be displayed.

4 Touch [07 Security Setting].



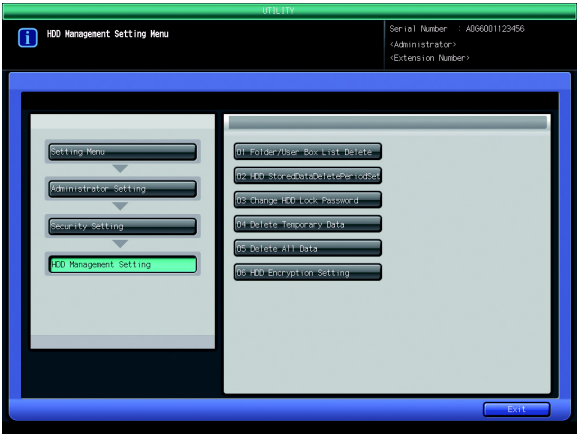
The Security Setting Screen will be displayed.

5 Touch [02 HDD Management Setting].



The HDD Management Setting Screen will be displayed.

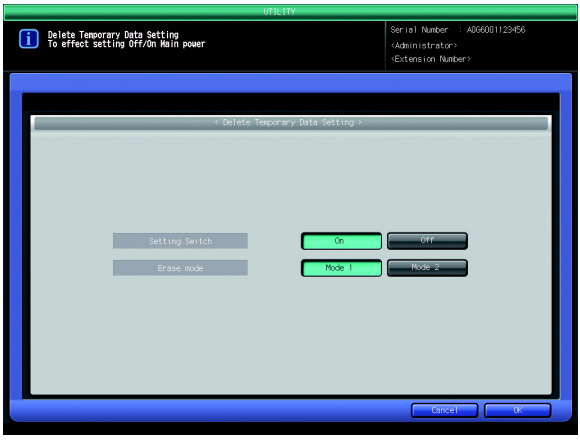
6 Touch [04 Delete Temporary Data].



The Delete Temporary Data Screen will be displayed.

7 Select whether or not to overwrite the temporary data.

– Touch [On] or [Off] to highlight it.



8 Select the desired mode, when selecting [On] in step 7.

– Touch [Mode 1] or [Mode 2] to highlight it.
– When selecting Off in step 7, this mode selection does not make any difference.

9 Touch [OK] on the Delete Temporary Data Screen.

10 Turn OFF the sub power switch and main power switch.

– While the message “Cooling in progress After cooling, Power off automatically” is displaying, do not turn OFF the main power.

11 Wait about 10 seconds or larger.

12 Turn ON the main power switch and sub power switch.

5.4 Delete All Data

Use this function to delete all the data on HDD, selecting one of the eight erase modes provided.

Note

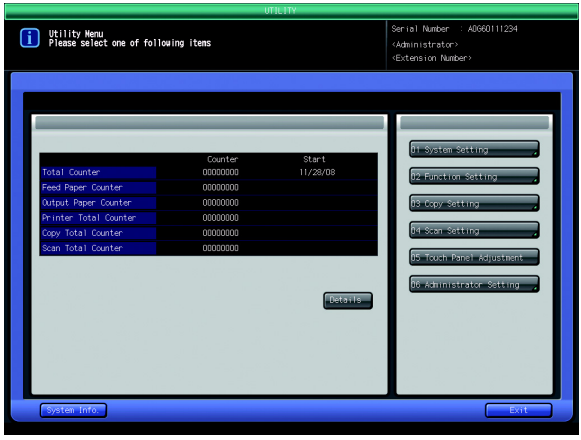
When using this function, contact your service representative.

Procedure

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

The Utility Screen will be displayed.

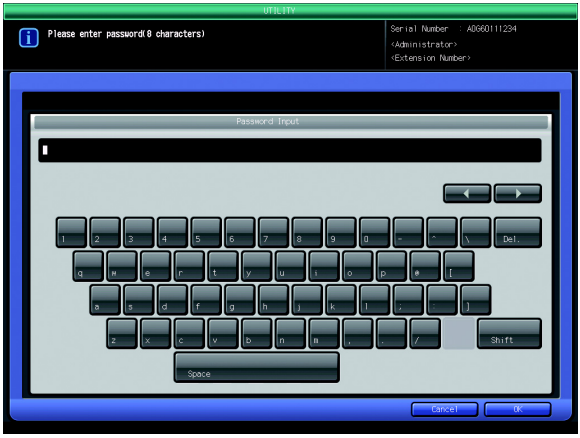
2 Touch [06 Administrator Setting].



The Input Administrator Password Screen will be displayed.

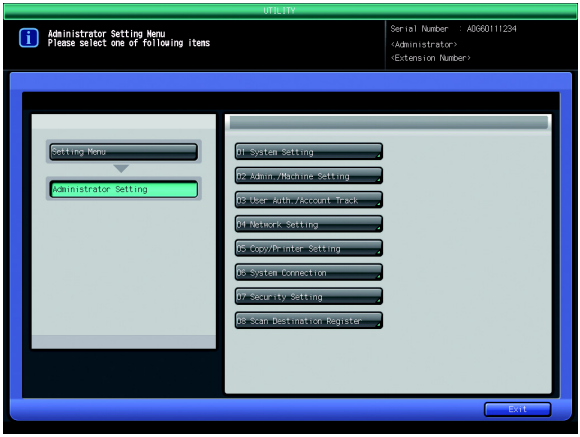
3 Enter the password.
Use the touch panel keypad to enter the 8-digit administrator password, then touch [OK].

- Passwords are case sensitive.
- If a wrong password or fewer than 8 alphanumerical characters are entered and the [OK] is touched, the warning message “Incorrect password Please wait for a while” 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.



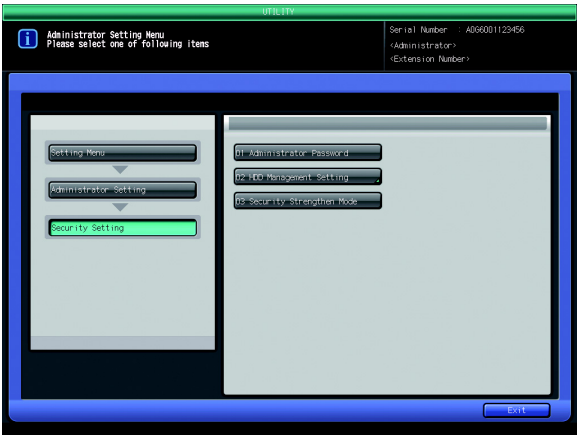
The Administrator Setting Screen will be displayed.

4 Touch [07 Security Setting].



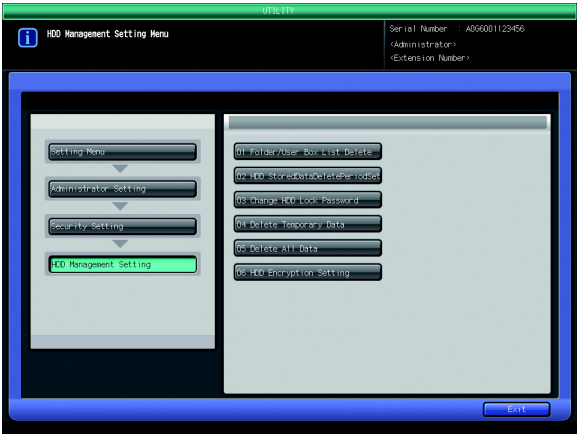
The Security Setting Screen will be displayed.

5 Touch [02 HDD Management Setting].



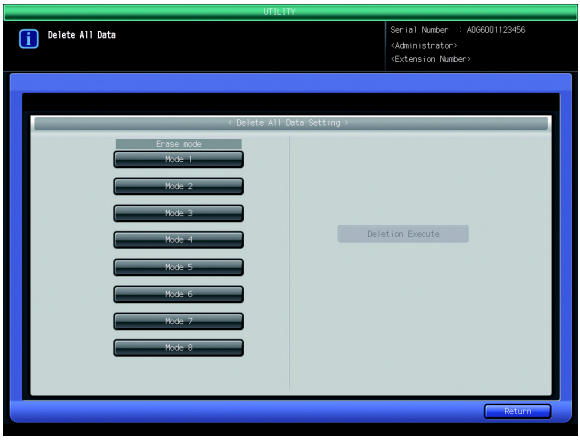
The HDD Management Setting Screen will be displayed.

6 Touch [05 Delete All Data].



The Delete All Data Screen will be displayed.

7 Select the desired erase mode, then touch [Deletion Execute].



8 Touch [Return] on the Delete All Data Screen.

...

Reminder

Touching [Deletion Execute] will clear all the data on HDD and never allow you to recover them. If necessary, save the desired data in another device beforehand.

5.5 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 "Incorrect password Please wait for a while" 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

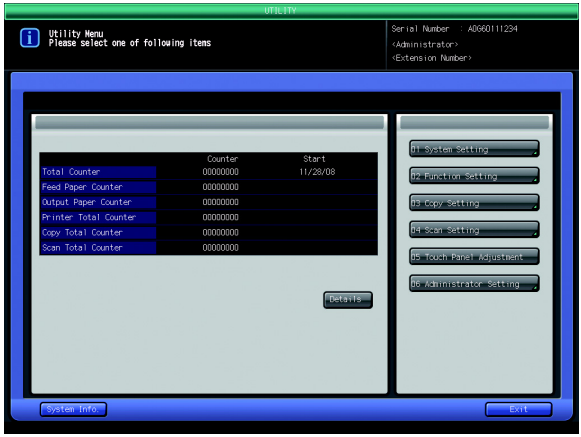
To stop printing, press [Stop] on the control panel, then touch [Cancel] on the confirmation popup screen.

Procedure

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

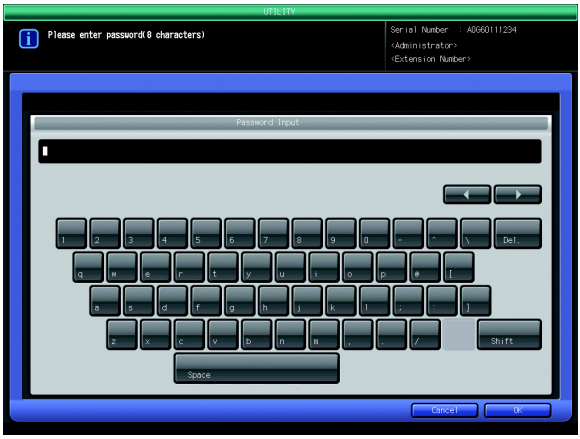
The Utility Screen will be displayed.

2 Touch [06 Administrator Setting].



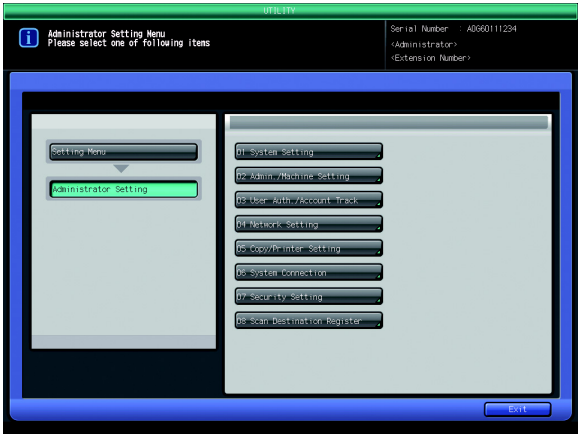
The Input Administrator Password Screen will be displayed.

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



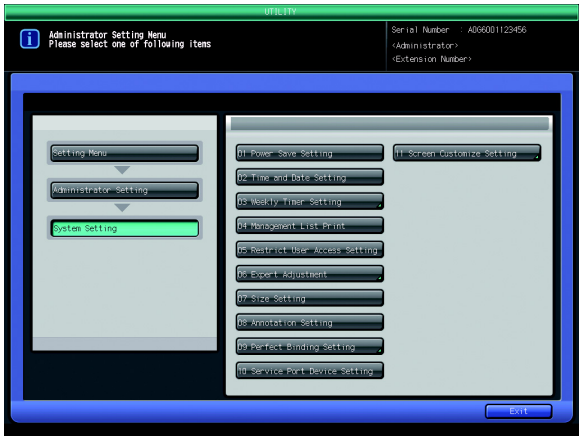
The Administrator Setting Screen will be displayed.

4 Touch [01 System Setting].



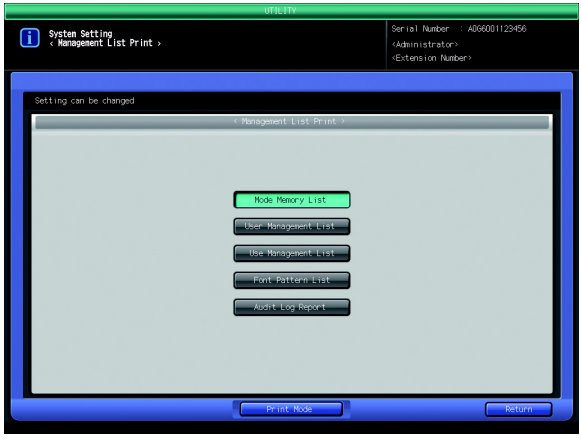
The System Setting Screen will be displayed.

5 Touch [04 Management List Print].



The Print Management List Screen will be displayed.

6 Touch [Audit Log Report], then touch [Print Mode].



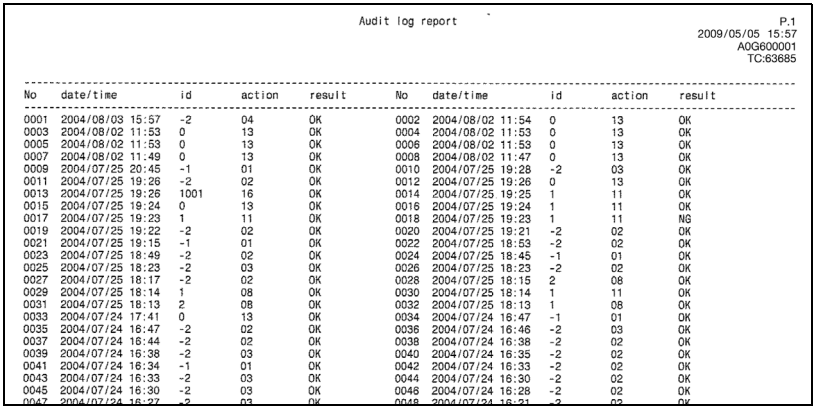
The Print Management List Screen will be displayed.

7 Press [Start] on the control panel.

5.6 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 Security Strengthen 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
2009/05/05 15:57
A0G600001
TC:63685

No	date/time	id	action	result	No	date/time	id	action	result
0001	2004/08/03 15:57	-2	04	OK	0002	2004/08/02 11:54	0	13	OK
0003	2004/08/02 11:53	0	13	OK	0004	2004/08/02 11:53	0	13	OK
0005	2004/08/02 11:53	0	13	OK	0006	2004/08/02 11:53	0	13	OK
0007	2004/08/02 11:49	0	13	OK	0008	2004/08/02 11:47	0	13	OK
0009	2004/07/25 20:45	-1	01	OK	0010	2004/07/25 19:28	-2	03	OK
0011	2004/07/25 19:26	-2	02	OK	0012	2004/07/25 19:26	0	13	OK
0013	2004/07/25 19:26	1001	16	OK	0014	2004/07/25 19:25	1	11	OK
0015	2004/07/25 19:24	0	13	OK	0016	2004/07/25 19:24	1	11	OK
0017	2004/07/25 19:23	1	11	OK	0018	2004/07/25 19:23	1	11	NG
0019	2004/07/25 19:22	-2	02	OK	0020	2004/07/25 19:21	-2	02	OK
0021	2004/07/25 19:15	-1	01	OK	0022	2004/07/25 18:53	-2	02	OK
0023	2004/07/25 18:49	-2	02	OK	0024	2004/07/25 18:45	-1	01	OK
0025	2004/07/25 18:23	-2	03	OK	0026	2004/07/25 18:23	-2	02	OK
0027	2004/07/25 18:17	-2	02	OK	0028	2004/07/25 18:15	2	08	OK
0029	2004/07/25 18:14	1	08	OK	0030	2004/07/25 18:14	1	11	OK
0031	2004/07/25 18:13	2	08	OK	0032	2004/07/25 18:13	1	08	OK
0033	2004/07/24 17:41	0	13	OK	0034	2004/07/24 16:47	-1	01	OK
0035	2004/07/24 16:47	-2	02	OK	0036	2004/07/24 16:46	-2	03	OK
0037	2004/07/24 16:44	-2	02	OK	0038	2004/07/24 16:38	-2	02	OK
0039	2004/07/24 16:38	-2	03	OK	0040	2004/07/24 16:35	-2	02	OK
0041	2004/07/24 16:34	-1	01	OK	0042	2004/07/24 16:33	-2	02	OK
0043	2004/07/24 16:33	-2	03	OK	0044	2004/07/24 16:30	-2	02	OK
0045	2004/07/24 16:30	-2	03	OK	0046	2004/07/24 16:28	-2	02	OK
0047	2004/07/24 16:27	-2	03	OK	0048	2004/07/24 16:21	-2	02	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.

5.7 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 Security Strengthen 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.

6 Index

A

Administrator Security Functions 49

Audit log
- Analyze 70
- Box 27, 33, 39, 44
- Change a user data 14
- Change password 23
- Delete a user 19
- Print 67

D

Delete All Data 63

Delete Temporary Data 59

O

Output
- Data in the Secure Box 44

R

Recall/Delete
- Data in a Box 39
- Register a new user 8

S

Security Strengthen mode 49
- Administrator authentication 4
- Administrator setting mode 4
- Audit log 3
- Data protected 5
- Enhanced password 3
- Environments 2
- HDD 27
- HDD lock password 55
- HDD store function 27
- Normal mode 1
- Protect and delete used data ...3, 6
- Turn ON/OFF 5

Store 27
- Data in a Box while copying 27
- Scanned data in a Box 33

User authentication 7

KONICA MINOLTA

http://konicaminolta.com

A0G6956722

Printed in China
2010. 7