KONICA MINOLTA

Giving Shape to Ideas

bizhub PRESS 1250/1052

User's Guide Security

1 Introduction
- 1.1 Welcome
- 1.2 Conventions Used in This Manual

2 Security Funtions
- 2.1 Control Software
- 2.2 Security Functions
- 2.3 User Authentication in Enhanced Security Mode
- 2.4 HDD Store Function in Enhanced Security Mode
- 2.5 Administrator Security Functions

3 Index

Contents

1 Introduction

1.1 Welcome ... 1-2
1.1.1 Composition of User's Guide ... 1-2
1.1.2 User's Guide ... 1-3
1.2 Conventions Used in This Manual ... 1-4
1.2.1 Symbols Used in This Manual ... 1-4
1.2.2 Original and Paper Indications ... 1-5

2 Security Functions

2.1 Control Software ... 2-2
2.1.1 Control Software Version ... 2-2
2.1.2 About the ROM Version Display Function ... 2-2
2.2 Security Functions ... 2-3
2.2.1 Security Mode ... 2-3
2.2.2 Environment ... 2-3
2.2.3 Description of Enhanced Security Mode ... 2-4
2.2.4 Data Protected by the Enhanced Security Mode ... 2-6
2.2.5 Protecting and Deleting of Remaining Data After Being Used ... 2-6
2.3 User Authentication in Enhanced Security Mode ... 2-7
2.3.1 Adding User Registration ... 2-7
2.3.2 Changing User Registration ... 2-13
2.3.3 Deleting User Data ... 2-18
2.3.4 Changing Password by User ... 2-20
2.4 HDD Store Function in Enhanced Security Mode ... 2-24
2.4.1 Saving Data While Copying ... 2-24
2.4.2 Saving Data in User Box ... 2-27
2.4.3 Recalling and Deleting of Data ... 2-31
2.4.4 Output Data in the Secure Box ... 2-35
2.5 Administrator Security Functions ... 2-39
2.5.1 Turning the Enhanced Security Mode ON/OFF ... 2-39
2.5.2 HDD Lock Password ... 2-42
2.5.3 Deleting Temporary Data ... 2-44
2.5.4 Deleting All Data ... 2-47
2.5.5 Printing Audit Log ... 2-50
2.5.6 Analyzing Audit Log ... 2-52

3 Index

3.1 Index by item ... 3-2
3.2 Index by button ... 3-3

MEMO

1 Introduction

1 Introduction

1.1 Welcome

Thank you for purchasing this machine.

This User's Guide describes security functions. Please read this guide for comprehension of how to use the Enhanced Security mode and detailed machine operations in Enhanced Security mode.

1.1.1 Composition of User's Guide

Printed manuals	Overview
[User's Guide - Security]	This guide describes the security functions. Please read this guide for comprehension of how to use the Enhanced Security mode and detailed machine operations in Enhanced Security mode.
[Operation Quick Guide]	This guide mainly describes how to use frequently used functions. Please read this guide for quick comprehension of various features available on the machine.
[Safety Information]	This guide provides precautions and requests that should be followed to ensure safe usage of this machine. Please be sure to read this guide before using the machine.

User's guide CD manuals	Overview
[User's Guide - Copier]	This guide describes an outline of the machine and copy operations. • Configuration and specifications of the main body and options • Turning on/off the machine • Paper information • Making a basic copy and setting procedures • Supplies and disposals • Application, Output Setting, and Job List • Troubleshooting
[User's Guide - POD Administrator's Reference]	This guide provides you with detailed information on machine management and how to customize the machine according to your daily use. • Tray Setting • Both Sides Adjust • Controller Setting • Adjustment, Utility Menu Screen • Network Setting • PageScope Web Connection • Web Utilities
[User's Guide - Printer]	This guide describes the settings of the printer drivers and utility tools. • PCL driver • PS Plug-in driver • PS PPD driver • PageScope Web Connection

User's guide CD manuals	Overview
[User's Guide - Network Scanner]	This guide describes operations of the network scanner functions. • Saving on the HDD for main body/Outputting • Sending via e-mail • Saving on the HDD for controllers • Sending to FTP server • Sending to SMB server • Sending to group
[Trademarks/Copyrights]	This guide describes trademarks, licenses, and copyrights concerning this machine. Please be sure to refer to this guide before using the machine.

1.1.2 User's Guide

This User's Guide is intended for users ranging from those using this machine for the first time to administrators.

This guide provides those users to manage security functions.

Should you experience any problems, please contact your service representative.

1.2 Conventions Used in This Manual

1.2.1 Symbols Used in This Manual

Symbols are used in this manual to express various types of information.

The following describes each symbol related to correct and safe usage of this machine.

To use this machine safely

⚠ WARNING

- This symbol indicates that a failure to heed the instructions may lead to death or serious injury.

⚠ CAUTION

- This symbol indicates that negligence of the instructions may lead to mishandling that may cause injury or property damage.

NOTICE

This symbol indicates a risk that may result in damage to this machine or originals. Follow the instructions to avoid property damage.

Procedural instruction

✔ This check mark indicates an option that is required in order to use conditions or functions that are prerequisite for a procedure.

1 This format number "1" represents the first step.

2 This format number represents the order of serial steps.

➔ This symbol indicates a supplementary explanation of a procedural instruction.

The operation procedures are described using illustrations.

➔ This symbol indicates transition of the control panel to access a desired menu item.

The relevant page is shown.

Reference

This symbol indicates a reference.

View the reference as required.

Key symbols

[ ]

Key names on the touch panel or computer screen, or a name of user's guide are indicated by these brackets.

Bold text

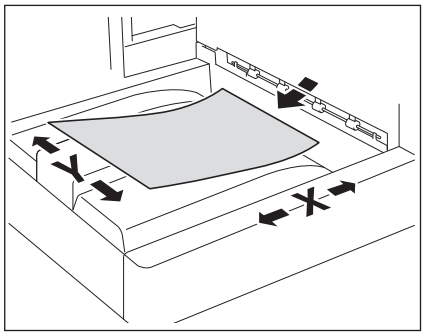
Key names on the **control panel**, part names, product names and option names are indicated in bold text.

1.2.2 Original and Paper Indications

Paper size

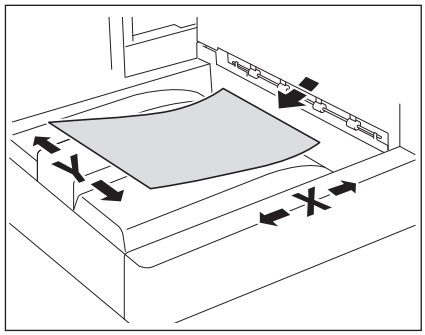
The following explains the indication for originals and paper described in this manual.

When indicating the original or paper size, the Y side represents the width and the X side the length.

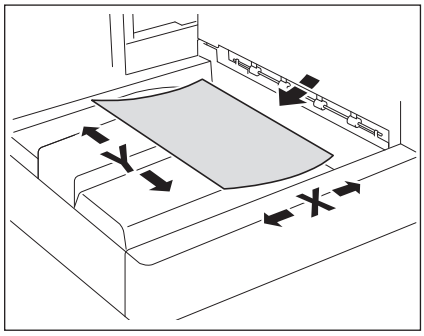


Paper indication

▭ indicates the paper size with the length (X) being longer than the width (Y).



▯ indicates the paper size with the length (X) being shorter than the width (Y).



MEMO

2 Security Functions

2 Security Functions

2.1 Control Software

2.1.1 Control Software Version

The version of control software is as follows.

This software consists of an image control program and a controller control program.

Image control program (Image Control I1) version:

A4EU0Y0-00I1-G00-20

Controller control program (IC Controller P) version:

A4EU011-00P1-G00-20

2.1.2 About the ROM Version Display Function

The version of **bizhub PRESS 1250/1052** control software (image control program) mentioned above can be checked by the ROM version display function in the customer engineer (CE) service mode.

When the ROM version display function is used, the version of image control program will be displayed as follows.

A4EU0Y0-00I1-G00-**

Image control program (Image Control I1) version: G00-2 digits (ex. G00-**)

Please keep this in mind when checking the version of image control program.

2.2 Security Functions

2.2.1 Security Mode

The **bizhub PRESS 1250/1052** has two security modes.

Normal mode

Use this mode when the machine is used by a single person and there is low possibility of illicit access or operation. This mode is already set as factory default. To use the machine in normal mode, please refer to the user's guides provided for each operation.

Enhanced Security mode

Use the Enhanced Security mode when the machine is connected to a local area network, or to external networks through a telephone line or other means. An administrator determined for the machine management should follow the instructions in this guide, so that users can have a safe operating environment.

To use the Enhanced Security mode, please contact your service representative for the following settings.

A service representative should set a CE password for CE authentication and administrator password on the machine. The service representative uses the CE password for CE works. The administrator, who obtains the administrator password from the service representative, uses that password to make settings related to the Enhanced Security mode.

The administrator should never leak the administrator password out to others.

The administrator who acquired the administrator password manages the machine set up with the Enhanced Security mode by making the following settings:

- Turning on/off the Enhanced Security mode
- Adding/Changing registered users
- Deleting registered users
- HDD lock password

The administrator is also responsible in providing users with the following instructions:

- Never leak his/her password out to others.
- Be sure to log out when completing the machine operation after logging in upon the user authentication.

Please be sure to use the Enhanced Security mode to prevent unauthorized access to HDD.

With the Enhanced Security mode activated, the machine displays a security icon 

in the lower-right area of the touch panel.

The security icon will disappear when the Enhanced Security mode is deactivated. If the administrator accidentally deactivates the Enhanced Security mode, please contact your service representative. You should ask a customer engineer (CE) to check the security environment and settings before activating the Enhanced Security mode again.

2.2.2 Environment

Environment in which the Enhanced Security mode is recommended

An environment where the machine is monitored by a telephone line or a network

Creating a secure environment

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

Secure print files and authentication print files are not encrypted during transmission from a client PC to the machine. Please implement measures against wiretapping, such as installing a cryptographic communication device or antibugging equipment, in order to protect secure print files and authentication print files.

- Qualifications to be an administrator:
  A supervisor selects a reliable person who has adequate knowledge, technical ability, and experience as an administrator, to whom to delegate administration of the machine.

- Guarantee of customer engineer (CE):
  A supervisor or an administrator can use the Enhanced Security mode after confirming that a service contract has been signed with a customer engineer (CE). Clearly state in the service contract that the customer engineer (CE) will not engage in any fraudulent actions.
- Secure LAN:
  Be sure to connect the machine to a local area network protected by firewall in order to prohibit access from external networks. Be also sure not to have any illicit device connected to the LAN.
- An administrator should designate the installation location to be available only for product users. Install the machine in a place securely locked during the night, and during the day in a place that allows the administrator to monitor the machine, so that any parts such as an HDD should not get stolen or any special device such as an internal analyzer should not be hooked up to the machine. Equipment removed from the main body, such as an HDD, should also be managed similar to the main body.
- An administrator is required to be present at customer engineer (CE) works such as installation or maintenance.
- An administrator should check at regular intervals that the date/time setting is correctly made on the machine.

2.2.3 Description of Enhanced Security Mode

Security functions will be enhanced as follows.

Protecting and deleting of remaining data after being used

There are two types of Image data stored in memory or HDD: AHA compressed data and uncompressed data, which are TIFF format, PDF format, and PS data. The image area of memory or HDD with AHA compressed data will be released after clearing the used data. In normal mode, the data is not completely deleted, which may allow for unauthorized reading of the data. In Enhanced Security mode, the image area of memory or HDD is overwritten with data unrelated to the image before the area is released, irrespective of whether the stored image data is compressed.

Enhanced passwords

There are 5 different passwords provided for security functions.

- CE password
- Administrator password
- User password
- Account password
- HDD lock password

The CE password and account password should be comprised of 8 alphanumeric characters (the alphabetic characters are case-sensitive).

For the administrator password, the following 32 symbols can be used in addition to alphanumerics (case-sensitive) to comprise 8 characters:

-^\@[]:;,./!"#$%&'()=~|`{+*}<>?_

The user password is normally made from 1 to 64 alphanumeric characters (case-sensitive); however, the user password less than 8 characters will be unavailable in the Enhanced Security mode. If you enter 64 or more characters, the last entered character will be identified as the 64th character.

The HDD lock password should be made from 8 to 32 alphanumeric characters (case-sensitive). If you enter 32 or more characters, the last entered character will be identified as the 32nd character.

As for the CE password, administrator password and account password, the machine recognizes the last entered character as the eighth character if 8 or more characters are entered.

The machine in the Enhanced Security mode also refuses any entry for 5 seconds, if a wrong password is entered for one of the 5 passwords mentioned above.

Should you forget any security-related password, please take action as follows depending on the type of password.

- For a user password or account password, please contact your administrator.
- If you have forgotten the administrator password or HDD lock password, please contact your service representative.

We recommend that each password should be changed on a regular basis in order to prevent illicit access or falsification of data.

Data access

Ensure that a user is required to enter an enhanced password which has been set by the administrator, in order to save data into the user box stored in HDD or output the stored data.

When saving scanned data into a user box, you can improve security by setting an enhanced password. Only administrators can delete folders and user boxes in which scanned data resides. Once a user box attribute has been changed, user authentication with an enhanced password is required. User authentication is also required for using saved scanned data.

Machine NIC settings

While the Enhanced Security mode is activated, the machine NIC cannot be used.

Blocking external accesses

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 as an audit log. 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 accesses. This log will be overwritten if the audit area is depleted.

Administrator authentication

A service representative is supposed to set up an authentication data for an administrator. According to this authentication data, the administrator gains authorized access by entering the administrator password. Only one authentication string can be registered per machine.

Administrator setting mode

The machine enters the administrator setting mode when password authentication is successfully made by the administrator. In the administrator setting mode, setting change of various machine functions is available.

Be sure to exit the administrator setting mode if you leave in front of the machine while using this mode.

IC card

With the Enhanced Security mode activated, the machine rejects the user authentication using an IC card.

USB port functions

The following functions are still available using a USB port even when the Enhanced Security mode is activated:

- USB Memory ISW
- Printing charts via USB (for CE)
- Keyboard, mouse

Printer

A printer controller and a printer driver are required for printed output. Using the printer controller which supports the Enhanced Security mode, you can store the print data in the internal memory or on the HDD by entering a user name from the printer driver. The stored data can be output after successful authentication of the user name with its corresponding password entered from the printer driver when the data was stored. Please note that the stored data can potentially be output by others if you use somebody else's user name to store the print data.

For details of the printer controller and printer driver which support the Enhanced Security mode, contact your service representative.

For the operation procedure of the printer controller or printer driver, please refer to the user's guide for each.

2.2.4 Data Protected by the Enhanced Security Mode

Enhanced Security Mode improves the security of data for users. Such data includes:

- Data stored within a personal folder (with password)

Also, the following data managed by the administrator is better secured:

- User data
- Data to manage the machine

Data exempted from the protection of Enhanced Security mode

When the machine is connected to PCs on a local network, passwords entered from PCs are not subject to the Enhanced Security mode. Please do not enter any password from such PCs for prevention of leakage.

Turning Enhanced Security mode ON/OFF

The administrator is responsible for turning the Enhanced Security mode ON/OFF.

The administrator should never fail to activate the Enhanced Security mode. Please be especially careful when turning the Enhanced Security mode OFF, being aware that data can potentially be accessed.

2.2.5 Protecting and Deleting of Remaining Data After Being Used

Data from copy, scan, and printer modes are stored temporarily into memory or HDD, and then deleted after being used if there was no operation such as storing them into a user box.

The data is compressed in a special way and generally it cannot be externally decompressed. When compressed data is deleted, a part of the data is either destroyed or overwritten and will not be able to be decompressed.

- The data temporarily stored in memory will be overwritten with invalid data when the job is interrupted or ended.
- The data stored in several areas of memory will be overwritten with invalid data simultaneously.

The data stored in a box will be overwritten with invalid data when a delete order is issued.

- If data is transmitted externally, it will be overwritten with invalid data when the transmission is completed.
- If the administrator issues a delete order for each box, it will be overwritten with invalid data.

2.3 User Authentication in Enhanced Security Mode

When the Enhanced Security mode is activated, functions related to the user authentication will be enhanced as follows.

- The setting item [User Authentication] on the screen accessed from [06 Administrator Setting] - [03 User Auth./Account Track] - [01 Authentication Method] is automatically set to [ON (MFP)].
- User authentication is always required under the following conditions to deal with user data to be protected:

– The **main power switch** is turned off.
– The **sub power switch** is turned off.
– **Access** on the **control panel** is pressed.
– [RECALL], [COPY], [SCAN], or [STORE] on the touch panel is pressed.
– Auto reset function is activated.

- The password for user authentication (user password) must be 8 to 64 alphanumeric characters (the alphabetic characters are case-sensitive). Otherwise, the password becomes unavailable. To continue using the user name with a password less than 8 characters specified, the administrator should change the password to be 8 characters or more.
- If a wrong user name/password (or account name/password) is entered in authentication, attempts to retry cannot be made for 5 seconds.
- With the Enhanced Security mode activated, the machine rejects the user authentication using an IC card.

When a user accesses a user box with a specified password in HDD, all the password authentication operations are recorded as audit logs.

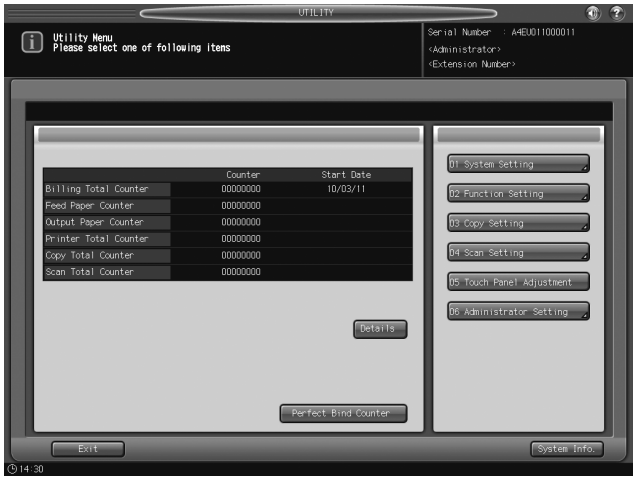
Initially, user authentication is not available. When enabling the user authentication, you should change the number of accounts to be distributed according to your needs. Please refer to the POD Administrator's Reference for details.

2.3.1 Adding User Registration

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

1 Press **Utility/Counter** on the **control panel** to display the Utility Menu Screen.

2 Press [06 Administrator Setting].



A password entry screen will be displayed.

3 Enter the administrator password.

Use the touch panel keypad to enter the administrator password consisting of 8 alphanumeric characters and symbols, then press [OK].

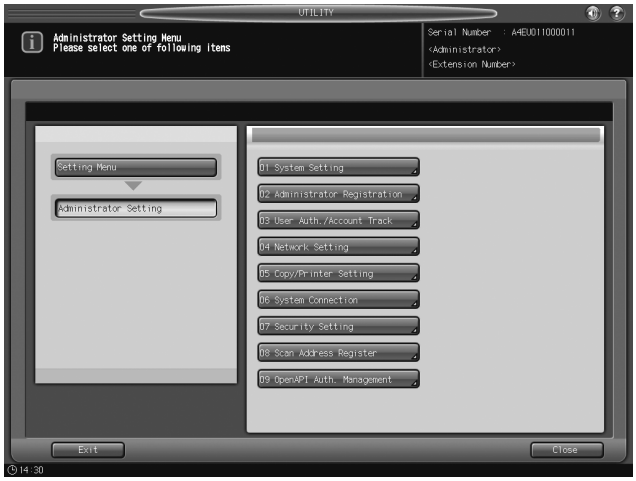
➔ Passwords are case-sensitive.

➔ If a wrong password or fewer than 8 alphanumeric characters/symbols are entered and [OK] is pressed, the warning message [Incorrect password / Please wait for a while] will appear, and no key will work for five seconds. Enter the correct password after five seconds.

➔ The most recently used password cannot be set.
➔ The information on failed authentication will be saved in the audit log.
➔ The number of characters entered will appear as the same number of asterisks "*" on the screen.

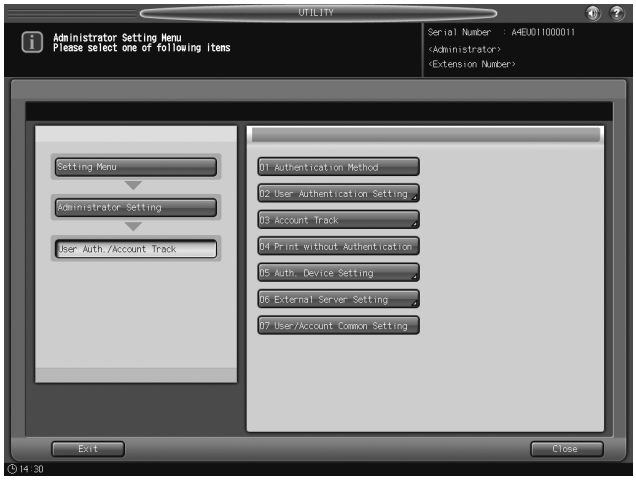
The Administrator Setting Menu Screen will be displayed.

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



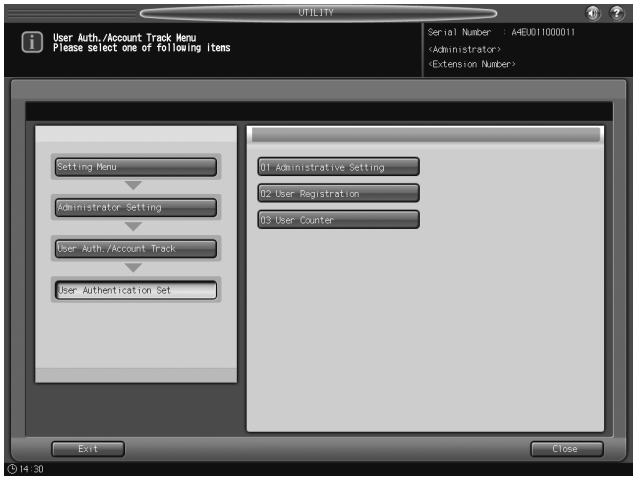
The User Auth./Account Track Menu Screen will be displayed.

5 Press [02 User Authentication Setting].



The User Authentication Setting Menu Screen will be displayed.

6 Press [02 User Registration].

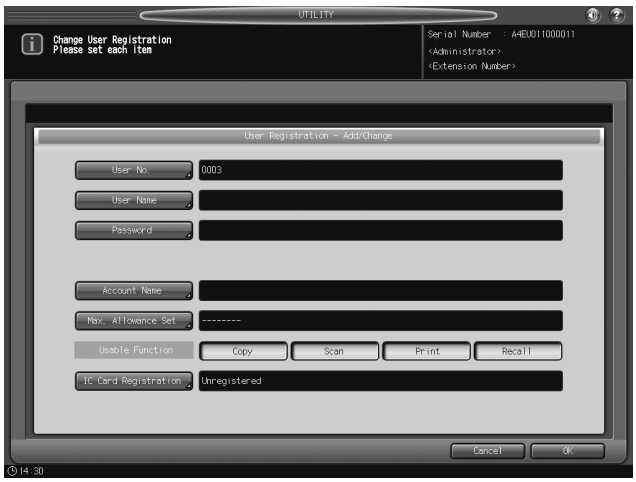


The User Registration Screen will be displayed.

7 Press [Add].

The User Registration - Add/Change Screen will be displayed.

8 Press [User No.].



Use the touch panel keypad, [▼], or [▲] to enter the desired user number.

➔ You may use 1 to 1000 for the user number.

Press [OK] to return to the User Registration - Add/Change Screen.

9 Press [User Name].

The User Name Setting Screen will be displayed. Enter the desired user name.

➔ You may enter up to 64 alphanumeric characters including symbols for the user name. The user name cannot be duplicated.

Press [OK] to return to the User Registration - Add/Change Screen.

10 Press [Password].

The Password Setting Screen will be displayed. Enter a user password which corresponds to the user name entered in step 9.

➔ Enter 8 to 64 alphanumeric characters for the user password (the alphabetic characters are case-sensitive).

NOTICE

Be sure to use 8 or more alphanumeric characters for the password. A password less than 8 characters cannot be used when the Enhanced Security mode is activated.

Press [OK] to return to the User Registration - Add/Change Screen.

11 Press [Account Name].

The Account Name Screen will be displayed. Select the desired account.

NOTICE

If [Synchronize User/Account Track] of Authentication Method is set to [Synchronize], you can set [Account Name].

NOTICE

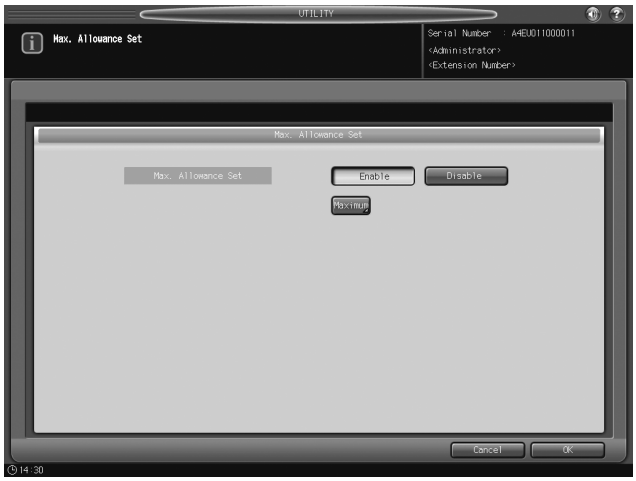
The account should be registered in advance. Select one of the registered accounts provided on the screen.

Press [OK] to return to the User Registration - Add/Change Screen.

12 Press [Max. Allowance Set].

➔ Specify the maximum number of prints to be allowed for the user after a successful authentication.

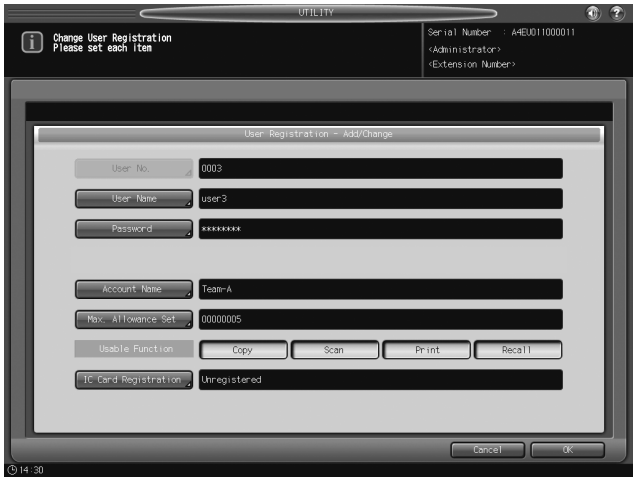
➔ In [Max. Allowance Set], press [Enable] on the right, and then press [Maximum].



➔ Use the touch panel keypad, [▼], or [▲] to enter the desired number of allowed prints. Available range for the allowance is from 1 to 99,999,999.

➔ Press [OK] twice to return to the User Registration Screen.

13 Press [Copy], [Scan], [Print], or [Recall] on the right of [Usable Function] to select function(s) of the machine available to the user.



14 Press [OK].

➔ When settings are completed, press [Return] on the User Registration Screen.

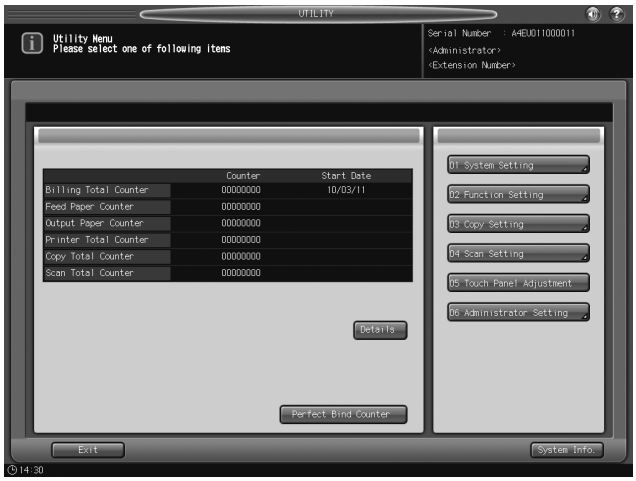
The User Authentication Setting Menu Screen will be restored.

2.3.2 Changing User Registration

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

1 Press **Utility/Counter** on the **control panel** to display the Utility Menu Screen.

2 Press [06 Administrator Setting].



A password entry screen will be displayed.

3 Enter the administrator password.

Use the touch panel keypad to enter the administrator password consisting of 8 alphanumeric characters and symbols, then press [OK].

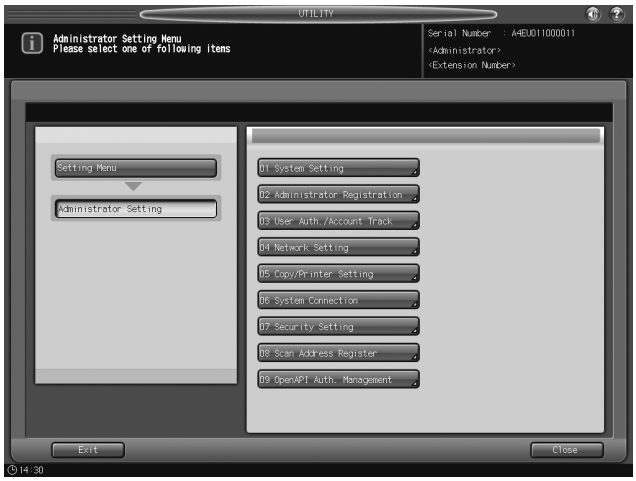
➔ The alphabetic characters are case-sensitive.

➔ If a wrong password or fewer than 8 alphanumeric characters/symbols are entered and [OK] is pressed, the warning message [Incorrect password / Please wait for a while] will appear, and no key will work for five seconds. Enter the correct password after five seconds.

➔ The information on failed authentication will be saved in the audit log.

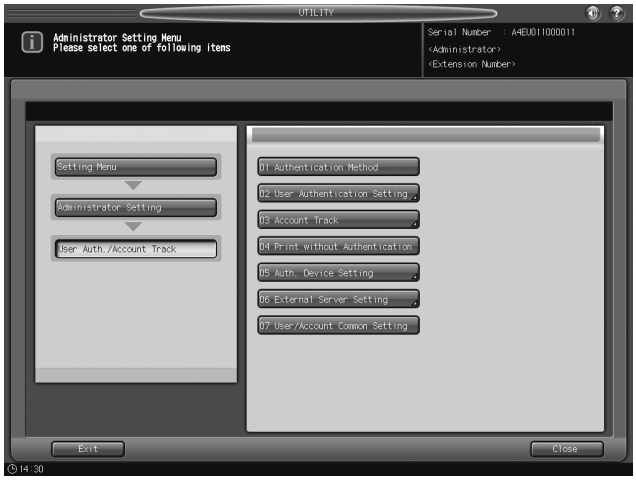
The Administrator Setting Menu Screen will be displayed.

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



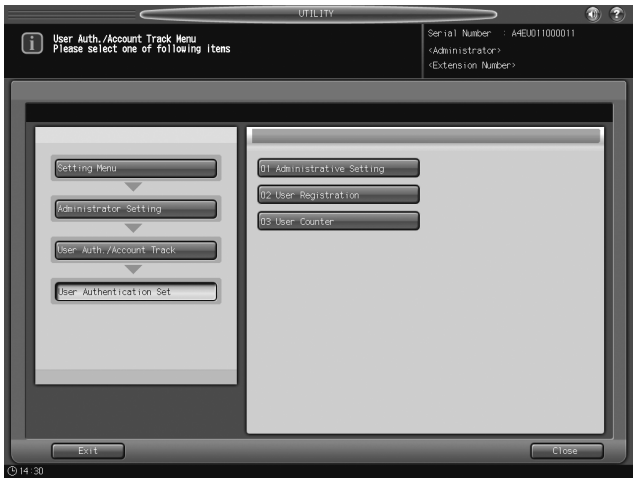
The User Auth./Account Track Menu Screen will be displayed.

5 Press [02 User Authentication Setting].



The User Authentication Setting Menu Screen will be displayed.

6 Press [02 User Registration].



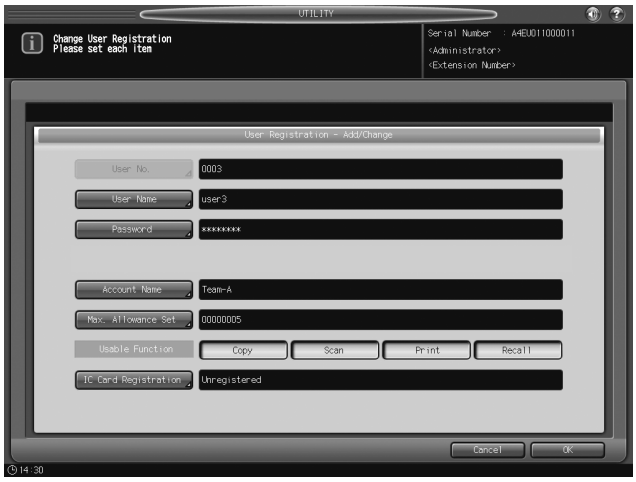
The User Registration Screen will be displayed.

7 Select the key with the user number and user name to be changed.

8 Press [Change] to display the User Registration - Add/Change Screen.

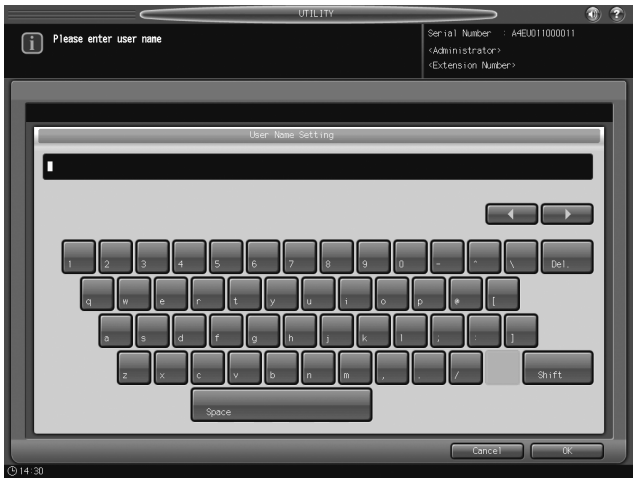
➔ The user number cannot be changed.

9 To change the user name, press [User Name].



10 Enter a new user name.

➔ You may enter up to 64 alphanumeric characters including symbols for the user name. The user name cannot be duplicated.



Press [OK] to return to the User Registration - Add/Change Screen.

11 To change the password, press [Password].

➔ The Password Setting Screen will be displayed. Enter a new user password which corresponds to the user name entered in step 9.

➔ Enter 8 to 64 alphanumeric characters for the user password (the alphabetic characters are case-sensitive).

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

Press [OK] to return to the User Registration - Add/Change Screen.

12 To change the account, press [Account Name].

➔ The Account Name Screen will be displayed. Select the desired account.

NOTICE

If [Synchronize User/Account Track] of Authentication Method is set to [Synchronize], you can set [Account Name].

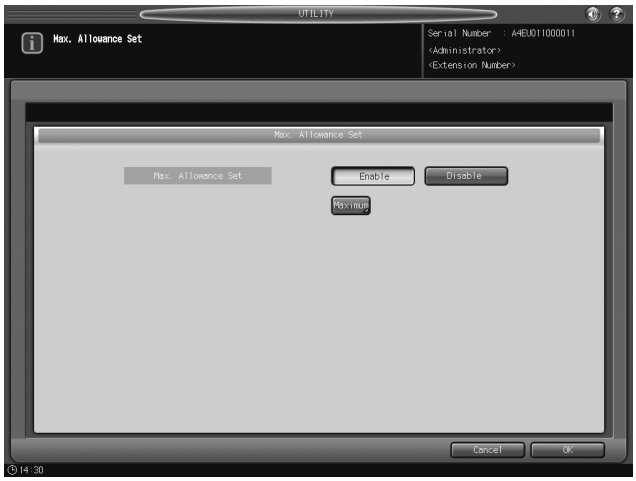
NOTICE

The account should be registered in advance. Select one of the registered accounts provided on the screen.

Press [OK] to return to the User Registration - Add/Change Screen.

13 To change the allowance, press [Max. Allowance Set]. Change the maximum number of prints to be allowed for the user after a successful authentication.

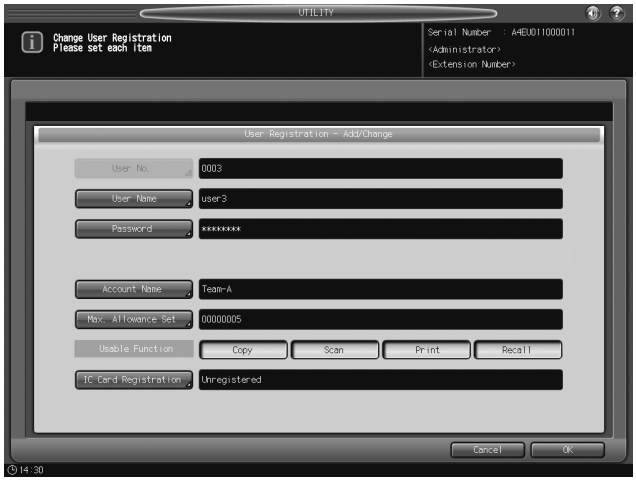
➔ In [Max. Allowance Set], press [Enable] on the right, and then press [Maximum].



➔ Use the touch panel keypad, [▼], or [▲] to enter the desired number of allowed prints. Available range for the allowance is from 1 to 99,999,999.

➔ Press [OK] twice to return to the User Registration Screen.

14 Press [Copy], [Scan], [Print], or [Recall] on the right of [Usable Function] to specify which functions the user is allowed to use.



15 Press [OK].

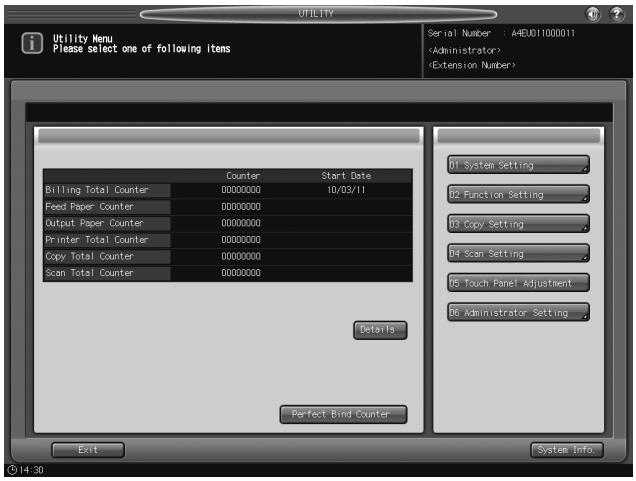
➔ When settings are completed, press [Return] on the User Registration Screen.
The User Authentication Setting Menu Screen will be restored.

2.3.3 Deleting User Data

Follow the procedure below to delete a user name and password to be required for user authentication in Enhanced Security mode, and also to delete a personal folder.

1 Press **Utility/Counter** on the **control panel** to display the Utility Menu Screen.

2 Press [06 Administrator Setting].



A password entry screen will be displayed.

3 Enter the administrator password.

➔ Use the touch panel keypad to enter the administrator password consisting of 8 alphanumeric characters and symbols, then press [OK].

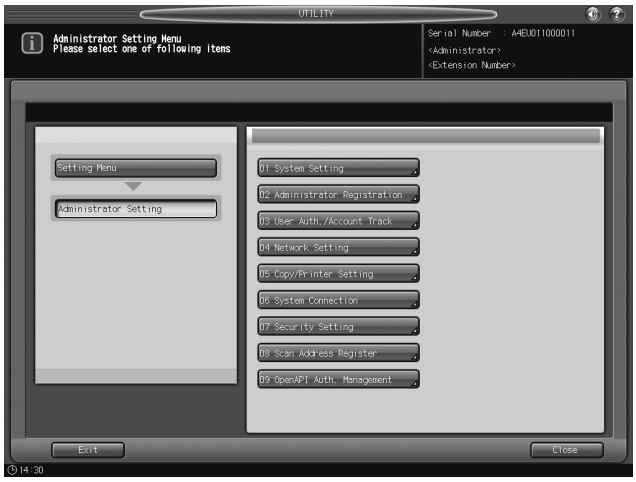
➔ The alphabetic characters are case-sensitive.

➔ If a wrong password or fewer than 8 alphanumeric characters/symbols are entered and [OK] is pressed, the warning message [Incorrect password / Please wait for a while] will appear, and no key will work for five seconds. Enter the correct password after five seconds.

➔ The information on failed authentication will be saved in the audit log.

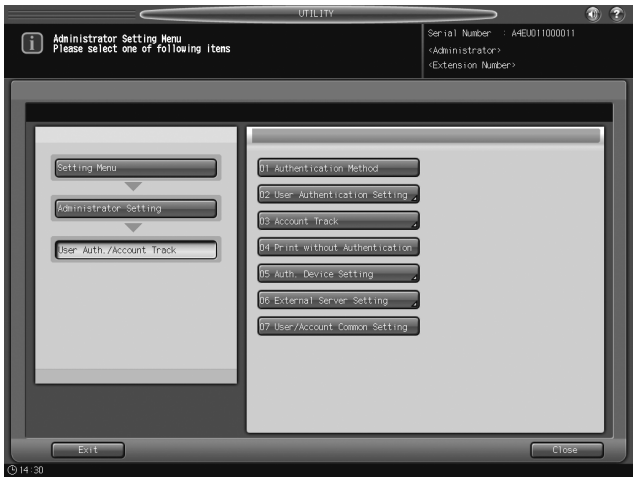
The Administrator Setting Menu Screen will be displayed.

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



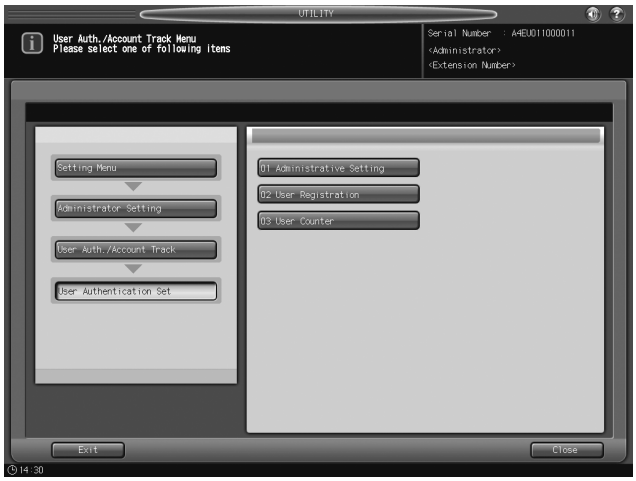
The User Auth./Account Track Menu Screen will be displayed.

5 Press [02 User Authentication Setting].



The User Authentication Setting Menu Screen will be displayed.

6 Press [02 User Registration].



The User Registration Screen will be displayed.

7 Press the user name key to be deleted.

8 Press [Delete].

➔ A confirmation dialog will be displayed.

Press [Yes]. Selected user data and the personal folder will be deleted.

2.3.4 Changing Password by User

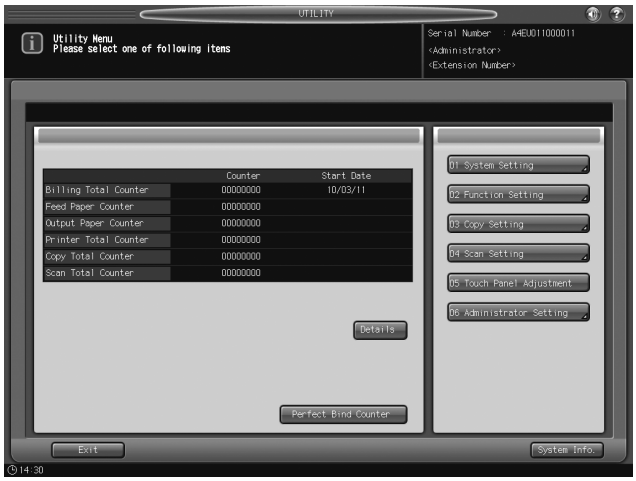
General users can change the password required for user authentication. We recommend that a user himself/herself changes the password assigned by the administrator for security.

NOTICE

To change a user password without user authentication made, the user name specified with that password should be entered.

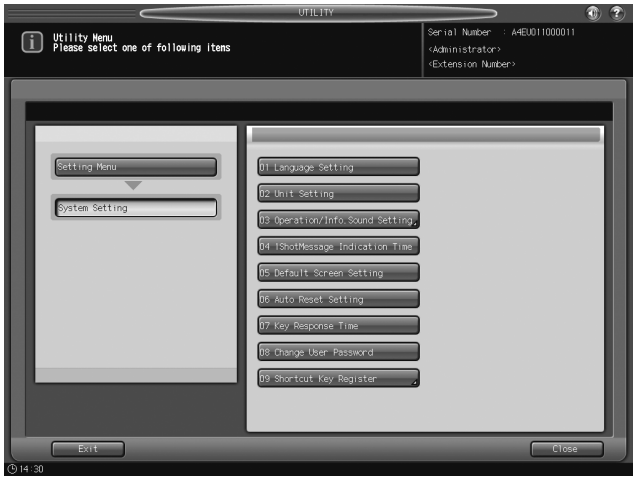
1 Press **Utility/Counter** on the **control panel** to display the Utility Menu Screen.

2 Press [01 System Setting].



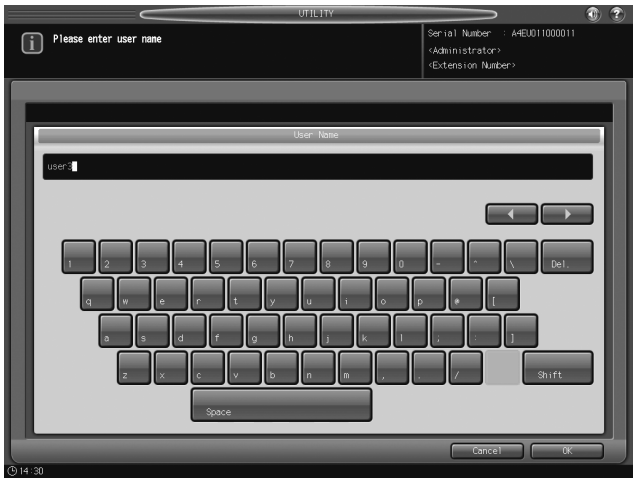
The System Setting Menu Screen will be displayed.

3 Press [08 Change User Password].



The screen to change the user password will be displayed.

4 Press [User Name], then enter the user name specified with that password.



Press [OK].

5 Press [Current Password] and enter the current password corresponding to the user name entered in step 4.

Press [OK].

The entered password will appear as asterisks (********) on the screen.

➔ Passwords are case-sensitive.

➔ If a wrong password or fewer than 8 alphanumeric characters are entered and [OK] is pressed, the warning message [Incorrect password] will appear, and no key will work for five seconds. Enter the correct password after five seconds.

➔ The information on failed authentication will be saved in the audit log.

6 When user authentication is completed successfully, the Change User Password Screen will be displayed.

➔ Press [New Password] and enter a new password corresponding to the user name entered in step 4.

➔ Enter 8 to 64 alphanumeric characters for the user password (the alphabetic characters are case-sensitive).

Press [OK].

NOTICE

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

➔ The information on failed authentication will be saved in the audit log.

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

7 Enter the new password again for confirmation.

➔ Press [Input Confirmation] to enter the same password as above.

Press [OK].

8 Press [OK].

The System Setting Menu Screen will be displayed.

9 Press [Exit].

The screen resumes the one previously displayed before the Utility Menu Screen.

2.4 HDD Store Function in Enhanced Security Mode

When saving or outputting data is necessary, use a user box built on the HDD. We recommend using a user box with a password specified, in order to prevent data leakage or tampering.

Please be sure to activate the Enhanced Security mode when you need to save sensitive documents.

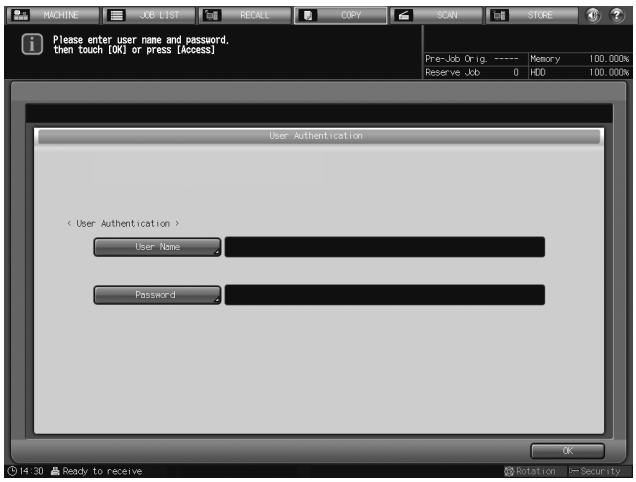
If the Enhanced Security mode is turned OFF by the administrator for some reason, users should be alerted to the fact.

Please refer to the User's Guide - Network Scanner to see how to store data into a user box and how to output the stored data.

2.4.1 Saving Data While Copying

This section describes how to save data into a user box in HDD while copying the data in the Enhanced Security mode.

1 On the User Authentication Screen displayed, press [User Name].



The User Name Setting Screen will be displayed.

2 Enter the specified user name, and press [OK].

➔ You may enter up to 64 alphanumeric characters including symbols for the user name. The alphabetic characters are case-sensitive.

The User Authentication Screen will be restored.

3 Press [Password].

The Password Setting Screen will be displayed.

4 Enter the specified password, and press [OK].

➔ You may enter from 8 to 64 alphanumeric characters for the user password.

➔ If a wrong password or fewer than 8 alphanumeric characters are entered and [OK] is pressed, a warning dialog with the message [Authentication failure] will be displayed. Press [OK] on the dialog, and then enter the correct password.

➔ The information on failed authentication will be saved in the audit log.

The User Authentication Screen will be restored.

5 Press [OK].

The Copy Screen will be displayed.

➔ Position the original.

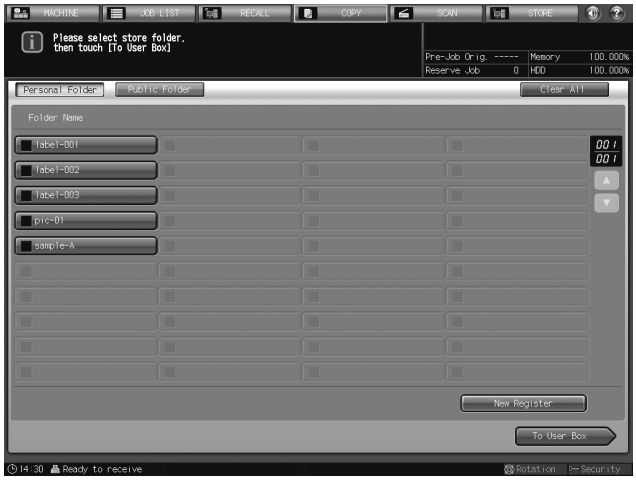
6 Press [Output Setting].

The Output Setting Screen will be displayed.

7 Press [HDD Store].

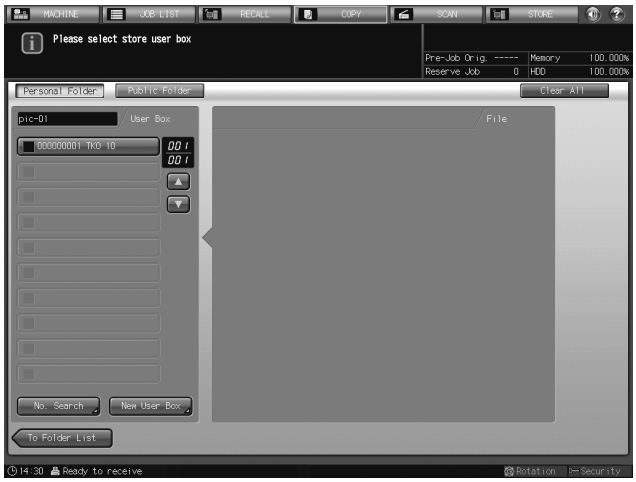
The list of personal folders will be displayed.

8 Select the desired personal folder and press [To User Box].



All the user boxes included in the selected personal folder will be displayed.

9 Select the desired user box.



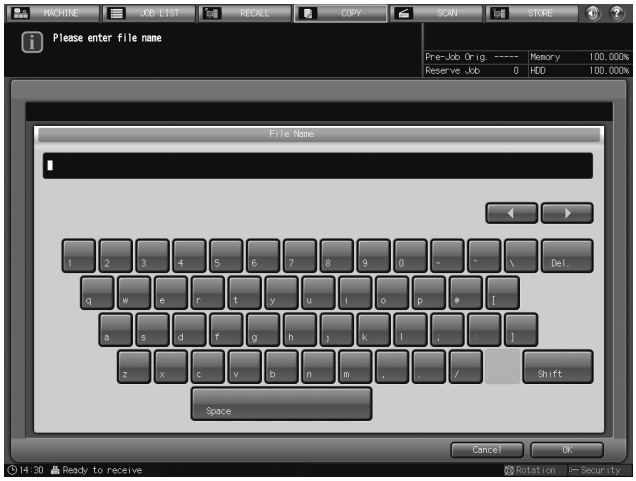
All the files included in the selected user box will be displayed.

10 Press [New File Store].

The File Name Setting Screen will be displayed.

11 Enter a file name and press [OK].

➔ You may enter up to 64 alphanumeric characters including symbols for the file name. The alphabetic characters are case-sensitive.



12 Press [OK].

The Copy Screen will be displayed.

13 On the **control panel**, press **Start**.

➔ The output process starts.

➔ Also, storing data into HDD starts.

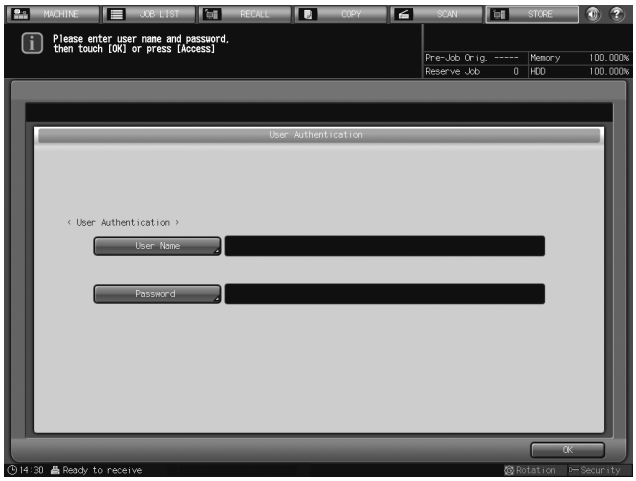
14 When all operations are completed, press **Access** on the **control panel** to release the authentication.

The User Authentication Screen will be displayed and it will no longer accept any operation.

2.4.2 Saving Data in User Box

This section describes how to save data into a user box in HDD in the Enhanced Security mode.

1 Press [Store] tab and then press [User Name] on the User Authentication Screen displayed.



The User Name Setting Screen will be displayed.

2 Enter the specified user name, and press [OK].

➔ You may enter up to 64 alphanumeric characters including symbols for the user name. The alphabetic characters are case-sensitive.

The User Authentication Screen will be restored.

3 Press [Password].

The Password Setting Screen will be displayed.

4 Enter the specified password, and press [OK].

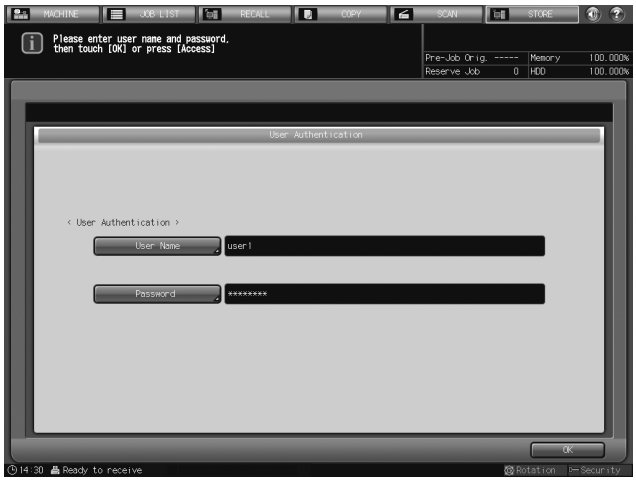
➔ You may enter from 8 to 64 alphanumeric characters for the user password.

➔ If a wrong password or fewer than 8 alphanumeric characters are entered and [OK] is pressed, a warning dialog with the message [Authentication failure] will be displayed. Press [OK] on the dialog, and then enter the correct password.

➔ The information on failed authentication will be saved in the audit log.

The User Authentication Screen will be restored.

5 Press [OK].



The Store Screen will be displayed.

6 Select [Scan to HDD].

The list of personal folders will be displayed.

7 Select the desired personal folder and press [To User Box].

All the user boxes included in the selected personal folder will be displayed.

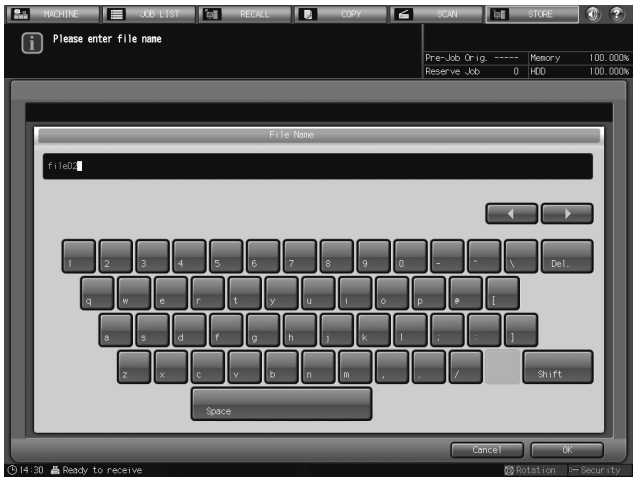
8 Select the desired user box.

All the files included in the selected user box will be displayed.

9 Press [New File Store].

10 Enter a file name and press [OK].

➔ You may enter up to 64 alphanumeric characters including symbols for the file name. The alphabetic characters are case-sensitive.



The Scan Screen will be displayed.

11 On the **control panel**, press **Start** to load and save the file.

12 Press one of the following keys:

➔ Press [Yes] to continue loading.

➔ Press [No] to exit.

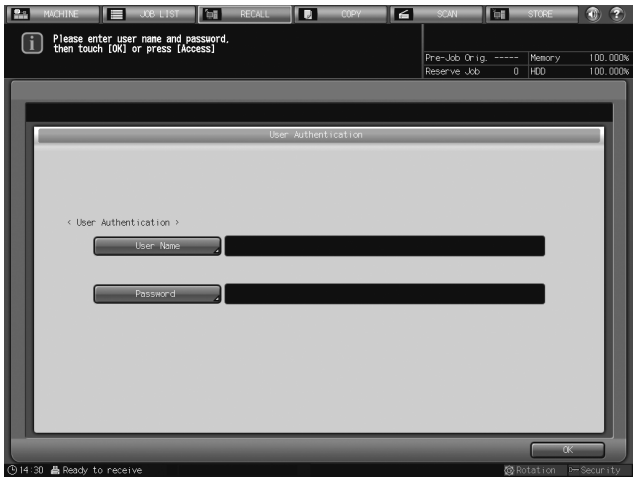
13 When all operations are completed, press **Access** on the **control panel** to release the authentication.

The User Authentication Screen will be displayed and it will no longer accept any operation.

2.4.3 Recalling and Deleting of Data

This section describes how to recall or delete data stored in a user box in HDD in the Enhanced Security mode.

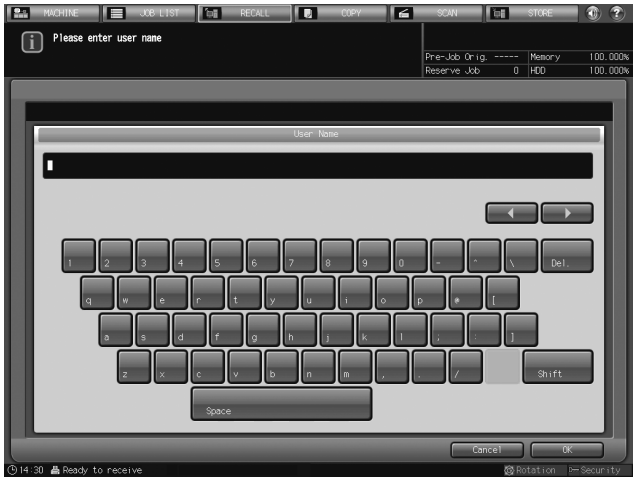
1 Press [RECALL] tab and then press [User Name] on the User Authentication Screen displayed.



The User Name Setting Screen will be displayed.

2 Enter the specified user name, and press [OK].

➔ You may enter up to 64 alphanumeric characters including symbols for the user name. The alphabetic characters are case-sensitive.



The User Authentication Screen will be restored.

3 Press [Password].

The Password Setting Screen will be displayed.

4 Enter the specified password, and press [OK].

➔ You may enter from 8 to 64 alphanumeric characters for the user password.

➔ If a wrong password or fewer than 8 alphanumeric characters are entered and [OK] is pressed, a warning dialog with the message [Authentication failure] will be displayed. Press [OK] on the dialog, and then enter the correct password.

➔ The information on failed authentication will be saved in the audit log.

The User Authentication Screen will be restored.

5 Press [OK].

The Recall Screen will be displayed.

6 Select the desired folder and press [To User Box].

The list of user boxes will be displayed.

7 Select the desired user box.

All the files included in the selected user box will be displayed.

8 You can either recall or delete the file.

➔ If you need to recall the file, proceed to step 9.

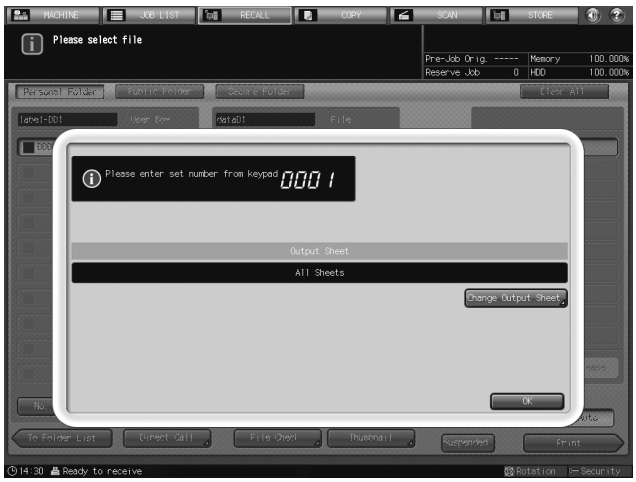
➔ If you need to delete the file, proceed to step 14.

9 Select the name of the file to be recalled and press [▶].

10 Select [Auto], [Proof], [Proof (1st Sheet)], or [Wait], and press [Print].

➔ [Proof (1st Sheet)] can be displayed by using the Utility menu. It does not appear with the initial settings. Please refer to the POD Administrator's Reference for details.

11 Use the control panel keypad to enter the print quantity.



12 Press [Change Output Sheet] to change the output sheet of the file to be recalled.

➔ To specify sheets to be output, press [Sheet Specify] and use the touch panel keypad to enter the sheet numbers.

➔ Use a comma "," to separate the sheet numbers. To specify consecutive sheet numbers, use a hyphen "-" between the beginning and ending sheet numbers.

➔ To output all sheets, press [All Sheets].

Press [OK] to output.

13 Press one of the following keys:

➔ Press [Yes] to continue recalling.

➔ Press [No] to exit.

14 Select the name of the file to be deleted and press [File Delete].

A confirmation dialog will be displayed.

15 Press [Yes].

The selected file will be deleted and the file selection screen will be restored.

16 When all operations are completed, press **Access** on the **control panel** to release the authentication.

The User Authentication Screen will be displayed and it will no longer accept any operation.

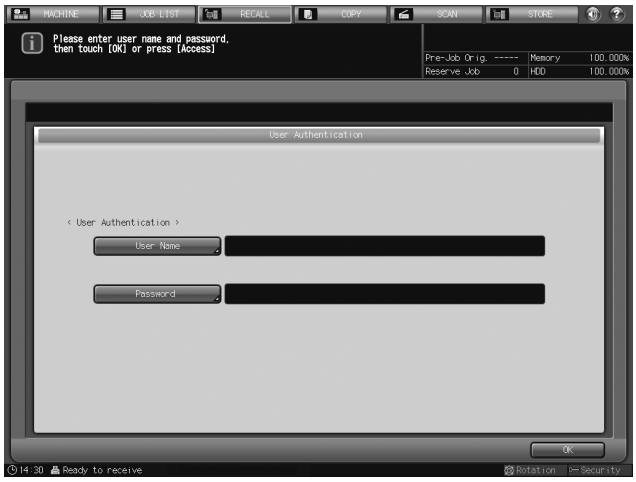
2.4.4 Output Data in the Secure Box

Secure printing using a PC

To set up data output using the Secure Print function on PC, a secure folder with a specific password must be prepared. Enter the secure folder name consisting of up to 8 alphanumeric characters.

Secure printing on the machine

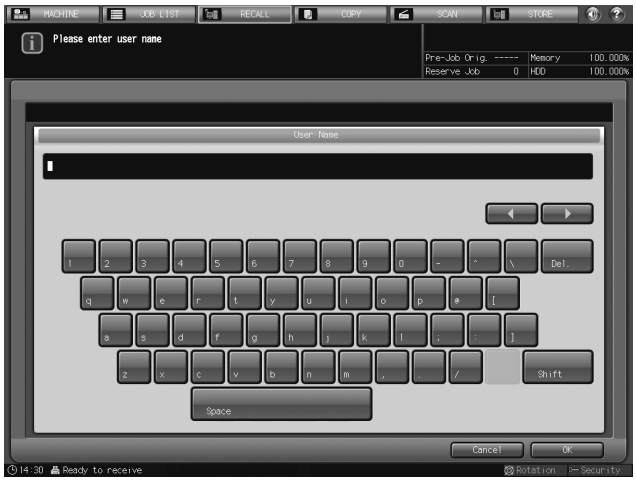
1 Press [RECALL] tab and then press [User Name] on the User Authentication Screen displayed.



The User Name Setting Screen will be displayed.

2 Enter the specified user name, and press [OK].

➔ You may enter up to 64 alphanumeric characters including symbols for the user name. The alphabetic characters are case-sensitive.



The User Authentication Screen will be restored.

3 Press [Password].

The Password Setting Screen will be displayed.

4 Enter the specified password, and press [OK].

➔ You may enter from 8 to 64 alphanumeric characters for the user password.

➔ If a wrong password or fewer than 8 alphanumeric characters are entered and [OK] is pressed, a warning dialog with the message [Authentication failure] will be displayed. Press [OK] on the dialog, and then enter the correct password.

➔ The information on failed authentication will be saved in the audit log.

The User Authentication Screen will be restored.

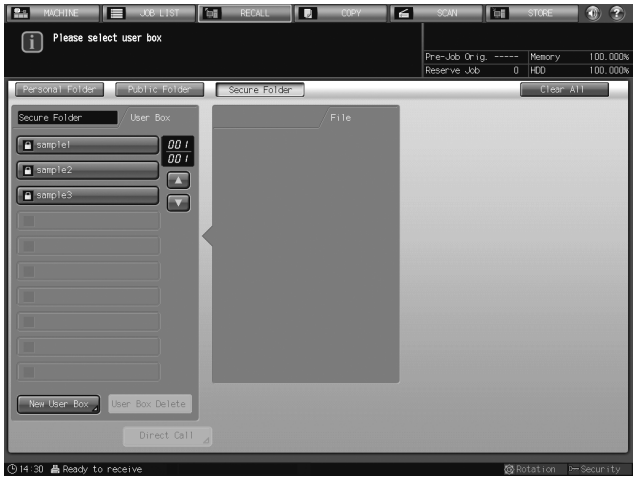
5 Press [OK].

The Recall Screen will be displayed.

6 Press [Secure Folder].

The list of secure boxes will be displayed.

7 Select the desired secure box.



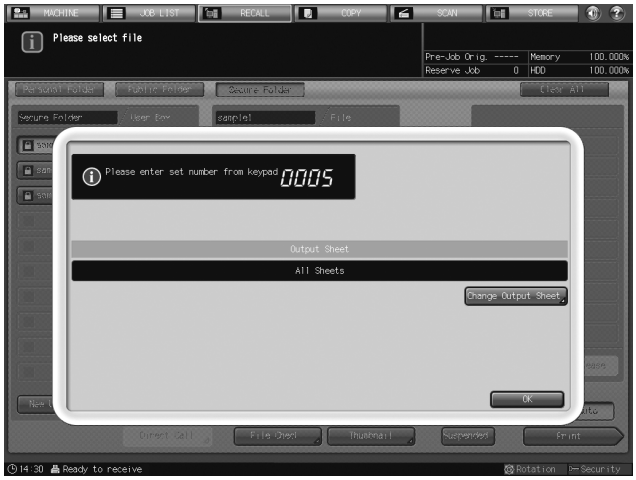
8 Enter the secure password specified in secure printing and press [OK].
The list of secure files will be displayed.

9 Select the desired secure file.

10 Select [Auto], [Proof], [Proof (1st Sheet)], or [Wait], and press [Print].

➔ [Proof (1st Sheet)] can be displayed by using the Utility menu. It does not appear with the initial settings. Please refer to the POD Administrator's Reference for details.

11 Use the control panel keypad to enter the print quantity.



12 Press [Change Output Sheet] to change the output sheet of the file to be recalled.

➔ To specify sheets to be output, press [Sheet Specify] and use the touch panel keypad to enter the sheet numbers.

➔ Use a comma "," to separate the sheet numbers. To specify consecutive sheet numbers, use a hyphen "-" between the beginning and ending sheet numbers.

➔ To output all sheets, press [All Sheets].

Press [OK] to output.

13 Press one of the following keys:

➔ Press [Yes] to continue recalling.

➔ Press [No] to exit.

14 When all operations are completed, press **Access** on the **control panel** to release the authentication.

The User Authentication Screen will be displayed and it will no longer accept any operation.

2.5 Administrator Security Functions

The administrator turns ON/OFF the Enhanced Security mode from the Utility Menu Screen. For that operation, a CE password and administrator password should be set up on the machine. Ask your service representative to set up an administrator password. Once specified, the password can be changed by the administrator himself/herself. For details on changing the administrator password, see Section 7 of the User's Guide - POD Administrator's Reference.

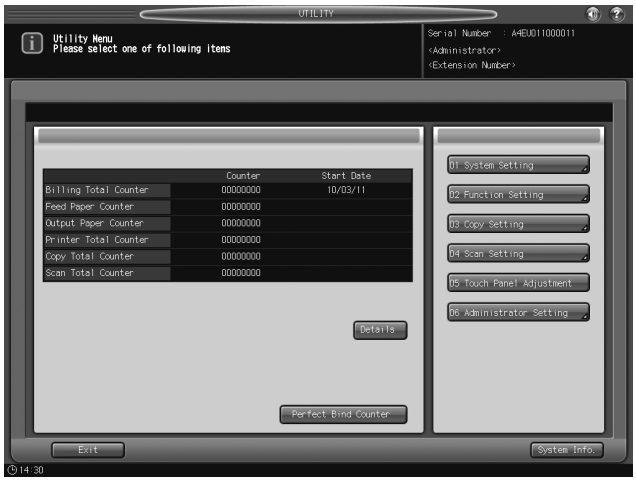
To protect the data on the machine from leakage or tampering, please be sure to designate an administrator and activate the Enhanced Security mode.

2.5.1 Turning the Enhanced Security Mode ON/OFF

This section describes how to turn the Enhanced Security mode ON/OFF.

1 Press **Utility/Counter** on the **control panel** to display the Utility Menu Screen.

2 Press [06 Administrator Setting].



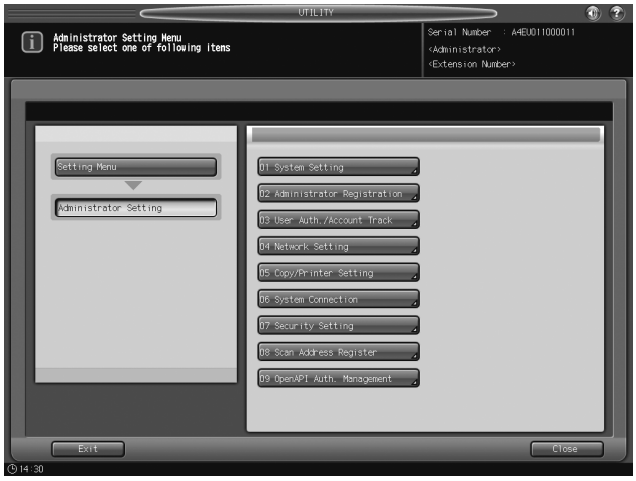
A password entry screen will be displayed.

3 Enter the administrator password.

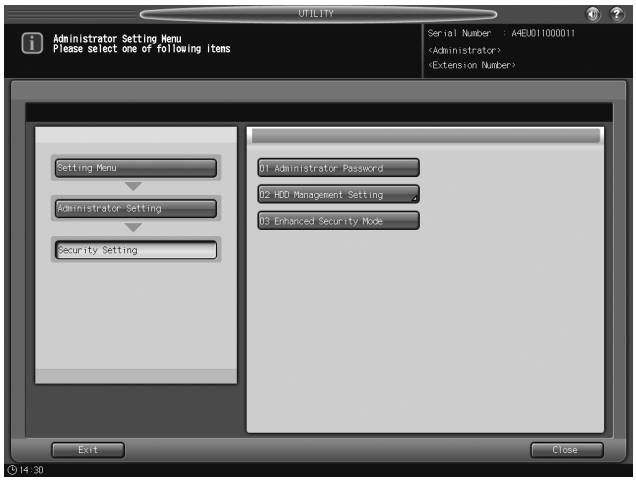
- ➔ Use the touch panel keypad to enter the administrator password consisting of 8 alphanumeric characters and symbols, then press [OK].
- ➔ The alphabetic characters are case-sensitive.
- ➔ If a wrong password or fewer than 8 alphanumeric characters/symbols are entered and [OK] is pressed, the warning message [Incorrect password / Please wait for a while] will appear, and no key will work for five seconds. Enter the correct password after five seconds.
- ➔ The information on failed authentication will be saved in the audit log.

The Administrator Setting Menu Screen will be displayed.

4 Press [07 Security Setting].

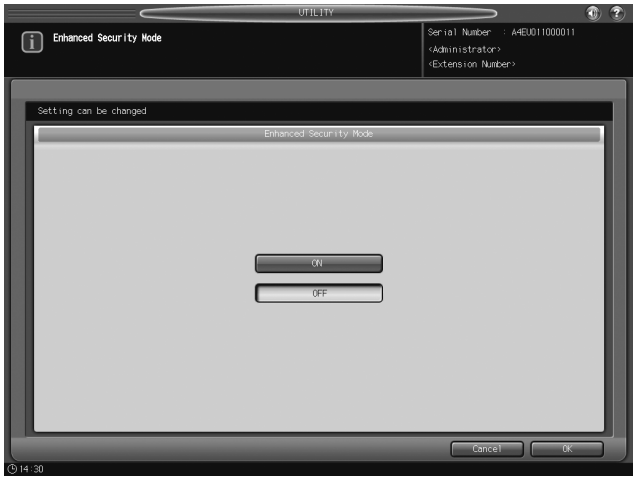


5 Press [03 Enhanced Security Mode].



6 Turn ON/OFF the Enhanced Security mode.

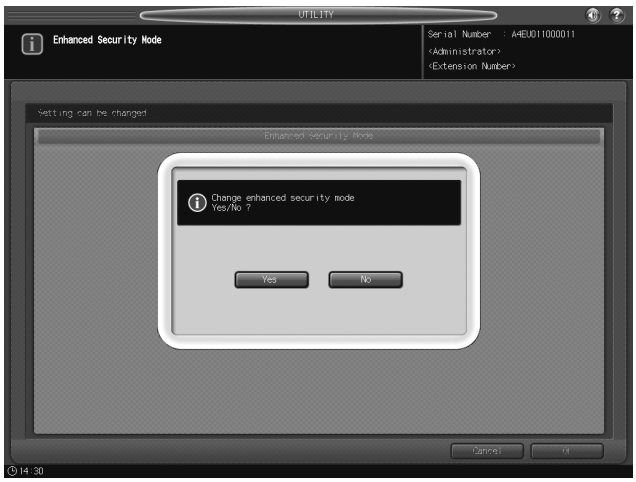
➔ Select [ON] to activate the Enhanced Security mode, or select [OFF] to deactivate it.



7 Press [OK].

➔ A dialog to confirm the change to the Enhanced Security mode setting will be displayed.

➔ Press [Yes].



8 Turn OFF the **sub power switch**, and turn OFF the **main power switch**.

NOTICE

Do not turn off the main power while the message [Cooling in progress / After cooling, power off automatically] is displayed.

9 Please wait for more than 10 seconds.

10 Turn ON the **main power switch**, and turn ON the **sub power switch**.

2.5.2 HDD Lock Password

With the Enhanced Security mode activated, you can specify a new lock password (8 to 32 alphanumeric characters, case-sensitive) by changing the default lock password initially given to the HDD. Setting up a lock password will prevent the leakage of document data by taking out an illicitly-switched HDD. If the HDD itself is externally accessed, the data readout will not be available until the correct lock password is entered.

NOTICE

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

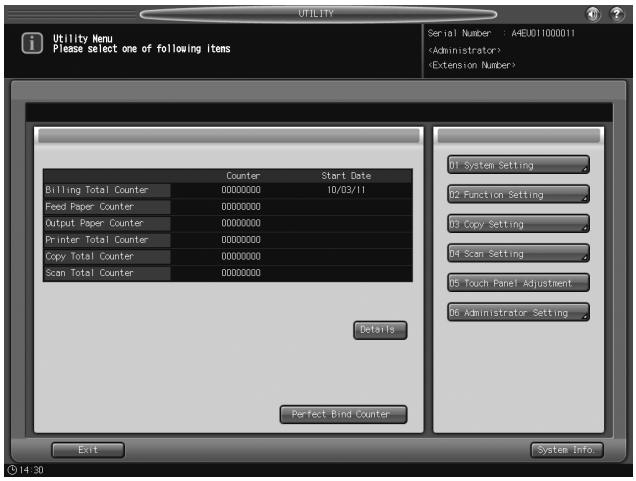
Be careful not to inform anybody else of the password, or not to let it known to others.

1 Press **Utility/Counter** on the **control panel** to display the Utility Menu Screen.

2 Press [06 Administrator Setting].

➔ The HDD lock password only functions when the Enhanced Security mode is activated. With the Enhanced Security mode turned off, the message [Please set enhanced security mode] is displayed.

➔ Please be sure to set up an HDD lock password when using the Enhanced Security mode.



A password entry screen will be displayed.

3 Enter the administrator password.

➔ Use the touch panel keypad to enter the administrator password consisting of 8 alphanumeric characters and symbols, then press [OK].

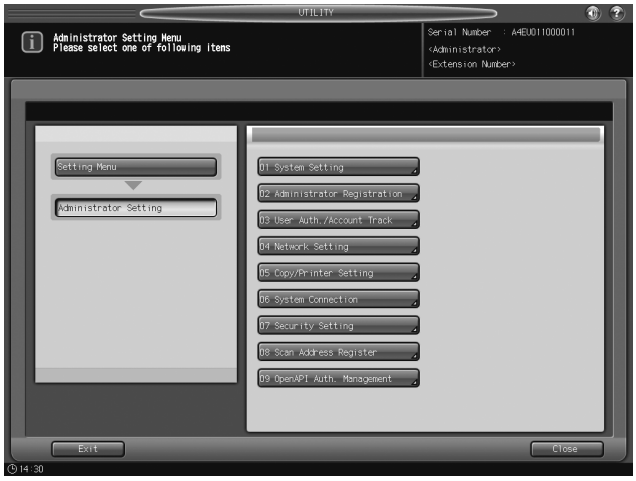
➔ The alphabetic characters are case-sensitive.

➔ If a wrong password or fewer than 8 alphanumeric characters/symbols are entered and [OK] is pressed, the warning message [Incorrect password / Please wait for a while] will appear, and no key will work for five seconds. Enter the correct password after five seconds.

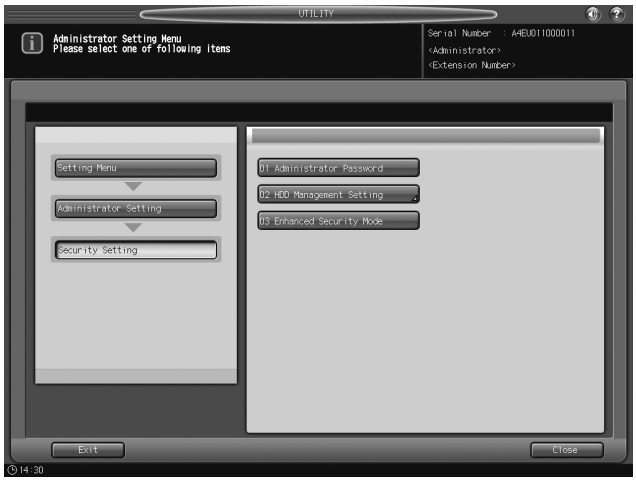
➔ The information on failed authentication will be saved in the audit log.

The Administrator Setting Menu Screen will be displayed.

4 Press [07 Security Setting].

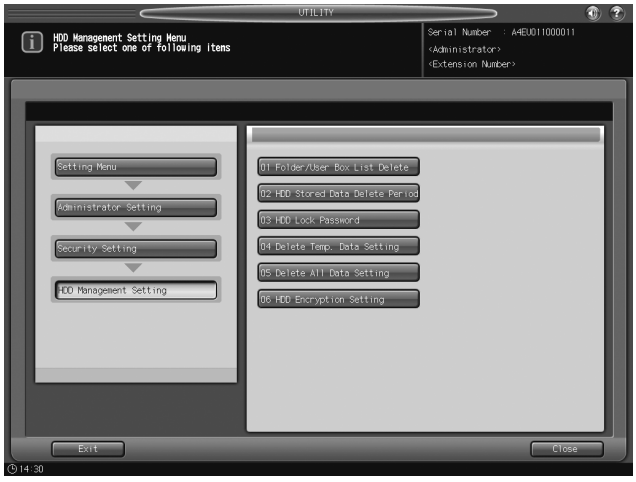


5 Press [02 HDD Management Setting].



The HDD Management Setting Menu Screen will be displayed.

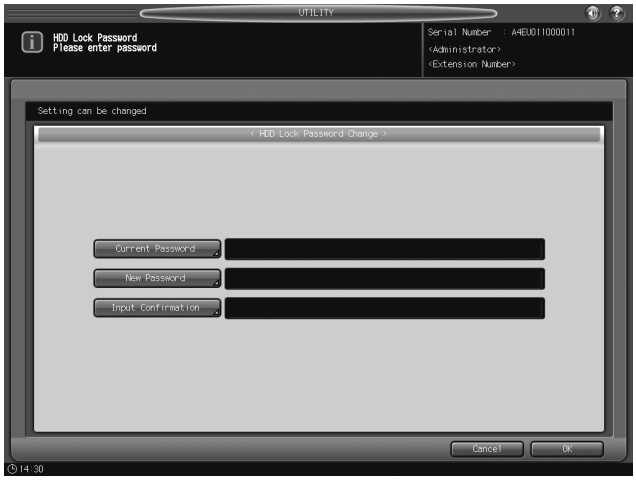
6 Press [03 HDD Lock Password].



The HDD Lock Password Screen will be displayed.

7 Press [Current Password] to enter the password currently used, then press [OK].

Default password is the main body serial number consisting of 13 alphanumeric characters.



➔ The main body serial number as 13 alphanumeric characters is displayed on the upper left corner of the Utility Menu Screen or to be printed on the upper right corner of the audit log. For details, see the next section "Printing Audit Log."

8 If the authentication has succeeded, press [New Password] to enter a new password.

NOTICE

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

➔ You may enter 8 to 32 alphanumeric characters for the HDD lock password.

➔ If a wrong password or fewer than 8 alphanumeric characters are entered and [OK] is pressed, the warning message [Incorrect password / Please wait for a while] will appear, and no key will work for five seconds. Enter the correct password after five seconds.

➔ The information on failed authentication will be saved in the audit log.

➔ The information on changing password will be saved in the audit log.

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

➔ Press [OK] when completed.

9 Press [Input Confirmation] to enter the same password as above.

➔ Press [OK] when completed.

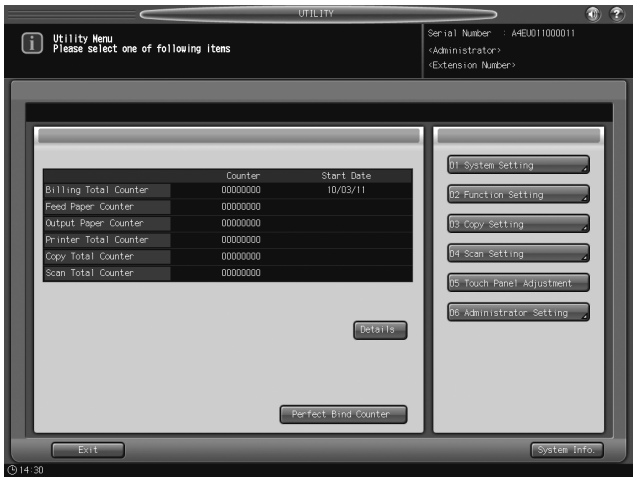
10 Press [OK] on the HDD Lock Password Screen.

2.5.3 Deleting 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.

1 Press **Utility/Counter** on the **control panel** to display the Utility Menu Screen.

2 Press [06 Administrator Setting].



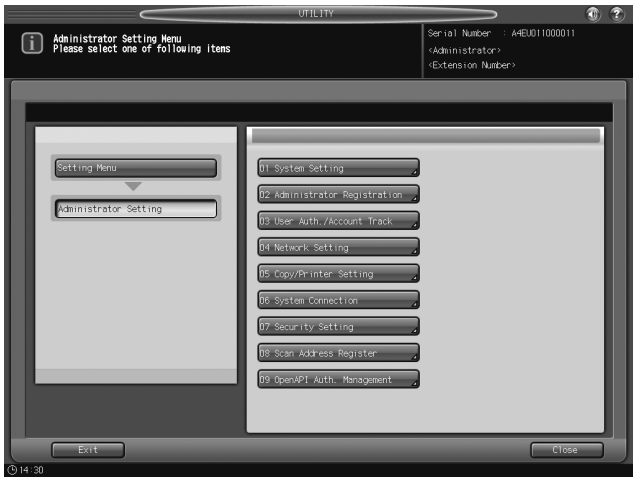
A password entry screen will be displayed.

3 Enter the administrator password.

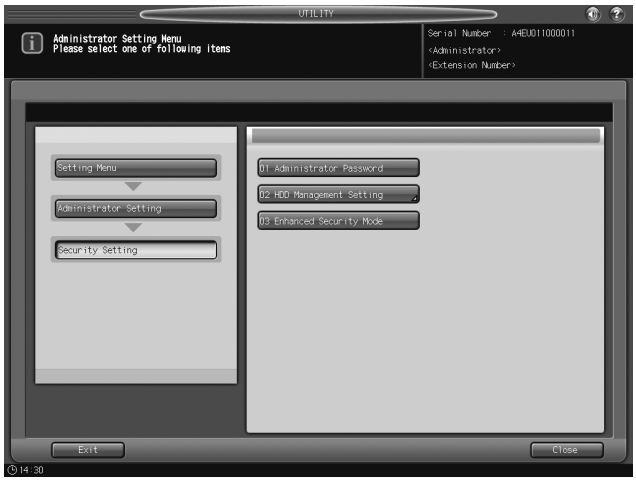
- ➔ Use the touch panel keypad to enter the administrator password consisting of 8 alphanumeric characters and symbols, then press [OK].
- ➔ The alphabetic characters are case-sensitive.
- ➔ If a wrong password or fewer than 8 alphanumeric characters/symbols are entered and [OK] is pressed, the warning message [Incorrect password / Please wait for a while] will appear, and no key will work for five seconds. Enter the correct password after five seconds.
- ➔ The information on failed authentication will be saved in the audit log.

The Administrator Setting Menu Screen will be displayed.

4 Press [07 Security Setting].

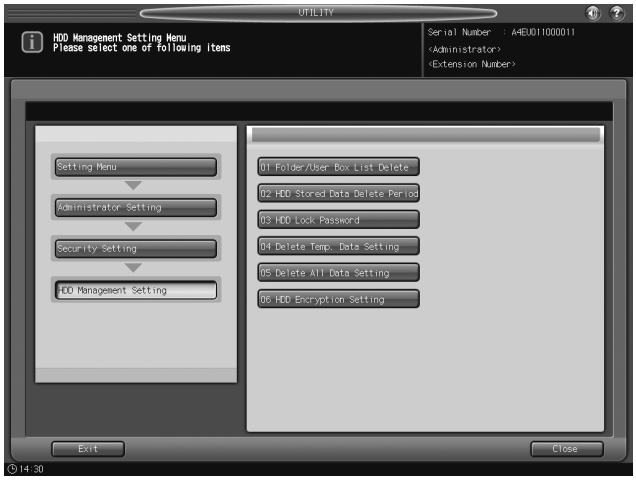


5 Press [02 HDD Management Setting].



The HDD Management Setting Menu Screen will be displayed.

6 Press [04 Delete Temp. Data Setting].



The Delete Temporary Data Setting Screen will be displayed.

7 Select whether or not to overwrite the temporary data.

➔ To overwrite the temporary data, press [ON]. Otherwise, press [OFF].

8 If you choose to overwrite the data, select the desired erase mode.

➔ Press [Mode 1] or [Mode 2]. Please refer to the POD Administrator's Reference for details.

➔ If you choose not to overwrite the data, the mode selection does not make any difference.

9 Press [OK] on the Delete Temporary Data Setting Screen.

10 Turn OFF the **sub power switch**, and turn OFF the **main power switch**.

➔ Do not turn off the main power while the message [Cooling in progress / After cooling, power off automatically] is displayed.

11 Please wait for more than 10 seconds.

12 Turn ON the **main power switch**, and turn ON the **sub power switch**.

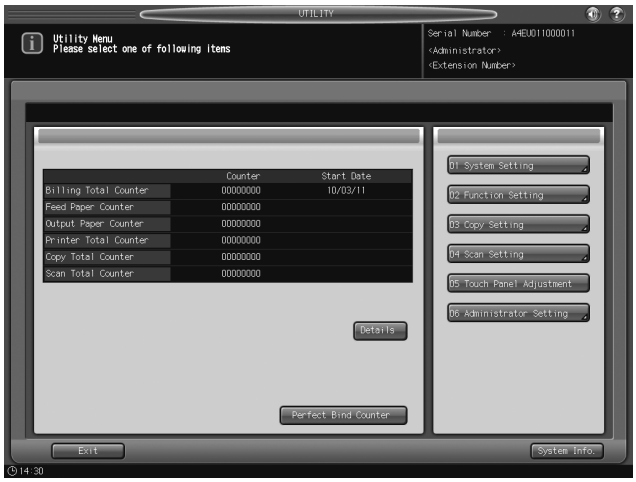
2.5.4 Deleting All Data

You can choose to delete all the document data stored on HDD. When you choose to delete all the data, select one of the 8 erase modes provided.

1 Press **Utility/Counter** on the **control panel** to display the Utility Menu Screen.

➔ To use this function of deleting all the data, please contact your service representative.

2 Press [06 Administrator Setting].



A password entry screen will be displayed.

3 Enter the administrator password.

➔ Use the touch panel keypad to enter the administrator password consisting of 8 alphanumeric characters and symbols, then press [OK].

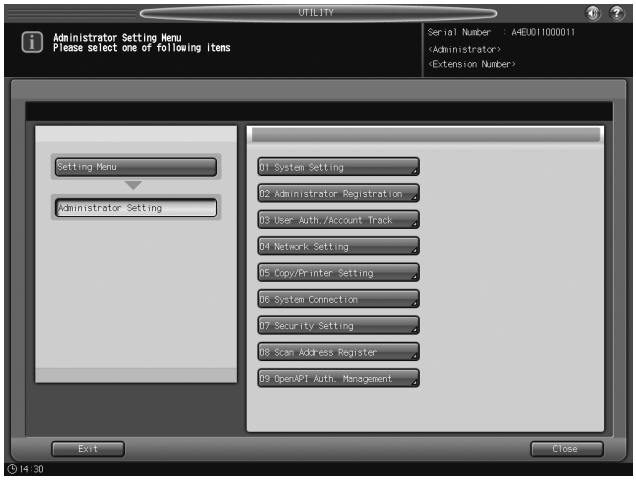
➔ The alphabetic characters are case-sensitive.

➔ If a wrong password or fewer than 8 alphanumeric characters/symbols are entered and [OK] is pressed, the warning message [Incorrect password / Please wait for a while] will appear, and no key will work for five seconds. Enter the correct password after five seconds.

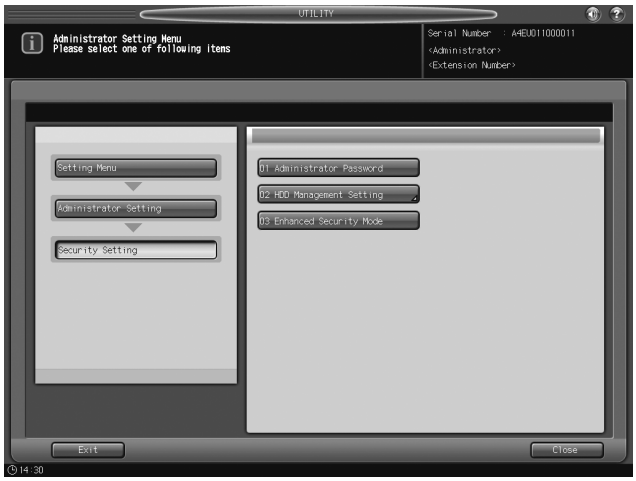
➔ The information on failed authentication will be saved in the audit log.

The Administrator Setting Menu Screen will be displayed.

4 Press [07 Security Setting].

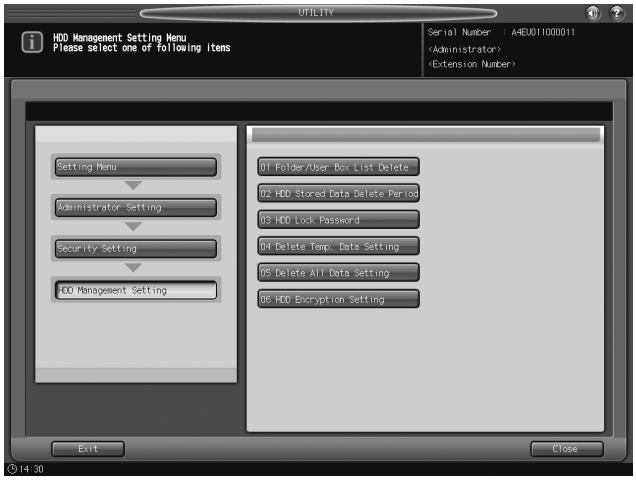


5 Press [02 HDD Management Setting].



The HDD Management Setting Menu Screen will be displayed.

6 Press [05 Delete All Data Setting].



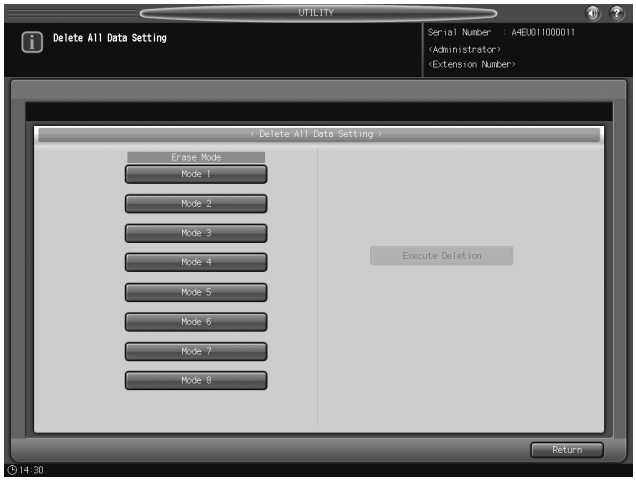
The Delete All Data Setting Screen will be displayed.

7 Select the desired erase mode and press [Execute Deletion].

➔ Please refer to the POD Administrator's Reference for details of the erase mode.

NOTICE

If you delete data using the [Execute Deletion] key, no data on HDD can be used again. All the necessary data should be moved to another device beforehand.



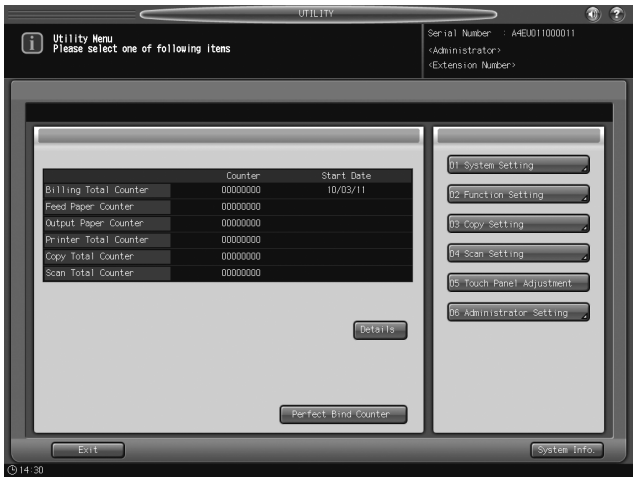
8 Press [Return] on the Delete All Data Setting Screen.

2.5.5 Printing Audit Log

An audit log will be automatically created when the data saved on the machine have been accessed. All the audit log data can be output as follows.

1 Press **Utility/Counter** on the **control panel** to display the Utility Menu Screen.

2 Press [06 Administrator Setting].



A password entry screen will be displayed.

3 Enter the administrator password.

➔ Use the touch panel keypad to enter the administrator password consisting of 8 alphanumeric characters and symbols, then press [OK].

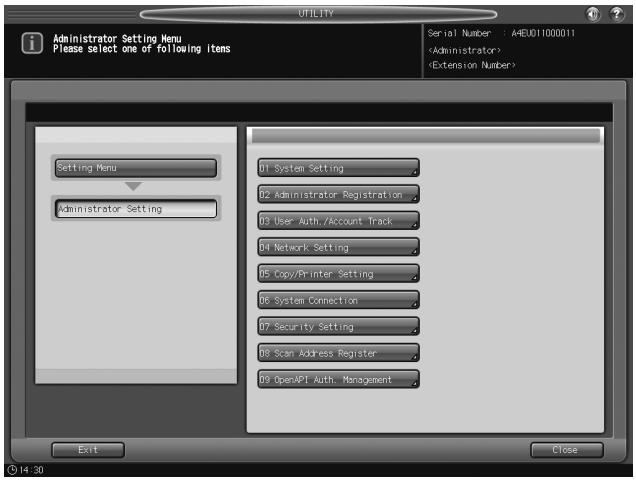
➔ The alphabetic characters are case-sensitive.

➔ If a wrong password or fewer than 8 alphanumeric characters/symbols are entered and [OK] is pressed, the warning message [Incorrect password / Please wait for a while] will appear, and no key will work for five seconds. Enter the correct password after five seconds.

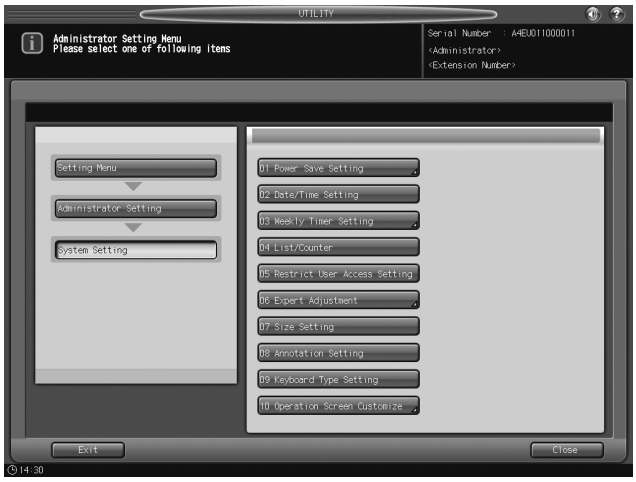
➔ The information on failed authentication will be saved in the audit log.

The Administrator Setting Menu Screen will be displayed.

4 Press [01 System Setting].

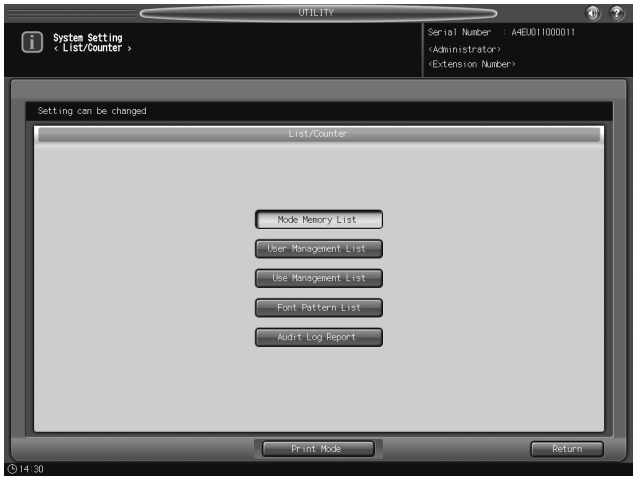


5 Press [04 List/Counter].



The List/Counter Screen will be displayed.

6 Select [Audit Log Report], then press [Print Mode].



7 Print the log.

➔ Press **Start** on the **control panel**.

➔ To stop printing, press **Stop** on the **control panel**. A dialog will pop up for confirmation. Press [Cancel Job] to cancel the print job.

➔ When the print job is completed, press [Close].

2.5.6 Analyzing Audit Log

Audit log needs to be analyzed by the administrator regularly (once per month), or when the data saved in the machine are illegally accessed or even tampered.

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 unanalyzed logs reach that number.

Audit log report

P.1
04/04/2012 18:29
A4EU011901010
TC:931

No	date/time	id	action	result	No	date/time	id	action	result
0001	04/04/2012 18:29	-2	04	OK	0002	04/04/2012 15:35	-3	11	NG
0003	04/04/2012 14:26	1	11	OK	0004	04/04/2012 14:24	1	11	OK
0005	04/04/2012 14:24	1	11	NG	0006	04/04/2012 14:23	-3	11	NG
0007	04/04/2012 14:23	1	11	NG	0008	04/04/2012 14:22	2	07	OK
0009	04/04/2012 14:22	1	07	OK	0010	04/04/2012 14:22	2	07	OK
0011	04/04/2012 14:21	1	07	OK	0012	04/04/2012 14:18	-2	02	OK
0013	04/04/2012 14:17	2	07	OK	0014	04/04/2012 14:17	-2	02	OK
0015	04/04/2012 14:15	-2	02	OK	0016	04/04/2012 14:11	-2	02	OK
0017	04/04/2012 11:23	-2	02	OK	0018	04/04/2012 11:21	-2	02	OK
0019	04/04/2012 11:20	-2	02	OK	0020	04/04/2012 11:19	-1	06	OK
0021	04/04/2012 11:19	-1	06	OK	0022	04/04/2012 11:18	1	11	OK
0023	04/04/2012 11:17	-3	11	NG	0024	04/04/2012 11:15	1	11	NG
0025	04/04/2012 11:14	1	11	NG	0026	04/04/2012 11:11	1	11	OK

Audit log information

The audit log contains the following information:

1. date/time: registers date and time of the operation that resulted in the creation of a log entry.
2. id: specifies person who made the operation, or subject for security protection.

– -1: operation by customer engineer (CE)
– -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: numbers from 1 to 1000. Secure User ID: numbers from 1 to 99999.

3. action: indicates number that specifies the operation. Refer to the following table for details.
4. result: records result of the operation. For password authentication, success/failure will be indicated as OK/NG. For operations without password authentication, all log entries will be indicated as OK.

Table of items saved in audit log

No.	Operation	Audit 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	CE 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	User ID	09	OK
10	Change user attribute	User ID	10	OK
11	Password authentication for user	User ID[*1]/Unregistered user ID[*2]	11	OK/NG
12	Change attributes of user by user (user password, etc.)	User ID	12	OK
13	Access to file (Read document data)	User ID	13	OK

No.	Operation	Audit ID	Stored action	Result
14	Delete file Delete document data	User ID	14	OK
15	Change file attribute	User ID	15	OK
16	Password authentication for secure print	Secure user ID[*3]/Unregistered user ID[*4]	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

[*1]: Audit log ID will be saved as user ID when user authentication is successfully made, or when password inconformity occurs with a registered user name.

[*2]: Audit log ID will be saved as unregistered user ID when authentication failure occurs with an unregistered user name.

[*3]: Audit log ID will be saved as secure user ID when secure print authentication in successfully made, or when password inconformity occurs with a registered secure user name.

[*4]: Audit log ID will be saved as unregistered user ID when secure print authentication failure occurs with an unregistered user name.

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
- Result of attack

For specific analysis methods, see the following description.

Specifying unauthorized actions: password authentication

If logs have NG as the result of password authentication (action: 01, 02, 11), 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), you may need to check whether a legitimate user created the action. Careful check is recommended especially when successful authentication occurs after series of failures, or for those made during times other than normal operating hours.

Specifying unauthorized actions: actions other than password authentication

Since all operation results other than password authentication are indicated as successful (OK), use ID and action to determine if any unauthorized actions were made.

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

For example:

If a document saved in a box is printed with fraudulent authentication, the following audit log entry will be created.

1. Password authentication to the box:

action = 11

id = Box for which the authentication was performed

result = OK/NG

2. Access to the document in the box:

action = 13

id = Box for which the authentication was performed

Check the date and time of the operation, and see if the user who operated on documents in the specific personal/secure box was a legitimate owner of the box.

Remedy for unauthorized operations

If you find that a password has leaked out after analyzing the audit log, change the password immediately.

- The legitimate user may not be able to access the box because the password has been fraudulently altered. The administrator must contact the user to confirm the situation, and if that is the case, he/she must address the problem either by changing the password or by deleting the stored data.
- If a stored document cannot be found or its content is altered, unauthorized actions may have been occurred. If that is the case, similar countermeasures are needed.

3 Index

3 Index

3.1 Index by item

A

Adding User Registration 2-7
Administrator authentication 2-5
Administrator security functions 2-39
Administrator setting mode 2-5
Analyzing audit log 2-52
Audit log 2-5

B

Blocking external accesses 2-5

C

Changing password by user 2-20
Changing User Registration 2-13
Control Software 2-2
Control software version 2-2

D

Data access 2-5
Data exempted from the protection of Enhanced Security mode 2-6
Data protected by the Enhanced Security mode 2-6
Deleting All Data 2-47
Deleting Temporary Data 2-44
Deleting user data 2-18

E

Enhanced passwords 2-4
Enhanced Security mode 2-3
Environment for Enhanced Security mode 2-3

H

HDD lock password 2-42
HDD Store Function in Enhanced Security Mode 2-24

I

IC card 2-5

M

Machine NIC settings 2-5

N

Normal mode 2-3

O

Output Data in the Secure Box 2-35

P

Printing audit log 2-50
Protecting and Deleting of Remaining Data After Being Used 2-6
Protecting and deleting of remaining data on memory or HDD after being used 2-4

R

Recalling and Deleting of Data 2-31
ROM version display function of control software 2-2

S

Saving Data in User Box 2-27
Saving Data While Copying 2-24

T

Turning Enhanced Security mode ON/OFF 2-6
Turning the Enhanced Security mode ON/OFF 2-39

U

USB port functions 2-5
User authentication in Enhanced Security mode 2-7

3.2 Index by button

A

Account Name 2-11, 2-16
Add 2-9
Administrator Setting ...2-7, 2-13, 2-18, 2-39, 2-42, 2-44, 2-47, 2-50
All Sheets 2-34, 2-38
Audit Log Report 2-51
Auto 2-33, 2-37

C

Cancel Job 2-51
Change 2-15
Change Output Sheet 2-34, 2-38
Change User Password 2-21
Close 2-51
Copy 2-12, 2-17
Current Password 2-21, 2-44

D

Delete 2-20
Delete All Data Setting 2-49
Delete Temp. Data Setting 2-46

E

Enable 2-11, 2-16
Enhanced Security Mode 2-40
Execute Deletion 2-49
Exit 2-23

F

File Delete 2-34

H

HDD Lock Password 2-43
HDD Management Setting 2-43, 2-46, 2-48
HDD Store 2-25

I

Input Confirmation 2-22, 2-44

L

List/Counter 2-51

M

Max. Allowance Set 2-11, 2-16
Maximum 2-11, 2-16
Mode 1 2-47
Mode 2 2-47

N

New File Store 2-26, 2-30
New Password 2-22, 2-44
No 2-31, 2-34, 2-38

O

OFF 2-40, 2-46
ON 2-40, 2-46
Output Setting 2-25

P

Password 2-10, 2-16, 2-24, 2-28, 2-32, 2-36
Print 2-12, 2-17, 2-33, 2-37
Print Mode 2-51
Proof 2-33, 2-37
Proof (1st Sheet) 2-33, 2-37, 2-38

R

RECALL 2-31, 2-35
Recall 2-12, 2-17

S

Scan 2-12, 2-17
Scan to HDD 2-29
Secure Folder 2-36
Security Setting 2-40, 2-43, 2-45, 2-48
Sheet Specify 2-34, 2-38
Start 2-51
Stop 2-51
Store 2-27
Synchronize 2-11, 2-16
Synchronize User/Account Track 2-11, 2-16
System Setting 2-20, 2-50

T

To User Box 2-26, 2-29, 2-33

U

User Auth./Account Track 2-8, 2-13, 2-18
User Authentication Setting 2-8, 2-14, 2-19
User Name 2-10, 2-15, 2-21, 2-24, 2-27, 2-31, 2-35
User No. 2-9
User Registration 2-9, 2-14, 2-19
Utility/Counter 2-7, 2-13, 2-18, 2-20, 2-39, 2-42, 2-44, 2-47, 2-50

W

Wait 2-33, 2-37

Y

Yes 2-20, 2-31, 2-34, 2-35, 2-38, 2-41

MEMO

MEMO

MEMO

MEMO

MEMO

MEMO

MEMO

KONICA MINOLTA

http://konicaminolta.com

A4EU957311

Printed in China
2013. 2