

bizhub 368/308

User's Guide **Security Operations**

Contents

1 Security

1.1	Introduction	1-2
	Administrators	1-2
	Compliance with the ISO15408 Standard	1-2
	Operating Precautions	1-2
	INSTALLATION CHECKLIST	1-4
1.2	Security Functions	1-7
	Check Count Clear Conditions	1-7
1.3	Precautions for Operation Control	1-9
	Roles of the Owner of the Machine	1-9
	Roles and Requirements of the Administrator	1-9
	Password Usage Requirements	1-9
	External authentication server control requirements	1-10
	Security function operation setting operating requirements	1-10
	Operation and control of the machine	1-10
	Machine Maintenance Control	1-12
	Precautions for using the printer driver	1-12
1.4	Miscellaneous	1-13
	Password Rules	1-13
	Precautions for Use of Various Types of Applications	1-14
	Encrypting communications	1-14
	IPsec setting	1-14
	Print functions	1-15
	IPP printing	1-15
	Items of Data Cleared by Overwrite All Data Function	1-16
	Fax functions	1-16
	USB keyboard	1-16
	Different types of boxes	1-17
	Hardware and software used in the machine	1-17
	Firmware integrity verification function	1-17
	CS Remote Care function	1-18
	Terminating a Session and Logging out	1-18
	Authentication error during external server authentication	1-18

2 Administrator Operations

2.1	Accessing the Administrator Mode	2-2
2.1.1	Accessing the Administrator Mode	2-2
2.1.2	Accessing the User Mode	2-8
2.2	Enhancing the Security Function	2-12
2.2.1	Items cleared by HDD Format	2-14
2.2.2	Setting the Password Rules	2-15
2.2.3	Setting the Enhanced Security Mode	2-17
2.3	Protecting Machine from Illegal Firmware Update	2-20
	Setting the FW Update (USB) Password	2-20
2.4	Preventing Unauthorized Access	2-23
	Setting Prohibited Functions When Authentication Error	2-23
2.5	Canceling the Operation Prohibited State	2-25
	Performing Release Setting	2-25
2.6	Setting the Authentication Method	2-27
2.6.1	Setting the Authentication Method	2-27
2.6.2	Setting the External Server	2-30
2.7	ID & Print Setting Function	2-32
	Setting ID & Print	2-32

2.8	ID & Print Operation Setting Function.....	2-34
	Making ID & Print Operation Setting.....	2-34
2.9	Auth. Operation Setting when print Documents are Stored Function	2-35
	Setting Auth. Operation Setting when print Documents are Stored Function.....	2-35
2.10	System Auto Reset Function	2-36
	Setting the System Auto Reset function.....	2-36
2.11	User Setting Function	2-38
	Making user setting.....	2-39
2.12	Account Track Setting Function.....	2-44
	Making account setting.....	2-44
2.13	User Box Function	2-49
2.13.1	Setting the User Box.....	2-49
2.13.2	Changing the user/account attributes and box password	2-54
2.13.3	Setting Memory RX.....	2-59
2.14	Changing the Administrator Password.....	2-62
	Changing the Administrator Password	2-62
2.15	Protecting Data in the HDD.....	2-65
2.15.1	Setting the Encryption Key (encryption word)	2-65
2.15.2	Changing the Encryption Key	2-69
2.15.3	Setting the Overwrite HDD Data	2-71
2.16	Overwrite All Data Function	2-73
	Setting the Overwrite All Data function.....	2-73
2.17	Obtaining Job Log.....	2-75
2.17.1	Obtaining and deleting a Job Log.....	2-75
2.17.2	Downloading the Job Log data.....	2-77
	Job Log data.....	2-79
2.18	Setting time/date in machine	2-88
2.18.1	Setting time/date.....	2-88
2.18.2	Setting daylight saving time.....	2-91
2.19	SSL Setting Function	2-93
2.19.1	Device Certificate Setting	2-93
2.19.2	SSL Setting	2-95
2.19.3	Removing a Certificate.....	2-96
2.20	TCP/IP Setting Function.....	2-97
2.20.1	Setting the IP Address	2-97
2.20.2	Registering the DNS Server	2-98
2.21	E-Mail Setting Function	2-99
	Setting the SMTP Server (E-Mail Server).....	2-99

3 User Operations

3.1	User Authentication Function.....	3-2
3.1.1	Performing user authentication.....	3-2
3.1.2	Accessing the ID & Print Document.....	3-6
3.2	Change Password Function.....	3-7
	Performing Change Password	3-7
3.3	Secure Print Function	3-10
	Accessing the Secure Print Document	3-10
3.4	User Box Function	3-13
3.4.1	Setting the User Box.....	3-13
3.4.2	Changing the user/account attributes and box password	3-18
3.4.3	Accessing the User Box and User Box file.....	3-24



4 **Application Software**

4.1	Data Administrator.....	4-2
4.1.1	Accessing from Data Administrator	4-2
4.1.2	Setting the user authentication method.....	4-5
4.1.3	Changing the authentication mode.....	4-6
4.1.4	Making the user settings.....	4-8
4.1.5	Making the account settings.....	4-9
4.1.6	DNS Server Setting Function	4-10
4.1.7	E-Mail Setting Function.....	4-11

1 Security

1 Security

1.1 Introduction

Thank you for purchasing our product.

This User's Guide contains the operating procedures and precautions to be used when using the security functions offered by the bizhub 368/308 machine. To ensure the best possible performance and effective use of the machine, read this manual thoroughly before using the security functions. The administrator of the machine should keep this manual for ready reference. The manual should be of great help in finding solutions to operating problems and questions.

This User's Guide (version 1.01) covers the following.

Model name	bizhub 368/bizhub 308
Version	G00-09

Administrators

<Administrator of the machine>

There are two types of administrators; one who is implemented on the machine in advance, and the other who is registered by the implemented administrator. The former is called the built-in administrator and the latter is called a user administrator. Below, the administrator of the machine means the built-in administrator.

<User administrator>

The user administrator is a user who is given the authority to operate the machine as an administrator. The administrator of the machine or the user administrator can register the user administrator. Be sure that "Precautions for Operation Control" applies to the user administrator. For details, see page 1-9.

The differences from the administrator of the machine are as follows:

- The same procedure as a user applies to the user administrator when he or she changes the password or fails authentication.
- To change password, log on to the User Mode.

<Note>

Below, the administrator collectively means both the administrator of the machine and the user administrator.

Compliance with the ISO15408 Standard

When the Enhanced Security Mode on this machine is set to [ON], more enhanced security functions are available.

This machine offers the security functions that comply with the ISO/IEC15408 (level: EAL2) and U.S. Government Approved Protection Profile - U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std 2600.2TM-2009).

Operating Precautions

The machine gives an alarm message or an alarm sound (peep) when a wrong operation is performed or a wrong entry is made during operation of the machine. (No "peep" alarm sound is issued if a specific sound setting in Sound Setting of Accessibility Setting is set to [OFF].) If the alarm message or alarm sound is given, perform the correct operation or make the correct entry according to the instructions given by the message or other means.

The administrator must not leave the machine with each setting screen left displayed before, during, and after access to each mode. If he or she has to leave the machine, make sure that he or she logs out and returns the screen to the authentication screen.

The administrator must make sure that each individual general user logs out and returns the screen to the authentication screen if he or she leaves the machine with each mode screen left displayed before, during, and after access to each mode.

If an error message appears during operation of the machine, perform steps as instructed by the message. For details of the error messages, refer to the User's Guide furnished with the machine. If the error cannot be remedied, contact your service representative.

Page rotation in the preview during scanning of the document in each of the copying, E-mail, and fax functions provided by the machine is reflected in the output. In the E-mail and fax functions, data can be deleted by the page and the deletion is reflected in the output.

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

For any query, request, or opinion concerning the machine, please contact your dealer from which you purchased your machine or Service Representative.

Any notice concerning this machine will be given in writing by the dealer from which you purchased your machine or Service Representative.

INSTALLATION CHECKLIST

This Installation Checklist contains items that are to be checked by the Service Engineer installing this machine. The Service Engineer should check the following items, then explain each checked item to the administrator of the machine.

To Service Engineer

Make sure that each of these items is properly carried out by checking the box on the right of each item.

1.	Perform the following steps before installing this machine.	
	Check with the administrator of the machine to determine if the security functions of this machine should be enhanced. If the functions should be enhanced, check the following. If the security functions are not to be enhanced, quit the operation without checking the following.	<input type="checkbox"/>
	<p>Before installing the machine, check with the administrator of the machine to determine if the following is confirmed.</p> <ul style="list-style-type: none"> • Whether the Service Engineer has been informed that the unpacking procedure is to be performed by the Service Engineer in the presence of the administrator. • Whether the machine has been under the control of the administrator of the machine with a check made to ensure that evidently the machine has not been unpacked or used. <p>The Service Engineer should obtain the administrator's consent to the performance of this item.</p> <p>If the machine has been unpacked, check with the administrator that it was the administrator who unpacked the machine and nobody but the administrator has gain access to the machine after the unpacking. Then, obtain the administrator's consent to the performance of the installation procedure for the unpacked machine before attempting to start the procedure. If the administrator's consent cannot be obtained, call the dealer.</p>	<input type="checkbox"/>
	I swear that I would never disclose information as it relates to the settings of this machine to anybody, or perform malicious or intentional act during setup and service procedures for the machine.	<input type="checkbox"/>
	<p>When giving a copy of the User's Guide, explain the following to the administrator:</p> <ul style="list-style-type: none"> • A digital signature is assigned to the data certified by ISO15408. To ensure integrity of the file, have the administrator of the machine confirm the digital signature using the property of the provided data file in the user's PC environment. Confirm the digital signature as follows. Right click the provided exe file to display the property screen. Select [Digital Signatures] - [Details] - [General], and check that Konica Minolta, Inc. is displayed in the Name of signer field. Select [View Certificate] - [General]. Then, check that the signing time is within the validated date of the certificate and that the certificate has been issued by a reliable certification authority. Write down the serial number shown in [View Certificate] - [Details]. Access to the URL for CRL Distribution Points and confirm that the serial number is not shown in [Revocation List]. For confirmation, the Internet environment is required. • Two versions are available, the HTML version and User's Guide Security Operations (this User's Guide). • In HTML version, option settings are described including functions those can be universally configured, but it does not mean that all of them are available. • This User's Guide must first be read and the conditions described in this User's Guide take precedence over the HTML version. • If the security functions of the machine are to be enhanced, the machine and its surrounding environment should be set up and operated according to this User's Guide. 	<input type="checkbox"/>
	<p>Refer to the Service Manual and perform the required installation and setup steps. During the installation and setup procedure, make sure that no unnecessary parts are mounted on the machine and have the administrator of the machine confirm that no unnecessary parts are mounted on the machine.</p> <ul style="list-style-type: none"> • Explain to the administrator making him/her check the cover of the Service Manual to be referred that it is for bizhub 368/bizhub 308 (Version: G00-09). Explain to the administrator that the following settings must be performed referring to the manuals above. • The Service Engineer must have the administrator confirm that the digital signature is assigned to the firmware and the version of the firmware to be updated is the one that is written on the Service Manual. 	<input type="checkbox"/>

2. After this machine is installed, refer to the Service Manual and perform the following steps.		
	Check that the model name and the Firmware version (card version) checked with the Service Manual agree with the value shown on the Firmware version display screen. Check also that the MFP model name and the part numbers of the MFP board and the eMMC board agree with those described in the Service Manual. If there is a mismatch in the Firmware version number, explain to the administrator of the machine that upgrading of the Firmware is necessary and perform upgrading of the Firmware.	<input type="checkbox"/>
	Check that the Fax Kit has been mounted and set up properly, if fax functions are to be used. After the installation, conduct transmission and reception tests to make sure that the Fax Kit has been mounted and set up properly.	<input type="checkbox"/>
	Let the machine read the Custom Function Pattern Selection setting file to which an electronic signature is assigned. Explain to the administrator that the Custom Function Pattern Selection setting file is dedicated to the machine in question.	<input type="checkbox"/>
	Get the administrator of the machine to confirm that [ISO15408] is selected for [Send/Save] of [Custom Function Pattern Selection] in the Administrator Settings and obtain his or her consent not to change the setting.	<input type="checkbox"/>
	Set CE Authentication to [ON] and set the CE Password.	<input type="checkbox"/>
	Make the service settings necessary for the Enhanced Security Mode.	<input type="checkbox"/>
3. After this machine is installed, refer to this User's Guide and perform the following steps.		
	Check that the Administrator Password has been set by the administrator of the machine. Select [Restrict] when the confirmation screen of machine usage information is displayed. If [Allow] is mistakenly selected, make the following settings: <ul style="list-style-type: none"> Set the function counter (Transmission Meter Count and Device Information) to [Restrict]. Set the TX Operation Log setting to [Do not Save]. For the setting procedure, see bizhub 558/458/368/308 User's Guide version 1.00 A9HJ-9590BA-00. Setting by the Service Engineer is required for the following: <ul style="list-style-type: none"> Debug Log Collection System function (software SW No. 155) Export Debug Log 	<input type="checkbox"/>
	Check that the Encryption Key has been set by the administrator of the machine.	<input type="checkbox"/>
	Check that the Overwrite HDD Data has been set by the administrator of the machine.	<input type="checkbox"/>
	Check that User Authentication has been set to [ON (MFP)], [External Server Authentication] (Active Directory only), or [Main + External Server] (Active Directory only) by the administrator of the machine.	<input type="checkbox"/>
	Check that the date and time have been correctly set in the machine by the administrator of the machine.	<input type="checkbox"/>
	Check that the Job Log Settings (Audit Log) has been set to [Yes] by the administrator of the machine.	<input type="checkbox"/>
	Check that the certificate for SSL communications has been registered by the administrator of the machine. In accordance with the security policies of the organization, register the certificate that is issued by a reliable authentication authority.	<input type="checkbox"/>
	Check that the ID & Print Settings has been set to [ON] by the administrator of the machine.	<input type="checkbox"/>
	Check that the Memory RX Setting has been set to [Yes] by the administrator of the machine.	<input type="checkbox"/>
	Check that IPsec has been set by the administrator of the machine for communications between the machine and the external authentication server.	<input type="checkbox"/>
	Check that IPsec has been set by the administrator of the machine for communications between the machine and the DNS server.	<input type="checkbox"/>
	Check that IPsec has been set by the administrator of the machine for communications between the machine and the SMTP server.	<input type="checkbox"/>
	Check that IPsec has been set by the administrator of the machine for communications between the machine and a client PC.	<input type="checkbox"/>

	Let the administrator of the machine set Enhanced Security Mode to [ON].	<input type="checkbox"/>
	Check that the FW Update (USB) Password has been set by the administrator of the machine.	<input type="checkbox"/>
	Check that the various functions to be disabled manually have been properly disabled by the administrator of the machine.	<input type="checkbox"/>
	The languages, in which the contents of the User's Guide Security Operations have been evaluated, are Japanese and English. The following lists the manuals compatible with bizhub 368/bizhub 308 (Version: G00-09). <ul style="list-style-type: none"> • bizhub 558/458/368/308 User's Guide Ver. 1.00 A9HJ-9590BA-00 • bizhub 368/308 User's Guide Security Operations 2017. 2 Ver. 1.01 	<input type="checkbox"/>
	Explain to the administrator of the machine that the settings for the security functions for this machine have been specified.	<input type="checkbox"/>

After completing the checks, keep a copy of this list in the Service Representative and give the original of this list to the administrator of the machine.

Please direct your any queries about using the machine to the Service Representative shown below.

Product Name		Company Name	User Division Name, Contact	Person in charge
Customer (administrator of the machine)				
Service Representative				

1.2 Security Functions

Setting the Enhanced Security Mode to [ON] will validate the security function of this machine. For details of the settings of different security functions to be changed by turning [ON] the Enhanced Security Mode, see page 2-12.

The following are the major security functions when the Enhanced Security Mode is set to [ON].

Function	Description
Identification and authentication function	Access control is then provided through password authentication for any access to the Administrator Mode, User Authentication mode, User Box, a User Box data file, and a Secure Print document. Access is thereby granted only to the authenticated user. A password that can be set must meet the Password Rules. The machine does not accept setting of an easily decipherable password. For details of the Password Rules, see page 1-13. If a wrong password is entered, during password authentication, a predetermined number of times (once to three times.) or more set by the administrator, the machine determines that it is unauthorized access through Prohibited Functions When Authentication Error, prohibiting any further entry of the password. By prohibiting the password entry operation, the machine prevents unauthorized use or removal of data. The administrator is responsible for resetting the prohibition of the password entry operation. For details, see page 2-25.
User limiting function	Specific functions to be used by each user/account may be limited. For details, see page 2-38.
HDD encryption function	By setting the Encryption Key, the data stored in the HDD is encrypted, thereby protecting the data in the HDD. For details, see page 2-65.
Auditing function	Information including operations performed on the machine and a job history can be stored in the HDD. Setting the Job Log (Audit Log) allows an illegal act or inadequate operation performed on the machine to be traced. The obtained Job Log can be downloaded and viewed from the Web Connection . For details, see page 2-75.
Residual information deleting function	When the machine is to be discarded or use of a leased machine is terminated at the end of the leasing contract, setting of the Overwrite HDD Data function while the machine was in use allows residual unnecessary data to be deleted, because the machine overwrites a specific overwrite value over the unnecessary data. This prevents data leakage. (Passwords, addresses, and other data set while the machine was in use should, however, be deleted manually.) For details, see page 2-71. To delete data including the passwords, addresses, and other data all at once, the Overwrite All Data function overwrites and erases all data stored in all spaces of the HDD. The function also resets all passwords saved in the flash memory and eMMC to factory settings, preventing data from leaking. For details, see page 2-73. For details of items to be cleared by Overwrite All Data function, see page 1-16.
Network communication protecting function	Communication data transmitted to or from the machine and client PC can be encrypted using the IPsec, which prevents information leakage through sniffing over the network. For details, see page 1-14.

Check Count Clear Conditions

In the Enhanced Security Mode, the number of wrong entries at the time of authentication is checked. The following are the conditions for clearing or resetting the number.

<Administrator Authentication>

- Authentication of Administrator of the machine is successful.

<User Authentication Mode>

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

<Account Track Mode>

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

<Secure Print>

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

<Box>

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

1.3 Precautions for Operation Control

This machine and the data handled by this machine should be used in an office environment that meets the following conditions. The machine must be controlled for its operation under the following conditions to protect the data that should be protected.

Roles of the Owner of the Machine

The owner (an individual or an organization) of the machine should take full responsibility for controlling the machine, thereby ensuring that no improper operations are performed.

- The owner of the machine should have the administrator recognize the organizational security policy and procedure, educate him or her to comply with the guidance and documents prepared by the manufacturer, and allow time for him or her to acquire required ability. The owner of the machine should also operate and manage the machine so that the administrator can configure and operate the machine appropriately according to the policy and procedure.
- The owner of the machine should have users of the machine recognize the organizational security policy and procedure, educate them to follow the policy and procedure, and operate and manage the machine so that the users acquire the required ability.
- The owner of the machine should vest the user with authority to use the machine according to the organizational security policy and procedure.
- The owner of the machine should operate and manage the machine so that the administrator checks the Job Log (Audit Log) data at appropriate timing to thereby determine whether a security compromise or a faulty condition has occurred during an operating period.
- If the Job Log (Audit Log) data is to be exported to another product, the owner of the machine should ensure that only the administrator performs the task. The owner of the machine should also operate and manage the machine so that the Job Log (Audit Log) data is not illegally accessed, deleted, or altered.

Roles and Requirements of the Administrator

The administrator should take full responsibility for controlling the machine, thereby ensuring that no improper operations are performed.

- A person who is capable of taking full responsibility for controlling the machine should be appointed as the administrator to make sure that no improper operations are performed.
- When using an external authentication server, an SMTP server (mail server), or a DNS server, each server should be appropriately managed by the administrator and should be periodically checked to confirm that settings have not been changed without permission.

Password Usage Requirements

The administrator must control the Administrator Password, Encryption Key, FW Update (USB) Password, and User Box Password appropriately so that they may not be leaked. These passwords should not be ones that can be easily guessed. The user, on the other hand, should control the Secure Print Password and User Password appropriately so that they may not be leaked. Again, these passwords should not be ones that can be easily guessed.

<To Achieve Effective Security>

- Make absolutely sure that only the administrator of the machine knows the Administrator Password.
- Make absolutely sure that only the administrator knows the Encryption Key, FW Update (USB) Password, and User Box Password.
- Make sure that the administrator of the machine changes the Administrator Password regularly.
- The administrator must change the Encryption Key, FW Update (USB) Password, and User Box Password at regular intervals.
- The administrator of the machine should make sure that any number that can easily be guessed from birthdays, employee identification numbers, and the like is not set for the Administrator Password.
- The administrator should make sure that any number that can easily be guessed from birthdays, employee identification numbers, and the like is not set for the Account Password, Encryption Key, FW Update (USB) Password, and User Box Password.
- If a User Password has been changed, the administrator should have the corresponding user change the password as soon as possible.
- If the Administrator Password has been changed by the Service Engineer, the administrator of the machine should change the Administrator Password as soon as possible.

- The administrator should have users ensure that the passwords set for the User Authentication, Secure Print, and the box that can be used by the user are known only by the user concerned.
- The administrator should have users change the passwords set for the User Authentication at regular intervals.
- The administrator of the machine should have the user administrator log on to the User Mode and change his or her password in [Utility] - [User Settings] - [Change Password] if he or she changes the password.
- The administrator should make sure that any user does not set any number that can easily be guessed from birthdays, employee identification numbers, and the like for the passwords set for the User Authentication and Secure Print.
- The administrator should disclose the Account Password to the user in accordance with the operating environment of the machine and the security policies of the organization on his or her own responsibility.

External authentication server control requirements

The administrator and the server administrator are required to apply patches to, or perform account control for, this machine and the external authentication server connected to the office LAN in which the machine is installed to ensure operation control that achieves appropriate access control.

This machine can be used only after the user who uses this machine has been registered in the external authentication server. The server administrator should also check registered users at regular intervals to thereby ensure that any unnecessary users are left registered.

Security function operation setting operating requirements

The administrator should observe the following operating conditions.

- The administrator should make sure that the machine is operated with the settings described in the installation checklist made properly in advance.
- The administrator should make sure of correct operation control so that the machine is used with the Enhanced Security Mode set to [ON].
- The administrator should make sure of correct operation control so that the appropriate FW Update (USB) Password is used with [FW Update (USB) Permission Setting] set to [Password Priority].
- When the Enhanced Security Mode is turned [OFF], the administrator is to make various settings according to the installation checklist and then set the Enhanced Security Mode to [ON] again. For details of settings made by the service engineer, contact your service representative.
- When the machine is to be discarded or use of a leased machine is terminated at the end of the leasing contract, the administrator should use the Overwrite HDD Data function and the Overwrite All Data function to thereby prevent data to be protected from leaking.

Operation and control of the machine

The administrator should perform the following operation control.

- The administrator should log off from the Administrator Mode whenever the operation in the Administrator Mode is completed. The administrator of the machine should also make sure that each individual user logs off from the User Authentication mode after the operation in the User Authentication mode is completed, including operation of the Secure Print document, User Box, and User Box file.
- During user registration and box registration, the administrator should make sure that the correct settings are made for the correct users, including functional restrictions and box attributes.
- The administrator should set the Encryption Key and FW Update (USB) Password according to the environment, in which this machine is used.
- The administrator should appropriately control the device certificate (SSL certificate) registered in the machine.
- The administrator should ensure that no illegal connection or access is attempted when the machine is to be connected to an external interface.
- The administrator should appropriately control the file of Job Log (Audit Log) data downloaded to, for example, a PC and ensure that none other than the administrator of the machine handle it.
- The administrator should check the Job Log (Audit Log) data at appropriate timing, thereby determining whether a security compromise or a faulty condition has occurred during an operating period.
- When generating or deleting Job Log (Audit Log) and Job Log (Audit Log) data, the administrator should check conditions of using this machine by the user.

- The administrator should make sure that each individual user updates the OS of the user's terminal and applications installed in it to eliminate any vulnerabilities.
- The administrator should set the account track and make sure that the machine is operated through operative association with the account track.
- The administrator should delete cache following the procedure specified for each browser when seeing previews on a web browser because the contents can be cached on PCs and make sure that users perform the same procedure.
- The administrator must not select a modem method when setting CS Remote Care.
- The administrator should make sure that a USB device is not illegally connected to the machine.

The administrator disables the following functions and operates and manages the machine under a condition in which those functions are disabled.

Function Name	Setting Procedure
IP Address Fax Function *	Using [Administrator Settings] - [Network Settings] - [Network Fax Settings] - [Network Fax Function Settings], set [IP Address Fax Function] to [OFF].
Internet Fax Function *	Using [Administrator Settings] - [Network Settings] - [Network Fax Settings] - [Network Fax Function Settings], set [Internet Fax Function] to [OFF].
Relay User Box	Using [Administrator Settings] - [Fax Settings] - [Function Settings] - [Function ON/OFF Setting], set [Relay RX] to [OFF].
File Re-TX Box	Using [Administrator Settings] - [Fax Settings] - [Function Settings], set [Incomplete TX Hold] to [No].
PC-Fax Permission	Using [Administrator Settings] - [Fax Settings] - [Function Settings], set [PC-Fax Permission Setting] to [Restrict].
ID & Print Delete after Print Setting	Using [Administrator Settings] - [System Settings] - [User Box Settings], set [ID & Print Delete after Print Setting] to [Always Delete].
User Box Settings	Using [Administrator Settings] - [System Settings] - [User Box Settings], set [Allow/Restrict User Box] to [Prohibit].
Report Settings	Using [Administrator Settings] - [Fax Settings], set all report output settings of [Report Settings] to [OFF].
Bulletin Board User Box	<ul style="list-style-type: none"> • Do not create [Bulletin Board User Box] using [Utility] - [One-Touch/User Box Registration] - [Create User Box]. • Do not create [Bulletin Board User Box] using [Administrator Settings] - [One-Touch/User Box Registration] - [Create User Box].
Delete Other User Jobs	Using [Administrator Settings] - [System Settings] - [Restrict User Access] - [Restrict Access to Job Settings], set [Delete Other User Jobs] to [Restrict].
RAW Port Number	Using [Administrator Settings] - [Network Settings] - [TCP/IP Settings] - [RAW Port Number], set [Port 1 to Port 6] to [OFF].
FTP TX Settings	Using [Administrator Settings] - [Network Settings] - [FTP Settings], set [FTP TX Settings] to [OFF].
SMB Settings	<ul style="list-style-type: none"> • Using [Administrator Settings] - [Network Settings] - [SMB Settings], set [Client Settings] to [OFF]. • Using [Administrator Settings] - [Network Settings] - [SMB Settings], set [SMB Server Settings] to [OFF]. • Using [Administrator Settings] - [Network Settings] - [SMB Settings], set [WINS/NetBIOS Settings] to [OFF]. • Using [Administrator Settings] - [Network Settings] - [SMB Settings], set [Direct Hosting Setting] to [OFF].
E-Mail RX (POP)	Using [Administrator Settings] - [Network Settings] - [E-Mail Settings], set [E-Mail RX (POP)] to [OFF].
SNMP Settings	Using [Administrator Settings] - [Network Settings], set [SNMP Settings] to [OFF].
TCP Socket Settings	<ul style="list-style-type: none"> • Using [Administrator Settings] - [Network Settings] - [Forward] - [TCP Socket Settings], set [TCP Socket] to [OFF]. • Using [Administrator Settings] - [Network Settings] - [Forward] - [TCP Socket Settings], set [TCP Socket (ASCII Mode)] to [OFF].

Function Name	Setting Procedure
SSL/TLS Version Setting	Start the Web Connection and, using [Security] - [PKI Settings] - [SSL Setting] of the administrator mode, cancel the selection of [SSLv3] of [SSL/TLS Version Setting].
WebDAV Settings	<ul style="list-style-type: none"> Using [Administrator Settings] - [Network Settings] - [WebDAV Settings], set [WebDAV Client Settings] to [OFF]. Using [Administrator Settings] - [Network Settings] - [WebDAV Settings], set [WebDAV Server Settings] to [OFF].
DPWS Settings (Printer Settings/Scanner Settings)	<ul style="list-style-type: none"> Using [Administrator Settings] - [Network Settings] - [DPWS Settings], set [Printer Settings] to [OFF]. Using [Administrator Settings] - [Network Settings] - [DPWS Settings], set [Scanner Settings] to [OFF].
LPD Setting	Using [Administrator Settings] - [Network Settings] - [Detail Settings], set [LPD Setting] to [Disable].
Remote Access Setting	Using [Administrator Settings] - [Network Settings], set [Remote Access Setting] to [OFF].
LLMNR Setting	Using [Administrator Settings] - [Network Settings] - [TCP/IP Settings], set [LLMNR Setting] to [Disable].
AirPrint	Using [Administrator Settings] - [Authorization function Setting] - [Install License] - [Function Code], prohibit entering the AirPrint-enabling code and enabling AirPrint.
Bonjour Setting	Using [Administrator Settings] - [Network Settings], set [Bonjour Setting] to [OFF].
Mopria Setting	Using [Administrator Settings] - [Network Settings] - [Mopria Setting], set [Terminal Request Response Setting] to [OFF] and do not to set it to [ON].
Send Domain Limit Settings	Using [Administrator Settings] - [Network Settings], set [Send Domain Limit Settings] to [Do Not Limit] and do not to set it to [Limit].
LLTD Setting	Using [Administrator Settings] - [Network Settings] - [Detail Settings] - [Device Setting], set [LLTD Setting] to [Disable] and do not to set it to [Enable].
Personal Data Security Settings	Using [Administrator Settings] - [Security Settings] - [Security Details], set [Job History] and [Current Job] under [Personal Data Security Settings] to [Yes].

*: It will not be displayed in case of service mode where the setting is not configured (the function is set to OFF when it is not displayed).

Machine Maintenance Control

The administrator should perform the following maintenance control activities.

- Provide adequate control over the machine to ensure that only the Service Engineer is able to perform physical service operations on the machine.
- Provide adequate control over the machine to ensure that any physical service operations performed on the machine by the Service Engineer are overseen by the administrator.
- Some options require that Enhanced Security Mode be turned [OFF] before they can be used on the machine. If you are not sure whether a particular option to be additionally purchased is fully operational with the Enhanced Security Mode turned [ON], contact your Service Representative.
- Install the machine at a safe site that can be monitored and operate and manage the machine while ensuring that the machine is protected from unauthorized physical access.

Precautions for using the printer driver

The following precautions should be used when the printer driver is to be used in this machine:

- When a document is to be transmitted from the PC to the machine, user registration is necessary in advance.
- With the external server authentication, a user is registered in this machine when he or she has been successful in identification authentication on the control panel.
- Any document that has been transmitted by a user who is yet to be registered is discarded.

1.4 Miscellaneous

Password Rules

Study the following table for details of the number and types of characters that can be used for each password. For details of the settings of the Password Rules, see page 2-15.

Types of passwords	Number of characters	Types of characters	Conditions for setting/changes
Administrator Password	8 to 64 characters*	<ul style="list-style-type: none"> Numeric characters: 0 to 9 Alpha characters: upper and lower case letters Symbols: !, #, \$, %, &, ', (,), *, ,, -, ., /, :, ;, <, =, >, ?, @, [, \,], ^, _ , ` , {, , }, ~, + Special characters (98 characters) Selectable from among a total of 191 characters	<ul style="list-style-type: none"> A password only consisting of identical characters cannot be registered or changed. The current password must be entered before a change can be made in the setting. A new password to be set should not be the same as the current one.
User Password			
Account Password			
Public User Box Password			
Annotation User Box Password	8 to 64 characters*	<ul style="list-style-type: none"> Numeric characters: 0 to 9 Alpha characters: upper and lower case letters Symbols: !, #, \$, %, &, ', (,), *, ,, -, ., /, :, ;, <, =, >, ?, @, [, \,], ^, _ , ` , {, , }, ~, +, SPACE Selectable from among a total of 94 characters	<ul style="list-style-type: none"> A password only consisting of identical characters cannot be registered.
Secure Print Password			
Confidential RX password	8 characters	<ul style="list-style-type: none"> Numeric characters: 0 to 9 Symbols: *, # 	<ul style="list-style-type: none"> A password only consisting of identical characters cannot be registered or changed.
FW Update (USB) Password	0 to 20 characters	<ul style="list-style-type: none"> Numeric characters: 0 to 9 Alpha characters: upper and lower case letters Symbols: !, #, \$, %, &, ', (,), *, ,, -, ., /, :, ;, <, =, >, ?, @, [, \,], ^, _ , ` , {, , }, ~, +, SPACE Selectable from among a total of 94 characters	<ul style="list-style-type: none"> A new password needs to be re-entered.
Memory RX User Box Password	1 to 8 characters	<ul style="list-style-type: none"> Numeric characters: 0 to 9 	<ul style="list-style-type: none"> The password rules are not applicable.
Encrypted PDF Password	-	-	<ul style="list-style-type: none"> The password rules are not applicable. Password that is set when PDF document is created.

*: The minimum number of characters set in [Set Minimum Password Length] must be set for the password. The default value is 12.

Precautions for Use of Umlaut

- Setting or entering an umlaut from the control panel may be disabled depending on the setting made in this machine, but not on the client PC side including **Web Connection**. If an umlaut is set in a password on the PC side, therefore, the umlaut cannot be entered from the control panel, which means that this particular password is not usable.

Precautions for Use of Various Types of Applications

Comply with the following requirements when using the **Web Connection** or an application of various other types

The administrator should make sure that the user observes the following requirements.

- The password control function of each application stores the password that has been entered in the PC being used. Disable the password management function of each application and perform an operation without storing a password.
Use a web browser or an application of various other types that shows "*" or "●" for the password entered.
- Once the password has been entered, do not leave your PC idle without logging on.
- Set the web browser so that cache files are not saved.
- Do not access any other site once you have logged onto the machine with the **Web Connection**. Accessing any other site or a link included in e-mail, in particular, can lead to execution of an unintended type of operation. Whenever access to any other site is necessary, be sure first to log off from the machine through the **Web Connection**.
- Using the same password a number of times increases the risk of spoofing.
- If a web browser such as Internet Explorer is used on the client PC side, "TLS v1.0" or more should be used for the SSL setting.
- Optional applications not described in this User's Guide are not covered by certification of ISO15408.

Encrypting communications

This machine guarantees encrypted communication via IPsec.

IPsec setting

This machine offers a choice of two authentication methods of [Pre-Shared Key] and [Digital Signature] for authenticating the remote machine with which to communicate.

When [Pre-Shared Key] is to be used, control the pre-shared key appropriately to ensure that it is not leaked to any third party other than the remote machine with which to communicate. For the shared key, set a value that consists of a combination of eight or more alphanumeric characters and that cannot be easily guessed. Do not set a value that can be easily guessed from your birthday, employee identification number, and the like.

[Digital Signature] has a higher security strength than [Pre-Shared Key].

The ISO15408 evaluation for the machine is performed on the basis of the [Pre-Shared Key].

Do not use DES or 3DES in the encryption algorithm of [IKE Settings]. Use AES. [Main Mode] and [Aggressive Mode] are available in [Negotiation Mode]. The default setting is [Main Mode]. The administrator should operate the machine with the [Main Mode] setting.

Leaking the pre shared key for IPsec set on the MFP increases the risk of spoofing of the MFP, etc. Therefore, set machine-specific pre shared keys and manage them safely.

An illegal DNS response (e.g., a response exceeding 2048 bytes) made by the DNS server may cause the TOE to perform an unexpected operation. The administrator should control such that the DNS server does not make such a response. It should also be noted that setting of multiple DNS servers increases the risk.

Note that unencrypted communication can be established if the IPsec setting is not made over the whole address range (0 to 255 for IPv4) and an IP address outside the range is assigned to a client PC.

Select an ESP Encryption Algorithm from AES-GCM, AES-CBC, and AES-CTR for IPsec SA Settings. Furthermore, when AES-CBC or AES-CTR is selected, select an ESP Authentication Algorithm from SHA-1, SHA-2, and AES-XCBC.

NOTICE

The administrator of the machine should make sure that SSL encryption communication is not performed with the SSL set in SSL v3.

Do not use an SSL certificate that is electronically signed by MD5, as an increased risk results of data to be protected being tampered with or leaked.

To eliminate the risk of the data to be protected being tampered with or leaked, refer to the recommended ciphers list disclosed by, for example, NIST and CRYPTREC and use the appropriate cryptographic technique.

Use the following browsers to ensure safety. Use of any of the following browsers achieves communication that ensures confidentiality of the image data transmitted and received.

Microsoft Internet Explorer

- 9/10/11

Mozilla Firefox

- 20 or later

Microsoft Internet Explorer 11 is used for the ISO15408 evaluation for this machine.

Print functions

Only the following procedures are guaranteed for the print functions performed from the client PC.

- Use IPPS printing for the print functions performed using the printer driver.
- Use direct printing from the **Web Connection** for the print functions not performed via the printer driver.

IPP printing

IPP (Internet Printing Protocol) is a function that allows printing via the Internet by using the HTTP (HyperText Transfer Protocol) of the TCP/IP Protocol. IPPS (IPP over SSL/TLS) is the type of IPP that performs the SSL encryption communication.

<Installing printer driver>

To perform IPPS printing, the printer driver must be installed. Start the printer addition wizard of the Windows Vista/7/8/8.1/Server 2008/Server 2008 R2/Server 2012/Server 2012 R2 and type [DNS Host Name] and [Default DNS Domain Name] of this machine in the following format in the "URL" field.

https://[DNS host name].[default DNS domain name]/ipp

For [DNS host name] and [default DNS domain name], specify the names set with the DNS server.

<Registering the certificate in Windows Vista or later>

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

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

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

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

Items of Data Cleared by Overwrite All Data Function

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

Items of Data Cleared	Description
Password Rules	Sets [Disable] and disables [Set Minimum Password Length]
User registration data	Deletes all user-related data that has been registered
Account track registration data	Deletes all account track-related data that has been registered
Box registration data/file	Deletes all User Box-related information and files saved in User Box
Secure Print ID/Password/document	Deletes all Secure Print document-related information and files saved
ID & Print document	Deletes all ID & Print documents saved in ID & Print User Box
Image files	<ul style="list-style-type: none"> Image files other than Secure Print documents, ID & Print documents, and User Box files Data files left in the HDD data space, used as image files and not deleted through the general deletion operation Temporary data files generated during print image file processing
Destination recipient data files	Deletes all destination recipient data including e-mail addresses and telephone numbers
Encryption Key	Clears the currently set Encryption Key
Administrator Password	Clears the currently set password, resetting it to the factory setting (1234567812345678)
FW Update (USB) Password	Clears the currently set FW Update (USB) Password
Device certificate (SSL certificate)	Deletes the currently set Device certificate (SSL certificate)
SSL encryption strength	Deletes the SSL certificate to thereby clear the SSL encryption strength
SSL-compliant protocol	Makes the protocol not complying with SSL
Network Setting	Clears the currently set network settings (DNS Server setting, IP Address setting, and SMTP Server setting), resetting it to the factory setting
Daylight Saving Time	Set to [No]
Time Adjustment Setting (NTP)	Set to [OFF]
Time/date data	Varies corrected data, if the time-of-day data is corrected due to, for example, the daylight saving time

Fax functions

An optional Fax Kit is required for using fax functions. Contact your Service Representative.

USB keyboard

The USB keyboard is not used for the ISO15408 evaluation for this machine.

Do not use a USB keyboard.

Different types of boxes

A box may be a user box or a system box. The user can store documents in the User Box. Also, the user can print a file from the User Box or send a file to another user. The System Box is used by the system to temporarily store files when the user uses the facsimile or print function together with the file storage function of the box.

The User Box (*) cannot be used under the operation and control of this machine.

Type	Description
Public User Box *	This is the public box in which all users can store documents and use them. Note that a password is set for the box and the set password needs to be entered before access can be gained to the box.
Personal User Box *	This is a personal box. Only users who have logged in to the system can store and use documents in the Personal User Box.
Group User Box *	This is a group box. Only users belonging to the same department (or group) can store and use documents in the Group User Box.
Secure Print Box	When you print a document from the PC or when you select the Secure Print function using the printer driver, this data file is stored in the Secure Print User Box.
Memory RX Box	When a facsimile is received by the Memory RX function, it is stored in the Memory RX User Box.
ID & Print Box	When you print a document from the PC, the files transferred with the ID & Print function are stored in the ID & Print User Box.
Annotation User Box	When a stored file is printed out or sent to another user, its date, time and any annotations are added to this box automatically.
Password Encrypted PDF Box	When a password protected PDF file is printed out or stored in the User Box, the file is stored in the Password Encrypted PDF User Box.

Hardware and software used in the machine

The following lists the software, hardware, and their versions used for the ISO15408 evaluation for this machine and they are the same as those listed on the security target.

The ISO15408 evaluation assumes that the HDD is mounted in the machine. Any configuration not including the HDD is not guaranteed by the ISO15408 evaluation.

The user should appropriately manage the hardware and software used with the machine on his or her own responsibility.

Hardware/software	Version, etc.
FAX Kit	FK-514
Printer Driver	PCL: Ver. 6.1.2.0
	PS: Ver. 6.1.2.0
	XPS: Ver. 6.1.2.0
Data Administrator with Device Set-Up and Utilities	Ver. 1.0.09000
Data Administrator	Ver. 4.1.38000
External authentication server	Active directory mounted on Windows Server 2008 R2 Standard Service Pack 1
DNS server	Windows Server 2008 R2 Standard Service Pack1

Firmware integrity verification function

When the **main power switch** is turned ON with the Enhanced Security Mode set to [ON], the machine checks the encryption key and the hash value to thereby determine that its firmware is fully operational.

If a fault occurs in the firmware, a malfunction screen appears when the machine is started, warning that a fault has occurred. To reset the fault condition, turn [OFF] the Enhanced Security Mode and restart the machine, or update the firmware. For more details, consult your Service Representative.

CS Remote Care function

CS Remote Care is a system that manages the machine through transmission and reception of various types of data for managing the machine between the machine and the CS Remote Care center computer via a telephone/fax line, a network, or E-mail. Functions are disabled to access the LAN from the telephone line and to directly transfer received fax.

When the Enhanced Security Mode is set to [ON], the following functions are no longer usable: instructing to rewrite the firmware, sending and receiving account counter information, rewriting settings of the machine, and the Counter Remote Control function.

Terminating a Session and Logging out

The machine allows the operator to automatically log out from or terminate a session, if it is unable to detect an operation on the control panel or a communication packet on the network. Additionally, if a user changes the user password on the control panel while the same user accessing the machine via **Web Connection**, the session of **Web Connection** is terminated.

The following shows the setting range and the default setting of each function. Set the time according to the environment in which the machine is used.

The administrator should explain to the user that the following settings are made. The administrator should also explain to the user immediately as soon as the setting has been changed.

Function name/software, etc	Description
System Auto Reset	Setting range <ul style="list-style-type: none"> [1] to [9] minutes, Default setting: [1] minute Setting procedure <ul style="list-style-type: none"> [Utility] - [Administrator Settings] - [System Settings] - [Reset Settings] - [System Auto Reset]
Auto Logout (Web Connection)	Setting range <ul style="list-style-type: none"> [Admin. Mode Logout Time]: [1] to [60] minutes Default setting: [10] minutes [User Mode Logout Time]: [1] to [60] minutes Default setting: [60] minutes Setting procedure <ul style="list-style-type: none"> Start the Web Connection and, in the Administrator Mode, select [Security] - [Auto Logout].
Data Administrator	Default setting: [60] minutes (No change can be made in the setting) The time setting represents consideration for the time-consuming task, such as downloading the registered information. Be careful about leaving your seat, because the time setting is rather long.

Authentication error during external server authentication

If a user is unable to log in successfully during user authentication using the external server authentication, possible causes include the status of connection to the external server, the condition of the external server (the server is down), and the status of user registration with the external server such as the number of users to be controlled by the machine reaching its limit and the user password quality on the external server.

The administrator should check these points and make the appropriate settings.



Administrator Operations

2 Administrator Operations

2.1 Accessing the Administrator Mode

In Administrator Mode, the settings for the machine system and network can be registered or changed.

This machine implements authentication of the user of the Administrator Mode function through the Administrator Password or User Password that verifies the identity as the administrator of the person who accesses the function. During the authentication procedure, the Administrator Password entered for the authentication purpose appears as "*" or "●" on the display.

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

NOTICE

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

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

The user who is given the administrative right by the administrator can access the Administrator Mode when logging on as the user administrator.

2.1.1 Accessing the Administrator Mode

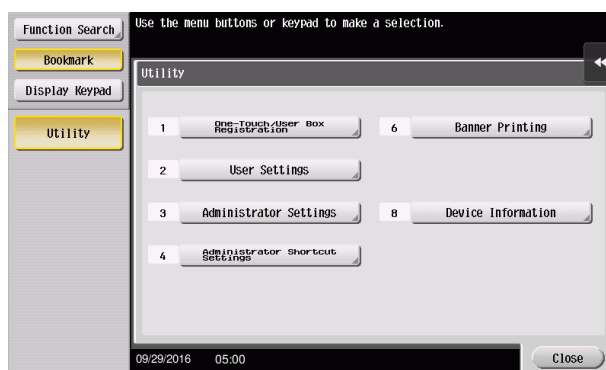
The machine does not accept access to the Administrator Mode under any of the following conditions. Wait for some while before attempting to gain access to the Administrator Mode again.

- The Administrator Mode has been logged on to through access made from the PC.
- A remote operation is being performed from an application on the PC.
- There is a job being executed by the machine.
- There is a reserved job (timer TX, fax redial waiting, etc.) in the machine.
- Immediately after the **main power switch** has been turned ON.
- A malfunction code is displayed on the machine.

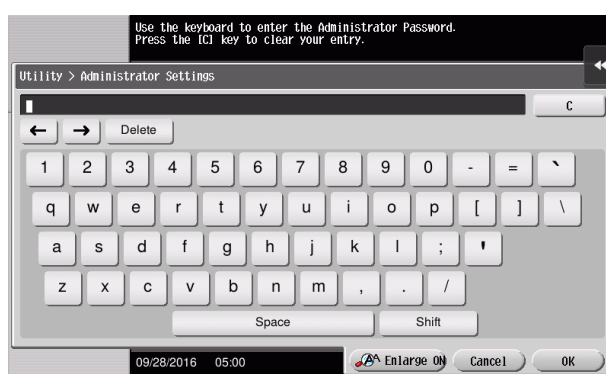
<From the Control Panel as the Administrator of the Machine>

- ✓ If another administrator has already logged on to the Administrator Mode using Web Connection, the machine displays a message saying that other administrator has logged on and rejects access as the administrator. Wait until the message disappears before attempting to access the Administrator Mode once again.
- ✓ When accessing the Administrator Mode from the control panel, if [Export to the device] operation is being executed using the **Data Administrator**, the machine displays a message that tells not to turn off the power because of the remote operation being performed and rejects any operation on the control panel. Wait until the message disappears before attempting to access the Administrator Mode once again.
- ✓ Do not leave the machine with the setting screen of Administrator Mode left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Mode.

- 1 Touch [Utility].
- 2 Touch [Administrator Settings].



- 3 Enter the Administrator Password from the keyboard.



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

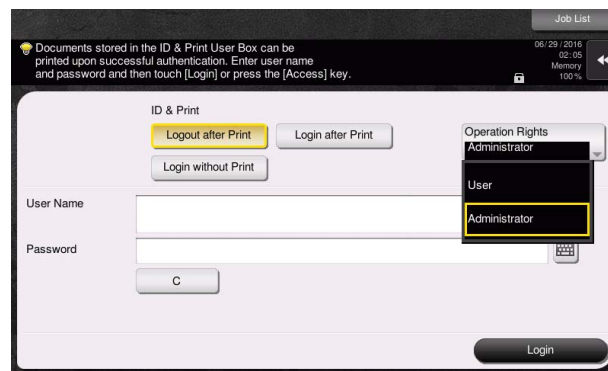
- 4 Touch [OK].

- If a wrong Administrator Password is entered, a message that tells that the Administrator Password does not match appears. Enter the correct Administrator Password.
- If the Enhanced Security Mode is set to [ON], entry of a wrong password is counted as unauthorized access. If a wrong Administrator Password is entered a predetermined number of times (once to three times) or more set by the administrator, a message appears saying that the machine accepts no more Administrator Passwords because of unauthorized access for any subsequent entry of the Administrator Password. The machine is then set into an access lock state. To cancel the access lock state, settings must be made by the Service Engineer; or, turn off, and then turn on, the **main power switch** of the machine. If the **main power switch** is turned off and on, the access lock state is canceled after the lapse of time set for [Release Time Settings]. When the **main power switch** is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. If there is no wait period between turning the **main power switch** off, then on again, the machine may not function properly.

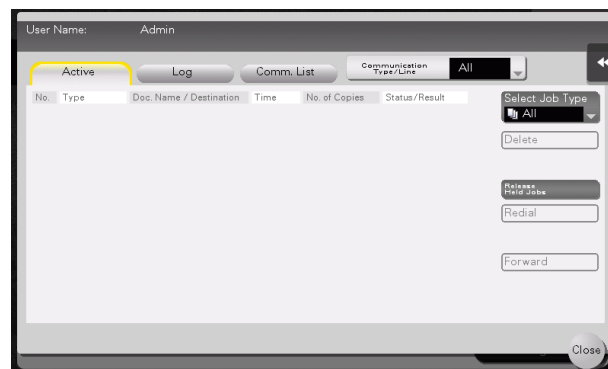
- 5 Press the **Reset** key to log off from the Administrator Mode.

<From the Control Panel as the User Administrator>

- 1 Touch [Operation Rights] to select [Administrator].



- 2 Enter the user name and the password, then touch [OK].
- 3 Touch [Login] or press the **Access** key to log in to this machine.



- 4 Touch Menu - [Utility] - [Administrator Settings].
- 5 The Administrator Mode is displayed. Perform a desired operation.
- 6 Press the **Reset** key to log off from the Administrator Mode.

<From the **Web Connection** as the Administrator of the machine>

- ✓ If you have already logged on to the Admin Mode from the control panel or using **Web Connection**, the machine displays a message that tells that another administrator has previously logged on and rejects any attempt to log on to the Admin Mode using the **Web Connection**. Click [OK] and wait for some while before attempting to access the Admin Mode once again.
- ✓ If [Export to the device] operation is being executed using the **Data Administrator**, the machine displays a message that tells you cannot log on to the mode because of the remote operation being performed and rejects any attempts to the Admin Mode via the **Web Connection**. Click [OK] and wait for some while before attempting to access the Admin Mode once again.
- ✓ Do not leave the machine with the Admin Mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin Mode.
- ✓ If you have logged on to the Admin Mode using the **Web Connection** and if you close the web browser without clicking [Logout], the control panel remains locked for 160 sec.
- ✓ Different initial screens appear after you have logged on to the Admin Mode depending on the Customize setting. The descriptions herein given are concerned with the display screen set in [Meter Counter] of Maintenance.

- 1 Start the Web browser.
- 2 Enter the IP address of the machine in the address bar.
- 3 Press the [Enter] key to start **Web Connection**.
- 4 Click the Administrator radio button and [Login].

- 5 Select the "Administrator (Admin Mode)" in the Administrator, and enter the Administrator Password in the "Password" box.

- If "Administrator (Admin Mode)" is selected, the settings for the machine system and network can be registered or changed.
- When accessing the Admin Mode using the **Web Connection**, enter the same Administrator Password as that for the machine.

6 Click [OK].

- If a wrong Administrator Password is entered, a message that tells that the authentication has failed appears. Enter the correct Administrator Password.
- If the Enhanced Security Mode is set to [ON], entry of a wrong password is counted as unauthorized access. If a wrong Administrator Password is entered a predetermined number of times (once to three times) or more set by the administrator, a message appears saying that the machine accepts no more Administrator Passwords because of unauthorized access for any subsequent entry of the Administrator Password. The machine is then set into an access lock state.
To cancel the access lock state, settings must be made by the Service Engineer; or, turn off, and then turn on, the **main power switch** of the machine. If the **main power switch** is turned off and on, the access lock state is canceled after the lapse of time set for [Release Time Settings]. When the **main power switch** is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. If there is no wait period between turning the **main power switch** off, then on again, the machine may not function properly.

7 Click [Logout].

8 Click [OK].

This allows you to log off from the Admin Mode.

<From the **Web Connection** as the User Administrator>

- 1 Start the Web browser.
- 2 Enter the IP address of the machine in the address bar.
- 3 Press the [Enter] key to start **Web Connection**.
- 4 Click the Administrator radio button and [Login].

- 5 Select "Administrator (Admin Mode)" in the Registered User and enter the user name in the "User Name" box and the user password in the "Password" box.

- If "Administrator (Admin Mode)" is selected, the settings for the machine system and network can be registered or changed.
- When accessing the Admin Mode using the **Web Connection**, enter the same User Password as that for the machine.

- 6 Click [OK].
 - If a user administrator enters a wrong User Password, a message that tells that the authentication has failed appears. Enter the correct User Password.
 - If the Enhanced Security Mode is set to [ON], the entry of a wrong User Password is counted as unauthorized access. If a wrong User Password is entered a predetermined number of times (once to three times) or more set by the administrator, a message appears saying that the machine accepts no more User Passwords because of unauthorized access for any subsequent entry of the User Password. The machine is then set into an access lock state. To cancel the access lock state, the administrator must perform the Release Setting. Contact the administrator.

- 7 Click [Logout].

- 8 Click [OK].

This allows you to log off from the User Administrator Mode.

2.1.2 Accessing the User Mode

You can log on to the User Mode as an administrator. In the User Mode, you can check or delete a job, which is disabled in Administrator Mode.

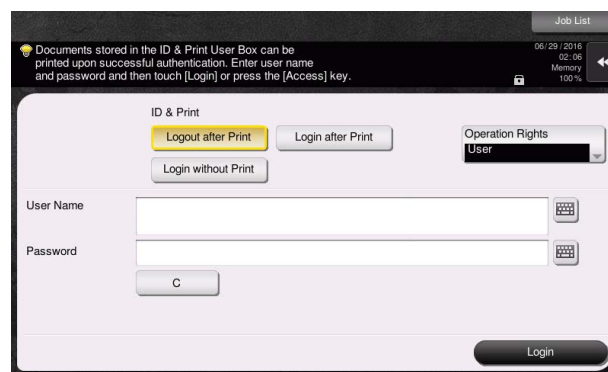
Tips

The authority relating to box settings is the same as that of Administrator Mode.

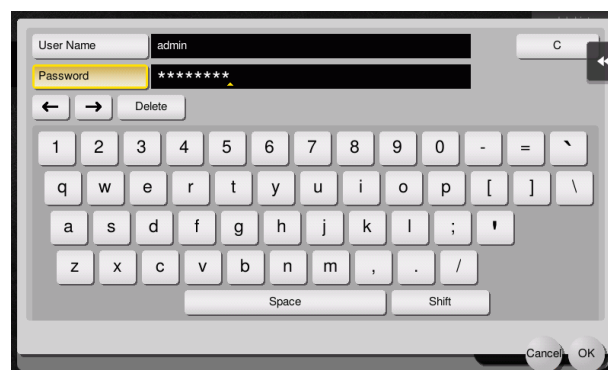
<From the Control Panel>

- ✓ The administrator must first make User Authentication settings before he or she can access User Mode. For details of the User Authentication, see page 2-27.
- ✓ Do not leave the machine with the User Mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the User Mode.

- 1 Touch the keyboard icon in the [User Name] field.



- 2 Enter "admin" in [User Name]. Enter the password set for this machine in [Password].



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

- 3 Touch [OK].

- 4 Press the **Access** key or touch [Login].
 - If a wrong Administrator Password is entered, a message that tells that the authentication has failed appears. Enter the correct Administrator Password.
 - If the Enhanced Security Mode is set to [ON], entry of a wrong password is counted as unauthorized access. If a wrong Administrator Password is entered a predetermined number of times (once to three times) or more set by the administrator, a message appears saying that the machine accepts no more Administrator Passwords because of unauthorized access for any subsequent entry of the Administrator Password. The machine is then set into an access lock state.
To cancel the access lock state, settings must be made by the Service Engineer; or, turn off, and then turn on, the **main power switch** of the machine. If the **main power switch** is turned off and on, the access lock state is canceled after the lapse of time set for [Release Time Settings]. When the **main power switch** is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. If there is no wait period between turning the **main power switch** off, then on again, the machine may not function properly.
- 5 Perform a desired operation.
 - To delete a job, touch [Job List] and select a target job, and then touch [Delete].
- 6 Press the **Access** key or touch [Close] to log off from the User Mode.

<From **Web Connection**>

- ✓ If you have already logged on to the Admin Mode from the control panel or using **Web Connection**, the machine displays a message that tells that another administrator has previously logged on and rejects any attempt to log on to the Admin Mode using the **Web Connection**. Click [OK] and wait for some while before attempting to access the Admin Mode once again.
- ✓ If [Export to the device] operation is being executed using the **Data Administrator**, the machine displays a message that tells you cannot log on to the mode because of the remote operation being performed and rejects any attempts to the Admin Mode via the **Web Connection**. Click [OK] and wait for some while before attempting to access the Admin Mode once again.
- ✓ Do not leave the machine with the Admin Mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin Mode.
- ✓ If you have logged on to the Admin Mode using the **Web Connection** and if you close the web browser without clicking [Logout], the control panel remains locked for 70 sec.
- ✓ Different initial screens appear after you have logged on to the Admin Mode depending on the Customize setting. The descriptions herein given are concerned with the display screen set in [Meter Counter] of Maintenance.

- 1 Start the Web browser.
- 2 Enter the IP address of the machine in the address bar.
- 3 Press the [Enter] key to start **Web Connection**.
- 4 Click the Administrator radio button and [Login].

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

- If "Administrator (User Mode)" is selected, you can log on to the User Mode as an Administrator. In the User Mode, you can check or delete a job, which is disabled in Administrator Mode. Note, however, that the authority relating to box settings is the same as that of Administrator Mode.
- When a user administrator accesses Administrator (User Mode) in the Registered User using **Web Connection**, enter the User Name and Password.

6 Click [OK].

- If a wrong Administrator Password is entered, a message that tells that the authentication has failed appears. Enter the correct Administrator Password.
- If the Enhanced Security Mode is set to [ON], entry of a wrong password is counted as unauthorized access. If a wrong Administrator Password is entered a predetermined number of times (once to three times) or more set by the administrator, a message appears saying that the machine accepts no more Administrator Passwords because of unauthorized access for any subsequent entry of the Administrator Password. The machine is then set into an access lock state.
To cancel the access lock state, settings must be made by the Service Engineer; or, turn off, and then turn on, the **main power switch** of the machine. If the **main power switch** is turned off and on, the access lock state is canceled after the lapse of time set for [Release Time Settings]. When the **main power switch** is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. If there is no wait period between turning the **main power switch** off, then on again, the machine may not function properly.

7 Click the [Job] tab.

8 Perform a desired operation.

9 Click [Logout].

10 Click [OK].

This allows you to log off from the User Mode.

2.2 Enhancing the Security Function

When a log-on to the Administrator Mode becomes successful, the machine enables setting of the Enhanced Security Mode that allows settings for enhancing each of different security functions to be converted all at once.

In the Enhanced Security Mode, the machine allows selection of whether to use the Enhanced Security Mode or not. If the Enhanced Security Mode is set to [ON], a count is taken of the number of unauthorized accesses to the Administrator Authentication, User Authentication, Account Track, all Secure Print, and all User Boxes. A function is also set that determines whether each password meets predetermined requirements. The security function is thus enhanced in the Enhanced Security Mode.

The following settings must first be made before the Enhanced Security Mode is set to [ON].

NOTICE

First, set the Encryption Key. To set the Encryption Key, HDD Format must first be executed. Execution of the HDD Format clears various setting values. For details of items that are cleared by HDD Format, see page 2-14.

If initialization is executed by the Service Engineer, the Password Rules are set to [Disable] and the Administrator Password is reset to the factory setting (1234567812345678). To set the Administrator Password and turn [ON] the Enhanced Security Mode again.

Settings to be Made in Advance	Description
Administrator Password	Meet the Password Rules. The factory setting is "1234567812345678."
User Authentication	Check that [Authenticate] (the server type is Active Directory only for External Server Authentication) is set.
Encryption Key	Set the Encryption Key.
Certificate for SSL	Register the self-signed certificate for SSL communications.
Service settings	Calls for setting made by the Service Engineer. For details, contact your Service Representative.

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

NOTICE

If an attempt is made to change a setting that has been changed as a result of setting the Enhanced Security Mode to [ON], a screen may appear indicating that the Enhanced Security Mode is to be canceled. Note that executing this screen will cancel the Enhanced Security Mode.

The description "not to be changed" given in parentheses in the table below indicates that the specific setting cannot be changed with the Enhanced Security Mode set to [ON].

Function Name	Factory Setting	When Enhanced Security Mode is set to [ON]
Password Rules	Disable	Enable (not to be changed) * If [Enable] is set for Password Rules, the types and number of characters to be used for each password are limited. For details of the Password Rules, see page 1-13.
Prohibited Functions When Authentication Error	Mode 1	Mode 2 (not to be changed): Three times is set. * The number of times can be changed to once, twice, or three times.
Release Time settings	5 min.	The setting value should be 5 min. or more (no value less than 5 can be set)
Confidential Document Access Method	Mode 1	Mode 2 (not to be changed) * In association with Prohibit Functions When Authentication Error, the method is changed from authentication using Secure Print ID and password (Mode 1) to that using the password with the Secure Print document first narrowed down by Secure Print ID (Mode 2).
Secure Print User Box Preview	Thumbnail View, Detail View, and Document Details are enabled	Only Detail View is enabled before password authentication (Mode 2)
Public User Access	Restrict	Restrict (not to be changed)

Function Name	Factory Setting	When Enhanced Security Mode is set to [ON]
User Name List	OFF	OFF (not to be changed)
Print Without Authentica- tion	Restrict	Restrict (not to be changed)
User Box Administrator Setting	Restrict	Restrict (not to be changed)
Mode using SSL/TLS	None	Admin. Mode and User Mode (not to be changed)
SSL Encryption Strength	AES-256, 3DES-168, RC4-128	AES/3DES (not to be changed to one containing strength lower than AES/3DES)
FTP Server	ON	OFF (not to be changed)
Print Data Capture	Allow	Restrict (not to be changed)
Network Setting Clear (Web Connection)	Enabled	Restrict
Registering and Chang- ing Address by the user (Address Book and Pro- gram)	Allow	Restrict (not to be changed)
Initialize (Network Set- tings)	Enabled	Restrict (not to be changed)
Image Log Transfer Set- tings	OFF	OFF (not to be changed)
CS Remote Care	Usable	Remote device setting disabled
Counter Remote Control	Restrict	Restrict (not to be changed)
Remote Panel Settings (Server Settings/Client Settings)	OFF	OFF (not to be changed)
Print Simple Auth. (Authentication Setting)	Restrict	Restrict (not to be changed)
External Application Connection	Yes	No (not to be changed)
E-mail RX Print	OFF	OFF (not to be changed)
Machine Update Settings	No	No (not to be changed)
IWS Settings	OFF	OFF (not to be changed)
HDD backup data Set- tings	Restrict	Restrict (not to be changed)
USB Connection Permis- sion setting	Allow	Restrict
QR Code Display Setting	OFF	OFF (not to be changed)
Enable NFC	OFF	OFF (not to be changed)
URL Home Settings	Enable	Disable

2.2.1 Items cleared by HDD Format

Following are the items that are cleared by HDD Format.

Whenever HDD Format is executed, be sure to set the Enhanced Security Mode to [ON] again.

Items of Data Cleared	Description
Enhanced Security Mode	Set to [OFF]
Device certificate (SSL certificate)	Deletes the device certificate (SSL certificate) registered in the machine
SSL encryption strength	Deletes the SSL certificate to thereby clear the SSL encryption strength
SSL-compliant protocol	Makes the protocol not complying with SSL
User Authentication	Set to [OFF]
Account Track Authentication	Set to [OFF]
User Box Administrator	Set to [Restrict]
User Name List	Set to [OFF]
Print Simple Auth.	Set to [Restrict]
Print Without Authentication	Set to [Restrict]
User registration data	Deletes all user-related data that has been registered
Account Track registration data	Deletes all account track-related data that has been registered
Box registration data/file	Deletes all User Box-related information and files saved in User Box
Secure Print ID/Password/document	Deletes all Secure Print document-related information and files saved
Destination recipient data files	Deletes all destination recipient data including e-mail addresses and telephone numbers
Audit log	Deletes the audit log

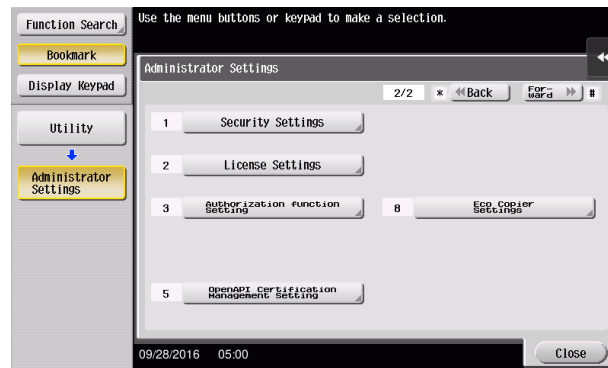
2.2.2 Setting the Password Rules

- ✓ For the procedure to call the Administrator Mode on the display, see page 2-2.
- ✓ Do not leave the machine with the setting screen of Administrator Mode left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Mode.

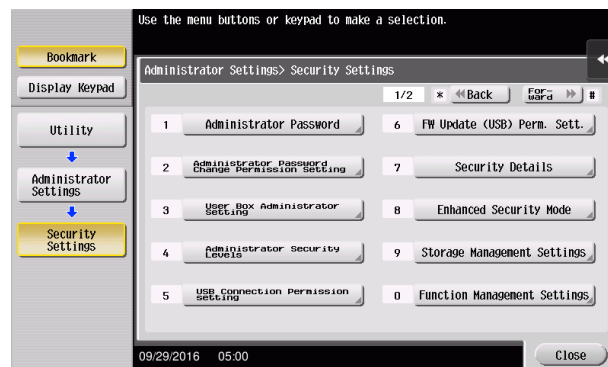
NOTICE

Before enabling the Password Rules, change the currently set password so as to meet the Password Rules. For details of the Password Rules, see page 1-13.

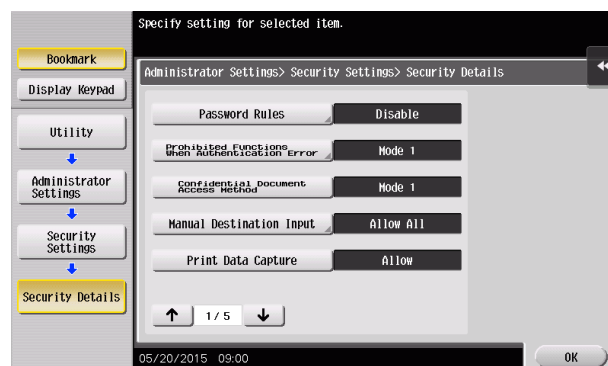
- 1 Call the Administrator Mode on the display from the control panel.
- 2 Touch [Forward].
- 3 Touch [Security Settings].



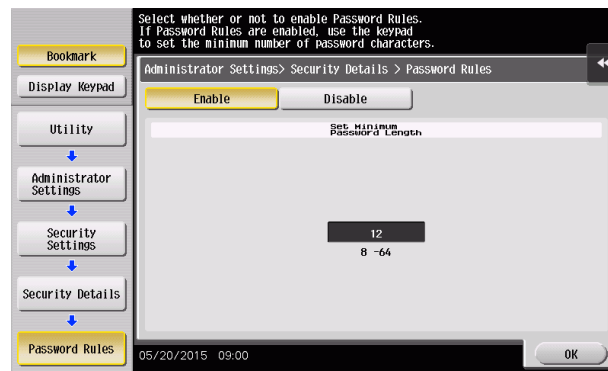
- 4 Touch [Security Details].



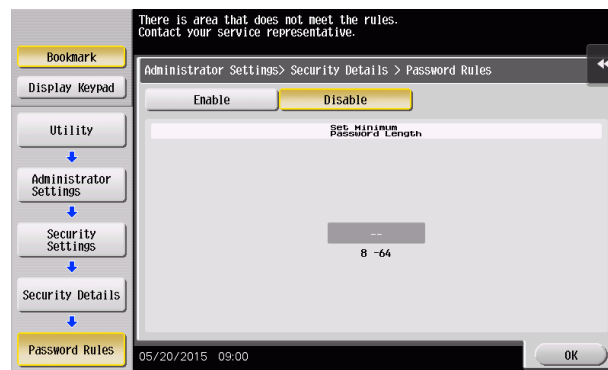
- 5 Touch [Password Rules].



- 6 Select [Enable] and set [Set Minimum Password Length] (8 to 64 characters).



- The following screen appears if the previously required settings are yet to be made by the Service Engineer. Contact your Service Representative.

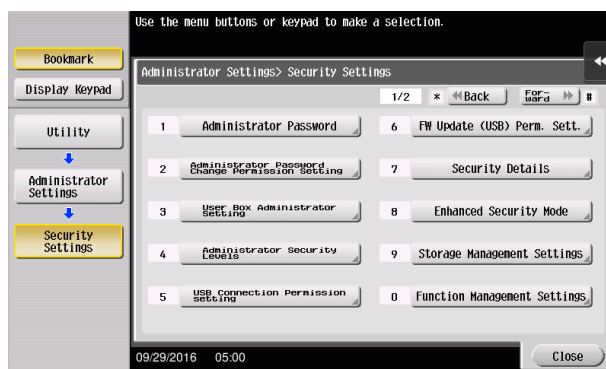


- 7 Touch [OK].

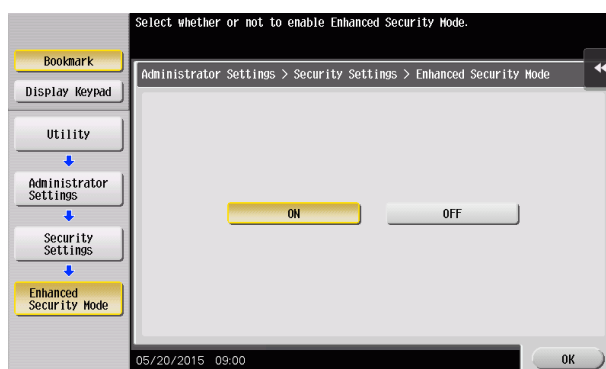
2.2.3 Setting the Enhanced Security Mode

- ✓ For the procedure to call the Security Settings screen on the display, see steps 1 through 3 of page 2-15.
- ✓ Do not leave the machine with the setting screen of Administrator Mode left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Mode.
- ✓ The Enhanced Security Mode is factory-set to [OFF]. Be sure to turn [ON] the Enhanced Security Mode so as to enable the security function of the machine.

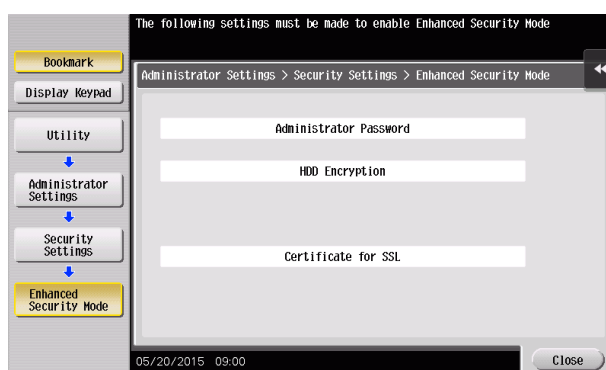
- 1 Call the Security Settings screen on the display from the control panel.
- 2 Touch [Enhanced Security Mode].



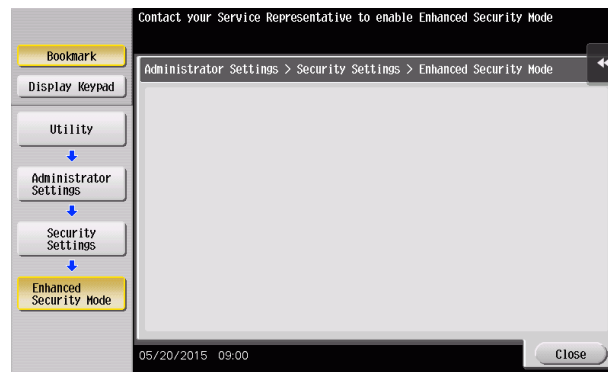
- 3 Select [ON] to enable the Enhanced Security Mode and touch [OK].



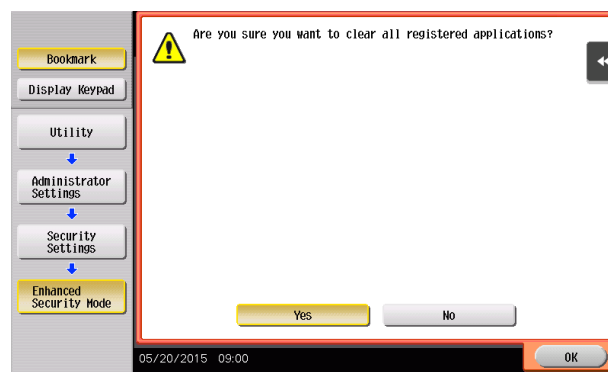
→ The following screen appears if the previously required settings are yet to be made by the administrator. Make the necessary settings according to the corresponding set procedure.



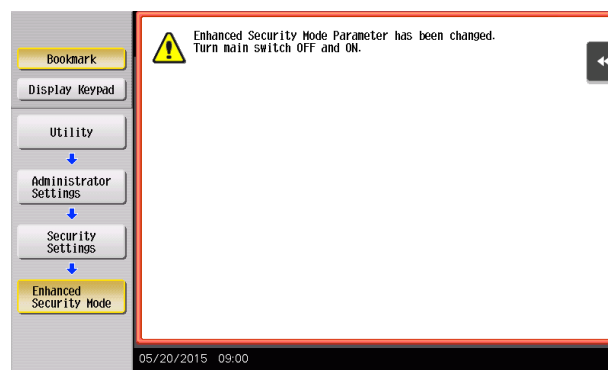
- The following screen appears if the previously required settings are yet to be made by the Service Engineer. Contact your Service Representative.



- 4 Any external applications registered using OpenAPI will be deleted when the Enhanced Security Mode is set to [ON]. A confirmation message appears. Select [Yes] and touch [OK].

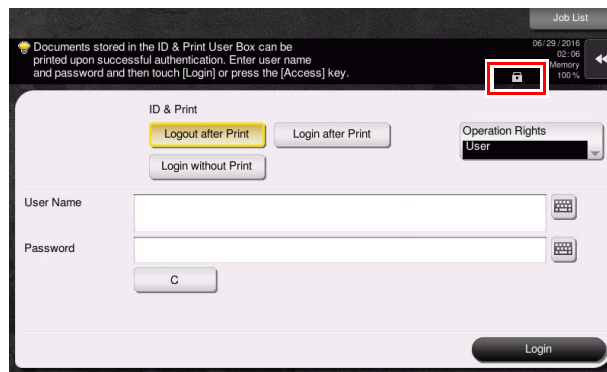


- 5 Make sure that a message appears prompting you to turn OFF and then ON the **main power switch**. Now, turn OFF and then turn ON the **main power switch**.



- When the **main power switch** is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. If there is no wait period between turning the **main power switch** off, then on again, the machine may not function properly.

- If the Enhanced Security Mode is properly set to [ON], a key icon appears at the portion on the screen enclosed by a red frame, indicating that the machine is in the Enhanced Security Mode.



2.3 Protecting Machine from Illegal Firmware Update

When a log-on to the Administrator Mode becomes successful, this machine enables the operation of setting or changing the password required to update the firmware, which is performed by a service engineer using a USB memory.

By setting the FW Update (USB) Password, the firmware of the machine can be protected from illegal update. The FW Update (USB) Password entered is displayed as "*"."

NOTICE

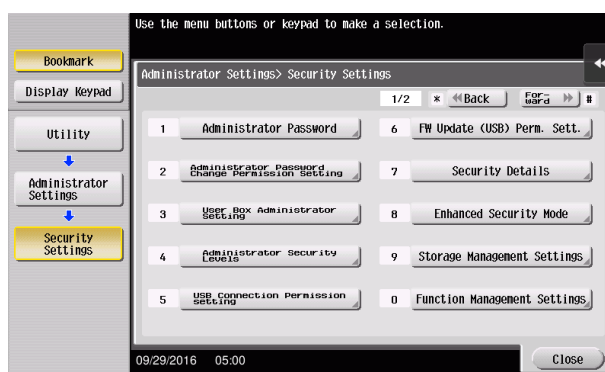
The following shows setting conditions for the FW Update (USB) Password. Perform settings for the FW Update (USB) Password fitting these conditions.

Types of passwords	Number of characters	Types of characters	Conditions for setting/changes
FW Update (USB) Password	0 to 20 characters	<ul style="list-style-type: none"> Numeric characters: 0 to 9 Alpha characters: upper and lower case letters Symbols: !, #, \$, %, &, ', (,), *, ,, -, ., /, :, ;, <, =, >, ?, @, [\,], ^, _ ` , {, , }, ~, + Selectable from among a total of 93 characters	A new password needs to be re-entered.

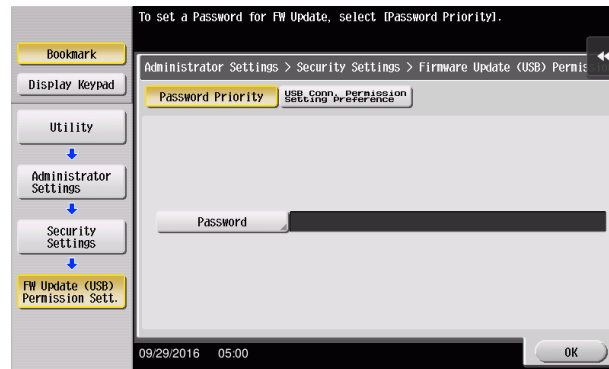
Setting the FW Update (USB) Password

<From the Control Panel>

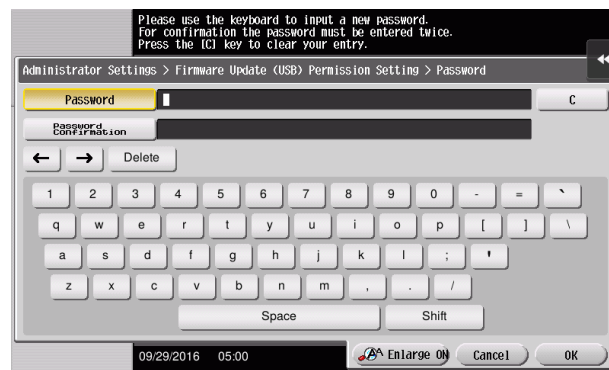
- ✓ For the procedure to call the Security Settings screen on the display, see steps 1 through 3 of page 2-15.
 - ✓ Do not leave the machine with the setting screen of Administrator Mode left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Mode.
- 1 Call the Security Settings screen on the display from the control panel.
 - 2 Touch [FW Update (USB) Perm. Sett.].



3 Touch [Password Priority].



4 Enter the new FW Update (USB) Password from the keyboard. To prevent entry of a wrong password, enter the password again in [Password Confirmation].



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

5 Touch [OK].

- If the entered FW Update (USB) Password does not meet the Password Rules, a message that tells that the entered FW Update (USB) Password cannot be used appears. Enter the correct FW Update (USB) Password. For details of the Password Rules, see page 1-13.

<From **Web Connection**>

- ✓ For the procedure to access the Admin Mode, see page 2-2.
- ✓ Do not leave the machine with the Admin Mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin Mode.

- 1 Start **Web Connection** and access the Admin Mode.
- 2 Click the [Security] tab.
- 3 In the menu, set [USB Update] to [Password Priority] in [FW Update (USB) Permission Setting].
- 4 Select the "Password is changed" check box.
Enter the new FW Update (USB) Password. Then, to make sure that you have entered the correct new password, enter the new FW Update (USB) Password once again.

The screenshot shows the Admin Mode web interface. At the top, there's a header with 'Administrator', a 'Logout' button, and a help icon. Below the header, there are status indicators: 'Ready to Scan' and 'Ready to Print'. A navigation bar contains tabs: 'Maintenance', 'System Settings', 'Security' (selected), 'User Auth/Account Track', 'Network', and 'Box'. Below this is a secondary bar with 'Print Setting', 'Store Address', 'Fax Settings', 'Wizard', 'Customize', and 'To Main Menu'. The left sidebar lists various settings categories, with 'FW Update (USB) Permission Setting' selected. The main content area is titled 'FW Update (USB) Permission Setting' and contains a 'USB Update' dropdown menu set to 'Password Priority'. Below this is a checkbox labeled 'Password is changed.' which is checked. There are two text input fields: 'Password' and 'Retype Password'. At the bottom right of the form are 'OK' and 'Cancel' buttons.

- 5 Click [OK].
 - ➔ If the entered FW Update (USB) Password in the [Password] box does not meet the Password Rules, a message that tells that the entered FW Update (USB) Password cannot be used appears. Enter the correct FW Update (USB) Password. For details of the Password Rules, see page 1-13.

2.4 Preventing Unauthorized Access

When a log-on to the Administrator Mode becomes successful, the machine enables setting of the operation of Prohibited Functions When Authentication Error. The machine takes a count of the cumulative number of unsuccessful accesses from each interface to the Administrator Authentication, User Authentication, Account Track, Secure Print authentication, and User Box authentication to prohibit the authentication operation.

Either [Mode 1] or [Mode 2] can be selected for Prohibited Functions When Authentication Error. The factory setting is [Mode 1]. If the Enhanced Security Mode is set to [ON], the setting is changed to [Mode 2] (check count: three times). It is nonetheless possible to change the check count to select from among once, twice, or three times.

If [Mode 2] is selected, the Release Time Settings function is enabled. When the Administrator Authentication is set into the access lock state, the **main power switch** is turned off and on and, after the lapse of a predetermined period of time after the machine is turned on again, the access lock state of the Administrator Authentication is canceled. The Release Time Settings function allows the period of time, after the lapse of which the access lock state of the Administrator Authentication is canceled, to be set in the range between 1 and 60 min. The factory setting is 5 min. For details of each mode, see the table below.

Mode	Description
Mode 1	If authentication fails, the authentication operation (entry of the password) is prohibited for 5 sec.
Mode 2	If authentication fails, the authentication operation (entry of the password) is prohibited for 5 sec. The number of times, in which authentication fails, is also counted and, when the failure count reaches a predetermined value, the authentication operation is prohibited and the machine is set into an access lock state.

NOTICE

For details of boxes subject to the User Box authentication, see page 1-17.

If the access lock state of the Administrator Authentication is canceled by the Service Engineer, the setting of the Release Time Settings function is not applied.

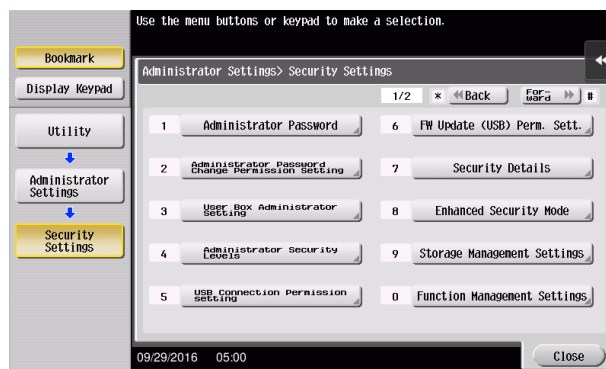
Making any of the following settings when the Enhanced Security Mode is set to [ON] will cancel the Enhanced Security Mode.

- Changing [Prohibited Functions When Authentication Error] to [Mode 1]
- Changing the check count for [Prohibited Functions When Authentication Error] to four times or more
- Setting [Release Time Settings] to 1 to 4 min.

Setting Prohibited Functions When Authentication Error

- ✓ For the procedure to call the Security Settings screen on the display, see steps 1 through 3 of page 2-15.
- ✓ Do not leave the machine with the setting screen of Administrator Mode left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Mode.

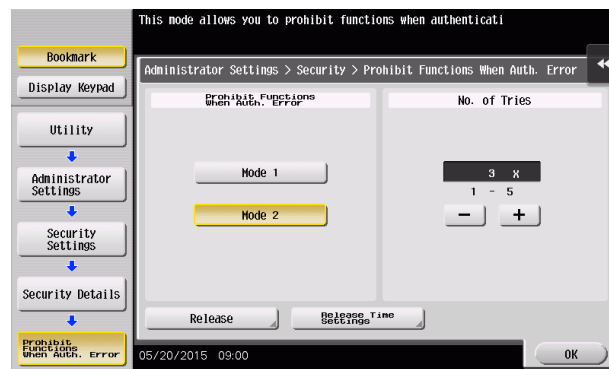
- 1 Call the Security Settings screen on the display from the control panel.
- 2 Touch [Security Details].



3 Touch [Prohibited Functions When Authentication Error].



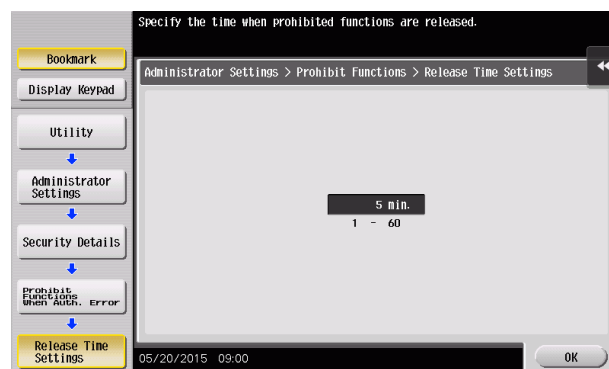
4 Touch [Mode 2].



- Select [Mode 2] when the Enhanced Security Mode is set to [ON]. Selecting [Mode 1] will cancel the Enhanced Security Mode.
- Set three times or less when the Enhanced Security Mode is set to [ON]. Setting four times or more will cancel the Enhanced Security Mode.
- To change the check count, touch [+] to increase the count or [-] to decrease it.

5 Touch [Release Time Settings].

6 Touch [C] and, from the keypad, enter the time, after the lapse of which the access lock state of the Administrator Authentication is canceled.



- Touch [Display Keypad] to display the keypad.
- Release Time can be set to any value between 1 min. and 60 min. in 1-min. increments. An input data error message appears when any value falling outside the range of 1 to 60 min. is set. Enter the correct Release Time.
- Set 5 min. or more when the Enhanced Security Mode is set to [ON]. Setting 1 to 4 min. will cancel the Enhanced Security Mode.

7 Touch [OK].

2.5 Canceling the Operation Prohibited State

When a log-on to the Administrator Mode becomes successful, the machine enables the operation of Release Setting performed for canceling the state of Prohibited Functions When Authentication Error (access lock state) as a result of unauthorized access.

Release Setting clears the unauthorized access check count for all User Authentication, Account Track, all Secure Print authentication, and all User Box authentication, resetting it to zero and canceling the operation prohibited state. Perform the following procedure to cancel the operation prohibited state.

Operation Prohibited State	Canceling procedure
Administrator Authentication	The operation prohibited state is canceled after the main power switch is turned off and on and the period of time set in [Release Time Settings] elapses.
User/Account authentication	The Administrator touches [Release] to cancel the operation prohibited state.
Secure Print authentication	
User Box authentication	

NOTICE

For details of boxes subject to the User Box authentication, see page 1-17.

Never allow any general user to know the Administrator Password.

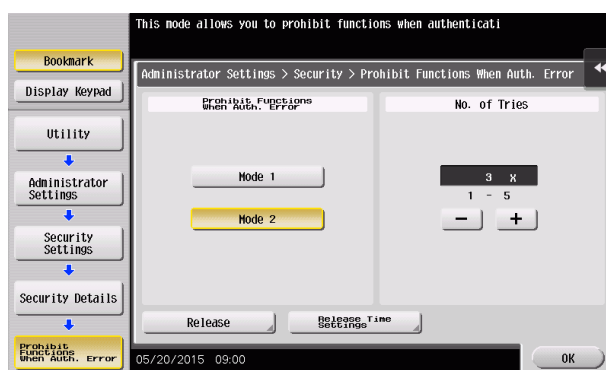
Forgetting the Administrator Password requires that a setting be made by the service engineer. Call your Service Representative.

It is also possible for the service engineer to cancel the state of Prohibited Functions When Authentication Error (access lock state) of the Administrator Authentication. Contact your Service Representative.

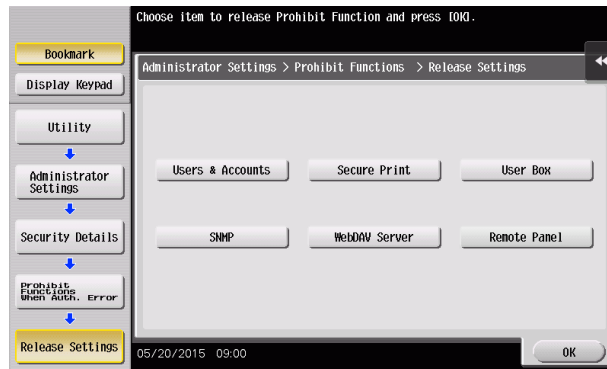
Performing Release Setting

- ✓ For the procedure to call the Prohibited Functions When Authentication Error screen on the display, see steps 1 through 3 of page 2-23.
- ✓ Do not leave the machine with the setting screen of Administrator Mode left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Mode.
- ✓ When the **main power switch** is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. If there is no wait period between turning the **main power switch** off, then on again, the machine may not function properly.

- 1 Call the Prohibited Functions When Authentication Error screen on the display from the control panel.
- 2 Touch [Release].



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



→ The Remote Panel function cannot be used when the Enhanced Security Mode is set to [ON].

- 4 Touch [OK].

This clears the unauthorized access check count of the specific function selected in step 4 and cancels the operation prohibited state.

2.6 Setting the Authentication Method

When a log-on to the Administrator Mode becomes successful, the machine enables setting of the authentication method for User Authentication and for Account Track.

The following three types of authentication methods available for User Authentication.

Mode	Description
[ON (MFP)]	The authentication function of this machine is used for user authentication.
[External Server Authentication] (Active Directory only)	Interacts with the authentication server used for user authentication in the operating environment.
[Main + External Server] (Active Directory only)	The authentication function of the machine may also be used, in consideration of a possible problem occurring in the external authentication server.



Related setting (for the administrator)

The Account Track authentication method may be set to [ON] or [OFF]. If [ON] is selected, be sure to set "Synchronize" in "Synchronize User Authentication & Account Track".

NOTICE

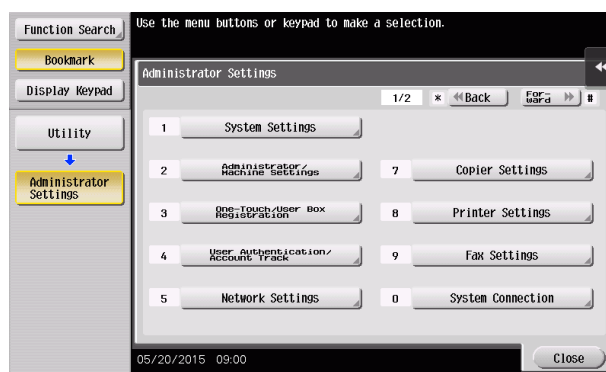
Changing the Account Track setting erases all user and account information data that has previously been registered. At this time, Personal User Boxes owned by the users who are deleted and Group User Boxes owned by the accounts that are deleted may be deleted or changed to Public User Boxes. If the boxes are changed to Public User Boxes and if the password set for a particular box before this change does not meet the Password Rules, no access can be made to the Public User Box, to which that specific box was changed. In this case, the administrator must first newly set a password that meets the Password Rules. For details of the Password Rules, see page 1-13.

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

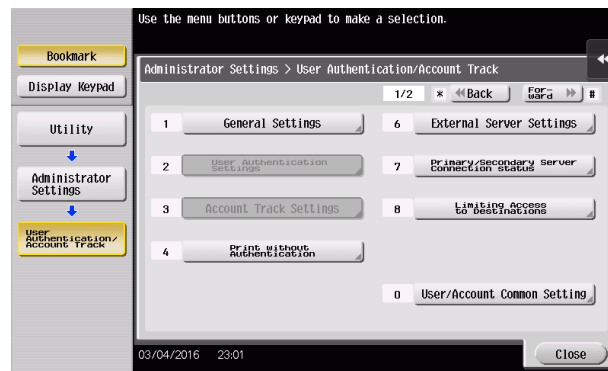
2.6.1 Setting the Authentication Method

- ✓ For the procedure to call the Administrator Mode on the display, see page 2-2.
- ✓ Do not leave the machine with the setting screen of Administrator Mode left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Mode.

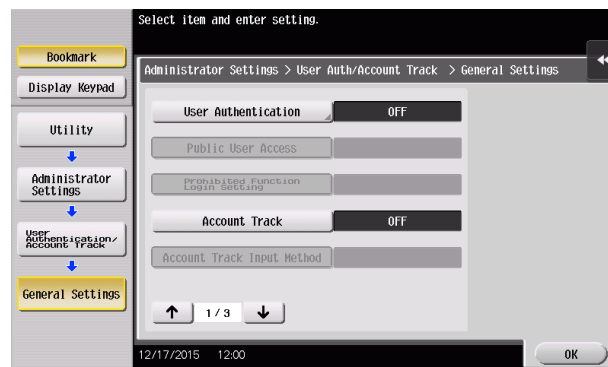
- 1 Call the Administrator Mode on the display from the control panel.
- 2 Touch [User Authentication/Account Track].



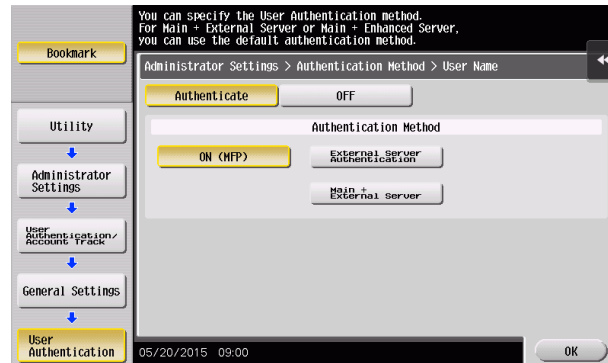
- 3 Touch [General Settings].



- 4 Touch [User Authentication].



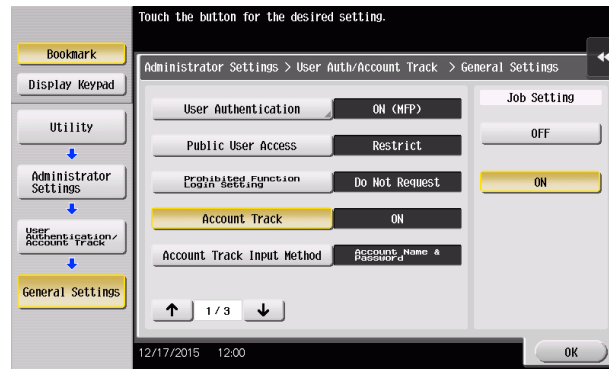
- 5 Select [Authenticate] and then select the authentication method.



→ To use the External Server, the External Server must be registered in advance. For how to make the External Server Settings, see page 2-30.

- 6 Touch [OK].

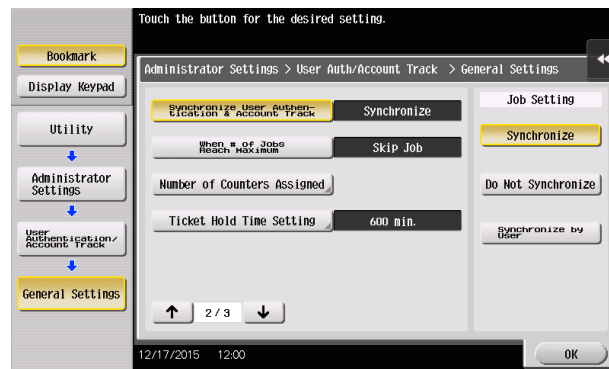
- 7 Select [Account Track] and touch [ON].



→ If the Account Track is not to be used, go to step 10.

- 8 Touch [↓].

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



- 10 Touch [OK].

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

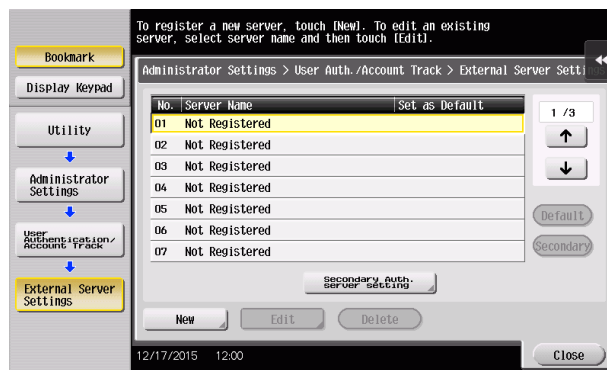
2.6.2 Setting the External Server

- ✓ If [External Server Authentication] is selected for the authentication method, the External Server must be registered in the machine in advance.
- ✓ For the procedure to call the User Authentication/Account Track screen on the display, see steps 1 and 2 of page 2-27.
- ✓ Do not leave the machine with the setting screen of Administrator Mode left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Mode.

NOTICE

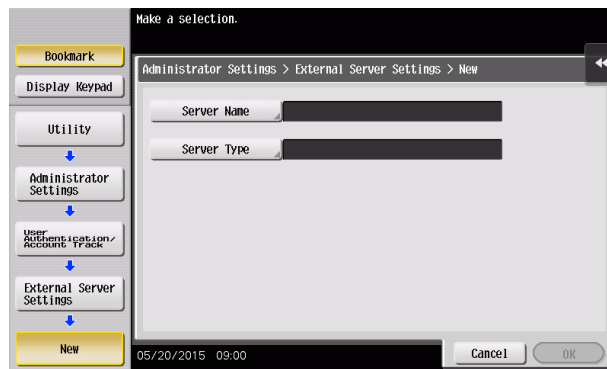
For the Kerberos protocol of the Active Directory, specify AES-128 or AES-256 instead of DES as the encryption level on the server settings.

- 1 Call the User Authentication/Account Track screen on the display from the control panel.
- 2 Touch [External Sever Settings].
- 3 Touch the specific Sever Registration key, in which no sever has been registered.
- 4 Touch [New].

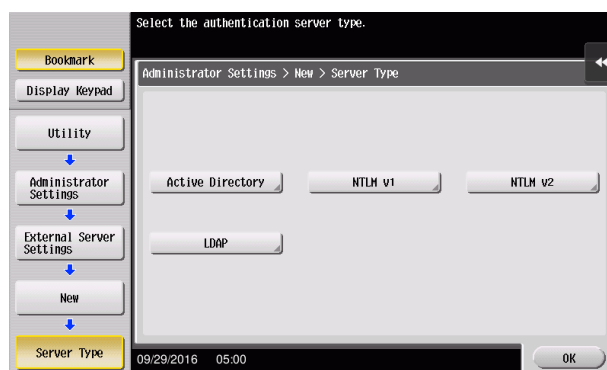


→ To change or delete a previously registered server, touch [Edit] or [Delete].

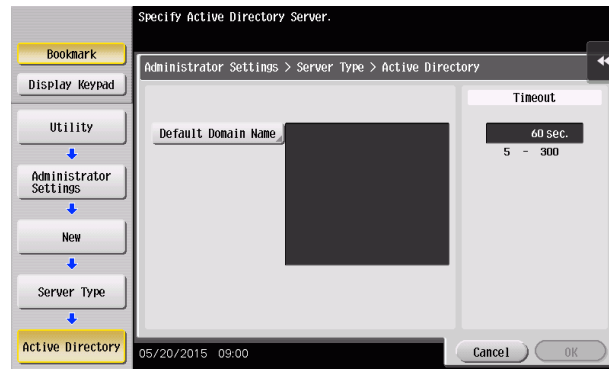
- 5 Touch [Server Type].



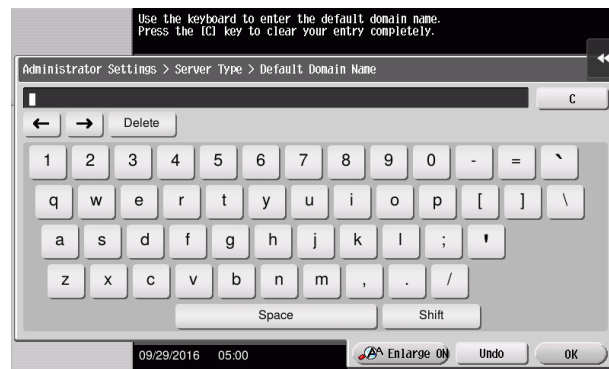
- 6 Touch [Active Directory].



- 7 Touch [Default Domain Name].



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



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

- 9 Touch [OK].

- 10 Make the necessary settings.

- If the Sever Name is yet to be entered, [OK] cannot be touched. Be sure to enter the Sever Name.
- A Sever Name that already exists cannot be redundantly registered.

- 11 Touch [OK].

- 12 Touch [Close].

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

2.7 ID & Print Setting Function

When a log-on to the Administrator Mode becomes successful, the machine enables setting of the operation of the ID & Print Setting function.

ID & Print is a function to authenticate a user using a user name and password, then automatically print the print jobs saved in the ID & Print User Box of this machine, when user authentication is enabled.

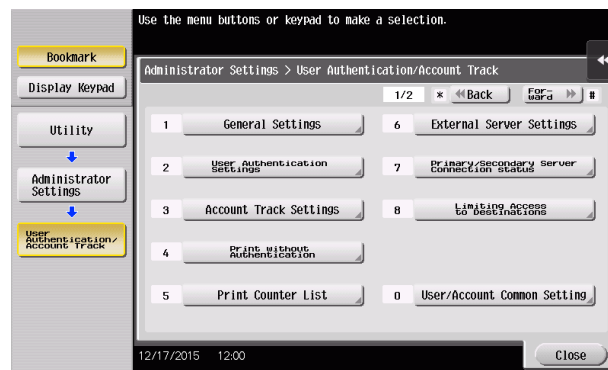
Related setting (for the administrator)

The administrator must first make User Authentication settings before setting the ID & Print. For details of the User Authentication, see page 2-27.

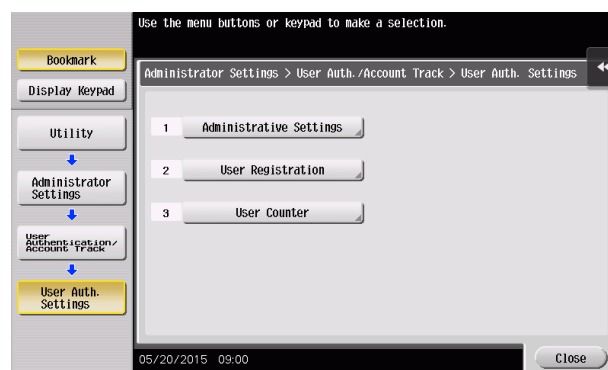
Setting ID & Print

- ✓ For the procedure to call the User Authentication/Account Track screen on the display, see steps 1 and 2 of page 2-27.
- ✓ Do not leave the machine with the setting screen of Administrator Mode left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Mode.

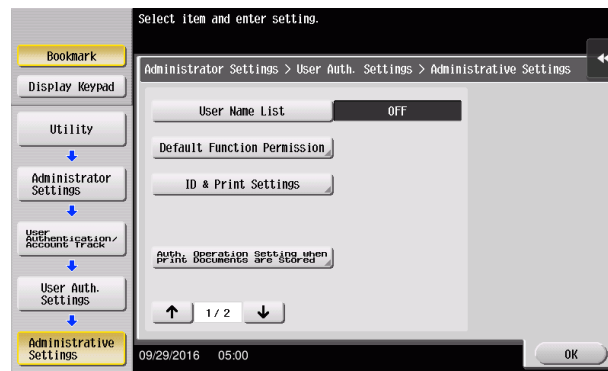
- 1 Call the User Authentication/Account Track screen on the display from the control panel.
- 2 Touch [User Authentication Settings].



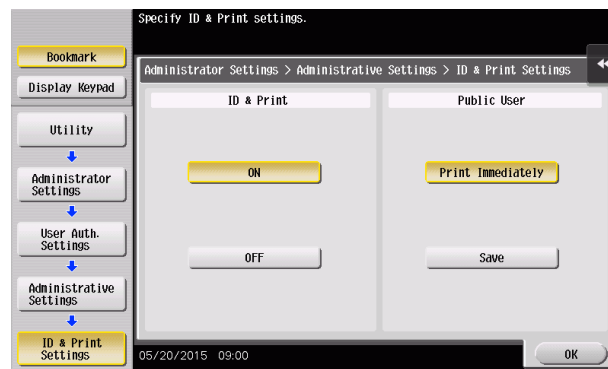
- 3 Touch [Administrative Settings].



4 Touch [ID & Print Settings].



5 Select [ON].



6 Touch [OK].

- If [ON] is set, the document is stored as ID & Print document even if [Print] is selected on the printer driver side.
- Even if [OFF] is set, the document is stored as ID & Print document if [ID & Print] is selected on the printer driver side.

2.8 ID & Print Operation Setting Function

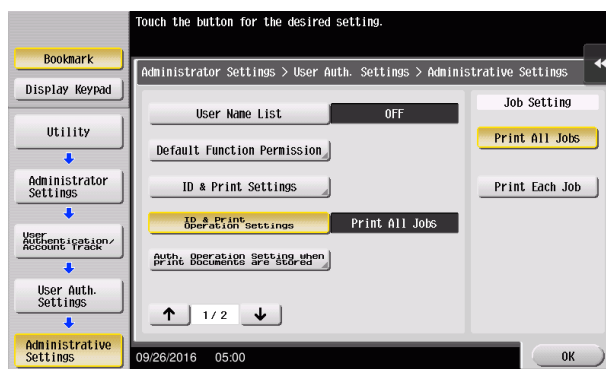
When a log-on to the Administrator Mode becomes successful, the machine enables setting of the operation of the ID & Print Operation Setting function.

ID & Print operation setting function is a function to set by a single authentication whether to print all jobs or to print one of jobs.

Making ID & Print Operation Setting

- ✓ For the procedure to call the Administrative Settings screen on the display, see steps 1 through 3 of page 2-32.
- ✓ Do not leave the machine with the setting screen of Administrator Mode left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Mode.

- 1 Call the Administrative Settings screen on the display from the control panel.
- 2 Touch [ID & Print Operation Settings].



- 3 Make the necessary settings.
- 4 Touch [OK].

2.9 Auth. Operation Setting when print Documents are Stored Function

When a log-on to the Administrator Mode becomes successful, the machine enables setting of the operation of the Auth. Operation Setting when print Documents are Stored Function.

Auth. Operation Setting when print Documents are Stored Function is a function to set the default value for the operation when authentication is performed on the login page with ID & Print jobs stored.

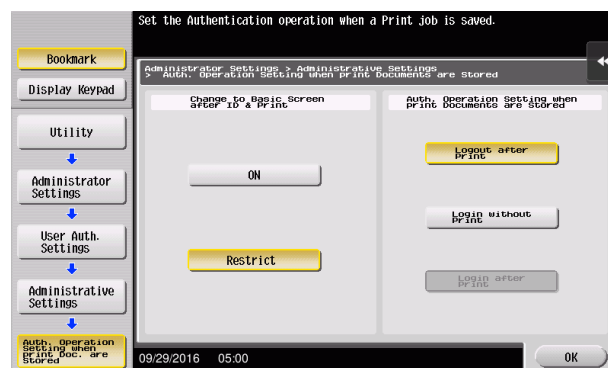
Setting Auth. Operation Setting when print Documents are Stored Function

- ✓ For the procedure to call the Administrative Settings screen on the display, see steps 1 through 3 of page 2-32.
- ✓ Do not leave the machine with the setting screen of Administrator Mode left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Mode.

- 1 Call the Administrative Settings screen on the display from the control panel.
- 2 Touch [Auth. Operation Setting when print Documents are Stored].



- 3 Make the necessary settings.



- 4 Touch [OK].

2.10 System Auto Reset Function

When a log-on to the Administrator Mode becomes successful, the machine enables setting of the operation of the System Auto Reset function.

If no operations are performed for a predetermined period of time during access to the Administrator Mode or user mode (during setting of User Authentication) from the control panel, the System Auto Reset function automatically causes the user to log off from the mode.

The predetermined period of time, after which the System Auto Reset function is activated, can be selected from among nine values between 1 min. and 9 min. System Auto Reset can also be set to [OFF]. If no operations are performed for 1 min. even with System Auto Reset set to [OFF], the function causes the user to log off from the mode automatically.



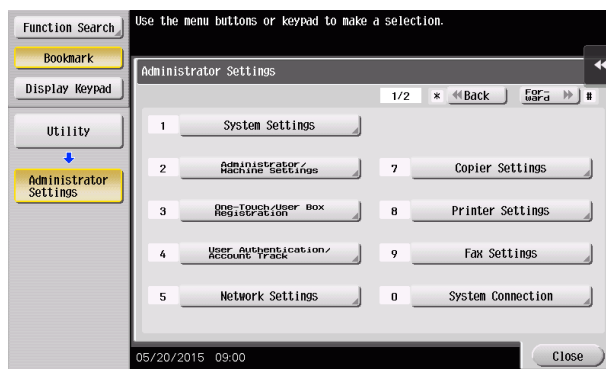
Tips

Processing of a specific job, however, takes precedence over the System Auto Reset function. That is, even if a predetermined period of time elapses during which no operations are performed, once the processing of the specific job has been started, the System Auto Reset function does not cause the user to log off from the mode. The user logs off from the mode after the lapse of a predetermined period of time after the processing of the specific job is completed.

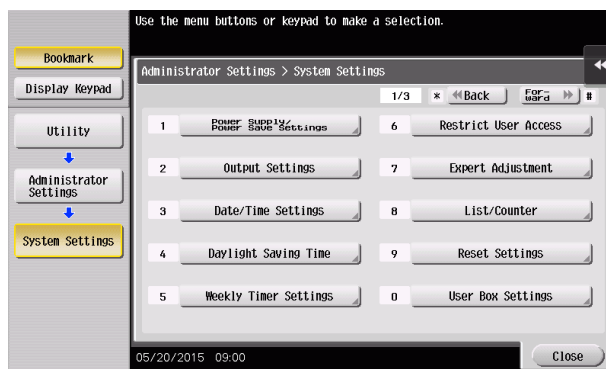
Setting the System Auto Reset function

- ✓ For the procedure to call the Administrator Mode on the display, see page 2-2.
- ✓ Do not leave the machine with the setting screen of Administrator Mode left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Mode.

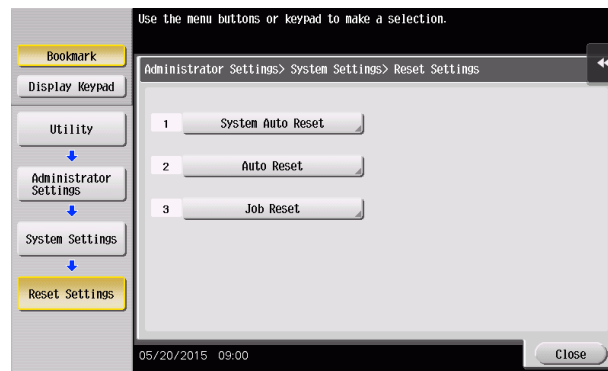
- 1 Call the Administrator Mode on the display from the control panel.
- 2 Touch [System Settings].



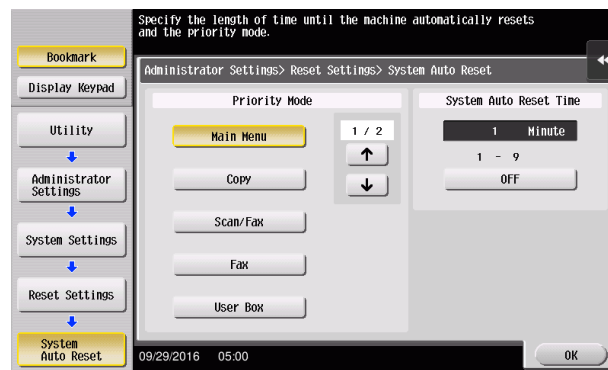
- 3 Touch [Reset Settings].



4 Touch [System Auto Reset].



5 Touch [C] and enter the period of time (1 min. to 9 min.) after which System Auto Reset is activated from the keypad.



- Touch [Display Keypad] to display the keypad.
- The time for System Auto Reset can be set to a value between 1 min. and 9 min., variable in 1-min. increments. An input data error message appears when any value falling outside the range of 1 to 9 min. is set. Enter the correct System Auto Reset Time.
- If no operations are performed for 1 min. even with System Auto Reset set to [OFF], the function is activated to cause the user to log off from the mode automatically.
- Touch [C] to clear all characters.

6 Touch [OK].

2.11 User Setting Function

When a log-on to the Administrator Mode becomes successful, the machine enables registration of the user who can use the machine. Also, the machine enables the operations of giving the administrative right to a user, deleting a user, and changing a user password. The user administrator can access the Administrator Mode.

In **Web Connection**, import/export of the user registration information is enabled, allowing the backup data of the user registration information to be saved or the saved backup data to be restored.

User Registration allows the User Name, User Password, and other user information to be registered for enabling access to, or operation of, the machine. Up to 1,000 different users can be registered. User Registration allows identification and authentication of each individual user, thereby preventing unauthorized use of the machine. The User Password is controlled based on passwords that meets the Password Rules and the password entered is displayed as "*" or "●."

Tips

- If [External Server Authentication] (Active Directory) is set for the authentication method, it is not possible to make user registration or change a User Password from the control panel. To register or change a user, make the settings on the server side. If **Data Administrator** is used for registering user information, however, the user name must match that registered in the External Server. Further, a User Password can be set, but is not to be used for authentication.
- If [External Server Authentication] (Active Directory) is set for the authentication method and if a user not registered with this machine is authenticated through user authentication, that particular user name is automatically registered in the machine.
- If [External Server Authentication] (Active Directory) is set for the authentication method and if a user registered with this machine is authenticated through user authentication, that particular user name, along with the External Server name, is automatically registered in the machine. No two User Names registered in an External Server may be alike.
- If the user authentication method is changed between [ON (MFP)] and [External Server Authentication], the user information registered under the previous authentication method cannot be used under the new authentication method.
- If [External Server Authentication] is set for the authentication method, a log-on attempt made successfully by a user who has been registered in the external server causes a predetermined default authority to be given to this particular user. Make the individual authority setting thereafter. Once the individual authority setting has been made, that individual authority setting is valid and assigned to the user each successful log-on attempt made by the user.
- If the user authentication method is to be changed, be sure first to delete all user information used under the old authentication method and then change the user authentication method as necessary.
When a registered user is deleted, the Personal User Box owned by the user who has been deleted can be deleted or changed to a Public User Box. Deleting a user also delete documents stored in ID & Print and Password Encrypted PDF boxes for the user.
If the boxes are changed to Public User Boxes and if the password set for a particular box before this change does not meet the Password Rules, no access can be made to the Public User Box, to which that specific box was changed. In this case, the administrator must first newly set a password that meets the Password Rules. For details of the Password Rules, see page 1-13.
- If [ON (MFP)] is set for the authentication method, a specific registered user may be temporarily suspended from using the machine or a suspended user may be allowed to use the machine again. While a user is suspended from using the machine, he or she cannot log onto the machine.



Related setting (for the administrator)

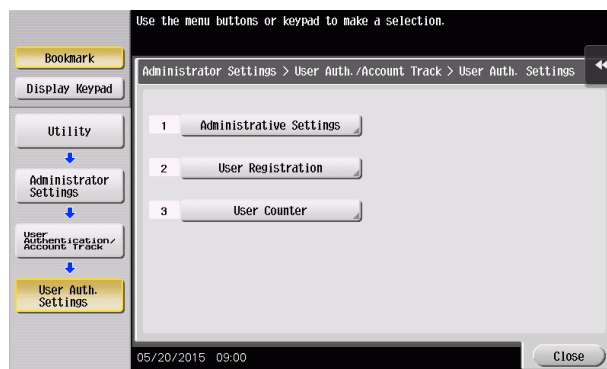
If synchronization with Account Track has been set, the account should be registered in advance. For how to make the Account Track Registration, see page 2-44.

Making user setting

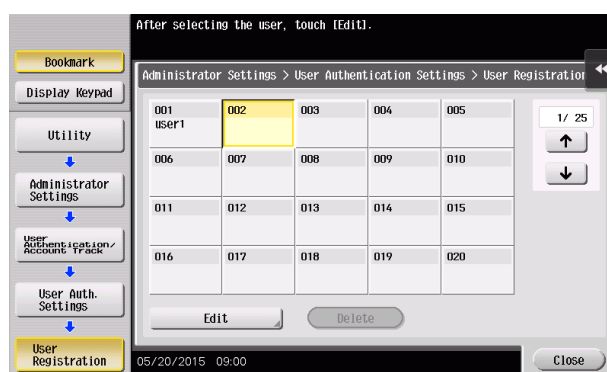
<From the Control Panel>

- ✓ For the procedure to call the User Authentication Settings screen on the display, see steps 1 and 2 of page 2-32.
- ✓ Do not leave the machine with the setting screen of Administrator Mode left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Mode.

- 1 Call the User Authentication Settings screen on the display from the control panel.
- 2 Touch [User Registration].



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



- To change settings for a registered user, select the registered user in question and touch [Edit].
- To delete a registered user, select the registered user in question and touch [Delete]. The following screen appears if the user to be deleted owns a Personal User Box. Select whether to delete the Personal User Box or change it to the Public User Box.

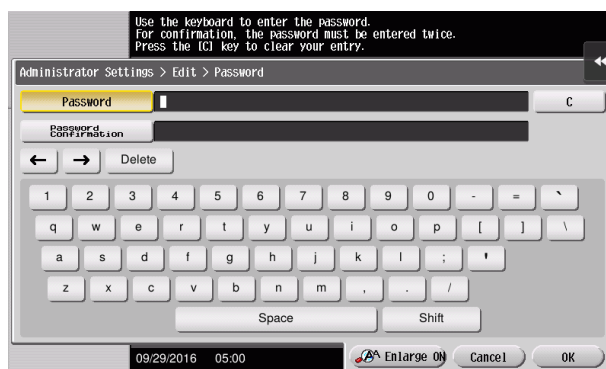


- If the boxes are changed to Public User Boxes and if the password set for a particular box before this change does not meet the Password Rules, no access can be made to the Public User Box, to which that specific box was changed. In this case, the administrator must first newly set a password that meets the Password Rules. For details of the Password Rules, see page 1-13.

4 Touch [Password].



- 5 From the keyboard, enter a new User Password.
To prevent entry of a wrong password, enter the password again in [Password Confirmation].



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

6 Touch [OK].

- If the entered User Password does not meet the Password Rules, a message that tells that the entered User Password cannot be used appears. Enter the correct User Password. For details of the Password Rules, see page 1-13.
- If the entered User Password does not match, a message that tells that the User Password does not match appears. Enter the correct User Password.

7 Touch [Account Name].

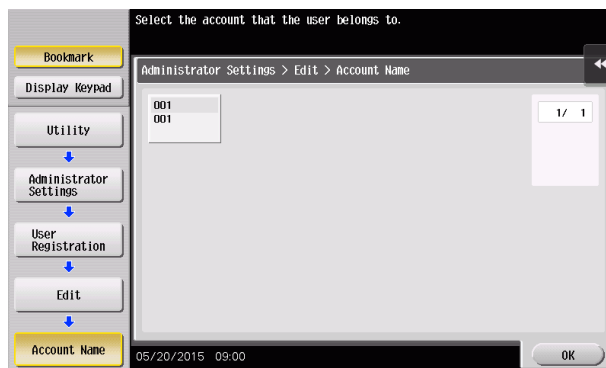


- If Account Name is not registered, Account Track becomes necessary even with [Synchronize] set for [Synchronize User Authentication & Account Track]. Account Track is, however, necessary only for the first time. Once any account is authenticated, that particular account is registered for Account Name. The machine can thereafter be used only through User Authentication.

It should be noted that this function is valid only through operation from the control panel of the machine. In operation from **Web Connection** or application software, if Account Name is not registered, you cannot log onto the mode.

- [Account Name] does not appear, if Account Track has not been set for the authentication method or any option other than [Synchronize] has been selected for [Synchronize User Authentication & Account Track].

8 Select the desired account.



9 Touch [OK].

10 Make the necessary settings.

- If the User Name is yet to be entered, [OK] cannot be touched. Be sure to enter the User Name.
- When a double quotation mark (") is used in the User Name and a print or save operation is performed using the ID & Print or Secure Print function, a log-in error occurs in the machine and the print job is discarded. It is recommended that the double quotation mark (") not be used in the User Name.
- A User Name that already exists cannot be redundantly registered.
- To suspend temporarily a registered user from using the machine, touch [Pause] and select [Stop Job]. If the account to which the user belongs is temporarily suspended from using the machine, however, selecting [Continue Job] does not allow the user to use the machine.
- To restrict the functions the user can use, use [Function Permission] and set Allow or Restrict for each function. Setting [All Users] applies the same [Function Permission] to all users.
- If [Copy] is restricted by the Function Permission setting, the copy function cannot be used.
- If [Scan] is restricted by the Function Permission setting, the transmission function cannot be used or a document in the Memory RX Box cannot be downloaded.
- If [Fax] is restricted by the Function Permission setting, the fax function cannot be used.
- If [Print] is restricted by the Function Permission setting, a document cannot be registered from the printer driver or **Web Connection** in the box or a document previously registered in the box cannot be printed.
- If [Print] is restricted by the Function Permission setting, a document in the Password Encrypted PDF box cannot be printed or a document cannot be saved in the Password Encrypted PDF box.
- If [User Box] is restricted by the Function Permission setting, a document cannot be registered in the Annotation Box or Secure Print Box, or a document in the Annotation Box or Secure Print Box cannot be operated.
- If [Print Scan/Fax TX] is restricted by the Function Permission setting, a document in the Annotation Box cannot be printed or simultaneous printing available from the transmission function cannot be used.
- To give the administrative right to a user, select [Allow] in [Function Permission/Authority] - [Permission Setting] - [Administrative Rights]. Deletion of the administrative right of a user is reflected after the user is logged out.

11 Touch [OK].

<From **Web Connection**>

- ✓ For the procedure to access the Admin Mode, see page 2-2.
- ✓ Do not leave the machine with the Admin Mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin Mode.

- 1 Start **Web Connection** and access the Admin Mode.
- 2 Click the [User Auth/Account Track] tab.
- 3 Click [User Authentication Setting] - [User Registration] from the menu.
- 4 Click the [New Registration].

No.	User Name	Edit	Delete	Counter
1	user1	Edit	Delete	Counter

- Click [Edit] to change settings for a previously registered user.
- To delete a registered user, select the registered user in question and click [Delete]. The following screen appears if the user to be deleted owns a Personal User Box. Select whether to delete the Personal User Box or change it to the Public User Box.

No.	User Name
1	user1

Please select what should occur to the Personal User Box when the User Authentication conditions change (user is deleted, account is deleted, etc.).

Box Operation: Change To Public Box

Documents stored in the ID & Print User Box owned by the user will also be deleted.

Are you sure you want to delete this user?

OK Cancel

- If the boxes are changed to Public User Boxes and if the password set for a particular box before this change does not meet the Password Rules, no access can be made to the Public User Box, to which that specific box was changed. In this case, the administrator must first newly set a password that meets the Password Rules. For details of the Password Rules, see page 1-13.

5 Make the necessary settings.

The screenshot shows the 'User Registration' screen within a system settings application. At the top, there's a header bar with 'Administrator' and a 'Logout' button. Below this is a navigation bar with tabs: Maintenance, System Settings, Security, User Auth/Account Track (selected), Network, and Box. Under 'System Settings', there are sub-tabs: Print Setting, Store Address, Fax Settings, Wizard, Customize, and To Main Menu. The left sidebar lists various settings categories, with 'User Authentication Setting' expanded to show 'User Registration'. The main content area is titled 'User Registration' and contains the following fields and options:

- No.**: Radio buttons for 'Use opening number' (selected) and 'Input directly'. A text box next to 'Input directly' has '(1-500)' as a placeholder.
- User Name**: Text box containing 'user1'.
- E-mail Address**: Text box.
- User Password**: Password field with masked characters.
- Retype User Password**: Password field with masked characters.
- Account Name**: Text box.
- Search from List**: Button.
- Registered Account Name**: Text box.
- Temporarily stop use**: Text label.
- Continue Job**: Pull-down menu.

- A number that already exists cannot be redundantly registered.
- A User Name that already exists cannot be redundantly registered.
- [Account Name] does not appear, if Account Track has not been set for the authentication method or any option other than [Synchronize] has been selected for [Synchronize User Authentication & Account Track].
- To suspend temporarily a registered user from using the machine, select [Stop Job] from the pull-down menu of [Temporarily stop use]. If the account to which the user belongs is temporarily suspended from using the machine, however, selecting [Continue Job] does not allow the user to use the machine.
- To restrict the functions the user can use, use [Function Permission] and set Allow or Restrict for each function.
- To give the administrative right to a user, select [Allow] in [Permission Setting] - [Administrative Rights]. Deletion of the administrative right of a user is reflected after the user is logged out.
- Click [Cancel] to go back to the previous screen.

6 Click [OK].

- If the entered User Password does not meet the Password Rules, a message that tells that the entered User Password cannot be used appears. Enter the correct User Password. For details of the Password Rules, see page 1-13.
- If the entered User Password does not match, a message that tells that the User Password does not match appears. Enter the correct User Password.

7 Check the message that tells that the setting has been completed.

2.12 Account Track Setting Function

When a log-on to the Administrator Mode becomes successful, the machine enables registration of accounts, for which use of the machine is restricted. It also enables operations for deleting an account and changing an Account Password. In **Web Connection**, import/export of the account registration information is enabled, allowing the backup data of the account registration information to be saved or the saved backup data to be restored.

Account Track Registration allows the Account Name, Account Password, and other account information to be registered for enabling access to, or operation of, the machine. Up to 1,000 different users or accounts can be registered. The Account Password is controlled based on passwords that meets the Password Rules and the password entered is displayed as "*" or "•."

Tips

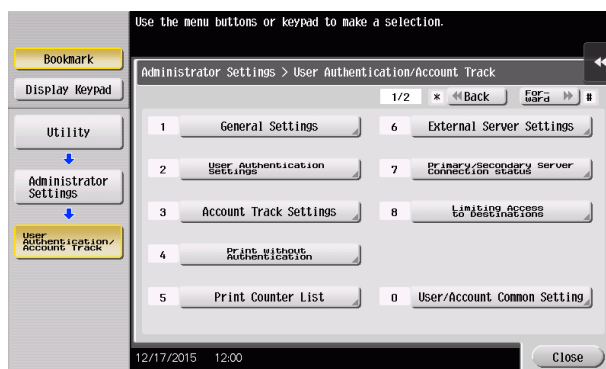
- A specific registered account may be temporarily suspended from using the machine or a suspended account may be allowed to use the machine again. While an account is suspended from using the machine, it cannot log onto the machine. If a registered account to which a particular user belongs is suspended from using the machine, that particular user is also unable to log onto the machine.
- [Pause] setting of the account is enabled even if [External Server Authentication] (Active Directory) is set for the authentication method.
- An input of an Account Password during an initial log-on procedure establishes the account to which the user belongs. Be careful that leakage of the Account Password may cause an unintended account to be set.
- A change made in the Account Password requires that the new Account Password be input during the initial log-on procedure after the change. Make sure that only the user involved is notified of the new Account Password as soon as possible.

Making account setting

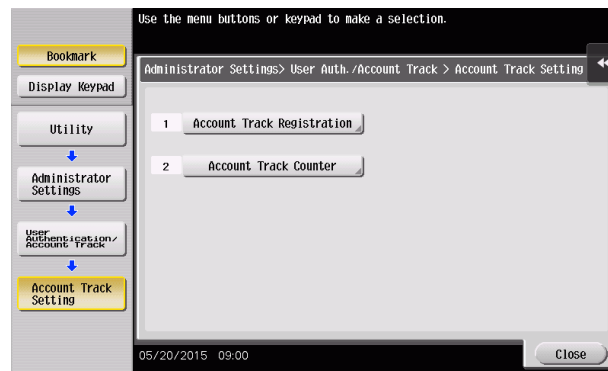
<From the Control Panel>

- ✓ For the procedure to call the User Authentication/Account Track screen on the display, see steps 1 and 2 of page 2-27.
- ✓ Do not leave the machine with the setting screen of Administrator Mode left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Mode.

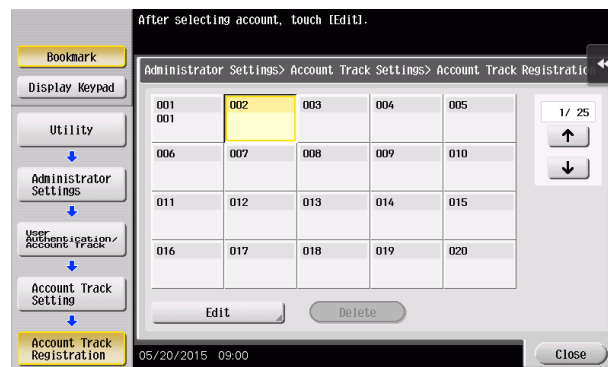
- 1 Call the User Authentication/Account Track screen on the display from the control panel.
- 2 Touch [Account Track Settings].



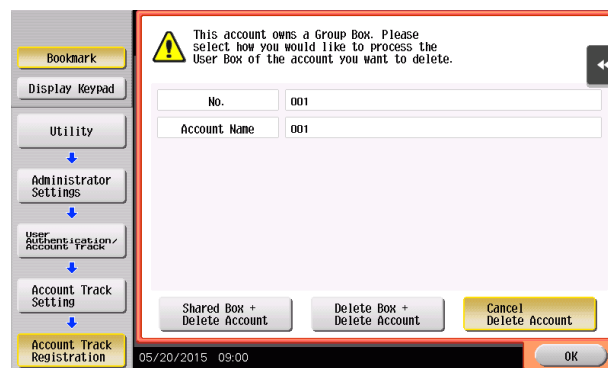
3 Touch [Account Track Registration].



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

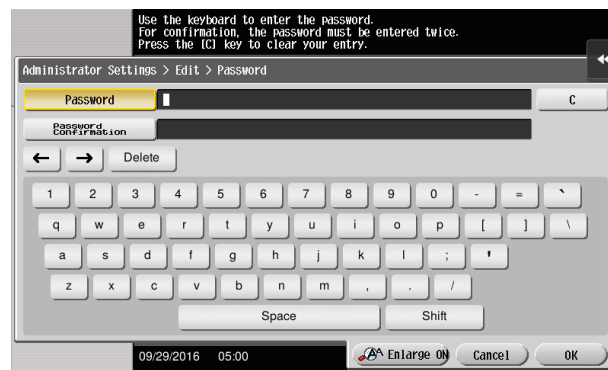


- To change settings for a registered account, select the registered account in question and touch [Edit].
- To delete a registered account, select the registered account in question and touch [Delete]. The following screen appears if the account to be deleted owns a Group User Box. Select whether to delete the Group User Box or change it to the Public User Box.



- If the boxes are changed to Public User Boxes and if the password set for a particular box before this change does not meet the Password Rules, no access can be made to the Public User Box, to which that specific box was changed. In this case, the administrator must first newly set a password that meets the Password Rules. For details of the Password Rules, see page 1-13.

5 Touch [Password].

6 From the keyboard, enter a new Account Password.
To prevent entry of a wrong password, enter the password again in [Password Confirmation].

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

7 Touch [OK].

- If the entered Account Password does not meet the Password Rules, a message that tells that the entered Account Password cannot be used appears. Enter the correct Account Password. For details of the Password Rules, see page 1-13.
- If the entered Account Password does not match, a message that tells that the Account Password does not match appears. Enter the correct Account Password.

8 Make the necessary settings.

- If the Account Name is yet to be entered, [OK] cannot be touched. Be sure to enter the Account Name.
- An Account Name that already exists cannot be redundantly registered.
- To suspend temporarily a registered account from using the machine, touch [Pause] and select [Stop Job]. If [Stop Job] is selected, a user who belongs to that particular account is also temporarily suspended from using the machine.
- To restrict the functions the account can use, use [Function Permission] and set Allow or Restrict for each function. Setting [All Accounts] applies the same [Function Permission] to all accounts.

9 Touch [OK].

<From **Web Connection**>

- ✓ For the procedure to access the Admin Mode, see page 2-2.
- ✓ Do not leave the machine with the Admin Mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin Mode.

- 1 Start **Web Connection** and access the Admin Mode.
- 2 Click the [User Auth/Account Track] tab.
- 3 Click [Account Track Settings] from the menu.
- 4 Click [New Registration].

The screenshot shows the 'Account Track Registration' screen. At the top, there's a header with 'Administrator', 'Logout', and a help icon. Below the header are status indicators: 'Ready to Scan' and 'Ready to Print'. A navigation bar contains tabs: Maintenance, System Settings, Security, User Auth/Account Track (selected), Network, and Box. Below this is a secondary bar with Print Setting, Store Address, Fax Settings, Wizard, Customize, and To Main Menu. The left sidebar lists settings categories: General Settings, User Authentication Setting, Account Track Settings (selected), Prohibited Function Login Setting, Print without Authentication, Simple Print Authentication Setting, and External Server Settings. The main content area is titled 'Account Track Registration' and features a 'New Registration' button. Below this is a search bar with 'Search by number' and a dropdown set to '1-50'. A table displays the following data:

No.	Account Name	Edit	Delete	Counter
1	001	Edit	Delete	Counter

- Click [Edit] to change settings for a previously registered account.
- To delete a registered account, select the registered account in question and click [Delete]. The following screen appears if the account to be deleted owns a Group User Box. Select whether to delete the Group User Box or change it to the Public User Box.

The screenshot shows the 'Delete Account' screen. It has the same header and navigation as the previous screen. The left sidebar is the same. The main content area is titled 'Delete Account'. It contains fields for 'No.' (value: 1) and 'Account Name' (value: 001). Below these is a message: 'Please select what should occur to the Group User Box when User Authentication conditions change (user is deleted, account is deleted, etc.)'. There is a 'Box Operation' dropdown menu currently set to 'Change To Public Box'. At the bottom, it asks 'Are you sure you want to delete?' with 'OK' and 'Cancel' buttons.

- If the boxes are changed to Public User Boxes and if the password set for a particular box before this change does not meet the Password Rules, no access can be made to the Public User Box, to which that specific box was changed. In this case, the administrator must first newly set a password that meets the Password Rules. For details of the Password Rules, see page 1-13.

5 Make the necessary settings.

The screenshot shows the 'Account Track Registration' screen. At the top, there's a header with 'Administrator' and a 'Logout' button. Below the header, there are status indicators: 'Ready to Scan' and 'Ready to Print'. A navigation bar contains several tabs: 'Maintenance', 'System Settings', 'Security', 'User Auth/Account Track' (which is highlighted), 'Network', and 'Box'. Below the navigation bar, there's a sub-menu with 'Print Setting', 'Store Address', 'Fax Settings', 'Wizard', 'Customize', and 'To Main Menu'. The main content area is titled 'Account Track Registration' and contains the following fields and options:

- No.**: Radio buttons for 'Use opening number' (selected) and 'Input directly'. A text box next to 'Input directly' has '(1-500)' as a placeholder.
- Account Name**: A text box containing '001'. Below it, a note says 'Use alphanumeric characters or symbols. The " (double quotation symbol) cannot be used.'
- Password**: A text box with masked characters (dots).
- Retype Password**: A text box with masked characters (dots).
- Temporarily stop use**: A pull-down menu currently showing 'Continue Job'.

- A number that already exists cannot be redundantly registered.
- An Account Name that already exists cannot be redundantly registered.
- To suspend temporarily a registered account from using the machine, select [Stop Job] from the pull-down menu of [Temporarily stop use]. If [Stop Job] is selected, a user who belongs to that particular account is also temporarily suspended from using the machine.
- To restrict the functions the account can use, use [Function Permission] and set Allow or Restrict for each function.
- Click [Cancel] to go back to the previous screen.

6 Click [OK].

- If the entered Account Password does not meet the Password Rules, a message that tells that the entered Account Password cannot be used appears. Enter the correct Account Password. For details of the Password Rules, see page 1-13.
- If the entered Account Password does not match, a message that tells that the Account Password does not match appears. Enter the correct Account Password.

7 Check the message that tells that the setting has been completed.

2.13 User Box Function

When a log-on to the Administrator Mode becomes successful, the machine enables the User Box. It also allows the User Box Password and user and account attributes to be changed.

User Box prepares a User Box in the HDD as a space for saving image files. Up to 1,000 Personal, Public and Group User Boxes can be registered. The User Box Password is controlled based on passwords that meets the Password Rules and the password entered is displayed as "*" or "•."

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

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



Related setting (for the administrator)

Setting the Memory RX function allows a received fax to be stored in the box without its being printed. Because the received faxes are forcibly stored in this box, this will prevent important faxes from being stolen or lost and therefore enhance security. For details, see page 2-59.



Tips

- If [External Server Authentication] (Active Directory) is set for the authentication method, the same Personal User Box name as that registered with the machine can be created and registered along with the External Server name. No two Personal User Box names registered in an External Server may be alike.
- When a document is saved in a box with a box number yet to be registered specified from the PC, the Personal User Box owned by the user who logged on through User Authentication is automatically registered.

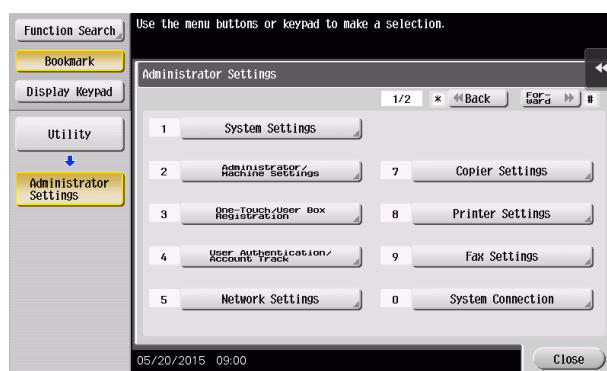
2.13.1 Setting the User Box

<From the Control Panel>

- ✓ For the procedure to call the Administrator Mode on the display, see page 2-2.
- ✓ Do not leave the machine with the setting screen of Administrator Mode left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Mode.
- ✓ For the procedure to change the user attributes, account attributes, and User Box Password, see page 2-54.

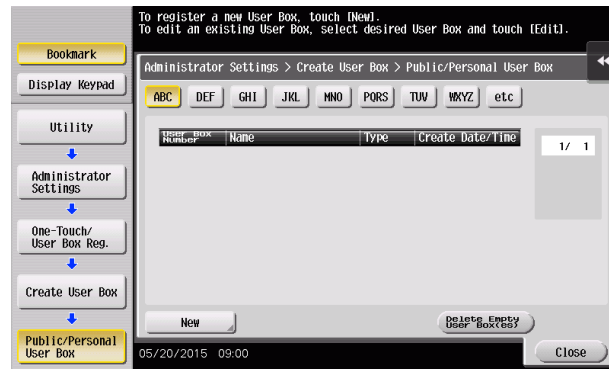
1 Call the Administrator Mode on the display from the control panel.

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



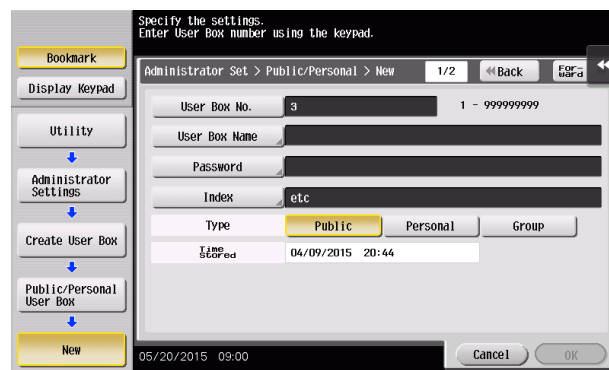
3 Touch [Create User Box], and select the desired box type.

4 Touch [New].

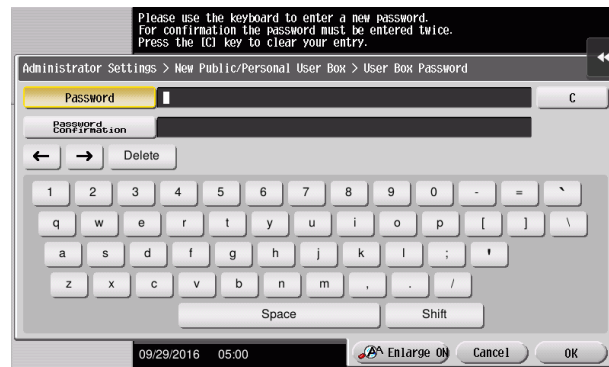


→ To delete a User Box, select the desired user box key and touch [Delete]. A confirmation message appears. Select [Yes] and touch [OK] to delete the specified User Box.

5 Touch [Password].



6 Enter the new User Box Password from the keyboard.
To prevent entry of a wrong password, enter the password again in [Password Confirmation].



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

- 7 If [Public/Personal User Box] is selected in step 3, select the User Box Type.

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

Administrator Set > Public/Personal > New 1/2 << Back Forward >>

User Box No. 3 1 - 999999999

User Box Name

Password

Index etc

Type Public Personal Group

Time stored 04/09/2015 20:44

05/20/2015 09:00 Cancel OK

- When [Personal] is selected, [Change Owner] is displayed. Then, select the desired owner name.

Select the owner of the User Box.

Administrator Settings > New Public/Personal User Box > Change Owner <<

Owner Name

user1 1/ 1

05/20/2015 09:00 OK

- When [Group] is selected, [Change Account Name] is displayed. Then, select the desired account name.

Select the account that owns the User Box.

Administrator Settings > New Public/Personal User Box > Change Owner <<

Account Name

001 1/ 1

05/20/2015 09:00 OK

- 8 Touch [OK].
- Set a User Box Password that meets the Password Rules. For details of the Password Rules, see page 1-13.
 - If the entered User Box Password does not match, a message that tells that the User Box Password does not match appears. Enter the correct User Box Password.
- 9 Make the necessary settings.
- A User Box No. that already exists cannot be redundantly registered.
 - If no User Box Name has been registered, [OK] cannot be touched. Be sure to register the User Box Name.
- 10 Touch [OK].

<From **Web Connection**>

- ✓ For the procedure to access the Admin Mode, see page 2-2.
- ✓ Do not leave the machine with the Admin Mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin Mode.
- ✓ For the procedure to change the user attributes, account attributes and User Box Password, see page 2-54.

1 Start **Web Connection** and access the Admin Mode.

2 Click the [Box] tab.

3 Click [New Registration].

User Box List

A new User Box can be registered.

New Registration

Page Display(50/page) 1

Search from Index ALL Go

User Box Number	User Box Name	Type	Owner Name	Box Operation
1	Box1	Public	Public	Edit Delete
2	Box2	Personal	user1	Edit Delete
3	Box3	Group	001	Edit Delete

4 Make the necessary settings.

Create User Box(Public/Group/Personal)

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

User Box Number

☒ Use opening number

☐ Input directly (1-99999999)

User Box Name Box1

☒ Assign User Box Password

User Box Password

Retype User Box Password

Index

Specify a keyword for Box search and display by Name.

ABC

Type Public

Auto Delete Document

☐ Do Not Delete

☒ Specify days 1 day

☐ Specify Time min.(5-720)

User Box Expansion Function Display

OK Cancel

- Be sure to enter the User Box Number, User Box Name, User Box Password, and Retype User Box Password.
- A User Box Number that already exists cannot be redundantly registered.

- If [Personal] is selected from the User Box Type pull-down menu, click [User List] and select the user from the registered user list. Or, directly enter in the "Owner Name" box the previously registered User Name.
- If [Group] is selected from the User Box Type pull-down menu, click [Account List] and select the account from the registered account list. Or, directly enter in the "Account Name" box the previously registered Account Name.

5 Click [OK].

- Set a User Box Password that meets the Password Rules. For details of the Password Rules, see page 1-13.
- If the entered User Box Password does not match, a message that tells that the User Box Password does not match appears. Enter the correct User Box Password.
- If no Owner Name is entered, a message appears that tells that no Owner Names have been entered. Enter the correct Owner Name.
- If a user name not registered with the machine is entered in the "Owner Name" box, a message appears that tells that the Owner Name entered in the box is illegal. Enter the correct Owner Name.
- If no Account Name is entered, a message appears that tells that no Account Names have been entered. Enter the correct Account Name.
- If an account name not registered with the machine is entered in the "Account Name" box, a message appears that tells that the Account Name entered in the box is illegal. Enter the correct Account Name.

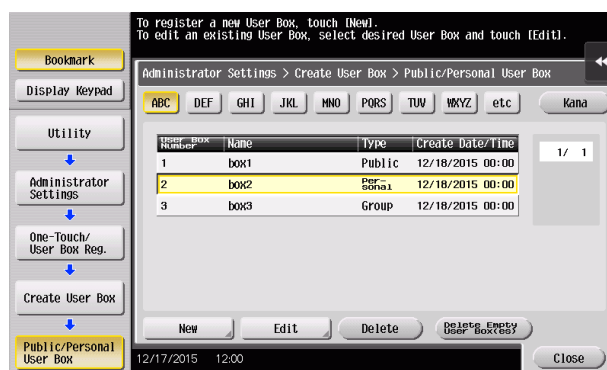
2.13.2 Changing the user/account attributes and box password

The administrator can change the box type of the box previously registered. The owner user can be changed for the Personal User Box, the owner account can be changed for the Group User Box, and the password can be changed or deleted for the Annotation Box.

<From the Control Panel>

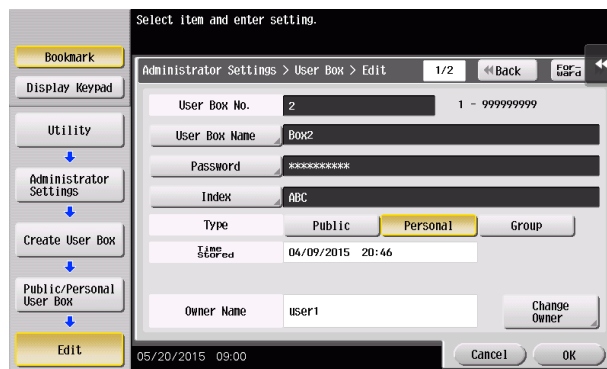
- ✓ For the procedure to call the User Box setting screen on the display, see steps 1 through 3 of page 2-49.
- ✓ Do not leave the machine with the setting screen of Administrator Mode left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Mode.
- ✓ Changing the box type to [Public] nullifies the setting of the owner user or owner account.

- 1 Call the User Box setting screen on the display from the control panel.
- 2 Select the desired User Box key and touch [Edit].



- To change the User Box Type, perform steps 3 through 6.
- To change the owner user or owner account, perform steps 4 through 6.
- To change the User Box Password, go to step 7.

- 3 Select the User Box Type.



- [Change Owner] appears if the Box Type is changed to [Personal]. Select the desired owner name.
- [Change Account Name] appears if the Box Type is changed to [Group]. Select the desired account name.
- Set a User Box Password that meets the Password Rules. For details of the Password Rules, see page 1-13.

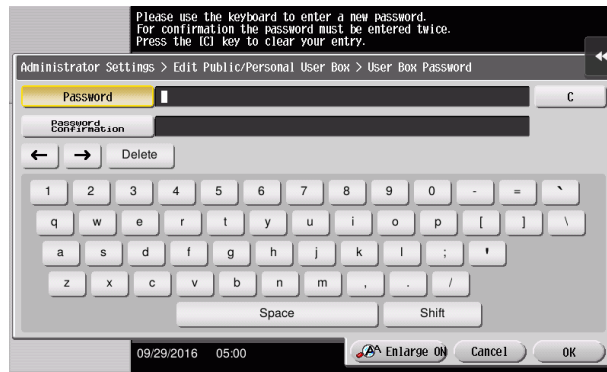
- 4 Touch [Change Owner] if the Box Type is [Personal] and touch [Change Account Name] if the Box Type is [Group].

- 5 For [Change Owner], select the desired owner name.

→ For [Change Account Name], select the desired account name.

- 6 Touch [OK].
- 7 Touch [Password].

- 8 Enter the new User Box Password from the keyboard.
To prevent entry of a wrong password, enter the password again in [Password Confirmation].



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

- 9 Touch [OK].
- Set a User Box Password that meets the Password Rules. For details of the Password Rules, see page 1-13.
 - If the entered User Box Password does not match, a message that tells that the User Box Password does not match appears. Enter the correct User Box Password.

- 10 Touch [OK].

<From **Web Connection**>

- ✓ For the procedure to access the Admin Mode, see page 2-2.
- ✓ Do not leave the machine with the Admin Mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin Mode.

1 Start **Web Connection** and access the Admin Mode.

2 Click the [Box] tab.

3 Click [Edit] of the target box.

User Box List

A new User Box can be registered.

New Registration

Page Display(50/page) 1

Search from Index ALL Go

User Box Number	User Box Name	Type	Owner Name	Box Operation
1	Box1	Public	Public	Edit Delete
2	Box2	Personal	user1	Edit Delete
3	Box3	Group	001	Edit Delete

→ Go to step 5 to change the User Box Password.

→ To delete a User Box, click [Delete User Box]. A confirmation message appears. Click [OK] to delete the specified User Box.

4 Click the "User Box Owner is changed." check box and change Type and Owner Name (or Account Name).

User Box Attribute Change

User Box Number 2

User Box Name Box2

Index PQRS

☐ User Box Expansion Function is changed.

Confidential RX OFF

New Communication Password

Retype New Communication Password

☐ User Box Password is changed.

New Password

Retype New Password

☒ User Box Owner is changed.

Type Personal

Owner Name user1

OK Cancel

→ If [Personal] is selected from the User Box Type pull-down menu, click [User List] and select the user from the registered user list. Or, directly enter in the "Owner Name" box the previously registered User Name.

- If [Group] is selected from the User Box Type pull-down menu, click [Account List] and select the account from the registered account list. Or, directly enter in the "Account Name" box the previously registered Account Name.
- If the "User Box Owner is changed." check box is not clicked, the changes made will not be validated. If the changes need to be made, make sure that the "User Box Owner is changed." check box has been clicked.
- To change the User Box Type, click the Type pull-down menu and select the desired box type.

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

6 Click [OK].

- Set a User Box Password that meets the Password Rules. For details of the Password Rules, see page 1-13.
- If the entered User Box Password does not match, a message that tells that the User Box Password does not match appears. Enter the correct User Box Password.
- If no Owner Name is entered, a message appears that tells that no Owner Names have been entered. Enter the correct Owner Name.
- If a user name not registered with the machine is entered in the "Owner Name" box, a message appears that tells that the Owner Name entered in the box is illegal. Enter the correct Owner Name.
- If no Account Name is entered, a message appears that tells that no Account Names have been entered. Enter the correct Account Name.
- If an account name not registered with the machine is entered in the "Account Name" box, a message appears that tells that the Account Name entered in the box is illegal. Enter the correct Account Name.

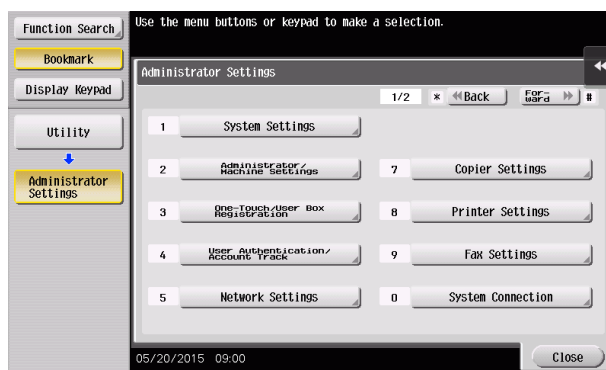
2.13.3 Setting Memory RX

<From the Control Panel>

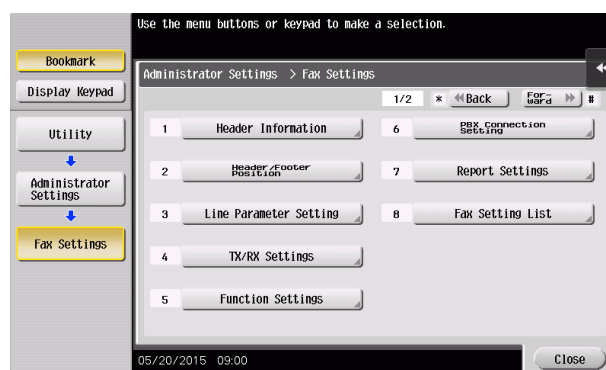
- ✓ For the procedure to call the Administrator Mode on the display, see page 2-2.
- ✓ Do not leave the machine with the setting screen of Administrator Mode left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Mode.

1 Call the Administrator Mode on the display from the control panel.

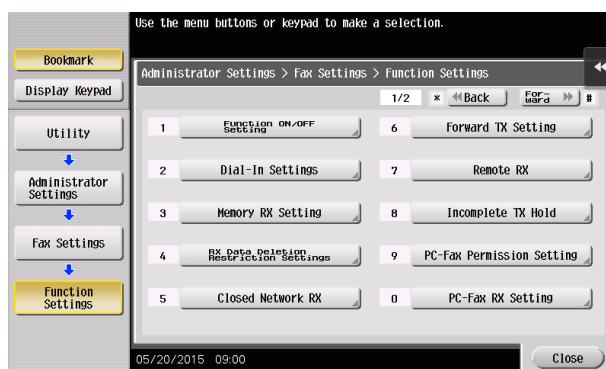
2 Touch [Fax Settings].



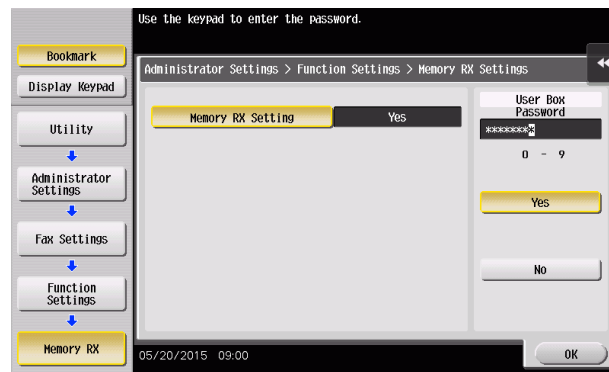
3 Touch [Function Settings].



4 Touch [Memory RX Setting].



- 5 Touch [Memory RX Setting]. Then, select [Yes] and enter the Memory RX User Box Password consisting of eight characters from the ten-key pad.



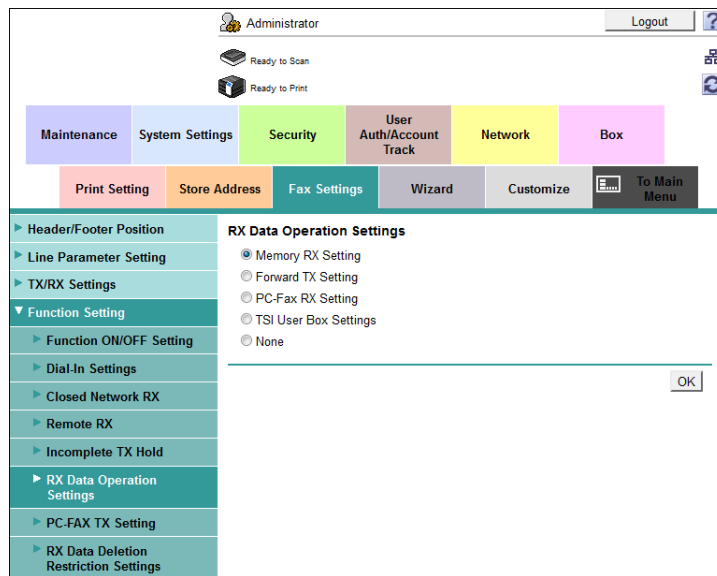
- Touch [Display Keypad] to display the keypad.
- Make sure that the Memory RX User Box Password consists of eight characters.
- To change a password for the Memory RX, overwrite the new password.

- 6 Touch [OK].

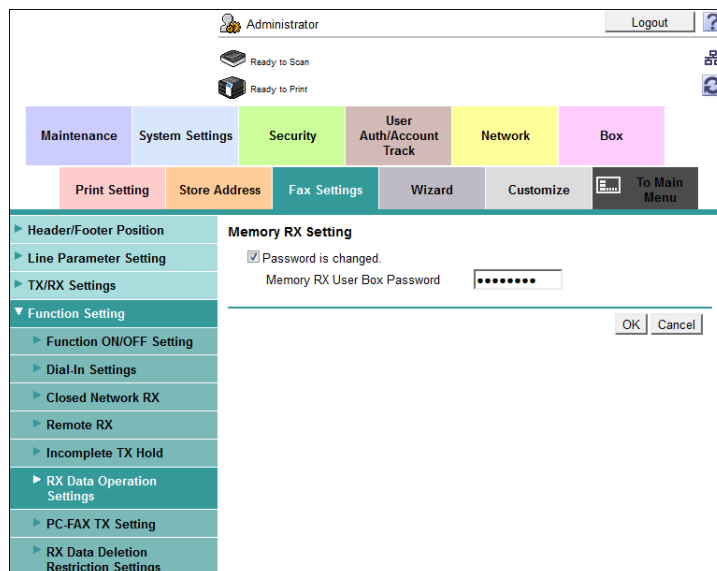
<From **Web Connection**>

- ✓ For the procedure to access the Admin Mode, see page 2-2.
- ✓ Do not leave the machine with the Admin Mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin Mode.

- 1 Start **Web Connection** and access the Admin Mode.
- 2 Click the [Fax Settings] tab.
- 3 Click [Function Setting] - [RX Data Operation Settings] from the menu.
- 4 Select [Memory RX Setting] and click [OK].



- 5 Select the check box under [Password is changed] and set the Memory RX User Box Password that should consist of eight characters.



→ Make sure that the Memory RX User Box Password consists of eight characters.

- 6 Click [OK].

2.14 Changing the Administrator Password

When a log-on to the Administrator Mode becomes successful, the machine enables the operation of changing the Administrator Password required for accessing the Administrator Mode.

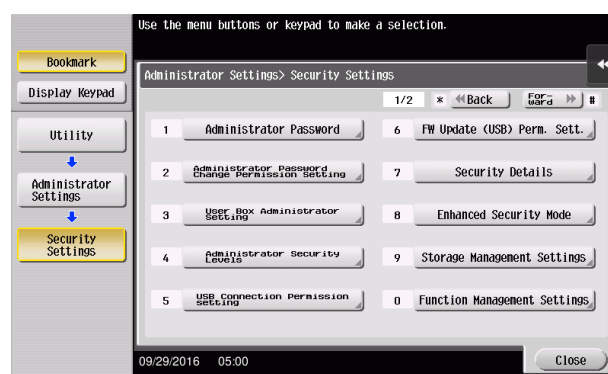
The Administrator Password entered for the authentication purpose appears as "*" on the display.

Changing the Administrator Password

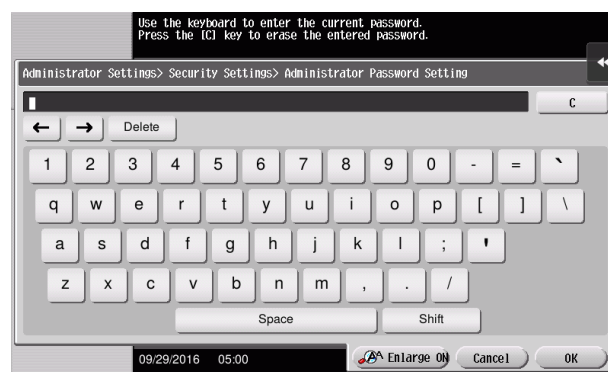
<From the Control Panel>

- ✓ For the procedure to call the Security Settings screen on the display, see steps 1 through 3 of page 2-15.
- ✓ Do not leave the machine with the setting screen of Administrator Mode left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Mode.

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



- 3 Enter the currently set Administrator Password from the keyboard.



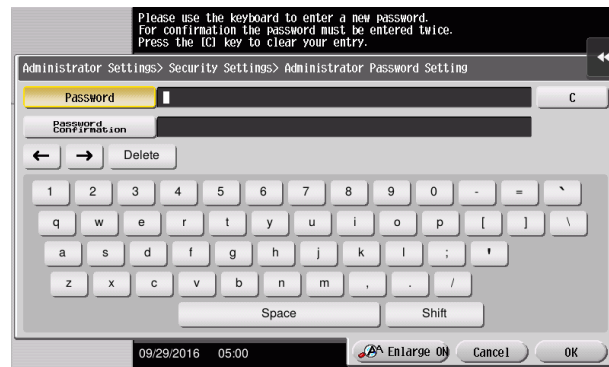
- Touch [C] to clear all characters.
- Touch [Delete] to delete the last character entered.
- Touch [Shift] to show the upper case/symbol screen.
- Touch [Cancel] to go back to the Security Settings screen.

- 4 Touch [OK].

- If a wrong Administrator Password is entered, a message that tells that the Administrator Password does not match appears. Enter the correct Administrator Password.
- If the Enhanced Security Mode is set to [ON], entry of a wrong password is counted as unauthorized access. If a wrong Administrator Password is entered a predetermined number of times (once to three times) or more set by the administrator, the Utility screen appears and the machine is set into an access lock state.
To cancel the access lock state, settings must be made by the Service Engineer; or, turn off, and then turn on, the **main power switch** of the machine. If the **main power switch** is turned off and on, the access lock state is canceled after the lapse of time set for [Release Time Settings]. When

the **main power switch** is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. If there is no wait period between turning the **main power switch** off, then on again, the machine may not function properly.

- 5 Enter the new Administrator Password from the keyboard.
To prevent entry of a wrong password, enter the password again in [Password Confirmation].



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

- 6 Touch [OK].
- If the entered Administrator Password does not meet the Password Rules, a message that tells that the entered Administrator Password cannot be used appears. Enter the correct Administrator Password. For details of the Password Rules, see page 1-13.
 - If the entered Administrator Password does not match, a message that tells that the Administrator Password does not match appears. Enter the correct Administrator Password.

<From **Web Connection**>

- ✓ For the procedure to access the Admin Mode, see page 2-2.
- ✓ Do not leave the machine with the Admin Mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin Mode.

1 Start **Web Connection** and access the Admin Mode.

2 Click the [Security] tab.

3 Click [Administrator Password Setting] from the menu.

→ If the SSL Setting is disabled, [Administrator Password Setting] is not displayed. For details, see page 2-95.

4 Select the "Password is changed" check box. Enter the currently registered Administrator Password and a new Administrator Password. Then, to make sure that you have entered the correct new password, enter the new Administrator Password once again.

5 Click [OK].

→ If a wrong Administrator Password is entered in the "Current Administrator Password" box, a message that tells that the Administrator Password does not match appears. Enter the correct Administrator Password.

→ If the Enhanced Security Mode is set to [ON], entry of a wrong password is counted as unauthorized access. If a wrong Administrator Password is entered a predetermined number of times (once to three times) or more set by the administrator, the Utility screen appears and the machine is set into an access lock state.

To cancel the access lock state, settings must be made by the Service Engineer; or, turn off, and then turn on, the **main power switch** of the machine. If the **main power switch** is turned off and on, the access lock state is canceled after the lapse of time set for [Release Time Settings]. When the **main power switch** is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. If there is no wait period between turning the **main power switch** off, then on again, the machine may not function properly.

→ If the entered Administrator Password in the "New Administrator Password" box does not meet the Password Rules, a message that tells that the entered Administrator Password cannot be used appears. Enter the correct Administrator Password. For details of the Password Rules, see page 1-13.

→ If the entered Administrator Password in the "New Administrator Password" box and "Re-type New Administrator Password" box does not match, a message that tells that the Administrator Password does not match appears. Enter the correct Administrator Password.

6 Click [OK].

2.15 Protecting Data in the HDD

When a log-on to the Administrator Mode becomes successful, the machine enables the operation for setting and changing the Encryption Key. The machine also enables the Overwrite HDD Data function.

By setting the Encryption Key, the data stored in the HDD is encrypted, thereby protecting the data in the HDD. The Encryption Key entered is displayed as "**."

NOTICE

If the HDD develops a fault, call your Service Representative.

The following shows setting conditions for the Encryption Key. Perform settings for the Encryption Key fitting these conditions.

Types of passwords	Number of characters	Types of characters	Conditions for setting/changes
Encryption Key	20 characters	<ul style="list-style-type: none"> Numeric characters: 0 to 9 Alpha characters: upper and lower case letters Symbols: !, #, \$, %, &, ', *, +, -, ., /, =, ?, @, ^, _ , ` , {, , }, ~ Selectable from among a total of 83 characters 	<ul style="list-style-type: none"> An Encryption Key only consisting of identical characters cannot be registered or changed. The current Encryption Key must be entered before a change can be made in the setting. A new Encryption Key to be set should not be the same as the current one.



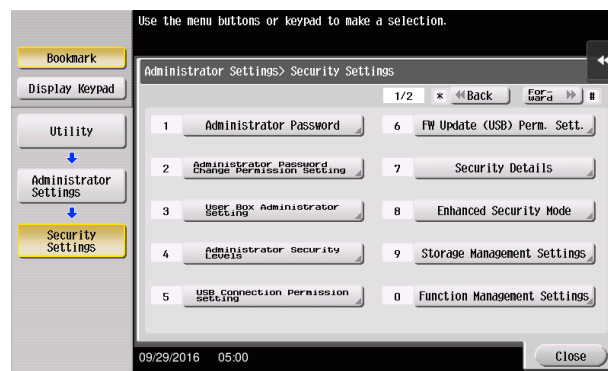
Tips

When an Encryption Key (encryption word) is set using HDD Encryption Setting, an Encryption Key with a key length of 256 bits is generated. The generated encryption key is used to encrypt or decrypt data through AES encryption algorithm.

2.15.1 Setting the Encryption Key (encryption word)

- ✓ For the procedure to call the Security Settings screen on the display, see steps 1 through 3 of page 2-15.
- ✓ Do not leave the machine with the setting screen of Administrator Mode left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Mode.
- ✓ To prevent data from leaking as a result of reinstallation of the HDD on another machine, a unique value that varies from one machine to another must be set for the encryption key.
- ✓ Do not set any number that can easily be guessed from birthdays, employee identification numbers, and the like for the Encryption Key. Try to change the Encryption Key at regular intervals.
- ✓ Make sure that nobody but the administrator comes to know the Encryption Key.
- ✓ If only the Encryption Key is to be set while the machine is being used without setting the Encryption Key, the Service Engineer must perform some setting procedures in advance. For details, contact your Service Representative.
- ✓ To edit/release the Encryption Key, see page 2-69. Do not release the Encryption Key when the Enhanced Security Mode is set to [ON]. Releasing the Encryption Key will cancel the Enhanced Security Mode.
- ✓ Executing HDD Format erases data in the HDD. It is recommended that important data should be saved in a backup medium in advance. Execution of HDD Format will also reset the setting values of different functions to the default values. Set the Enhanced Security Mode to [ON] again. For the functions whose settings are reset to the default values, see page 2-14.

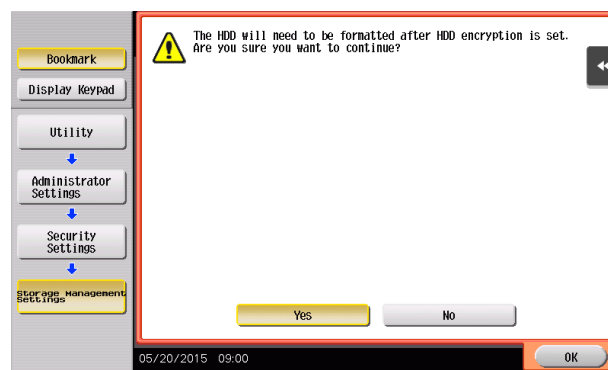
- 1 Call the Security Settings screen on the display from the control panel.
- 2 Touch [Storage Management Settings].



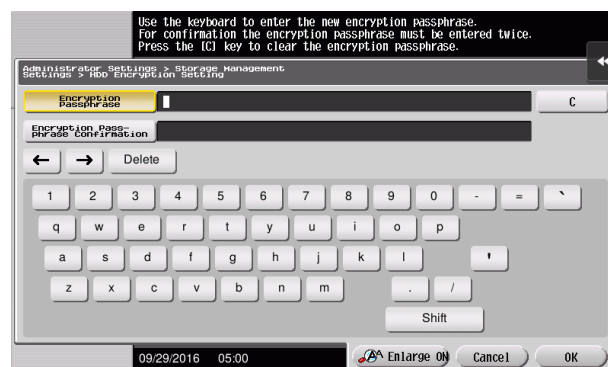
- 3 Touch [HDD Encryption Setting].



- 4 A confirmation message appears. Select [Yes] and touch [OK].



- 5 Enter the new 20 characters Encryption Key from the keyboard. To prevent entry of a wrong Encryption Key, enter the Encryption Key again in [Encryption Passphrase Confirmation].

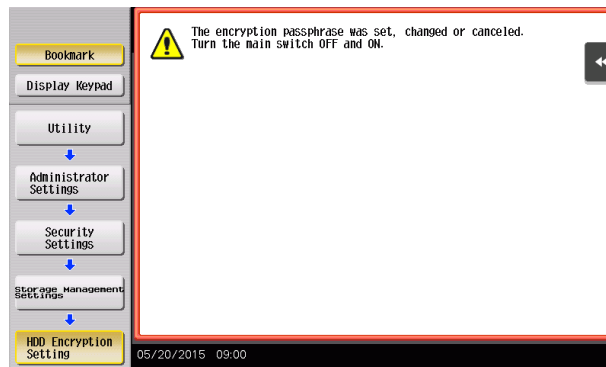


- Touch [C] to clear all characters.
- Touch [Delete] to delete the last character entered.
- Touch [Shift] to show the upper case/symbol screen.
- Touch [Cancel] to go back to the Storage Management Settings screen.

6 Touch [OK].

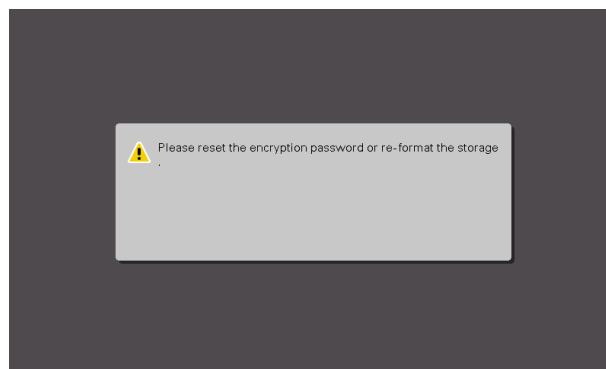
- If the entered Encryption Key does not meet the setting requirements, a message that tells that the entered Encryption Key cannot be used appears. Enter the correct Encryption Key.
- If the entered Encryption Key does not match, a message that tells that the Encryption Key does not match appears. Enter the correct Encryption Key.

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



- When the **main power switch** is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. If there is no wait period between turning the **main power switch** off, then on again, the machine may not function properly.

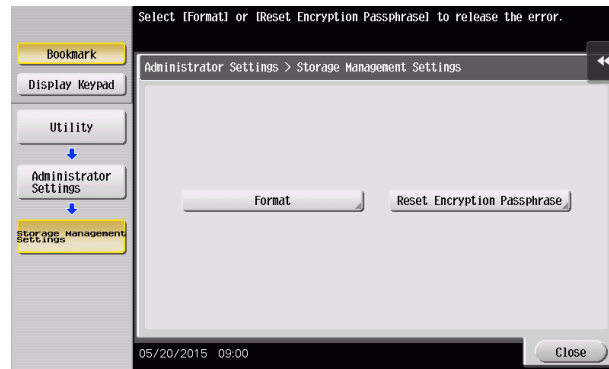
8 The following screen appears after the machine has been restarted.



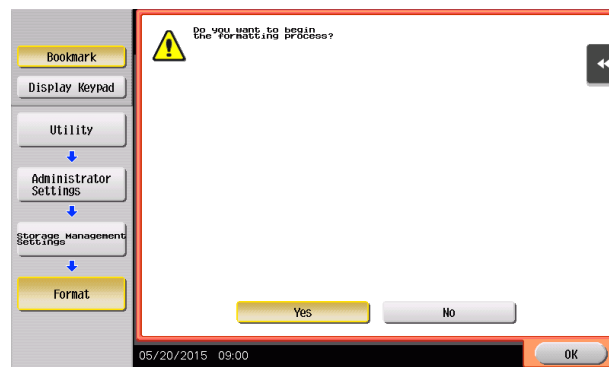
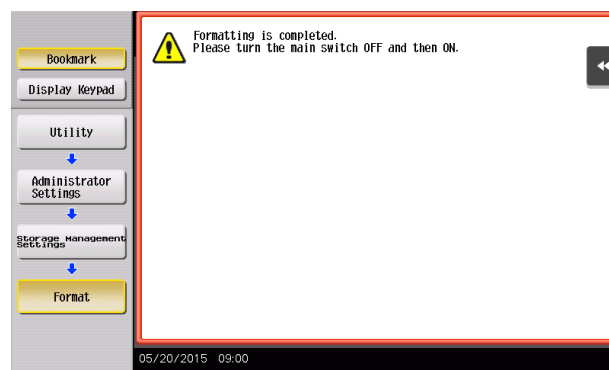
9 Call the Administrator Mode on the display from the control panel.

- For the procedure to call the Administrator Mode on the display, see page 2-2.

10 Touch [Format].



11 A confirmation message appears. Select [Yes] and touch [OK].

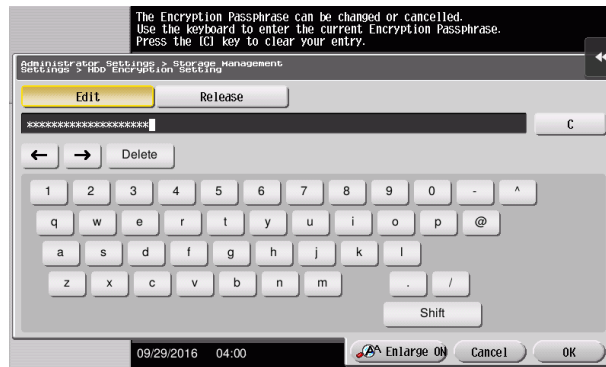
12 Make sure that a message appears prompting you to turn OFF and then ON the **main power switch**. Now, turn OFF and then turn ON the **main power switch**.

- When the **main power switch** is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. If there is no wait period between turning the **main power switch** off, then on again, the machine may not function properly.

2.15.2 Changing the Encryption Key

- ✓ For the procedure to call the Encryption Key entry screen on the display, see steps 1 through 4 of page 2-65.
- ✓ Do not leave the machine with the setting screen of Administrator Mode left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Mode.

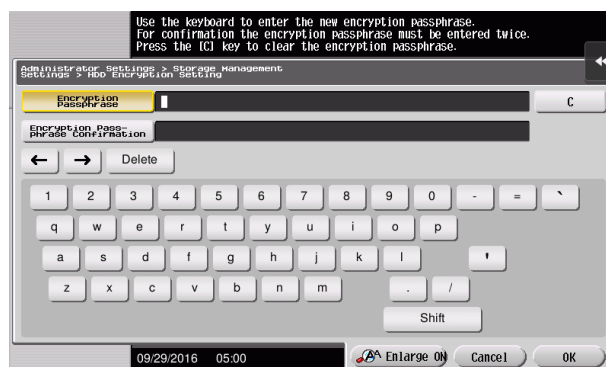
- 1 Call the Encryption Key entry screen on the display from the control panel.
- 2 Enter the currently registered 20 characters Encryption Key from the keyboard.



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

- 3 Select [Edit] and touch [OK].
 - If a wrong Encryption Key is entered, a message that tells that the Encryption Key does not match appears. Enter the correct Encryption Key.
 - Releasing the Encryption Key by selecting [Release] will cancel the Enhanced Security Mode.
- 4 Enter the new 20 characters Encryption Key from the keyboard.

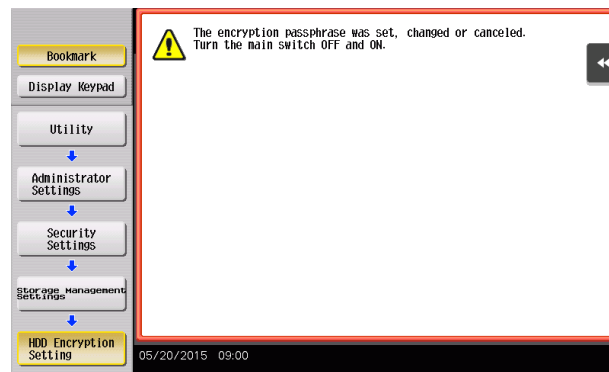
To prevent entry of a wrong Encryption Key, enter the Encryption Key again in [Encryption Passphrase Confirmation].



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

- 5 Touch [OK].
 - If the entered Encryption Key does not meet the setting requirements, a message that tells that the entered Encryption Key cannot be used appears. Enter the correct Encryption Key.
 - If the entered Encryption Key does not match, a message that tells that the Encryption Key does not match appears. Enter the correct Encryption Key.

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



- When the **main power switch** is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. If there is no wait period between turning the **main power switch** off, then on again, the machine may not function properly.

2.15.3 Setting the Overwrite HDD Data

Setting the Overwrite HDD Data function allows data stored in the HDD to be deleted at such timing as the end of the print cycle by writing specific data over the data that is no longer required. By deleting residual data that is no longer necessary, data leakage can be prevented from occurring.

The following types of data are subject to the Overwrite HDD Data function:

- Copy, scan, print, or fax job data that is no longer necessary
- PC print job data (direct print, PS print) that is no longer necessary
- Data that is no longer necessary as a result of the data being specified to be deleted

Data stored in the HDD is to be deleted at the following timing:

- At the end (including an end as a result of cancellation) of a copy, scan, print, or fax job performed by a user who has been authenticated by User Authentication
- A job is deleted by the administrator or a user (who has been authenticated by User Authentication)
- A document in a Box is deleted by the administrator or a user (who has been authenticated by User Authentication)
- A document is deleted in a Box through Delete User Box
- A document is automatically deleted after the lapse of a predetermined period of time set in the machine *

*: The machine offers the following types of automatic box document deleting functions based on a predetermined period of time set in it.

<Administrator>

- To be set through [Utility] - [Administrator Settings] - [System Settings] - [User Box Settings] - [Document Delete Time Setting].
- To be set through [Utility] - [Administrator Settings] - [System Settings] - [User Box Settings] - [Auto Delete Secure Document].
- To be set through [Utility] - [Administrator Settings] - [System Settings] - [User Box Settings] - [ID & Print Delete Time].

<User>

- To be set through [Utility] - [One-Touch/User Box Registration] - [Create User Box] - [Public/Personal User Box] - [New] - [Forward] - [Auto Document Delete Time].
Time to delete documents automatically cannot be set by the user, if [Yes] is set in [Utility] - [Administrator Settings] - [System Settings] - [User Box Settings] - [Document Delete Time Setting].



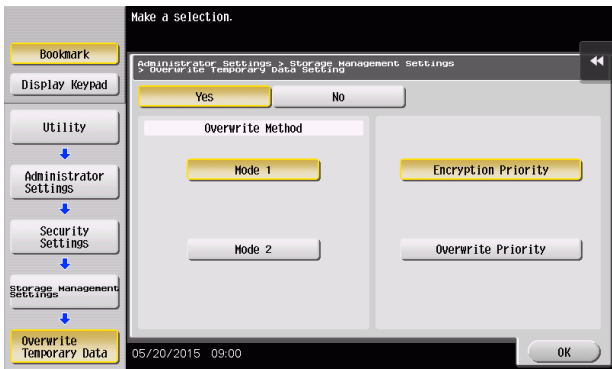
Tips

- If a job being processed is abnormally terminated, the residual data is deleted through Overwrite HDD Data.
 - If the machine is turned off during an Overwrite HDD Data sequence, the Overwrite HDD Data sequence is resumed automatically after the machine is turned on again.
 - If an Overwrite HDD Data sequence being performed is interrupted by, for example, a fault, a response is detected at 30-sec. intervals and the Overwrite HDD Data sequence, if found interrupted, is resumed automatically.
- ✓ For the procedure to call the Storage Management Settings screen on the display, see steps 1 and 2 of page 2-65.
 - ✓ Do not leave the machine with the setting screen of Administrator Mode left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Mode.
 - ✓ Executing HDD Format erases data in the HDD. It is recommended that important data should be saved in a backup medium in advance. Execution of HDD Format will also reset the setting values of different functions to the default values. Set the Enhanced Security Mode to [ON] again. For the functions whose settings are reset to the default values, see page 2-14.

- 1 Call the Storage Management Settings screen on the display from the control panel.
- 2 Touch [Overwrite HDD Data].



- 3 Select [Yes] and then select [Mode 1] or [Mode 2].



Item	Description
[Mode 1]	Overwritten with "0x00"
[Mode 2]	Overwritten with "0x00" - Overwritten with "0xff" - Overwritten with letter "a" (0x61) - Verified

→ [No] is the default setting.

- 4 Touch [OK].

2.16 Overwrite All Data Function

When a log-on to the Administrator Mode becomes successful, the machine enables setting of the operation of the Overwrite All Data function.

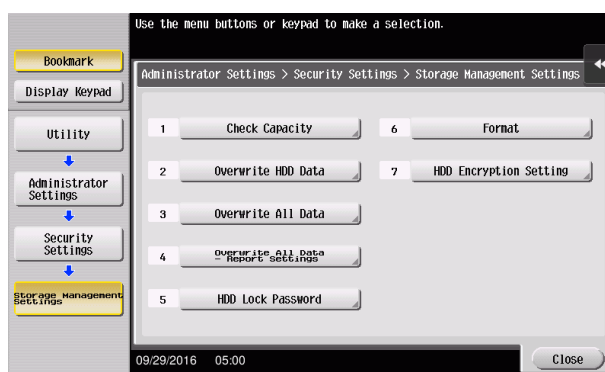
When the machine is to be discarded, or use of a leased machine is terminated at the end of the leasing contract, the Overwrite All Data function overwrites and erases all data stored in all spaces of the HDD. The function also resets all passwords saved in the flash memory and eMMC to factory settings, preventing data from leaking. For details of items that are cleared by the Overwrite All Data function, see page 1-16.

The HDD Overwrite Method offers the choice of eight different modes, [Mode 1] through [Mode 8]. Overwrite All Data takes about less than one hour in [Mode 1] at the minimum and about 9 hours in [Mode 8] at the maximum.

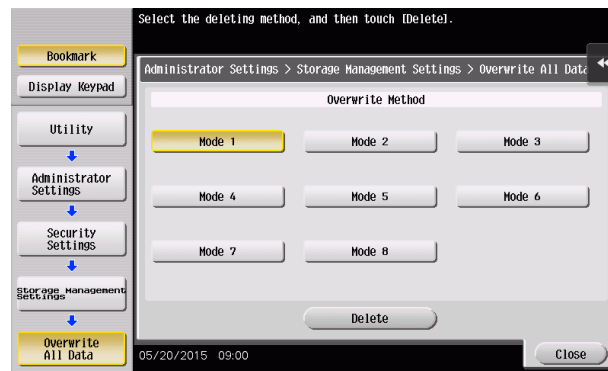
Mode	Description
[Mode 1]	Overwrites once with "0x00."
[Mode 2]	Overwrites with "random numbers" - "random numbers" - "0x00."
[Mode 3]	Overwrites with "0x00" - "0xff" - "random numbers" - verifies.
[Mode 4]	Overwrites with "random numbers" - "0x00" - "0xff."
[Mode 5]	Overwrites with "0x00" - "0xff" - "0x00" - "0xff."
[Mode 6]	Overwrites with "0x00" - "0xff" - "0x00" - "0xff" - "0x00" - "0xff" - "random numbers."
[Mode 7]	Overwrites with "0x00" - "0xff" - "0x00" - "0xff" - "0x00" - "0xff" - "0xaa."
[Mode 8]	Overwrites with "0x00" - "0xff" - "0x00" - "0xff" - "0x00" - "0xff" - "0xaa" - verifies.

Setting the Overwrite All Data function

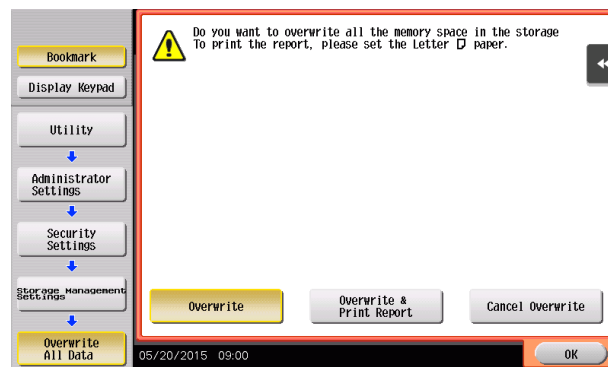
- ✓ For the procedure to call the Storage Management Settings screen on the display, see steps 1 and 2 of page 2-65.
 - ✓ Do not leave the machine with the setting screen of Administrator Mode left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Mode.
- 1 Call the Storage Management Settings screen on the display from the control panel.
 - 2 Touch [Overwrite All Data].



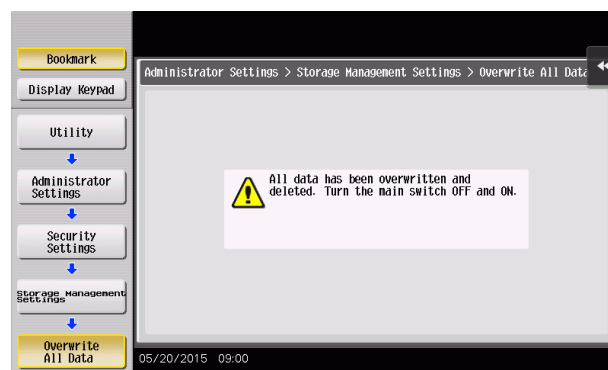
- 3 Select the desired mode and touch [Delete].



- 4 Select [Overwrite] and touch [OK].



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



- Check that all data has been overwritten and erased properly. Data is not erased properly if an error occurs during the procedure. For details, contact your Service Representative.
- When the **main power switch** is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. If there is no wait period between turning the **main power switch** off, then on again, the machine may not function properly.
- After the **main power switch** has been turned on, quickly turn it off and give the machine to the Service Engineer. If the Overwrite All Data function is executed by mistake, contact the Service Engineer. For details, contact your Service Representative.

2.17 Obtaining Job Log

When a log-on to the Administrator Mode becomes successful, the machine enables acquisition and deletion of a Job Log. The Job Log (Audit Log) is a function that stores information on, for example, operations performed in the machine and a job history in the HDD. Setting the Job Log (Audit Log) allows an illegal act or inadequate operation performed on the machine to be traced.

The obtained Job Log can be downloaded and viewed from the **Web Connection**.



Related setting (for the administrator)


Job Log obtains time/date information. So, set an accurate time/date in the machine in advance. For more details on the time/date setting, see page 2-88.

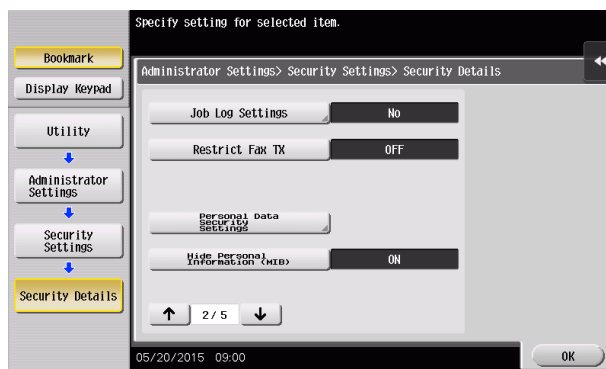
Log Type	Description	
[Accounting Log]	Enables you to obtain information relevant to paper consumption for each user or account.	
[Counting Log]	Enables you to obtain information about paper consumption and the reduction rate of paper used for printing.	
[Audit Log]	Enables you to obtain user operation or job history. <ul style="list-style-type: none"> It is recommended that Audit Log be backed up at regular intervals. The machine is capable of saving up to about 20,000 records of Audit Log. The maximum number of days the records can be saved depends on the operating condition of the machine. For example, identify the output volume of the audit log by operating the machine for several days and estimate adequate frequency of the backup operation. Audit Log is concerned mainly with the following events.	
	Log relating to jobs	<ul style="list-style-type: none"> Jobs stored in boxes in the copy, scan, or box mode from the control panel Jobs stored in boxes via the printer driver, and print jobs Jobs stored in boxes after fax reception Jobs output from boxes
	Log relating to authentication	<ul style="list-style-type: none"> Successful or failed administrator of the machine authentication Successful or failed user administrator authentication Successful or failed user/account authentication Successful or failed Public User Box authentication Successful or failed authentication of access to a Secure Print document
	Turning ON/OFF the main power switch (including starting of the Audit Log function)	

2.17.1 Obtaining and deleting a Job Log

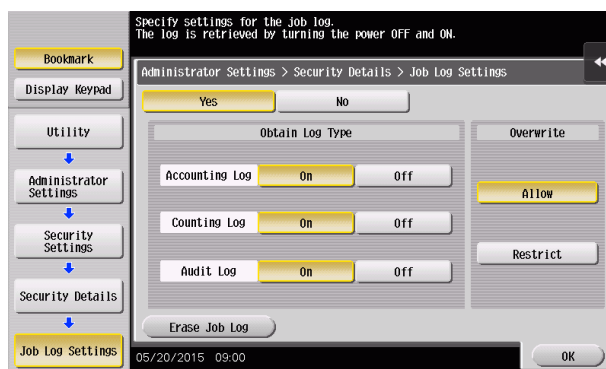
- ✓ For the procedure to call the Security Details screen on the display, see steps 1 and 2 of page 2-23.
- ✓ Do not leave the machine with the setting screen of Administrator Mode left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Mode.

- 1 Call the Security Details screen on the display from the control panel.

- 2 Touch [] and touch [Job Log Settings].



- 3 Select [Yes] and touch [On] of the specific type of log to be obtained.



- Under [Overwrite], whether to enable writing over old Job Logs when the Job Log space in the HDD is full of old Job Logs can be selected.

Item	Description
[Allow]	Allows Job Logs to be continuously stored by writing over old Job Logs in chronological order even when the Job Log space in the HDD is full.
[Restrict]	Displays, when the Job Log space in the HDD is full, an alarm indicating that no more Job Logs can be stored and stops storing Job Logs. After this event, no more jobs will be accepted.

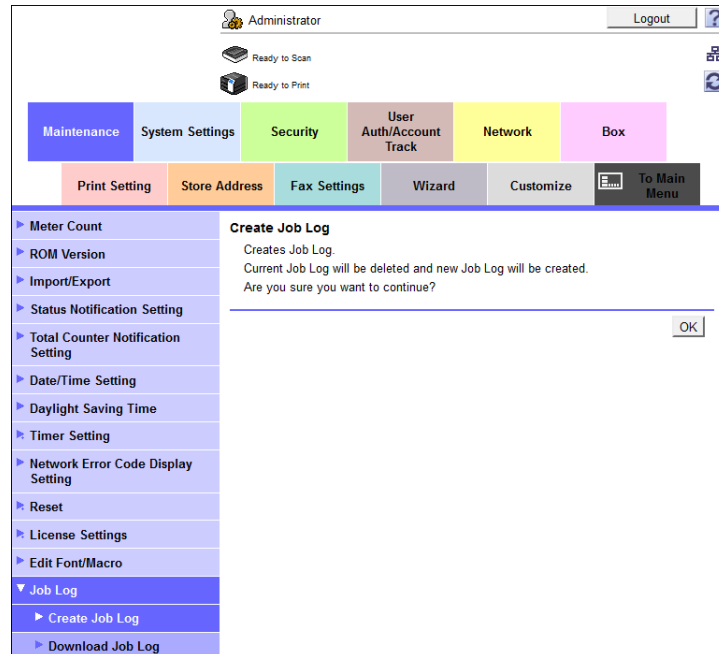
- If [Allow] is set for [Overwrite], illegal operations performed from an external environment (such as repeated log-on procedures performed over the network) make the Job Log space full of data within a short period of time, so that older Job Log data is deleted. To avoid such a situation, the administrator should download the Job Log data at regular intervals or select [Restrict] for [Overwrite]. For details of downloading of the Job Log data, see page 2-77.
- If [Restrict] is selected for [Overwrite], the administrator should download Job Log data at regular intervals to thereby delete Job Logs from the machine and to ensure that the Job Log space in the HDD is not full. For details of downloading of the Job Log data, see page 2-77.
- If the setting for [Overwrite] is switched from [Restrict] to [Allow] after saving of Job Logs is started, overwriting is enabled with the Job Logs saved so far left as they are.
- If the setting for [Overwrite] is switched from [Allow] to [Restrict] after saving of Job Logs is started, overwriting is prohibited with all previously saved Job Logs deleted.
- Touching [Erase Job Log] erases all Job Logs saved in the machine.

- 4 Click [OK].
When the machine is restarted, it starts obtaining Job Logs.

2.17.2 Downloading the Job Log data

- ✓ For the procedure to access the Admin Mode, see page 2-2.
- ✓ Do not leave the machine with the Admin Mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin Mode.

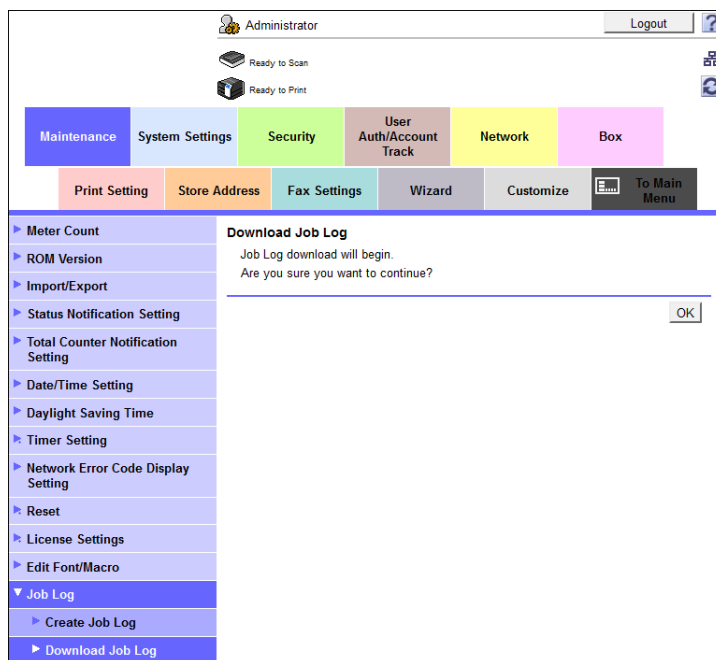
- 1 Start **Web Connection** and access the Admin Mode.
- 2 Click the [Maintenance] tab.
- 3 Click [Job Log] - [Create Job Log] from the menu.
- 4 Click [OK]. This starts creating job log data.



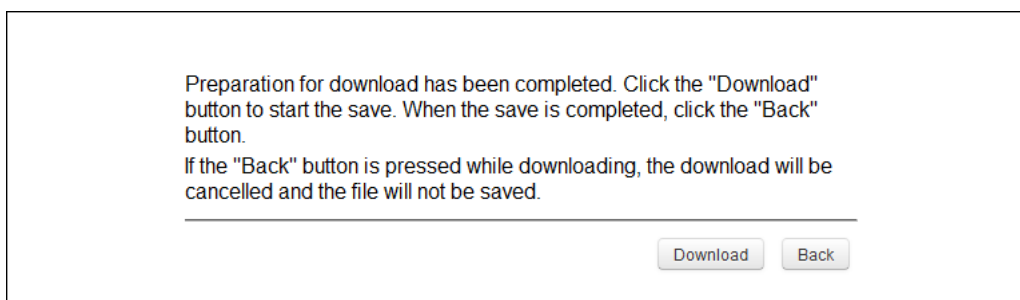
- If no Job Logs are saved in the machine, the machine displays an error message indicating that no Job Log data to be created is available.
- When the Job Log data is successfully created, the Job Log in the machine is deleted.
- The sequence of creating the Job Log data continues even when the browser is closed during the creating sequence. Restart the **Web Connection** and check that the Job Log data has been created.
- If any job logs have not been obtained, download them before creating new job log data. The job logs that have not been obtained are deleted when the new job log data is created.

- 5 Click [OK].
- 6 Click [Job Log] - [Download Job Log] from the menu.

7 Click [OK].



8 Click [Download].
This starts downloading the job log data.



- If a message appears indicating that a Job Log data file size is too large to be output, try to create the Job Log data yet to be obtained after downloading is completed.
- Only the administrator may handle the Job Log data that has been downloaded.
- The administrator should download the Job Log data at regular intervals to thereby ensure that the machine is properly used.

Job Log data

The Job Log data is read in an XML format file. The file allows various types of information to be determined, including the time/date information of log collection, information on user operations, job types, and job results.

The Job Log data represents chronological records of both "log relating to jobs" and "log relating to operations."

A network communication failure may be analyzed in detail by referring to the operation code, IF code, result code, and the like.

<Log relating to jobs>

Tag name	Tag description	Typical display	Description
ColTim	Log collection time/date	2012/4/1 12:34	Time-of-day and date when the log is collected. Time/date information of the machine is used.
LogID	Log ID	0000000001	ID number assigned to the log.
JobNam	Job name	User X	The name of the job. If a user name is known, the user name is shown.
JobTyp	Job type	1	Denotes the type of the job. [1]: Copy [2]: Print [3]: Scan [4]: Fax [5]: Fax/scan broadcast and others
JobEntTim	Job registration time/date	2012/4/1 12:34	Time/date when the job is registered.
JobFinTim	Job finish time/date	2012/4/1 12:34	Time/date when the job is finished.
Opelnf	Operator information	-	Operator who registers the job. The operator information is displayed when user operation is involved.
OpeCode	Operator code	268435457	Coded operator information. [0]: Unknown user [16777216]: Service engineer [33554432]: Administrator [83886080]: System (machine) [268435456+X]: User (X denotes a number assigned to the user) and others
OpeNam	Operator name	User X	Name of the operator.
TrcCode	Account code	268435457	Coded account information. [0]: Unknown account [67108864]: Administrator [268435456+X]: Account (X denotes a number assigned to the account) and others
TrcNam	Account name	Account X	Name of the account.

Tag name	Tag description	Typical display	Description
IFNo	Interface name	16	Denotes the interface with which the job is performed [16]: Control panel [32]: Printer reception [64]: Fax reception [80]: System [96]: Web Connection [112]: TCP Socket [128]: OpenAPI* [200]: IPP (AirPrint printing, Mopria printing, IPP printing) [240]: IWS and others * May be recorded as OpenAPI even when the Web Connection is used.
JobResInf	Job result	-	Result of the job.
JobRes	Job result	0	Denotes the result of the job. [0]: Normally terminated [513]: Deleted by user and others
ScProc	Scan process	-	Scan process information.
ActStTim	Scan start time/date	2012/4/1 12:34	Time/date when the scan operation is started.
ActFinTim	Scan finish time/date	2012/4/1 12:34	Time/date when the scan operation is finished.
Res	Scan process result	0	Result of the scan process. [0]: Normally terminated [65535]: Abnormally terminated
PrtProc	Print process	-	Print process information.
Res	Print process result	0	Result of the print process. [0]: Normally terminated [65535]: Abnormally terminated
ProcNetTX	Network transmission process	-	Network transmission process information.
Protocol	Protocol/address type	7	Denotes the protocol/address type used for transmission. The Web Connection protocol is HTTP. [7]: HTTP [241]: Box and others
Port	Port number	50001	Denotes the port number used during transmission.
DstInf	Destination information	XXX.XXX.XXX.XXX	Denotes information on the destination.
FileNam	File name	SCXXX.pdf	Denotes the name of the transmission file.
Res	Network transmission process result	0	Result of the network transmission process. [0]: Normally terminated [65535]: Abnormally terminated
NetFaxProcTX	Network fax transmission process	-	Information on the network fax transmission process.
Res	Network fax transmission process result	0	Result of the network fax transmission process. [0]: Normally terminated [65535]: Abnormally terminated

Tag name	Tag description	Typical display	Description
NetFaxPro-cRX	Network fax reception process	-	Information on the network fax reception process.
Res	Network fax reception process result	0	Result of the network fax reception process. [0]:Normally terminated [65535]:Abnormally terminated
FaxProcTX	Fax transmission process	-	Information on the fax transmission process.
ActTimTX	Time/date of transmission	2012/4/1 12:34	Denotes the time/date of transmission.
DstInfTX	Destination information	00-0000-0000	Denotes information on the destination.
Res	Fax transmission process result	0	Result of the fax transmission process. [0]: Normally terminated [65535]: Abnormally terminated
FaxProcRX	Fax reception process	-	Information on the fax reception process.
ActTimRX	Time/date of reception	2012/4/1 12:34	Denotes the time/date of reception.
DstInfRX	Transmitter information	00-0000-0000	Denotes information on the transmitter.
Res	Fax reception process result	0	Result of the fax reception process. [0]: Normally terminated [65535]: Abnormally terminated
BxRdProc	Retrieve from box process	-	Information on the process of retrieving from box.
BoxNo	Box number	XXXXXXXXXX	Denotes the number assigned to the box from which the document is to be retrieved. [0]: Memory RX Box [1000020130]: Password Encrypted PDF Box [1000020150]: ID & Print box [1000030040]: Secure Print box [1 to 999999999]: Displays the box number if it has been registered, such as with a Public User Box or an Annotation Box. and others
DcNam	Document name	XXXXX	Denotes the name of the document to be retrieved from the box.
Res	Retrieve from box process result	0	Result of the process of retrieving from box. [0]: Normally terminated [65535]: Abnormally terminated
BxWtProc	Save to box process	-	Information on the process of saving data in box.
WtBxNo	Box number	XXXXXXXXXX	Denotes the number assigned to the box in which the document is to be stored. [0]: Memory RX Box [1000020130]: Password Encrypted PDF Box [1000020150]: ID & Print box [1000030040]: Secure Print box [1 to 999999999]: Displays the box number if it has been registered, such as with a Public User Box or an Annotation Box. and others
WtDcNam	Document name	XXXXX	Denotes the name of the document to be stored in the box.

Tag name	Tag description	Typical display	Description
Res	Save to box process result	0	Result of the process of saving data in the box. [0]: Normally terminated [65535]: Abnormally terminated
PrtProcRX	Network reception process	-	Information on the network reception process.
Res	Network reception process result	0	Result of the network reception process. [0]: Normally terminated [65535]: Abnormally terminated
ExtOutProc	External output process	-	Information on the external output process.
Res	External output process result	0	Result of the external output process. [0]: Normally terminated [65535]: Abnormally terminated

<Log relating to operations>

Tag name	Tag description	Typical display	Description
Code	Operation code	1281	<p>Denotes the specific operation performed.</p> <p>[1]: Turning ON or OFF the log function</p> <p>[2]: Log overflow</p> <p>[3]: Deleting log</p> <p>[4]: Missing log detected *</p> <p>[257]: Service mode authentication (logon)</p> <p>[258]: Service mode authentication (logoff)</p> <p>[259]: Shift to locked state upon Service Mode authentication failure</p> <p>[260]: Canceling the lock state when Service Mode authentication fails</p> <p>[263]: Changing the service authentication password in the Service Mode</p> <p>[264]: Changing the service authentication mode in the Service Mode (Changing CE authentication mode)</p> <p>[265]: Changing the release time setting in the Service Mode</p> <p>[272]: Changing the administrator password in the Service Mode</p> <p>[513]: Administrator Mode authentication (logon)</p> <p>[514]: Administrator Mode authentication (logoff)</p> <p>[515]: Shift to locked state upon Administrator Mode authentication failure</p> <p>[516]: Canceling the lock state when the Administrator Mode authentication fails</p> <p>[517]: Changing the administrator password in the Administrator Mode</p> <p>[518]: Authentication for the Administrator Mode</p> <p>[521]: Administrator Mode authentication by User Administrator (logon)</p> <p>[522]: Administrator Mode authentication by User Administrator (logoff)</p> <p>[523]: Shift to locked state upon Administrator Mode authentication failure by User Administrator</p> <p>[525]: Changing the administrator password in the Administrator Mode by User Administrator</p> <p>[526]: Authentication for the Administrator Mode by User Administrator</p> <p>[785]: Changing the authentication mode setting in the Administrator Mode</p> <p>[804]: Canceling the lock state when the user/account authentication fails in the Administrator Mode</p> <p>[805]: Registering a user in the Administrator Mode</p> <p>[806]: Deleting a user in the Administrator Mode</p> <p>[807]: Changing a user password in the Administrator Mode</p> <p>[809]: Changing a user attribute in the Administrator Mode</p> <p>[810]: Writing user information in the Administrator Mode (batch writing)</p> <p>[811]: Registering a user (automatic registration)</p> <p>[812]: Setting/changing the account to which a user belongs in the Administrator Mode</p> <p>[813]: Temporarily suspending or resuming use by a user in the Administrator Mode</p> <p>[814]: Changing the function permission for a user in the Administrator Mode</p> <p>[821]: Registering an account in the Administrator Mode</p> <p>[822]: Deleting an account in the Administrator Mode</p>

Tag name	Tag description	Typical display	Description
Code	Operation code	1281	<p>[823]: Changing an account password in the Administrator Mode</p> <p>[825]: Changing an account attribute in the Administrator Mode</p> <p>[826]: Writing account information in the Administrator Mode (batch writing)</p> <p>[827]: Changing an account name in the Administrator Mode</p> <p>[828]: Temporarily suspending or resuming use by an account in the Administrator Mode</p> <p>[829]: Changing the function permission for an account in the Administrator Mode</p> <p>[835]: Canceling the lock of a box in the Administrator Mode</p> <p>[837]: Registering a box in the Administrator Mode</p> <p>[838]: Deleting a box in the Administrator Mode</p> <p>[839]: Changing a box password in the Administrator Mode</p> <p>[841]: Changing a box attribute in the Administrator Mode</p> <p>[842]: Writing box information in the Administrator Mode (batch writing)</p> <p>[843]: Deleting document in a batch from box in the Administrator Mode</p> <p>[851]: Canceling the lock state when secure print authentication fails in the Administrator Mode</p> <p>[856]: Changing ID & Print setting in the Administrator Mode</p> <p>[865]: Changing the "user change permission" setting in address settings in the Administrator Mode</p> <p>[869]: Preparing, changing, or deleting address data in the Administrator Mode</p> <p>[874]: Writing address data in the Administrator Mode (batch writing)</p> <p>[875]: Registering, changing, or deleting a S/MIME certificate in the Administrator Mode</p> <p>[883]: Canceling the lock state when authentication fails with Write authority in SNMPv3 in the Administrator Mode</p> <p>[884]: Canceling the lock state when WebDAV access authentication fails in the Administrator Mode</p> <p>[885]: Canceling the lock state when access authentication for the remote panel fails in the Administrator Mode</p> <p>[886]: [Currently Not Used] Canceling the lock state when authentication for FTP printing fails</p> <p>[887]: Setting the time adjustment function in the Administrator Mode</p> <p>[1025]: Enhanced security setting in the Administrator Mode</p> <p>[1026]: Changing the password rule setting in the Administrator Mode</p> <p>[1027]: Changing the User Box Administrator Setting in the Administrator Mode</p> <p>[1028]: Changing an operation prohibited function when the authentication fails in the Administrator Mode</p> <p>[1029]: Changing the HDD lock password setting in the Administrator Mode</p> <p>[1030]: Changing the HDD lock password in the Administrator Mode</p> <p>[1031]: Changing the Overwrite HDD Data setting in the Administrator Mode</p> <p>[1032]: Changing the Print Data Capture setting in the Administrator Mode</p>

Tag name	Tag description	Typical display	Description
Code	Operation code	1281	<p>[1033]: Registering a digital certificate in the Administrator Mode</p> <p>[1034]: Network setting change in the Administrator Mode</p> <p>[1035]: Changing the HDD encryption setting in the Administrator Mode</p> <p>[1036]: Changing the HDD encryption word in the Administrator Mode</p> <p>[1037]: Changing the overwrite log setting in the Administrator Mode</p> <p>[1038]: Changing the release time settings in the Administrator Mode</p> <p>[1039]: Changing the check count for Prohibited Functions When Authentication Error in the Administrator Mode</p> <p>[1040]: Changing a digital certificate used in the protocol in the Administrator Mode</p> <p>[1041]: Changing the TPM setting in the Administrator Mode</p> <p>[1042]: Changing the administrator password change permission setting in the Administrator Mode</p> <p>[1043]: Changing the administrator password change permission individual setting in the Administrator Mode</p> <p>[1044]: Changing firmware update setting in the Administrator Mode</p> <p>[1045]: Changing firmware update password in the Administrator Mode</p> <p>[1050]: Setting the USB Connection Permission setting in the Administrator Mode</p> <p>[1054]: Setting the USB Connection Permission setting in the Administrator Mode (batch)</p> <p>[1281]: User authentication (logon)</p> <p>[1282]: User authentication (logoff)</p> <p>[1283]: Shift to locked state in user authentication</p> <p>[1287]: Changing the user password by a user</p> <p>[1290]: User authentication (auto logoff)</p> <p>[1291]: Setting or changing the account to which a particular user belongs by the user</p> <p>[1297]: Account authentication (logon)</p> <p>[1298]: Account authentication (logoff)</p> <p>[1299]: Shift to locked state in account authentication</p> <p>[1300]: Account authentication (auto logoff)</p> <p>[1313]: Authentication by Write authority in SNMPv3 (password matching only)</p> <p>[1314]: Shift to locked state when authentication by Write authority in SNMPv3 fails</p> <p>[1315]: Authentication by WebDAV access (password matching only)</p> <p>[1316]: Shift to locked state when authentication by WebDAV access fails</p> <p>[1317]: Authentication by remote panel access (password matching only)</p> <p>[1318]: Shift to locked state when authentication by remote panel access fails</p> <p>[1321]: Authentication by WebDAV access (ID/password)</p> <p>[1322]: Changing WebDAV server password</p> <p>[1409]: Failure in secure communication (SSL/TLS) (Https)</p> <p>[1410]: Failure in secure communication (SSL/TLS) (OpenAPI)</p> <p>[1411]: Failure in secure communication (SSL/TLS) (TCP Socket)</p> <p>[1412]: Failure in secure communication (SSL/TLS) (WebDAV)</p>

Tag name	Tag description	Typical display	Description
Code	Operation code	1281	<p>[1413]: Failure in secure communication (SSL/TLS) (IPPS)</p> <p>[1414]: Failure in secure communication (IPsec)</p> <p>[1537]: Box authentication by user (ID/password matching only)</p> <p>[1539]: Shift to locked state when box authentication by user fails</p> <p>[1541]: Box registration by user</p> <p>[1542]: Deleting the User Box by user</p> <p>[1543]: Changing the User Box Password by user</p> <p>[1545]: Changing the User Box attribute by user</p> <p>[1558]: Deleting document from box by user</p> <p>[1562]: Changing document name in box by user</p> <p>[1563]: Moving documents across boxes by user</p> <p>[1564]: Copying documents in box by user</p> <p>[1565]: Changing document in box by user (modify and write in document)</p> <p>[1569]: Authentication of access to Secure Print document by user (ID/password matching only)</p> <p>[1571]: Shift to the lock state when authentication of access to Secure Print document fails by user</p> <p>[1574]: Deleting Secure Print document by user</p> <p>[1577]: Changing Secure Print document attribute by user</p> <p>[1792]: Report/list print</p> <p>[1825]: Backup, export</p> <p>[1826]: Restore, import</p> <p>[2561]: Turning main power switch ON</p> <p>[2577]: Turning main power switch OFF</p> <p>[3000]: Registering application in the Administrator Mode</p> <p>[3001]: Application expiration date in the Administrator Mode</p> <p>[3002]: Setting restriction code list in the Administrator Mode</p> <p>[3003]: Deleting restriction code list in the Administrator Mode</p> <p>[3073]: Changing time/date in the Administrator Mode (manual setting)</p> <p>[3074]: Changing time/date in the Administrator Mode (auto correction)</p> <p>[3075]: Changing the system auto reset time in the Administrator Mode</p> <p>[3076]: Changing the auto logoff time in the Administrator Mode</p> <p>[3077]: Daylight saving time setting in the Administrator Mode</p> <p>[3329]: Changing the S/MIME setting in the Administrator Mode</p> <p>[3330]: Changing the S/MIME encryption strength in the Administrator Mode</p> <p>[3331]: Changing the SNMPv3 Write Auth/Priv password in the Administrator Mode</p> <p>[3332]: Changing the SNMPv3 Write authentication level in the Administrator Mode</p> <p>[3333]: Changing the SSL/TLS strength setting in the Administrator Mode</p> <p>[3337]: Changing the SMB signature setting (client)</p> <p>[3338]: Changing the SMB signature setting (server)</p> <p>[3585]: Changing the TSI reception setting in the Administrator Mode</p> <p>[3841]: Changing the management role and others</p> <p>* Displayed if there is a logon event but not a logoff event, such as when the machine develops a fault after a user logged on, so that the user was unable to log off.</p>

Tag name	Tag description	Typical display	Description
Tim	Time/date of operation	2012/4/1 12:34	Denotes time/date when the operation is performed.
ResCode	Result code	0	Denotes the result of operation. [0]: Normally terminated [257]: Authentication failed and others
OperatCont	Details of operation	1	Denotes the specific detail of operation. [1]: Enable [2]: Disable and others
BoxOperat	Box operation information	-	Denotes information on box operation.
TrgBoxNo	Box number to be operated	XXXXXXXXXX	Denotes the box number relative to box operations or document operations in a box. [0]: Memory RX Box [1000020130]: Password Encrypted PDF Box [1000020150]: ID & Print box [1000030040]: Secure Print box [1 to 999999999]: Displays the box number if it has been registered, such as with a Public User Box or an Annotation Box. and others
MovBoxNo	Move destination box number	XXXXXXXXXX	Denotes the number assigned to the box to which the document in question is to be moved.
CpyBoxNo	Copy destination box number	XXXXXXXXXX	Denotes the number assigned to the box to which the document in question is to be copied.
SecretID	Secure Print ID	XXXXX	Denotes the ID used for accessing a Secure Print document
Authorization	Authorization code	4095	Denotes the right possessed by the corresponding user [0]: No right (Disable) [4095]: Administrative right [4096]: Box administrative right

2.18 Setting time/date in machine

When a log-on to the Administrator Mode becomes successful, the machine enables setting of the time-of-day and date. Use of the network time protocol (NTP) server allows the current time/date to be adjusted automatically.

NOTICE

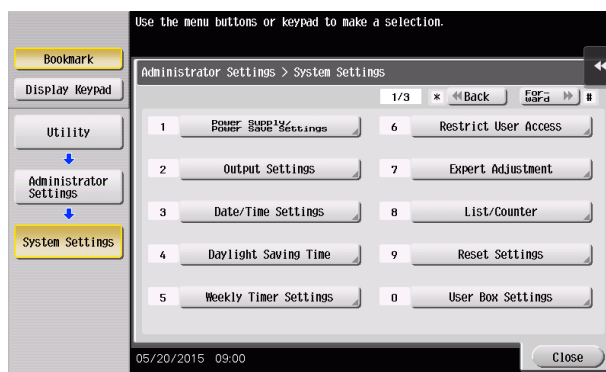
If the NTP server is to be used, make sure that the NTP server is a correct one and take necessary action to protect communications between the NTP server and the machine.

2.18.1 Setting time/date

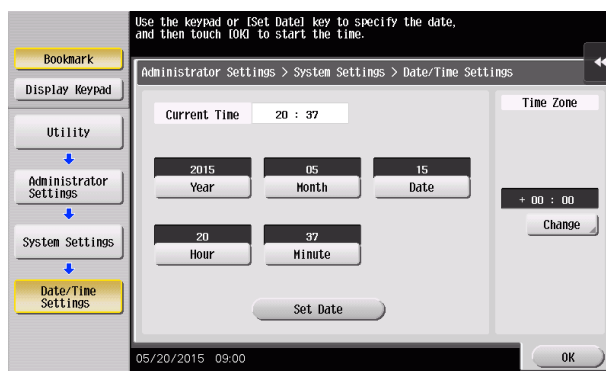
<From the Control Panel>

- ✓ For the procedure to call the System Settings screen on the display, see steps 1 and 2 of page 2-36.
- ✓ Do not leave the machine with the setting screen of Administrator Mode left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Mode.

- 1 Call the System Settings screen on the display from the control panel.
- 2 Touch [Date/Time Settings]



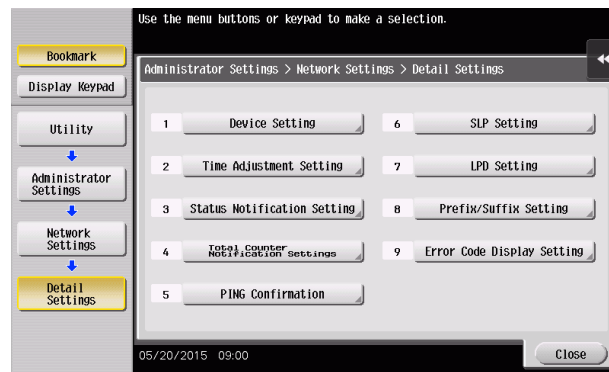
- 3 Select the item to be set. Then, touch [C] and next set the time-of-day and date. Touching [Set Date] lets the NTP server to adjust the current time/date automatically.



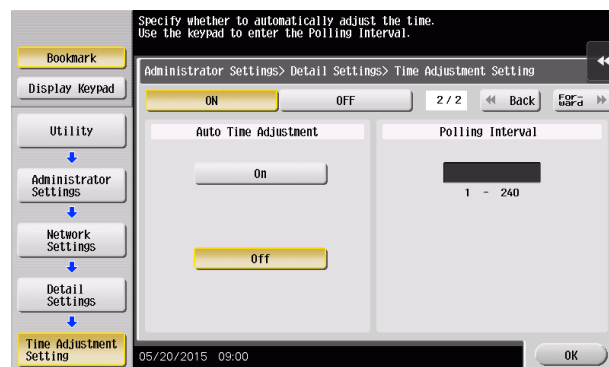
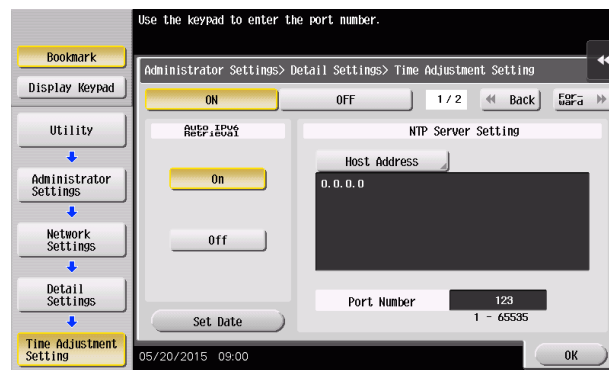
- Touch [Display Keypad] to display the keypad.
- If [Set Date] is to be used for the setting, set the time difference from the coordinated universal time (UTC) using [Time Zone].
- [Set Date] can be used if the NTP server is registered. For more details, make settings of step 5 and onward.

- 4 Touch [OK].

- 5 Touch [Administrator Settings] - [Network Settings] - [Forward] - [Detail Settings] - [Time Adjustment Setting].



- 6 Select [ON], and make the necessary settings.



→ If [Auto Time Adjustment] is set to [On], the machine connects to the NTP server at regular intervals to thereby adjust the time-of-day and date. In this case, use [Polling Interval] to set the interval at which the time/date adjustment is to be made (unit: hours).

- 7 Touch [OK].

<From **Web Connection**>

- ✓ For the procedure to access the Admin Mode, see page 2-2.
- ✓ Do not leave the machine with the Admin Mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin Mode.

- 1 Start **Web Connection** and access the Admin Mode.
- 2 Click the [Maintenance] tab.
- 3 Click [Date/Time Setting] - [Manual Setting] from the menu.
- 4 Enter the time-of-day and date and click [OK].

The screenshot shows the Web Connection Admin Mode interface. At the top, there's a header with 'Administrator' and a 'Logout' button. Below the header, there are status indicators: 'Ready to Scan' and 'Ready to Print'. A navigation bar contains several tabs: 'Maintenance', 'System Settings', 'Security', 'User Auth/Account Track', 'Network', and 'Box'. Below this, there's a sub-navigation bar with 'Print Setting', 'Store Address', 'Fax Settings', 'Wizard', 'Customize', and 'To Main Menu'. The main content area is divided into two sections. On the left, there's a list of settings: 'Meter Count', 'ROM Version', 'Import/Export', 'Status Notification Setting', 'Total Counter Notification Setting', 'Date/Time Setting' (expanded), 'Manual Setting' (selected), 'Time Adjustment Setting', and 'Daylight Saving Time'. On the right, the 'Manual Setting' form is displayed. It has fields for 'Date' (Year: 2015, Month: 5, Day: 15) and 'Time' (Hour: 23, Minute: 44, Time Zone: GMT 0:00). At the bottom right of the form are 'OK' and 'Cancel' buttons.

→ To correct the time-of-day, use [Time Zone] to set the time difference from the coordinated universal time (UTC).

- 5 Check that a message indicating that the setting is completed appears. Then, click [OK].

→ To correct the time-of-day using the NTP server, make the following settings.

- 6 Click [Date/Time Setting] - [Time Adjustment Setting] from the menu.
- 7 Click [ON] from the pull-down menu of [Time Adjustment Setting], and make the necessary settings.

The screenshot shows the Web Connection Admin Mode interface, similar to the previous one, but with the 'Time Adjustment Setting' selected in the left menu. The main content area shows the 'Time Adjustment Setting' form. It has a 'Time Adjustment Setting' dropdown menu set to 'ON'. Below it are fields for 'Auto IPv6 Retrieval' (set to 'ON'), 'NTP Server Address' (with a note 'Please check to enter host name.' and a value of '0.0.0.0'), 'Port No.' (set to '123' with a range '(1-65535)'), 'Auto Time Adjustment' (set to 'OFF'), and 'Polling Interval' (set to '24' with a range '(1-240)'). At the bottom right of the form are 'Adjust', 'OK', and 'Cancel' buttons.

→ If [Auto Time Adjustment] is set to [ON], the machine connects to the NTP server at regular intervals to thereby adjust the time-of-day and date. In this case, use [Polling Interval] to set the interval at which the time/date adjustment is to be made (unit: hours).

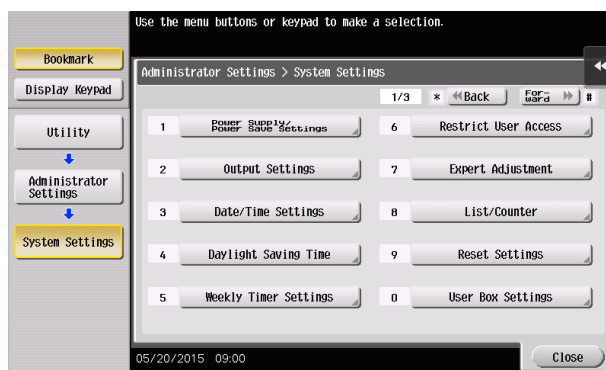
- 8 Click [Adjust].
- 9 Check that a message indicating that the adjustment is completed appears. Then, click [OK].

2.18.2 Setting daylight saving time

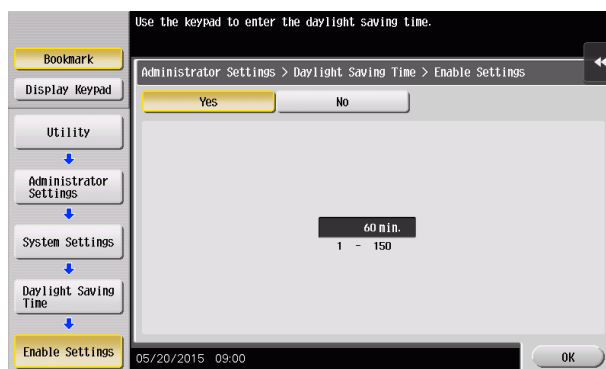
<From the Control Panel>

- ✓ For the procedure to call the System Settings screen on the display, see steps 1 and 2 of page 2-36.
- ✓ Do not leave the machine with the setting screen of Administrator Mode left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Mode.

- 1 Call the System Settings screen on the display from the control panel.
- 2 Touch [Daylight Saving Time] - [Enable Settings].

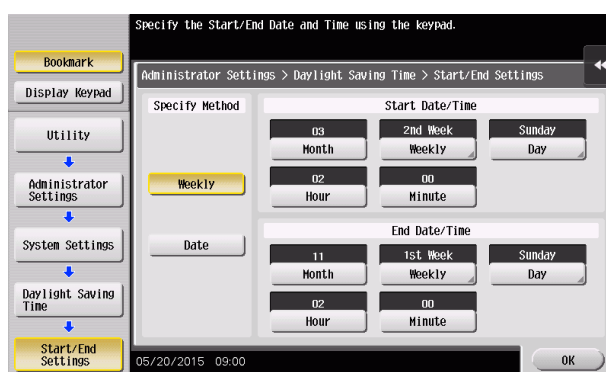


- 3 Select [Yes]. Then, touch [C] and enter time to be advanced as the daylight saving time.



- Touch [Display Keypad] to display the keypad.
- The current time is set forward to reflect daylight saving time.

- 4 Touch [OK].
- 5 Touch [Start/End Settings].
- 6 Select [Weekly] or [Daily]. Then, specify the start date/time and the end date/time of a period of time to which the daylight saving time is applicable.



- 7 Touch [OK].

<From **Web Connection**>

- ✓ For the procedure to access the Admin Mode, see page 2-2.
- ✓ Do not leave the machine with the Admin Mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin Mode.

- 1 Start **Web Connection** and access the Admin Mode.
- 2 Click the [Maintenance] tab.
- 3 Click [Daylight Saving Time] from the menu.
- 4 Select [ON] from the pull-down menu of [Daylight Saving Time], and enter time to be advanced as the daylight saving time.
From the [Specify Method] pull-down menu, select [Weekly] or [Day] and specify the start date/time and the end date/time of a period of time to which the daylight saving time is applicable.

The screenshot shows the Web Connection Admin Mode interface. At the top, there is a header bar with 'Administrator' and a 'Logout' button. Below this is a status bar showing 'Ready to Scan' and 'Ready to Print'. The main navigation area consists of several tabs: Maintenance, System Settings, Security, User Auth/Account Track, Network, and Box. Below these are more specific settings tabs: Print Setting, Store Address, Fax Settings, Wizard, Customize, and To Main Menu. The 'Daylight Saving Time' settings are currently selected. On the left, a list of settings is shown, with 'Daylight Saving Time' highlighted. The main area contains the following fields:

- Daylight Saving Time**: A pull-down menu set to 'ON'.
- Daylight Saving Time**: A text input field set to '60' with a label 'Minute (1-150)'.
- Specify Method**: A pull-down menu set to 'Day'.
- Start Date/Time**: Fields for Month, Day, Weekly (set to '1st Week'), Day (set to 'Sun'), Hour, and Minute.
- End Date/Time**: Fields for Month, Day, Weekly (set to '1st Week'), Day (set to 'Sun'), Hour, and Minute.

At the bottom right, there are 'OK' and 'Cancel' buttons.

- 5 Click [OK].
- 6 Check that a message indicating that the adjustment is completed appears. Then, click [OK].

2.19 SSL Setting Function

When a log-on to the Administrator Mode becomes successful, the machine enables the setting of encryption of image data transmitted and received between the PC and the machine.

NOTICE

Do not use 1024-bit RSA and SHA-1 after 2014, as an increased risk results of data to be protected being tampered with or leaked.

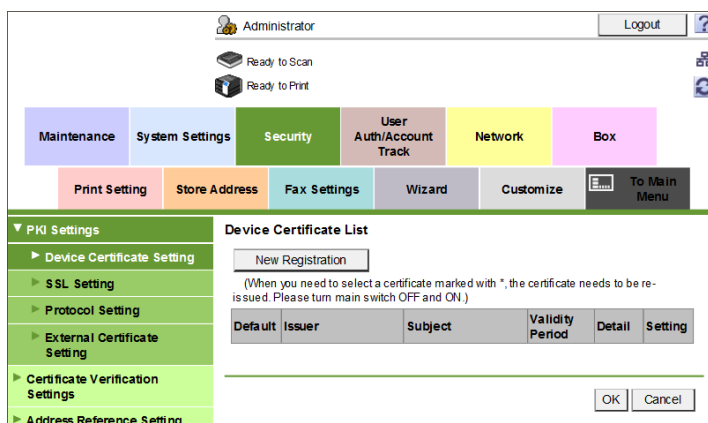
2.19.1 Device Certificate Setting

- ✓ For the procedure to access the Admin Mode, see page 2-2.
- ✓ Do not leave the machine with the Admin Mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin Mode.
- ✓ RSA-1024_SHA-1 is selected as the type of the encryption key for setting the device certificate. To ensure security, change the type of the encryption key to RSA-2048_SHA-256 before preparing a certificate.

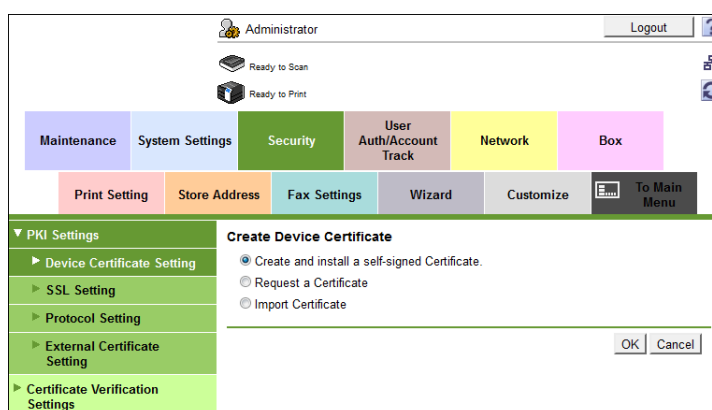
1 Start **Web Connection** and access the Admin Mode.

2 Click the [Security] tab.

3 Click [New Registration].



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



5 Make the necessary settings.

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

6 Click [OK]. The certificate can now be registered.

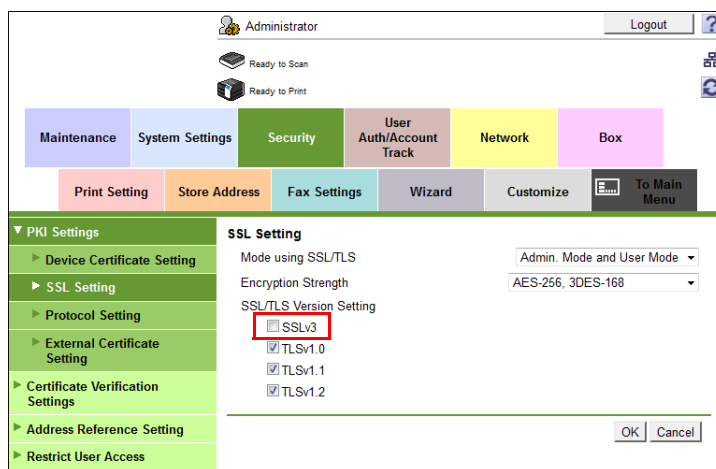
2.19.2 SSL Setting

④ Related setting (for the administrator)

When making the SSL Setting, be sure to make sure in advance that the device certificate has been registered in the machine. For the procedure to register the device certificate, see page 2-93.

- ✓ For call the PKI Settings screen on the display, see steps 1 and 2 of page 2-93.
- ✓ Do not leave the machine with the Admin Mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin Mode.

- 1 Start **Web Connection** and call the PKI Settings screen on the display.
- 2 Click [SSL Setting] from the menu.
- 3 Set "Mode using SSL/TLS" and "Encryption Strength" and click [OK].



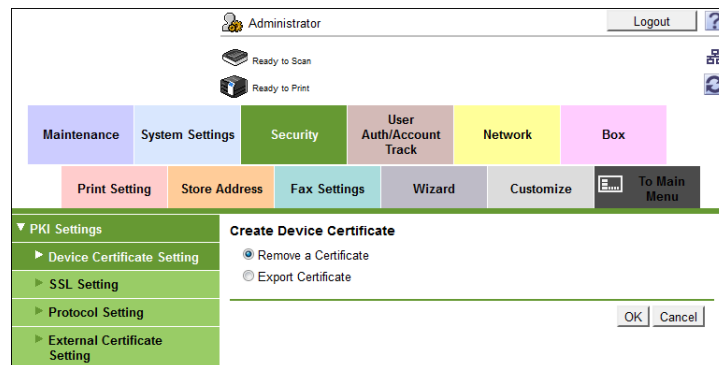
- Select "Admin. Mode and User Mode" for "Mode using SSL/TLS."
- For encryption strength, select the strong "AES-256, 3DES-168." Note, however, selecting "AES-256, 3DES-168" does not allow the encryption strength to connect in 3DES.
- The Enhanced Security Mode is canceled, if setting containing strength lower than AES/3DES is selected when the Enhanced Security Mode is [ON].
- Cancel the selection of "SSLv3" of SSL/TLS Version Setting.

- 4 Click [OK].

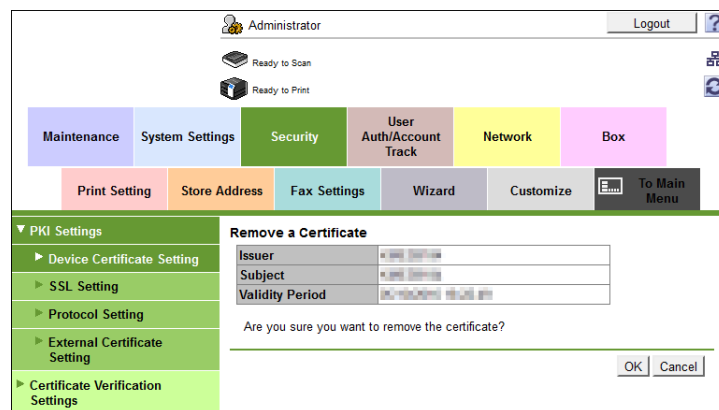
2.19.3 Removing a Certificate

- ✓ For call the PKI Settings screen on the display, see steps 1 and 2 of page 2-93.
- ✓ Do not leave the machine with the Admin Mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin Mode.
- ✓ In the Enhanced Security Mode, no certificates can be removed.

- 1 Start **Web Connection** and call the PKI Settings screen on the display.
- 2 Click [Setting].
- 3 Select [Remove a Certificate] and click [OK].



- 4 Click [OK].



- 5 Click [OK] and restart the machine.

2.20 TCP/IP Setting Function

When a log-on to the Administrator Mode becomes successful, the machine enables setting of the IP Address and registration of the DNS Server.

2.20.1 Setting the IP Address

<From the Control Panel>

- ✓ For the procedure to call the Administrator Mode on the display, see page 2-2.
 - ✓ Do not leave the machine with the setting screen of Administrator Mode left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Mode.
- 1 Call the Administrator Mode screen on the display from the control panel.
 - 2 Touch [Network Settings].
 - 3 Touch [TCP/IP Settings].
 - 4 Touch [IPv4 Settings].
 - 5 Touch [Manual Input].
 - 6 Select [IP Address] and set the IP Address.
 - If [Auto Input] is selected for IP Application Method in step 4, select the means of acquiring the IP Address automatically from among DHCP Settings, BOOTP Settings, ARP/PING Settings, AUTO IP Settings, and the like.
 - 7 Touch [OK].
 - 8 Touch [OK].
 - If a message appears that prompts you to turn OFF and ON the **main power switch**, turn OFF and ON the **main power switch**. When the **main power switch** is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. If there is no wait period between turning the **main power switch** off, then on again, the machine may not function properly.

<From **Web Connection**>

- ✓ For the procedure to access the Admin Mode, see page 2-2.
 - ✓ Do not leave the machine with the Admin Mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin Mode.
- 1 Start **Web Connection** and access the Admin Mode.
 - 2 Click the [Network] tab.
 - 3 Click [TCP/IP Setting] - [TCP/IP Setting] from the menu.
 - 4 Select [Manual Setting] from the IP Address Setting Method pull-down menu.
 - 5 Enter the IP Address in the "IP Address" box.
 - If [Auto Setting] is selected from the IP Address Setting Method pull-down menu in step 4, select the means with which to acquire the IP Address automatically, including DHCP, BootP, ARP/PING, and Auto IP setting, and click the check box.
 - 6 Click [OK].

2.20.2 Registering the DNS Server

<From the Control Panel>

- ✓ For the procedure to call the TCP/IP settings screen on the display, see steps 1 through 3 of page 2-97.
- ✓ Do not leave the machine with the setting screen of Administrator Mode left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Mode.

- 1 Call the TCP/IP Settings screen on the display from the control panel.
- 2 Make the necessary settings for the DNS Server.
 - If [Enable] is selected from the DNS Server Auto Obtain and DNS Domain Name Auto Retrieval, the DNS Server Address and DNS Domain Name are automatically acquired.
- 3 Touch [OK].
 - If a message appears that prompts you to turn OFF and ON the **main power switch**, turn OFF and ON the **main power switch**. When the **main power switch** is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. If there is no wait period between turning the **main power switch** off, then on again, the machine may not function properly.

<From **Web Connection**>

- ✓ For the procedure to access the TCP/IP Setting screen on the display, see steps 1 through 3 of page 2-97.
- ✓ Do not leave the machine with the Admin Mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin Mode.

- 1 Start the **Web Connection** and call the TCP/IP Setting screen on the display.
- 2 Enter the address in the DNS Server box.
 - If [Enable] is selected from the DNS Server Auto Obtain and DNS Domain Auto Obtain pull-down menus, the DNS Server Address and DNS Domain Name are automatically acquired.
- 3 Make the necessary settings.
- 4 Click [OK].

2.21 E-Mail Setting Function

When a log-on to the Administrator Mode becomes successful, the machine enables setting of the SMTP Server (E-Mail Server).

Setting the SMTP Server (E-Mail Server)

<From the Control Panel>

- ✓ For the procedure to call the Network Settings screen on the display, see steps 1 and 2 of page 2-97.
- ✓ Do not leave the machine with the setting screen of Administrator Mode left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Mode.

- 1 Call the Network Settings screen on the display from the control panel.
- 2 Touch [E-Mail Settings].
- 3 Touch [E-Mail TX (SMTP)].
- 4 Make the necessary settings.
- 5 Touch [OK].
- 6 Touch [Close].
 - ➔ If a message appears that prompts you to turn OFF and ON the **main power switch**, turn OFF and ON the **main power switch**. When the **main power switch** is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. If there is no wait period between turning the **main power switch** off, then on again, the machine may not function properly.

<From **Web Connection**>

- ✓ For the procedure to access the Admin Mode, see page 2-2.
- ✓ Do not leave the machine with the Admin Mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin Mode.

- 1 Start **Web Connection** and access the Admin Mode.
- 2 Click the [Network] tab.
- 3 Click [E-mail Setting] - [E-mail TX Setting (SMTP)] from the menu.
- 4 Make the necessary settings.
- 5 Click [OK].



User Operations

3 User Operations

3.1 User Authentication Function

When [ON (MFP)] or [External Server Authentication] (Active Directory) is set for Authentication Method of the Administrator Mode, the machine authenticates a user as an authorized user of this machine through the User Password that meets the Password Rules before he or she actually uses it. During the authentication procedure, the User Password entered for the authentication purpose appears as "*" or "●" on the display.

After authentication by a user is successful using the User Name and Password entered from the control panel with the ID & Print Setting function set in the machine, the user can automatically print his or her print data saved in the ID & Print User Box. Because printing occurs after user authentication is performed via the control panel of this machine, it is suitable for printing highly confidential documents. Operate the machine with the ID & Print Setting function set.

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

NOTICE

If [ON (MFP)] is set for the authentication method and [Pause] is set for a user or account by the administrator, that particular user or account cannot log onto the machine. For details, contact the administrator.

The user who is given the administrative right by the administrator can access the Administrator Mode when logging on as the user administrator. For details of logging-on, see page 2-2.

If a screen appears that warns that the job log has reached its upper limit, contact the administrator.

For the user administrator, the number of failed authentication attempts is counted as access by the same user, independent of the mode in the Administrator Mode or the User Mode that the user logs on to.

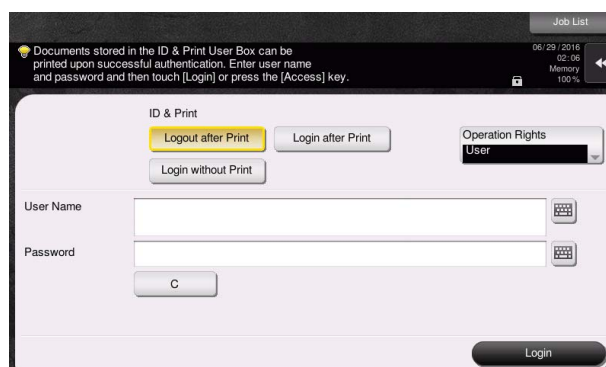
If the machine is set into the access lock state by the operation of the user administrator, the user administrator cannot log on to the Administrator Mode or the User Mode. To cancel the access lock state, the administrator must perform the Release Setting. Contact the administrator.

3.1.1 Performing user authentication

<From the Control Panel>

- ✓ Before operating the machine, the user him/herself should change the User Password from that registered by the administrator. For details of changing the User Password, see page 3-7. For details of User Name and User Password, ask the administrator.
- ✓ If the User Password is changed by the administrator during operation of this machine, the user him/herself should immediately change the User Password.
- ✓ Make absolutely sure that your User Password is not known by any other users.
- ✓ Do not leave the machine while you are in the user (account) operation mode. If it is absolutely necessary to leave the machine, be sure first to log off from the user (account) operation mode.
- ✓ If any User Name not registered with this machine is authenticated through User Authentication when [External Server Authentication] (Active Directory) is set for Authentication Method, the User Name is automatically registered with this machine.

- 1 Touch the keyboard icon in the [User Name] field.



- 2 Enter the User Name and the Password from the keyboard.



- Touch [C] to clear the value entered.
- Touch [Delete] to delete the last character entered.
- Touch [Shift] to show the upper case/symbol screen.
- Touch [Cancel] to go back to the previous screen.

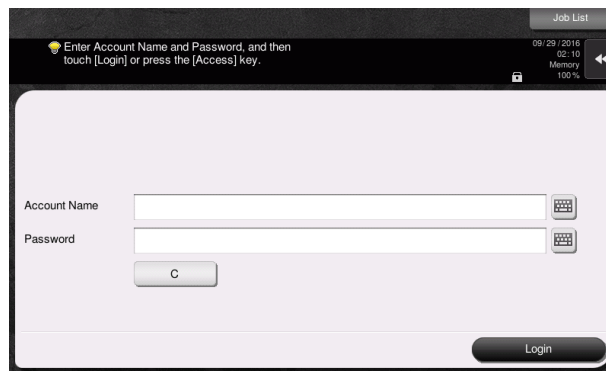
- 3 Touch [OK].

- 4 Press the **Access** key or touch [Login]. If a document is stored in the ID & Print User Box, select the target logon method and then press the **Access** key or touch [Login].

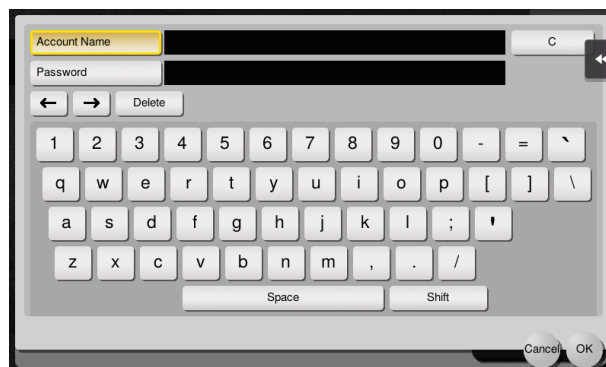
Login Method	Description
[Logout after Print]	The ID & Print document of the corresponding user is printed. After printing, the user does not log in on the machine.
[Logout without Print]	If [Logout without Print] is selected, only the ordinary login procedure is applicable and no ID & Print documents are printed.
[Login after Print]	The ID & Print document of the corresponding user is printed. After printing, the user logs in on the machine.

- If a wrong User Name is entered, a message that tells that the authentication has failed appears. Enter the correct User Name.
- If a wrong User Password is entered, a message that tells that the authentication has failed appears. Enter the correct User Password.
- If the Enhanced Security Mode is set to [ON], the entry of a wrong User Password is counted as unauthorized access. If a wrong User Password for the corresponding User Name entered is entered a predetermined number of times (once to three times) or more set by the administrator, a message appears that tells that authentication has not been successful for any subsequent operation for authentication. The machine is then set into an access lock state, rejecting any more logon attempts.
To cancel the access lock state, the administrator must perform the Release Setting. Contact the administrator.
- If there are two or more ID & Print documents are involved, all of them will be printed. To select and print only a desired document, select the **Access** key or [Login] and select the desired document from those in the ID & Print User Box. For the detailed procedure to access the ID & Print document, see page 3-6.
- Go to step 9 if User Authentication only has been set, or "Synchronize" has been set for Synchronize User Authentication & Account Track. If the account to which the user belongs has not been registered by the administrator, however, Account Track becomes necessary even with [Synchronize] set for [Synchronize User Authentication & Account Track]. Account Track is, however, necessary only for the first time. Once any account is authenticated, that particular account is registered for Account Name. The machine can thereafter be used only through User Authentication. It should be noted that this function is valid only through operation from the control panel of the machine. In operation from **Web Connection** or application software, if Account Name is not registered, you cannot log onto the mode.

- 5 Touch the keyboard icon in the [Account Name] field.



- 6 Enter the Account Name and the Password from the keyboard.



- Touch [C] to clear the value entered.
- Touch [Delete] to delete the last character entered.
- Touch [Shift] to show the upper case/symbol screen.
- Touch [Cancel] to go back to the previous screen.

- 7 Touch [OK].

- 8 Press the **Access** key or touch [Login].

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

- 9 Pressing the **Access** key will show the confirmation screen.
To log off, select [Yes].

<From **Web Connection**>

- ✓ Do not leave the machine while you are in the user (account) operation mode. If it is absolutely necessary to leave the machine, be sure first to log off from the user (account) operation mode.
- ✓ If any User Name not registered with this machine is authenticated through User Authentication when [External Server Authentication] (Active Directory) is set for Authentication Method, the User Name is automatically registered with this machine.
- ✓ Different initial screens appear after you have logged on depending on the Customize setting made by the administrator or user. The descriptions herein given are concerned with the display screen set in [Device Information] of Information.

- 1 Start the Web browser.
- 2 Enter the IP address of the machine in the address bar.
- 3 Press the [Enter] key to start **Web Connection**.
- 4 Click the Registered User radio button and enter the User Name and User Password.

- When [External Server Authentication] (Active Directory) is set for the Authentication Method, select the external authentication server from the pull-down menu of the server name.

- 5 Click [Login].

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

To cancel the access lock state, the administrator must perform the Release Setting. Contact the administrator.

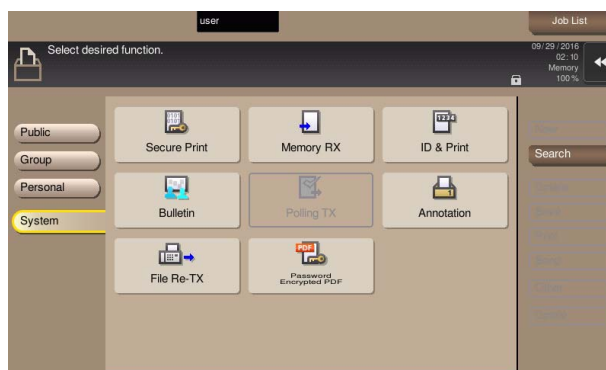
- 6 Clicking [Logout] will show the following screen.
Click [OK] to log off from the user operation mode.

3.1.2 Accessing the ID & Print Document

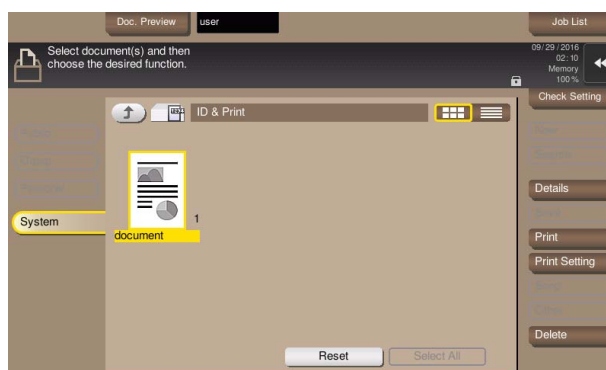
If a user, whose document is stored in the ID & Print User Box, is authenticated by **Access** key or [Login], he or she can gain access to the document in the ID & Print User Box.

- ✓ For the logon procedure, see page 3-2.
- ✓ Do not leave the machine while you are in the user operation mode. If it is absolutely necessary to leave the machine, be sure first to log off from the user operation mode.
- ✓ Save the ID & Print document through the printer driver on the PC side. As in the ordinary user authentication procedure, enter the User Name and User Password in the printer driver on the PC side and then specify [ID & Print]. The password entered is displayed as "*". If the User Password does not correspond to the User Name entered, the ID & Print document is discarded without being saved. Entry of a wrong User Password is counted as unauthorized access. If a wrong User Password is entered a predetermined number of times (once to three times) or more set by the administrator, the subsequent authentication operation is an access lock state and it is not possible to transmit the print job. As a result, the access lock state disables user authentication attempts from the control panel or **Web Connection**. To cancel the access lock state, the administrator must perform the Release Setting. Contact the administrator.
- ✓ If an attempt is made to print or save a file by specifying a user name that contains [""] (a double quotation mark), a login error results and the machine cancels the print job.
- ✓ For the user whose access to [User Box] in Function Permission is not permitted, the message appears that tells that access is not permitted for documents in the ID & Print User Box and the user cannot access the documents.

- 1 Log on to the user operation mode through user authentication from the control panel.
- 2 Touch [User Box] - [System].
- 3 Touch [ID & Print].



- 4 Select the desired ID & Print document and touch [Print].



→ To delete ID & Print document, select the specific document and touch [Delete].

- 5 To delete the document from the Box after the printing, select [Yes]. To leave the document as is, select [No].

3.2 Change Password Function

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

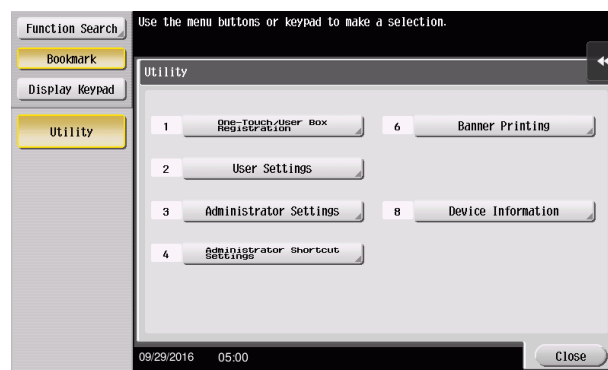
The User Password entered is displayed as "*" or "●."

Performing Change Password

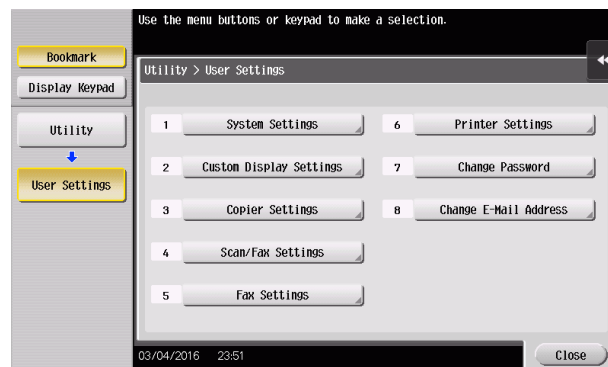
<From the Control Panel>

- ✓ For the login procedure, see page 3-2.
- ✓ Do not leave the machine while you are in the user operation mode. If it is absolutely necessary to leave the machine, be sure first to log off from the user operation mode.

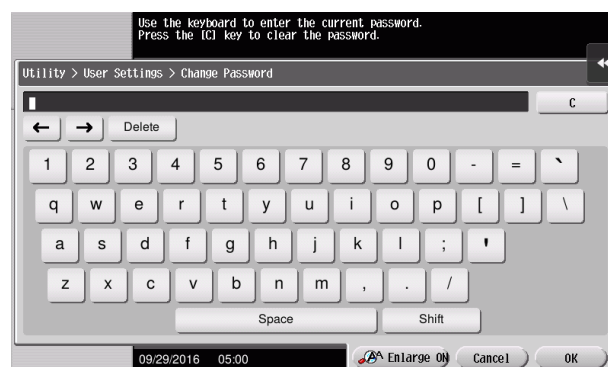
- 1 Log on to the user operation mode through User Authentication from the control panel.
- 2 Touch [Utility].
- 3 Touch [User Settings].



- 4 Touch [Change Password].



- 5 Enter the currently registered User Password from the keyboard.



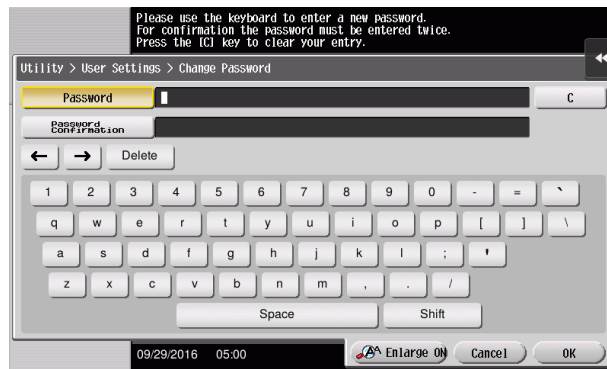
- Touch [C] to clear all characters.
- Touch [Delete] to delete the last character entered.
- Touch [Shift] to show the upper case/symbol screen.
- Touch [Cancel] to go back to the previous screen.

6 Touch [OK].

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

7 From the keyboard, enter the new User Password.

To prevent entry of a wrong password, enter the password again in [Password Confirmation].



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

8 Touch [OK].

- If the entered User Password does not meet the Password Rules, a message that tells that the entered User Password cannot be used appears. Enter the correct User Password. For details of the Password Rules, see page 1-13.
- If the entered User Password does not match, a message that tells that the User Password does not match appears. Enter the correct User Password.

<From **Web Connection**>

- ✓ For the logon procedure, see page 3-2.
- ✓ Do not leave the machine while you are in the user operation mode. If it is absolutely necessary to leave the machine, be sure first to log off from the user operation mode.

- 1 Log on to the user operation mode through User Authentication from the **Web Connection**.
- 2 Click [Change Password] on the upper right of the **Web Connection** screen.
- 3 Enter the currently registered User Password and a new User Password. Then, to make sure that you have entered the correct new password, enter the new User Password once again.

- 4 Click [OK].
 - If a wrong User Password is entered in the "Current Password" box, a message that tells that the User Password does not match appears. Enter the correct User Password.
 - If the entered User Password in the "New Password" box does not meet the Password Rules, a message that tells that the entered User Password cannot be used appears. Enter the correct User Password. For details of the Password Rules, see page 1-13.
 - If the entered User Password in the "New Password" box and "Retype New Password" box does not match, a message that tells that the User Password does not match appears. Enter the correct User Password.
- 5 Click [OK].

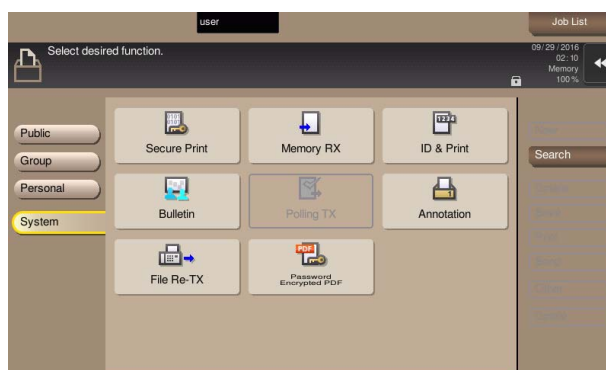
3.3 Secure Print Function

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

To access a Secure Print document, the machine authenticates a user as an authorized user of the Secure Print document file through the Secure Print Password that meets the Password Rules. The password entered is displayed as "**." When the Enhanced Security Mode is set to [ON], the number of times in which authentication fails is counted.

Accessing the Secure Print Document

- ✓ For the logon procedure, see page 3-2.
 - ✓ Do not leave the machine while you are in the user operation mode. If it is absolutely necessary to leave the machine, be sure first to log off from the user operation mode.
 - ✓ When the Enhanced Security Mode is set to [ON], go through User Authentication by entering the User Name and User Password registered in the machine through the printer driver of the PC. The password entered is displayed as "**." If the User Password does not correspond to the User Name entered, the Secure Print Job is discarded without being saved. Entry of a wrong User Password is counted as unauthorized access. If a wrong User Password is entered a predetermined number of times (once to three times) or more set by the administrator, the subsequent authentication operation is an access lock state and it is not possible to transmit the print job. As a result, the access lock state disables user authentication attempts from the control panel or **Web Connection**.
To cancel the access lock state, the administrator must perform the Release Setting. Contact the administrator.
 - ✓ Enter the Secure Print ID and password through the printer driver on the PC side. The password entered is displayed as "**."
 - ✓ For the Secure Print Password, enter the password that meets the Password Rules. Any Secure Print document, the password for which does not meet the Password Rules, will not be saved in the machine. For details of the Password Rules, see page 1-13.
 - ✓ If an attempt is made to print or save a file by specifying a user name that contains ["] (a double quotation mark), a login error results and the machine cancels the print job.
- 1 Log on to the user operation mode through User Authentication from the control panel.
 - 2 Touch [User Box] - [System].
 - 3 Touch [Secure Print].



4 Enter the Secure Print ID from the keyboard.

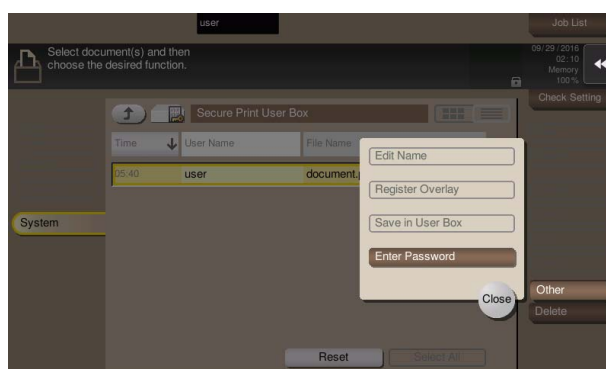


- For the Secure Print ID, enter the one that has been set on the printer driver side.
- Touch [C] to clear the value entered last.
- Touch [Delete] to delete the last character entered.
- Touch [Shift] to show the upper case/symbol screen.
- Touch [Cancel] to go back to the previous screen.

5 Touch [OK].

- If a wrong Secure Print ID is entered, the desired Secure Print document will not be displayed. Enter the correct Secure Print ID.

6 Select the desired Secure Print document and touch [Other] - [Enter Password].



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

7 Enter the Secure Print Password from the keyboard.

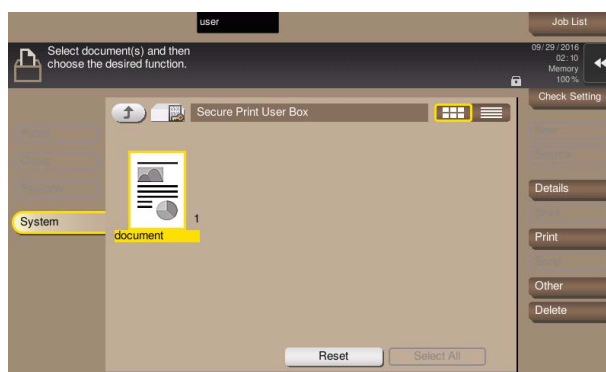


- Any Secure Print Password that does not meet the Password Rules is not accepted.
- For the Secure Print Password, enter the one that has been set on the printer driver side.
- Touch [C] to clear the value entered last.
- Touch [Delete] to delete the last character entered.
- Touch [Shift] to show the upper case/symbol screen.
- Touch [Cancel] to go back to the previous screen.

8 Touch [OK].

- If a wrong Secure Print Password is entered, a message that tells that the authentication has failed appears. Enter the correct Secure Print Password.
- If two or more Secure Print documents have been selected in step 7, the machine counts as unauthorized access any Secure Print document, the Secure Print Password of which is a mismatch.
- If the Enhanced Security Mode is set to [ON], entry of a wrong Secure Print Password is counted as unauthorized access. If a wrong Secure Print Password is entered a predetermined number of times (once to three times) or more set by the administrator, a message appears that tells that authentication has not been successful for any subsequent operation for authentication. The machine is then set into an access lock state, disabling access to the Secure Print document. To cancel the access lock state, the administrator must perform the Release Setting. Contact the administrator.

9 Touch [Print].



10 Check the details of the document and press the **Start** key.

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

3.4 User Box Function

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

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

When a user accesses a Public User Box, he or she is authenticated by a box password that meets the Password Rules. The password entered for the authentication purpose appears as "*" or "●" on the display.

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



Tips

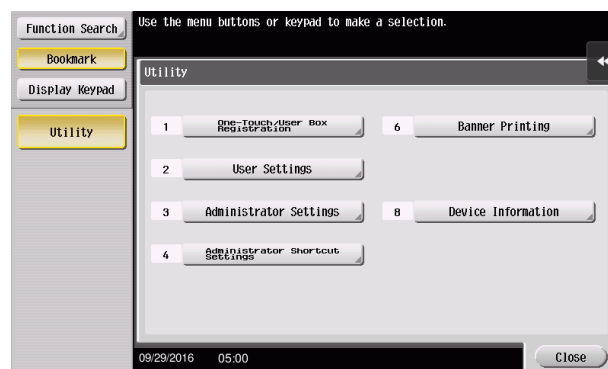
- If a document is saved in the Copy mode, Fax/Scan mode, or User Box mode selected from the control panel, by specifying a User Box number that has not been registered, a Personal User Box owned by the user who logged on through User Authentication or a Group User Box owned by the account to which the user who logged on through User Authentication belongs is automatically created. No Public User Boxes are automatically created.
- When a document is saved in a box with a box number yet to be registered specified from the PC, the Personal User Box owned by the user who logged on through User Authentication is automatically registered.
- If Account Track has not been enabled, Group User Box cannot be created.

3.4.1 Setting the User Box

<From the Control Panel>

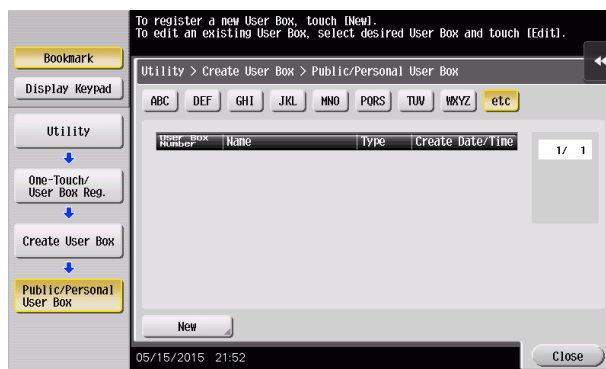
- ✓ For the logon procedure, see page 3-2.
- ✓ Do not leave the machine while you are in the user operation mode. If it is absolutely necessary to leave the machine, be sure first to log off from the user operation mode.
- ✓ For the procedure to change the User Box setting, see page 3-18.

- 1 Log on to the user operation mode through User Authentication from the control panel.
- 2 Touch [Utility].
- 3 Touch [One-Touch/User Box Registration].

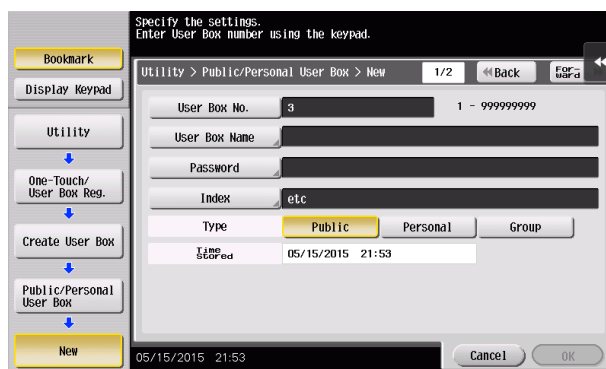


- 4 Touch [Create User Box] - [Public/Personal User Box].

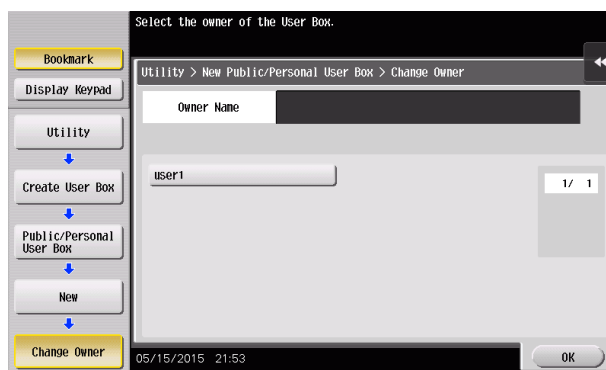
5 Touch [New].



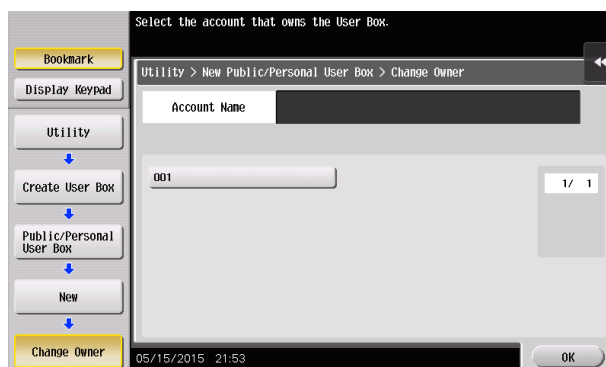
6 Select the User Box type.



→ When [Personal] is selected, [Change Owner] is displayed. Then, select the desired owner name. The default value of [Owner Name] is the user who has currently logged on to the function.



→ When [Group] is selected, [Change Account Name] is displayed. Then, select the desired account name. The default value of [Account Name] is the account to which the user who has currently logged on to the function belongs.



7 Touch [Password].

- 8 Enter the new User Box Password from the keyboard.
To prevent entry of a wrong password, enter the password again in [Password Confirmation].

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

9 Touch [OK].

- If the User Box Type is set to [Public], set a User Box Password that meets the Password Rules. For details of the Password Rules, see page 1-13.
- If the entered User Box Password does not match, a message that tells that the User Box Password does not match appears. Enter the correct User Box Passwords.

10 Make the necessary settings.

- A User Box No. that already exists cannot be redundantly registered.
- If no Name has been registered, [OK] cannot be touched. Be sure to register the Name.

11 Touch [OK].

<From **Web Connection**>

- ✓ For the login procedure, see page 3-2.
- ✓ Do not leave the machine while you are in the user operation mode. If it is absolutely necessary to leave the machine, be sure first to log off from the user operation mode.
- ✓ For the procedure to change the User Box setting, see page 3-18.

- 1 Log on to the user operation mode through User Authentication from the **Web Connection**.
- 2 Click the [Box] tab
- 3 Click [User Box List] from the menu and [New Registration].

User Box Number	User Box Name	Type	Owner Name	Box Operation
1	Box1	Public	Public	Edit Delete
2	Box2	Personal	user1	Edit Delete
3	Box3	Group	001	Edit Delete

- 4 Make the necessary settings.

- Be sure to enter the User Box Number, User Box Name, User Box Password, and Retype User Box Password.
- A User Box Number that already exists cannot be redundantly registered.
- If [Personal] is selected from the User Box Type pull-down menu, click [User List] and select the user from the registered user list. Or, directly enter in the "Owner Name" box the previously registered User Name.
- If [Group] is selected from the User Box Type pull-down menu, click [Account List] and select the account from the registered account list. Or, directly enter in the "Account Name" box the previously registered Account Name.

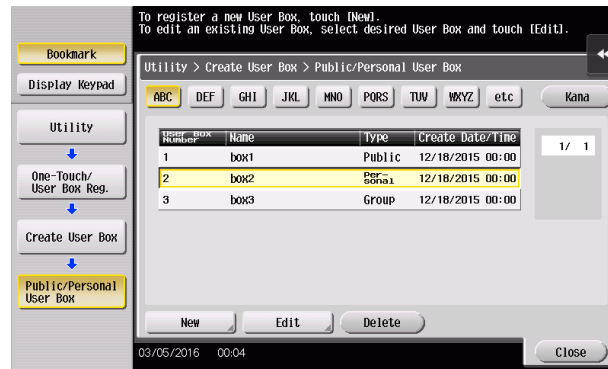
- 5 Click [OK].
 - If the User Box Type is set to [Public], set a User Box Password that meets the Password Rules. For details of the Password Rules, see page 1-13.
 - If the entered User Box Password does not match, a message that tells that the User Box Password does not match appears. Enter the correct User Box Password.
 - If no Owner Name is entered, a message appears that tells that no Owner Names have been entered. Enter the correct Owner Name.
 - If a user name not registered with the machine is entered in the "Owner Name" box, a message appears that tells that the Owner Name entered in the box is illegal. Enter the correct Owner Name.
 - If no Account Name is entered, a message appears that tells that no Account Names have been entered. Enter the correct Account Name.
 - If an account name not registered with the machine is entered in the "Account Name" box, a message appears that tells that the Account Name entered in the box is illegal. Enter the correct Account Name.
- 6 Check the message that tells that the setting has been completed. Then, click [OK].

3.4.2 Changing the user/account attributes and box password

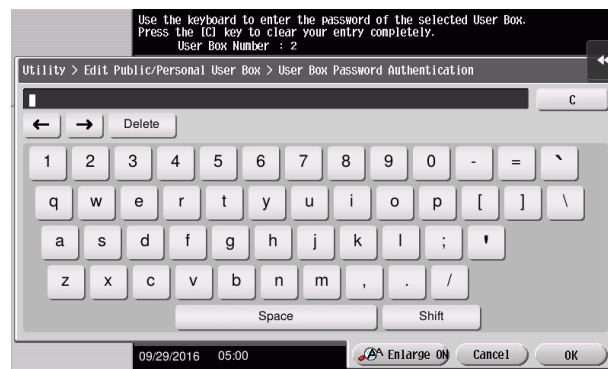
<From the Control Panel>

- ✓ For the procedure to call the User Box screen to the display, see steps 1 through 5 of page 3-13.
- ✓ Do not leave the machine while you are in the user operation mode. If it is absolutely necessary to leave the machine, be sure first to log off from the user operation mode.

- 1 Call the User Box screen to the display from the control panel.
- 2 Select the desired User Box and touch [Edit].



- 3 Enter the currently set User Box Password from the keyboard.



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

- 4 Touch [OK].

- If a wrong User Box Password is entered, a message that tells that the authentication has failed appears. Enter the correct User Box Password.
- If the Enhanced Security Mode is set to [ON], entry of a wrong User Box Password is counted as unauthorized access. If a wrong User Box Password is entered a predetermined number of times (once to three times) or more set by the administrator, the screen of step 2 reappears and the machine is set into an access lock state.
To cancel the access lock state, the administrator must perform the Release Setting. Contact the administrator.
- To change the User Box Type, perform steps 5 through 8.
- To change the owner user or owner account, perform steps 6 through 8.
- To change the User Box Password, go to step 9.

5 Select the User Box Type.

Select item and enter setting.

Utility > Public/Personal User Box > Edit 1/2 Back Forward

User Box No. 2 1 - 999999999

User Box Name Box2

Password *****

Index PQRS

Type Public Personal Group

Time Stored 05/15/2015 21:55

Owner Name user1 Change Owner

05/15/2015 21:57 Cancel OK

- [Change Owner] appears if the Box Type is changed to [Personal]. Select the desired owner name.
- [Change Account Name] appears if the Box Type is changed to [Group]. Select the desired account name.
- If the User Box Type is changed to [Public], set a User Box Password that meets the Password Rules. For details of the Password Rules, see page 1-13.

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

Select item and enter setting.

Utility > Public/Personal User Box > Edit 1/2 Back Forward

User Box No. 2 1 - 999999999

User Box Name Box2

Password *****

Index PQRS

Type Public Personal Group

Time Stored 05/15/2015 21:55

Owner Name user1 Change Owner

05/15/2015 21:57 Cancel OK

7 For [Change Owner], select the desired owner name.

Select the owner of the User Box.

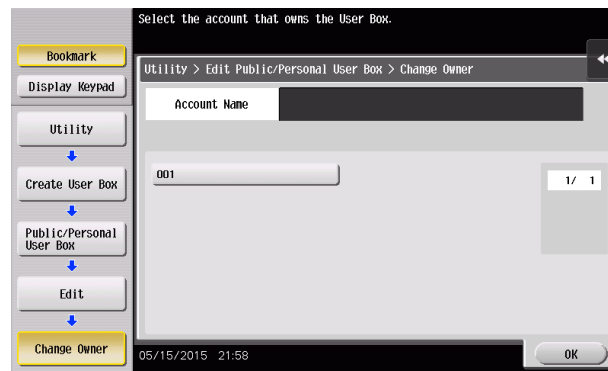
Utility > Edit Public/Personal User Box > Change Owner

Owner Name

user1 1/ 1

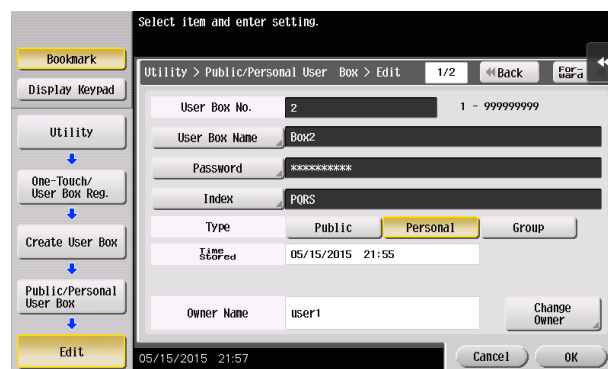
05/15/2015 21:58 OK

→ For [Change Account Name], select the desired account name.

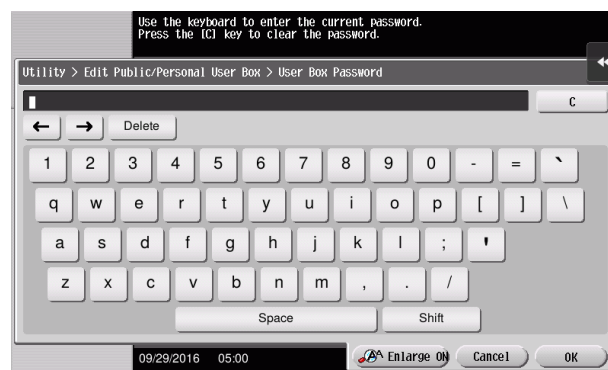


8 Touch [OK].

9 Touch [Password].



10 Enter the currently set User Box Password from the keyboard.



→ Touch [C] to clear all characters.

→ Touch [Delete] to delete the last character entered.

→ Touch [Shift] to show the upper case/symbol screen.

→ Touch [Cancel] to go back to the previous screen.

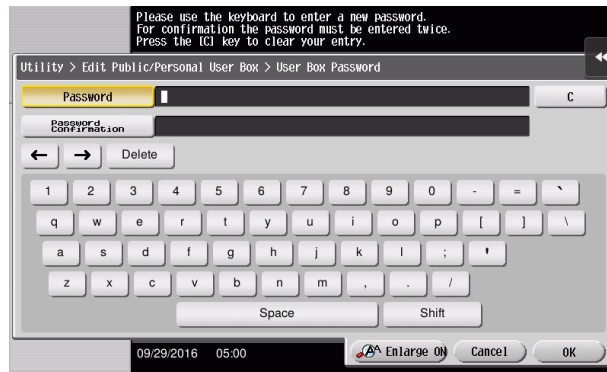
11 Touch [OK].

→ If a wrong User Box Password is entered, a message that tells that the User Box Password does not match appears. Enter the correct User Box Password.

→ If the Enhanced Security Mode is set to [ON], entry of a wrong User Box Password is counted as unauthorized access. If a wrong User Box Password is entered a predetermined number of times (once to three times) or more set by the administrator, the screen of step 2 reappears and the machine is set into an access lock state.

To cancel the access lock state, the administrator must perform the Release Setting. Contact the administrator.

- 12** Enter the new User Box Password from the keyboard.
To prevent entry of a wrong password, enter the password again in [Password Confirmation].



- Touch [C] to clear all characters.
- Touch [Delete] to delete the last character entered.
- Touch [Shift] to show the upper case/symbol screen.
- Touch [Cancel] to go back to the screen shown in step 9.

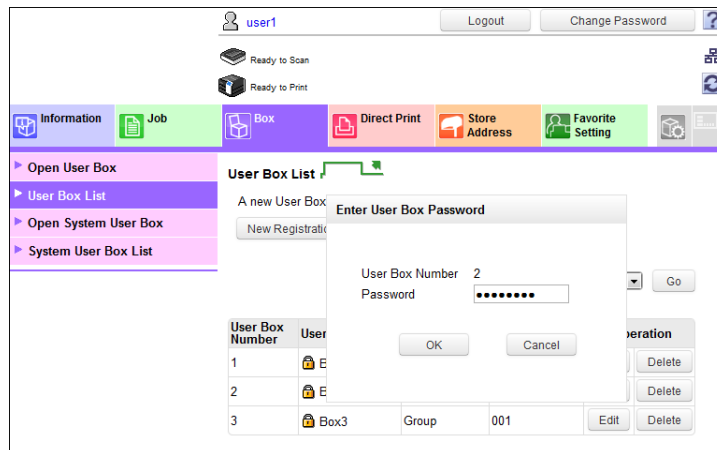
- 13** Touch [OK].

- If the User Box Type is changed to [Public], set a User Box Password that meets the Password Rules. For details of the Password Rules, see page 1-13.
- If the entered User Box Password does not match, a message that tells that the User Box Password does not match appears. Enter the correct User Box Password.

- 14** Touch [OK].

<From **Web Connection**>

- ✓ For the login procedure, see page 3-2.
 - ✓ Do not leave the machine while you are in the user operation mode. If it is absolutely necessary to leave the machine, be sure first to log off from the user operation mode.
- 1 Log on to the user operation mode through User Authentication from the **Web Connection**.
 - 2 Click the [Box] tab.
 - 3 Click [User Box List].
 - 4 Click [Edit] of the target box.
 - 5 Enter the user box password and click [OK].



- If a wrong User Box Password is entered, a message that tells that the authentication has failed appears. Enter the correct User Box Password.
- If the Enhanced Security Mode is set to [ON], entry of a wrong User Box Password is counted as unauthorized access. If a wrong User Box Password is entered a predetermined number of times (once to three times) or more set by the administrator, a message appears that tells that authentication has not been successful for any subsequent operation for authentication. The machine is then set into an access lock state.
To cancel the access lock state, the administrator must perform the Release Setting. Contact the administrator.
- Go to step 7 to change the User Box Password.
- To delete a User Box, click [Delete User Box]. A confirmation message appears. Click [OK] to delete the specified User Box.

- 6 Click the "User Box Owner is changed." check box and change Type and Owner Name (or Account Name).

- If [Personal] is selected from the User Box Type pull-down menu, click [User List] and select the user from the registered user list. Or, directly enter in the "Owner Name" box the previously registered User Name.
- If [Group] is selected from the User Box Type pull-down menu, click [Account List] and select the account from the registered account list. Or, directly enter in the "Account Name" box the previously registered Account Name.
- If the "User Box Owner is changed." check box is not clicked, the changes made will not be validated. If the changes need to be made, make sure that the "User Box Owner is changed." check box has been clicked.
- To change the User Box Type, click the User Box Type pull-down menu and select the desired User Box Type.

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

The screenshot shows a dialog box titled "User Box Function". It contains three main sections:

- User Box Expansion Function is changed.** (unchecked)
 - Confidential RX: OFF
 - New Communication Password: [empty field]
 - Retype New Communication Password: [empty field]
- User Box Password is changed.** (checked)
 - Current Password: [field with dots]
 - New Password: [field with dots]
 - Retype New Password: [field with dots]
- User Box Owner is changed.** (unchecked)
 - Type: Personal (dropdown menu)
 - Owner Name: user1 (text field)

At the bottom right are "OK" and "Cancel" buttons.

- In the "Current Password" box, enter the currently set User Box Password.

8 Click [OK].

- If a wrong current User Box Password is entered, a message that tells that the User Box Password does not match appears. Enter the correct User Box Password.
- If the User Box Type is changed to [Public], set a User Box Password that meets the Password Rules. For details of the Password Rules, see page 1-13.
- If the entered User Box Password does not match, a message that tells that the User Box Password does not match appears. Enter the correct User Box Password.
- If no Owner Name is entered, a message appears that tells that no Owner Names have been entered. Enter the correct Owner Name.
- If a user name not registered with the machine is entered in the "Owner Name" box, a message appears that tells that the Owner Name entered in the box is illegal. Enter the correct Owner Name.
- If no Account Name is entered, a message appears that tells that no Account Names have been entered. Enter the correct Account Name.
- If an account name not registered with the machine is entered in the "Account Name" box, a message appears that tells that the Account Name entered in the box is illegal. Enter the correct Account Name.

9 Click [OK].

3.4.3 Accessing the User Box and User Box file

<From the Control Panel>

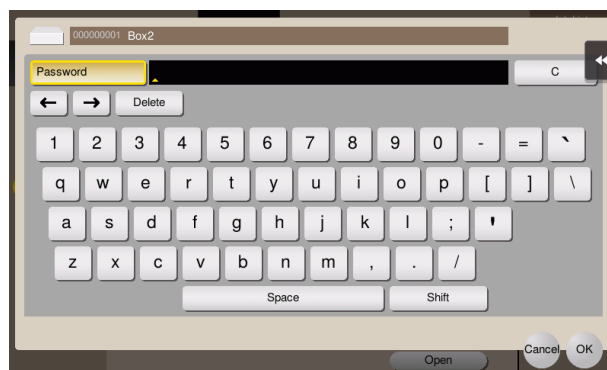
- ✓ For the logon procedure, see page 3-2.
- ✓ Do not leave the machine while you are in the user operation mode. If it is absolutely necessary to leave the machine, be sure first to log off from the user operation mode.

- 1 Log on to the user operation mode through User Authentication from the control panel.
- 2 Touch [User Box].
- 3 Select the desired User Box and touch [Open].



→ To save a new document, select [Save].

- 4 Enter the User Box Password from the keyboard.

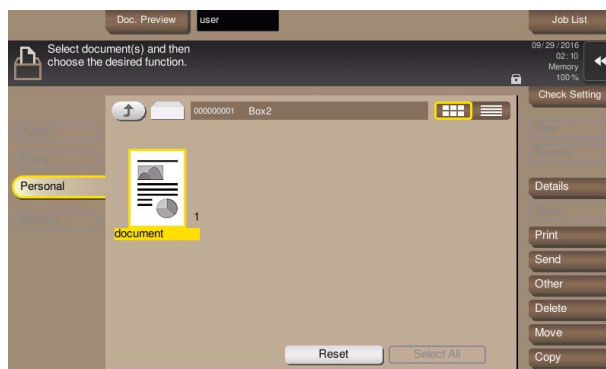


- Touch [C] to clear the value entered last.
- Touch [Delete] to delete the last character entered.
- Touch [Shift] to show the upper case/symbol screen.
- Touch [Cancel] to go back to the previous screen.

- 5 Touch [OK].

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

6 Select the desired file from each tab.



7 Select the desired function.

- Page rotation allows a document in the Annotation Box, ID & Print Box, and Secure Print Box to be printed and a document in the Annotation Box to be transmitted. Page rotation is reflected in the output.
- For the Memory RX Box, page rotation can be performed from document details; however, page rotation is not reflected in power output.
- Page deletion allows a document in the Annotation Box to be transmitted.
- If the destination is to be specified using the corresponding one-touch key for executing [Fax] or [Fax TX] from the control panel, always check that the destination is correct to make sure that the data is sent to the correct destination.
- If the destination is to be specified through direct input for executing [Fax] or [Fax TX] from the control panel, always check that the destination is correct to make sure that the data is sent to the correct destination.
- To delete the file, select the specific document and touch [Delete].

8 Press the **Start** key.

<From **Web Connection**>

- ✓ For the logon procedure, see page 3-2.
 - ✓ Do not leave the machine while you are in the user operation mode. If it is absolutely necessary to leave the machine, be sure first to log off from the user operation mode.
- 1 Log on to the user operation mode through User Authentication from the **Web Connection**.
 - 2 Click the [Box] tab.
 - 3 Enter the User Box Number and User Box Password of the desired User Box or select the target box from [Select User Box] and input the box password.

- 4 Click [OK].
 - If a wrong User Box Password is entered, a message that tells that the authentication has failed appears. Enter the User Box Password.
 - If the Enhanced Security Mode is set to [ON], entry of a wrong User Box Password is counted as unauthorized access. If a wrong User Box Password is entered a predetermined number of times (once to three times) or more set by the administrator, a message appears that tells that authentication has not been successful for any subsequent operation for authentication. The machine is then set into an access lock state, rejecting any more logon attempts. To cancel the access lock state, the administrator must perform the Release Setting. Contact the administrator.
- 5 Select the document and perform the desired function.

Select	Document Name	Number of Originals	Time Stored	Selectable Operation
<input type="checkbox"/>	001	1	05/15/2015 22:00	[Icons]

- Different functions can be performed on different types of operation menu.
See the table given below for the relation between the menu type and functions that can be performed.

File Type	Functions that can be Performed
Copy job files	Print, TX, Combine, Combine, Download, Move, Copy, Delete
Print job files	Print, TX, Combine, Combine, Download, Move, Copy, Delete
Scan job files	Print, TX, Combine, Combine, Download, Move, Copy, Delete
Fax job files	Print, TX, Combine, Combine, Download, Move, Copy, Delete

- If [Delete] is selected, a confirmation message appears. Click [OK] to delete the specified file.

<To use the Direct Print function>

- ✓ For the logon procedure, see page 3-2.
- ✓ Do not leave the machine while you are in the user operation mode. If it is absolutely necessary to leave the machine, be sure first to log off from the user operation mode.

- 1 Log on to the user operation mode through User Authentication from the **Web Connection**.
- 2 Click the [Direct Print] tab.
- 3 Click [Display] of the Application Setting.
- 4 Click [Save in User Box].
- 5 Enter the User Box Number of the desired User Box or select the target box from [Search from List].
- 6 Select the document and perform the desired function.
- 7 Click [OK].



Application Software

4 Application Software

4.1 Data Administrator

Data Administrator is an application for the administrator of the machine that allows the authentication, destination and network functions of the machine to be edited or registered from a PC connected to the network.

It allows the authentication, destination and network setting list to be downloaded in your PC, the data in the list to be edited on the PC, and then the data to be written in the machine.

A destination list of file formats including XML, CSV, TAB, LDIF, and Lotus Notes Structured Text can be downloaded. A destination list can also be downloaded by searching through or browsing destinations using the LDAP protocol for a directory server such as Active Directory.

NOTICE

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

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



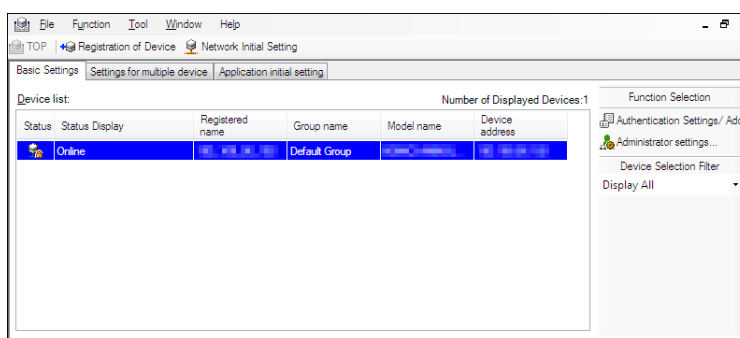
Tips

- The time-of-day and date on which this machine was registered in the **Data Administrator** may be changed. For details, see the **Data Administrator** User's Guide.
- The destination and authentication data read from this machine may be written as a backup file and can be restored. For details, see the **Data Administrator** User's Guide.
- Destination setting can be made from the **Data Administrator**. For details, see the **Data Administrator** User's Guide.

4.1.1 Accessing from Data Administrator

- ✓ Do not leave the site while you are gaining access to the machine through **Data Administrator**. If it is absolutely necessary to leave the site, be sure first to log off from the **Data Administrator**.

- 1 Start the **Data Administrator**.
- 2 Select this machine from Device List and click [Authentication Settings/Address Settings] or [Administrator settings].



- Select [Authentication Settings/Address Settings] to edit or register the authentication or destination function of the machine, and select [Administrator settings] to edit or register the network function of the machine.

- 3 Check the settings on the "Import the device information" screen and click [Import].
- The following screen appears if [Authentication Settings/Address Settings] is selected in step 2.

Import the device information.

Registered group: Default Group

Registered name: [Placeholder]

Device address: [Placeholder]

Scan settings

Import functions	Target of importing
<input type="checkbox"/> Administrator settings	<input checked="" type="radio"/> Obtain from the device <input type="radio"/> Previous data(Not access)
<input checked="" type="checkbox"/> Authentication Settings	<input checked="" type="radio"/> Obtain from the device <input type="radio"/> Previous data(Not access)
<input checked="" type="checkbox"/> Address settings	<input checked="" type="radio"/> Obtain from the device <input type="radio"/> Previous data(Not access)

Help(F1) Import... Cancel

- The following screen appears if [Administrator settings] is selected in step 2.

Import the device information.

Registered group: Default Group

Registered name: [Placeholder]

Device address: [Placeholder]

Scan settings

Import functions	Target of importing
<input checked="" type="checkbox"/> Administrator settings	<input checked="" type="radio"/> Obtain from the device <input type="radio"/> Previous data(Not access)
<input type="checkbox"/> Authentication Settings	<input checked="" type="radio"/> Obtain from the device <input type="radio"/> Previous data(Not access)
<input type="checkbox"/> Address settings	<input checked="" type="radio"/> Obtain from the device <input type="radio"/> Previous data(Not access)

Help(F1) Import... Cancel

- 4 Type the Administrator Password registered in the machine and click [OK].

Registered name: [Placeholder]

Registered group name: Default Group

Model name: SECURITY SYSTEM FOR ACCESS CONTROL

Device address: [Placeholder]

Device name: [Placeholder]

☒ Save

Administrator password: [Masked]

Administrator password (Confirmation): [Placeholder]

Help(F1) OK Cancel

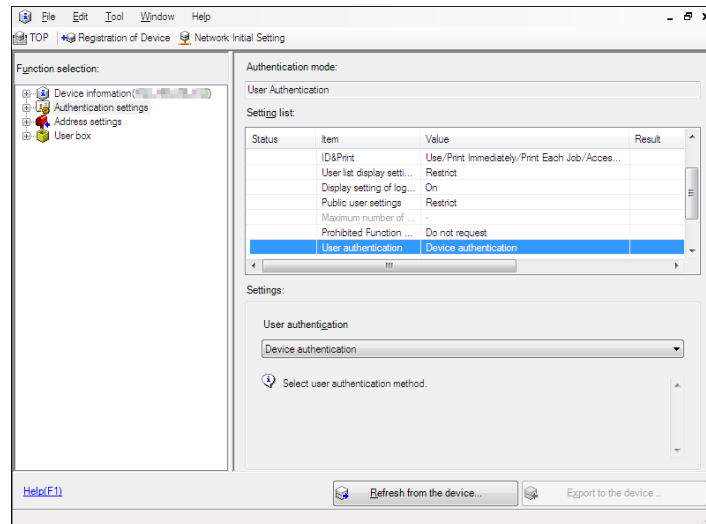
- If the "Save" check box has been selected, the Administrator Password entered is stored in the PC being used. If you do not want the Administrator Password stored, clear the "Save" check box.
- If a wrong Administrator Password is entered, a message appears that tells that there is a mismatch in the passwords. Enter the correct Administrator Password.
- If the "Save" check box is selected, enter the Administrator Password once again to make sure that the Administrator Password has been entered correctly.

- If a wrong Administrator Password is entered for confirmation, a message appears that tells that there is a mismatch in the Administrator Password. Enter the correct Administrator Password.
- If the Enhanced Security Mode is set to [ON], entry of a wrong password is counted as unauthorized access. If a wrong Administrator Password is entered a predetermined number of times (once to three times) or more set by the Administrator, a message appears that tells that the machine accepts no more Administrator Passwords because of unauthorized access for any subsequent entry of the Administrator Password. The machine is then set into an access lock state.
To cancel the access lock state, settings must be made by the Service Engineer; or, turn off, and then turn on, the **main power switch** of the machine. If the **main power switch** is turned off and on, the access lock state is canceled after the lapse of time set for [Release Time Settings]. When the **main power switch** is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. If there is no wait period between turning the **main power switch** off, then on again, the machine may not function properly.

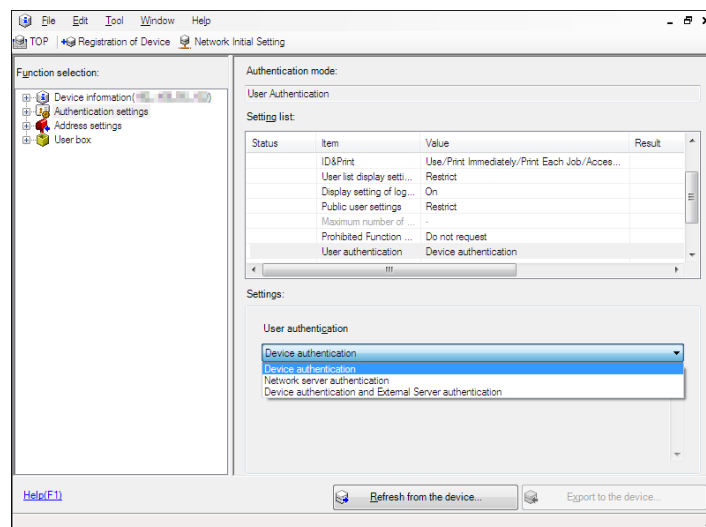
- 5 Check the data displayed on the SSL certificate check screen and click [Yes].

4.1.2 Setting the user authentication method

- ✓ For the procedure to access the machine, see steps 1 through 5 of page 4-2.
 - ✓ Do not leave the site while you are gaining access to the machine through **Data Administrator**. If it is absolutely necessary to leave the site, be sure first to log off from the **Data Administrator**.
- 1 Access the machine through [Authentication Settings/Address Settings] mode of **Data Administrator**.
 - 2 Click [Authentication settings] of the function selection tree.
 - 3 Click [User authentication].



- 4 From the pull-down menu of User authentication, select the user authentication method.



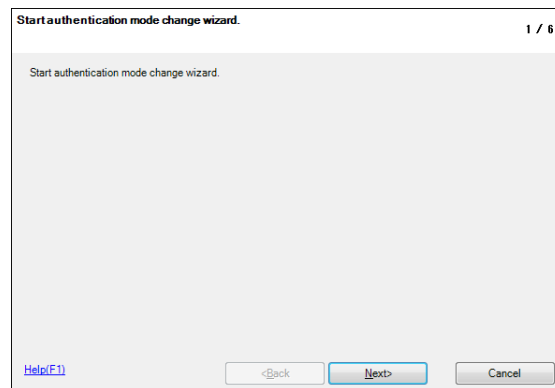
- To change the user authentication method from "Device authentication" to "Network server authentication," it is necessary first to register the domain name of Active Directory on the machine side.
- If "Network server authentication" is selected, "Active Directory" must invariably be selected.

- 5 Click [Export to the device].

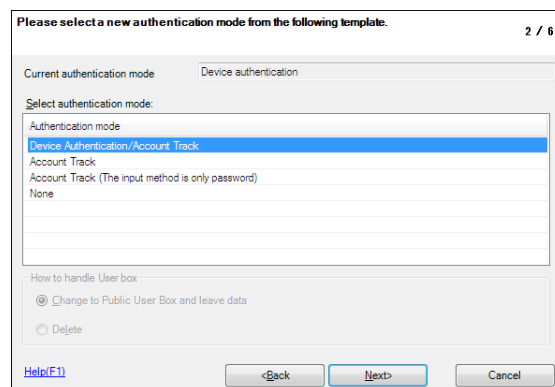
- If you have already logged on to the Administrator Mode via the control panel or using **Web Connection**, the machine displays a message that tells that the write operation has not been successful because of a device lock error. Click [OK] and wait for some while before attempting to execute [Export to the device] again.
- If there is a job being executed or a reserved job (timer TX, fax redial waiting, etc.) in the machine, the machine displays a message that tells that the write operation has not been successful because of a device lock error. Click [OK] and wait for some while before attempting to execute [Export to the device] again.

4.1.3 Changing the authentication mode

- ✓ For the procedure to access the machine, see steps 1 through 5 of page 4-2.
 - ✓ Do not leave the site while you are gaining access to the machine through **Data Administrator**. If it is absolutely necessary to leave the site, be sure first to log off from the **Data Administrator**.
- 1 Access the machine through [Authentication Settings/Address Settings] mode of **Data Administrator**.
 - 2 Click [Authentication settings] of the function selection tree.
 - 3 From [Edit] on the tool bar, select [Authentication] and click [Change authentication mode].
 - 4 Click [Next].



- 5 Select the specific [Authentication mode] to be changed and click [Next].



- Changing the Account Track setting erases all user and account information data that has previously been registered. At this time, Personal User Boxes owned by the users who are deleted and Group User Boxes owned by the accounts that are deleted may be deleted or changed to Public User Boxes.

If the boxes are changed to Public User Boxes and if the password set for a particular box before this change does not meet the Password Rules, no access can be made to the Public User Box, to which that specific box was changed. In this case, the administrator must first newly set a password that meets the Password Rules. For details of the Password Rules, see page 1-13.

- If [Device Authentication/Account Track] is selected, set [The number of Users] and [The number of Accounts].

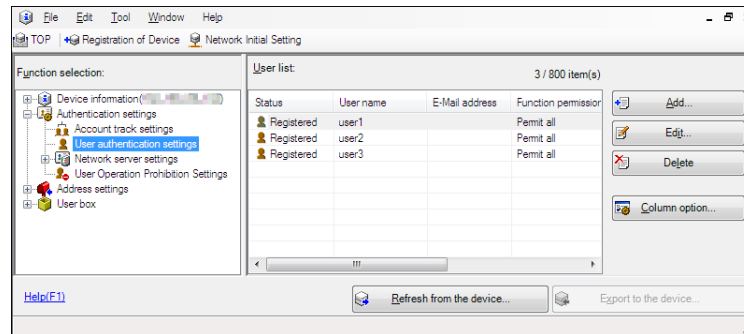
- 6 Verify the new authentication mode and click [Write].

- If you have already logged on to the Administrator Mode via the control panel or using **Web Connection**, the machine displays a message that tells that the write operation has not been successful because of a device lock error. Click [OK] and wait for some while before attempting to execute [Export to the device] again.
- If there is a job being executed or a reserved job (timer TX, fax redial waiting, etc.) in the machine, the machine displays a message that tells that the write operation has not been successful because of a device lock error. Click [OK] and wait for some while before attempting to execute [Export to the device] again.

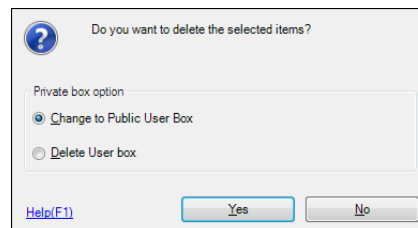
- 7 Click [Finished].

4.1.4 Making the user settings

- ✓ For the procedure to access the machine, see steps 1 through 5 of page 4-2.
 - ✓ Do not leave the site while you are gaining access to the machine through **Data Administrator**. If it is absolutely necessary to leave the site, be sure first to log off from the **Data Administrator**.
- 1 Access the machine through [Authentication Settings/Address Settings] mode of **Data Administrator**.
 - 2 Click the Authentication settings expand button of the function selection tree.
 - 3 Click [User authentication settings].



- 4 Select the desired function.
 - To register the user, click [Add].
 - To change data registered for the user, click [Edit].
 - To delete the user, click [Delete]. The following screen appears if the user to be deleted owns a Personal User Box. Select whether to delete the Personal User Box or change it to the Public User Box.



- If the boxes are changed to Public User Boxes and if the password set for a particular box before this change does not meet the Password Rules, no access can be made to the Public User Box, to which that specific box was changed. In this case, the administrator must first newly set a password that meets the Password Rules. For details of the Password Rules, see page 1-13.
- If the User Password does not meet the Password Rules, a message that tells that the entered User Password cannot be used appears. Enter the correct User Password. For details of the Password Rules, see page 1-13.
- If the User Name has not been entered, a message appears that tells that the User Name is yet to be entered. Click [OK] and enter the User Name.
- A User Name that already exists cannot be redundantly registered.

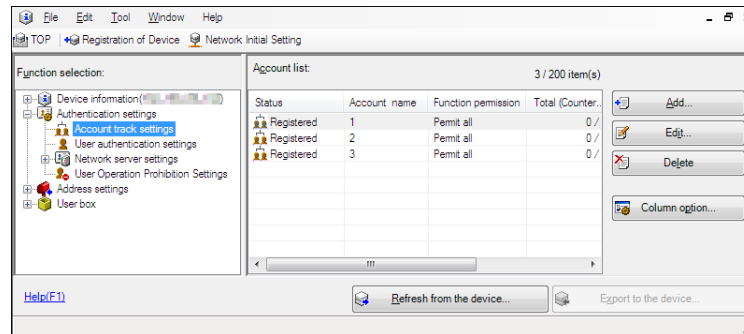
- 5 Click [OK].

- 6 Click [Export to the device].

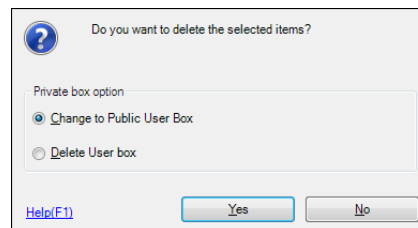
- If you have already logged on to the Administrator Mode via the control panel or using **Web Connection**, the machine displays a message that tells that the write operation has not been successful because of a device lock error. Click [OK] and wait for some while before attempting to execute [Export to the device] again.
- If there is a job being executed or a reserved job (timer TX, fax redial waiting, etc.) in the machine, the machine displays a message that tells that the write operation has not been successful because of a device lock error. Click [OK] and wait for some while before attempting to execute [Export to the device] again.

4.1.5 Making the account settings

- ✓ For the procedure to access the machine, see steps 1 through 5 of page 4-2.
 - ✓ Do not leave the site while you are gaining access to the machine through **Data Administrator**. If it is absolutely necessary to leave the site, be sure first to log off from the **Data Administrator**.
- 1 Access the machine through [Authentication Settings/Address Settings] mode of **Data Administrator**.
 - 2 Click the Authentication settings expand button of the function selection tree.
 - 3 Click [Account track settings].



- 4 Select the desired function.
 - To register the account, click [Add].
 - To change data registered for the account, click [Edit].
 - To delete the account, click [Delete]. The following screen appears if the account to be deleted owns a Group User Box. Select whether to delete the Group User Box or change it to the Public User Box.



- If the boxes are changed to Public User Boxes and if the password set for a particular box before this change does not meet the Password Rules, no access can be made to the Public User Box, to which that specific box was changed. In this case, the administrator must first newly set a password that meets the Password Rules. For details of the Password Rules, see page 1-13.
- If the Account Password does not meet the Password Rules, a message that tells that the entered Account Password cannot be used appears. Enter the correct Account Password. For details of the Password Rules, see page 1-13.
- If the Account Name has not been entered, a message appears that tells that the Account Name is yet to be entered. Click [OK] and enter the Account Name.
- An Account Name that already exists cannot be redundantly registered.

- 5 Click [OK].

- 6 Click [Export to the device].

- If you have already logged on to the Administrator Mode via the control panel or using **Web Connection**, the machine displays a message that tells that the write operation has not been successful because of a device lock error. Click [OK] and wait for some while before attempting to execute [Export to the device] again.
- If there is a job being executed or a reserved job (timer TX, fax redial waiting, etc.) in the machine, the machine displays a message that tells that the write operation has not been successful because of a device lock error. Click [OK] and wait for some while before attempting to execute [Export to the device] again.

4.1.6 DNS Server Setting Function

<Registering the DNS Server>

- ✓ For the procedure to access the machine, see steps 1 through 5 of page 4-2.
 - ✓ Do not leave the site while you are gaining access to the machine through **Data Administrator**. If it is absolutely necessary to leave the site, be sure first to log off from the **Data Administrator**.
- 1 Access the machine through [Administrator settings] mode of **Data Administrator**.
 - 2 Click the Administrator settings expand button.
 - 3 Click the Network expand button.
 - 4 Click [DNS].
 - 5 Make the necessary settings for the DNS Server.
 - If the DNS Server Auto Obtain and DNS Domain Auto Obtain check boxes are selected, the DNS Server Address and DNS Domain Name are automatically obtained.
 - 6 Click [Export to the device].
 - If you have already logged on to the Administrator Mode via the control panel or using **Web Connection**, the machine displays a message that tells that the write operation has not been successful because of a device lock error. Click [OK] and wait for some while before attempting to execute [Export to the device] again.

4.1.7 E-Mail Setting Function

<Setting the SMTP Server (E-Mail Server)>

- ✓ For the procedure to access the machine, see steps 1 through 5 of page 4-2.
- ✓ Do not leave the site while you are gaining access to the machine through **Data Administrator**. If it is absolutely necessary to leave the site, be sure first to log off from the **Data Administrator**.

1 Access the machine through [Administrator settings] mode of **Data Administrator**.

2 Click the Administrator settings expand button.

3 Click the Network expand button.

4 Click [E-Mail TX (SMTP)].

5 Make the necessary settings.

6 Click [Export to the device].

- If you have already logged on to the Administrator Mode via the control panel or using **Web Connection**, the machine displays a message that tells that the write operation has not been successful because of a device lock error. Click [OK] and wait for some while before attempting to execute [Export to the device] again.



KONICA MINOLTA

<http://konicaminolta.com>