

bizhub C360/C280/C220

User's Guide [Security Operations]



Contents

1 Security

1.1	Introduction	1-2
	Compliance with the ISO15408 Standard	1-2
	Operating Precautions	1-2
	INSTALLATION CHECKLIST	1-3
1.2	Security Functions	1-4
	Check Count Clear Conditions	1-4
1.3	Data to be Protected	1-5
1.4	Precautions for Operation Control	1-6
	Roles and Requirements of the Administrator	1-6
	Password Usage Requirements	1-6
	Network Connection Requirements for the Machine	1-7
	User information control server control requirements	1-7
	Security function operation setting operating requirements	1-7
	Operation and control of the machine	1-7
	Machine Maintenance Control	1-7
1.5	Miscellaneous	1-8
	Password Rules	
	Precautions for Use of Various Types of Applications	1-8
	Encrypting communications	1-9
	IPP printing	1-9
	Items of Data Cleared by Overwrite All Data Function	1-10
	Fax functions	1-10

2 Administrator Operations

2.1	Accessing the Administrator Settings	2-2
2.1.1	Accessing the Administrator Settings	
2.1.2	Accessing the User Mode	
2.2	Enhancing the Security Function	2-8
2.2.1	Items cleared by HDD Format	2-10
2.2.2	Setting the Enhanced Security Mode	
2.3	Preventing Unauthorized Access Setting Prohibited Functions When Authentication Error	2-13
2.4	Canceling the Operation Prohibited State Performing Release Setting	
2.5	Setting the Authentication Method	2-17
2.5.1	Setting the Authentication Method	2-17
2.5.2	Setting the External Server	2-19
2.6	ID & Print Setting Function Setting ID & Print	
2.7	System Auto Reset Function Setting the System Auto Reset function	
2.8	User Setting Function Making user setting	
2.9	Account Track Setting Function	
2.10	User Box Function	
2.10.1	Setting the User Box	
2.10.2	Changing the user attributes and account attributes	
2.11	Changing the Administrator Password Changing the Administrator Password	2-48 2-48
2.12	Protecting Data in the HDD	
2.12.1	Setting the Encryption Key (encryption word)	

0 10 0	Changing the Energy stien Key	0 55
2.12.2		2-00
2.13	Setting the Overwrite All Data function	2-57 2-57
2.14	SSL Setting Function	2-59
2.14.1	Device Certificate Setting	2-59
2.14.2	SSL Setting	2-61
2.14.3	Removing a Certificate	2-62
2.15	S/MIME Communication Setting Function	2-63
2.15.1	Setting the S/MIME Communication	2-63
2.15.2	Registering the certificate	2-67
2.16	SNMP Setting Function	2-69
2.16.1	Changing the auth-password and priv-password	2-69
2.16.2	SNMP access authentication function	2-76
2.16.3	SNMP v3 setting function	2-76
2.16.4	SNMP network setting function	2-77
2.17	WebDAV Function	2-78
	Setting the webDAV Server Password	2-10
2.18	PC-Fax RX Setting Function PC-Fax RX Setting	2-82 2-82
2.19	TSI User Box Setting Function	2-86
	TSI User Box Setting	2-86
2.20	TCP/IP Setting Function	2-90
2.20.1	Setting the IP Address	2-90
2.20.2	Registering the DNS Server	2-91
2.21	NetWare Setting Function	2-92 2-92
2.22	SMB Setting Function Setting the NetBIOS Name	2-93 2-93
2.23	AppleTalk Setting Function	2-94 2-94
2.24	E-Mail Setting Function	2-95 2-95

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	3-10
3.2	Change Password Function	 3-11 3-11
3.3	Secure Print Function Accessing the Secure Print Document	 3-14 3-14
3.4	User Box Function	3-17
3.4.1	Setting the User Box	3-17
3.4.2	Changing the User Box Password and user attributes and account attributes	3-23
3.4.3	Accessing the User Box and User Box file	3-31
3.4.4	Sending S/MIME box files	3-35

4 Application Software

4.1	PageScope Data Administrator	4-2
4.1.1	Accessing from PageScope Data Administrator	4-2
4.1.2	Setting the user authentication method	4-4
4.1.3	Changing the authentication mode	4-6
4.1.4	Making the user settings	4-9
4.1.5	Making the account settings	4-10
4.1.6	Registering the certificate	4-11

4.1.7	SNMP Setting Function	4-13
4.1.8	DNS Server Setting Function	4-15
4.1.9	NetWare Setting Function	4-16
4.1.10	SMB Setting Function	4-17
4.1.11	AppleTalk Setting Function	4-18
4.1.12	E-Mail Setting Function	4-19
4.2	PageScope Box Operator	4-20
4.2.1	Accessing the User Box	4-20
4.2.2	Creating a User Box	4-22
4.2.3	Changing the User Box properties (user attributes, account attributes)	4-23
4.2.4	Accessing the User Box file	4-25
4.3	HDD TWAIN driver Accessing from the HDD TWAIN driver	 4-26 4-26
4.4	PageScope Direct Print Printing through PageScope Direct Print	 4-28 4-28
4.5	HDD Backup Utility	4-30
4.5.1	Backup	4-30
4.5.2	Restore	4-33



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 C360/C280/C220 machine. To ensure the best possible performance and effective use of the machine, read this manual thoroughly before using the security functions. The Administrator of the machine should keep this manual for ready reference. The manual should be of great help in finding solutions to operating problems and questions.

This User's Guide (Ver. 1.02) describes bizhub C360/bizhub C280/bizhub C220/ineo⁺ 360/ineo⁺ 280/ineo⁺ 220/VarioLink 3622c/VarioLink 2822c/VarioLink 2222c Multi Function Peripheral Control Software (MFP Controller:A0ED0Y0-0100-GM0-12).

Compliance with the ISO15408 Standard

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

The security functions offered by the bizhub C360/C280/C220 machine comply with ISO/IEC15408 (level: EAL3).

Operating Precautions

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

The Administrator of the machine should make sure that each individual general user exits from the current mode to return to the basic screen whenever the access to that mode is completed or if the user leaves the machine with the mode screen left displayed.

The Administrator of the machine should exit from the current mode to return to the basic screen whenever the access to that mode is completed or if he or she leaves the machine with the mode screen left displayed.

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

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

To Service Engineer

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

1.	Perform the following steps before installing this machine.	Completed
	Check with the Administrator to determine if the security functions of this machine should be enhanced. If the functions should be enhanced, check the following. If the security functions are not to be enhanced, quit the operation without checking the following.	
	I swear that I would never disclose information as it relates to the settings of this ma- chine to anybody, or perform malicious or intentional act during setup and service procedures for the machine.	
	When giving the User's Guide Security Operations to the Administrator of the ma- chine, check that the User's Guide is the security-compatible version and explain to the Administrator that it is security-compatible.	
2.	After this machine is installed, refer to the Service Manual and perform the following steps.	
	Check that the Firmware version (MFP Controller, CheckSum) indicated in the Ser- vice Manual matches the values shown in the Firmware Version screen. If there is a mismatch in the Firmware version number, explain to the Administrator of the machine that upgrading of the Firmware is necessary and perform upgrading of the Firmware.	
	Set CE Authentication to [ON] and set the CE Password.	
	Check that Management Function Choice to Unset, HDD to Installed, and Image Controller Setting to Controller0.	
	Check that the Fax Kit has been mounted and set up properly, if fax functions are to be used.	
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 ma- chine.	
	Check that data has been backed up by the Administrator of the machine using the HDD Backup Utility if necessary.	
	Check that the Encryption Key has been set by the Administrator of the machine.	
	Check that User Authentication has been set to [ON (MFP)] or [ON (External Server)] (Active Directory only) by the Administrator of the machine.	
	Check that the self-signed certificate for SSL communications has been registered by the Administrator of the machine.	
	Check that data has been restored by the Administrator of the machine using the HDD Backup Utility if necessary.	
	Let the Administrator of the machine set Enhanced Security Mode to [ON].	
	The languages, in which the contents of the User's Guide Security Operations have been evaluated, are Japanese and English. Explain the way how to get the manual in the language, in which it is evaluated.	
	Explain to the administrator that the settings for the security functions for this ma- chine have been specified.	

When the above steps have been properly carried out, the Service Engineer should make a copy of this page and give the original of this page to the Administrator of the machine. The copy should be kept at the corresponding Service Representative for filing.

Product Name	Company Name	User Division Name	Person in charge
Customer			
Service Representative		-	

1.2 Security Functions

Setting the Enhanced Security Mode to [ON] will validate the security function of this machine. For details of the settings of different security functions to be changed by turning [ON] the Enhanced Security Mode, see page 2-8.

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

A password that can be set must meet the requirements of the Password Rules. The machine does not accept setting of an easily decipherable password. For details of the Password Rules, see page 1-8.

If a wrong password is entered, during password authentication, a predetermined number of times (once to three times) or more set by the Administrator of the machine, the machine determines that it is unauthorized access through Prohibited Functions When Authentication Error, prohibiting any further entry of the password. By prohibiting the password entry operation, the machine prevents unauthorized use or removal of data, thereby ensuring secured used of the machine.

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

By setting the Encryption Key, the data stored in the HDD is encrypted, thereby protecting the data in the HDD. Note, however, that the Encryption Key does not prevent the HDD from being physically removed. Make sure of a good operation control.

When the machine is to be discarded, or use of a leased machine is terminated at the end of the leasing contract, the Overwrite All Data function overwrites and erases all data stored in all spaces of the HDD. The function also resets all passwords saved in the NVRAM to factory settings, preventing leak of data. For details of items to be cleared by Overwrite All Data function, see page 1-10.

Check Count Clear Conditions

The following are the conditions for clearing or resetting the check count of the number of wrong entries at the time of authentication by the Enhanced Security Mode.

<Administrator Settings>

• Authentication of Administrator Settings is successful.

<User Authentication Mode>

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

<Account Track Mode>

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

<Secure Print>

- 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.

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

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

<WebDAV authentication>

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

1.3 Data to be Protected

The underlying concept of this machine toward security is "to protect data that can be disclosed against the intention of users."

The following types of image files that have been stored in the machine and made available for use by its users are protected while the machine is being used.

- Image files stored by Secure Print
- Image files stored as ID & Print Document when print data is to be registered using the ID & Print Setting function
- Image files stored in Personal User Box, Public User Box and Group User Box

The following types of data stored in the HDD are protected when use of a leased machine is terminated at the end of the leasing contract, the machine is to be discarded, or when the HDD is stolen.

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

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

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

1.4 Precautions for Operation Control

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

Roles and Requirements of the Administrator

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

<To Achieve Effective Security>

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

Password Usage Requirements

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

<To Achieve Effective Security>

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

Network Connection Requirements for the Machine

Packets being transmitted over the LAN installed in the office, in which the machine is installed, should be protected from unauthorized manipulation. If the LAN is to be connected to an outside network, no unauthorized attempt to establish connection from the external network should be permitted.

<To Achieve Effective Security>

- If the LAN, in which the machine is installed, is connected to an outside network, install a firewall or similar network device to block any access to the machine from the outside network and make the necessary settings.
- Configure the LAN installed in the office, in which the machine is installed, by using a switching hub and other devices to ensure that the packets are protected from unauthorized manipulation.
- Provide an appropriate network control at all times to make sure that packets are protected from unauthorized manipulation and no other copying machine is connected without prior notice to the office LAN to which this machine is connected.

User information control server control requirements

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

Security function operation setting operating requirements

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

Operation and control of the machine

The Administrator of the machine should perform the following operation control.

- The Administrator of the machine should log off from the Administrator Settings whenever the operation in the Administrator Settings is completed. The Administrator of the machine should also make sure that each individual user logs off from the User Authentication mode after the operation in the User Authentication mode is completed, including operation of the Secure Print Document, User Box, and User Box file.
- The Administrator of the machine should set the Encryption Key according to the environment, in which this machine is used.

Machine Maintenance Control

The Administrator of the machine should perform the following maintenance control activities.

- Provide adequate control over the machine to ensure that only the Service Engineer is able to perform physical service operations on the machine.
- Provide adequate control over the machine to ensure that any physical service operations performed on the machine by the Service Engineer are overseen by the Administrator of the machine.

1.5 Miscellaneous

Password Rules

According to certain Password Rules, registration of a password consisting of a string of a single character or change of a password to one consisting of a string of a single character is rejected for the Administrator Password, User Password, Account Password, User Box Password, Secure Print Password, SNMP Password, WebDAV Server Password, and Encryption Key. For the Administrator Password, User Password, User Password, SNMP Password, WebDAV Server Password, SNMP Password, WebDAV Server Password, SnMP Password, WebDAV Server Password, User Box Password, WebDAV Server Password, User Box Password, WebDAV Server Password, SnMP Password, WebDAV Server Password, and Encryption Key, the same password as that currently set is not accepted.

Study the following table for more details of the number of digits and characters that can be used for each password.

Types of passwords	No. of digits	Characters
User Password	8 digits	 Numeric characters: 0 to 9 Alpha characters: upper and lower case letters Symbols: !, #, \$, %, &, ', (,), *, ,, -, ., /, :, ;, <, =, >, ?, @, [,], ^, _, `, {, , }, ~, + Characters with umlaut (95 characters) Selectable from among a total of 188 characters
Encryption Key	20 digits	 Numeric characters: 0 to 9 Alpha characters: upper and lower case letters Symbols: !, #, \$, %, &, ', *, +, -, ., /, =, ?, @, ^, _, `, {, , }, ~ Selectable from among a total of 83 characters
Administrator Password	8 digits	Numeric characters: 0 to 9
Account Password	 Alpha characters: upper and lowe Symbols: !, #, \$, %, &, ', (,), *, ,, -, ?, @, [,], ^, _, `, {, , }, ~, + Selectable from among a total of 93 c 	 Alpha characters: upper and lower case letters Symbols: !, #, \$, %, &, ', (,), *,, /, :, :, <, =, >.
User Box Password		?, $@$, [,], ^, _, `, {, , }, ~, +
Secure Print Password		Selectable from among a total of 93 characters
WebDAV Server Password		
SNMP Password • auth-Password • priv-Password	8 digits or more	 Numeric characters: 0 to 9 Alpha characters: upper and lower case letters Symbols: !, \$, %, &, (,), *, ,, -, ., /, :, ;, <, =, >, ?, @, [,], ^, _, `, {, , }, ~, + Selectable from among a total of 90 characters

Precautions for Use of Umlaut

- The maximum number of digits allowed for the User Password is 64, if umlaut is used with all characters, however, the maximum number of digits allowed becomes 32 digits.
- 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 PageScope 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 various types of applications.

- When PageScope Web Connection or an application of various other types is used, the password control function of the application stores the password that has been entered in your PC. If you want the password not stored, disable the password control function of the application.
 When using the PageScope Web Connection or an application of various other types, use one that shows "*" or "●" for the password entered.
- Internet Explorer or other type of web browser, "SSL v3" or "TLS v1" should be used, not "SSL v2," for the SSL setting.
- Expanded functions, which can be used in association with applications by registering the optional License Kit, are available, including collecting and controlling user and account information by means of the WebDAV function. Use of these expanded functions is not covered by certification of ISO15408.

Encrypting communications

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

- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA

NOTICE

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

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

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

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

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

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

Linux

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

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

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

NOTICE

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

IPP printing

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

<IPP setting on Windows Vista>

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

First, register Host Name and IP address of this machine in the DNS server in advance. Then, in TCP/IP Settings of PageScope 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 PageScope Web Connection and exported in advance as the certificate including the public key.

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

<IPPS printing settings in Windows Vista>

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

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

<Installing printer driver>

To perform IPP printing, the printer driver must be installed. From "Add Printer Wizard," select "Connect to a printer on the Internet or on a home or office network" and type the URL of this machine in the following format in the "URL" field. The printer, for which the settings have been made, can be used in the same manner as the ordinary local printer.

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

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

Items of Data Cleared by Overwrite All Data Function

Items of Data Cleared	Description
User registration data	Deletes all user-related data that has been registered
Box registration data/file	Deletes all User Box-related information and files saved in User Box
Secure Print ID/Password/Document	Deletes all Secure Print Document-related information and files saved
ID & Print file	Deletes all ID & Print files saved in ID & Print User Box
Image files	 Image files saved other than Secure Print Documents, ID & Print files and User Box files Image files of jobs in job queue state Data files left in the data space used as image files Temporary data files generated during print image file processing
Destination recipient data files	Deletes all destination recipient data including e-mail ad- dresses and telephone numbers
Encryption Key	Clears the currently set Encryption Key
Administrator Password	Clears the currently set password, resetting it to the factory setting
SNMP Password	Clears the currently set password, resetting it to the factory setting (MAC address)
WebDAV Server Password	Clears the currently set password, resetting it to the factory setting (sysadm)
Account registration data	Deletes all account track-related data that has been regis- tered
S/MIME certificate data	Deletes the currently set S/MIME certificate
SSL certificate	Deletes the currently set SSL certificate
Network Setting	Clears the currently set network settings (DNS Server setting, IP Address setting, SMTP Server setting, NetWare Setting, NetBIOS setting and AppleTalk Printer Name setting), reset- ting it to the factory setting

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

Fax functions

An optional Fax Kit is required for using fax functions.

bizhub C360/C280/C220



2 Administrator Operations

2.1 Accessing the Administrator Settings

This machine implements authentication of the user of the Administrator Settings function through the 8-digit Administrator Password that verifies the identity as the Administrator of the person who accesses the function. During the authentication procedure, the Administrator Password entered for the authentication purpose appears as "*" or "●" on the display.

Two different methods are available for accessing Administrator Settings. In Administrator Settings, the settings for the machine system and network can be registered or changed. In User Mode, the same settings as the user authority can be made. For box setting operations, however, the same functions can be set as those of Administrator Settings. User Mode also allows jobs to be checked or deleted, which is not possible in Administrator Settings.

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

2.1.1 Accessing the Administrator Settings

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

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

<From the Control Panel>

- ✓ When accessing the Administrator Settings from the control panel, if you have already logged on to the Administrator Settings using PageScope Web Connection, the machine displays a message that tells not to turn off the power because of the remote operation being performed and rejects any operation on the control panel. Wait until the message disappears before attempting to access the Administrator Settings once again.
- ✓ When accessing the Administrator Settings from the control panel, if [Export to the device] operation is being executed using the PageScope Data Administrator, the machine displays a message that tells not to turn off the power because of the remote operation being performed and rejects any operation on the control panel. Wait until the message disappears before attempting to access the Administrator Settings once again.
- ✔ Make sure that none of the general users of the machine will know the Administrator Password.
- ✓ If the Administrator Password is forgotten, it must be set again by the Service Engineer. Contact your Service Representative.
- ✓ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.
- 1 Press the [Utility/Counter] key.

2 Touch [Administrator Settings].



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

Use the keyboard or keypad to type in the Administrator Password. Press ICI to clear the entered Administrator Password.					
Utility > Administrator Settings					

+ Petc					
1 2 3 4 5 6 7 8 9 0					
q v e r t y i i o p e l					
a s d f g h j k 1 ; ;]					
Z X C V b n n , . / N Shift					
Space					
2009/09/10 13:29 Henory 100%					

- → Press the [C] key to clear all characters.
- → Touch [Delete] to delete the last character entered.
- → Touch [Shift] to show the upper case/symbol screen.
- → Touch [Cancel] to go back to the screen shown in step 2.
- 4 Touch [OK].
 - → If a wrong Administrator Password is entered, a message appears saying that there is a mismatch in the Administrator Passwords and entry of the Administrator Password will be prohibited for five sec. Wait for some while before entering the correct Administrator Password.
 - → If the Enhanced Security Mode is set to [ON], entry of a wrong password is counted as unauthorized access. If a wrong Administrator Password is entered a predetermined number of times (once to three times) or more set by the Administrator of the machine, a message appears saying that the machine accepts no more Administrator Passwords because of unauthorized access for any subsequent entry of the Administrator Password. The machine is then set into an access lock state. To cancel the access lock state, settings must be made by the Service Engineer; or, turn off, and then turn on, the main power switch of the machine. If the main power switch is turned off and on, the access lock state is canceled after the lapse of time set for [Release Time Settings]. When the main power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. If there is no wait period between turning the main power switch off, then on again, the machine may not function properly.

Here is the sequence, through which the main power switch and sub power switch are turned on and off:

Turn off the sub power switch \rightarrow Turn off the main power switch \rightarrow Turn on the main power switch \rightarrow Turn on the sub power switch

5 Press the [Utility/Counter] key to log off from the Administrator Settings.

2.1.2 Accessing the User Mode

<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 2-17.
- Make sure that none of the general users of the machine will know the Administrator Password.
- ✓ If the Administrator Password is forgotten, it must be set again by the Service Engineer. Contact your Service Representative.
- ✓ Do not leave the machine with the User Mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the User Mode.
- 1 Touch [User Name].

Job List	<pre>@Enter User Name and password, and then touch [Login] or press the [Access] key.</pre>	
Kans Status	User Name	
	Password	
Delete		
Job Details	04/03/2007 14:42 Hemory 1007	

2 Type "admin" in User Name.

♥Use the keyboard or keyped to type in the user name. Press ICL to erase the entered user name.
User Authentication > Enter User Name
adnin
• • Pete
1 2 3 4 5 6 7 8 9 0 - = -
9 V e r t y I 1 0 P [] \
a s d f g h j k l ;
ZXCVbnn,./Shift
Space
2009/09/10 13:30 Honory 1002

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

Job List	Enter User Name and password, and then touch Llogin] or press the faccess] key.
Neer Status	User Name admin
	Password
Delete	Login
Y M C K	07/27/2007 08:22 Hemory 100%

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



- → Press the [C] key to clear all characters.
- → Touch [Delete] to delete the last character entered.
- → Touch [Shift] to show the upper case/symbol screen.
- → Touch [Cancel] to go back to the screen shown in step 4.
- 6 Touch [OK].
- 7 Press [Access] or touch [Login].
 - → If a wrong Administrator Password has been entered, the machine gives a message that tells that authentication has not been successful. Enter the correct Administrator Password.
 - → If the Enhanced Security Mode is set to [ON], entry of a wrong password is counted as unauthorized access. If a wrong Administrator Password is entered a predetermined number of times (once to three times) or more set by the Administrator of the machine, a message appears saying that the machine accepts no more Administrator Passwords because of unauthorized access for any subsequent entry of the Administrator Password. The machine is then set into an access lock state. To cancel the access lock state, settings must be made by the Service Engineer; or, turn off, and then turn on, the main power switch of the machine. If the main power switch is turned off and on, the access lock state is canceled after the lapse of time set for [Release Time Settings]. When the main power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. If there is no wait period between turning the main power switch off, then on again, the machine may not function properly.

Here is the sequence, through which the main power switch and sub power switch are turned on and off:

Turn off the sub power switch \rightarrow Turn off the main power switch \rightarrow Turn on the main power switch \rightarrow Turn on the sub power switch

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

<From PageScope Web Connection>

- Make sure that none of the general users of the machine will know the Administrator Password.
- ✓ While you are logging onto the Admin Mode using PageScope Web Connection, any operations from the machine's control panel are disabled.
- ✓ If you have already logged on to the Admin Mode from the control panel or using PageScope 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 PageScope 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 PageScope 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 PageScope Web Connection. Click [OK] and wait for some while before attempting to access the Admin Mode once again.
- ✓ If an attempt is made to log on to the Admin Mode while a job is being executed, the machine gives a message that tells that it is now impossible to log on to the Admin Mode. Click [OK] and try logging on to the Admin Mode after the execution of the job is completed.
- ✓ 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 PageScope Web Connection and if you close the web browser without clicking [Logout], the touch panel of the machine remains locked for 70 sec.
- 1 Start the Web browser.
- 2 Enter the IP address of the machine in the address bar.
- **3** Press the [Enter] key to start PageScope Web Connection.
- 4 Click the Administrator radio button and [Login].

Language	English (English)
Login	C Registered User User Name Password
	© Administrator
View Mode	C Flash C Flash Flash Flash Flash form.
User Assist	Display dialog box in case of warning. Login
Starting-u	p Data Management Utility er is remuired to use the Data Management Hility
Manag	e no required to use the Data wanagement othing.
Manag	e Stamp Data
CEM anag	e Font/Macro (*1)
(*1) Can on	nly run on Windows Internet Explorer and Flash Player Version 9 and above

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

a											[
File	Edit	View	Favorites	Tools	Help							<u></u>
				Se	lect Logi	n						
								Adminis	strator (Adr	nin Mode)		
								Adminis	strator (Use	r Mode)		
				65077								
				Pa	ssword			•••••				
					Help Dis	olay Set	ting					
					Help D	splay is	a netw	ork-only functi	on.			
					On Mou	ise		OFF 🔽				
					On Foo	us		OFF 💙				
											OK Car	icel

- → Administrator (Admin Mode) is a mode, in which settings of the machine can be registered or changed. In this mode, system and network settings can be made.
- → Administrator (User Mode) is a mode, in which the same settings as the user authority can be made. For box setting operations, however, the same functions can be set as those of Admin Mode. User Mode also allows jobs to be checked or deleted, which is not possible in Admin Mode.
- → When accessing the Admin Mode using the PageScope Web Connection, enter the same Administrator Password as that for the machine.
- 6 Click [OK].
 - → If a wrong Administrator Password has been entered, the machine gives a message that tells that authentication has not been successful. In this case, click [OK] and enter the correct Administrator Password in the "Password" box.
 - → If the Enhanced Security Mode is set to [ON], entry of a wrong password is counted as unauthorized access. If a wrong Administrator Password is entered a predetermined number of times (once to three times) or more set by the Administrator of the machine, a message appears saying that the machine accepts no more Administrator Passwords because of unauthorized access for any subsequent entry of the Administrator Password. The machine is then set into an access lock state. To cancel the access lock state, settings must be made by the Service Engineer; or, turn off, and then turn on, the main power switch of the machine. If the main power switch is turned off and on, the access lock state is canceled after the lapse of time set for [Release Time Settings]. When the main power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. If there is no wait period between turning the main power switch off, then on again, the machine may not function properly.

Here is the sequence, through which the main power switch and sub power switch are turned on and off:

Turn off the sub power switch \rightarrow Turn off the main power switch \rightarrow Turn on the main power switch \rightarrow Turn on the sub power switch

- 7 Click [Logout].
- 8 Click [OK].

This allows you to log off from the Admin Mode.

2.2 Enhancing the Security Function

When access to the machine by the Administrator of the machine through the Administrator Settings from the control panel is authenticated, the machine enables setting of the Enhanced Security Mode that allows settings for enhancing each of different security functions to be converted all at once.

In the Enhanced Security Mode, the machine allows selection of whether to use the Enhanced Security Mode or not. If the Enhanced Security Mode is set to [ON], a count is taken of the number of unauthorized accesses to the Administrator Settings, User Authentication, Account Track, SNMP authentication, WebDAV authentication, 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 2-10.

If initialization is executed by the Service Engineer, set the Administrator Password and turn [ON] the Enhanced Security Mode again.

Settings to be Made in Advance	Description	
Administrator Password	An 8-digit password that meets the Password Rules. The factory setting is "12345678."	
User Authentication	Set to either [ON (MFP)] or [ON (External Server)] (Active Directory).	
Encryption Key	Set the 20-digit Encryption Key.	
Certificate for SSL	Register the self-signed certificate for SSL communications.	
Image Controller Setting	Calls for setting made by the Service Engineer. For details, ask	
Management Function Choice	your Service Representative.	
CE Password		
CE Authentication		
HDD		

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

Function Name	Factory Setting	When Enhanced Security Mode is set to [ON]				
Password Rules	Invalid	Enable (not to be changed)				
Prohibited Functions When Authentication Er- ror	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 (twice, four times, or six times for the WebDAV Server Password).				
Confidential Document Access Method	Mode 1	Mode 2 (not to be changed) * In association with Prohibit Functions When Authenti- cation Error the method is changed from authentication using Secure Print ID and password (Mode 1) to that us- ing the password with the Secure Print Document first narrowed down by Secure Print ID (Mode 2).				
Public User Access	Restrict	Restrict (not to be changed)				
User List	OFF	OFF (not to be changed)				
Print Without Authentica- tion	Restrict	Restrict (not to be changed)				
User Box Admin. Setting	Restrict	Restrict (not to be changed)				
SSL	OFF	ON (not to be changed)				
SSL Encryption Strength	AES-256, 3DES-168, RC4-128, DES-56, RC4-40	AES/3DES (not to be changed to one containing strength lower than AES/3DES)				
Automatically Obtain Cer- tificates of S/MIME	No	No (not to be changed)				
S/MIME Encryption Method	3DES	3DES (not to be changed to DES or RC-2)				
FTP Server	ON	OFF (not to be changed)				
SNMPv1/v2c	Read/Write en- abled	Only Read is enabled (not to be changed)				
SNMP v3 Security Level and auth/priv-password	auth/priv-pass- word	The security level can be selected from among [auth- password] and [auth/priv-password]. An 8-digit-or-more auth-password and priv-password can both be set.				
Print Data Capture	Allow	Restrict (not to be changed)				
Network Setting Clear (Pagescope Web Con- nection)	Enabled	Restrict				
Administrator Password Change Via Network (Pagescope Web Con- nection)	Enabled	Restrict (not to be changed)				
Release Time settings	5 min.	The setting value should be 5 min. or more (no value less than 5 can be set)				
Change by the user of destination data previ- ously registered (Address Book and Program)	Allow	Restrict (not to be changed)				
Secure Print User Box Preview	Thumbnail View, Detail View, and Document De- tails are enabled	Only Detail View is enabled before password authenti- cation (Mode 2)				
Initialize (Network Set- tings)	Enabled	Restrict (not to be changed)				
Image Log Transfer Set- tings	OFF	OFF (not to be changed)				

Function Name	Factory Setting	When Enhanced Security Mode is set to [ON]
CS Remote Care	Usable	Remote device setting disabled

NOTICE

When Password Rules is set to [ON] the characters and the number of digits used for each password are restricted. For details of the Password Rules, see page 1-8.

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]
User Authentication	Set to [OFF]
Account Track Authentica- tion	Set to [OFF]
Public User Access	Set to [Restrict]
User List	Set to [OFF]
Print Without Authentica- tion	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/Pass- word/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 tele- phone numbers

2.2.2 Setting the Enhanced Security Mode

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



bizhub C360/C280/C220

3 Touch [Enhanced Security Mode].



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

	Select whether	r or not to enable En	hanced Security Mode.	
Bookmark	Administrator	r Settings > Security	Settings > Enhanced Se	curity Mode
Utility Administrator Settings Security Settings Enhanced Security Hode		(<u>N</u>	OFF	
	08/24/2007 0 Memory 1)8:13 100%		ОК

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

Bookmark	The followin	g settings	must be m	ade to er	nable f	Enhanced	Security	Mode.
DOONING	Administrat	or Settings	> Securi	ty Settir	ngs > f	Inhanced	Security	Mode
Utility			Administr	ator Pass	word			
Administrator Settings			HDD E	ncryptio	n			
Security			User Aut	henticat	ion			
Settings			Certific	ate for :	SSL			
Enhanced Security Mode								
	06/01/2007 Memory	15:45 100%						Close

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

Paolmarth	Contact	your S	ervice R	eprese	entative	to enabl	e Enhanceo	l Security	Mode.
BUUKillark	Adminis	strator	Setting	s > S€	curity	Settings	> Enhanced	l Security	Mode
Utility									
Administrator Settings									
Security Settings									
Enhanced Security Mode									
	01/06/20	007 1	5:29	-	_	_		_	Close

- 5 Touch [OK].
- 6 Make sure that a message appears prompting you to turn OFF and then ON the main power switch. Now, turn OFF and then turn ON the main power switch.

Bookmark	A Ent Tur	hanced Security Mode Parameter has been chan rn main switch OFF and ON.	ged.
Utility Administrator Settings			
Security Settings Enhanced Security Hode			
	01/06/2007 Memory	15:31 100%	

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

Here is the sequence, through which the main power switch and sub power switch are turned on and off:

Turn off the sub power switch \rightarrow Turn off the main power switch \rightarrow Turn on the main power switch \rightarrow Turn on the sub power switch

→ If the Enhanced Security Mode is properly set to [ON], the following icon appears at the center of the User Authentication screen, indicating that the machine is in the Enhanced Security Mode.

Job List	Enter User Name and Password, and then touch [Login] or press the [Access] key.	
NSRC Status	User Name	
	Password	
Delete	Login	
Y M C K	04/03/2007 12:54 🙆 See Henory 100%	Ĩ

2.3 Preventing Unauthorized Access

When access to the machine by the Administrator of the machine through the Administrator Settings from the control panel is authenticated, the machine enables setting of the operation of Prohibited Functions When Authentication Error. The machine then takes a count of the number of unsuccessful accesses to the Administrator Settings, User Authentication, Account Track, SNMP authentication, WebDAV authentication, Secure Print authentication, and User Box authentication to prohibit the authentication operation.

Either [Mode 1] or [Mode 2] can be selected for Prohibited Functions When Authentication Error. The factory setting is [Mode 1]. If the Enhanced Security Mode is set to [ON], it is prohibited to change the setting from [Mode 2] (check count: three times). It is nonetheless possible to change the check count to select from among once, twice, or three times (twice, four times, or six times for the WebDAV authentication). If [Mode 2] is selected, the Release Time Settings function is enabled. When the Administrator Settings is set into the access lock state, the main power switch is turned off and on and, after the lapse of a predetermined period of time after the machine is turned on again, the access lock state of the Administrator Settings is canceled. The Release Time Settings 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

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

Setting Prohibited Functions When Authentication Error

- ✓ For the procedure to call the Security Settings screen on the display, see steps 1 and 2 of page 2-10.
- ✓ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.
- 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].

	This mode allows you to prohibit functio	ns when authentication fails.
BOOKMARK	Administrator Settings > Security > Pro	hibit Functions When Auth. Error
	Prohibit Functions When Auth. Error	No. of Tries
Utility	Hode 1	3
Security	Hode 2	1 - 5
Settings		
Prohibit Functions When Auth. Error	Release Release Settings Ti	ве ОК

- → To change the check count, touch [+] to increase the count or [-] to decrease it.
- 5 Touch [Release Time Settings].
- 6 Press the [C] key and, from the keypad, enter the time, after the lapse of which the access lock state of the Administrator Settings is canceled.



- → 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.
- \rightarrow In the Enhanced Security Mode, Release Time less than 5 min. cannot be set.
- 7 Touch [OK].

2.4 Canceling the Operation Prohibited State

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

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

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

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

Performing Release Setting

- ✓ For the procedure to call the Security Details screen on the display, see steps 1 and 2 of page 2-13.
- ✓ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.
- When the main power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. if there is no wait period between turning the main power switch off, then on again, the machine may not function properly.

Here is the sequence, through which the main power switch and sub power switch are turned on and off:

Turn off the sub power switch \rightarrow Turn off the main power switch \rightarrow Turn on the main power switch \rightarrow Turn on the sub power switch

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



3 Touch [Release].



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

	Choose item to release Prohibit Function and press [OK].
Bookmark	Administrator Settings > Prohibit Functions > Release Settings
Utility	House a Assaunts - Statuya Diriat - House Dati
Administrator Settings	USEPS & ACCOUNTLS SECURE PYTHL USEP BOX
Security Details	SNMP NebDAV Server
Prohibit Functions When Auth. Error	
Release Settings	25/02/2008 15:41 Henory 100%

5 Touch [OK].

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

2.5 Setting the Authentication Method

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

The User Authentication method may be [ON (MFP)] that uses the authentication system the machine has, [ON (External Server)] that uses a user information control system of the external server, or [OFF]. If the Enhanced Security Mode is set to [ON], the authentication method should be operated by either [ON (MFP)] or [ON (External Server)] (Active Directory).

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

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

NOTICE

Changing the Account Track setting erases all user and account information data that has previously been registered. This changes all Personal User Boxes owned by the users who are deleted and all Group User Boxes owned by the accounts that are deleted to Public User Boxes. If the password set for a particular box before this change does not meet the requirements of the Password Rules, however, no access can be made to the Public User Box, to which that specific box was changed. In this case, the Administrator must first new-ly set a password that meets the requirements of the Password Rules. For details of the Password Rules, see page 1-8.

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

2.5.1 Setting the Authentication Method

- ✓ For the procedure to call the Administrator Settings on the display, see page 2-2.
- ✓ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.
- 1 Call the Administrator Settings on the display from the control panel.
- 2 Touch [User Authentication/Account Track].



3 Touch [General Settings].



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



- → To use the External Server, the External Server must be registered in advance. For how to make the External Server Settings, see page 2-19.
- 5 Select [Account Track] and touch [ON].

	Touch the button for the desired	i setting.	
Bookmark	Administrator Settings > User #	Auth/Account Track > 0	General Settings
111:11:14	User Authentication	ON (MFP)	Job Setting
	Public User Access	Restrict	OFF
Administrator Settings	Account Track	ON	ON
User Authentication/	Account Track Input Wethod	Account Name & Password	
Account Track	Synchronize User Authen- tication & Account Track	Synchronize	
General Settings	1/2		
	12/26/2008 08:29 Memory 100%		ОК

- → If the Account Track is not to be used, go to step 7.
- 6 Select [Synchronize User Authentication & Account Track] and touch [Synchronize].

Decimant	Touch the button for the desired	d setting.	
DUUKIIAFK	Administrator Settings > User (Auth/Account Track > G	eneral Settings
Iltility	User Authentication	ON (MFP)	Job Setting
•	Public User Access	Restrict	Synchronize
Administrator Settings	Account Track	ON	Do Not Synchronize
↓ Vser	Account Track Input Hethod	Account Name & Password	
Account Track	Synchronize User Authen- tication & Account Track	Synchronize	
General Settings	↑ 1/2 ↓		
	04/02/2007 15:32 Memory 0%		ОК

- → When [Do Not Synchronize] is selected, both User Authentication and Account Track are checked each time the machine is used.
- 7 Touch [OK].
- 8 A message appears that prompts you to clear the use control data. Now, select [Yes] and touch [OK].

2.5.2 Setting the External Server

- If [ON (External Server)] 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 2-17.
- ✓ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.
- 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].

Poolmaria	To register a new server, touc server, select server name and	h [New]. To edit an existing then touch [Edit].	
BUUKIIIAFK	Administrator Settings > User	Auth./Account Track > External Se	erver Settings
Utility Administrator Settings	No. Server Name 01 02 03 04 03 04 05 06 07	Set as Default	1 /3
External Server Settings	New Edit	Delete	Close

- → To change or delete a previously registered server, touch [Edit] or [Delete].
- 5 Touch [Server Type].

	Make a selection.
Bookmark	[
	Administrator Settings > External Server Settings > New
()	Server Name
Utility	Server Type
Settings	
Vser	
Account Track	
External Server	
New	
	Menory 0%

6 Touch [Active Directory].

	Select the authentication server type.
Bookmark	Administrator Settings > New > Server Type
Utility	
Administrator Settings	Active Directory NTLH v1 NTLH v2
External Server Settings	NDS over TPX NDS over TCP/TP LDAP
New	
Server Type	12/26/2008 08:31

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



8 Touch [OK].

	Select the authentication server type.
Bookmark	Administrator Settings > New > Server Type
Utility	
Administrator Settings	Active Directory NTLH v1 NTLH v2
External Server Settings	NDS over IPX NDS over TCP/IP LDAP
New 🔸	
Server Type	12/26/2008 08:31 Henory 100%

- 9 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.
- 10 Touch [OK].
- 11 Touch [Close].
 - → If two or more External Servers have been registered, select any desired server and touch [Set as Default].

bizhub C360/C280/C220

2.6 ID & Print Setting Function

When access to the machine by the Administrator of the machine through the Administrator Settings from the control panel is authenticated, 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.

NOTICE

The Administrator must first make User Authentication settings before setting the ID & Print. For details of the User Authentication, see page 2-17.

Setting ID & Print

- ✓ For the procedure to call the Administrator Settings on the display, see page 2-2.
- ✓ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.
- 1 Call the Administrator Settings on the display from the control panel.
- 2 Touch [User Authentication/Account Track].



3 Touch [User Authentication Settings].



4 Touch [Administrative Settings].

Doolmant	Use the menu buttons or keypad to make a selection.
	Administrator Settings $>$ User Auth./Account Track $>$ User Auth. Settings
Utility	1 <u>ŝdeinistrative</u>
Administrator Settings	2 User Registration
User Authentication/	3 User Counter
User Auth.	
Settings	
	04/02/2007 15:46 Memory 0%

5 Touch [ID & Print Settings].

	Select item and enter setting.
Bookmark	Administrator Settings > User Auth. Settings > Administrative Settings
Utility	User Name List OFF
	Default Function Permission
Administrator Settings	ID & Print Settings
User Authentication/ Account Track	
User Auth. Settings	
Administrative Settings	25/02/2008 15:42 Webory 100%

6 Select [ON].

(Declaration)	Specify ID & Print settings.	
BOOKMARK	Administrator Settings > Administrative	e Settings > ID & Print Settings
	ID & Print	Public User
Utility Administrator Settings	<u>он</u>	Print Immediately
User Auth. Settings Administrative Settings	OFF	Save
ID & Print Settings	25/02/2008 15:43 Menory 100%	ОК

- 7 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.
2.7 System Auto Reset Function

When access to the machine by the Administrator of the machine through the Administrator Settings from the control panel is authenticated, the machine enables setting of the operation of the System Auto Reset function.

If no operations are performed for a predetermined period of time during access to the Administrator Settings or user mode (during setting of User Authentication) from the control panel, the System Auto Reset function automatically causes the user to log off from the mode. Processing of a specific function, however, takes precedence over the System Auto Reset function. That is, even if a predetermined period of time elapses during which no operations are performed, once the processing of the specific function has been started, the System Auto Reset function does not cause the user to log off from the mode.

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

Setting the System Auto Reset function

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



3 Touch [Reset Settings].

(Decimaria	Use the menu buttons or keypad to make a	selection.
DUUKIIIAFK	Administrator Settings > System Setting	5
		1/2 * -Back For- + #
Utility	1 Power Save Settings	6 Restrict User Access
Administrator Settings	2 Output Settings	7 Expert Adjustment
	3 Date/Time Settings	8 List/Counter
System Settings	4 Daylight Saving Time	9 Reset Settings
	5 Weekly Timer Settings	0 User Box Settings
	04/02/2007 15:41 Memory 02	Close

4 Touch [System Auto Reset].

Boolmark	Use the menu buttons or keypad to make a selection.
Bookmark Utility Administrator Settings System Settings Reset Settings	Administrator Settings> System Settings> Reset Settings 1 System Auto Reset 2 Auto Reset 3 Job Reset
	04/02/2007 15:42

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

Poolmark	Specify the length of time until the mag and the priority mode.	chine autonatically resets
DOOKIIIAT K	Administrator Settings> Reset Settings:	> System Auto Reset
	Priority Mode	System Auto Reset Time
Utility		1 Hinute
Administrator Settings	User Box	OFF
System Settings	Scan/Fax	
Reset Settings	Сору	
+		
System Auto Reset	2009/09/10 13:36 Memory 100%	ОК

- → 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.
- → Press the [C] key to clear all characters.
- 6 Touch [OK].

2-24

2.8 User Setting Function

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

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

Reference

- If [ON (External Server)] (Active Directory) is set for the authentication method, it is not possible to make user registration or change a User Password from the control panel. To register or change a user, make the settings on the server side. If PageScope Data Administrator is used for registering user information, however, the user name must match that registered in the External Server. Further, a User Password can be set, but is not to be used for authentication.
- If [ON (External Server)] (Active Directory) is set for the authentication method and if a user not registered with this machine is authenticated through user authentication, that particular user name is automatically registered in the machine.
- If [ON (External Server)] (Active Directory) is set for the authentication method and if a user registered with this machine is authenticated through user authentication, that particular user name, along with the External Server name, is automatically registered in the machine. No two User Names registered in an External Server may be alike.
- If the user authentication method is changed between [ON (MFP)] and [ON (External Server)], the user information registered under the previous authentication method cannot be used under the new authentication method.
- If the user authentication method is to be changed, be sure first to delete all user information used under the old authentication method and then change the user authentication method as necessary. If a previously registered user is deleted, the Personal User Box owned by that specific user is changed to Public User Box. If the password set for a particular box before this change does not meet the requirements of the Password Rules, however, no access can be made to the Public User Box, to which that specific box was changed. In this case, the Administrator must first newly set a password that meets the requirements of the Password Rules. For details of the Password Rules, see page 1-8.

Making user setting

<From the Control Panel>

- ✔ For the procedure to call the Administrator Settings on the display, see page 2-2.
- ✓ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.
- ✓ If synchronization with Account Track has been set, the account should be registered in advance. For how to make the Account Track Registration, see page 2-31.
- 1 Call the Administrator Settings on the display from the control panel.
- 2 Touch [User Authentication/Account Track].



3 Touch [User Authentication Settings].



4 Touch [User Registration].

	Use the menu buttons or keypad to make a selection.
Bookmark	Administrator Settings > User Auth./Account Track > User Auth. Settings
Utility	
Administrator Settings	2 User Registration
User Authentication/ Account Track	3 User Counter
User Auth.	
Settings	
	04/02/2007 15:46 Menory 0%

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

	After select	ing the user	, touch [Ed	it].		
Bookmark	Administrat	or Settings	> User Auth	entication :	Settings > Us	er Registration
Utility	001 user1	002 user2	003 user3	004	005	1/ 25
↓ Administrator	006	007	008	009	010	
Settings	011	012	013	014	015	
User Authentication/ Account Track	016	017	018	019	020	
User Auth. Settings	E	dit	De:	lete		
User Registration	04/27/2007 Memory	10:33				Close

- → To delete a previously registered user or change a User Password, touch the desired User Registration key.
- → To change a User Password, perform steps 6 through 8.

6 Touch [Password].

	Select the item to be registered/changed.
Bookmark	Admin. Settings > User Registration > Edit 1 /2 +Back For-
Iltility	User Name
•	Password
Administrator Settings	E-Hail Address
User Auth. Settings	Account Name
User	Output Permission Max. Allowance Set
Registration	Function Permission
Edit	12/26/2008 08:37 Kenory 1007

7 From the keyboard and keypad, enter a new User Password that may consist of 8 or more digits. To prevent entry of a wrong password, enter the password again in [Password Confirmation].

Use the keyboard or keypad to enter the password. Enter the password twice to confirm. Press Cit to Clear your entry.
Administrator Settings > Edit > Password
Password xxxxxxxx
Password Confirmation XXXXXXXX
+ + Pere
1 2 3 4 5 6 7 8 9 0
q w e r t y u i o p s t
a 5 d f 9 h i k 1 i i 1
Z X C V b n n , . / X Shift
2009/09/10 13:38 Henory 100%

- → Press the [C] key to clear all characters.
- → Touch [Delete] to delete the last character entered.
- → Touch [Shift] to show the upper case/symbol screen.
- → Touch [Cancel] to go back to the screen shown in step 6.
- 8 Touch [OK].
 - → If the User Password entered does not meet the requirements of the Password Rules, a message appears that tells that the User Password entered cannot be used. Enter the correct User Password. For details of the Password Rules, see page 1-8.
 - → If there is a mismatch in the User Passwords, a message appears that tells that there is a mismatch in the User Passwords. Enter the correct User Password.

9 Touch [Account Name].

	Select the item to be registered/changed.
Bookmark	Admin. Settings > User Registration > Edit 1 /2 +Back For +
	User Name
Utility	Password xxxxxxxxxx
Administrator Settings	E-Mail Address
User Auth.	
	Output Permission Hax. Allowance Set
User Registration	Function Parnission
Edit	12/26/2008 08:39

- → 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 PageScope Web Connection or application software, if Account Name is not registered, you cannot log onto the mode.
- → [Account Name] is not displayed if Account Track has not been set or synchronization with Account Track has not been set for the authentication method.
- **10** Select the desired Account.



- 11 Touch [OK].
- **12** Make the necessary settings.
 - → If the User Name is yet to be entered, [OK] cannot be touched. Be sure to enter the User Name.
 - → A User Name that already exists cannot be redundantly registered.
- 13 Touch [OK].
 - → To delete a previously registered user, touch [Delete] in step 5.
 - Check the contents of registration on the confirmation screen and select [Yes] and touch [OK] if the previously registered user is to be deleted. Note that, if a previously registered user is deleted, the Personal User Box owned by that specific user is changed to Public User Box. If the password set for a particular box before this change does not meet the requirements of the Password Rules, however, no access can be made to the Public User Box, to which that specific box was changed. In this case, the Administrator must first newly set a password that meets the requirements of the Password Rules. For details of the Password Rules, see page 1-8.

<From PageScope 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 PageScope Web Connection and access the Admin Mode.
- 2 Select [User Authentication Setting] from the pull-down menu of User Auth/Account Track and click [Display].

Edit View Favorites Tools Help	
🍇 Administrator	Logout 🥻
Ready to Scan	
in Menu (Admin Mo	ode) 🖸
Maintenance	Bex
Maintenance related settings.	User Box creation and operation.
Confirm ROM version, Import and Export data.	Document can be printed and routed from the User Box.
Meter Count 💽 Display	Open User Box 💽 Display
System Cottings	Brint Cotting
aystem aettings	Print Setting
User Box and Stamp settings.	Finit Settings Fonts and XPS Settings.
Machine Setting Visplay	Basic Setting 🔽 Display
Security	Store Address
Security related settings	
	Destination (addresses) registration.
Administrator Password and Address Permission Settings.	Destination (addresses) registration. E-mail, Subject and PrefbdSuffix Settings.
Administrator Password and Address Permission Settings. PKI Settings Viperation	Destination (addresses) registration. E-mail, Subject and Prefix/Suffix Settings.
Administrator Password and Address Permission Settings. PKI Settings Visplay	Destination (addresses) registration. E-mail, Subject and Prefix/Suffix Settings. Address Book
Administrator Password and Address Permission Settings. PKI Settings <u>Display</u> User Auth/Account Track	Destination (addresses) registration. E-mail, Subject and Prefx/Suffix Settings. Address Book
Administrator Password and Address Permission Settings. PKI Settings Display User Auth/Account Track User Authentication and Account Track Settings. Evanoral Server and Account Dates Pars Settings	Destination (addresses) registration. E-mail, Subject and Prefix/Suffix Settings. Address Book Display Fax Settings Fax Settings Fax Settings
Administrator Password and Address Permission Settings. Display VSer Auth/Account Track User Authentication and Account Track Settings. External Server and Group User Box Settings.	Destination (addresses) registration. E-mail, Subject and Prefix/Suffix Settings. Address Book V Display Fax Settings Fax Settings. Fax Settings. Fax Functions and Fax Report Settings.
Administrator Password and Address Permission Settings. PKJ Settings Display User Auth/Account Track User Authentication and Account Track Settings. External Server and Group User Box Settings. Authentication Method Display	Destination (addresses) registration. E-mail, Subject and Prefix/Suffix Settings. Address Book Fax Settings Fax Settings. Fax Functions and Fax Report Settings. Header/Footer Position Display
Administrator Password and Address Permission Settings. PKI Settings Display User Auth/Account Track User Authentication and Account Track Settings. External Server and Group User Box Settings. Authentication Method Display Authentication Method Display	Destination (addresses) registration. E-mail, Subject and Prefx/Suffix Settings. Address Book V Display Fax Settings Fax Settings. Fax Functions and Fax Report Settings. Header/Footer Position V Display
Administrator Password and Address Permission Settings. PKI Settings Display User Auth-Account Track User Authentication and Account Track Settings. External Server and Group User Box Settings. Authentication Method Juser Authentication Method Juser Authentication Setting Account Track Settings External Server Petitings	Destination (addresses) registration. E-mail, Subject and Prefx/Suffix Settings. Address Book V Display Fax Settings Fax Functions and Fax Report Settings. Fax Functions and Fax Report Settings. Header/Footer Position V Display Wizard
Administrator Password and Address Permission Settings. PKI Settings Display User Auth-Account Track External Server and Group User Box Settings. External Server and Group User Box Settings Authentication Method User Authentication Setting Account Track Settings External Server Settings External Server Settings External Server Settings	Destination (addresses) registration. E-mail, Subject and Prefix/Suffix Settings. Address Book Fax Settings Fax Settings Fax Functions and Fax Report Settings. Heeader/Footer Position Vizard Vizard Vizard Setup is performed.
Administrator Password and Address Permission Settings. PKJ Settings Display User Auth/Account Track User Authentication and Account Track Settings. External Server and Group User Box Settings. Authentication Method User Authentication Settinn Account Track Settings External Server Settings Public User Box Setting Public User Box Setting	Destination (addresses) registration. E-mail, Subject and Prefx/Suffix Settings. Address Book V Display Fax Settings Fax Settings Fax Functions and Fax Report Settings. Header/Footer Position V Display Wizard Wizard Wizard Setting setformed. The setting can be easily performed by following the orthographic arresdures
Administrator Password and Address Permission Settings. PKJ Settings Display User AuthAccount Track User Authentication and Account Track Settings. External Server and Group User Box Settings. Authentication Method Display Authentication Method Display User Authentication Setting External Server Settings Public User Box Settings User/Account Common Setting Scan to Home Settings	Destination (addresses) registration. E-mail, Subject and Prefx/Suffix Settings. Address Book V Display Fax Settings Fax Settings. Fax Functions and Fax Report Settings. Header/Footer Position V Display Wizard Wizard Setup is performed. The Setting can be easily performed by following the outlined procedures.

3 Click [New Registration].

<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools	Help				
	& Adm	inistrator		L	.ogout
	🤝 Rea	idy to Scan			
	n N	lenu (Admin Mode)			C
User Auth/Account Track 🔽 Dis	play			Ξ	, To Main Menu
Authentication Method	User Re	egistration			
⁷ User Authentication Setting	N	ew Registration			
User Registration			Course hu sumbar	4.50	
Default Function Permission			Search by humber.	1-50	
Account Track Settings	No.	User Name		Edit	Delete
External Server Settings	1	user1		Edit	Delete
Public User Box Setting	2	user2		Edit	Delete
User/Account Common Setting	2	10002		E dit	Delete
 User/Account Common Setting Scan to Home Settings 	3	user3		Edit	Delete

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

4 Make the necessary settings.

File Edit View Eavorites Tools	Help			1
	Administrator		Logout ?	
	Ready to Scan			
	n Menu (Admin Mode)		Q	
User Auth/Account Track 💌 Dis	play		E To Main Menu	
Authentication Method	User Registration			
▼ User Authentication Setting	No.			
User Registration	 Use opening number 			
Default Function Permission	C Input directly	(1-500)		
Account Track Settings	User Name	user1		
▶ External Server Settings	E-mail Address			
▶ Public User Box Setting	User Password			
User/Account Common Setting	Retype User Password			
Scan to Home Settings	Account Name			
Scan to Authorized Folder Settings		Search from List		
	<u> </u>	Registered Account Name		
		1	1	

- → A number that already exists cannot be redundantly registered.
- → A User Name that already exists cannot be redundantly registered.
- → The User Password to be registered must meet the requirements of the Password Rules. For details of the Password Rules, see page 1-8.
- → [Account Name] is not displayed if Account Track has not been set or synchronization with Account Track has not been set for the authentication method.
- → Click [Cancel] to go back to the previous screen.
- 5 Click [OK].
 - → If the User Password entered does not meet the requirements of the Password Rules, a message appears that tells that the User Password entered cannot be used. Click [OK] to go back to the screen of step 3. Perform steps 3 through 5 once again. For details of the Password Rules, see page 1-8.
 - → If there is a mismatch in the User Passwords, a message appears that tells that there is a mismatch in the User Passwords. Enter the correct User Password.
- 6 Check the message that tells that the setting has been completed. Then, click [OK].
 - → To delete a previously registered user, click [Delete] in step 3. Check the contents of registration on the confirmation screen and click [OK], then click it again if the previously registered user is to be deleted. Note that, if a previously registered user is deleted, the Personal User Box owned by that specific user is changed to Public User Box. If the password set for a particular box before this change does not meet the requirements of the Password Rules, however, no access can be made to the Public User Box, to which that specific box was changed. In this case, the Administrator must first newly set a password that meets the requirements of the Password Rules. For details of the Password Rules, see page 1-8.

2.9 Account Track Setting Function

When access to the machine by the Administrator of the machine through the Administrator Settings is authenticated, the machine enables registration of accounts, for which use of the machine is restricted. It also enables operations for deleting an account and changing an Account Password. In PageScope 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. An Account Password may consist of 8 digits. The password entered is displayed as "*" or "•."

Making account setting

<From the Control Panel>

- ✔ For the procedure to call the Administrator Settings on the display, see page 2-2.
- ✓ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.
- 1 Call the Administrator Settings on the display from the control panel.
- 2 Touch [User Authentication/Account Track].



3 Touch [Account Track Settings].



4 Touch [Account Track Registration].



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

	After select	ing account,	touch [Edi	t].		
Bookmark	Administrat	or Settings)	• Account Tr	ack Settings	> Account Trac	k Registration
Utility	001	002 2	003 3	004	005	1/ 25
	006	007	008	009	010	Í
Settings	011	012	013	014	015	
User Authentication/ Account Track	016	017	018	019	020	
Account Track Setting		dit _) [lete		J
Account Track Registration	12/26/2008 Memory	08:41				Close

- → To delete a previously registered account or change an Account Password, touch the desired Account Track Registration key.
- → To change an Account Password, perform steps 6 through 8.
- 6 Touch [Password].



7 From the keyboard and keypad, enter a new Account Password that may consist of 8 digits. To prevent entry of a wrong password, enter the password again in [Password Confirmation].

Use the keyboard or keypad to enter the password. Enter the password twice to confirm. Press [C] to clear your entry.
Administrator Settings > Edit > Password
Password xxxxxxxx
Password xxxxxxx
+ + Pete
1 2 3 4 5 6 7 8 9 0
q v e r t y u i o p c t
Z X C V b n n , . / X Shift
2009/09/10 13:45 Henory 1002

- → Press the [C] key to clear all characters.
- → Touch [Delete] to delete the last character entered.
- → Touch [Shift] to show the upper case/symbol screen.
- → Touch [Cancel] to go back to the screen shown in step 6.
- 8 Touch [OK].
 - → If the Account Password entered does not meet the requirements of the Password Rules, a message appears that tells that the Account Password entered cannot be used. Enter the correct Account Password. For details of the Password Rules, see page 1-8.
 - → If there is a mismatch in the Account Passwords, a message appears that tells that there is a mismatch in the Account Passwords. Enter the correct Account Password.
- 9 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.
- 10 Touch [OK].
 - → To delete a previously registered account, touch [Delete] in step 5. Check the contents of registration on the confirmation screen and select [Yes] and touch [OK] if the previously registered account is to be deleted. Note that, if a previously registered account is deleted, the Group User Box owned by that specific account is changed to Public User Box. If the password set for a particular box before this change does not meet the requirements of the Password Rules, however, no access can be made to the Public User Box, to which that specific box was changed. In this case, the Administrator must first newly set a password that meets the requirements of the Password Rules. For details of the Password Rules, see page 1-8.

<From PageScope 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 PageScope Web Connection and access the Admin Mode.
- 2 Select [Account Track Settings] from the pull-down menu of User Auth/Account Track and click [Display].

Edit View Favorites Tools Help	
Administrator	Logout ?
Ready to Scan	
In Menu (Admin Mode)	2
Maintenance	Box
Maintenance related settings. Confirm ROM version, Import and Export data.	User Box creation and operation. Document can be printed and routed from the User Box.
Meter Count 💽 Display	Open User Box 💌 Display
System Settings	Print Setting
Initial settings. User Box and Stamp settings.	Print Settings. Fonts and XPS Settings.
Machine Setting Display	Basic Setting Display
-	
security	Store Address
Security related settings. Administrator Password and Address Permission Settings.	Destination (addresses) registration. E-mail, Subject and Prefix/Suffix Settings.
PKI Settings 💽 Display	Address Book
User Auth/Account Track	Fax Settings
User Authentication and Account Track Settings. External Server and Group User Box Settings.	Fax Settings. Fax Functions and Fax Report Settings.
Authentication Method 🛛 🖌 Display	Header/Footer Position 💽 Display
Authentication Method	
Account Track Settings	Wizard
	Witzard Saturi is nerformed
External Server Settings	The second of the second
External Server Settings Public User Box Setting User/Account Common Setting	The setting can be easily performed by following the
External Server Settings Public User Box Setting User/Account Common Setting Scan to Home Settings	The setting can be easily performed by following the outlined procedures.

3 Click [New Registration].

no Far Teur (Franco Tean i	Adm	inistrator			Logout
	Rea	idy to Scan			
	🚺 ln N	lenu (Admin Mode)			8
User Auth/Account Track 🔽 Dis	play			Ξ.	To Main Menu
Authentication Method	Account	t Track Registration			
User Authentication Setting	N	ew Registration			
Account Track Settings			Search by pumber	1.50	Col
External Server Settings			Search by humber.	1-50	
Public User Box Setting	llo.	Account Name		Edit	Delete
User/Account Common Setting	1	1		Edit	Delete
Scan to Home Settings	2	2		Edit	Delete
Scan to Authorized Folder	3	3		Edit	Delete

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

4 Make the necessary settings.

<u>File Edit View Favorites Tools</u>	Help			
	🌆 Administrator		Logout ?	
	Ready to Scan			
	n Menu (Admin Mode)		2	
User Auth/Account Track 🔽 Di	splay		E To Main Menu	Ê
Authentication Method	Account Track Registration			
🕨 User Authentication Setting	No.			
Account Track Settings	Use opening number	2		
External Server Settings	C Input directly	(1-500)		
Public User Box Setting	Account Name	1		
User/Account Common Setting	(Use alphanumeric cl	naracters or symbols, with exception of sp	ace and ")	
Scan to Home Settings	Password	•••••		
	Retype Password	•••••		

- → A number that already exists cannot be redundantly registered.
- → An Account Name that already exists cannot be redundantly registered.
- → The Account Password to be registered must meet the requirements of the Password Rules. For details of the Password Rules, see page 1-8.
- → Click [Cancel] to go back to the previous screen.
- 5 Click [OK].
 - → If the Account Password entered does not meet the requirements of the Password Rules, a message appears that tells that the Account Password entered cannot be used. Click [OK] to go back to the screen of step 3. Perform steps 3 through 5 once again. For details of the Password Rules, see page 1-8.
 - → If there is a mismatch in the Account Passwords, a message appears that tells that there is a mismatch in the Account Passwords. Enter the correct Account Password.
- 6 Check the message that tells that the setting has been completed. Then, click [OK].
 - → To delete a previously registered account, click [Delete] in step 3. Check the contents of registration on the confirmation screen and click [OK], then click it again if the previously registered account is to be deleted. Note that, if a previously registered account is deleted, the Group User Box owned by that specific account is changed to Public User Box. If the password set for a particular box before this change does not meet the requirements of the Password Rules, however, no access can be made to the Public User Box, to which that specific box was changed. In this case, the Administrator must first newly set a password that meets the requirements of the Password Rules. For details of the Password Rules, see page 1-8.

bizhub C360/C280/C220

2.10 User Box Function

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

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

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

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

Reference

- If [ON (External Server)] (Active Directory) is set for the authentication method, the same Personal User Box name as that registered with the machine can be created and registered along with the External Server name. No two Personal User Box names registered in an External Server may be alike.
- If a document is saved in the copy, fax, or scan mode or from an external memory by specifying a User Box number that has not been registered, the Personal User Box owned by the user who logged on through User Authentication is automatically registered.

2.10.1 Setting the User Box

<From the Control Panel>

- ✓ For the procedure to call the Administrator Settings on the display, see page 2-2.
- ✓ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.
- ✓ For the procedure to change the user attributes, account attributes, and User Box Password, see page 2-42.
- 1 Call the Administrator Settings on the display from the control panel.
- 2 Touch [One-Touch/User Box Registration].



3 Touch [Create User Box].



4 Touch [Public/Personal User Box].



5 Touch [New].

Job List	To register a new User Box, touch [New]. To edit an existing User Box, select desired User Box and touch [Edit].
DOONIILITY	Administrator Settings > Create User Box > Public/Personal User Box
	ABC DEF GHI JKL MNO PORS TUV WKYZ etc
Utility	Name Type Create Date/Time
Administrator Settings	
One-Touch/	
User Box Reg.	
Create User Box	
+	New Delete Empty User Box(es)
User Box	04/02/2007 16:29 Memory 0%

→ To change the setting of a User Box, touch the desired User Box key.

Poolmark	To register To edit an e	a new User Box, touch [xisting User Box, selec	New]. t desired	User Box and touc	h [Edit].
DOOKIIAI K	Administrat	or Settings > Create Us	er Box > P	Public/Personal Us	er Box
	ABC DE	F GHI JKL MNO	PQRS	TUV WXYZ <mark>etc</mark>)
Utility	User Box Number	Nane	Туре	Create Date/Time	
+	1	Public User Box	Public	12/17/2008 13:58	
Administrator	2	Personal User Box	Per- sonal	12/17/2008 13:59	
Jettings	3	Group User Box	Group	12/17/2008 13:59	
One-Touch/ User Box Reg.					
Create User Box	Nou	Fut	Delete	Delete Engly	
Public/Personal User Box	12/26/2008 Memory	08:45 100%	Derete	USEF Box (ES)	Close

- → To change the User Box Password, user attributes and account attributes, touch [Edit].
- → To delete a User Box, touch [Delete]. A confirmation message appears. Select [Yes] and touch [OK] to delete the specified User Box.

bizhub C360/C280/C220

6 Select the User Box Type.

Poolmanda	Enter the User Box passw	ord.			
<u> </u>	Administrator Set > Put	lic/Personal > Ne	1/2	←Back	For- ward →
	User Box No.	4	1 -	9999999999	
Utility	User Box Nane				
4 Administrator	Password				
Settings	Index	etc			
Create User Boy	Туре	Public	Personal	Group	
	Time Stored	12/26/2008 08:4	6		
Public/Personal					
New	12/26/2008 08:46 Memory 1002			ance1	0К]

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

	Select the owner of the User Box.
Bookmark	Administrator Settings > Edit Public/Personal User Box > Change Owner
	Owner Name
Utility	
Administrator Settings	User1 User2 1/ 1
Public/Personal User Box	
Edit	
Change Owner	12/26/2008 08:46

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

	Select the account that owns the User Box.
()	
Bookmark	Administrator Settings > Edit Public/Personal User Box > Change Owner
	Account Name
Iltility	
Administrator	1 2 1 1
Settings	
+	3
Public/Personal User Box	
+	
Edit	
· · ·	
Chenge Owner	12/26/2008 08:47 OK
	Menory 100%

7 Touch [Password].

Decimant	Enter the User Box passw	ord.			
	Administrator Set > Pub	lic/Personal >	New 1/2	← Back	For- ⊎ard →
	User Box No.	4	1.	9999999999	
Utility	User Box Name				
Administrator	Password				
Settings	Index	etc			
Create User Boy	Туре	Public	Personal	Group	
Create Oser DOA	Time Stored	12/26/2008 0	8:46		
Public/Personal User Box					
New	12/26/2008 08:46			Cance1	OK)

bizhub C360/C280/C220

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

Pie Pao The	ase input a new password with the keyboard or ten-key . It is necessary to input it twice to confirm password. : password input with a clear key can be deleted.
Administrator Settings	> New Public/Personal User Box > User Box Password
Password	xxxxxxxx
Password Confirmation	хохококок
	Pete
1 2 3	4 5 6 7 8 9 0
q w e	rtyui opet
a s d	f g h i k l : :]
Z X C	V b n n / X Shift
200 Mer	9/09/10 13:47 007 100%

- → Press the [C] key to clear all characters.
- → Touch [Delete] to delete the last character entered.
- → Touch [Shift] to show the upper case/symbol screen.
- → Touch [Cancel] to go back to the screen shown in step 7.
- 9 Touch [OK].
 - → If the User Box Type is set to [Public], set a User Box Password that meets the requirements of the Password Rules. For details of the Password Rules, see page 1-8.
 - → If there is a mismatch in the User Box Passwords, a message appears that tells that there is a mismatch in the User Box Passwords. Enter the correct User Box Password.
- **10** Make the necessary settings.

	Specify the settings. Enter User Box number us	ing the keypad.		
BOOKMARK	Administrator Set > Pub	lic/Personal > New	1/2 -Back For	•
	User Box No.	4	1 - 999999999	
Utility	User Box Name			
Administrator	Password	*>>>>		
Settings	Index	etc		
Create User Box	Туре	Public Pe	rsonal Group	J
	Time Stored	12/26/2008 08:47	_	
Public/Personal User Box				
New	12/26/2008 08:47		Cance1 01	к)

- → 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.
- 11 Touch [OK].

<From PageScope 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 2-42.
- 1 Start PageScope Web Connection and access the Admin Mode.
- 2 Select [Create User Box] from the pull-down menu of Box and click [Display].

Edit View Eavorites Tools He	alo		
For Tex Line Lines Teen Lin	Administrator	Logout	2
	Ready to Scan		
	In Menu (Admin Mode	•)	
Maintonanco	_	Bay	
Maintenance related settings. Confirm ROM version, Import and E	Export data.	User Box creation and operation. Document can be printed and routed from the User Box.	
Meter Count	Display	Open User Box Display	
System Settings Initial settings. User Box and Stamp settings.		<u>Create User Box</u> Open System User Box Create System User Box Frimt seutings Fonts and XPS settings.	
Machine Setting	V Display	Basic Setting Display	
Security Security related settings. Administrator Password and Addre Sattings	ss Permission	Store Address Destination (addresses) registration. E-mail, Subject and PrefuxSuffix Settings.	
Security Security related settings. Administrator Password and Addre Settings. PKI Settings	ss Permission	Store Address Destination (addresses) registration. E-mail, Subject and PrefwSuffix Settings. Address Book	
Security Security related settings. Administrator Password and Addre Settings PKI Settings User Auth/Account Track	ss Permission	Store Address Destination (addresses) registration. E-mail, Subject and PrefoxSuffix Settings. Address Book	
Security Security related settings. Administrator Password and Addre Settings. PKI Settings User Auth/Account Track User Authentication and Account Tr External Server and Group User Bo	Display	Store Address Destination (addresses) registration. E-mail, Subject and PrefwSuffix Settings Address Book Fax Settings Fax Settings Fax Settings Fax Settings. Fax Functions and Fax Report Settings.	
Security Security related settings. Administrator Password and Addre Settings PKI Settings User Auth/Account Track User Authentication and Account Tr External Server and Group User Bo Authentication Method	S Permission Display Display Ack Settings. Settings. Display	Store Address Destination (addresses) registration. E-mail, Subject and Prefx/Suffix Settings. Address Book	
Security Security Security related settings. Administrator Password and Addre Settings PKI Settings User Auth/Account Track User Authentication and Account Tr External Server and Group User Bo Authentication Method Network	v Display rack Settings. v Settings.	Store Address Destination (addresses) registration. E-mail, Subject and Prefu%Suffix Settings. Address Book Fax Settings Pax Settings Pax Settings. Pax Settings. Header/Footer Position Wizard Stare	
Security Security related settings. Administrator Password and Addre Settings. PKI Settings User Auth/Account Track User Auth/Account Track User Authentication and Account Tr External Server and Group User Bo Authentication Method Network Network E-mail and Open API Settings.	v Display vack Settings. v Settings. v Display	Store Address Destination (addresses) registration. E-mail, Subject and Prefu%Suffx Settings. Address Book	

3 Make the necessary settings.

<u>8</u>		
<u>Eile E</u> dit <u>View</u> Favorites <u>T</u> ools	Help	
	凝 Administrator	Logout ?
	Ready to Scan	
	n Menu (Admin Mode)	3
Box 🕑	Display	E To Main Menu
▶ Open User Box	Create User Box(Public/Group/Persona	l)
Create User Box	Box is the function to save documents in the n Documents in the Box can be used for printing	nachine. 1. sending etc.
Open System User Box	User Box Number	
Create System User Box	Use opening number	
	C Input directly	(1-999999999)
	User Box Name	Public User Box
	Vise Box Password.	
	User Box Password	•••••
	Retype User Box Password	•••••
	Index	
	Specify a keyword for Box search and dis	splay by Name.
		etc 💌
	Туре	Public 💌
	Auto Delete Document	
	Do Not Delete	
	C Specify days	1 day
	C 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 enter the User Name of the owner of the User Box in the "Owner Name" box.
- → If [Group] is selected from the User Box Type pull-down menu, click [Account List] and select the account from the registered account list, or enter the Account Name of the owner of the User Box in the "Account Name" box.
- 4 Click [OK].
 - → If the User Box Type is set to [Public], set a User Box Password that meets the requirements of the Password Rules. For details of the Password Rules, see page 1-8.
 - → If there is a mismatch in the User Box Passwords, a message appears that tells that there is a mismatch in the User Box Passwords. Enter the correct User Box Password.
 - → If no Owner Name is entered, a message appears that tells that no Owner Names have been entered. Enter the correct Owner Name.
 - → If a user name not registered with the machine is entered in the "Owner Name" box, a message appears that tells that the Owner Name entered in the box is illegal. Click [OK] to go back to the screen of step 3. Perform steps 3 and 4 once again.
 - → 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. Click [OK] to go back to the screen of step 3. Perform steps 3 and 4 once again.

2.10.2 Changing the user attributes and account attributes

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

<From the Control Panel>

- ✓ For the procedure to call the User Box setting screen on the display, see steps 1 through 4 of page 2-36.
- ✓ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.
- ✔ 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].

Rookmark	To register To edit an e	a new User Box, touch E kisting User Box, selec	Ne₩]. t desired	User Box and touch	[Edit].
DOONIIUTK	Administrat	or Settings > Create Us	er Box > F	Public/Personal User	Вох
	ABC DEF	GHI JKL MNO	PQRS	TUV WXYZ etc	
Utility	User Box	Nane	Туре	Create Date/Time	
+	1	Public User Box	Public	12/17/2008 13:58	1/ 1
Administrator	2	Personal User Box	Per- sonal	12/17/2008 13:59	
Jettings	3	Group User Box	Group	12/17/2008 13:59	
One-Touch/ User Box Reg.					
Create User Box					
Public/Personal	New	Edit	Delete	Delete Empty User Box(es)]
User Box	12/26/2008 Memory	08:45 100%			Close

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

	Select item and enter set	tting.
Bookmark	Select index in the Addre	ess Book.
DOONIIUTK	Administrator Settings >	> User Box > Edit 1/2 ←Back 🛛 🛱 →
	User Box No.	2 1 - 999999999
Utility	User Box Name	Personal User Box
↓ Administrator	Password	****
Settings	Index	etc
	Туре	Public Personal Group
Create User Box	Time Stored	12/17/2008 13:59
Dublic/Dorconal		
User Box	Owner Name	user1 Change Owner
Edit	12/26/2008 08:51 Memory 100%	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 requirements of the Password Rules. For details of the Password Rules, see page 1-8.

bizhub C360/C280/C220

4

5

is [Group].



- For [Change Owner], select the desired owner name.
 - the owner of the User Box. Job List Administrator Settings > Edit Public/Personal User Box > Change Owner Owner Name user1 Administrator Settings 1/ 1 usera blic/Per Change Own ОК 06/11/2007 15:44
 - → For [Change Account Name], select the desired account name.

	Select the account that owns the User Box.
Bookmark	Administrator Settings > Edit Public/Personal User Box > Change Owner
	Account Name
Utility	
Administrator Settings	2 1/ 1
₽ublic/Personal	3
User Box	
Edit	
Change Owner	
Chenge Owner	12/26/2008 08:51 Memory 100%

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

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



- → Press the [C] key to clear all characters.
- → Touch [Delete] to delete the last character entered.
- → Touch [Shift] to show the upper case/symbol screen.
- → Touch [Cancel] to go back to the screen shown in step 3.
- 9 Touch [OK].
 - → If the User Box Type is changed to [Public], set a User Box Password that meets the requirements of the Password Rules. For details of the Password Rules, see page 1-8.
 - → If there is a mismatch in the User Box Passwords, a message appears that tells that there is a mismatch in the User Box Passwords. Enter the correct User Box Password.
- **10** Touch [OK].

<From PageScope 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 PageScope Web Connection and access the Admin Mode.
- 2 Select [Open User Box] from the pull-down menu of Box and click [Display].

Edit View Favorites Tools Help	
🌆 Administrator	Logout ?
Ready to Scan	
In Menu (Admin Mo	ode)
Maintenance	Box
Maintenance related settings.	User Box creation and operation.
Confirm RUM version, import and Export data.	Document can be printed and routed from the User Box.
Meter Count	Open User Box
Pustom Pottings	Create User Box
aystem aetungs	Create System User Box
User Box and Stamp settings.	Fonts and XPS Settings.
Machine Setting 🗸 Display	Basic Setting V Display
Security	Store Address
Security Security related settings.	Store Address Destination (addresses) registration.
Security Security related settings. Administrator Password and Address Permission Settings.	Store Address Destination (addresses) registration. E-mail, Subject and Prefix/Suffix Settings.
Security Security related settings. Administrator Password and Address Permission Settings. PKI Settings Display	Store Address Destination (addresses) registration. E-mail, Subject and Prenu9Suffix Settings. Address Book
Security Security related settings. Administrator Password and Address Permission Settings PKI Settings Vipplay	Store Address Destination (addresses) registration. E-mail, Subject and Prefix/Suffix Settings. Address Book
Security Security related settings. Administrator Password and Address Permission Settings PKI Settings User Auth/Account Track	Store Address Destination (addresses) registration. E-mail, Subject and Prefix/Suffix Settings. Address Book Fax Settings
Security Security related settings. Administrator Password and Address Permission Settings PKI Settings User Auth/Account Track User Authentication and Account Track Settings. Federal Server and Crunu Lister Prox Settings	Store Address Destination (addresses) registration. E-mail, Subject and Prefix/Suffix Settings. Address Book Display Fax Settings. Fax Settings. Fax Settings. Fax Settings.
Security Security Security Security Security Security Security Display VSer Auth/Account Track User Authentication and Account Track Settings. External Server and Group User Box Settings. External Server and Group User Box Settings.	Store Address Destination (addresses) registration. E-mail, Subject and Prefix/Suffix Settings. Address Book
Security Security related settings. Administrator Password and Address Permission Settings PKI Settings User Auth/Account Track User Authentication and Account Track Settings. External Server and Group User Box Settings. Authentication Method Setters	Store Address Destination (addresses) registration. E-mail, Subject and Prefix/Suffix Settings. Address Book Display Fax Settings Fax Settings. Fax Functions and Fax Report Settings. Header/Footer Position
Security Security Security Security Security Security Display VSer Auth/Account Track User Auth/Account Track Settings. External Server and Account Track Settings. External Server and Group User Box Settings. Authentication Method Display Network	Store Address Destination (addresses) registration. E-mail, Subject and PrefloSuffix Settings. Address Book Display Fax Settings Fax Functions and Fax Report Settings. Header/Footer Position Display Wizard
Security Security Security Security Security Security Security Display VSer Auth/Account Track User Auth/Account Track User Authentication and Account Track Settings. External Server and Group User Box Settings. External Server and Group User Box Settings. Setter Server and Settings. Setwork Network related Settings.	Store Address Destination (addresses) registration. E-mail, Subject and Prefix/Suffix Settings. Address Book Display Fax Settings. Fax Functions and Fax Report Settings. Header/Footer Position Display Wizard Wizard Setup is performed.
Security Security Security Administrator Password and Address Permission Settings PKI Settings V Display USer Auth/Account Track User Authentication and Account Track Settings. External Server and Group User Box Settings Authentication Method Display Network Network Network E-mail and Open API Settings.	Store Address Destination (addresses) registration. E-mail, Subject and PrefixeSuffix Settings. Address Book Display Fax Settings. Fax Functions and Fax Report Settings. Header/Footer Position Display Wizard Wizard Setting is performed. The setting rocedures.

3 Enter the desired User Box Number and click [OK].

2 Elle Edit View Enviroites Teals	Hele			
Elle Edit Alexa Legaquites Tools	Administrator			Logout ?
	Ready to Scar			
	In Menu (Admi	n Mode)		3
Box 🔽 D	isplay			E To Main Menu
▶ Open User Box	Open User Box(F	ublic/Group/Personal)		
► Create User Box	Box is the function	to save documents in the machin	1e.	
Open System User Box	vocuments in the B	ox can be used for printing, seni	ang etc.	
Create System User Box	User Box Numbe	r	2 (1-9	199999999)
	_			OK
	User Box List	Search from In	dex	ALL 🖌 Go
		Page (Display	by 50 cases)	1 💌 Go
	User Box Number	User Box Name	Туре	Time Stored
	1	Public User Box	Public	2008/12/17 13:58
	2	Personal User Box	Personal	2008/12/17 13:59
	3	Group User Box	Group	2008/12/17 13:59
				8

4 Click [User Box Setting].

2										
Eile	Edit	View	Favorites	Tools	Help					
					Administrator				Logout ?	
					Ready to Scan					
					In Menu (Admin M	lode)			8	
Bo>				■ D	isplay				E To Main Menu	
► 0j	oen Us	er Box			User Box Number	2	User Box Name	Personal User Box		
► Cr	eate l	Jser Bo	x		Туре	Personal	Owner Name	user1		
⊳ oj	oen Sy	rstem U	lser Box		Box Operation	User	Box Setting	Delete User Box		
► Ci	eate s	System	User Box							
_					_				Cancel	

- → Go to step 6 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.
- 5 Click the "User Box Owner is changed." check box and change the user attributes of the box.

<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites	ools <u>H</u> elp	
	Administrator	Logout ?
	Ready to Scan	
	In Menu (Admin Mode)	3
Box	Display	E To Main Menu
▶ Open User Box	User Box Attribute Change	
Create User Box	User Box Number 2	2
Open System User Box	User Box Name	Personal User Box
Create System User Box	Index	etc 💌
	User Box Expansion Function is changed.	
	Confidential RX	OFF M
	New Communication Password	
	Retype New Communication Password	
	User Box Password is changed.	
	New Password	
	Returns New Persound	
	TOTADE JADAA LOSSAACH O	
	Vuser Box Owner is changed.	
	Туре	Personal 🗸
	Owner Name	llearlist
	Overlai Marid	
		OK Const

→ The following screen appears if the account attributes are to be changed.

)			
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools	Help		
	Search Administrator	Logout ?	
	Ready to Scan		
	In Menu (Admin Mode)	3	
Box 🔽 🚺	Display	E To Main Menu	Ľ
 Open User Box Create User Box Open System User Box Create System User Box 	User Box Attribute Change User Box Number User Box Name Index	2 Personal User Box etc	
	User Box Expansion Function is changed. Confidential RX New Communication Password Retype New Communication Password	OFF V	
	User Box Password is changed. New Password Retype New Password		
	Ver Box Owner is changed. Type Account Name	Group	
		OK Cancel	

- → Click [User List] to select a specific user from the registered User List.
- → A user name may be directly entered in the Owner Name box.
- → Click [Account List] to select a specific account from the registered Account List.
- → An account name may be directly entered in the Account Name box.
- → 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.
- → Enter the User Name that has been registered through User Registration for the Owner Name.
- → Enter the Account Name that has been registered through Account Registration for the Account Name.
- 6 Click the "User Box Password is changed." check box and enter the User Box Password.
- 7 Click [OK].
 - → If the User Box Type is changed to [Public], set a User Box Password that meets the requirements of the Password Rules. For details of the Password Rules, see page 1-8.
 - → If there is a mismatch in the User Box Passwords, a message appears that tells that there is a mismatch in the User Box Passwords. Enter the correct User Box Password.
 - → If no Owner Name is entered, a message appears that tells that no Owner Names have been entered. Enter the correct Owner Name.
 - → If a user name not registered with the machine is entered in the "Owner Name" box, a message appears that tells that the Owner Name entered in the box is illegal. Click [OK] to go back to the screen of step 4. Perform steps 4 through 7 once again.
 - → 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. Click [OK] to go back to the screen of step 4. Perform steps 4 through 7 once again.

2.11 Changing the Administrator Password

When access to the machine by the Administrator of the machine through the Administrator Settings from the control panel is authenticated, the machine enables the operation of changing the Administrator Password required for accessing the Administrator Settings.

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

Changing the Administrator Password

- ✔ For the procedure to call the Security Settings screen on the display, see steps 1 and 2 of page 2-10.
- ✓ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.
- 1 Call the Security Settings screen on the display from the control panel.
- 2 Touch [Administrator Password].

Dealmark	Use the menu buttons or keypad to make a selection.	
	Administrator Settings> Security Settings	
Utility	1 Administrator Password 6 HDD Settings	
4 Administrator	2 <u>Veer Box Administrator</u> 7 Function Hanagement Setting	ettings
Settings	3 Administrator Security 8 Stamp Settings	
Security Settings	4 Security Details	
	5 Enhanced Security Hode 0 BRAYSER TONS SECTION	19
	01/06/2007 15:24 Menory 100%	Close

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

Use the keyboard or keypad to enter the current password. Press ICI to erase the entered password.
Administrator Settings> Security Settings> Administrator Password Setting
xxxxxxxxx
1 2 3 4 5 6 7 8 9 0 - ^
9 V E F L Y U I D P D L
a 5 d f g h i k l : :]
ZXCVbnn,./XShift
Space
2009/09/10 13:55 Henory 1002

- → Press the [C] key to clear all characters.
- → Touch [Delete] to delete the last character entered.
- → Touch [Shift] to show the upper case/symbol screen.
- → Touch [Cancel] to go back to the Security Settings screen.
- 4 Touch [OK].
 - → If there is a mismatch between the currently registered Administrator Password and the Administrator Password entered, a message appears that tells that there is a mismatch in the Administrator Passwords. Enter the correct Administrator Password.
 - → If the Enhanced Security Mode is set to [ON], entry of a wrong password is counted as unauthorized access. If a wrong Administrator Password is entered a predetermined number of times (once to three times) or more set by the Administrator of the machine, the Utility screen appears and the machine is set into an access lock state. To cancel the access lock state, settings must be made by the Service Engineer; or, turn off, and then turn on, the main power switch of the machine. If the main power switch is turned off and on, the access lock state is canceled after the lapse of time set for [Release Time Settings]. When the main power switch is turned off, then on again, wait at least

bizhub C360/C280/C220

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

Here is the sequence, through which the main power switch and sub power switch are turned on and off:

Turn off the sub power switch \rightarrow Turn off the main power switch \rightarrow Turn on the main power switch \rightarrow Turn on the sub power switch

5 Enter the new 8-digit Administrator Password from the keyboard and keypad. To prevent entry of a wrong password, enter the password again in [Password Confirmation].



- → Press the [C] key to clear all characters.
- → Touch [Delete] to delete the last character entered.
- → Touch [Shift] to show the upper case/symbol screen.
- → Touch [Cancel] to go back to the Security Settings screen.
- 6 Touch [OK].
 - → If the Administrator Password entered does not meet the requirements of the Password Rules, a message appears that tells that the Administrator Password entered cannot be used. Enter the correct Administrator Password. For details of the Password Rules, see page 1-8.
 - → If there is a mismatch in the Administrator Passwords, a message appears that tells that there is a mismatch in the Administrator Passwords. Enter the correct Administrator Password.

2.12 Protecting Data in the HDD

When access to the machine by the Administrator of the machine through the Administrator Settings from the control panel is authenticated, the machine enables the operation for setting and changing the Encryption Key.

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 "*."

Reference

- When an Encryption Key (encryption word) is set using HDD Encryption Setting, an Encryption Key with a key length of 128 bits is generated using the SHA-1 algorithm. The generated encryption key is used to encrypt or decrypt data through AES encryption algorithm.
- When the Encryption Key (encryption word) is set, the encryption strength can be selected from among [Encryption Priority] or [Overwrite Priority]. For more details, see page 2-50.

2.12.1 Setting the Encryption Key (encryption word)

- ✓ For the procedure to call the Security Settings screen on the display, see steps 1 and 2 of page 2-10.
- ✓ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.
- ✓ 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 of the machine 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 more details, ask the Service Representative.
- ✓ To change the Encryption Key, see page 2-55.
- 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 2-10.
- 1 Call the Security Settings screen on the display from the control panel.
- 2 Touch [HDD Settings].



3 Touch [HDD Encryption Setting].



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

Bookmark	The HDD will need to be formatted after HDD encryption is set. Are you sure you want to continue?
Utility Administrator Settings Security Settings HDD Settings	Yes No
	04/03/2007 13:42

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



- → Press the [C] key to clear all characters.
- → Touch [Delete] to delete the last character entered.
- → Touch [Shift] to show the upper case/symbol screen.
- → Touch [Cancel] to go back to the HDD Settings screen.
- 6 Touch [OK].
 - → If the Encryption Key entered does not meet the requirements of the Password Rules, a message appears that tells that the Encryption Key entered cannot be used. Enter the correct Encryption Key. For details of the Password Rules, see page 1-8.
 - → If there is a mismatch in the Encryption Keys, a message appears that tells that there is a mismatch in the Encryption Keys. 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.

Bookmark	The encryption passphrase was set, changed or canceled. Turn the main switch OFF and ON.
Utility	
Administrator Settings	
Security Settings	
HDD Settings	
Setting	04/03/2007 13:43 Memory 0%

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

Here is the sequence, through which the main power switch and sub power switch are turned on and off:

Turn off the sub power switch \rightarrow Turn off the main power switch \rightarrow Turn on the main power switch \rightarrow Turn on the sub power switch

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

Job List	Reset the encryption passphrase or format the HDD.
Name Status	
Delete	
🛛 Job Details 🚽	
Y M C K	10/06/2006 09:28 Memory 100%

- 9 Call the Administrator Settings on the display from the control panel.
 - → For the procedure to call the Administrator Settings on the display, see page 2-2.
- 10 Touch [HDD Format].

Booknark	Select	(HDD F	ornat]	or	[Reset	Encryption	Passphras	sel to	release	the error.	
	Admini	strato	or Sett	i ngs	> HDD	Encryption	Setting				
Utility Administrator Settings HDD Encryption Setting			HD	D Fo	rmat		Reset E	псгур	tion Pass	phrase	
	10/06/2 Memory	2006	09:29 100%							Close)

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

Booknark	A ^{D0}	you want to	format the H	IDD ?		
Utility Administrator Settings HDD Encryption Setting						
Format HDD	10/06/2006	09:29	Yes		No	ОК

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.

Bookmark	HDD Plea	was formatted. ase turn the main switch OFF and ON.
Utility Administrator Settings		
HDD Encryption Setting		
	10/06/2006 Henory	09:31 100%

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

Here is the sequence, through which the main power switch and sub power switch are turned on and off:

Turn off the sub power switch \to Turn off the main power switch \to Turn on the main power switch \to Turn on the sub power switch

- → To make the setting of [Encryption Priority] or [Overwrite Priority], go to step 13.
- → [Encryption Priority] refers to writing of data in HDD with an enhanced encryption strength. It is recommended that [Encryption Priority] be selected to achieve a greater effect of encryption.
- → [Overwrite Priority] refers to writing of data in HDD through the standard encryption technique.
- → [Encryption Priority] is the default setting.
- 13 Call the HDD Settings screen on the display from the control panel.
 - → For the procedure to call the HDD Settings screen on the display, see steps 1 and 2 of page 2-50.
- **14** Touch [Overwrite HDD Data].

Bookmark	Use the menu buttons or keypad to make a selection.
	Administrator Settings> Security Settings> HDD Settings
Utility	Check HDD Capacity 6 HDD Encryption Setting
Administrator Settings	2 Overwrite HDD Data
Security Settings	3 Overwrite All Data
	4 HOD Lock Password
HUD Settings	5 TOTRIAL HOU
	01/28/2009 15:00 Close

15 Touch [Encryption Priority] or [Overwrite Priority].



- 16 Touch [OK].
 - → If the setting is changed in step 15, the screen shown in step 17 will appear. Perform HDD Format.
- **17** A confirmation message appears. Select [Yes] and touch [OK].

Bookmark	The hard disk must be reformatted after changing encryption priority/overwrite priority. Are you sure you want to continue?	
Utility		
Administrator Settings		
Security Settings		
HDD Settings	Yes No	
Temporary Data	04/03/2007 14:04 Memory 02	ОК

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



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

Here is the sequence, through which the main power switch and sub power switch are turned on and off:

Turn off the sub power switch \rightarrow Turn off the main power switch \rightarrow Turn on the main power switch \rightarrow Turn on the sub power switch

2.12.2 Changing the Encryption Key

- For the procedure to call the Encryption Key entry screen on the display, see steps 1 through 4 of page 2-50.
- ✓ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.
- 1 Call the Encryption Key entry screen on the display from the control panel.
- 2 Enter the currently registered 20-digit Encryption Key from the keyboard and keypad.



- → Press the [C] key to clear all characters.
- → Touch [Delete] to delete the last character entered.
- → Touch [Shift] to show the upper case/symbol screen.
- → Touch [Cancel] to go back to the HDD Settings screen.
- **3** Select [Edit] and touch [OK].
 - → If there is a mismatch in the Encryption Keys, a message appears that tells that there is a mismatch in the Encryption Keys. Enter the correct Encryption Key.
- 4 Enter the new 20-digit Encryption Key from the keyboard and keypad. To prevent entry of a wrong Encryption Key, enter the Encryption Key again in [Encryption Passphrase Confirmation].



- → Press the [C] key to clear all characters.
- → Touch [Delete] to delete the last character entered.
- → Touch [Shift] to show the upper case/symbol screen.
- → Touch [Cancel] to go back to the HDD Settings screen.
- 5 Touch [OK].
 - → If the Encryption Key entered does not meet the requirements of the Password Rules, a message appears that tells that the Encryption Key entered cannot be used. Enter the correct Encryption Key. For details of the Password Rules, see page 1-8.
 - → If there is a mismatch in the Encryption Keys, a message appears that tells that there is a mismatch in the Encryption Keys. 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.

Bookmark	The encryption passphrase was set, changed or canceled. Turn the main switch OFF and ON.
Utility	
Administrator Settings	
Security Settings	
HDD Settings	
HDD Encryption	
Setting	04/03/2007 13:43
	Memory 02
	nenor y u/a

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

Here is the sequence, through which the main power switch and sub power switch are turned on and off:

Turn off the sub power switch \rightarrow Turn off the main power switch \rightarrow Turn on the main power switch \rightarrow Turn on the sub power switch

2.13 Overwrite All Data Function

When access to the machine by the Administrator of the machine through the Administrator Settings from the control panel is authenticated, the machine enables setting of the operation of the Overwrite All Data function.

When the machine is to be discarded, or use of a leased machine is terminated at the end of the leasing contract, the Overwrite All Data function overwrites and erases all data stored in all spaces of the HDD. The function also resets all passwords saved in the NVRAM to factory settings, preventing leak of data. For details of items that are cleared by the Overwrite All Data function, see page 1-10.

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 \rightarrow random numbers \rightarrow 0x00.
Mode 3	Overwrites with $0x00 \rightarrow 0xff \rightarrow random numbers \rightarrow verifies.$
Mode 4	Overwrites with random numbers \rightarrow 0x00 \rightarrow 0xff.
Mode 5	Overwrites with $0x00 \rightarrow 0xff \rightarrow 0x00 \rightarrow 0xff$.
Mode 6	Overwrites with $0x00 \rightarrow 0xff \rightarrow 0x00 \rightarrow 0xff \rightarrow 0x00 \rightarrow 0xff \rightarrow random numbers.$
Mode 7	Overwrites with $0x00 \rightarrow 0xff \rightarrow 0x00 \rightarrow 0xff \rightarrow 0x00 \rightarrow 0xff \rightarrow 0xaa$.
Mode 8	Overwrites with $0x00 \rightarrow 0xff \rightarrow 0x00 \rightarrow 0xff \rightarrow 0x00 \rightarrow 0xff \rightarrow 0xaa \rightarrow verifies.$

Setting the Overwrite All Data function

- ✓ For the procedure to call the HDD Settings screen on the display, see steps 1 and 2 of page 2-50.
- ✓ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.
- 1 Call the HDD Settings screen on the display from the control panel.
- 2 Touch [Overwrite All Data].



3 Select the desired mode and touch [Delete].



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

Bookmark	Are you sure you want to overwrite all data in the hard disk and system memory?
Utility	
Administrator Settings	
Security Settings	
0verwrite	Yes No
Overwrite All Data	2009/09/10 14:09 Weeks the first /

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.

Bookmark		
	Administrat	or Settings> HDD Settings> Overwrite All Data
Utility		
+		
Administrator Settings		All data has been overwritten and erased. Turn the main switch OFF and ON
Security Settings		
+		
HDD Settings		
+		
Overwrite	03/04/2002	12.21
	Memory	100%

- → Check that all data has been overwritten and erased properly. Data is not erased properly if an error occurs during the procedure. For more details, consult the 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.

Here is the sequence, through which the main power switch and sub power switch are turned on and off:

Turn off the sub power switch \rightarrow Turn off the main power switch \rightarrow Turn on the main power switch \rightarrow Turn on the sub power switch

→ After the main power switch has been turned on, quickly turn it off and give the machine to the Service Engineer. If the Overwrite All Data function is executed by mistake, contact the Service Engineer. For more details, consult the Service Representative.

bizhub C360/C280/C220
2.14 SSL Setting Function

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

2.14.1 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.
- ✔ The key length set for the public key of the server generated in SSL certificate setting is 1024 bits.
- 1 Start PageScope Web Connection and access the Admin Mode.
- 2 Select [PKI Settings] from the pull-down menu of Security and click [Display].

a			
<u>E</u> lle <u>E</u> dit <u>V</u> lew F <u>a</u> vorites <u>T</u> ools <u>H</u> elp			A
Administrator	Logout	?	^
Ready to Scan			
In Menu (Admin Mode	e)	2	
Maintenance	Box		
Maintenance related settings. Confirm ROM version, Import and Export data.	User Box creation and operation. Document can be printed and routed from the User Box.		
Meter Count 💽 Display	Open User Box 🛛 Display		
System Settings	Print Setting		
Initial settings. User Box and Stamp settings.	Print Settings Fonts and XPS Settings.		
Machine Setting 🛛 🖌 Display	Basic Setting 🗾 Display		
Security	Store Address		
Security related settings. Administrator Password and Address Permission Settings.	Destination (addresses) registration. E-mail, Subject and Prefix/Suffix Settings.		
PKI Settings V Display	Address Book 🗸 Display		
PKI Settings			
Address Reference Setting	Fax Settings		
Restrict User Access Auto Logout Settings.	Fax Settings.		
Administrator Password Setting	Fax Functions and Fax Report Settings.		
Authentication Method Visplay	Header/Footer Position VIsplay		
Network	Wizard		
Network-related Settings. E-mail and Open API Settings.	Wizard Setup is performed. The setting can be easily performed by following the outlined procedures.		
TCP/IP Setting Display	TX Setting for scan documents. 🔽 Display		~

3 Click [New Registration].

<u>e</u>]					
<u>Eile Edit View Favorites Iools E</u>	<u>t</u> elp				
	🌆 Administrator			Logout	?
	Ready to Scan				
	In Menu (Admin Mode)			1	3
Security 🔽 Dis	play			E To Main Mer	nu
▼ PKI Settings	Device Certificate List				
Device Certificate Setting	New Periotration				
▶ SSL Setting	New Registration	-	N	1	
▶ Protocol Setting	Default Issuer	Subject	Period	Detail Setting	
External Certificate Setting					_
 Certificate Verification Settings 			[OK Cancel	
Address Reference Setting					
Restrict User Access					
► Auto Logout					

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



5 Make the necessary settings.

<u>ð</u>		
Eile Edit Yiew Favorites Iools E	telp	
	🌆 Administrator	Logout ?
	Ready to Scan	
	In Menu (Admin Mode)	G
Security 🗸 Dis	play	E To Main Menu
▼ PKI Settings	Create and install a self-sigr	ned Certificate.
Device Certificate Setting	Common Name	localhost
▶ SSL Setting	Organization	
▶ Protocol Setting	Organizational Unit	
▶ External Certificate	Locality	
Setting	State/Province	
Certificate Verification	Country	
Settings	Admin. E-mail Address	admin@test.local
Address Reference Setting		
Restrict User Access	Validity Start Date	01/20/2009 11:17:00
▶ Auto Logout	Validity Period	Day(s)(1-3650)
	- Encryption Key Type	RSA-1024 ¥
	8	OK Cancel

- → 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.

Certifica	ate has been created and installed. SSL/TLS can now be used.	
(Alter O	N IS CIICKEU, SSL MODE SELLING WIII DE AVAIIADIE.)	
	Certifica (After O	Certificate has been created and installed. SSL/TLS can now be used. (After OK is clicked, SSL Mode setting will be available.)

2.14.2 SSL Setting

- ✓ For call the PKI Settings screen on the display, see steps 1 and 2 of page 2-59.
- ✓ 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.

NOTICE

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 2-59.

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

Eile Edit View Favorites Iools E	telp			1
	🌆 Administrator		Logout	?
	Ready to Scan			
	In Menu (Admin Mode)		6	3
Security 🔽 Dis	play		🚛 To Main Men	iu
▼ PKI Settings	SSL Setting			
▶ Device Certificate Setting	Mode using SSL/TLS	[Admin. Mode and User Mode 🔽	
► SSL Setting	Encryption Strength	AES-256, 3DES-16	8 💌	
▶ Protocol Setting				
External Certificate Setting			OK Cancel	
Certificate Verification Settings				
▶ Address Reference Setting				
▶ Restrict User Access				

- → Select "Admin. Mode and User Mode" for "Mode using SSL/TLS."
- → For encryption strength, select the strong "AES-256, 3DES-168."
- → In the Enhanced Security Mode, the setting cannot be changed to one containing strength lower than AES/3DES.
- 4 Click [OK].

8						
Eile	<u>E</u> dit	⊻iew	Favorites <u>T</u> ools	Help		1
			Comp	eted.		
					UK	

2.14.3 Removing a Certificate

- ✔ For call the PKI Settings screen on the display, see steps 1 and 2 of page 2-59.
- ✓ 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 PageScope Web Connection and call the PKI Settings screen on the display.
- 2 Click [Setting].
- 3 Select [Remove a Certificate] and click [OK].

2		
<u>Elle E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools !	Help	
	🌆 Administrator	Logout ?
	Ready to Scan	
	In Menu (Admin Mode)	3
Security 🔽 Dis	play	E To Main Menu
▼ PKI Settings	Create Device Certificate	
Device Certificate Setting	Remove a Certificate	
▶ SSL Setting	○ Export Certificate	
▶ Protocol Setting		
External Certificate Setting		OK Cancel
 Certificate Verification Settings 		
Address Reference Setting		
Restrict User Access		
► Auto Logout		

4 Click [OK].

<u>File Edit View Favorites Tools E</u>	telp		
	Administrator		Logout ?
	Ready to Scan		
	In Menu (Admin Mode		3
Security 🔽 Dis	play		💷 To Main Menu
▼ PKI Settings	Remove a Certific:	ate	
Device Certificate Setting	lssuer	test	
	Subject	test	
▶ SSL Setting	Validity Period	05/23/2009 11:17:00	
▶ Protocol Setting		ant to remove the certificate?	
External Certificate Setting		and to remove the certificater	
 Certificate Verification Settings 			OK Cancel
▶ Address Reference Setting			
Restrict User Access			
Auto Logout			
Auto Logout			

5 Click [OK] and restart the machine.

4															[
Eile	<u>E</u> dit	View	F <u>a</u> vorites	Tools	Help											.
			т	urn the	main s	vitch O)FF, ar	nd then	NON.	wher	n chan	aina s	ettings			
			-				•							OK		

bizhub C360/C280/C220

2.15 S/MIME Communication Setting Function

When access to the machine by the Administrator of the machine through the Administrator Settings is authenticated, the machine enables the setting of encryption of text of e-mail transmitted and received between the PC and the machine.

NOTICE

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

2.15.1 Setting the S/MIME Communication

<From the Control Panel>

- ✓ For the procedure to call the Administrator Settings on the display, see page 2-2.
- ✓ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.
- 1 Call the Administrator Settings on the display from the control panel.
- 2 Touch [Network Settings].
- **3** Touch [E-Mail Settings].

	Use the menu buttons or keypad to make	a selection.
Bookmark	Administrator Settings > Network Setti	ngs
		1/2 * ← Back 📴 → #
Utility	1 TCP/IP Settings	6 LDAP Settings
Administrator	2 NetWare Settings	7 E-Mail Settings
Network	3 HTTP Server Settings	8 SNMP Settings
Settings	4 FTP Settings	9 AppleTalk Settings
	5 SHB Settings	0 Bonjour Setting
	06/12/2007 13:26 Menory 100%	Close

4 Touch [S/MIME Communication Settings].

Bookmark	Use the menu buttons or keypad to make a selection. Administrator Settings> Network Settings> E-Mail Settings	
Utility Administrator Settings Hetwork Settings E-Mail Settings	1 E-Hail TX (SHTP) 2 E-Hail RX (POP) 3 Sattring communication	
	26/04/2007 14:43	Close

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



6 Select encryption method and touch [OK].

	Specify	the encrypti	on method f	or e-mail	text.		
BOOKMALK	Adnin.	Settings > S	MIME Conn.	Settings	> E-Mail Text	Encryption	Method
Utility			RC2-40		RC2-64		
Administrator Settings			RC2-128		DES		
E-Mail Settings			3DES		AES-128		
S/NIME Conn. Settings			AES-192		AES-256		
E-Mail Text Encrypt. Method	26/04/20 Memory	007 14:47 100%					ОК

- → For encryption method, select the strong "3DES," "AES-128," "AES-192," or "AES-256." If the mail software being used does not support AES, encrypted mail messages may be received, but they cannot be decrypted. Use AES-compliant mail software or select the encryption method that is the strongest of all compliant with the currently used mail software.
- → Each encryption method represents the following. Name: encryption algorithm: encryption key length 3DES: 3 key triple DES: 168 bits AES-128: AES: 128bit AES-192: AES: 192bit AES-256: AES: 256bit
- → In the Enhanced Security Mode, the setting cannot be changed to "RC2" or "DES."
- 7 Touch [OK].

<From PageScope 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 PageScope Web Connection and access the Admin Mode.
- 2 Select [E-mail Setting] from the pull-down menu of Network and click [Display].

<u>E</u> ile <u>E</u> dit <u>Vi</u> ew F <u>a</u> vorites <u>T</u> ools <u>H</u> elp	🕂 💦 👘
加 Administrator	Logout 🤗
Ready to Scan	
in Menu (Admin Mo	de)
Maintenance	Box
Maintenance related settings. Confirm ROM version, Import and Export data.	User Box creation and operation. Document can be printed and routed from the User Box.
Meter Count 💽 Display	Open User Box 💽 Display
System Settings	Print Setting
Initial settings. User Box and Stamp settings.	Print Settings Fonts and XPS Settings.
Machine Setting 🔽 Display	Basic Setting V Display
Security	Store Address
Security related settings. Administrator Password and Address Permission Settings.	Destination (addresses) registration. E-mail, Subject and Prefix/Suffix Settings.
TCP/IP Setting E-mail Setting Display	Address Book 💽 Display
LDAP Setting IPP Setting	
FTP Setting SNMP Setting	Fax Settings
SMB Setting Settings. Web Service Settings ttings.	Fax Settings. Fax Functions and Fax Report Settings.
Bonjour Setting Display	Header/Footer Position
AppleTalk Setting WebDAV Settings	
OpenAPI Setting	Wizard
ICP Socket Setting	Wizard Setup is performed.
LLTD Setting	The setting can be easily performed by following the
SSDP Settings	outlinea procédures.
TCP/IP Setting V Display	TX Setting for scan documents. 🔽 Display

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

<u>Eile E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools	Help	
	Administrator	Logout ?
	Ready to Scan	
	n Menu (Admin Mode)	3
Network 🔽 Dis	play	E To Main Menu
▶ TCP/IP Setting	E-mail RX (POP)	18 -
▼ E-mail Setting	E-mail RX Setting	ON 💌
► E-mail RX (POP)	POP Server Address	Please check to enter host name.
▶ E-mail TX (SMTP)		0.0.0.0
▶ S/MIME	Login Name	
▶ LDAP Setting	Password is changed.	
▶ IPP Setting	Password	
🕨 FTP Setting	APOP Authentication	OFF V
SNMP Setting	MDN Response	ON V
🖎 SMB Setting	Connection Timeout	30 🗸
🕨 Web Service Settings	Port Number	110
Bonjour Setting		(1-66535)
🕨 NetWare Setting	Dise SSLILS	hor
AppleTalk Setting	Certificate Verification Level Settings	[555] (1-65535)
🖹 Network Fax Setting	Validity Period	Confirm
🕨 WebDAV Settings	CN	Do Not Confirm 💙
OpenAPI Setting	Key Usage	
TCP Socket Setting	Chain	Do Not Confirm ¥
EEEE802.1X Authentication Setting	Expiration Date Confirmation	
LLTD Setting	Expiration Date Commitmation	
		OK Cancel

4 Make the necessary settings.



- → For encryption method, select the strong "3DES," "AES-128," "AES-192," or "AES-256." If the mail software being used does not support AES, encrypted mail messages may be received, but they cannot be decrypted. Use AES-compliant mail software or select the encryption method that is the strongest of all compliant with the currently used mail software.
- → Each encryption method represents the following. Name: encryption algorithm: encryption key length 3DES: 3 key triple DES: 168 bits AES-128: AES: 128bit AES-192: AES: 192bit AES-256: AES: 256bit
- \rightarrow In the Enhanced Security Mode, the setting cannot be changed to "RC2" or "DES."
- 5 Click [OK].
- 6 Click [OK].

8							
Eile	<u>E</u> dit	⊻iew	Favorites	Tools	Help		
			С	omple	eted.		
						OK	

2.15.2 Registering the certificate

- ✓ 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 PageScope Web Connection and access the Admin Mode.
- 2 Select [Address Book] from the pull-down menu of Store Address and click [Display].

e <u>E</u> dit <u>Vi</u> ew F <u>a</u> vorites <u>T</u> ools <u>H</u> elp	
🌆 Administrator	Logout ?
Ready to Scan	
in Menu (Admin Mode	
Maintenance	Box
Maintenance related settings.	User Box creation and operation.
Confirm ROM version, Import and Export data.	Document can be printed and routed from the User Box.
Meter Count 💽 Display	Open User Box 🔽 Display
System Settings	Print Setting
Initial settings. User Box and Stamp settings.	Print Settings Fonts and XPS Settings.
Machine Setting	Basic Setting V Display
Security	Store Address
Security related settings.	Destination (addresses) registration.
Administrator Password and Address Permission Settings.	E-mail, Subject and Prefix/Suffix Settings.
PKI Settings V Display	Address Book
	Address Book
liser Auth/Account Track	Group Program
Licer Authentication and Account Track Settings	Temporary One-Touch
External Server and Group User Box Settings.	Subject
Authentication Method 🛛 V Display	Prefix/Suffix Display
Network	Wizard
Network-related Settings.	Wizard Setup is performed.
E-mail and Open API Settings.	i ne seπing can be easily performed by following the outlined procedures.
TCD/ID Setting	TV Setting for econ decumente

3 Click [New Registration].

<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u>	ools <u>H</u> elp						
	🌆 Administr	ator			l	Logout	?
	ready to	o Scan					
	🚺 In Menu	(Admin Mode)					C
Store Address 🛛 👻	Display				Ξ	To Main Me	enu
▼ Address Book	Address Bo	ok List					
Store Address	The other pa	rty who wants to transmit data ca	n be registered.				
▶ Icon	New F	Registration					
 Icon Group 	New F	Registration	Search by number.	1	-50	Y Go	
 Icon Group Program 	New F	Registration	Search by number.	1	-50	Go	
loon froup Program Temporary One-Touch	New F	Registration	Search by number. Search from Index	[]	-50	Go Go	
 Icon Group Program Temporary One-Touch Subject 	New F	Registration	Search by number. Search from Index	S/MIME	-50 Edit	Go Go Delete	
Icon Vilan Coo Foron Frogram Temporary One-Touch Subject Text	New F	Registration	Search by number. Search from Index	_1 [S/MIME	-50 Edit	Go Go Delete Delete	

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

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

<u>Eile E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools	Help	
	Administrator	Logout ?
	Ready to Scan	
	In Menu (Admin Mode)	3
Store Address	Display	🚛 To Main Menu
▼ Address Book	New Registration	
Store Address	E-mail	
▶ Photo/Icon	C FTP	
P Photo/Icon	C SMB	
▶ Group	C WebDAV	
▶ Program	C User Box	
▶ Temporary One-Touch	C Fax	
▶ Subject	C IP Address Fax	
b T .	C Internet Fax	
P lext		
Prefix/Suffix		
		OK Cancel

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

ile <u>E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ool	s <u>H</u> elp	
	Administrator	Logout ?
	Ready to Scan	
	in Menu (Admin Mode)	8
Store Address	Display	E To Main Menu
▼ Address Book	Address Book (E-mail)	
Store Address	No.	
▶ Icon	Use opening number	
▶ Group	C Direct Input	
▶ Program	Name	
Temporary One-Touch	Index	
Subject	Specify a keyword for address search and display by registered name.	
> Subject	etc 💌	
⊫ lext	∏ Main	
	Destination Information E-mail Address	
		OK Cancel

- → Set 1024 bits or more for the key length of the RSA public key for the certificate of each destination.
- 6 Make the necessary settings.
 - → A number that already exists cannot be redundantly registered.
 - → If Name and E-mail Address have not been registered, a message appears that tells that Name and E-mail Address are yet to be entered. Enter the correct Name and E-mail Address.
- 7 Click [OK].

2.16 SNMP Setting Function

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

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

2.16.1 Changing the auth-password and priv-password

<From the Control Panel>

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

	Use the menu buttons or keypad to make	a selection.
Bookmark	Administrator Settings	
		1/2 * -Back 📴 - #
Utility	1 System Settings	6 Copier Settings
Administrator	2 Administrator/ Machine Settings	7 Printer Settings
Seccings	3 One-Touch/User Box Registration	8 Fax Settings
	4 User Authentication/ Account Track	9 System Connection
	5 Network Settings	0 Security Settings
	25/02/2008 15:40 Menory 1007	Close

3 Touch [SNMP Settings].



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



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

	To specify the context name, touch [Context Name].
Bookmark	
	Administrator Settings > SNMP Setting > SNMP v3 Setting
	1 /5 ←Back Fara →
Utility	Context Name Settings
·	
Administrator Settings	Context Name
+	
Network Settings	
+	
SNMP Setting	
+	
SNMP v3 Setting	08/24/2007 11:47

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

Paolemark	Specify SNMPv3/write setting. Password to do Security Level setting.	nust be set
DUUKIIIAFK	Administrator Settings > SNMP Setting :	> SNMP v3 Setting
		4 /5 ←Back For-→
Utility	Write User Name Settings	Security Level
Administrator Settings Network Settings	Write User Name	OFF auth-password auth-password/priv-password
SNMP Setting		Password Setting
SNMP v3 Setting	2007/09/03 15:23 Memory 100%	ОК

7 Touch [Write auth].

	Specify Pass	word Settings	of v3 Settings. Select a para	meter.
Bookmark	Administrat	or Settings >	SNMP v3 Setting > Password Se	tting
			Password Setting	
Utility		Read auth		
Administrator Settings		Read priv	жнононон	
SNMP Setting		Write auth	*******	
SNMP v3 Setting		Write priv	****	
Password Setting	04/03/2007	14:35		Close

bizhub C360/C280/C220

- → When a screen appears that prompts you to enter the current password, enter the MAC Address that is set in the machine. To check the MAC Address, from [Network Settings] of step 2, select [Forward] → [Detail Settings] → [Device Setting].
- → The entry of a wrong SNMP password (auth-password, priv-password) is counted as unauthorized access, if the Enhanced Security Mode is set to [ON]. If a wrong SNMP password (auth-password, priv-password) is entered a predetermined number of times (once to three times) or more set by the Administrator of the machine, the machine is set into an access lock state, rejecting any more logon attempts. To cancel the access lock state, perform the Release Setting by the Administrator of the machine.
- 8 Enter the new 8-digit-or-more auth-password from the keyboard and keypad.



- → Press the [C] key to clear all characters.
- → Touch [Delete] to delete the last character entered.
- → Touch [Shift] to show the upper case/symbol screen.
- → Touch [Cancel] to go back to the previous screen.
- 9 Touch [OK].
 - → If the auth-password entered does not meet the requirements of the Password Rules, a message appears that tells that the auth-password entered cannot be used. Enter the correct auth-password. For details of the Password Rules, see page 1-8.
- 10 To prevent entry of a wrong password, enter the auth-password again.



- → Press the [C] key to clear all characters.
- → Touch [Delete] to delete the last character entered.
- → Touch [Shift] to show the upper case/symbol screen.
- → Touch [Cancel] to go back to the previous screen.
- 11 Touch [OK].
 - → Go to step 12 if [auth-password/priv-password] is selected in step 6.
 - → If there is a mismatch in the auth-passwords, a message appears that tells that there is a mismatch in the auth-passwords. Enter the correct auth-password.

12 Touch [Write priv].

	Specify Pass	sword Settings of	v3 Settings. Select a parameter.	
Bookmark	Administrat	tor Settings > SN	MP v3 Setting > Password Setting	
			Password Setting	
Utility		Read auth		
Administrator Settings		Read priv	*****	
SNMP Setting		Write auth	*****	
SNMP v3 Setting		Write priv	*****	
Password Setting	04/03/2007 Memory	14:35 100%	[C10	5e]

- → When a screen appears that prompts you to enter the current password, enter the MAC Address that is set in the machine. To check the MAC Address, from [Network Settings] of step 2, select [Forward] → [Detail Settings] → [Device Setting].
- → The entry of a wrong SNMP password (auth-password, priv-password) is counted as unauthorized access, if the Enhanced Security Mode is set to [ON]. If a wrong SNMP password (auth-password, priv-password) is entered a predetermined number of times (once to three times) or more set by the Administrator of the machine, the machine is set into an access lock state, rejecting any more logon attempts. To cancel the access lock state, perform the Release Setting by the Administrator of the machine.
- **13** Enter the new 8-digit-or-more priv-password from the keyboard and keypad.

	Enter the new using the key your entry, i	W Write priv- Wooard or keyp press the [C]	assword ad. To erase key.			
Administrator Sett	ings > Passwor	rd Settings >	Enter Write	Priv-Password	I	

-						
1 2	3 4	56	7 8	90		<u> </u>
Q V	e r	t y	u i			ſ
a s	d f	g h	jk			1
Z X	C V	b n	n ,		/	Shift
	2009/09/10 Memory	14:16 100%		Enlarge ON	Cance1	ОК

- → Press the [C] key to clear all characters.
- → Touch [Delete] to delete the last character entered.
- → Touch [Shift] to show the upper case/symbol screen.
- → Touch [Cancel] to go back to the previous screen.
- 14 Touch [OK].
 - → If the priv-password entered does not meet the requirements of the Password Rules, a message appears that tells that the priv-password entered cannot be used. Enter the correct priv-password. For details of the Password Rules, see page 1-8.

15 To prevent entry of a wrong password, enter the priv-password again.



- → Press the [C] key to clear all characters.
- → Touch [Delete] to delete the last character entered.
- → Touch [Shift] to show the upper case/symbol screen.
- → Touch [Cancel] to go back to the previous screen.
- 16 Touch [OK].
 - → If there is a mismatch in the priv-passwords, a message appears that tells that there is a mismatch in the priv-passwords. Enter the correct priv-password.
- 17 Touch [Close] and [OK].

<From PageScope 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 PageScope Web Connection and access the Admin Mode.
- 2 Select [SNMP Setting] from the pull-down menu of Network and click [Display].

Edit View Favorites Tools Help	
Administrator 🏤	Logout ?
Ready to Scan	
In Menu (Admin Mode	<u>)</u>
Maintenance	Bex
Maintenance related settings. Confirm ROM version, Import and Export data.	User Box creation and operation. Document can be printed and routed from the User Box.
Meter Count 👽 Display	Open User Box 🔽 Display
System Settings	Print Setting
Initial settings	Print Settings
User Box and Stamp settings.	Fonts and XPS Settings.
Machina Satting	Rooid Setting
Machine Getting	Dasie Getting
Security	Store Address
Security related settings.	Destination (addresses) registration.
Administrator Password and Address Permission	E-mail, Subject and Prefix/Suffix Settings.
TCP/IP Setting	
E-mail Setting Display	Address Book 🔽 Display
LDAP Setting	
ETP Setting	Fou Cottinue
SNMP Setting	Fax settings
SMB Setting Bettings.	Fax Settings.
Web Service Settings tings.	Fax Functions and Fax Report Settings.
Bonjour Setting Display	Header/Footer Position 👽 Display
Netware Setting	
lAnnie Jalk Setting	
WebDAV Settings	
AppleTalk Setting WebDAV Settings OpenAPI Setting	Wizard
Apple laik Setting WebDAV Settings OpenAPI Setting TCP Socket Setting	Wizard Wizard Setup is performed
Apple Jak Setting WebDAV Settings OpenAPI Setting TCP Socket Setting IEEE802.1X Authentication Setting	Wizard Wizard Setup is performed. The setting can be easily performed by following the
Apple talk Setting WebDAV Settings OpenAPI Setting TCP Socket Setting IEEE802.1X Authentication Setting LITD Setting SCDD Setting	Wizard Wizard Setup is performed. The setting can be easily performed by following the odlined procedures.
Apple talk Setting WebDAY Settings OpenAPI Setting TCP Socket Setting IEEE802.1X Authentication Setting LITD Setting SSDP Settings	Wizard Wizard Setup is performed. The setting can be easily performed by following the outlined procedures.

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

Eile	Edit	⊻iew	F <u>a</u> vorites	Tools	Help			1
						pro-passwora		
						Write User Name	restrict	
						Security Level	auth-password/priv-password 💙	
						auth-password		
						Password is changed. (Passw	vord is currently set.)	
						Current Password		
						New Password		
						Retype New Password		
						priv-password		
						Password is changed. (Passw	vord is currently set.)	
						Current Password		
						New Password		
						Retype New Password		
						Encryption Algorithm	DES 💌	
						Authentication Method	MD5 V	

- → For the current password, enter the MAC Address that is set in the machine. To check the MAC Address, see step 7 of page 2-69.
- → The entry of a wrong SNMP password (auth-password, priv-password) is counted as unauthorized access, if the Enhanced Security Mode is set to [ON]. If a wrong SNMP password (auth-password, priv-password) is entered a predetermined number of times (once to three times) or more set by the Administrator of the machine, the machine is set into an access lock state, rejecting any more logon attempts. To cancel the access lock state, perform the Release Setting by the Administrator of the machine.

- 4 Click [OK].
 - → If the auth-password and priv-password entered does not meet the requirements of the Password Rules, a message appears that tells that the auth-password and priv-password entered cannot be used. Enter the correct auth-password and priv-password. For details of the Password Rules, see page 1-8.

2.16.2 SNMP access authentication function

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

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

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

Reference

- If [auth-password] has been selected for Security Level, hashing is used for the authentication information (auth-password) to be transmitted. The machine allows you to select either HMAC-MD5 or HMAC-SHA1 for hashing.
- If [auth-password/priv-password] has been selected for Security Level, the authentication information (auth-password/priv-password) and data (object ID that specifies the object to be changed, value to be set, etc.) to be transmitted are used for hashing and encryption. The machine allows you to select either CBC-DES or CBC-AES for encryption.
- For accessing the MIB, use the MIB browser corresponding to the above encryption algorithm.

2.16.3 SNMP v3 setting function

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

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

For the auth-password and priv-password, enter the password that meets the requirements of the Password Rules. For details of the Password Rules, see page 1-8.

To change the setting,	specify the	corresponding object ID	. See the table below for	the setting items.
0 0/				0

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

2.16.4 SNMP network setting function

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

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

2.17 WebDAV Function

When access to the machine by the Administrator of the machine through the Administrator Settings is authenticated, the machine enables setting of the WebDAV Server Password. The Administrator of the machine can gain access to the WebDAV Server over the network by using the WebDAV Server Password. WebDAV Server Password may consist of 8 digits. The password entered for the authentication purpose appears as "*" or "•" on the display.

Setting the WebDAV Server Password

<From the Control Panel>

- ✓ For the procedure to call the Network Settings screen on the display, see steps 1 and 2 of page 2-69.
- ✓ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.
- ✓ Unauthorized access could result if the WebDAV Server Password required for accessing the WebDAV Server is incorrectly set. The Administrator of the machine should therefore make sure to set the appropriate password and control its operation so that the password is not leaked.
- ✓ The entry of a wrong WebDAV Server password is counted as unauthorized access, if the Enhanced Security Mode is set to [ON]. If a wrong WebDAV Server password is entered a predetermined number of times (twice, four times, or six times) or more set by the Administrator of the machine, the machine is set into an access lock state, rejecting any more logon attempts. To cancel the access lock state, perform the Release Setting by the Administrator of the machine.
- 1 Call the Network Settings screen on the display from the control panel.
- 2 Touch [Forward \rightarrow] and touch [WebDAV Settings].

	Use the menu buttons or keypad to make a	selection.		
BOOKMARK	Administrator Settings > Network Settings			
		2/2 ★ ←Back For- → #		
Utility	1 TCP Socket Settings	6 SSDP Settings		
Administrator		7 Detail Settings		
	3 WebDAV Settings	8 IEEE802.1X Authentication Settings		
Settings	4 Web Service Settings	9 Web Browser Setting		
	5 BMLinkS Settings			
	2009/09/10 14:22 Ислогу 1007	Close		

3 Touch [WebDAV Server Settings].

Bookmark	Use the menu Administrat	i buttons or keypad to make a selection. .cor Settings > Network Settings > WebDAW Settings
Utility Administrator Settings Utility Administrator Settings Utility Administrator Settings	2	keDOAV Client Settings
	25/02/2008 Memory	15:53

4 Select [ON] and touch [Password Setting].

	Select a parameter.	
Bookmark	Administrator Cottings > WohDAU Cotting	an N NobDAIL Connor Cottings
	Administrator Settings > WebDAV Setting	JS > WebDAV Server Settings
	ON OFF	
Utility	SSL Setting	Password Setting
+		
Administrator		Password Setting

Network	SSL Only	
Settings		
WebUAV Settings		
Settings	12/26/2008 09:09	ОК
	Menory 100%	

5 Enter the new WebDAV Server Password from the keyboard and keypad. To prevent entry of a wrong password, enter the password again in [Password Confirmation].

Please input a new password with the keyboard or ten-key pad. It is necessary to input it twice to confirm password. The password input with a clear key can be deleted.
Administrator Settings > WebDAV Server Settings > Password Setting
Password
Passuord Confirmation XXXXXXXX
← → <u>Pête</u>
1 2 3 4 5 6 7 8 9 0
9 V C T L Y L 1 0 P D L
a 5 d f 9 h j k 1 ; ;]
ZXCVDNN, / NShift
Cancel OK

- → Press the [C] key to clear all characters.
- → Touch [Delete] to delete the last character entered.
- → Touch [Shift] to show the upper case/symbol screen.
- → Touch [Cancel] to go back to the screen shown in step 4.
- 6 Touch [OK].
 - → If the WebDAV Server Password entered does not meet the requirements of the Password Rules, a message appears that tells that the WebDAV Server Password entered cannot be used. Enter the correct WebDAV Server Password. For details of the Password Rules, see page 1-8.
 - → If there is a mismatch in the WebDAV Server Passwords, a message appears that tells that there is a mismatch in the WebDAV Server Passwords. Enter the correct WebDAV Server Password

<From PageScope 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 PageScope Web Connection and access the Admin Mode.
- 2 Select [WebDAV Settings] from the pull-down menu of Network and click [Display].

Talk How Provider Tark Hole	
Edit view Favorites Loois Help	
🎥 Administrator	Logout ?
Ready to Scan	
In Menu (Admin Mode	•) 🔂
Maintenance	Box
Maintanance related cettings	Licer Boy creation and operation
Confirm ROM version, Import and Export data.	Document can be printed and routed from the User Box.
Mater Count	Onen Licer Box
Mater Count	Open oser box
System Settings	Print Setting
Initial settings.	Print Settings
User Box and Stamp settings.	Fonts and XPS Settings.
Machine Setting 🗸 Display	Basic Setting V Display
2	1 (<mark>5</mark>
Security	Store Address
Security	JUNE AUGIESS
Security related settings. Administrator Password and Address Permission	Destination (addresses) registration. E-mail, Subject and Prefix/Suffix Settings
Settings.	E mai, easjer and Preixee and easy earlies.
TCP/IP Setting	Address Back
E-mail Setting	Address Book
IPP Setting	
FTP Setting	Fax Settings
SNMP Setting	Fax Settings
Web Service Settinge ttings.	Fax Functions and Fax Report Settings.
Boniour Setting	
Doniour Douring	Header/Footer Position
NetWare Setting Display	
NetWare Setting AppleTalk Setting	
AppleTalk Setting Display WebDAV Setting OnenAPI Setting	Wizard
AppleTalk Setting AppleTalk Setting OpenAPI Setting TCP Socket Setting	Wizard
AppleTalk Setting Display AppleTalk Setting VebDAV Setting OpenAPI Setting TCP Socket Setting IEEEB02.1X Authentication Setting	Wizard Wizard Setup is performed The setting can be assist performed by following the
AppleTalk Setting AppleTalk Setting WebDAV Settings OpenAPI Setting TCP Socket Setting IEEEB02.1X Authentication Setting LITD Setting	Wizard Wizard Setup is performed. The setting can be easily performed by following the outlined procedures.
Apple Talk Setting Apple Talk Setting WebDAY Setting OpenAPI Setting TCP Socket Setting IEEE002.1X Authentication Setting LILTD Setting SSDP Settings	Wizard Wizard Setup is performed The setting can be easily performed by following the outlined procedures.

- 3 Click [WebDAV Server Settings] from the [WebDAV Settings] menu.
- 4 Click the pull-down menu of WebDAV Settings and select [ON].
- 5 Click the [Password is changed] check box and enter the WebDAV Server Password.

Ø		
<u>Eile Edit View Favorites Iools E</u>	elp	
	Administrator	Logout ?
	Ready to Scan	
	n Menu (Admin Mode)	2
Network 🔽 Dis	lay	💷 To Main Menu
▶ TCP/IP Setting	WebDAV Server Settings	
▶ E-mail Setting	WebDAV Settings ON 💌	
▶ LDAP Setting	SSL Setting SSL Only 👻	
▶ IPP Setting	Access Rights Settings	
▶ FTP Setting	New Password	-
▶ SNMP Setting	Retype New Password	-
⊫ SMB Setting		
⊫ Web Service Settings		OK Cancel
▶ Bonjour Setting		
⊫ NetWare Setting		
► AppleTalk Setting		
▶ Network Fax Setting		
▼ WebDAV Settings		
▶ WebDAV Client Settings		
WebDAV Server Settings		
▶ OpenAPI Setting		
► TCP Socket Setting		~

- 6 Click [OK].
 - → If the WebDAV Server Password entered does not meet the requirements of the Password Rules, a message appears that tells that the WebDAV Server Password entered cannot be used. Enter the correct WebDAV Server Password. For details of the Password Rules, see page 1-8.
 - → If there is a mismatch in the WebDAV Server Passwords, a message appears that tells that there is a mismatch in the WebDAV Server Passwords. Enter the correct WebDAV Server Password
- 7 Check the message that tells that the setting has been completed. Then, click [OK].



2.18 PC-Fax RX Setting Function

When access to the machine by the Administrator of the machine through the Administrator Settings is authenticated, the machine enables setting of the operation of the PC-Fax RX Setting Function. This function enables received fax documents to be saved in user boxes on the hard disk installed in the machine. Memory RX User Boxes or any other user boxes specified are used as saving destination user boxes.

NOTICE

If the PC-Fax RX Setting is made, the TSI User Box Setting function cannot be used.

PC-Fax RX Setting

<From the Control Panel>

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

	Use the menu buttons or keypad to make a	selection.
Bookmark	Administrator Settings	
		1/2 * ←Back 🔓 🖓 🕂
Utility	1 System Settings	6 Copier Settings
↓ Administrator	2 Administrator/ Machine Settings	7 Printer Settings
Settings	3 One-Touch/User Box Registration	8 Fax Settings
	4 User Authentication/ Account Track	9 System Connection
	5 Network Settings	0 Security Settings
	25 (02 (2008 15 / 0	Close
	Memory 100%	Close

3 Touch [Function Settings].



4 Touch [PC-Fax RX Setting].



5 Make the necessary settings.

	Specify the conditions for	PC-Fax RX Function.	
Bookmark	Administrator Settings >	Function Settings > PC-F	ax RX Settings
	Allow	Dial-In only	Restrict
Utility	Receiving User Box Destination	Print	Password Check
↓ Administrator			Connunication Password
Settings	Memory BX User Box	ON	0 - 9, *, #
Fax Settings	Specified User Box	OFF	ON
Function Settings			OFF
Fax RX Settings	12/26/2008 09:12 Memory 100%		ОК

- → When [Specified User Box] is selected, the data is stored at the box whose number is assigned with F code Sub address.
- → When Dial-in is set ON, [Dial-In only] appears after [Allow]. PC-FAX receiving setting can be made only when the data is received with dial-in number.
- → FAX input data is saved to the box as TIFF.
- → When a user deleted [Specified User Box] specified at Receiving User Box Destination, the received data will be saved at print or forced memory inbox according to the conditions set for FAX receiving. Also when a new box is assigned with the same box number after [Specified User Box] specified at Receiving User Box Destination is deleted, the data will be saved at the newly assigned inbox, therefore you should be careful with the number assigned.
- 6 Touch [OK].

<From PageScope 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 PageScope Web Connection and access the Admin Mode.
- 2 Select [Function Setting] from the pull-down menu of Fax Settings and click [Display].

Edit View Favorites Tools Help	
Administrator	Logout
Ready to Scan	
In Menu (Admin Mode	
v	
Maintenance	Box
Maintenance related settings.	User Box creation and operation.
Confirm ROM version, Import and Export data.	Document can be printed and routed from the User Box.
Meter Count 🔽 Display	Open User Box 🔽 Display
System Settings	Print Setting
Initial settings. User Box and Stamp settings.	Print Settings Fonts and XPS Settings.
Machine Setting	Regio Sotting
Machine Gennig	Dasic Setting
Security	Store Address
Security related settings.	Destination (addresses) registration.
Administrator Password and Address Permission	E-mail, Subject and Prefix/Suffix Settings.
Dianlay Dianlay	Display
PKI Settings Display	Address Book
User Auth/Account Track	Fax Settings
User Authentication and Account Track Settings	Fax Settings
External Server and Group User Box Settings.	Fax Functions and Fax Report Settings.
Authentication Method 🛛 🔽 Display	Header/Footer Position 🛛 🔽 Display
	Header/Footer Position
Network	TX/RX Settings
	Function Setting
Network-related Settings.	LEBY L'oppoction Softing
Network-related Settings. E-mail and Open API Settings.	Report Setting following the
Network-related Settings. E-mail and Open API Settings.	PBX Connection Setting Report Settings Header Information

- 3 Click [PC-Fax RX Setting] from the [Function Setting] menu.
- 4 Click the pull-down menu of PC-Fax RX Setting and select [Allow].

<u>a</u>		
<u>Elle E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools	Help	
	凝 Administrator	Logout ?
	Ready to Scan	
	In Menu (Admin Mode)	8
Fax Settings 🔽 Di	splay	E To Main Menu
Header/Footer Position	PC-Fax RX Setting	
▶ Line Parameter Setting	PC-Fax RX Setting	Allow 👻
► TX/RX Settings	Receiving User Box Destination	Memory RX User Box 💌
▼ Function Setting	Print	ON Y
Function ON/OFF Setting	Password Check	
▶ Dial-In Settings	Communication Password	
Memory RX Setting		(one-byte numeric, '#', '")
Closed Network RX		
▶ Forward TX Setting		OK Cancel
▶ Remote RX		
Incomplete TX Hold		
PC-Fax RX Setting		
▶ TSI User Box Settings		
TSI User Box Registration		
▶ PBX Connection Setting		
▶ Report Settings		
▶ Multi Line Settings		
Header Information		

bizhub C360/C280/C220

- 5 Make the necessary settings.
- 6 Click [OK].
- 7 Check the message that tells that the setting has been completed. Then, click [OK].

2.19 TSI User Box Setting Function

When access to the machine by the Administrator of the machine through the Administrator Settings is authenticated, the machine enables setting of the operation of the TSI User Box Setting Function. This function automatically sorts documents received with fax IDs (TSIs) of the transmitters into other devices or boxes of the machine set up for each transmitter.

TSI User Box Setting

<From the Control Panel>

- ✓ For the procedure to call the Function Setting screen on the display, see page 2-82.
- ✓ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.
- ✔ When saving high confidential document, do not make box save via FAX.
- 1 Call the Function Setting screen on the display from the control panel.
- 2 Touch [TSI User Box Setting].

Paolectel	Use the men	u buttons or keypad to make a	a sele	ection.
	Administra	tor Settings > Fax Settings :	> Fund	tion Settings
Utility	1	Function ON/OFF Setting	6	Remote RX
Administrator Settings	2	Dial-In Settings	7	Tx Hold
	3	Memory RX Setting	8	PC-Fax RX Setting
Fax Settings	4	Closed Network RX	9	TSI User Box Setting
Function Settings	5	Forward TX Setting		
	12/26/2008 Memory	09:11		Close

3 Select [Yes] and touch [TSI User Box Registration].



4 Select the number to be set and touch [Edit].

Bookmark	Create, edit or delete TSI User I Administrator Settings > Function	Box settings. on Settings > TSI User Box Sett	ings
Utility Administrator Settings Fax Settings	No. Sender (TS1) 001 002 003 004 005 006 007 008	For Wordang	1 /16
Settings		Edit <u>Pête</u>	
Settings	12/26/2008 09:33 Memory 100%		ОК

- \rightarrow You can register up to 128 where the received data is distributed.
- → To delete the registered one, select the number and press [Delete].
- 5 Make the necessary settings.

	Select item and enter using keypad.
Bookmark	Administrator Settings > Function Settings > TSI User Box Settings
Utility	Sender (TSI)
Administrator Settings	+ SPACE <u>Tëre</u>
Fax Settings	
Function Settings	Sector by User Box
TSI User Box Settings	12/26/2008 09:33 Henory 1003

- \rightarrow Confidential inbox or terminal box cannot be set as the distribution target.
- → When [Box] specified to save TSI is not available, the data will be saved at print or forced memory inbox according to the condition set for [Action when TSI User Box is not set]. Also when a new box is assigned with the same box number after [Box] set for the TSI is deleted, the data will be stored at the newly assigned inbox, therefore you should be careful with the number assigned.
- 6 Touch [OK].

<From PageScope Web Connection>

- ✓ For the procedure to access the Function Setting screen on the display, see steps 1 and 2 of page 2-82.
- ✓ 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 PageScope Web Connection and call the Function Setting screen on the display.
- 2 Click [TSI User Box Setting] from the [Function Setting] menu.
- 3 Click the [TSI User Box Setting] check box.

2		
<u>File Edit View Favorites Tools</u>	: <u>H</u> elp	
	Administrator	Logout ?
	Ready to Scan	
	In Menu (Admin Mode)	Ø
Fax Settings	Display	E To Main Menu
Header Footer Position	TSI User Box Settings	
Line Parameter Setting	IV TSI User Box Setting	
TX/RX Settings	Action when TSI User Box is not set.	Automatically Print
▼ Function Setting	Print	OFF Y
▶ Function ON/OFF Setting		
▶ Dial-In Settings		OK Cancel
Memory RX Setting		
Closed Network RX		
▶ Forward TX Setting		
▶ Remote RX		
Incomplete TX Hold		
▶ PC-Fax RX Setting		
TSI User Box Settings		
TSI User Box Registration		
PBX Connection Setting		
Report Settings		
Multi Line Settings		
Header Information		

- 4 Make the necessary settings.
- 5 Click [OK].
- 6 Check the message that tells that the setting has been completed. Then, click [OK].
- 7 Click [TSI User Box Registration] from the [Function Setting] menu.
- 8 Click [Create].

9 Make the necessary settings.



- 10 Click [OK].
- 11 Check the message that tells that the setting has been completed. Then, click [OK].

2.20 TCP/IP Setting Function

When access to the machine by the Administrator of the machine through the Administrator Settings is authenticated, 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 Network Settings screen on the display, see steps 1 and 2 of page 2-69.
- ✓ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.
- 1 Call the Network Settings screen on the display from the control panel.
- 2 Touch [TCP/IP Settings].
- 3 Touch [IPv4 Settings].
- 4 Touch [Manual Input].
- 5 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.
- 6 Touch [OK].

<From PageScope 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 PageScope Web Connection and access the Admin Mode.
- 2 Select [TCP/IP Setting] from the pull-down menu of Network and click [Display].
- 3 Select [Manual Setting] from the IP Address Setting Method pull-down menu.
- 4 Enter the IP Address in the "IP Address" box.
 - → If [Auto Setting] is selected from the IP Address Setting Method pull-down menu in step 3, select the means with which to acquire the IP Address automatically, including DHCP, BOOTP, ARP/PING, and AUTO IP setting, and click the check box.
- 5 Click [OK].

<From the Control Panel>

- ✓ For the procedure to call the TCP/IP settings screen on the display, see steps 1 through 3 of page 2-90.
- ✓ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.
- 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 Auto Obtain, the DNS Server Address and DNS Domain Name are automatically acquired.
- 3 Touch [OK].

<From PageScope Web Connection>

- ✓ For the procedure to access the TCP/IP Setting screen on the display, see steps 1 and 2 of page 2-90.
- ✓ 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 PageScope 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 NetWare Setting Function

When access to the machine by the Administrator of the machine through the Administrator Settings is authenticated, the machine enables registration as the Print Server.

Making the NetWare Setting

<From the Control Panel>

- ✓ For the procedure to call the Network Settings screen on the display, see steps 1 and 2 of page 2-69.
- ✓ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.
- 1 Call the Network Settings screen on the display from the control panel.
- 2 Touch [NetWare Settings].
- 3 Make the necessary settings.
- 4 Touch [OK].

<From PageScope 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 PageScope Web Connection and access the Admin Mode.
- 2 Select [NetWare Setting] from the pull-down menu of Network and click [Display].
- 3 Make the necessary settings.
- 4 Click [OK].

bizhub C360/C280/C220

2.22 SMB Setting Function

When access to the machine by the Administrator of the machine through the Administrator Settings is authenticated, the machine enables setting of the NetBIOS Name.

Setting the NetBIOS Name

<From the Control Panel>

- ✓ For the procedure to call the Network Settings screen on the display, see steps 1 and 2 of page 2-69.
- ✓ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.
- 1 Call the Network Settings screen on the display from the control panel.
- 2 Touch [SMB Settings].
- 3 Touch [Print Settings].
- 4 Touch [NetBIOS Name].
- 5 Enter the NetBIOS Name.
- 6 Touch [OK].
- 7 Touch [OK].

<From PageScope 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 PageScope Web Connection and access the Admin Mode.
- 2 Select [SMB Setting] from the pull-down menu of Network and click [Display].
- 3 Click [Print Setting] from the [SMB Setting] menu.
- 4 Enter the NetBIOS Name in the "NetBIOS Name" box.
- 5 Click [OK].

bizhub C360/C280/C220

2.23 AppleTalk Setting Function

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

Making the AppleTalk Setting

<From the Control Panel>

- ✓ For the procedure to call the Network Settings screen on the display, see steps 1 and 2 of page 2-69.
- ✓ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.
- 1 Call the Network Settings screen on the display from the control panel.
- 2 Touch [AppleTalk Settings].
- 3 Make the necessary settings.
- 4 Touch [OK].

<From PageScope 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 PageScope Web Connection and access the Admin Mode.
- 2 Select [AppleTalk Setting] from the pull-down menu of Network and click [Display].
- 3 Make the necessary settings.
- 4 Click [OK].
2.24 E-Mail Setting Function

When access to the machine by the Administrator of the machine through the Administrator Settings is authenticated, 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 2-69.
- ✓ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.
- 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].

<From PageScope 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 PageScope Web Connection and access the Admin Mode.
- 2 Select [E-mail Setting] from the pull-down menu of Network and click [Display].
- 3 Click [E-mail TX (SMTP)] from the [E-mail Setting] menu.
- 4 Make the necessary settings.
- **5** Click [OK].



3 User Operations

3.1 User Authentication Function

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

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.

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

3.1.1 Performing user authentication

<From the Control Panel>

- Register 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 registered. Entry of a wrong User Password is counted as unauthorized access. If a wrong User Password is entered a predetermined number of times (once to three times) or more set by the Administrator of the machine, 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 PageScope Web Connection. To cancel the access lock state, the Administrator of the machine must perform the Release Setting. Contact the Administrator of the machine.
- Before operating the machine, the user him/herself should change the User Password from that registered by the Administrator of the machine. For details of changing the User Password, see page 3-11.
 For more details of User Name and User Password, ask the Administrator of the machine.
- ✓ If the User Password is changed by the Administrator of the machine during operation of this machine, the user him/herself should immediately change the User Password.
- ✓ 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 [ON (External Server)] (Active Directory) is set for Authentication Method, the User Name is automatically registered with this machine.

Job List	Enter User Name and password, and then touch ILogin] or press the IAccess] key.	
Nant Status	User Name	_
	Password	
t t		
Job Details	04/03/2007 14:42 Menory 1007	Login

1 Touch [User Name].

→ The following screen appears if any document is stored in the ID & Print User Box.



- → The following screen appears if [ID & Print] is selected on the printer driver side and documents are stored in the ID & Print User Box even with the ID & Print Setting function not set in the machine.
- → The following screen appears if the ID & Print Setting function is set in the machine, because documents are stored in the ID & Print User Box even if [Print] is selected on the printer driver side.
- 2 Enter the User Name from the keyboard and keypad.



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

Job List	Enter User Name and password, and then touch (Login) or press the increasily key.
Veer Status	User Name Juser 1
	Password
Delete Job Details Y M C K	Login Login Menory 08:10

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



- → Press the [C] key to clear all characters.
- → Touch [Delete] to delete the last character entered.
- → Touch [Shift] to show the upper case/symbol screen.
- → Touch [Cancel] to go back to the screen shown in step 4.
- 6 Touch [OK].
- 7 Press [Access] or touch [Login]. If a document is stored in the ID & Print User Box, select the desired login method.

Login Method	Description
[Begin Printing]	Prints only the ID & Print Document of the corresponding user. The user operation mode screen is not called to the screen.
[Print & Login]	The user operation mode screen is called to the screen after the ID & Print Document of the corresponding user is printed.
[Access] or [Login]	If [Access] or [Login] is selected, only the ordinary login procedure is applicable and no ID & Print Documents are printed.

- → If a wrong User Name is entered, a message appears that tells that authentication has not been successful. The machine then prohibits entry for User Authentication for 5 sec. and then causes the screen of step 1 to reappear. Perform User Authentication once again.
- → If there is a mismatch of User Password relative to the registered User Name, a message appears that tells that authentication has not been successful. The machine then prohibits entry of User Name and User Password for 5 sec. and then causes the screen of step 4 to reappear. Enter the correct User Password.
- → If the Enhanced Security Mode is set to [ON], the entry of a wrong User Password is counted as unauthorized access. If a wrong User Password for the corresponding User Name entered is entered a predetermined number of times (once to three times) or more set by the Administrator of the machine, a message appears that tells that authentication has not been successful for any subsequent operation for authentication. The machine is then set into an access lock state, rejecting any more logon attempts. To cancel the access lock state, the Administrator of the machine must perform the Release Setting. Contact the Administrator of the machine.
- → If there are two ore more ID & Print Documents are involved, all of them will be printed. To select and print only a desired document, select [Access] 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 3-10.
- → Go to step 15 if User Authentication only has been set, or "Synchronize" has been set for Synchronize User Authentication & Account Track.

8 Touch [Account Name].



9 Enter the Account Name from the keyboard and keypad.

◆Type in the login account name using the keyboard or keybad. Press IC1 to delete the entered account Name.
Account Track > Enter Account Name
1
10/09/2009 14:33 Monory 1002

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

Job List	Tenter Account Name and Password, and then touch [Login] or press the [Access] key.
Name Status	Account Name 1
	Password
↑ ↓ Delete	
	Login

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



- → Press the [C] key to clear all characters.
- → Touch [Delete] to delete the last character entered.
- → Touch [Shift] to show the upper case/symbol screen.
- → Touch [Cancel] to go back to the screen shown in step 11.
- 13 Touch [OK].
- 14 Press [Access] or touch [Login]. If documents are stored in the ID & Print User Box, the login method selected in step 7 will appear. Select the login method displayed on the screen.
 - → If a wrong Account Name is entered, a message appears that tells that authentication has not been successful. The machine then prohibits entry for Account authentication for 5 sec. and then causes the screen of step 1 to reappear. Perform Account authentication once again.
 - → If there is a mismatch of Account Password relative to the registered Account Name, a message appears that tells that authentication has not been successful. The machine then prohibits entry of Account Name and Account Password for 5 sec. and then causes the screen of step 11 to reappear. Enter the correct Account Password.
 - → If the Enhanced Security Mode is set to [ON], the entry of a wrong Account Password is counted as unauthorized access. If a wrong Account Password for the corresponding Account Name entered is entered a predetermined number of times (once to three times) or more set by the Administrator of the machine, a message appears that tells that authentication has not been successful for any subsequent operation for authentication. The machine is then set into an access lock state, rejecting any more logon attempts. To cancel the access lock state, the Administrator of the machine must perform the Release Setting. Contact the Administrator of the machine.
- **15** Pressing the [Access] key will show the following screen. To log off, select [Log off].

Job List	Are you sure y	you want to log-out?	٦
Neer Status	User Nane	user1	
1			
Delete Job Details	ĺ.	Log off Do not log off	
Y M C K	09/09/10 14:37 mory 100%		

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

Job List	Are you sure yo	ou want to log-out?
User ctatue	User Name	user1
Name Status	Account Name	1
Delete		Log off Do not log off
Job Details	2000/00/10 1/ 22	
Y M C K	Memory 100%	

<From PageScope 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 [ON (External Server)] (Active Directory) is set for Authentication Method, the User Name is automatically registered with this machine.
- 1 Start the Web browser.
- 2 Enter the IP address of the machine in the address bar.
- 3 Press the [Enter] key to start PageScope Web Connection.
- 4 Click the Registered User radio button and enter the User Name and User Password.

<u>E</u> dit <u>V</u> iew	F <u>a</u> vorites <u>T</u> ools <u>H</u> elp			
	Language	English (English)	V	
	Login	Registered User		
		User Name	user1	
		Password	•••••	
		C Administrator		
	View Mode	C Flash	• HTML	
		Flash Player is necessar	y to see in Flash form. FLASH PLAYER	
	User Assist	🗆 Display dialog box in d	ase of warning.	
				Login
	Starting-u	p Data Management Utility		
	Flash Play	er is required to use the Data M	anagement Utility.	
	S Manag	e Copy Protect Data		
	🔧 Manag	e Stamp Data		
	Se Manag	e Font/Macro (*1)		
	(*1) Can or environmer	ly run on Windows Internet Exp ts.	orer and Flash Player Version 9 and above	

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

Edit View	u Esuaritas Taals Hala			
Ear Dev	A LEADURES TOOR Tech			
	Language	English (English)	Y	
	Login	 Registered User 		
		User Name	user1	
		Password	•••••	
		Account Name	1	
		Account Password	•••••	
		C Administrator		
	View Mode	C Flash		
		Flash Player is necessary to	o see in Flash form. Get ADOBE FLASH PLAYER	
	User Assist	🗆 Display dialog box in cas	e of warning.	
			Login	_
	Starting-u	o Data Management Utility		
	Flash Playe	er is required to use the Data Mana	igement Utility.	
	Manag	e Copy Protect Data		
	Kanage Manage	e Stamp Data		
	Manag	e Font/Macro (*1)		
	(*1) Can on environmen	ly run on Windows Internet Explore ts.	er and Flash Player Version 9 and above	

- → If "Synchronize" has been set for "Synchronize User Authentication & Account Track," successful authentication results from simply entering the User Name and User Password.
- 5 Click [Login].
 - → If there is a mismatch of User/Account Password relative to the registered User/Account Name, a message appears that tells that authentication has not been successful. Click [OK] to go back to the screen of step 4. Enter the correct User/Account Name and User/Account Password.
 - → If the Enhanced Security Mode is set to [ON], the entry of a wrong User/Account Password is counted as unauthorized access. If a wrong User/Account Password for the corresponding User/Account Name entered is entered a predetermined number of times (once to three times) or more set by the Administrator of the machine, a message appears that tells that authentication has not been successful for any subsequent operation for authentication. The machine is then set into an access lock state, rejecting any more logon attempts. To cancel the access lock state, the Administrator of the machine must perform the Release Setting. Contact the Administrator of the machine.
- 6 Clicking [Logout] will show the following screen. Click [OK] to log off from the user operation mode.

	A user1		Logout	Change Password	?
	Ready to S	Scan			
	Ready to P	Print			C
_ogout					
Logout User Name	user1				
Logout User Hame Are you sure you want to	user1 log-out?				

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] 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.
- 1 Perform the user authentication procedure from the control panel and login procedure through [Access] or [Login].
- 2 Press the [Box] key.
- 3 Touch the [System User Box] tab.

Job List	Select the desired User Box to use or file document. Use the keypad to input and specify the box number to use	
Check Job	Public Personal System Group	Save Document
Kang Status	C 900000001 Public Use P Box	1/ 1
		Search User Box
Delete Job Details	Enter User Box No.	Use/File
Y м с к	12/26/2008 10:41 Memory 100%	

4 Select [ID & Print User Box] and touch [Use/File].

Job List	Select the desired User Box to use or file document. Use the keypad to input and specify the box number to use.
Check Job	Public Personal Barrenox Group Save Document
Veer Box Information	Bulletin Board Polling TX Secure Document Secure Docu User Box User Box User Box User Box
	Annotation User Box User Box User Box User Box User Box
	External Henory
	Enter User Box No.
Y м с к	2009/09/10 14:40 Language Selection

5 Select the desired ID & Print Document and touch [Print].

Job List	Select document(s) and then choose the desired function.
Check Job	Print Sidding
Selected Documents	Ver Boxnt
test	1/ 1 Print
	e 'e test
	Select
	Reset
T 17 1 ¥	Detail View Details
Y M C K	2/26/2008 10:43 Kenory 992

→ To delete ID & Print Document, select the specific document from the [Filing Settings] tab and press [Delete].

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 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 Press the [Utility/Counter] key.
- **3** Touch [User Settings].

Job List	Use the menu buttons or keypad to make a	a selection.
neter count	Utility	
Name Status	1 One-Touch/User Box Registration	6 Banner Printing
	2 User Settings	
	3 Administrator Settings	8 Device Information
	4 Check Consumable Life	
Delete		
Y M C K	2009/09/10 14:41 Memory 100%	Close

4 Touch [Change Password].



bizhub C360/C280/C220

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



- → Press the [C] key to clear all characters.
- → Touch [Delete] to delete the last character entered.
- → Touch [Shift] to show the upper case/symbol screen.
- → Touch [Cancel] to go back to the previous screen.
- 6 Touch [OK].
 - → If there is a mismatch in the User Passwords, a message appears that tells that there is a mismatch in the User Passwords. Enter the correct User Password.
 - → If the Enhanced Security Mode is set to [ON], the entry of a wrong User Password is counted as unauthorized access. If the current password is mistakenly entered a predetermined number of times (once to three times) or more set by the Administrator of the machine, the user authentication screen will reappear. A message then appears that tells that authentication has not been successful for any subsequent operation for authentication. The machine is now set into an access lock state, rejecting any more logon attempts. To cancel the access lock state, the Administrator of the machine.
- 7 From the keyboard or keypad, enter the new User Password that can consist of 8 to 64 digits. To prevent entry of a wrong password, enter the password again in [Password Confirmation].



- → Press the [C] key to clear all characters.
- → Touch [Delete] to delete the last character entered.
- → Touch [Shift] to show the upper case/symbol screen.
- → Touch [Cancel] to go back to the screen shown in step 4.
- 8 Touch [OK].
 - → If the User Password entered does not meet the requirements of the Password Rules, a message appears that tells that the User Password entered cannot be used. Enter the correct User Password. For details of the Password Rules, see page 1-8.
 - → If there is a mismatch in the User Passwords, a message appears that tells that there is a mismatch in the User Passwords. Enter the correct User Password.

<From PageScope 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 PageScope Web Connection.
- 2 Click [Change User Password] of the Information menu or [Change Password].

	2		
Edit View Favorites Tools Help	0		
	A user1	Logout Change Password	?
e	Ready to Scan		
	Ready to Print		3
i htormation			
Check device information and c	onsumables information such as Toner.		
Device Information	Online Assistance	Change User Password	
Function Permission Information	Network Setting Information	Print Setting Information	
Print Information			
Job			
Job Check the status of your job and	job history.		
Job Check the status of your job and Current Jobs	job history. Job History	Communication List	
Job Check the status of your job and Current Jobs	job history. Job History	Communication List	
Job Check the status of your job and Current Jobs	job history. Job History	Communication List	
Job Check the status of your job and Current Jobs Box Store data in the HDD, print zhon Crate User Boxes according to	job history Job History ed date from the HDD, purpose, and save documents.	Communication List	
Job Check the status of your job and Current Jobs Box Store data in the HDD, print stor Create User Boxes according to Open User Box	Job history. Job History ed date from the HDD purpose, and save documents. Create User Box	Communication List	

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.

8				
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools <u>H</u>	<u>t</u> elp			
	A user1	Logout	nange Password 🛛 🥐	
	Ready to Scan		3	
			E To Main Menu	
Device Information	Change User Password			
Online Assistance	User Name	user1		
Change User Password	Current Password	******		
Function Permission Information	New Password	•••••		
Network Setting Information	Retype New Password	•••••		
Print Setting Information				
Print Information			OK Cancel	

- 4 Click [OK].
 - → If there is a mismatch in the password between the currently registered User Password and the User Password typed in the "Current Password" box, a message appears that tells there is a mismatch in the User Password. Click [OK] to go back to the screen of step 3. Then, perform steps 3 and 4 once again.
 - → If the User Password entered in the "New Password" box fails to meet the requirements of the Password Rules, a message appears that tells that the User Password entered cannot be used, as it fails to meet the requirements of the Password Rules. Click [OK] to go back to the screen of step 3. Perform steps 3 and 4 once again. For details of the Password Rules, see page 1-8.
 - → If there is a mismatch in the password between that entered in the "New Password" box and that entered in the "Retype New Password" box, a message appears that tells that there is a mismatch in the User Password. Enter the correct User Password.
- 5 Click [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 registered in the machine.

To access a Secure Print Document, authentication is performed through an 8-digit password that verifies an authenticated user of the Secure Print Document. 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 registered. Entry of a wrong User Password is counted as unauthorized access. If a wrong User Password is entered a predetermined number of times (once to three times) or more set by the Administrator of the machine, 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 PageScope Web Connection. To cancel the access lock state, the Administrator of the machine must perform the Release Setting. Contact the Administrator of the machine.
- ✓ Enter the Secure Print ID and password through the printer driver on the PC side. The password entered is displayed as "*."
- ✓ The Secure Print password must consist of 8 digits and meet the requirements of the Password Rules. Any Secure Print Document, the password for which does not meet the requirements of Password Rules, will not be registered in the machine. For details of the Password Rules, see page 1-8.
- 1 Log on to the user operation mode through User Authentication from the control panel.
- 2 Press the [Box] key.
- 3 Touch the [System User Box] tab.



4 Select [Secure Document User Box] and touch [Use/File].



bizhub C360/C280/C220

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



- \rightarrow For the Secure Print ID, enter the one that has been set on the printer driver side.
- → Press the [C] key to clear all characters.
- → Touch [Delete] to delete the last character entered.
- → Touch [Shift] to show the upper case/symbol screen.
- → Touch [Cancel] to go back to the screen shown in step 4.
- 6 Touch [OK].
 - → If a wrong Secure Print ID is entered, the desired Secure Print Document will not be displayed. Enter the correct Secure Print ID.
- 7 Select the desired Secure Print Document and touch [Enter Password].

Job List	Select docum choose the d	ent(s) and t esired funct	hen ion.		
Check Job	Print		Filing Settings		
Salacted Documents	Secure Pri	nt User Box			
Jereven Douments	Stored 10:42	User Name	Document Name test	1/ 1	Print Settings Enter Password
				Select	
↑ 1/ 1 ↓				Reset	
Y м с к	12/26/2008 Memory	10:56 99%		Cance	

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

Tyre in the password for the Secure Print document. Press ICI to erase the entered password.
Secure Print Document Password

1 2 3 4 5 6 7 8 9 0
a s d f g h j k l : •
Z X C V b n n , . / Shift
Space
2009/09/10 14:46 Henory 100%

- → The machine rejects any Secure Print Password that consists of less than 8 digits.
- → For the Secure Print Password, enter the 8-digit one set on the printer driver side.

bizhub C360/C280/C220

- → Press the [C] key to clear all characters.
- → Touch [Delete] to delete the last character entered.
- → Touch [Shift] to show the upper case/symbol screen.
- → Touch [Cancel] to go back to the screen shown in step 7.
- 9 Touch [OK].
 - → If there is a mismatch of the Secure Print Password relative to the Secure Print ID, a message appears that tells that authentication has not been successful. The machine then prohibits entry of the Secure Print Password for 5 sec. Enter the correct Secure Print Password.
 - → If two or more Secure Print Documents have been selected in step 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 of the machine, a message appears that tells that authentication has not been successful for any subsequent operation for authentication. The machine is then set into an access lock state, disabling access to the Secure Print Document. To cancel the access lock state, the Administrator of the machine must perform the Release Setting. Contact the Administrator of the machine.
- **10** Select the desired Secure Print Document and touch [Print].



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



- ➔ If two or more Secure Print Documents, each having an identical Secure Print ID and Secure Print Password, have been registered, multiple Secure Print Documents can be printed at once.
- → Touch [Cancel] to go back to the screen shown in step 10.

3.4 User Box Function

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

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

A user who accesses the Personal User Box or Public User Box or Group User Box is authenticated through an 8-digit User Box Password. The password entered for the authentication purpose appears as "*" or "•" on the display.

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

Reference

- If a document is saved in the copy, fax, or scan mode or from an external memory by specifying a User Box number that has not been registered, the Personal User Box owned by the user who logged on through User Authentication is automatically registered.
- If Account Track has not been enabled, Group User Box cannot be created.

3.4.1 Setting the User Box

<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 3-23.
- 1 Log on to the user operation mode through User Authentication from the control panel.
- 2 Press the [Utility/Counter] key.
- 3 Touch [One-Touch/User Box Registration].



4 Touch [Create User Box].



5 Touch [Public/Personal User Box].

Job List	Use the menu buttons or keypad to make a selection.
Bookmark Utility One-Touch/ User Box Reg. Create User Box	Utility > One-Touch Destination/User Box Registration > Create User Box 1 Public/Personal User Box 2 Bulletin Board User Box 3 Relay User Box
	04/13/2007 15:57

6 Touch [New].

Job List	To register a new User Box, touch [New]. To edit an existing User Box, select desired User Box and touch [Edit].
Bookmark	
	Utility > Create User Box > Public/Personal User Box
	ABC DEF GHI JKL MNO PORS TUV WXYZ etc
Iltility	
000000	Were Box Nane Type Create Date/Tine
+	
Ope-Touch/	
User Box Reg.	
· · · · · · · · · · · · · · · · · · ·	
Croato licor Poy	
create user box	
+	
Dublic (Dorconal)	
Public/Personal	
	New
	04/03/2007 16:12 Close
	Menory UZ

7 Select the User Box type.

Job List	Enter the User Box password.
Bookmark	Utility > Public/Personal User Box > New 1/2 + Back 557 +
	User Box No. 4 1 - 999999999
Utility	User Box Nane
One-Touch/	Password
User Box Reg.	Index etc
	Type Public Personal Group
Lreate User Box	Time Stored 12/26/2008 11:19
♥ Public/Personal User Box	
New	12/26/2008 11:19 Cancel OK

bizhub C360/C280/C220

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



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

8 Touch [Password].

Job List	Specify the settings. Enter User Box number us	ing the keypad.	
Bookmark	Utility > Public/Person	al User Box > New	1/2 ←Back For-
	User Box No.	4	1 - 999999999
Utility	User Box Name		
↓ One-Touch/	Password		
User Box Reg.	Index	etc	
	Туре	Public Perso	onal Group
	Time Stored	12/26/2008 11:20	
Public/Personal			
User Box	Owner Name	user1	Change Owner
New			Comert
	12/26/2008 11:20 Memory 100%		

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

P16 Pac The	ase input a new password with the keyboard or ten-key . It is necessary to input it twice to confirm password. password input with a clear key can be deleted.
Utility > New Public/F	ersonal User Box > User Box Password
Password	****
Password Confirmation	хохожжи
	Pere
1 2 3	4 5 6 7 8 9 0
q w e	r t y u i o p s t
a s d	f g h i k l : : l
Z X C	V b n n , . / 🔪 Shift
200 Mer	9/09/10 14:50 ory 100%

- → Press the [C] key to clear all characters.
- → Touch [Delete] to delete the last character entered.
- → Touch [Shift] to show the upper case/symbol screen.
- → Touch [Cancel] to go back to the screen shown in step 8.
- 10 Touch [OK].
 - → If the User Box Type is set to [Public], set a User Box Password that meets the requirements of the Password Rules. For details of the Password Rules, see page 1-8.
 - → If there is a mismatch in the User Box Passwords, a message appears that tells that there is a mismatch in the User Box Passwords. Enter the correct User Box Passwords.
- **11** Make the necessary settings.

Job List	Specify the settings. Enter User Box number us	ing the keypad.	
Bookmark	Utility > Public/Person	al User Box > New	1/2 ←Back For- →
1	User Box No.	4	1 - 999999999
Utility	User Box Name		
One-Touch/	Password	*>>>>>	
User Box Reg.	Index	etc	
Croato Ucor Roy	Туре	Public Pers	onal Group
	Time	12/26/2008 11:21	
Public/Personal			
User Box	Owner Name	user1	Change Owner
New	12/26/2008 11:21		Cancel OK

- → 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.
- **12** Touch [OK].

<From PageScope 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.
- ✓ For the procedure to change the User Box setting, see page 3-23.
- 1 Log on to the user operation mode through User Authentication from the PageScope Web Connection.
- 2 Click [Create User Box] of the Box menu.

Edit View Favorites Tools Help			
ć	S user1	Logout Change Password	?
e	Ready to Scan		
	Ready to Print		0
i D Information			
Check device information and co	insumables information such as Toner.		
Device Information	Online Assistance	Change User Password	
Function Permission Information	Network Setting Information	Print Setting Information	
Print Information			
lab			
Check the status of your job and	job history.		
Current Jobs	Job History	Communication List	
Pay			
Box			
Box Store data in the HDD, print stor Create User Boxes according to ;	ed date from the HDD. surpose, and save documents.		
Box Store data in the HDD, print store Create User Boxes according to p Open User Box	ed date from the HDD. surpose, and save documents. Create User Box	Open System User Box	

3 Make the necessary settings.

ile <u>E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ool	s <u>H</u> elp	
	A user1	Logout Change Password ?
	Ready to Scan	
	Ready to Print	8
		E To Main Menu
Open User Box	Create User Box(Public/Group/Person	al)
Create User Box	Box is the function to save documents in the Documents in the Box can be used for printin	machine. 1g. sending etc.
Open System User Box	User Box Number	- Chronome Secul
Create System User Box	 Use opening number 	
	C Input directly	(1-999999999)
	User Box Name	
	Use Box Password.	
	User Box Password	
	Retype User Box Password	
	Index	
	Specify a keyword for Box search and d	isplay by Name.
		etc 💌
	Туре	Public 💌
	Auto Delete Document	
	O Not Delete	
	C Specify days	1 day
	C 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 enter the User Name of the owner of the User Box in the "Owner Name" box.

bizhub C360/C280/C220

- → 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 enter the Account Name of the owner of the User Box in the "Account Name" box.
- 4 Click [OK].
 - → If the User Box Type is set to [Public], set a User Box Password that meets the requirements of the Password Rules. For details of the Password Rules, see page 1-8.
 - → If there is a mismatch in the User Box Passwords, a message appears that tells that there is a mismatch in the User Box Passwords. Enter the correct User Box Password.
 - → If no Owner Name is entered, a message appears that tells that no Owner Names have been entered. Enter the correct Owner Name.
 - → If a user name not registered with the machine is entered in the "Owner Name" box, a message appears that tells that the Owner Name entered in the box is illegal. Click [OK] to go back to the screen of step 3. Perform steps 3 and 4 once again.
 - → 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. Click [OK] to go back to the screen of step 3. Perform steps 3 and 4 once again.
- 5 Check the message that tells that the setting has been completed. Then, click [OK].

3.4.2 Changing the User Box Password and user attributes and account attributes

<From the Control Panel>

- ✓ For the procedure to call the User Box screen to the display, see steps 1 through 5 of page 3-17.
- ✓ 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].

Job List	To register To edit an e	a new User Box, touch H Kisting User Box, selec	New]. t desired	User Box and touc	h [Edit].
	Utility > C	reate User Box > Public	:/Personal	User Box	
	ABC DEF	GHI JKL MNO	PQRS	TUV WXYZ etc	
Utility	User Box	Nane	Туре	Create Date/Time	
+	1	Public User Box	Public	12/17/2008 13:58	1/ 1
One-Touch/	2	Personal User Box	Per- sonal	12/17/2008 13:59	
USET DON Reg.	3	Group User Box	Group	12/17/2008 13:59	·
Create User Box					
Public/Personal User Box					
	New	Edit	Delete		_
	12/26/2008 Memory	11:25 100%			Close

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

Use the keyboard or keybad to enter the password of the selected User Box. To clear your entry computely, press the CCI key. Reflection : 2
Utility > Edit Public/Personal User Box > User Box Password Authentication
xxxxxxxxx
2009/09/10 14:51

- → Press the [C] key to clear all characters.
- → Touch [Delete] to delete the last character entered.
- → Touch [Shift] to show the upper case/symbol screen.
- → Touch [Cancel] to go back to the screen shown in step 2.
- 4 Touch [OK].
 - → If there is a mismatch between the currently registered User Box Password and the User Box Password entered, a message appears that tells that there is a mismatch in the User Box Password and the screen of step 2 reappears. Perform steps 2 through 4 once again.
 - → If the Enhanced Security Mode is set to [ON], entry of a wrong User Box Password is counted as unauthorized access. If a wrong User Box Password is entered a predetermined number of times (once to three times) or more set by the Administrator of the machine, the screen of step 2 reappears and the machine is set into an access lock state. To cancel the access lock state, the Administrator of the machine must perform the Release Setting. Contact the Administrator of the machine.
 - → To change the User Box Type, go to step 5. To change the User Box Password, go to step 9.
 - → To change the owner user or owner account, perform steps 6 through 8.

5 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.
- → If the User Box Type is changed to [Public], set a User Box Password that meets the requirements of the Password Rules. For details of the Password Rules, see page 1-8.
- **6** Touch [Change Owner] if the box type is [Personal] and touch [Change Account Name] if the box type is [Group].

Job List	Select item and enter setting.
Boolmark	Select index in the Address Book.
DOONIIUTK	Utility > Public/Personal User Box > Edit 1/2 ←Back 🖉ara →
	User Box No. 2 1 - 999999999
Utility	User Box Name Personal User Box
One-Touch/	Password *****
User Box Reg.	Index etc
	Type Public Personal Group
Create User Box	Stored 12/17/2008 13:59
Public/Porconal	
User Box	Owner Name user1 Change Owner
Edit	12/26/2008 11:26

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

Job List	Select the owner of the User Box.	
BOOKMARK	Utility > Edit Public/Personal User Box > Change Owner	
	Owner Name	
Create User Box	user1 user2 1/ 1	
Dublic/Dorconal	user3	
User Box		l
Edit		l
Change Owner	06/14/2007 13:39 Henory 1007	

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

Job List	Select the account that owns the User Box.
Bookmark	Utility > Edit Public/Personal User Box > Change Owner
()	Account Name
Utility	
Create User Box	2 1/ 1
Public/Porsonal	3
User Box	
Edit	
+	
Chenge Owner	12/26/2008 11:27

- 8 Touch [OK].
- 9 Touch [Password].

Job List	Select item and enter se	atting.
Bookmark	Select index in the Addr	ress Book.
DOONIIUT	Utility > Public/Person	nal User Box > Edit 1/2 ←Back 🛛 🚰 →
	User Box No.	2 1 - 999999999
Utility	User Box Name	Personal User Box
One-Touch/	Password	*00000****
User Box Reg.	Index	etc
	Туре	Public Personal Group
Create User Box	Time	12/17/2008 13:59
Public/Personal		
User Box	Owner Name	user1 Change Owner
Edit	12/26/2008 11:26 Memory 100%	Cance1 OK

10 Enter the currently set 8-digit User Box Password from the keyboard or keypad.

Enter the current password using the keyboard or keyhod. Press ICI to clear the password.
Utility > Edit Public/Personal User Box > User Box Password

a s d f g h i k l ; ;]
z x c v b n n , . / x Shift
Space
2009/09/10 14:52

- → Press the [C] key to clear all characters.
- → Touch [Delete] to delete the last character entered.
- → Touch [Shift] to show the upper case/symbol screen.
- → Touch [Cancel] to go back to the screen shown in step 9.
- 11 Touch [OK].
 - → If the User Box Password entered does not match the current password, a message appears that tells that the User Box Password entered is wrong. Enter the correct User Box Password.
 - → If the Enhanced Security Mode is set to [ON], entry of a wrong User Box Password is counted as unauthorized access. If a wrong User Box Password is entered a predetermined number of times (once to three times) or more set by the Administrator of the machine, the screen of step 2 reappears and the machine is set into an access lock state. To cancel the access lock state, the Administrator of the machine must perform the Release Setting. Contact the Administrator of the machine.

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



- → Press the [C] key to clear all characters.
- → Touch [Delete] to delete the last character entered.
- → Touch [Shift] to show the upper case/symbol screen.
- → Touch [Cancel] to go back to the screen shown in step 9.
- 13 Touch [OK].
 - → If the User Box Type is changed to [Public], set a User Box Password that meets the requirements of the Password Rules. For details of the Password Rules, see page 1-8.
 - → If there is a mismatch in the User Box Passwords, a message appears that tells that there is a mismatch in the User Box Passwords. Enter the correct User Box Password.
- 14 Touch [OK].

<From PageScope 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 PageScope Web Connection.
- 2 Click [Open User Box] of the Box menu.

<u>E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools <u>H</u>	elp		
	A user1	Logout Change Password	?
	Ready to Scan		
	Ready to Print		2
Linformation	and a star when the star to the star		
	consumables information such as 1 oner.		
Device Information	Online Assistance	Change User Password	
Function Permission Information	Network Setting Information	Print Setting Information	
Print Information			
Job			
Check the status of your job a	nd job history.		
Current Jobs	Job History	Communication List	
Box			
Store data in the HDD, prints Create User Boxes according	tored date from the HDD. to purpose, and save documents.		
Open User Box	Create User Box	Open System User Box	
Create System User Box			

3 Enter the User Box Number and User Box Password of the desired User Box and click [OK].

ile <u>E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools	Help			
	S user1		Logout	Change Password 🛛 🏆
Open User Box Create User Box Open System User Box Create System User Box	Ready to Scan Ready to Print Open User Box(P Box is the function in the B User Box Number	ublic/Group/Personal) o save documents in the machin xx can be used for printing, senc	e. ing etc	E To Main Menu
				OK
	User Box List	Search from In	dex	
		Page (Display I	vy 50 cases)	1 V G0
	User Box Number	User Box Name	Туре	Time Stored
	1	Public User Box	Public	2008/12/17 13:58
	2	Personal User Box	Personal	2008/12/17 13:59
	3	Group User Box	Group	2008/12/17 13:59

- → If there is a mismatch between the User Box Number and User Box Password, a message appears that tells that authentication has not been successful. Click [OK] and perform step 3 once again.
- → If the Enhanced Security Mode is set to [ON], entry of a wrong User Box Password is counted as unauthorized access. If a wrong User Box Password is entered a predetermined number of times (once to three times) or more set by the Administrator of the machine, a message appears that tells that authentication has not been successful for any subsequent operation for authentication. The machine is then set into an access lock state. To cancel the access lock state, the Administrator of the machine must perform the Release Setting. Contact the Administrator of the machine.

4 Click [User Box Setting].

Ready to Scan Ready to Print Ready to Print Inter Box InterBox Inter Box InterBox InterBox	X n Menu
Ready to Print Ready to Print Ready to Print Den User Box User Box Number User Box Number User Box Number Create User Box Type Personal Owner Name User Box Ready to Print Lear Box Lear Box	n Menu
Den User Rex User Box Number 2 User Box Name Personal User Box Orner Name User Box Number 2 User Box Name User Box Type Personal Owner Name user	n Menu
Create User Box User Box Number 2 User Box Name Personal User Box Type Personal Owner Name user	
Create User Box Type Personal Owner Name user1	
Bay Oversties User Ray Catting Dalate User Ray	
Open System User Box Operation Over BOX Setting Delete Over BOX	
Create System User Box	
File List Thumbnail View OFF	
First, select an operation. The selectable documents are displayed.	
Specify operation Display All Changes the display	
Select Thumbnail Document Name Number of Originals Edit Name	
Conso	

- → Go to step 6 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.
- 5 Click the "User Box Owner is changed." check box and change the user attributes of the box.

8							
Eile	Edit	View	F <u>a</u> vorites	Tools	Help		<i>R</i> r
						User Box Expansion Function is changed. Confidential RX New Communication Password Retype New Communication Password User Box Password is changed. Current Password New Password Retype New Password	
						User Box Owner is changed. Type Owner Name	Personal V User List

→ The following screen appears if the account attributes are to be changed.

3								
Elle	Edit	⊻iew	F <u>a</u> vorites	Tools	Help			
						User Box Expansion Function is changed. Confidential RX New Communication Password Retype New Communication Password	OFF V	
					-	User Box Password is changed. Current Password New Password Retype New Password		
						User Box Owner is changed. Type Account Name	Group Account List	-
							OK Cancel	1

- → Click [User List] to select a specific user from the registered User List.
- → A user name may be directly entered in the Owner Name box.
- → Click [Account List] to select a specific account from the registered Account List.
- → An account name may be directly entered in the Account Name box.
- → 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.
- → Enter the User Name that has been registered through User Registration for the Owner Name.
- → Enter the Account Name that has been registered through Account Track Registration for the Account Name.
- 6 Click the "User Box Password is changed." check box and enter the User Box Password.

<u>Elle E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools	Help			
	A user1	Logout Ch	ange Password	?
	Ready to Scan			
	Ready to Print		2	3
			-	
			E To Main Mer	ıu
Open User Box	User Box Attribute Change			
Create User Box	User Box Number	2		
Open System User Box	User Box Name	Personal User Box		
Create System User Box	Index	etc 💌		
	Auto Delete Document			
	Do Not Delete			
	C Specify days	1 day 📉		
	C Specify Time	min.(5-720)		
	 Oser Bux Expansion Functions changed. 	OFF IN		
	Confidential KX	UFF M		
	New Communication Password			
	Retype New Communication Password			
	User Box Password is changed.			
	Current Password	•••••		
	New Password	•••••		
	Retype New Password	•••••		
				2

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

- 7 Click [OK].
 - → If there is a mismatch in the Current User Box Passwords, a message appears that tells that there is a mismatch in the Current User Box Passwords. Click [OK] to go back to the screen of step 3. Perform steps 3 through 7 once again.
 - → If the User Box Type is changed to [Public], set a User Box Password that meets the requirements of the Password Rules. For details of the Password Rules, see page 1-8.
 - → If there is a mismatch in the User Box Passwords, a message appears that tells that there is a mismatch in the User Box Passwords. Enter the correct User Box Password.
 - → If no Owner Name is entered, a message appears that tells that no Owner Names have been entered. Enter the correct Owner Name.
 - → If a user name not registered with the machine is entered in the "Owner Name" box, a message appears that tells that the Owner Name entered in the box is illegal. Click [OK] to go back to the screen of step 4. Perform steps 4 through 7 once again.
 - → 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. Click [OK] to go back to the screen of step 4. Perform steps 4 through 7 once again.
- 8 Click [OK].



<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 Press the [BOX] key.
- 3 Select the desired User Box and touch [Use/File].



- → [Use/File] allows you to print or send the saved document. It also allows you to copy, delete, or file the document.
- → To save a new document, select [Save Document].
- 4 Enter the 8-digit User Box Password from the keyboard and keypad.

Enter the password of the selected User Box. To clear your entry, press the ICI key. 2 Personal User Box								
User Box Passuord								
xxxxxxxxx								
1 2 3 4 5 6 7 8 9 0								
as df ghikl;								
ZXCVDNN, / Shift								
Space								
2009/09/10 14:55 Henory 1002								

- → Press the [C] key to clear all characters.
- → Touch [Delete] to delete the last character entered.
- → Touch [Shift] to show the upper case/symbol screen.
- → Touch [Cancel] to go back to the screen shown in step 3.
- **5** Touch [OK].
 - → If there is a mismatch in the User Box Passwords, a message appears that tells that authentication has not been successful. The machine then prohibits entry of the User Box Password for 5 sec. Enter the correct User Box Password.
 - → If the Enhanced Security Mode is set to [ON], entry of a wrong User Box Password is counted as unauthorized access. If a wrong User Box Password is entered a predetermined number of times (once to three times) or more set by the Administrator of the machine, a message appears that tells that authentication has not been successful for any subsequent operation for authentication. The machine is then set into an access lock state, rejecting any more logon attempts. To cancel the access lock state, the Administrator of the machine must perform the Release Setting. Contact the Administrator of the machine.

6 Select the desired file from each tab.



7 Select the desired function.

Different functions can be performed on different types of files stored in the User Boxes. See the table given below for the relation between the file type and functions that can be performed.

File Type	Functions that can be Performed
Copy job files	Print, Combine, Send, Bind TX, Save to External Memory
Print job files	Print, Combine, Send, Bind TX, Save to External Memory
Scan job files	Print, Combine, Send, Bind TX, Save to External Memory
Fax job files	Print, Save to External Memory

→ 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 from the [Filing Settings] tab and press [Delete].
- → To save a file in External Memory, select the specific document from the [Filing Settings] tab and press [Save to External Memory].
- 8 Press the [Start] key or touch [Start].

bizhub C360/C280/C220

<From PageScope 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 PageScope Web Connection.
- 2 Click [Open User Box] of the Box menu.

<u>E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools <u>H</u> e	qle		
	요 user1	Logout Change Password	?
	Ready to Scan		
	Ready to Print		Q
			_
Information			
Check device information and	consumables information such as Toner.		
Device Information	Online Assistance	Change User Password	
Function Permission Information	Network Setting Information	Print Setting Information	
Print Information			
Job	41.6 614		
Job Check the status of your job an	d job history.		
Job Check the status of your job an Current Jobs	d job history. Job History	Communication List	
Job Check the status of your job an Current Jobs	d job history. Job History	Communication List	
Job Check the status of your job an Current Jobs	d job history Job History	Communication List	
Job Check the status of your job an Current Jobs Box Store data in the HDD, print sto Create User Boxes according to	d job history. Job History yed date from the HDD. y purpose, and save documents.	Communication List	
Job Chack the status of your job an Current Jobs Box Drast Box according to Create Vare Boxes according to Open User Box	d job history. Job History yeld date from the HDD. y puppose, and save documents. Create User Box	Communication List	

3 Enter the User Box Number and User Box Password of the desired User Box and click [OK].

le <u>E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools	Help			
	A user1		Logout	Change Password 🛛 ?
	Ready to Scar	1		
	Ready to Print			8
				E To Main Menu
Open User Box	Open User Box(Public/Group/Personal)		
Create User Box	Box is the function	to save documents in the machin	e. Ing etc	
Open System User Box	Licer Box Number	w	D	
Create System User Box	User Dox Nambe		[2](1-9	aaaaaaa)
	User Box Passw	vora		
				OK
	User Box List	Search from In	dex	ALL Go
		Page (Display t	oy 50 cases)	1 💌 Go
	User Box Number	User Box Name	Туре	Time Stored
	1	Public User Box	Public	2008/12/17 13:58
	2	Personal User Box	Personal	2008/12/17 13:59
	3	Group User Box	Group	2008/12/17 13:59

- → If there is a mismatch between the User Box Number and the User Box Password, a message appears that tells that authentication has not been successful. Click [OK] and perform step 3 once again.
- → If the Enhanced Security Mode is set to [ON], entry of a wrong User Box Password is counted as unauthorized access. If a wrong User Box Password is entered a predetermined number of times (once to three times) or more set by the Administrator of the machine, a message appears that tells that authentication has not been successful for any subsequent operation for authentication. The machine is then set into an access lock state, rejecting any more logon attempts. To cancel the access lock state, the Administrator of the machine must perform the Release Setting. Contact the Administrator of the machine.

4 Select the desired operation from the pull-down menu and click [Changes the display].

E To Main Mer nal User Box User Box
E To Main Mer
User Box
umbnail View ON
the display
ored Edit Name
21 11:19 Edit Name
21 11:22 Edit Name

→ 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, Move/Copy, Delete, Send to other device, Download to PC
Print job files	Print, Move/Copy, Delete, Send to other device, Download to PC
Scan job files	Print, Move/Copy, Delete, Send to other device, Download to PC
Fax job files	Print, Delete, Download to PC

- → If [Delete] is selected in step 4, a confirmation message appears. Click [OK] to delete the specified file.
- 5 Select the document and perform the desired function.

<u>ile E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools	Help				
	A user1		Logo	out Change	e Password 🤶 🥐
	Read	ly to Scan			
	Read	ly to Print			8
					E To Main Menu
► Open User Box	User Bo	× Number 2	User Box Na	me Personal User Box	
 Create User Box 	Туре	Personal	Owner Name	e user1	
Open System User Box	B	x Operation Use	r Box Setting	Delete User Box	
Create System User Box					
	- Filo Lie			Thumbooil View	ON
	THE LIS			annonion an vicv	
	ALC: 1	1 1 11 11 11 1	· · · · · · · · · · · · · · · · · · ·	and the second se	
	First, s	elect an operation. The selec	table documents are	displayed.	
	First, s Specify	elect an operation. The select operation Print	table documents are	displayed. Changes the display	t l
	First, s Specify Select	elect an operation. The select operation Print Document Name	table documents are Number of Originals	displayed. Changes the display Time Stored	Edit Name
	First, s Specify Select	operation Print Document Name S_test print	table documents are Number of Originals 1	Changes the display Changes the display Time Stored 2008/03/21 11:19	Edit Name
	First, s Specify Select	Print Print Document Name S_test print C_test print	Number of Originals	Changes the displayed. Changes the display Time Stored 2008/03/21 11:19 2008/03/21 11:22	Edit Name Edit Name
	First, s Specify Select I See Se	v operation Print Document Name S_test print C_test print lect document and exect	Number of Originals 1 1 :ute.	Description Description Time Stored 2008/03/21 11:19 2008/03/21 11:22 2008/03/21 11:22	Edit Name Edit Name Edit Name
	First, s Specify Select	elect on operation. The select operation Print Document Name S_test print C_test print lect document and exect	table documents are Number of Originals 1 1 .ute.	displayed. Changes the display Time Stored 2008/03/21 11:19 2008/03/21 11:22	Edit Name Edit Name Edit Name
	First, s Specify Select	elect an operation. The select roperation Print Document Name S_test print C_test print lect document and exect	Number of Originals 1 1	o displayed. Changes the display Time Stored 2008/03/21 11:19 2008/03/21 11:22 Print Setting	Edit Name Edit Name Edit Name

3.4.4 Sending S/MIME box files

- ✓ For the procedure to call the Use Document screen to the display, see steps 1 through 5 of page 3-31.
- ✓ 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 Use Document screen to the display from the control panel.
- 2 Touch the [Send] tab.
- 3 Select the file to be sent and click [Send].



4 Select [Communication Settings].

Job List	Select desired destination(s).	No. of Dest.	000
	Fax can be sent at any time using keypad.		
Check Job	Address Book Direct Input Job History		
Preview		_	
Broadcast		_	
Destinations	FEEST ABC DEF GHI JKL MNO PORS TUV WXYZ (etc	
		1/	1
	No registered one-touch		
	destination available.		
1/ 1		Grou	
		Searc	h
Delete			~
Check Job	Settings Settings Applicat	ion	
	12/26/2008 13:11 Cancel	Star	
Y M C K	Memory 99%		

5 Select [E-Mail Encryption] and touch [Close].

Job List	Specify the settings.		No. of 000
Check Job Send > Transmission Details > Communication Settings			5
Broadcast Destinations	Line Settings		Unit Notification Setting
	Communication Method	E-Mail Encryption	Digital Signature
1/ 1 Delete	Fax Header		
Y M C K	12/26/2008 13:13 Memory 997		Close

- → To select [E-Mail Encryption], the Administrator of the machine must make the S/MIME settings in advance.
- → If [E-Mail Encryption] is selected after the destination has been set, the set destination is canceled, making it necessary to set the destination once again.
6 Select the destination and touch [Start] or press the [Start] key.



→ To select the destination, the Administrator of the machine must register the certificate with the destination in advance.



4 Application Software

4.1 PageScope Data Administrator

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

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

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

4.1.1 Accessing from PageScope Data Administrator

- ✓ Do not leave the site while you are gaining access to the machine through PageScope Data Administrator. If it is absolutely necessary to leave the site, be sure first to log off from the PageScope Data Administrator.
- 1 Start the PageScope Data Administrator.
- 2 Select this machine from Device List and click [Authentication Settings/Address Settings] or [Administrator settings].

<u>Eile</u>	Function <u>I</u> o	ool <u>W</u> indow fDevice <u>∳</u> Ne	Help twork Initial Setting			_ 8 _ 8
asic Se	ttings Settings fo	r multiple device	Application initial setting			
evice li	st			Number o	f Displayed Devices:1	Home
Status	Status Display	Registered name	Group name	Model name	Device address	Authentication Settings/ A
٢	Online	MEP	Default Group			Administrator settings
						Function Selection
						Prestore
						🔏 Administrator settings
					>	Device Selection Filter

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

Import the device informat	ion.		
Import the device information.			
Registered group:	Default Group		
Registered name MFP		ĺ	
Device address:			5
⊂ Scan settings			
Import functions		Target of importing	
🛔 🗌 Administrator set	tings	Obtain from the device	
		Previous data(2008/03/19)	
😼 🗹 Authentication S	ettings	 Obtain from the device 	
		O Previous data(2008/03/19)	
🍕 🗹 Address setting:	;	Obtain from the device	
		O Previous data(2008/03/19)	
,			
Help(F1)		Import Can	icel

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

nport the device information.			1
Registered group:	Default Grou	(P	
Registered name	MFP		
Device address:			
Import functions		Target of importing	
🚊 🔽 Administrator	settings	 Obtain from the device 	
		Previous data(2008/03/19)	
Authenticatio	on Settings	Obtain from the device	
		Previous data(2008/03/19)	
Address set	ings	Dtain from the device	
		<u>Previous data(2008/03/19)</u>	
)			

4 Type the 8-digit Administrator Password registered in the machine and click [OK].

Administrator password	×
Registering name:	MFP
Registered group name:	MFP
Model name:	
Device address:	
Device name:	
	□ <u>S</u> ave
Administrator gassword:	XXXXXXXXX
Administrator password (Confirmation):	
Help(F1)	0K Cancel

- → 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 8-digit 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 of the machine, 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.

Here is the sequence, through which the main power switch and sub power switch are turned on and off:

Turn off the sub power switch \rightarrow Turn off the main power switch \rightarrow Turn on the main power switch \rightarrow Turn on the sub power switch

- → 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.
- → 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.
- 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 PageScope Data Administrator. If it is absolutely necessary to leave the site, be sure first to log off from the PageScope Data Administrator.
- 1 Access the machine through [Authentication Settings/Address Settings] mode of PageScope Data Administrator.
- 2 Click [Authentication settings].

unction selection:	Device information:	
E Uevice information[MFP] Authentication settings	Item Value	
Address settings User box	Registering name MFP Group name Default Group Model name Device address	
	< I m	
	The latest access date and time	
	Function The latest access date and time	
	Authentication se 2008/03/19 15:50:10 Address settings 2008/03/19 15:50:10	
	C	>

3 Click [User authentication].

<u> </u>	elp		- 8 ×	
🛃 TOP 🛛 📢 Registration of Device 💆	letwork Initial Setting			
Function selection:	Authentication mode:			
Device information(MEP)	User Authentication and Account	Track		
 Authentication settings Address settings 	Setting list:			
User box	Status Item	Value	^	
	When number o	fjob Job skip		
	Number of coun	ters 500 / 500		
	Print without aut	erau Synchronize hent Bestrict		
	User list display	setti Restrict		
	Public user setti	ngs Restrict		
	Maximum numbe	For Device authentication		
	Ticket Hold Tim	e Se	~	
	<		>	
	Settings:			
	User authentication			
	Device authentication			
	Select user authentication	n method.	-	
			M	
Help(F1)	Befresh from th	e device 🙀 Export to the devic	:e	

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

(j) <u>File</u> Edit <u>I</u> ool <u>W</u> indow He	∮p			_ @ ×	
😂 TOP 🛶 Registration of Device 💆 N	etwork Initial Setti	ng			
Function selection:	Authenticatio	n mode:			
Device information(MFP)	User Authent	ication and Account Track			
 Authentication settings Address settings 	Setting list:				
User box	Status	Item	Value	^	
		When number of job Number of counters	Job skip 500 / 500		
		Print without authent	Bestrict		
		User list display setti	Restrict		
		Public user settings	Restrict		
		Maximum number of	2		
		User authentication	Device authentication		
		TICKETHOID TIME SE			
	Settings:				
	User aut	nentication			
	Device authentication				
	Device authentication				
	Network	server authentication			
	C SEIE	or user aumentication metric	iu.		
				<u> </u>	
	_				
Help(F1)	8	Refresh from the devic	e Export to the	device	

- → 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 Settings via the control panel or using PageScope 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 PageScope Data Administrator. If it is absolutely necessary to leave the site, be sure first to log off from the PageScope Data Administrator.
- Changing the Account Track setting erases all user and account information data that has previously been registered. This changes all Personal User Boxes owned by the users who are deleted and all Group User Boxes owned by the accounts that are deleted to Public User Boxes. If the password set for a particular box before this change does not meet the requirements of the Password Rules, however, no access can be made to the Public User Box, to which that specific box was changed. In this case, the Administrator must first newly set a password that meets the requirements of the Password Rules. For details of the Password Rules, see page 1-8.
- 1 Access the machine through [Authentication Settings/Address Settings] mode of PageScope Data Administrator.
- 2 Click [Authentication settings].

3 File Edit Tool Window H	elp _ ć	3 ×
😥 TOP 🛶 Registration of Device 👱 N	letwork Initial Setting	
Function selection:	Device information: Device information Rem Value Registering name MFP Group name Defice address Device information The latest access date and time Function The latest access date and time Address settings 2008/03/19 15:50:10 Address settings 2008/03/19 15:50:10	
Help(F1)	Befresh from the device	

- 3 From [Edit] on the tool bar, select [Authentication] and click [Change authentication mode].
- 4 Click [Next].

Authentication mode change wizard			
Start authentication mode change wiz	ard.		1/6
Start authentication mode change wizard.			
Help(F1)	<b<u>ack</b<u>	Next>	Cancel

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

lease select a new authentication mode from the following template.		
Current authentication mode	User Authentication (Device local authentication)	
Select authentication mode:		
Authentication mode		
User Authentication (Device loca	al authentication)	
User Authentication (device) and	Account Tracking	
Account Track Account Track (The input metho	d is only password)	
None	d is only password)	

→ If [User Authentication and Account Track] is selected, set [The ratio of the number of Users] and [The ratio of the number of Accounts].

uthentication mode c	hange wizard		
Set the number of user	s and accounts to be reg	istered in device	3/6
Please set the allocation of	the number of Users /Accour	its.	
Sum total:	1000		
The allocation of the number	er of users	The allocation of the num	ber of Accounts
Before change:	1000	Before change:	0
After changed:	700 (1-999)	After changed:	300 (1-999)
The number of Users:			
1			999
Help(E1)			

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

Authentication mode change	wizard
Ready to write	4/6
Write a new authentication mode to	the device.
Current authentication mode	User Authentication (Device local authentication)
New authentication mode	User Authentication (device) and Account Tracking
Help(F1)	KBack Write Cancel

- → If you have already logged on to the Administrator Settings via the control panel or using PageScope 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.

bizhub C360/C280/C220

7 Click [Finished].

Complete the change authen	lication mode wizard.	6/6
Complete to write a new authentica	tion mode in the device.	
	Display	a log
Current authentication mode	User Authentication (Device local authentication)	
New authentication mode	User Authentication (device) and Account Tracking	

→ If [User Authentication and Account Track] is selected in step 5, [Synchronize] is set for "Synchronize user authentication and account track." If you want user authentication not synchronized with account track, click to deselect [Synchronize user authentication and account track] and execute [Export to the device] once again.

				. 🗆 🛛				
😟 <u>F</u> ile <u>E</u> dit <u>T</u> ool <u>W</u> indow Help	5			- 8 ×				
🕍 TOP 🛶 Registration of Device 👱 Net	work Initial Settin	g						
Function selection:	Authentication	mode:						
Gevice information(MFP)	User Authentic	cation and Account Track						
 Authentication settings Address settings 	Setti <u>ng</u> list:							
🖵 🍅 User box	Status	Item	Value	^				
2002.		When number of job Number of counters	Job skip 500 / 500					
		Synchronize user au	Synchronize					
	-	Print without authent	Restrict					
		Public user settings	Restrict					
	-	Maximum number of						
		User authentication	Device authentication					
	1	TICKETHOID TIME SE		3				
	Settings:							
	Synchi Wher accou	onize user authentication a nit is set to "synchronize", i nt linked automatically.	and account track. the user is logged in and it is also logged in to th	e 🔺				
Help(F1)	8	<u>R</u> efresh from the devic	e Export to the device					

- ✓ 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 PageScope Data Administrator. If it is absolutely necessary to leave the site, be sure first to log off from the PageScope Data Administrator.
- Access the machine through [Authentication Settings/Address Settings] mode of PageScope Data Administrator.
- 2 Click the Authentication settings expand button.
- 3 Click [User authentication settings].

Function selection:	User list: 3 / 500 item(s)					
🕞 Device information(MFP)	Status	User name	E-Mail address	Permi	+ Add	
Authentication settings Account track settings User authentication settings Buser of peration Prohibition Settings Suser Operation Prohibition Settings Address settings User box	Registered Registered Registered	user1 user2 user3		Outpu Outpu Outpu	Edit Edit Dejete	
	<			>		

- 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] and a screen appears that prompts you to confirm the execution of deletion. Click [Yes] to delete the user.
 - → If the User Password does not meet the requirements of the Password Rules, a message appears that tells that this particular User Password cannot be used. Click [OK] and enter the correct User Password. For details of the Password Rules, see page 1-8.
 - → 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 Settings via the control panel or using PageScope 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.
 - → If [Delete] is selected in step 4, the Personal User Box owned by that specific user is changed to Public User Box. If the password set for a particular box before this change does not meet the requirements of the Password Rules, however, no access can be made to the Public User Box, to which that specific box was changed. In this case, the Administrator must first newly set a password that meets the requirements of the Password Rules. For details of the Password Rules, see page 1-8.

- 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 PageScope Data Administrator. If it is absolutely necessary to leave the site, be sure first to log off from the PageScope Data Administrator.
- Access the machine through [Authentication Settings/Address Settings] mode of PageScope Data Administrator.
- 2 Click the Authentication settings expand button.
- 3 Click [Account track settings].

ction selection:	Account list:		3	/ 500 item(s)	
Device information(MFP)	Status	Account name	Permit function	Total (Cour	+ Add
Authentication settings	Registered	1	Permit all		
Account track settings Account track settings Comparison of the settings Comparison of the settings Address settings User box	Registered	2	Permit all		📝 Edit
	Registered	3	Permit all		M Dejete
					Column option
	-				

- 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] and a screen appears that prompts you to confirm the execution of deletion. Click [Yes] to delete the account.
 - → If the Account Password does not meet the requirements of the Password Rules, a message appears that tells that this particular Account Password cannot be used. Click [OK] and enter the correct Account Password. For details of the Password Rules, see page 1-8.
 - → 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 Settings via the control panel or using PageScope 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.
 - → If [Delete] is selected in step 4, the Group User Box owned by that specific account is changed to Public User Box. If the password set for a particular box before this change does not meet the requirements of the Password Rules, however, no access can be made to the Public User Box, to which that specific box was changed. In this case, the Administrator must first newly set a password that meets the requirements of the Password Rules. For details of the Password Rules, see page 1-8.

- ✓ 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 PageScope Data Administrator. If it is absolutely necessary to leave the site, be sure first to log off from the PageScope Data Administrator.
- 1 Access the machine through [Authentication Settings/Address Settings] mode of PageScope Data Administrator.
- 2 Click the Address settings expand button.
- 3 Click [Address book].

ction selection:	Address bo	ok list:		0 / 2000 iter	n(s)		
Device information(MFP)	Status	No.	Abbreviated name	Desti	^	3	Edjt
Authentication settings		0001				Xa	Distance
Address book	- Internet	0002				18	Delete
Group address	1	0003				E	Сору
Program address Page Name of Program		0005					
		0006					Paste
E-Mail text		0007				00	Eind
Prefix/Suffix		0008				90	
🏐 User box		0009				Cha	nge Registered No
	- prop	0010				D: 1 01	10.1
	- Link Pres	0012			_	Displayin	or Display.
	hough prove	0012			~	E-Mail	

4 Select the number to be registered and click [Edit].

ction selection:	Address bo	ook liist:		0 / 2000	item(s)		
Device information(MFP)	Status	No.	Abbreviated name	Desti	^	3	Edįt
Authentication settings	- proof	0001				Xa	Dialata
Address book	- Internet	0002					Dielere
📑 💼 Group address		0003			-	E.E	Copy
Program address Page Name of Program E-Mail title E-Mail text		0005					
		0006					<u>P</u> aste
		0007				80	Eind
Prefix/Suffix		0008				90	
🏐 Userbox		0009				Ch.	ange Registered No
		0010			-		
		0011			-	Display/N	lot Display:
	- long	0012			~	E-Ma	i

5 Select [E-Mail] and Click [OK].

Selection of destination type		
Destination Type		
⊖ Fax	⊙ <u>E</u> -Mail	
⊖ SJP Fax	O <u>U</u> ser box	
O I <u>P</u> Address Fax	<u>О s</u> мв	
Internet Fax	O F <u>I</u> P	
	○ WebDAV	
Machine Type of Destination		
Monochrome		
O <u>C</u> olor		
Help(F1)	OK Canc	əl

6 Click [Register] of S/MIME Certification file and select the certificate to be registered.

Add and edit of addres	s book(E-Mail)		X
Abbreviated No.: Abbreviated name [®] : Search character [®] : <u>R</u> eference Allowed Icon	etc Level[0] Setting	Main Sgtting	": Required field
 E-Mail configuration E-Mail address*: S/MIME Certification file Register 	Unregistered	Register Dejete	
Help(F1)		ОК	Cancel

- → Set 1024 bits or more for the key length of the RSA public key for the certificate of each destination.
- 7 Make the necessary settings.

Add and edit of addres	s book(E-Mail)		
Abbreviated No.:	0001		*: Required field
Abbreviated name*:	test		
Search character*:	etc	🔽 🗌 Majn	
Beference Allowed	Level[0]	S <u>e</u> tting	
lcon	Setting		
E-Mail configuration			
E- <u>M</u> ail address*:	test@co.jp		
S/MIME Certification file			
Register	Unregistered	Register	
		Dejete	
Help(F1)		ОК	Cancel

- → If the abbreviated name and E-mail address have not been entered, an input error message appears. Then, click [OK] and enter the abbreviated name and E-mail address.
- 8 Click [OK].
- 9 Click [Export to the device].
 - → If you have already logged on to the Administrator Settings via the control panel or using PageScope 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.

bizhub C360/C280/C220

4.1.7 SNMP Setting Function

<Changing the auth-password and priv-password>

- ✓ 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 PageScope Data Administrator. If it is absolutely necessary to leave the site, be sure first to log off from the PageScope Data Administrator.
- 1 Access the machine through [Administrator settings] mode of PageScope Data Administrator.
- 2 Click the Administrator settings expand button.
- 3 Click the Network expand button.
- 4 Click [SNMP].

	SIMMP setting	s:		
Scanner Fax Network Fax Security O' Power supply management O' Network	Status	Item SNMP Settings SNMP V1/V2c (IP) SNMP V3 (IP) SNMP V3 (IP) UDP Port Number V1/V2 Write Permission	Value Enable Enable Enable Enable 161 Enable	
- 17, IPv6 Address Informatic - 17, IPsec Information - 17, Raw Pot B ■ 11 Filtering - 2 NetWare	Setting:	V1/V2 Read Community Name V1/V2 Write Community Name V3 Context Name	public private	>
SINP SINP	♥ Enat	le the SNMP.		×

5 Click [V3 Write User] of Setting list.

		к.		
Device information	Setting list:			
🕂 👗 Administrator settings	Status	Item	Value	Result
- 🕂 Online Support	-	V1/V2 Write Permiss	Disable	
- 👌 Scanner	-	V1/V2 Read Commu	public	
- 🗳 Fax		V1/V2 Write Commu	private	
- 👰 Network Fax		V3 Context Name	Enable V2 Discovery Llog N	000-01
Security		V3 Bead User	Security Level=auth-password	Vniv-na
Power supply management		V3 Write User	Security Level=auth-password	/priv-pa
E YY Network		V3 Authentication Al	MD5	
DNS		V3 Encryption Algorit	DES	
-4% IPv6 Address Informatic	<			>
	User Name*:		restrict	
SNMP	<u>U</u> ser Na	ne:	restrict	
- 😝 SMB	<u> </u>	password.		
- 👰 AppleTalk	Curre	nt Password(auth)*:	(8-32 chars)	
Bonjour	Pass	word (auth)*:	(8-32 chars)	
	Pass	vord(auth)(Retype)*.	(8-32 chars)	
E-Mail RX (POP)	Set a	password.	· · · · ·	
TCP Socket	Curre	nt Password(priv)*:	(8-32 chars)	
Time adjustment	Press	word (priv)*:	(8-32 chars)	
Time adjustment S/MIME	L 9221			
	P-co	uord(priv)(Retupe) ^{×.}	(8,32 chara)	
Time adjustment S/MIME WebDAV Server WebDAV Client	P <u>a</u> ssi Passi	word(priv)(Retype)*:	(8-32 chars)	
Time adjustment S/MIME WebDAV Server WebDAV Client ₩ Web Service	Passi Set	word(priv)[Retype)*: the security level of the write	(8-32 chars) e setting, an user name and a pa	issword. 📉

6 Click the "Security Level" pull-down menu and select [auth-password] or [auth-password/priv-password].



7 Click the "Set a password" check box and enter the new 8-digit-or-more auth-password or priv-password.

Setting list:					
Status	Item	Value		Result	6
-	V1/V2 Write Permiss	Disable			
	V1/V2 Read Commu	public			
	V1/V2 Write Commu	private			
	V3 Context Name				
	V3 Discovery User P	Enable, V3 [Discovery User Name=pu		
	V3 Read User	Security Lev	el=auth-password/priv-pa		
Update	V3 Write User	Security Lev	el=auth-password/priv-pa		
	V3 Authentication Al	MU5			
	V3 Encryption Algorit	DES			-
<					>
User Nan	User Name*:				
Curren	nt Password(auth)*	NERNER	[8-32 chars]		
Passv	vord (auth)*:	NECENER	(8-32 chars)		
Passv	vord(auth)(Retype)*:	XXEXXEX	(8-32 chars)		
✓ Set a	password.				
Currer	nt Password(priv)*:	NNERNEE	(8-32 chars)		
P <u>a</u> ssv	vord (priv)*:	NNESSEE	(8-32 chars)		
Passv	vord(priv)(Retype)*:	NNERNE	(8-32 chars)		
(D) 0.11	Second States and a Color and				
	Update	Status I fem VTA2 Write Permiss VTA2 Write Read Commu- VTA2 Write Name VTA2	Status Item Value V1/X2 Write Permiss Disable V1/X2 Read Commun public V3 Discovery User P Enable.V3 I V3 Encorption Agont DES Setting Setting Setting Estimation of the setting Setting Setting Setting Estimation of the setting Set a password Estimation of the setting Set a password (suth)*: Estimation of the setting Set a password (priv)*: Estimation of the setting V2 Encorption Agont Estimation of the setting Set a password (priv)*: Estimation of the setting Password (priv)*: Estimation of the setting	Status Item Value V1/N2 Write Permiss Diable V1/N2 Write Commun public V1/N2 Write Commun public V1/N2 Write Learn Security Level-autrip-password/priv-pa V3 Discovery User P Security Level-autrip-password/priv-pa V3 Arekytoin Algoet DES Security Level-autrip-password/priv-password/priv-password/priv-password/priv-password/priv-password/priv-password/priv-password/priv-password Setting: setting Security Level auth-password/priv-password Upst Value setting Setting: setting Password(auth)*: setting Setting: setting Password(auth)*: setting Setting: setting Password(auth)*: setting Password(auth)*: setting Password(auth)*: setting Password(auth)*: setting Passwo	Status Item Value Herm V1/N2 Wite Permiss Diable public V1/N2 Wite Permiss Diable V1/N2 Wite Permiss Diable V3 Dicorvey User Name-put Security Level-suth_password/priv-pa V3 Dicorvey User Name-put Security Level-suth_password/priv-pa V3 Annovember Name M3 Enclose Name V3 Annovember Name Security Level-suth_password/priv-pa V3 Annovember Name Discovery User Name-put Security Level- Security Level-suth_password/priv-pa V3 Encryption Algorit Discovery User Name-put Security Level- Security Level-suth_password/priv-pa User Name*: earth-password/priv-password User Name*: iestinct V3 Encryption Algorit Bissover User Name*: iestinct V3 Encryption Algorit Bissover Current Password(auth)*: iestinct V3 Encryption Algorit Bissover Password(auth)*: iestinct V3 Encryption Algorit Bissover Current Password(auth)*: iestinct V3 Encryption Algorit Bissover Password(auth)*: iestinct V3 Encryption Algorit Bissover <td< td=""></td<>

- 8 Click [Export to the device].
 - → If the auth-password or priv-password entered does not meet the requirements of the Password Rules, [Export to the device] cannot be selected. Enter the correct auth-password or priv-password. For details of the Password Rules, see page 1-8.
 - → If you have already logged on to the Administrator Settings via the control panel or using PageScope 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.

4.1.8 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 PageScope Data Administrator. If it is absolutely necessary to leave the site, be sure first to log off from the PageScope Data Administrator.
- 1 Access the machine through [Administrator settings] mode of PageScope 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 Settings via the control panel or using PageScope 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.

4.1.9 NetWare Setting Function

<Making the NetWare Setting>

- ✓ 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 PageScope Data Administrator. If it is absolutely necessary to leave the site, be sure first to log off from the PageScope Data Administrator.
- 1 Access the machine through [Administrator settings] mode of PageScope Data Administrator.
- 2 Click the Administrator settings expand button.
- 3 Click the Network expand button.
- 4 Click [NetWare].
- 5 Make the necessary settings.
- 6 Click [Export to the device].
 - → If you have already logged on to the Administrator Settings via the control panel or using PageScope 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.

bizhub C360/C280/C220

4.1.10 SMB Setting Function

<Setting the NetBIOS Name>

- ✓ 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 PageScope Data Administrator. If it is absolutely necessary to leave the site, be sure first to log off from the PageScope Data Administrator.
- 1 Access the machine through [Administrator settings] mode of PageScope Data Administrator.
- 2 Click the Administrator settings expand button.
- 3 Click the Network expand button.
- 4 Click [SMB].
- 5 Click [NetBIOS Name] of Setting list, enter the NetBIOS Name.
- 6 Click [Export to the device].
 - → If you have already logged on to the Administrator Settings via the control panel or using PageScope 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.

bizhub C360/C280/C220

4.1.11 AppleTalk Setting Function

<Making the AppleTalk Setting>

- ✓ 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 PageScope Data Administrator. If it is absolutely necessary to leave the site, be sure first to log off from the PageScope Data Administrator.
- 1 Access the machine through [Administrator settings] mode of PageScope Data Administrator.
- 2 Click the Administrator settings expand button.
- 3 Click the Network expand button.
- 4 Click [AppleTalk].
- 5 Make the necessary settings.
- 6 Click [Export to the device].
 - → If you have already logged on to the Administrator Settings via the control panel or using PageScope 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.

4.1.12 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 PageScope Data Administrator. If it is absolutely necessary to leave the site, be sure first to log off from the PageScope Data Administrator.
- 1 Access the machine through [Administrator settings] mode of PageScope 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 Settings via the control panel or using PageScope 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.

4.2 PageScope Box Operator

PageScope Box Operator is application software used exclusively for changing the name of scan or fax data stored in a User Box, downloading or deleting such scan or fax data, creating a User Box, changing the properties (user attributes) of a User Box, and performing other tasks. It allows a network-connected PC to gain access to the HDD of the machine for accomplishing these tasks.

When an attempt is made to gain access to the machine through PageScope Box Operator, the user is authenticated to be an authorized user by using an 8-to-64-digit User Password and an 8-digit User Box Password. During the authentication procedure, the password entered appears as "*." When the Enhanced Security Mode is set to [ON], the number of times in which authentication fails is counted.

4.2.1 Accessing the User Box

- ✓ Do not leave the site while you are gaining access to the machine through PageScope Box Operator. If it is absolutely necessary to leave the site, be sure first to log off from the PageScope Box Operator.
- 1 Start the PageScope Box Operator.
- 2 Double-click this machine.



3 Type the User Name and the 8-to-64-digit User Password.

User authentication - [MFP1]		
Enter user name and password.		
C Log on as public user.		
Log on with the specified user name.		
User name: user1		
Password:		
🕅 Save logon user name.		
Select External Server		
Help (F1) OK Cancel		

- → If [ON (External Server)] is set for the authentication method, select the desired external server.
- 4 Click [OK].
 - → If the User Password entered does not correspond to the registered User Name, a message appears that tells that authentication has not been successful. Click [OK] and then enter the correct User Password.
 - → If the Enhanced Security Mode is set to [ON], the entry of a wrong User Password is counted as unauthorized access. If a wrong User Password is entered a predetermined number of times (once to three times) or more set by the Administrator of the machine, a message appears that tells that authentication has not been successful for any subsequent operation for authentication. The machine is then set into an access lock state, rejecting any more logon attempts. To cancel the access lock state, the Administrator of the machine must perform the Release Setting. Contact the Administrator of the machine.

- → If [ON (External Server)] (Active Directory) is set for the authentication method and if user authentication is successful, the User Name not registered in the machine is automatically registered.
- → If the "Save logon user name" check box has been selected, the User Password entered is stored in the PC being used. If you do not want the User Password stored, clear the "Save logon user name" check box.
- 5 Click or double-click the desired User Box icon.



6 Type the 8-digit User Box Password.

Password confirmation ? 🔀		
Enter the password for the user box(Personal User Box).		
Password:		
Save box password until disconnected.		
Help (F1) OK Cancel		

7 Click [OK].

- → If there is a mismatch in the User Box Password, a message appears that tells that authentication has not been successful. Click [OK] and then enter the correct User Box Password.
- → If the Enhanced Security Mode is set to [ON], the entry of a wrong User Box Password is counted as unauthorized access. If a wrong User Box Password is entered a predetermined number of times (once to three times) or more set by the Administrator of the machine, a message appears that tells that authentication has not been successful for any subsequent operation for authentication. The machine is then set into an access lock state, rejecting any more logon attempts. To cancel the access lock state, the Administrator of the machine must perform the Release Setting. Contact the Administrator of the machine.
- → To delete a User Box, select the desired User Box icon, and select [Delete] from the [File] menu. A confirmation message appears. Click [Yes] and enter the User Box Password corresponding to the specific User Box. This deletes the User Box.
- → If the "Save box password until disconnected" check box has been selected, the User Box Password entered is stored in the PC being used. If you do not want the User Box Password stored, clear the "Save box password until disconnected" check box.

4.2.2 Creating a User Box

- ✓ For the procedure to access the User Box, see steps 1 through 4 of page 4-20.
- ✓ Do not leave the site while you are gaining access to the machine through PageScope Box Operator. If it is absolutely necessary to leave the site, be sure first to log off from the PageScope Box Operator.
- ✓ For the procedure to change the User Box Password and properties (user attributes, account attributes), see page 4-23.
- 1 Access the User Box through PageScope Box Operator.
- 2 From the [Box Operator] menu, select [Create User Box]. Or, click 👩 .
- 3 Make the necessary settings.

Create box	?
User box <u>p</u> umber;	1 🔄 🔽 Use unused box numb
User box nam <u>e</u> :	Personal User Box
User box type:	C Public
	Select External Server
	v
	C <u>G</u> roup O <u>wner</u> 1
	,
Password:	
Confirm pass <u>w</u> ord:	XXXXXXXXX
<u>I</u> ndex:	etc 💌 🗖 Main
Auto Document	Static Save
Delete Time:	C Free Orth 52 m
	,,
Help (F1)	Create Cancel

- → Do not fail to enter data in the "User Box name," "Password," and "Confirm password" boxes.
- → If the "Use unused box number" check box is selected, the User Box No. is automatically assigned.
- → If "Public" is selected for User Box Type, set the User Box Password that meets the requirements of the Password Rules. For details of the Password Rules, see page 1-8.
- → A Use Box Number that already exists cannot be redundantly registered.
- → If [Personal] is selected for User Box Type, enter the User Name of the user who owns the User Box in the "Owner" box.
- → If [Group] is selected for the User Box Type, enter the name of the account that owns the box in the "Owner" box.
- 4 Click [Create].
 - → If the User Box Password entered does not meet the requirements of the Password Rules, a message appears that tells that the User Box Password entered cannot be used. Click [OK] and enter the correct User Box Password. For details of the Password Rules, see page 1-8.
 - → If there is a mismatch in the User Box Password between that entered in the "Password" box and that entered in the "Confirm password" box, a message appears that tells that there is a mismatch in the User Box Password. Enter the correct User Box Password.
 - → If the Owner Name is not entered with "Personal" selected for User Box Type, a message appears that warns that the Owner Name is yet to be entered. Enter the correct Owner Name.
 - → If the Account Name is not entered with "Group" selected for User Box Type, a message appears that warns that the Account Name is yet to be entered. Enter the correct Account Name.
 - → If a user name not registered with the machine is entered in the "Owner Name" box, a message appears that tells that the Owner Name entered in the box is illegal. Click [OK] and enter the correct Owner Name.
 - → If a account name not registered with the machine is entered in the "Account Name" box, a message appears that tells that the Account Name entered in the box is illegal. Click [OK] and enter the correct Account Name.

4.2.3 Changing the User Box properties (user attributes, account attributes)

- ✓ For the procedure to access the User Box, see steps 1 through 4 of page 4-20.
- ✓ Do not leave the site while you are gaining access to the machine through PageScope Box Operator. If it is absolutely necessary to leave the site, be sure first to log off from the PageScope Box Operator.
- 1 Access the User Box through PageScope Box Operator.
- 2 Select the icon of the desired User Box.
- 3 From the [File] menu, select [Property], or right-click to select [Property].
- 4 Make the necessary settings.

	Box namg: Personal User Box
User box number:	2
User box type:	C Public
	Select External <u>S</u> erver
	C Group
Connected to:	MFP1 []
Logged on user:	user1
Date/time registered	: 2009/01/19 11:08:56
Index:	etc Main
Auto Document Delete <u>T</u> ime:	Static 1 Day
	C Free h n
Click [Change Passy the password.	word] to set or change Change Password.

- → To change the owner of the User Box, enter the user name that has been registered with this machine as a user for a Personal User Box and that has been registered with this machine as an account for a Group User Box.
- → If the User Box Type has been changed to [Public], be sure to set a User Box Password that meets the requirements of the Password Rules.
- → To set the User Box Password, perform steps 7 through 9.
- 5 Click [OK].
 - → If a User Box Password has been set, the password confirmation screen appears. Then, enter the currently set 8-digit User Box Password and click [OK].

Password confirmation		
Enter the password for the user box(Personal User Box).		
Password:	*****	
□ <u>Save box password until disconnected.</u>		
Help (F1)	OK Cancel	

- → If User Box Type is changed from "Personal" or "Group" to "Public" and if the User Box Password set for the Personal or Group User Box before this change does not meet the requirements of the Password Rules, a message appears that tells that the User Box Password is illegal. When [OK] is then clicked, a password confirmation screen appears. Now, click [Cancel] and set a User Box Password that meets the requirements of the Password Rules. For the procedure to change the User Box Password, see steps 7 through 9. For details of the Password Rules, see page 1-8.
- → If a wrong User Box Password is entered, a message appears that tells that the User Box Password entered is wrong. Click [OK] and then enter the correct User Box Password.
- → If the Enhanced Security Mode is set to [ON], the entry of a wrong User Box Password is counted as unauthorized access. If a wrong User Box Password is entered a predetermined number of times (once to three times) or more set by the Administrator of the machine, a message appears that tells

Δ

that authentication has not been successful for any subsequent operation for authentication. The machine is then set into an access lock state, rejecting any more logon attempts. To cancel the access lock state, the Administrator of the machine must perform the Release Setting. Contact the Administrator of the machine.

- → If the "Save box password until disconnected" check box has been selected, the User Box Password entered is stored in the PC being used. If you do not want the User Box Password stored, clear the "Save box password until disconnected" check box.
- 6 Select [Property] from the [File] menu or right-click to select [Property].
- 7 Click [Change Password].
- 8 Enter the User Box Password.

×	Change password		
	ew <u>p</u> assword:		

	Confirm normanity		
_	minin new pass <u>w</u> uru.		
I	Help (F1) OK Cance		
>	Help (F1) OK Cance		

- → If Public is to be set for User Box Type, a password that meets the requirements of the Password Rules must be entered in the "New Password" box. For details of the Password Rules, see page 1-8.
- → In the "Confirm new password" box, enter the same User Box Password as that entered in the "New password" box.
- 9 Click [OK].
 - → When [OK] is clicked, the password confirmation screen of step 5 appears. Enter the 8-digit User Box Password, which was set before the change of the password, and click [OK].
 - → If the User Box Password entered does not meet the requirements of the Password Rules with "Public" selected for User Box Type, a message appears that tells that the User Box Password entered cannot be used. Click [OK] and perform steps 8 and 9 again. For details of the Password Rules, see page 1-8.
 - → If the Enhanced Security Mode is set to [ON], the entry of a wrong User Box Password is counted as unauthorized access. If a wrong User Box Password is entered a predetermined number of times (once to three times) or more set by the Administrator of the machine, a message appears that tells that authentication has not been successful for any subsequent operation for authentication. The machine is then set into an access lock state, rejecting any more logon attempts. To cancel the access lock state, the Administrator of the machine must perform the Release Setting. Contact the Administrator of the machine.

bizhub C360/C280/C220

Z

4.2.4 Accessing the User Box file

- ✓ For the procedure to access the User Box, see steps 1 through 4 of page 4-20.
- ✓ Do not leave the site while you are gaining access to the machine through PageScope Box Operator. If it is absolutely necessary to leave the site, be sure first to log off from the PageScope Box Operator.
- 1 Access the User Box through PageScope Box Operator.
- 2 Select the desired file.



3 Select the desired function.

Different functions can be operated depending on the file format.

Study the following table for the relationship between the file format and operable functions.

File format	Operable functions
PDF	Icon display, thumbnail display, detail display, opening in a specific applica-
Compact PDF	tion, file acquisition, file name change, file deletion, copy to another User Box, move to another User Box, copy to another Folder, move to another Folder
JPEG	Icon display, thumbnail display, detail display, opening in a specific applica-
TIFF	tion, opening in Box Operator viewer, file acquisition, file name change, file de- letion, copy to another User Box, move to another User Box, copy to another Folder, move to another Folder

→ The file saved in the User Box may be saved in your PC from PageScope Box Operator through drag-&-drop.

bizhub C360/C280/C220

Λ

4.3 HDD TWAIN driver

The HDD TWAIN driver, which is to be installed in the PC of a general user, is a TWAIN driver used exclusively for allowing the HDD of this machine to be recognized as a TWAIN device.

The HDD TWAIN driver is a utility function for downloading document data stored in the User Box in the scan or fax mode in the image processing application of the PC.

When an attempt is made to gain access to the machine through the HDD TWAIN driver, the user is authenticated to be an authorized user by using an 8-to-64-digit User Password and an 8-digit User Box Password. During the authentication procedure, the User Password entered for the authentication purpose appears as "*" on the display. When the Enhanced Security Mode is set to [ON], the number of times in which authentication fails is counted.

Accessing from the HDD TWAIN driver

- ✓ Do not leave the site while you are gaining access to the machine through the HDD TWAIN driver. If it is absolutely necessary to leave the site, be sure first to log off from the HDD TWAIN driver.
- **1** Start the image processing application.
- 2 From the [File] menu, click [Read], and then select [KONICA MINOLTA HDD TWAIN Ver.3].
- 3 Select this machine and click [Connect].

Select Devices		×
Device List		
● from Search Result	from <u>R</u> egistered Devices	
IP Address Device Name		
Add this to the registered device list	Search	
Connect Cancel	se this device for future session Help	1
		,

4 Select the "Login as the Registered User" radio button and enter the User Name and the 8-to-64-digit User Password.

User Authentication	
Enter User Name and Password	
C Login as Pyblic User	
Cogin as the <u>Registered</u> Use	a c
User <u>N</u> ame:	user1
Password:	RHNRENHR
 External Authentication Server 	
C External Authentication	
our or <u>D</u> omain	
OK	Cancel <u>H</u> elp

→ If [ON (External Server)] is set for the authentication method, enter the desired external server.

bizhub C360/C280/C220

- 5 Click [OK].
 - → If there is a mismatch of User Password relative to the registered User Name, a message appears that tells that authentication has not been successful. Click [OK] and then enter the correct User Name and User Password.
 - → If the Enhanced Security Mode is set to [ON], the entry of a wrong User Password is counted as unauthorized access. If a wrong User Password is entered a predetermined number of times (once to three times) or more set by the Administrator of the machine, a message appears that tells that authentication has not been successful for any subsequent operation for authentication. The machine is then set into an access lock state, rejecting any more logon attempts. To cancel the access lock state, the Administrator of the machine must perform the Release Setting. Contact the Administrator of the machine.
 - → If [ON (External Server)] (Active Directory) is set for the authentication method and if user authentication is successful, the User Name not registered in the machine is automatically registered.
- 6 Enter the desired Box No. and 8-digit Box Password.

Select Box		X
Enter Box No. and F	Password	
Device:		
User Name:	user1	
Вох <u>N</u> o.:	1	
Box Password:	XXXXXXXXX	
Box Name:		
	Select from Box List	
	OK Cancel Help	

- 7 Click [OK].
 - → If there is a mismatch between the User Box No. and User Box Password, a message appears that tells that authentication has not been successful. Click [OK] and perform step 6 once again.
 - → If the Enhanced Security Mode is set to [ON], the entry of a wrong User Password is counted as unauthorized access. If a wrong User Password is entered a predetermined number of times (once to three times) or more set by the Administrator of the machine, a message appears that tells that authentication has not been successful for any subsequent operation for authentication. The machine is then set into an access lock state, rejecting any more logon attempts. To cancel the access lock state, the Administrator of the machine must perform the Release Setting. Contact the Administrator of the machine.
- 8 Select the desired document data and click [Read].

4.4 PageScope Direct Print

PageScope Direct Print is an application that allows a PDF file or a TIFF file to be directly transmitted to, and printed on, the printer.

It permits printing of data through drag and drop to the desktop icon and using the context (right-click) menu of Windows, and automatic printing of data using a hot folder. The application also allows two or more different print job setups to be registered.

When data is to be printed through PageScope Direct Print, the user is authenticated to be an authorized user by using an 8-to-64-digit User Password or Account Password. When the Enhanced Security Mode is set to [ON], the number of times in which authentication fails is counted.

Printing through PageScope Direct Print

- If the "Edit Authentication/Account Track for each drag-and-drop printing" check box is not selected on the PageScope Direct Print main screen, no authentication screen appears for drag-and-drop printing. Select the "Edit Authentication/Account Track for each drag-and-drop printing" check box when using PageScope Direct Print.
- 1 Drag and drop the desired file to the PageScope Direct Print shortcut.
 - → Right-click the desired file. PageScope Direct Print can be selected from the menu that will then be displayed.
- 2 Select the "Use User Authentication" check box and the "Recipient User" radio button.

User Authentication/Accoun	t Track 🛛 🔀	
✓ Use User Authentication	Server Setting	
C Public User	Enhanced Server	
Recipient User		
User Name	•	
Password		
Account Track		
Password		

3 Enter the User Name and the 8-to-64-digit User Password that have been registered in the machine.

User Authentication/Account Track		
User Authentication		
Use User Authentication	Server Setting	
C Public User	Enhanced Server	
Recipient User		
User Name	user1 💌	
Password	RINKERNER	
- Account Track		
Use Account Track		
Department Name		
Password		
OK Cancel Help		

→ If [ON (External Server)] is set for the authentication method, select the desired external server.

4 To enable Account Track, click the [Use Account Track] check box.

User Authentication/Accou	nt Track	×
User Authentication		_
🔽 Use User Authentication	Server Setting	
C Public User	Enhanced Server	
Recipient User		_
User Name	user1 💌	
Password	RENERAR	
Account Track		
Use Account Track		
Department Name		
Password		
	-	
OK	Cancel Help	

5 Enter the Account Name and 8-to-64-digit Account Password registered with the machine.

User Authentication/Accou	nt Track 🛛 🔀
User Authentication	
✓ Use User Authentication	Server Setting
C Public User	Enhanced Server
Recipient User	
User Name	user1 💌
Password	NUKCENKK
A	
Account Track	
Use Account Track	
Department Name	1
Password	жиккеник
ОК	Cancel Help

- 6 Click [OK].
 - → If there is a mismatch between the Recipient User Name and User Password or between the Recipient Account Name and Account Password, the specified file is erased as an error from the machine without being printed.
 - → If the Enhanced Security Mode is set to [ON], the entry of a wrong User Password or Account Password is counted as unauthorized access. If a wrong User Password or Account Password is entered a predetermined number of times (once to three times) or more set by the Administrator of the machine, the machine is then set into an access lock state, rejecting any more logon attempts. To cancel the access lock state, the Administrator of the machine must perform the Release Setting. Contact the Administrator of the machine.

bizhub C360/C280/C220

4.5 HDD Backup Utility

The HDD Backup Utility, which is to be installed in the PC of the Administrator of the machine, is application software used exclusively for accessing the HDD in this machine.

The HDD Backup Utility functions performed by the Administrator of the machine allow the image data saved in the HDD of the machine to be backed up and restored. It is not possible to open directly the backup data.

To gain access to the machine from the HDD Backup Utility, the user is authenticated to be an authorized Administrator by using an 8-digit Administrator Password. The Administrator Password entered during the authentication procedure is displayed as "*." When the Enhanced Security mode is set to [ON], the number of times in which authentication fails is counted.

4.5.1 Backup

- ✓ In Backup, neither the Administrator Password nor CE Password is backed up.
- 1 Start the HDD Backup Utility.
- 2 Select this machine and click [Backup].

isic Se	ettings					
evice	list:			Number o	f Displayed Devices:1	Function Selection
tatus	Status Display	Registered name	Group name	Model name	Device address	🚰 Backup
\$	Online	MEP	Default Group			Hestore
						Device Selection Filter
						Display All

3 Enter the 8-digit Administrator Password registered in the machine in the "Administrator password" box.

Connect to the device to be backed up.		1/
Enter the Administrator password.		
Registered name:	Device address:	
MFP		
Administrator password:	816501000	
Administrator password (confirmation):		
Important		
Make sure the device has been prepare Do not turn off the device during backup Do not shut down the OS. Do not unplug the network cable of the c	d for backup. a. device or the PC during backup.	

- → If the "Save the administrator password" check box is selected, the Administrator Password entered is stored in the PC being used. If you do not want the Administrator Password stored, clear the "Save the administrator password" check box.
- 4 Click [Next].
 - → 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 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 of the machine, 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.

Here is the sequence, through which the main power switch and sub power switch are turned on and off:

Turn off the sub power switch \rightarrow Turn off the main power switch \rightarrow Turn on the main power switch \rightarrow Turn on the sub power switch

- → Make sure that none of the general users of the machine will know the Administrator Password.
- → If the Administrator Password is forgotten, it must be set again by the Service Engineer. Contact your Technical Representative.
- 5 From "Backup media," select the check box of the desired media and click [Next].

Select backup target Select the target of backup from the device			2/7
Select the backup target. © Backup Box © Backup Image			Connected
Image Backup Tage Media Media name ⊠∭W/RAM, FLASH, HOD	Size 198,689.00 MB		=
Help(F1)	< Back	<u>N</u> ext >	Cancel

6 Click [Browse] and specify the destination, in which the backup folder is to be saved.

Backup folder s Create the bac	t tings up folder.	3/7
For the boot of	the end of the second	Connect
Backup folder pat	ader parn and iname.	
C:N		Browse
Backup folder nar	8.	
Backup size:	148.1 MB	
Explanation The HDD Ba specified in [E	up Utility creates the folder specified in [Backup ckup folder path], and saves the data acquired I	folder name) in the location rom the device.
		[]

7 Type a backup folder name that consists of 1 to 50 characters in the "Backup folder name" text box and click [Next].

					_ 🗆 🛛
Backup folder Create the ba	settings skup folder.				3/7
					Connecte
Enter the backup	o folder path and name.				
Backup folder p	əth:				
C:\				Browse	
Backup folder n	me:				
Backup_20090	20_101357_001				
, Backup size:	148.1 MB				
Explanation					
The HDD B specified in	ackup Utility creates the fol Backup folder path], and s	der specified in (Bac aves the data acqui	kup folder name) in 1 red from the device.	he location	
Help(F1)			< Back	lext>	Cancel
		-	- [-

8 To set a password for the backup file, select the corresponding check box and type a password that consists of 1 to 64 digits in the box for "Password for backup file" and "Password for backup file (confirmation)" and then click [Next].

4/7
Connect
nd enter the password.
om malicious users.

9 Check the data that has been set and click [Start].

		Conr
If the settings are correct, click [Start].		
Setting information		
Device to be backed up:	MFP	
Backup type:	Box Backup	
Backup folder:	C:\Backup_20090120_101357_001	
Backup size:	148.1 MB	
Used disk space after backup:	18.3 GB	
Free disk space after backup:	18.9 GB	
Disk ratio after backup:		

10 Make sure that the backup procedure has been completed. Then, click [Finish].

Backup wa	s completed.	
Target device:	MFP	
Backup type:	Box Backup	
Backup folder:	C:\Backup_20090120_101357_001	
Report file:	C:\Documents and Settings\Administrator.DAD\L	ocal Settings\Application Data\K01
		View report

4.5.2 Restore

- 1 Start the HDD Backup Utility.
- 2 Select this machine and click [Restore].

Device	list:			Number o	f Displayed Devices:1	Function Sele	tion
Status	Status Display	Registered name	Group name	Model name	Device address	PB Bestore	
8	Online	MFP	Default Group			Device Selection	o Cibor
						Display All	rinei
						supply ris	

3 Click [OK].

	×
(į)	Restoring will overwrite the data on the media built into the device. Click [OK] to restore or [Cancel] to cancel restoration.
	OK Cancel

4 Click [Browse] and specify the destination, in which the backup file is to be saved.

Select the restoration sou	rce with the Browse button.		
Backup folder:	01357 001	Browse	ſ
C. 1040K0p_20000120_1	01001_001		
Restoration source info	mation		
Device name: Rocked up device:	NCD .		
Backup tupe:	MFP Roy Backup		
Backup size:	1481 MB		
Backup date:	01/20/2009 10:13:57		

→ If a password has been set for the backup data, type the password that consists of one to 64 digits set during Backup and click [OK].

A password has Enter the passw	been set for the backup files. ord that was set during backup.
Password:	
Help(F1)	OK Cancel

5 Click [Next].

6 Type the 8-digit Administrator Password registered in the machine in the "Administrator Password" box.

Connect to device Connect to the device to be restored.		2/5
Enter the Administrator password.		
Registered name:	Device address:	
MFP		
Administrator password:		-
Important Make sure the device has been prepar Do not turn off the device during restor Do not shut down the OS	ed for restoration. ation.	

→ If the "Save the administrator password" check box is selected, the Administrator Password entered is stored in the PC being used. If you do not want the Administrator Password stored, clear the "Save the administrator password" check box.

7 Click [Next].

- → 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 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 of the machine, 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.

Here is the sequence, through which the main power switch and sub power switch are turned on and off:

Turn off the sub power switch \rightarrow Turn off the main power switch \rightarrow Turn on the main power switch \rightarrow Turn on the sub power switch

- → Make sure that none of the general users of the machine will know the Administrator Password.
- → If the Administrator Password is forgotten, it must be set again by the Service Engineer. Contact your Technical Representative.
- 8 Check the data that has been set and click [Start].

		Conne
If the settings are correct,	click [Start]	
Restoration information		
Target device:	MFP	
Postoration source inform	a tion	
- Nestoration source mon		
Backup type:	Box Backup	
Backup folder:	C:\Backup_20090120_101357_001	
	1101110	

9 Click [OK].

Make sure that Restore procedure has been completed and then click [Finish].

Restoration end	d with the following result.	5/5
Restoratio	n was completed.	
Target device:	MFP	
Backup type:	Box Backup	
Backup folder:	C:\Backup_20090120_101357_001	
Report file:	C:\Documents and Settings\Administrator.DAD\Local Settings\	Application Data\K01
		View report


http://konicaminolta.com