Hard Disk Drive Security

Enabling bizhub HDD Security Features

- bizhub C650/C550/C451
- bizhub C353/C253/C203
- bizhub 501/421/361
- bizhub 751/601

COUNT ON KONICA MINOLTA

1 Enabling bizhub HDD Security - Overview

This guide is intended to assist the bizhub Multi-Function Printer (MFP) Administrator with the steps and procedures necessary to ensure that the appropriate HDD Security Features are enabled and functioning.

The process and procedure involved in setting up or enabling the HDD Security Functions of a typical bizhub MFP are outlined as follows;

✓ The first step in MFP security is changing the default Administrator Password to a secure password, an AlphaNumeric password is highly recommended (no spaces).

✓ Next, it is very critical that the user not forget any of the passwords created using this guide. Some of the passwords created in this guide will require a service technician, replacement parts and significant cost and down time to be corrected.

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

If the MFP in question is being installed for the first time or has been previously sanitized;

- Enable the Encryption Key Setting. See Section 2
- Enable Overwrite Temporary Data. See Section 3
- Enable HDD Lock Password. See Section 4
- Enable User Box/Secure Box Auto Deletion Settings. See Section 5
- Enable Overwrite All HDD Data – End of Life HDD Sanitization. See Appendix A

If the MFP is currently running and has stored information, addresses, on-touch locations, etc already in use the following is recommended;

- It is highly recommended to back up the HDD using the Konica Minolta HDD Backup Utility application. See Appendix B
- Enable the Encryption Key Setting. See Section 2
- Enable Overwrite Temporary Data. See Section 3
- Enable HDD Lock Password. See Section 4
- Enable User Box/Secure Box Auto Deletion Settings. See Section 5
- Enable Overwrite All HDD Data – End of Life HDD Sanitization. See Appendix A
- Re-install the HDD Back copy of the MFP

Important Items to Remember…

✓ Do not leave or walk away from the machine when Administrator Settings screen is open and 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/Passwords. Try to change the Encryption Key/Passwords at regular intervals.

✓ Make sure that nobody but the Administrator of the machine comes to know the Encryption Key/Passwords.

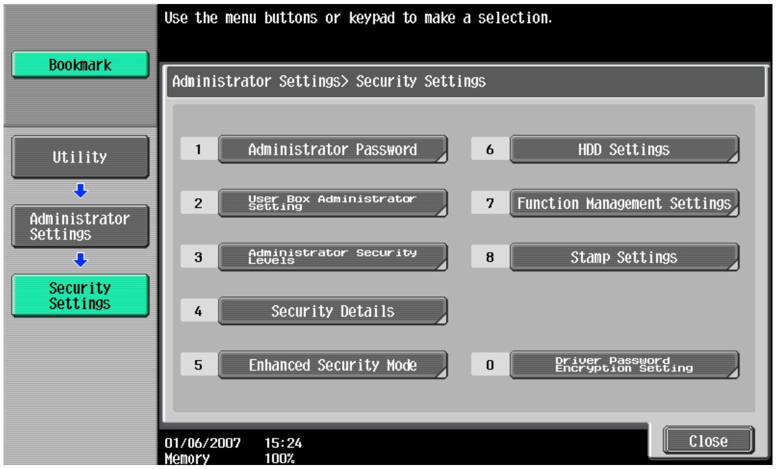
2 Enabling the Encryption Key Setting

✓ The supported MFP models in this guide can have the HDD Encryption Kit as an optional accessory. This accessory must be installed and enabled by a service technician prior to following the steps outlined in this section. This section will demonstrate the steps necessary to enable or change the Encryption Key. These settings can be completed by the MFP Administrator a service technician is not required.

Setting the Encryption Key (Encrypting the HDD)

1 Enter the Administrator Mode on the MFP display, *Utility/Counter button* > *Administrator Settings* > *Input Admin Password* > *Security Settings*.

2 Touch [HDD Settings].

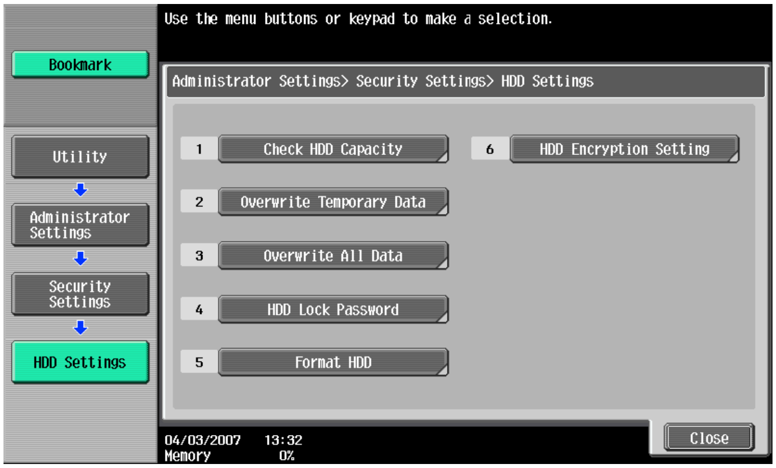


Use the menu buttons or keypad to make a selection.

Administrator Settings> Security Settings

01/06/2007 15:24
Memory 100%

3 Touch [HDD Encryption Setting].

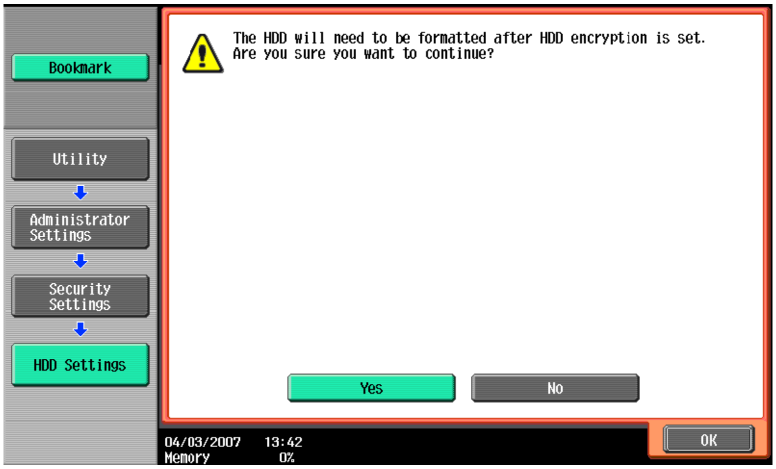


Use the menu buttons or keypad to make a selection.

Administrator Settings> Security Settings> HDD Settings

04/03/2007 13:32
Memory 0%

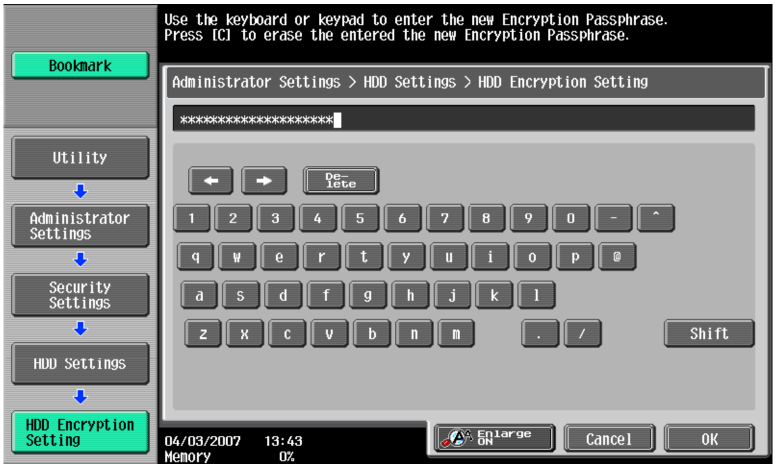
4 A confirmation message appears. Select [Yes] and touch [OK].



The HDD will need to be formatted after HDD encryption is set.
Are you sure you want to continue?

04/03/2007 13:42
Memory 0%

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].



Use the keyboard or keypad to enter the new Encryption Passphrase.
Press [C] to erase the entered the new Encryption Passphrase.

Administrator Settings > HDD Settings > HDD Encryption Setting

****

04/03/2007 13:43
Memory 0%

Keyboard Operation Notes:

→ To clear all characters Press the [C] key.

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

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

→ To go back to the HDD Settings screen Touch [Cancel].

6 Touch [OK], Re-Enter the Encryption Key and Touch [OK].

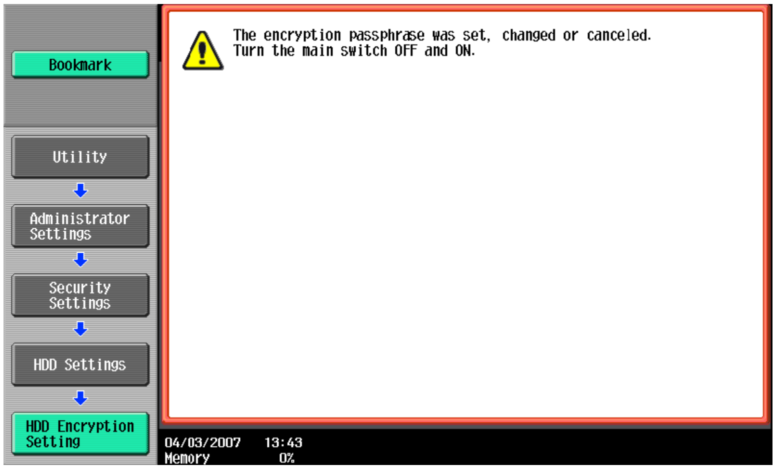
→ If the Encryption Key entered does not meet the requirements of the Password Rules, a message appears that tells that the Encryption Key entered cannot be used. Enter the correct Encryption Key. For details of the Password Rules, see Appendix C.

→ 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.

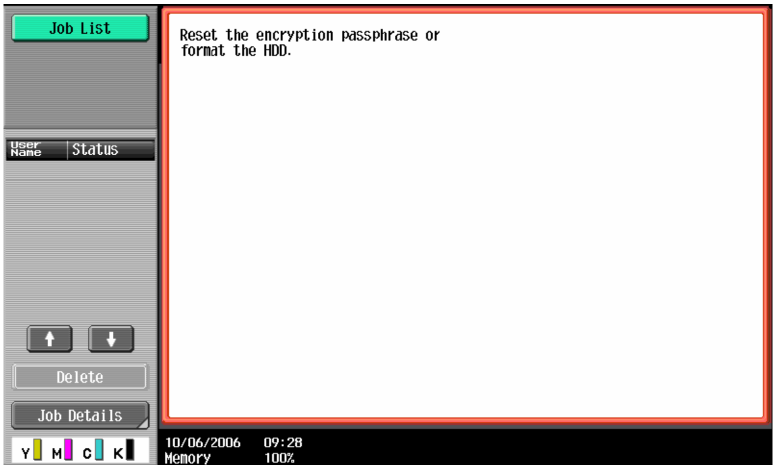
7 Make sure that a message appears prompting you to turn OFF and then ON the main power switch. Now, turn OFF and then turn ON the main power switch.

→ 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 > Turn off the main power switch > Turn on the main power switch > Turn on the sub power switch

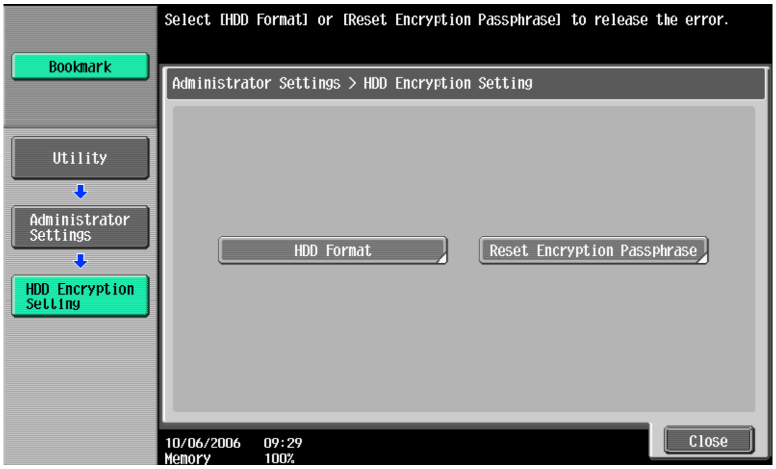

The encryption passphrase was set, changed or canceled.
Turn the main switch OFF and ON.

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

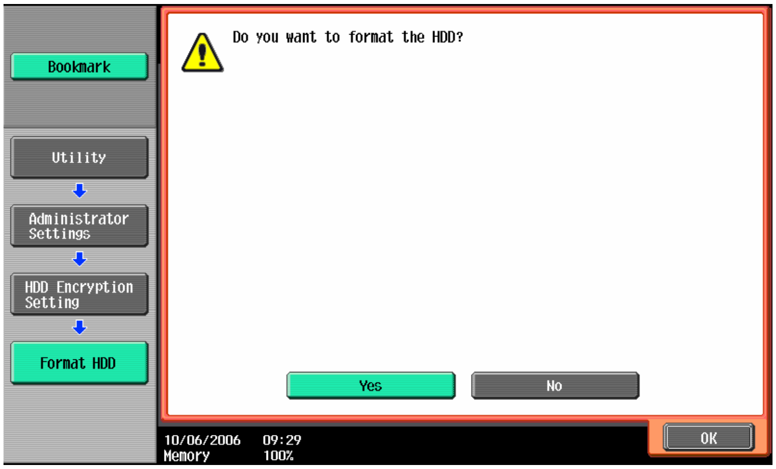

Reset the encryption passphrase or format the HDD.

9 Enter the Administrator Mode on the MFP display, *Utility/Counter button > Administrator Settings > Input Admin Password > HDD Encryption Settings*.

10 Touch [HDD Format].


Select [HDD Format] or [Reset Encryption Passphrase] to release the error.

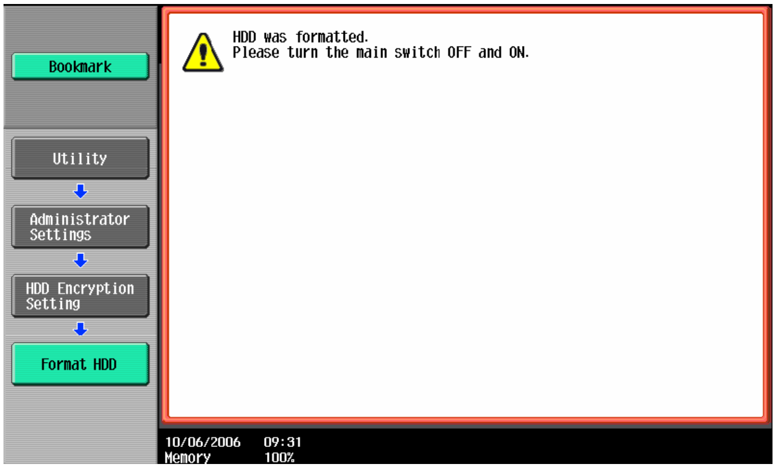
11 A confirmation message appears. Select [Yes] and touch [OK].



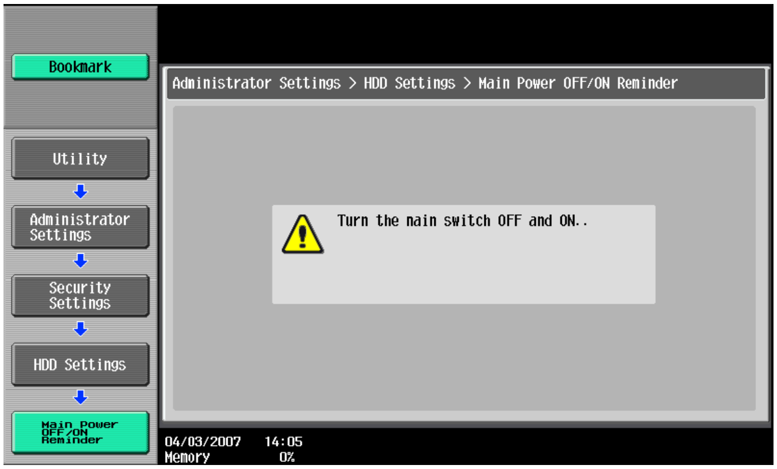
Do you want to format the HDD?

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

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



HDD was formatted.
Please turn the main switch OFF and ON.



Administrator Settings > HDD Settings > Main Power OFF/ON Reminder

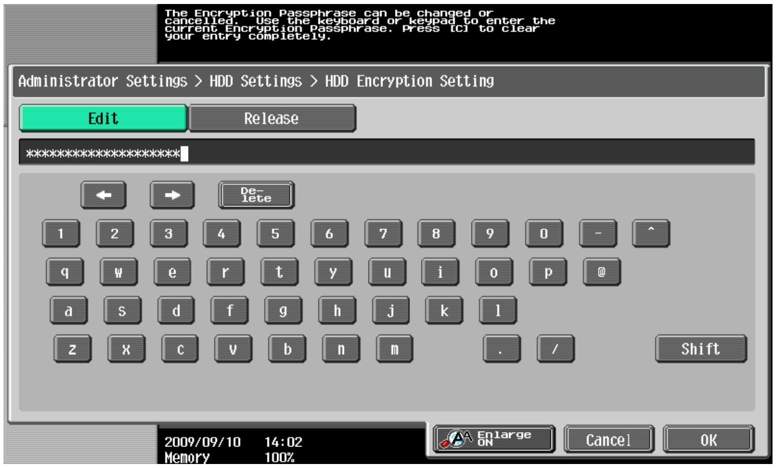
Turn the nain switch OFF and ON..

Changing the Encryption Key

- ✓ The Encryption Key can be changed or modified at any time by the Administrator using the Edit Button.
- ✓ The Encryption Key can be cancelled or released at any time by the Administrator using the Release Button.

1 Enter the Administrator Mode on the MFP display, *Utility/Counter button* > *Administrator Settings* > *Input Admin Password* > *HDD Settings* > *HDD Encryption Settings.*

2 Enter the currently registered 20-digit Encryption Key from the keyboard and keypad.



The Encryption Passphrase can be changed or cancelled. Use the keyboard or keypad to enter the current Encryption Passphrase. Press [C] to clear your entry completely.

Administrator Settings > HDD Settings > HDD Encryption Setting

****

2009/09/10 14:02
Memory 100%

Keyboard Operation Notes:

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

3 Select [Edit] and touch [OK].

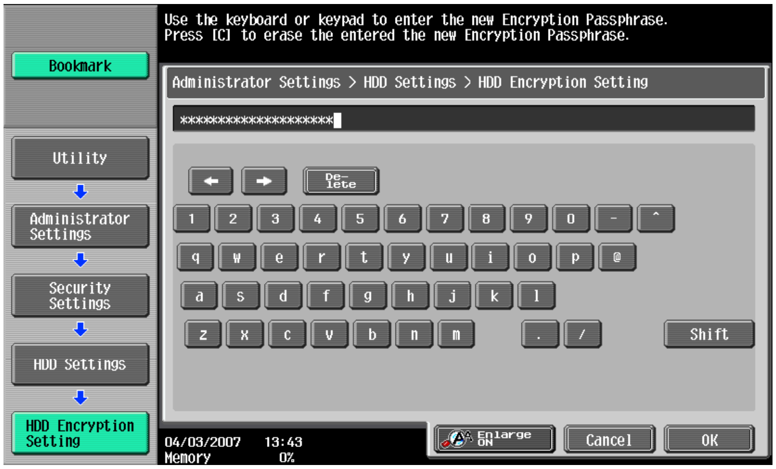
- → If there is a mismatch in the Encryption Keys, a message appears that tells that there is a mismatch in the Encryption Keys. Enter the correct Encryption Key.

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].

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 Appendix C.
- → 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.



Use the keyboard or keypad to enter the new Encryption Passphrase.
Press [C] to erase the entered the new Encryption Passphrase.

Administrator Settings > HDD Settings > HDD Encryption Setting

****

04/03/2007 13:43
Memory 0%

Keyboard Operation Notes:

→ To clear all characters Press the [C] key.

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

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

→ To go back to the HDD Settings screen Touch [Cancel].

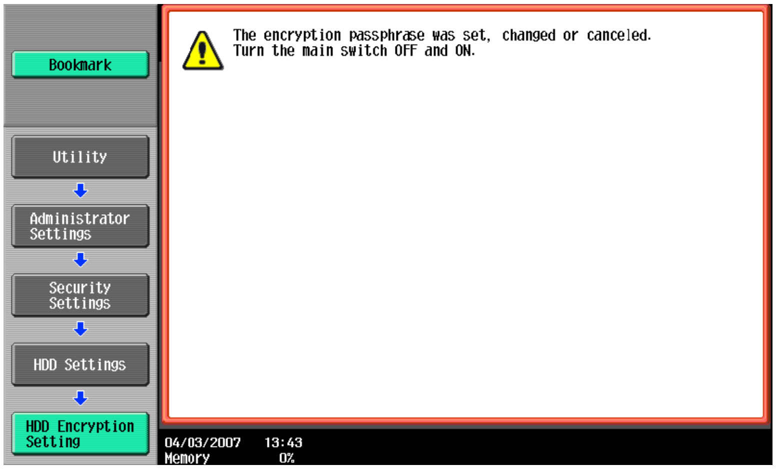
6 Touch [OK], Re-Enter the Encryption Key and Touch [OK].

→ 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 Appendix C.

→ 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.

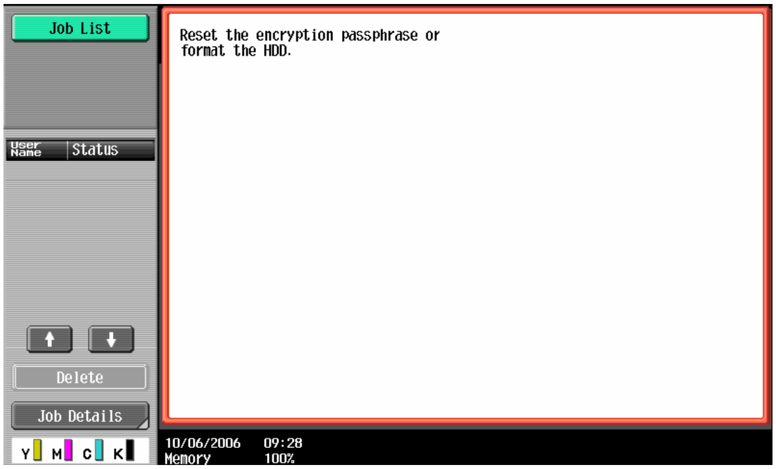
→ When the main power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. if there is no wait period between turning the main power switch off, then on again, the machine may not function properly. Here is the sequence, through which the main power switch and sub power switch are turned on and off:
Turn off the sub power switch > Turn off the main power switch > Turn on the main power switch > Turn on the sub power switch



The encryption passphrase was set, changed or canceled.
Turn the main switch OFF and ON.

04/03/2007 13:43
Memory 0%

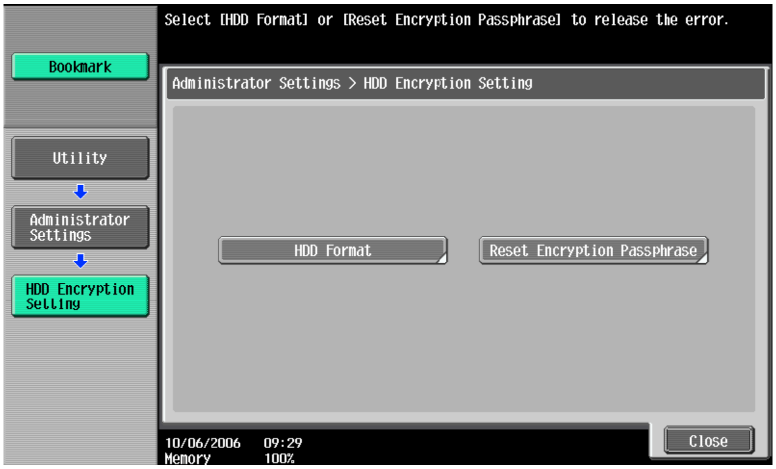
8 The following screen appears after the machine has been restarted.



Reset the encryption passphrase or format the HDD.

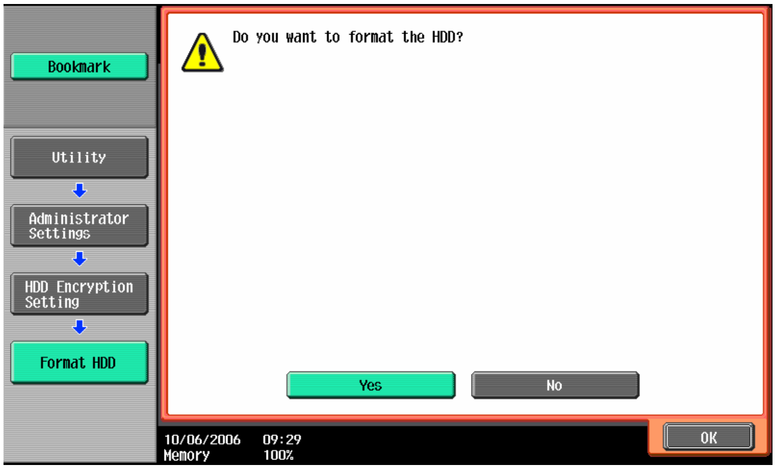
9 Enter the Administrator Mode on the MFP display, *Utility/Counter button* > *Administrator Settings* > *Input Admin Password* > *HDD Encryption Settings*.

10 Touch [HDD Format].



Select [HDD Format] or [Reset Encryption Passphrase] to release the error.

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

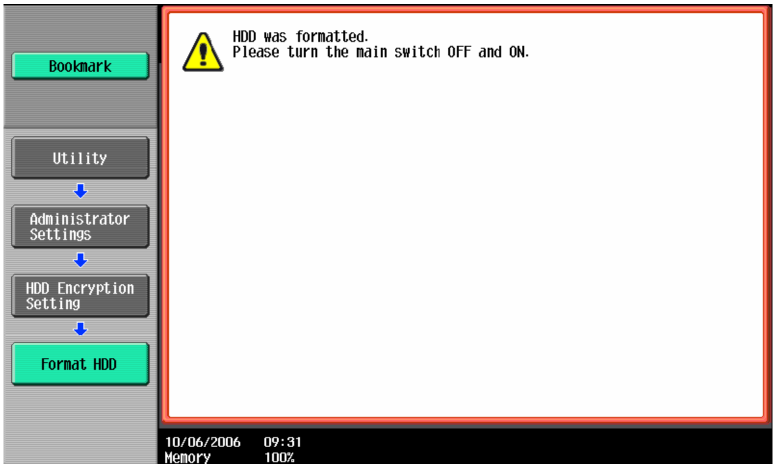


Do you want to format the HDD?

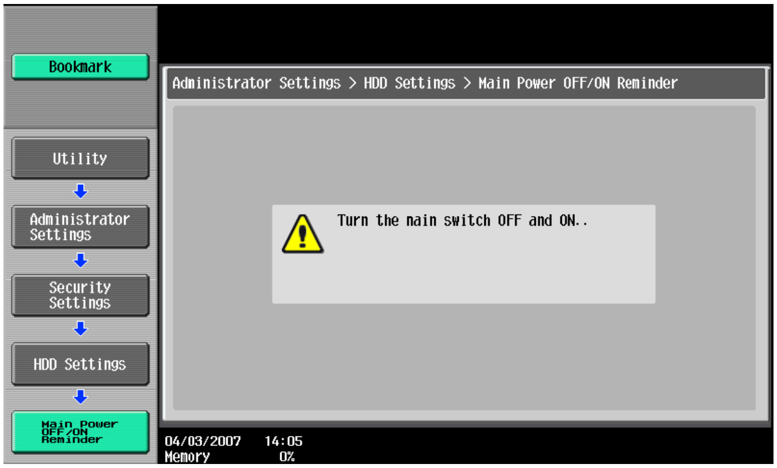
12 Make sure that a message appears prompting you to turn OFF and then ON the main power switch. Now, turn OFF and then turn ON the main power switch.

→ When the main power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. if there is no wait period between turning the main power switch off,

then on again, the machine may not function properly. 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 > Turn off the main power switch > Turn on the main power switch > Turn on the sub power switch



HDD was formatted.
Please turn the main switch OFF and ON.



Administrator Settings > HDD Settings > Main Power OFF/ON Reminder

Turn the main switch OFF and ON..

3 Enabling Overwrite Temporary Data

Overwrite Temporary Data should be enabled if the deletion of any latent image data that might be on the HDD after a print, scan or fax is required.

This feature requires two different settings;

→ Mode 1 (1x pass) or Mode 2 (3x pass)

Setting	Overwrite Method	Standards
Mode 1	Overwrite with 0 x 00	NAVSO P-5239-26 (US Navy) DoD 5220.22-M (Department of Defense)
Mode 2	Overwrite with 0 x 00 Overwrite with Oxff Overwrite with the letter “A” (Dx61) Verify	AFSSI5020 (US Air Force

→ [Encryption Priority] refers to overwriting the data in HDD and the buffered data at the full strength of the Encryption Key. It is recommended that [Encryption Priority] be selected to achieve a greater effect of encryption.

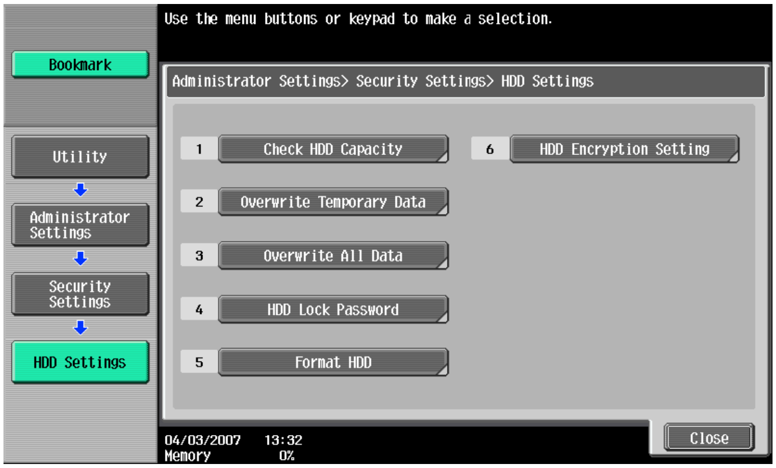
→ [Overwrite Priority] refers to overwriting the data in HDD and the buffered data at the strength of the selected overwrite mode (1 or 2)

→ [Encryption Priority] is the default setting.

→ NOTE: Encryption and Overwrite Priority will only be available when the Security Encryption Kit has been installed and enabled.

1 Enter the Administrator Mode on the MFP display, *Utility/Counter button* > *Administrator Settings* > *Input Admin Password* > *Security Settings* > *HDD Settings.*

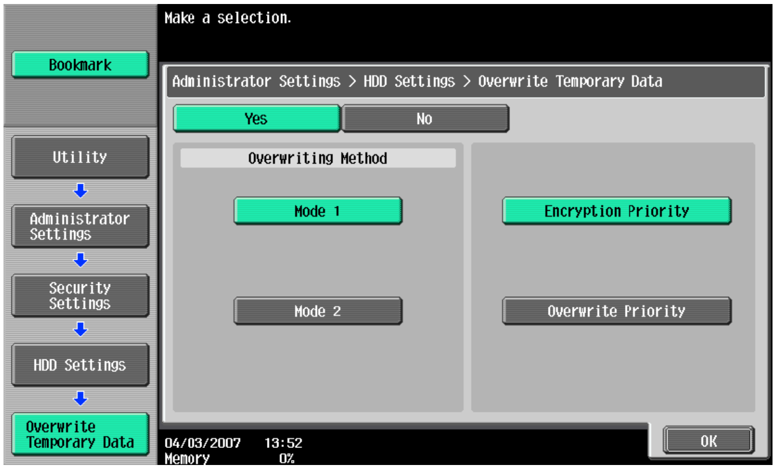
2 Touch [Overwrite Temporary Data].



Use the menu buttons or keypad to make a selection.

Administrator Settings> Security Settings> HDD Settings

3 Touch [Yes], Touch [Mode 1] or [Mode 2], then touch [Encryption Priority] or [Overwrite Priority].



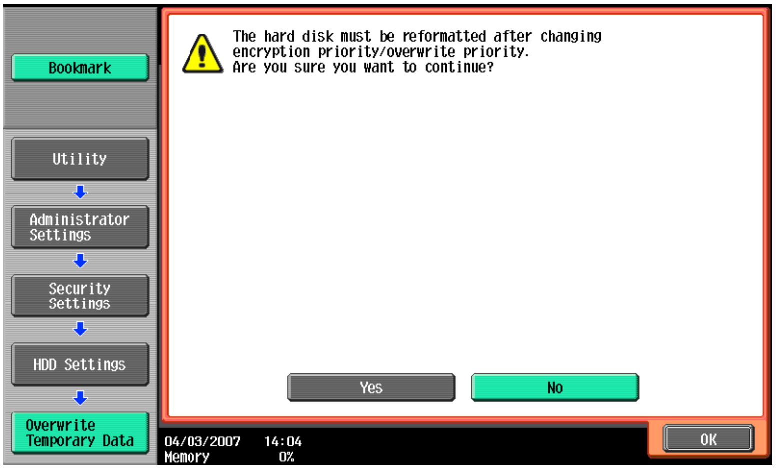
Make a selection.

Administrator Settings > HDD Settings > Overwrite Temporary Data

04/03/2007 13:52
Memory 0%

4 Touch [OK].

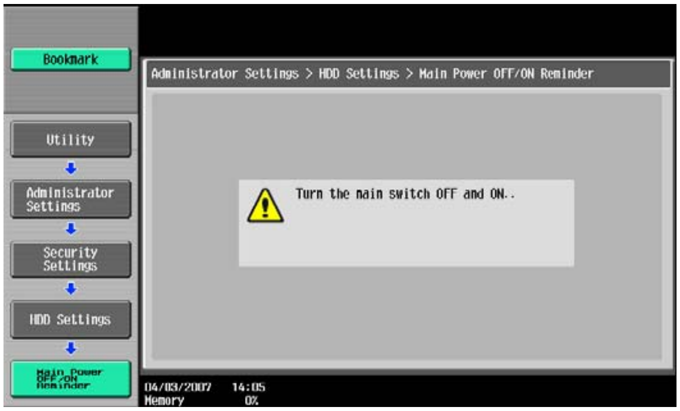
5 A confirmation message appears. Select [Yes] and touch [OK].



The hard disk must be reformatted after changing encryption priority/overwrite priority.
Are you sure you want to continue?

04/03/2007 14:04
Memory 0%

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.



Administrator Settings > HDD Settings > Main Power OFF/ON Reminder

Turn the main switch OFF and ON..

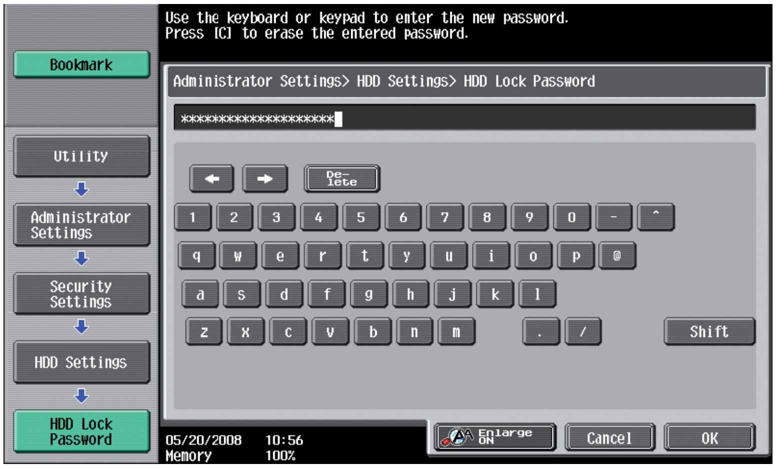
04/03/2007 14:05
Memory 0%

→ 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 > Turn off the main power switch > Turn on the main power switch > Turn on the sub power switch

4 Enabling HDD Lock Password

The HDD Lock Password function is standard in all bizhub MFP’s. When this function is enabled a password is applied to the HDD BIOS and prevents intruder access to the hard disk data.

1. Enter the Administrator Mode on the MFP display, *Utility button > Administrator Settings > Input Admin Password > Security Settings > HDD Settings > HDD Settings*
2. Enter a 20 character password.



Use the keyboard or keypad to enter the new password.
Press [C] to erase the entered password.

Administrator Settings> HDD Settings> HDD Lock Password

****

05/20/2008 10:56
Memory 100%

3. Re-enter the 20 character password.

   → If the password entered does not meet the requirements of the Password Rules, a message appears that tells that the password entered cannot be used. Enter the correct password. For details of the Password Rules, see Appendix C.

   → If there is a mismatch in the password, a message appears that tells that there is a mismatch in the password. Enter the correct password.

4. Turn MFP Off, then On as prompted.

Changing the HDD Lock Password

✓ The HDD Lock Password can be changed or modified at any time by the Administrator using the Edit Button.

✓ The HDD Lock Password can be cancelled or released at any time by the Administrator using the Release Button.

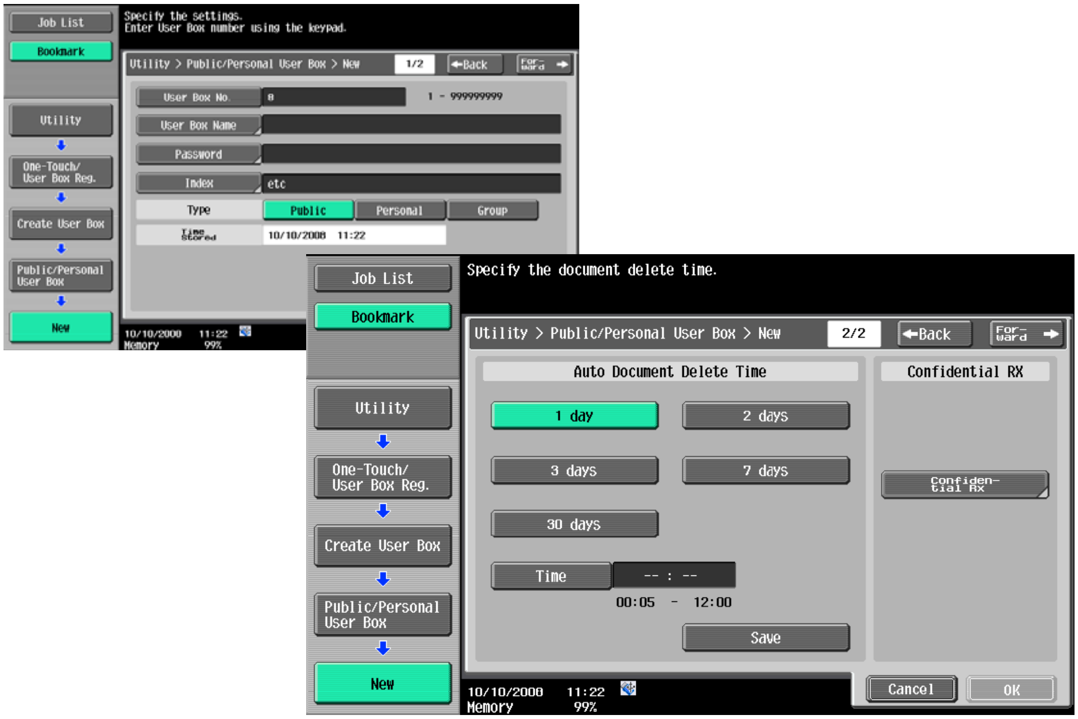
1. Enter the Administrator Mode on the MFP display, *Utility/Counter button > Administrator Settings > Input Admin Password > Security Settings > HDD Settings > HDD Lock Password*
2. Enter the currently registered 20-digit password from the keyboard and keypad.
3. Select Edit to change or modify the 20-digit password.
4. Select Release to cancel or release the 20-digit password.
5. Turn MFP Off, then On as prompted.

5 bizhub MFP Box Data Deletion

bizhub Box functions like User Box, Secure Print, Encrypted PDF and ID & Print allow document data to be saved to the machine's internal hard disk. This data may be stored temporarily for printing or it can be stored for a period of time for use at a later date. All of the bizhub Box functions have the ability to delete or auto delete these stored documents.

User Box Document Deletion Settings

During the creation of a User Box the end user has the ability to set the deletion settings for that User Box. It is highly recommended that he deletion time be set before completing the User Box creation.



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

Utility > Public/Personal User Box > New 1/2

User Box No.: 8 (1 - 999999999)
User Box Name:
Password:
Index: etc
Type: Public
Time Stored: 10/10/2008 11:22

10/10/2008 11:22
Memory 99%

Specify the document delete time.

Utility > Public/Personal User Box > New 2/2

Auto Document Delete Time: 1 day
Time: -- : -- (00:05 - 12:00)

10/10/2008 11:22
Memory 99%

→ Document deletion settings can be made, as seen above, for as little as 5 minutes through 30 days.

→ User Box creation can be completed at the MFP or via PageScope WebConnection remotely.

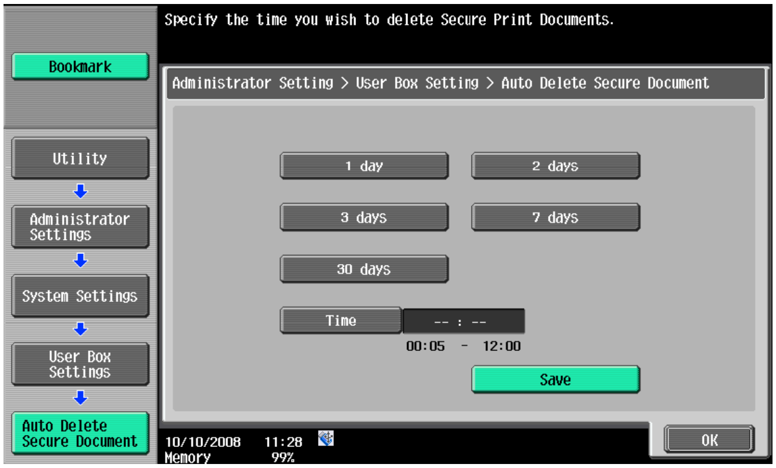
Auto Delete Secure Print Documents

1 Enter the Administrator Mode on the MFP display, *Utility/Counter button > Administrator Settings > Input Admin Password > System Settings > User Box Settings > Auto Delete Secure Documnents.*

2 Specify the period from the date/time when a secure document was saved or last retrieved to the date/time when it is to be deleted automatically.

Reference

- Using the Time button specify 5 minutes to 12 hours (on a 1-minute basis), or select 1 day, 2 days, 3 days, 7 days, or 30 days.



Specify the time you wish to delete Secure Print Documents.

Administrator Setting > User Box Setting > Auto Delete Secure Document

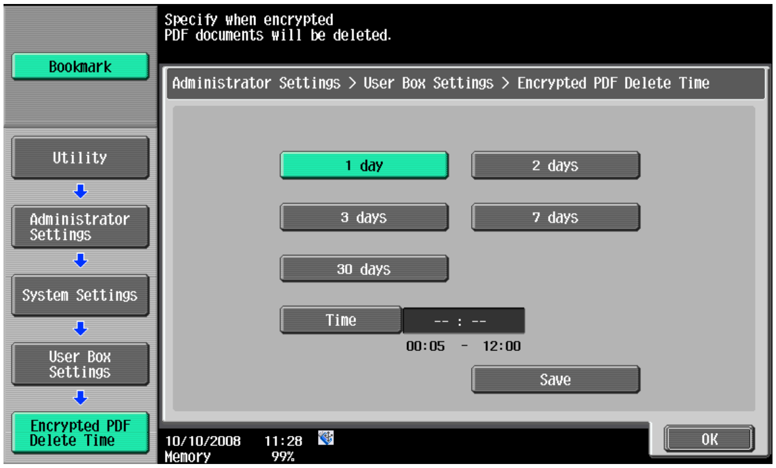
Encrypted PDF Delete Time

1 Enter the Administrator Mode on the MFP display, *Utility/Counter button > Administrator Settings > Input Admin Password > System Settings > User Box Settings > Encrypted PDF Delete Time.*

2 Specify the period from the date/time when a document was saved or last retrieved to the date/time when it is to be deleted automatically.

Reference

- Using the Time button specify 5 minutes to 12 hours (on a 1-minute basis), or select 1 day, 2 days, 3 days, 7 days, or 30 days.



Specify when encrypted PDF documents will be deleted.

Administrator Settings > User Box Settings > Encrypted PDF Delete Time

ID & Print Delete Time

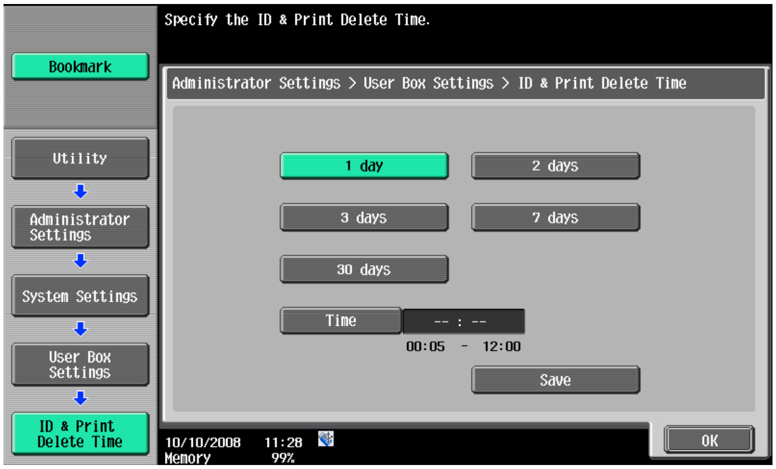
Before an Administrator can set the deletion times for ID & Print the ID & Print function must be enabled on the MFP. If it is not enabled the user will not see the ID & Print Delete Time button in Admin Mode.

1 Enter the Administrator Mode on the MFP display, *Utility/Counter button > Administrator Settings > Input Admin Password > System Settings > User Box Settings > ID & Print Delete Time.*

2 Specify the period from the date/time when a document was saved or last retrieved to the date/time when it is to be deleted automatically.

Reference

- Using the Time button specify 5 minutes to 12 hours (on a 1-minute basis), or select 1 day, 2 days, 3 days, 7 days, or 30 days.



Specify the ID & Print Delete Time.

Administrator Settings > User Box Settings > ID & Print Delete Time

10/10/2008 11:28
Memory 99%

Document Delete Time Setting

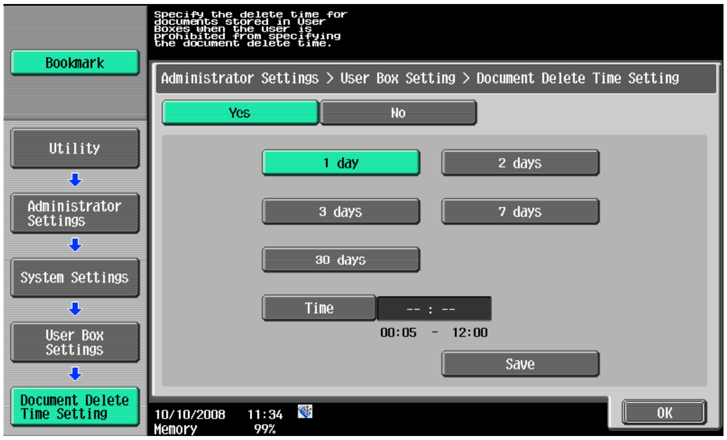
This function enables the administrator to specify the period from the date/time when a document was saved in or retrieved from a User Box to the date/time when it is to be deleted automatically when the user cannot specify the document deletion time. When automatically specifying the document deletion time, select [Yes] and select the deletion time.

1 Enter the Administrator Mode on the MFP display, *Utility/Counter button > Administrator Settings > Input Admin Password > System Settings > User Box Settings > Auto Delete Secure Documnents.*

2 Specify the period from the date/time when a document was saved or last retrieved to the date/time when it is to be deleted automatically.

Reference

- Using the Time button specify 5 minutes to 12 hours (on a 1-minute basis), or select 1 day, 2 days, 3 days, 7 days, or 30 days.



Specify the delete time for documents stored in User Boxes when the user is prohibited from specifying the document delete time.

Administrator Settings > User Box Setting > Document Delete Time Setting

10/10/2008 11:34
Memory 99%

Appendix A Overwrite All Data Function (HDD Sanitization)

At the 'End of Life' or 'End of Lease' where the MFP is to be discarded the Overwrite All Data function overwrites and erases all data stored in all spaces of the HDD. This function also resets all passwords back to factory default settings, preventing any leakage of data.

The HDD Overwrite Methods include the choice of eight different modes, [Mode 1] through [Mode 8] each Mode corresponding with a specific Government Standard.

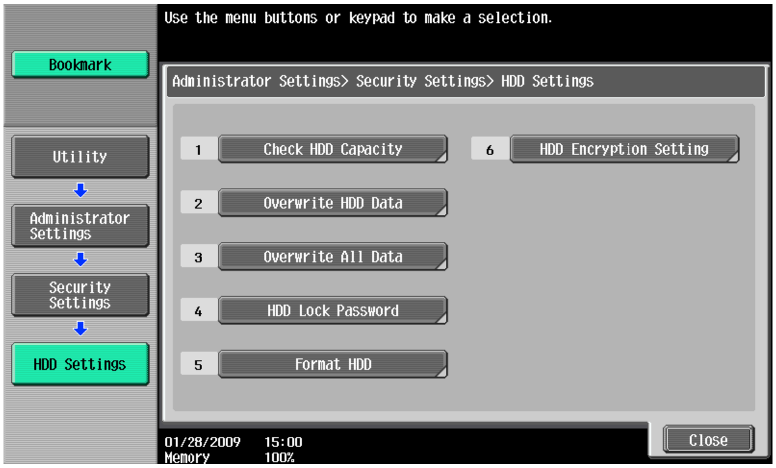
Overwrite All Data takes less than one hour in [Mode 1] at the minimum and approximately 9 hours in [Mode 8] at the maximum.

Mode	Description	
Mode 1	Overwrites once with 0x00.	Japan Electronic & Information Technology Association Russian Standard (GOST)
Mode 2	Overwrites with random numbers random numbers 0x00.	Current National Security Agency (NSA)
Mode 3	Overwrites with 0x00 0xff random numbers verifies.	National Computer Security Center (NCSC-TG-025) US Navy (NAVSO P-5239-26) Department of Defense (DoD 5220.22M)
Mode 4	Overwrites with random numbers 0x00 0xff.	Army Regulations (AR380-19)
Mode 5	Overwrites with 0x00 0xff 0x00 0xff.	Former NSA Standard
Mode 6	Overwrites with 0x00 0xff 0x00 0xff 0x00 0xff random numbers.	NATO Standard
Mode 7	Overwrites with 0x00 0xff 0x00 0xff 0x00 0xff 0xaa.	German Standard (VISTR)
Mode 8	Overwrites with 0x00 0xff 0x00 0xff 0x00 0xff 0xaa verifies.	US Air Force (AFSSI5020)

Setting the Overwrite All Data function

1 Enter the Administrator Mode on the MFP display, *Utility button* > *Administrator Settings* > *Input Admin Password* > *Security Settings* > *HDD Settings* > *HDD Settings*.

2 Touch [Overwrite All Data].

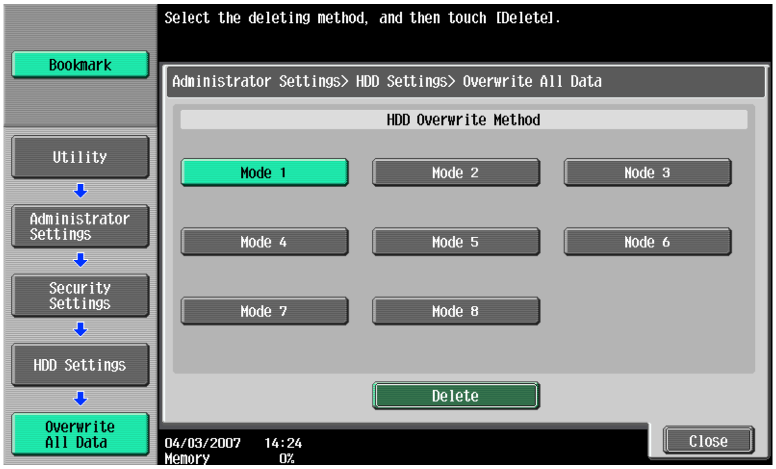


Use the menu buttons or keypad to make a selection.

Administrator Settings> Security Settings> HDD Settings

01/28/2009 15:00
Memory 100%

3 Select the desired mode and touch [Delete].



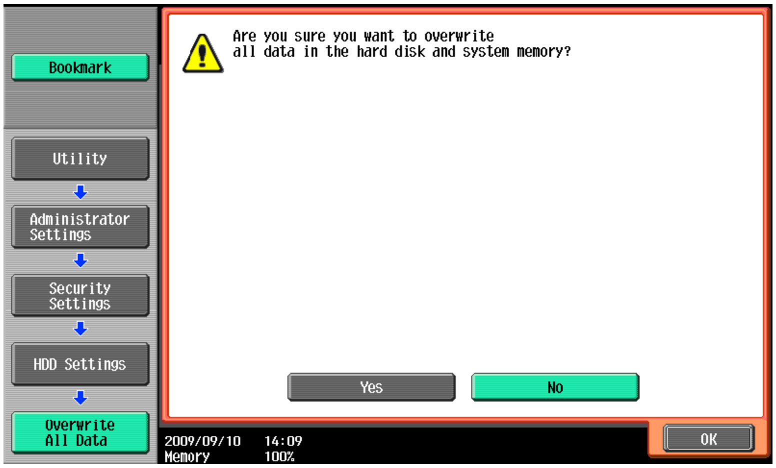
Select the deleting method, and then touch [Delete].

Administrator Settings> HDD Settings> Overwrite All Data

HDD Overwrite Method

04/03/2007 14:24
Memory 0%

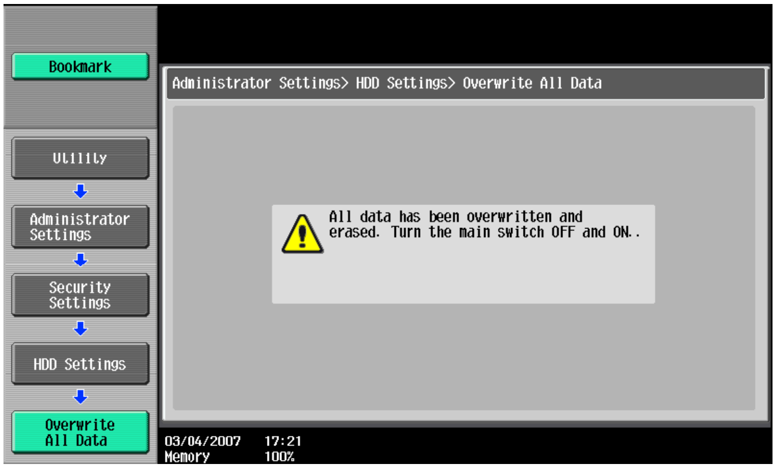
4 A confirmation message appears. Select [Yes] and touch [OK].



Are you sure you want to overwrite
all data in the hard disk and system memory?

2009/09/10 14:09
Memory 100%

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.



All data has been overwritten and erased. Turn the main switch OFF and ON..

→ 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 > Turn off the main power switch > Turn on the main power switch > 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.

Appendix B Utilizing the Konica Minolta HDD Back Up 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 of an MFP. 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 and review the backup data file directly.

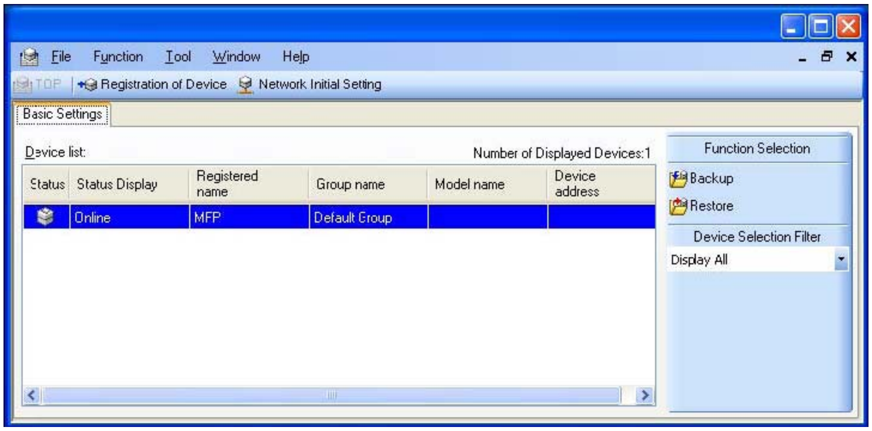
To gain access to the machine from the HDD Backup Utility, the user must be an Administrator with knowledge of the Administrator Password. The Administrator Password entered during the authentication procedure is displayed as "*." When the Enhanced Security mode is set to [ON], the number of times in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

2.1 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].

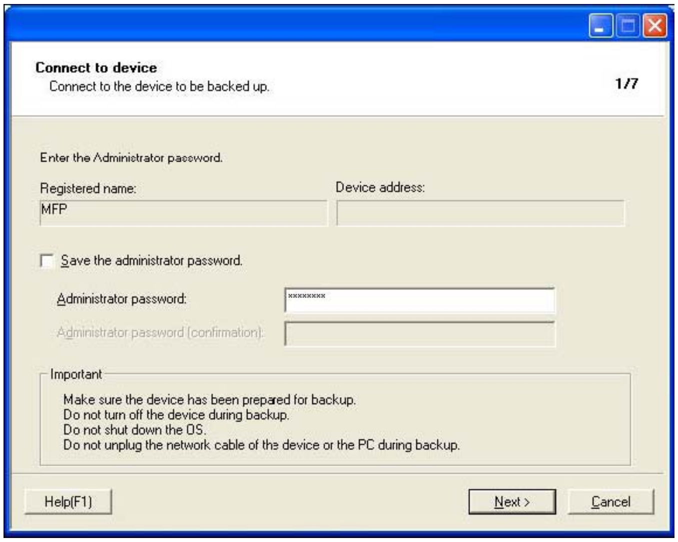


Device list:

Number of Displayed Devices:1

Status	Status Display	Registered name	Group name	Model name	Device address
	Online	MFP	Default Group		

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



Connect to device

Connect to the device to be backed up.

1/7

Enter the Administrator password.

Registered name: MFP

Device address:

☐ Save the administrator password.

Administrator password: ********

Administrator password (confirmation):

Important

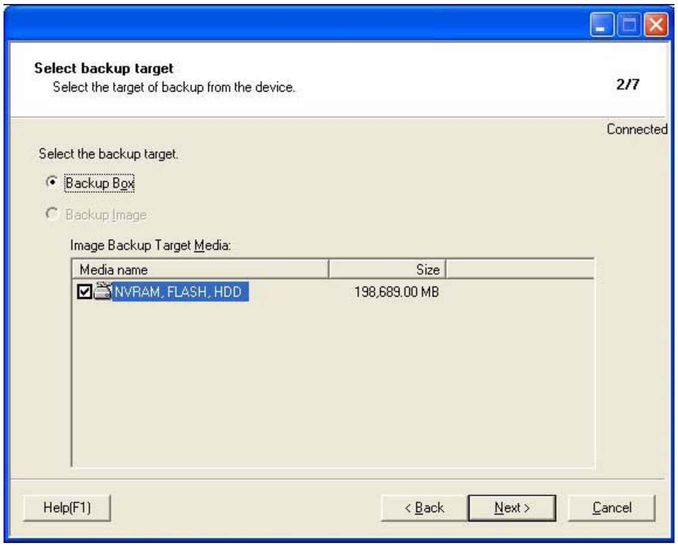
Make sure the device has been prepared for backup.
Do not turn off the device during backup.
Do not shut down the OS.
Do not unplug the network cable of the device or the PC during backup.

→ 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 → Turn off the main power switch → Turn on the main power switch → Turn on the sub power switch.
- → 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

Connected

Select the backup target.

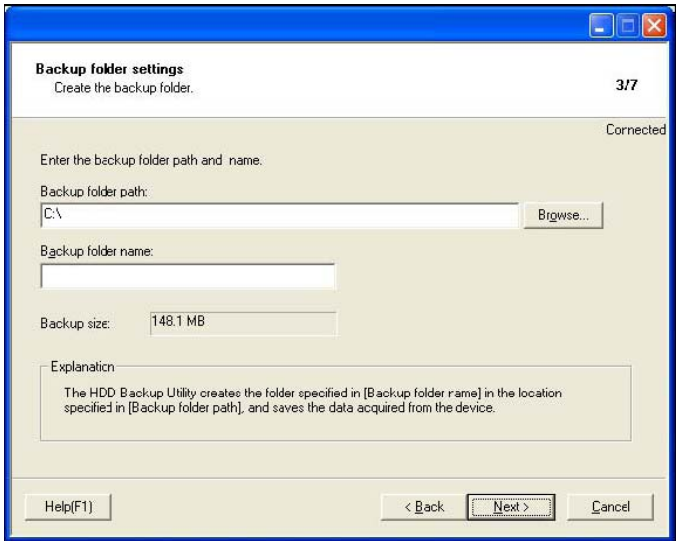
● Backup Box

○ Backup Image

Image Backup Target Media:

Media name	Size
☑ NVRAM, FLASH, HDD	198,689.00 MB

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



Backup folder settings
Create the backup folder.
3/7
Connected

Enter the backup folder path and name.

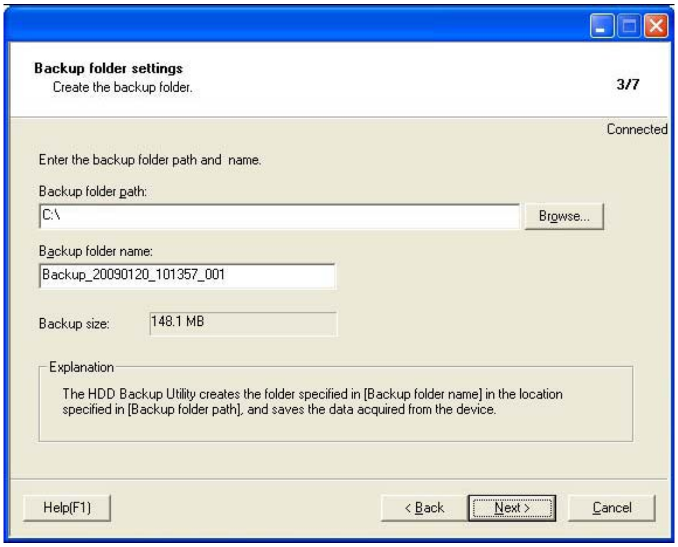
Backup folder path: C:\

Backup folder name:

Backup size: 148.1 MB

Explanation
The HDD Backup Utility creates the folder specified in [Backup folder name] in the location specified in [Backup folder path], and saves the data acquired from 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 settings
Create the backup folder.
3/7
Connected

Enter the backup folder path and name.

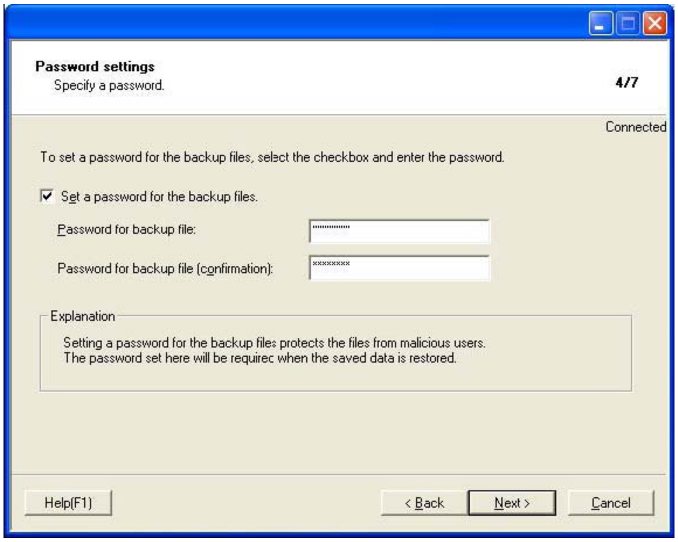
Backup folder path: C:\

Backup folder name: Backup_20090120_101357_001

Backup size: 148.1 MB

Explanation
The HDD Backup Utility creates the folder specified in [Backup folder name] in the location specified in [Backup folder path], and saves the data acquired from the device.

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].


Password settings
Specify a password.
4/7
Connected

To set a password for the backup files, select the checkbox and enter the password.

☑ Set a password for the backup files.

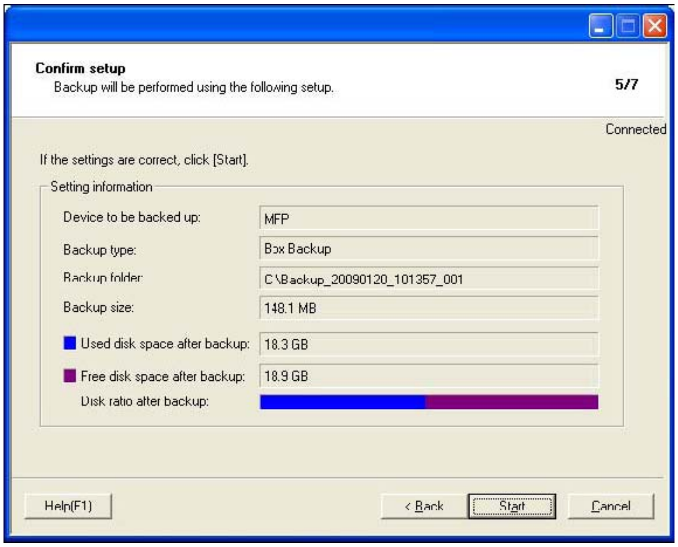
Password for backup file: ***********

Password for backup file (confirmation): ********

Explanation

Setting a password for the backup files protects the files from malicious users.
The password set here will be required when the saved data is restored.

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

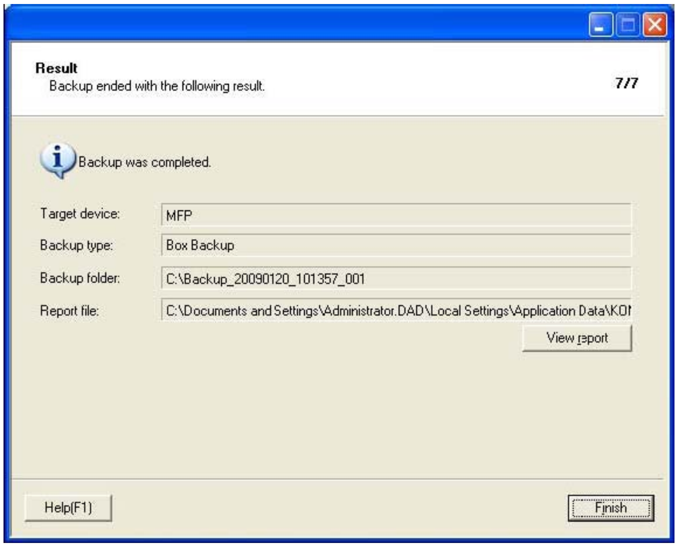

Confirm setup
Backup will be performed using the following setup.
5/7
Connected

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].


Result
Backup ended with the following result.
7/7

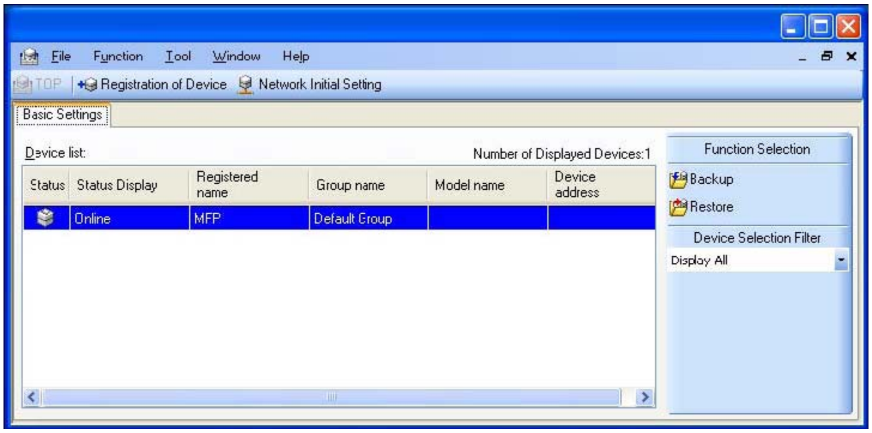
Backup was completed.

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\KOI

2.2 Restoring a Backup HDD File

1 Start the HDD Backup Utility.

2 Select this machine and click [Restore].

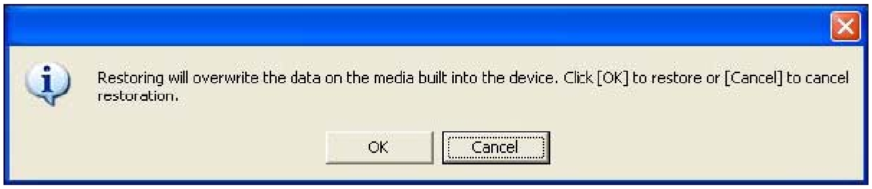


Device list:

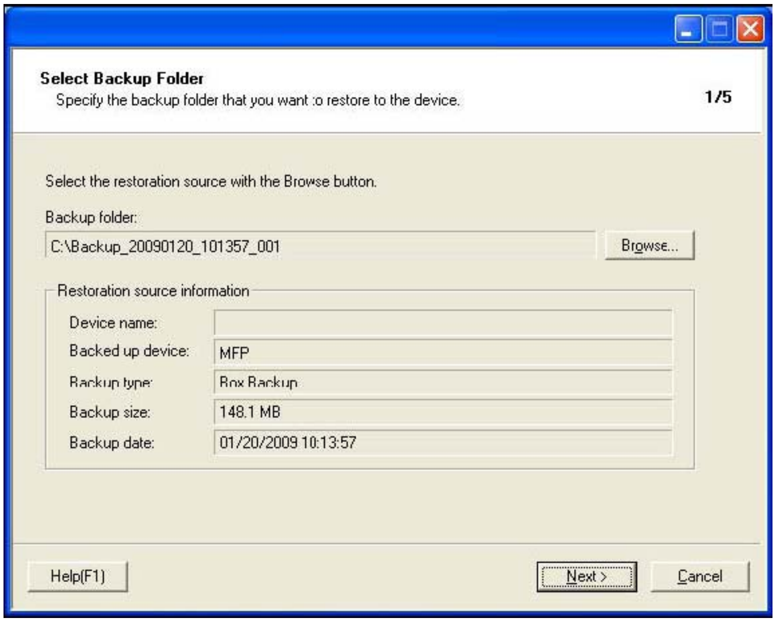
Number of Displayed Devices:1

Status	Status Display	Registered name	Group name	Model name	Device address
	Online	MFP	Default Group		

3 Click [OK].


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

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


Select Backup Folder

Specify the backup folder that you want to restore to the device.

1/5

Select the restoration source with the Browse button.

Backup folder: C:\Backup_20090120_101357_001

Restoration source information

Device name:

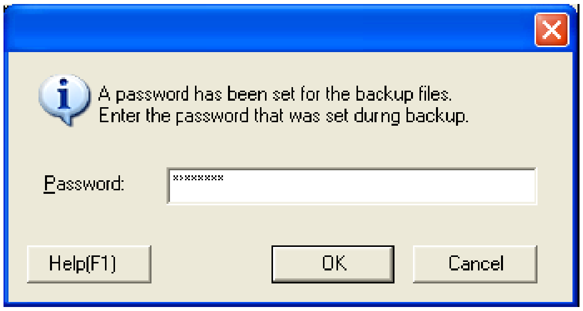
Backed up device: MFP

Backup type: Box Backup

Backup size: 148.1 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].

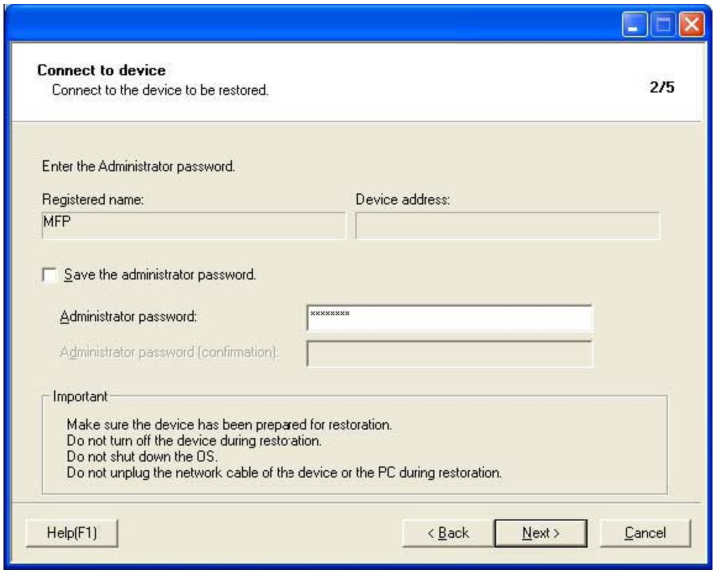


A password has been set for the backup files.
Enter the password that was set durng backup.

Password: ********

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: MFP

Device address:

□ Save the administrator password.

Administrator password: ********

Administrator password (confirmation):

Important
Make sure the device has been prepared for restoration.
Do not turn off the device during restoration.
Do not shut down the OS.
Do not unplug the network cable of the device or the PC during restoration.

→ 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.

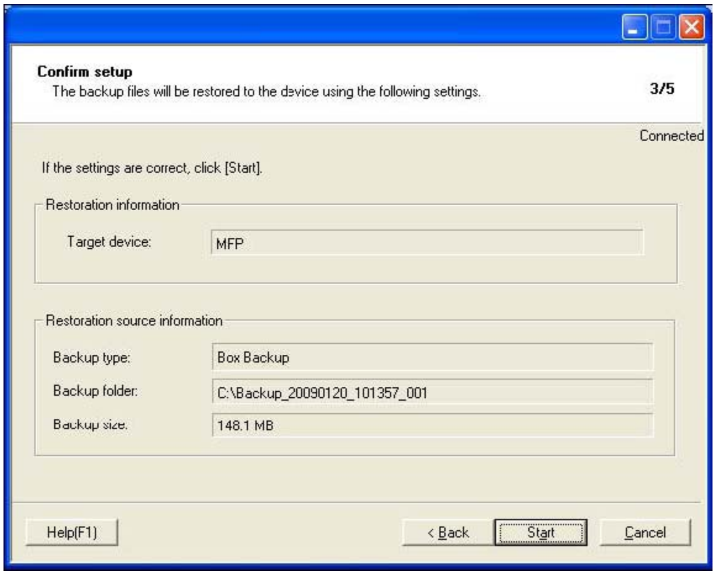
7 Click [Next].

→ 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 → Turn off the main power switch → Turn on the main power switch → Turn on the sub power switch.

→ 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].



Confirm setup
The backup files will be restored to the device using the following settings.
3/5

Connected

If the settings are correct, click [Start].

Restoration information

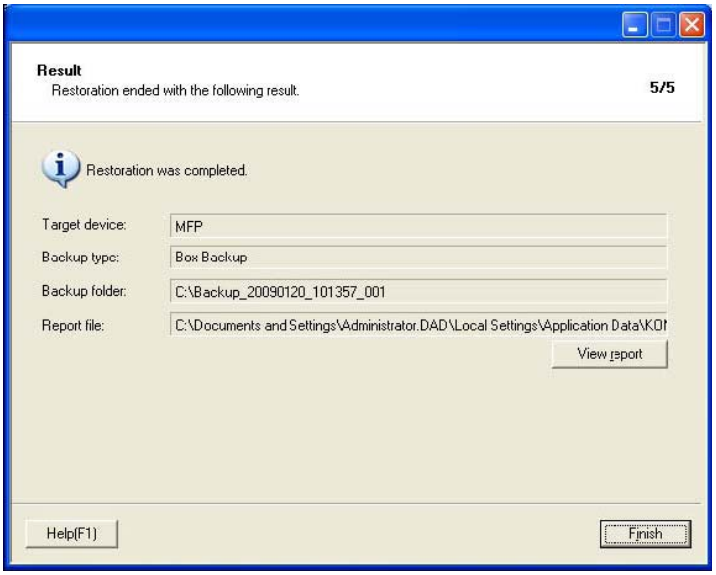
Target device:	MFP

Restoration source information

Backup type:	Box Backup
Backup folder:	C:\Backup_20090120_101357_001
Backup size:	148.1 MB

9 Click [OK].

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



Result
Restoration ended with the following result.
5/5

Restoration 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\KOI

Appendix C Recommended Password Rules

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, Account Password, User Box 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 • Alpha characters: upper and lower case letters • Symbols: !, #, $, %, &, ', (,), *, ,, -, ., /, :, ;, <, =, >, ?, @, [, \,], ^, _, `, {, |, }, ~, + Selectable from among a total of 93 characters
Account Password User Box Password Secure Print Password WebDAV Server 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.

Konica Minolta
Business Solutions U.S.A., INC.
100 Williams Drive
Ramsey, NJ 07446
www.kmbs.konicaminolta.us
www.kmbs.konicaminolta.us/solutions