KONICA MINOLTA

SERVICE MANUAL

SECURITY FUNCTION

bizhub C3851FS/C3851/C3351

This Service Manual (Ver. 1.02) describes
bizhub C3851/bizhub C3351/bizhub C3851FS (Version: G00-11)

2017. 6
Ver. 1.02

KONICA MINOLTA, INC.

CONTENTS

Security function

1. Overview 1
2. Compliance with the ISO15408 standard 1
3. Installation of the machine and steps to be performed before operation 1
3.1 Unpacking and setting up the machine 1
3.1.1 Removing the machine 1
3.1.2 Removing protective tape, packing and other shipping materials 2
3.1.3 Installing the toner cartridge and imaging unit 2
3.1.4 Removing protective materials 2
3.1.5 Setting paper 2
3.1.6 Installing other options 2
3.1.7 Mounting the accessory parts 2
3.1.8 Connecting the power cord 2
3.1.9 Connecting the modular cable (only when the fax kit is mounted as standard equipment) 3
3.1.10 Starting the machine 3
3.1.11 Setting the FAX (only when the fax kit is mounted as standard equipment) . 3
3.1.12 Make the necessary settings 3
3.1.13 Performing Non-Image Area Erase Check 4
3.1.14 Configuring other options 4
3.1.15 Setting up wireless connection kit (only when the wireless connection kit is mounted as standard equipment) 4
3.1.16 Restarting the machine 4
3.1.17 Connecting the network cable 4
3.1.18 Network setting 5
3.1.19 Affixing the labels/panel sheet 5
3.1.20 Checking for parts mounted on the machine 6
3.1.21 Switch setting for secured start 6
3.1.22 Setting for Custom Function Pattern Selection 6
3.1.23 Software Switch Setting 7
4. Precautions for operation control 8
5. Checking the firmware version number 10
5.1 Security authentication firmware version number 10
6. Accessing the Service Mode 10
6.1 Access method to the Service Mode 10
6.2 Access lock of Service Mode 12

6.2.1 Access lock release procedure 12
7. Enhancing the security function 13
7.1 Details of settings 13
7.2 Security enhancing procedure 14
7.2.1 Making and checking the service settings 14
7.2.2 Requests to the administrator 18
7.2.3 Functions disabled by the setting of Enhanced Security Mode 18
7.2.4 Functions whose settings are changed by Enhanced Security Mode 19
8. Service Mode functions 22
8.1 Firmware Version 22
8.1.1 Checking the firmware version number 22
8.2 CE Authentication function 23
8.2.1 Setting the CE Authentication function 23
8.3 Administrator Password function 24
8.3.1 Setting the administrator password 24
8.4 CE Password function 26
8.4.1 Setting the CE password 26
8.5 Initialization function 29
8.5.1 Initialize method 31
8.6 HDD Format 32
8.6.1 HDD format execution procedure 33
8.7 HDD installation setting 34
8.7.1 HDD installation setting procedure 34
8.8 Operation ban release time setting 35
8.8.1 Operation ban release time setting procedure 35
8.9 Administrator Unlocking function 36
8.9.1 Administrator Unlocking function procedure 36
9. Overwrite All Data function 37
9.1 Overwrite All Data procedure 37
9.2 Items to be cleared by Overwrite All Data 37
9.2.1 Items cleared by Overwrite All Data 37
10. Firmware rewriting 39
10.1 Outline 39
10.2 USB memory 39
10.2.1 Preparation 39
10.2.2 Procedure 39
10.2.3 Action when data transfer fails 43
10.2.4 Entering the machine type information 43
11. FAX function (only when the fax kit is mounted as optional equipment) 45

11.1 Installing/setting procedure of the FAX kit.. 45
11.1.1 Install procedure... 45
11.1.2 Connecting the modular cable.. 45
11.1.3 Affixing the labels 45
11.1.4 Configuration procedures 45

1. Overview

This Service Manual contains the essential operating procedures and precautions for using the security functions.

2. Compliance with the ISO15408 standard

This machine has an enhanced security function: Set the Enhanced Security Mode, in Administrator Settings, to [ON].
This machine offers the security functions that comply with the ISO/IEC15408 (level: EAL2) and U.S. Government Approved Protection Profile - U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std 2600.2^{TM}-2009).

3. Installation of the machine and steps to be performed before operation

The service engineer should first perform the following steps before setting the machine for the Enhanced Security Mode.
The ISO15408 evaluation for this machine assumes that the hard disk is installed in the machine. Thus, make sure that the hard disk has been installed.

3.1 Unpacking and setting up the machine

- **Be sure to correctly follow the procedures in order as explained in this Manual. If you do not follow the procedure in order, the image trouble may occur.**
- **If any part requires replacement due to a machine trouble, perform the relevant replacement procedure appropriately.**

3.1.1 Removing the machine

1. Make sure that the machine package has not been previously unpacked.
Pay attention to the following.

- If the PP band on the package has been re-fastened.
- If the PP tape on the package has been peeled off or re-stuck.
- If the plastic bag protrudes from the bottom of the package.

2. Raise and remove the packing carton.
3. Remove the accessory parts and cushions on the machine and open the plastic bag covering the machine.
Check the following information.

- If the Product Name indicated on the package matches the product name printed on the machine cover.
- If the Serial Number indicated on the package matches the serial number of the machine.

4. Assign two or more persons and put their hands at the specified positions to raise the machine from the box, and place the machine on the horizontal and robust place.
Machine mass: (C3851/C3351: approx. 49.2 kg/108-7/16 lb, C3851FS: approx. 53.1 kg/ 117-1/16 lb)

- Be sure to hold the place specified in the User’s Guide or other manuals to transfer the machine.
- Holding other places than the specified in transferring the machine could cause personal injury due to the drop of the machine or other reasons.

3.1.2 Removing protective tape, packing and other shipping materials

1. Remove the protective tape and the protective materials.
2. Slide the scanner lock lever to the unlock side and close the ADF.

3.1.3 Installing the toner cartridge and imaging unit

1. Open the front door.
2. Pull the front lever of a toner cartridge to the left.
3. Hold the handle of the toner cartridge, then pull it out.
4. Hold the toner cartridge with both your hands, then shake it several times.
5. Check that the color of the toner cartridge matches that of the insertion slot in the main body, then push the toner cartridge to the back.
   Never touch the electrical contacts of the toner cartridge or the imaging unit, as an electrostatic discharge may damage the product.
6. For the other toner cartridges, perform the same procedure as step 2 to 5.
7. Remove protective tapes for the toner cartridges of each color to remove protective films. Make sure that the toner cartridges are pushed all the way in.
8. Remove protective films for the imaging units of each color.

3.1.4 Removing protective materials

1. Close the front door.
2. Open the right door.
3. Push up the two levers of the fusing unit cover.
4. Remove the protective materials from the fusing section.
5. Push down the two levers of the fusing unit cover in step 3.
6. Remove the protective materials from the transfer roller unit.
7. Close the right door.
8. Slide out the tray 1 and remove the protective materials from the inside of the tray. Take care not to touch the surface of the paper feed roller. If you touch it by mistake, wipe off any dirt on the roller surface using dry cloth.

3.1.5 Setting paper

1. Slide the paper length guide to the appropriate paper size.
2. Set paper with the printing side upward and slide the paper width guide to the paper size. Make sure that the top level of the paper stack does not exceed the ▼ (MAX) paper level indicator.
3. Slide the tray 1 back in.

3.1.6 Installing other options

See the “Installation procedures” of the installation manual for each option.

3.1.7 Mounting the accessory parts

1. Install the supplied cover A. (Two supplied screws A)
2. Install the supplied cover B. (Two supplied screws B)
3. Attach the supplied cleaning cloth holder and put the supplied cleaning cloth into the holder.

3.1.8 Connecting the power cord

1. Connect the plug of the power cord into the main body.
2. Plug the power cord into the power outlet.

3.1.9 Connecting the modular cable (only when the fax kit is mounted as standard equipment)

1. Connect the supplied modular cable to the LINE port.
   If the user is connected with a key telephone system or a private branch exchange (PBX), do not connect the modular cable to where other than an analog line.

3.1.10 Starting the machine

1. Turn ON the power switch on the left side of the main body.

3.1.11 Setting the FAX (only when the fax kit is mounted as standard equipment)

1. Display the Service Mode screen. See P.10
2. Touch “System 1.”
3. Touch “Marketing Area.”
4. Touch “Fax Target.”
5. Use the “-” or “+” key to select “US.”
6. Touch “END” twice.
7. Touch “FAX.”
8. Touch “Initialization.”
9. Touch “Fax Function Parameter” and “Communication Journal Data.”
10. Touch “Yes.”
11. Touch “Yes.”
12. Touch “END.”
13. Touch “Exit” on the Service Mode screen.
14. Perform the sending and receiving tests between the Machine and either the store which offers the service or the local retailer, to check that it can be operated normally.

Notes when performing dial transfer

After setting the fax target, dialing operations may be selected after the switchboard dial tone is detected. In this case, depending on the switchboard connected to the machine and the type of dial tone received from the switchboard, dialing operations may not be available. If that happens, you may be able to avoid the problem with the following setting.

A. Turn the Dial Tone Detection function OFF

1. Display the Service Mode screen. See P.10
2. Touch “FAX.”
3. Touch “Network.”
4. Touch “Network Setting 2.”
5. Touch “OFF” of Dial Tone Detection.
6. Touch “END.”
7. Touch “Exit” on the Service Mode screen.

3.1.12 Make the necessary settings

- Date & Time Setting/Time Zone Setting ([Service Mode] → [Date & Time Setting/Time Zone Setting screen (To display the Date & Time Setting/Time Zone Setting screen, press Stop → 3 on the control panel)])
- Serial number input ([Service Mode] → [System 1] → [Serial Number])
- Unit change ([Service Mode] → [System 2] → [Unit Change])

3.1.13 Performing Non-Image Area Erase Check

Perform the below at the site where customer uses the machine.

1. Touch these keys in this order: [Service Mode] → [Machine] → [Non-Image Area Erase Check].
2. Open fully the ADF.

- Do NOT place a document on the document glass.
- Clean the document glass if dirty.

3. Press the Start key.
4. Make sure that “Result” is “OK”. If “Result” is “NG1” or “NG2”, review the place and direction of installation, or take measures to block the light source (by covering it, etc.), then perform installation checking again. If a fluorescent light or other bright light sources exist right above the machine, the light source can hinder installation checking and cause operation errors in the Non-Image Area Erase Check.
5. Touch “OK.”

3.1.14 Configuring other options

1. See the “Configuration procedures” of the installation manual for each option.

3.1.15 Setting up wireless connection kit (only when the wireless connection kit is mounted as standard equipment)

1. Display the Service Mode screen. See P.10
2. Touch “Network Settings.”
3. Touch “2nd Network Setting.”
4. Touch “Network Interface Settings.”
5. Select the appropriate option according to the user’s network environment.
6. Touch “Fix.”
7. Turn OFF and ON the power switch.
   When displayed the Service Mode screen, be sure to turn off the power after exiting the Service Mode screen and wait for 10 seconds or more before turning on.
8. Display the Service Mode screen.
9. Touch “System 1.”
10. Touch “Marketing Area.”
11. Touch “Wireless LAN Destination.”
12. Use the “-” or “+” key to select “US” and touch “decision.”

3.1.16 Restarting the machine

1. Turn the power switch on the left side of the main body OFF and ON again after 10 or more seconds have passed.

3.1.17 Connecting the network cable

1. Connect the main body and networking equipment (HUB) using the network cable. The following shows the recommended network cables that correspond to each communication speed.
   - 10BaseT/100BaseTX: Category5
   - 1000BaseT: Category5E, Category6
2. Check LEDs for lighting conditions.
   - LED1: Should light up steadily if the link network connection has been made.
   - LED2: Should blink according to the communications status of the ACT network.

3.1.18 Network setting

Make the TCP/IP address setting for the network. Consult the network administrator for the setting value to be entered and make settings as required.

1. Touch these keys in this order: [Utility] → [Administrator Settings] → [Network Settings] → [TCP/IP Settings] → [IPv4 Settings].
2. Touch “Manual Input” of IP Application Method and make the following settings.
   IP Address: IP address of the controller
   Subnet Mask: Subnet mask of the network, to which the machine is connected
   Default Gateway: IP address of the default gateway
3. Touch “OK.”
4. Touch “OK” after the “TCP/IP Settings” screen is displayed.
5. Select the function to be used as follows: [Forward] → [Detail Settings] → [PING Confirmation], and make the operation check of TCP/IP.

After completing all the steps, take a sample copy in color mode, and confirm the image. If image troubles occur, first turn OFF and ON the Main Power Switch, and then redo the steps from “Date & Time Setting/Time Zone Setting” to “Unit change.”

3.1.19 Affixing the labels/panel sheet

1. Affix the paper size label to the tray 1 according to the size of the paper used.
2. Affix the supplied panel sheet to the surface of the operation panel. The panel sheet is affixed on customer request. The panel sheet must be kept by the customer.

3.1.20 Checking for parts mounted on the machine

1. Check that the part numbers of the MFP board and the eMMC board are as specified below.

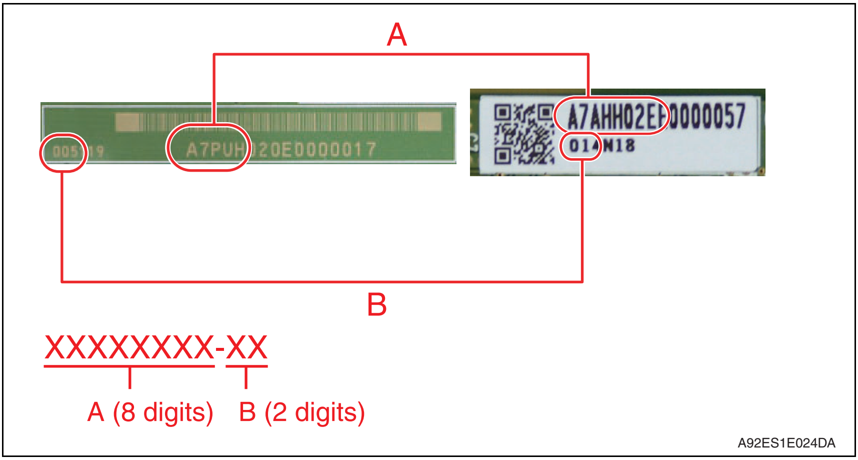
<MFP board>

- A92EH020-02

<eMMC board>

- A92EH02D-00

A part number is a 10-digit number consisting of A (8 digits) and B (2 digits) as in the portions encircled in red below.
However, on the MFP board, a part number is a 10-digit number of A.



3.1.21 Switch setting for secured start

1. Open the rear cover of the machine and place switch 1 of “SW1” on the MFP board in the ON position.

3.1.22 Setting for Custom Function Pattern Selection

1. Copy the Custom Function Pattern Selection setting file exclusively used for the target product where a digital signature is provided, to the route directory of a USB memory.
2. Connect the USB memory to the USB port of the MFP.
3. Call the service mode to the screen.
4. Touch [System 2] → [Custom Pattern].
5. Select [Custom Pattern 1], [Custom Pattern 2], or [Custom Pattern 3].
6. Select [Import] and press the start key to import the data.
7. Select functions as follows: [Administrator Settings] → [System Settings] → [Custom Display Settings] → [Custom Function Pattern Selection] → [Send/Save]. Then, select the registered custom pattern ([ISO15408]).
8. By ensuring that [Polling TX] does not appear in the System box of the Box function, you can confirm that whether the Custom Function Pattern Selection setting file has been installed successfully.

* To delete the registered data, select the target Custom Display Pattern from the [Custom Function Pattern Selection] menu while selecting [Administrator Settings] → [System Settings] → [Custom Display Settings], then touch [Delete] and [Fix]. Check that the result “OK” appears.

3.1.23 Software Switch Setting

NOTE

- **This setting always creates the common name of a device certificate in a form as "DNS Host Name + DNS default domain name".**

1. Call the service mode to the screen.
2. Touch [System 2] → [Software Switch Setting].
3. Change [HEX Assignment] for the switch number 215 to [04].
4. Touch [Fix].
5. Touch [END].

4. Precautions for operation control

A. Requirements of the service engineer

The service engineer should take full responsibility for controlling the machine during his or her procedures for setting up and servicing the machine so that no improper operations are performed.

<To achieve effective security>

- The service engineer who sets up and services the machine should have completed the course in security and be certified accordingly.
- The service engineer should swear that he or she would never disclose information as it relates to the settings of this machine to anybody in accordance with the Installation Checklist contained in User's Guide [Security Operations].
- The service engineer should perform his or her physical service jobs in the presence of the administrator of the machine.

B. Protection of setting data in Service Mode

The CE password used to access Service Mode must be adequately controlled by the service engineer concerned to ensure that it is not leaked. Make sure that any password that could be easily guessed by a third person is not used as the CE password.

<To achieve effective security>
The CE password should:

- Not be one that is easily guessed by third persons.
- Not be known by any third person.
- Be changed at regular intervals.
- Be set again quickly if one has been initialized.

C. Machine maintenance control

When the service engineer performs maintenance service jobs for the machine, he or she should check the firmware version (MFP Card Version), and make sure that the system has not been altered.

The service engineer should take the following precautions when the user is to purchase an additional option.

- For an option that requires that Enhanced Security Mode be turned "OFF" before the option can be used on the machine, notify the user that the mounting of the option makes the machine not guaranteed by the ISO15408 certification.
- Applications subject to the ISO15408 security evaluation and certification are described in User's Guide Security Operations. If any application (including options) not described in the User's Guide is to be used, notify the user that the use of the application is not guaranteed by the ISO15408 certification.

When the Enhanced Security Mode is set to [OFF], make various settings according to the installation checklist and then have the administrator set the Enhanced Security Mode to [ON] again.

D. Miscellaneous

The service engineer should explain to the administrator of the machine that the languages, in which the contents of the User's Guide [Security Operations] have been evaluated, are Japanese and English. He or she should also explain the way how to get the manual in the language, in which it is evaluated.
In addition, the service engineer should promptly provide the version of the User's Guide that has been evaluated for the user whenever the user needs one.

The following lists the manuals compatible with bizhub C3851/bizhub C3351/bizhub C3851FS (Version: G00-11).

- bizhub C3851FS/C3851/C3351 User's Guide Ver. 1.00 A92E-9640BA-00
- bizhub C3851FS/C3851/C3351 User's Guide Security Operations 2017. 6 Ver. 1.02
- bizhub C3851FS/C3851/C3351 SERVICE MANUAL SECURITY FUNCTION 2017. 6 Ver. 1.02
- bizhub C3851FS/C3851/C3351 SERVICE MANUAL Ver. 1.00: 2016/12/01

5. Checking the firmware version number

- Confirm the need to enhance or not to enhance the security function with the administrator of this machine: If administrator wants to enhance, check the firmware version (MFP Card Version).
- If the firmware version number of this machine is different from numbers shown in the list below, it will be necessary to re-write to the firmware version corresponding to security.
  Refer to P.39 for the method of how to re-write the firmware.

5.1 Security authentication firmware version number

	MFP Card Version
bizhub C3851FS/C3851/C3351	A92E0Y0-F000-G00-11

Refer to P.22 for the method of checking the firmware version.

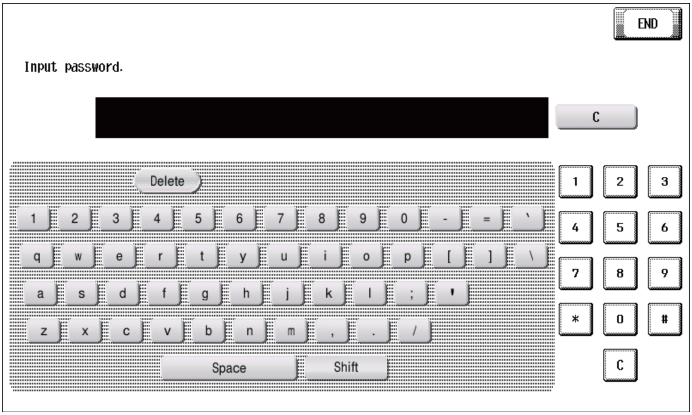
6. Accessing the Service Mode

6.1 Access method to the Service Mode

1. Press Menu.
2. Touch [Counter].
3. Touch [Display Keypad].
4. Press the following keys in this order:
   Stop → 0 → 0 → Stop → 0 → 1
5. Enter the CE password.

NOTE

- **Authentication using the CE password is carried out only if “ON” is set for [CE Authentication] as accessed through [Service Mode] → [Enhanced Security].**



Input password.

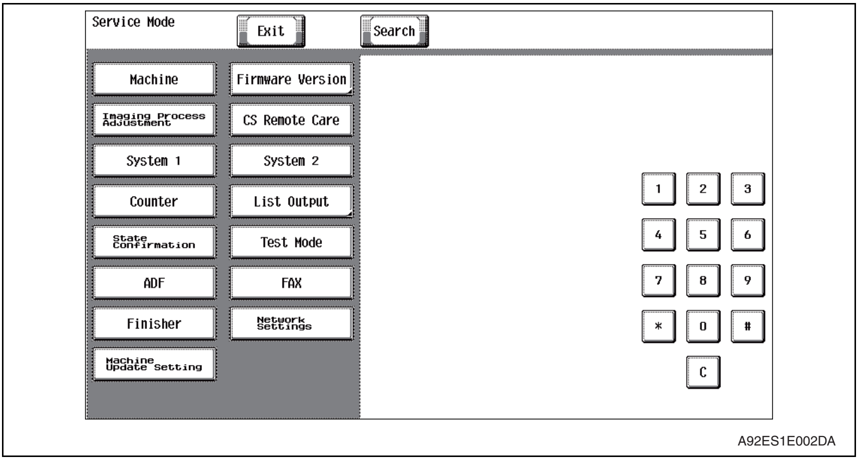
A92ES1E001DA

NOTE

- **The CE password entered is displayed as “∗.”**
- **NEVER forget the CE password. When forgetting the CE password, call responsible person of KONICA MINOLTA (hereafter called KM).**

- **If a wrong CE password has been entered, no further entry can be made for 5 sec. Wait, therefore, for at least 5 sec. before attempting to enter the correct CE password.**
- **Each time a wrong CE password is entered, the CE password illegal access count is incremented by one.**
  When the access to the Service Mode has been successful with the correct CE password entered, the CE password illegal access count is cleared and reset to 0.
- **When "ON" is set for Enhanced Security Mode, access to the Service Mode through the CE password is restricted by the number of times (1 to 3) set for Prohibited Functions When Authentication Error.**
  If the CE password illegal access count exceeds the set number of times, the machine is then set into an access lock state. Then, access to the Service Mode cannot be made until the access lock state is released.
  For the procedure to release the access lock state, see P.12.
- **To go from the CE password screen to another, enter the CE password and call the Service Mode menu to the screen. Then, quit the Service Mode. You can also exit from the CE password screen by turning OFF and ON the power key; however, be careful that any jobs entered will be cleared at this time.**

6. The Service Mode screen will appear.



NOTE

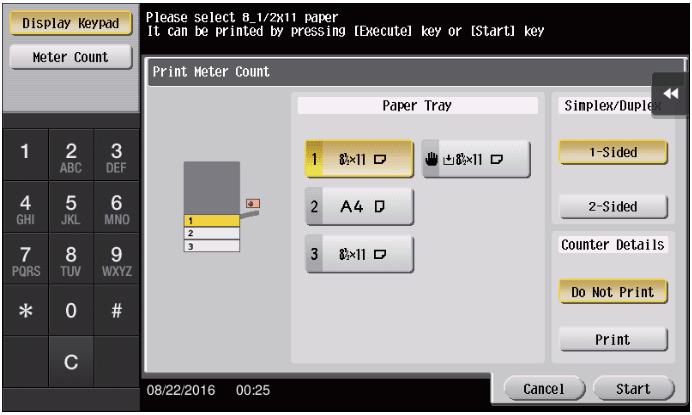
- **If you leave the site with the Service Mode setting screen being displayed, unauthorized changes could occur for any set values. When you finish the setting of Service Mode, or if you have to leave the site by necessity when the Service Mode has been set, be sure to touch [Exit] to the basic screen.**

6.2 Access lock of Service Mode

- Use the following procedure to release the access lock state of the Service Mode. Releasing the access lock state will also clear the illegal access count reached in CE authentication.

6.2.1 Access lock release procedure

1. Turn off the main power switch and turn it on again more than 10 seconds after.
2. Press Menu.
3. Touch [Counter].
4. Touch [Print List].
5. Touch [Display Keypad].



Please select 8_1/2x11 paper
It can be printed by pressing [Execute] key or [Start] key

A92ES1E003DA

6. Press the following keys in this order:
   Stop → 0 → 9 → 3 → 1 → 7
   (Performing this step will start the access lock release timer.)
7. Once started, the access lock release timer measures time intervals.
   The access lock state is released when the period of time set through [Service Mode] → [Enhanced Security] → [Operation Ban release time] elapses.
   See P.35

7. Enhancing the security function

- Perform the Enhanced Security Mode procedures while making checks of installation checklist in User’s Guide [Security Operations].
  For details of how to specify the PostScript password, refer to the separate document “SERVICE MANUAL SECURITY FUNCTION SUPPLEMENT”.
- To make the Enhanced Security Mode, service settings must first be made. Make the necessary service settings and check that they have been correctly made.

7.1 Details of settings

Item	Setting/Check	Default Setting
CE Authentication	Check the setting of [ON]	[ON]
CE Password	Set arbitrarily.	9272927292729272
HDD installation setting	Check the setting of [Installed].	[Installed]
Management Function Choice	Check the setting of [Unset].	[Unset]

NOTE

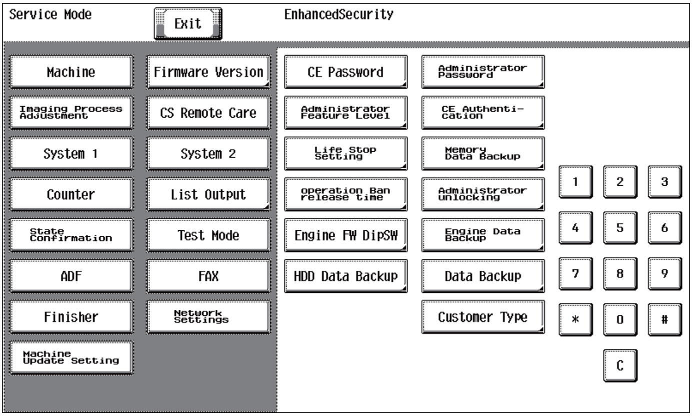
- **If any one of the above functions is not set properly, the machine does not allow the Enhanced Security setting to be made.**
- **The CE password must be set to any value other than the default one.**
- **If fax functions are to be used, check that the fax kit has been mounted and set up properly.**
  The fax kit is standard equipment: See P.3
  The fax kit is not standard equipment: See P.45
- **In addition to setting the Enhanced Security Mode, the service engineer disables the following functions and operates and manages the machine under a condition in which those functions are disabled.**

Item	Setting
IP Address Fax	Using [Service Mode] → [System 2] → [Network Fax Settings], set [IP Address Fax] to [OFF].
Internet Fax	Using [Service Mode] → [System 2] → [Network Fax Settings], set [Internet Fax] to [OFF].

7.2 Security enhancing procedure

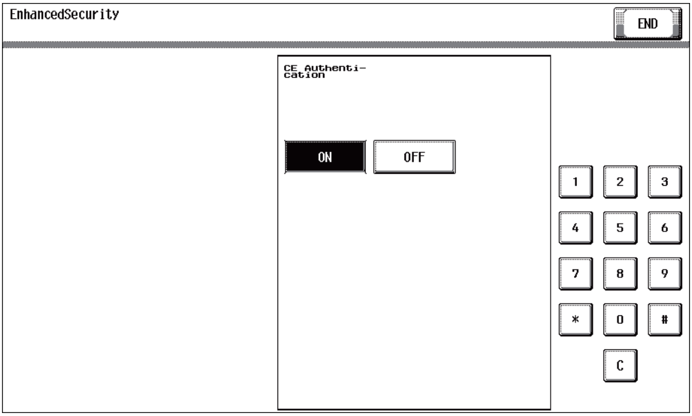
7.2.1 Making and checking the service settings

1. Call the Service Mode to the screen.
   See P.10
2. Press the following keys in this order to display the Enhanced Security screen:
   Stop → 0 → Clear



A92ES1E004DA

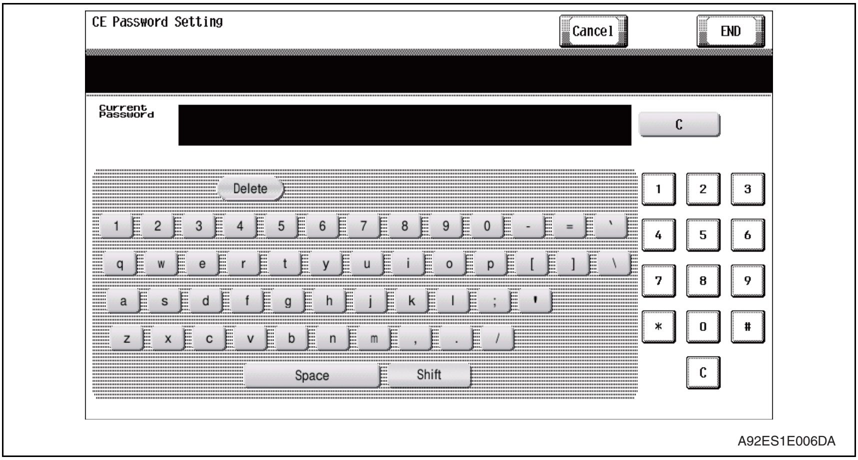
3. Touch [CE Authentication].
4. Check that [ON] is selected.



A92ES1E005DA

5. Touch [END] and [CE Password].

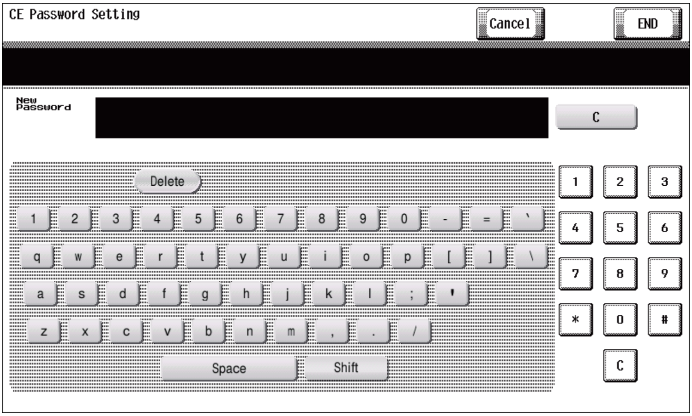
6. The default setting is “9272927292729272.” Using the keyboard shown on the display, enter “9272927292729272” in Current Password and touch [END].



7. From the keyboard shown on the display, enter a new password and touch [END].

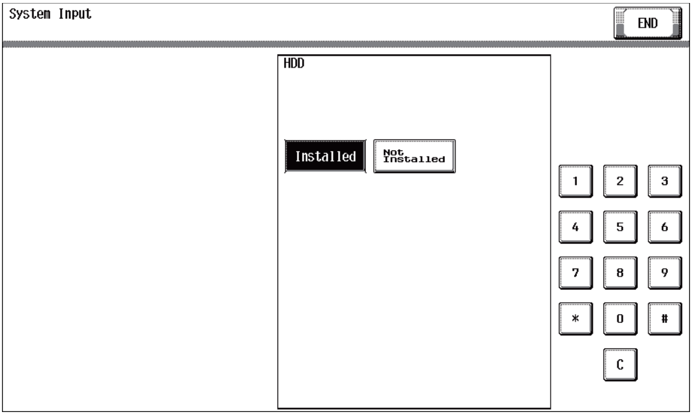
NOTE

- **Be sure to change the CE password.**
- **If the [Password Rules] is set to “ON,” a password consisting of only the same character or the same password as that set before the change cannot be set. In this case, therefore, do not set a password having only the same character or a same password as that set before the change.**
  Also, when the number of password characters is lower than the minimum number of characters (initial value: 12 characters) as set out under [Set Minimum Password Length] in the [Password Rules], a new password will not be able to be set.
- **The CE password should be set at a value which is not the initial value and which is difficult to guess.**
- **The CE password can be set with up to 64 characters.**
- **Exiting from the Service Mode after the new CE password has been set validates the setting of the new password.**
- **NEVER forget the CE password. When forgetting the CE password, call responsible person of KM.**



A92ES1E007DA

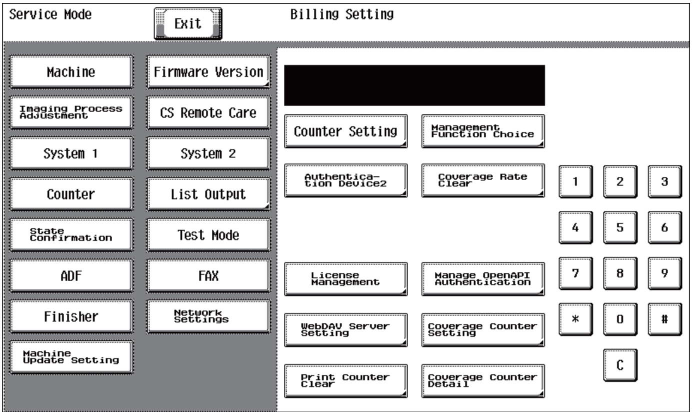
8. Type the new CE password again and touch [END].
9. Touch [System 2].
10. Touch [HDD] and check that [Installed] is selected.



A92ES1E009DA

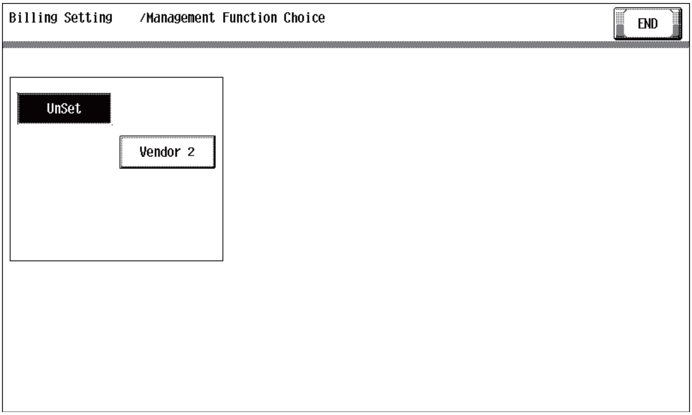
11. Touch [END].
12. Press the Reset key.

13. Press the following keys in this order to display the Billing Setting screen:
    Stop → 9



A92ES1E010DA

14. Touch [Management Function Choice].
15. Check that [UnSet] is selected and then touch [END].



A92ES1E011DA

7.2.2 Requests to the administrator

- When making the Enhance Security setting, the Administrator settings must first be made. The administrator must perform or check the following settings.

Item	Setting/Check	Default Setting
Administrator Password	Check that the password meets the requirements of the Password Rules.	1234567812345678
Encryption Key	Setting of encryption key.	No setting
User Authentication	Check that [Authenticate] (External sever type is “Active Directory” only) is set.	[OFF]
SSL	Check that the registration of the self-certificate is performed to perform SSL communication	No setting
Enhanced Security Mode	Set to [ON].	[OFF]

NOTE

- **Make sure that the Administrator Password has been changed to one that meets the requirements of the Password Rules.**

7.2.3 Functions disabled by the setting of Enhanced Security Mode

- Note that setting Enhanced Security Mode to “ON” disables the following functions.

(1) Terminal Debug (forcibly prohibited when Enhanced Security Mode is set to “ON”)

(2) Print Data Capture (forcibly prohibited when Enhanced Security Mode is set to “ON”)

(3) In CS Remote Care, the following operation is prohibited.
Rewriting instructions of firmware, communication of the account track counter information, the setting renewal of the machine, the function of remote counter management

(4) Firmware upgrading through Internet ISW (Machine Update Setting) (When the Enhanced Security Mode is set to ON, the setting of this function cannot be changed from “OFF.”)

7.2.4 Functions whose settings are changed by Enhanced Security Mode

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

NOTE

- **When attempting to change settings that have been changed in conjunction with the Enhanced Security Mode, the screen to release Enhanced Security Mode may be displayed for some settings. Note that if run, this will release Enhanced Security.**
- **In addition, the indicator of "not be changed" below indicates that the settings cannot be changed while Enhanced Security Mode is maintained "ON".**

Function Name	Default Setting	When Enhanced Security mode is set to [ON]
Password Rules • To apply the password rule to enhance security.	Disable	Enable (not to be changed)
Prohibited Functions When Authentication Error • To set the function for prohibiting Authentication operation in order to prevent the unauthorized access.	Mode 1	Mode 2 (not to be changed): Three times is set. * The number of times can be changed to once, twice, or three times.
Release Time Settings • To set the period of time to be elapsed before the access lock state is released.	5 min.	The setting value should be 5 min. or more (no value less than 5 can be set)
Confidential Document Access Method • To display the status of the Authentication system on the control panel for the Confidential document access.	Mode1	Mode 2 (not to be changed) * In association with Prohibited Functions When Authentication Error, the method is changed from authentication using Secure Document ID and password (Mode 1) to that using the password with the Secure Document first narrowed down by Secure Document ID (Mode 2).
Secure Print User Box Preview	Thumbnail View, Detail View, and Document Details are enabled	Only Detail View is enabled before password authentication (Mode 2)
Public User Access • To permit use by a public user having no user registration if user authentication setting has been made.	Restrict	Restrict (not to be changed)
User Name List • To display the list key for User names on User Authentication screen.	OFF	OFF (not to be changed)
Print without Authentication • To allow or restrict printing which user and account are not specified.	Restrict	Restrict (not to be changed)

Function Name	Default Setting	When Enhanced Security mode is set to [ON]
User Box Administrator Setting • To set whether to allow or restrict the Box Administrator to use the system.	Restrict	Restrict (not to be changed)
SSL/TLS • To set whether to encrypt access by SSL/TLS.	OFF	Administrator mode and User mode (not to be changed)
SSL Encryption Strength • To set the SSL encryption strength for the SSL encryption communication.	AES-256, 3DES-168, RC4-128	AES/3DES (not to be changed to one containing strength lower than AES/3DES)
FTP Server • To set whether to use FTP server or not.	ON	OFF (not to be changed)
Print Data Capture • To set whether to allow or restrict capturing the Print Job Data.	Allow	Restrict (not to be changed)
Network Setting Clear • To clear the network setting through PageScope Web Connection.	Enabled	Restrict
Registering and Changing Address by the user (Address Book and Program)	Allow	Restrict (not to be changed)
Initialize (Network Settings) • To clear the network related settings.	Enabled	Restrict (not to be changed)
Image Log Transfer Settings • Specifies whether to transfer the input or output image data to the server using whenever MFP inputs or outputs image data.	OFF	OFF (not to be changed)
Counter Remote Control • Specify whether to allow acquisition of counter information managed on this machine when a remote diagnosis system is used.	Restrict	Restrict (not to be changed)
CS Remote Care • CS Remote Care enables the machine and the computer at CS Remote Care center to exchange data through telephone/fax line, network or E-mail in order to control the machine.	Usable	Remote device setting disabled

Function Name	Default Setting	When Enhanced Security mode is set to [ON]
Remote Panel Settings (Server Settings/Client Settings) • Perform various settings for remote operation of the main unit operation panel.	OFF	OFF (not to be changed)
Print Simple Auth. (Authentication setting) • Allow printing from the printer driver for authentication only with user names (no password).	Restrict	Restrict (not to be changed)
External Application Connection • Set whether to integrate with OpenAPI external applications.	Yes	No (not to be changed)
Internet ISW Set (Machine Update Setting) • To set firmware upgrading by Internet ISW, and enable or disable various settings.	OFF	OFF (not to be changed)
E-mail RX Print • To print an E-mail attachment, send an E-mail to the E-mail address of this machine.	OFF	OFF (not to be changed)
IWS Settings • Set the operating environment of IWS (Internal Web Server) function.	OFF	OFF (not to be changed)
HDD backup data Settings • Set whether to permit our service representative to back up or restore the hard disk on this machine.	Restrict	Restrict (not be changed)
USB Connection Permission setting • Specify whether to permit a function that requires the USB Port.	Allow	Restrict
Operation Ban release time (CE authentication) • To set the period of time to be elapsed before the access lock state is released in CE password authentication.	5 min.	The setting value should be 5 min. or more (no value less than 5 can be set)
QR Code Display setting • To set whether to display QR code.	OFF	OFF (not to be changed)
Enable NFC • To set whether to use NFC authentication.	OFF	OFF (not to be changed)
URL Home Settings • To set whether to enable the Scan to URL function.	Enable	Disable

8. Service Mode functions

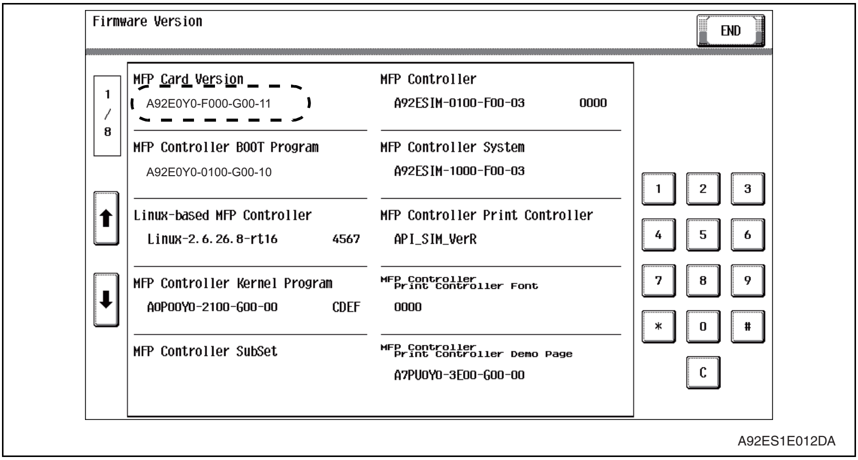
- The Service Mode is used to set various service functions.

8.1 Firmware Version

- This function is used to display the firmware version information of the machine. When the Enhanced Security Mode settings are to be made, this function should be used to check the MFP Card Version against the security authentication version.

8.1.1 Checking the firmware version number

1. Call the Service Mode to the screen.
   See P.10
2. Touch [Firmware Version].
3. Check the MFP Card Version using firmware version number.



Firmware Version

MFP Card Version
A92E0Y0-F000-G00-11

MFP Controller
A92ESIM-0100-F00-03 0000

MFP Controller BOOT Program
A92E0Y0-0100-G00-10

MFP Controller System
A92ESIM-1000-F00-03

Linux-based MFP Controller
Linux-2.6.26.8-rt16 4567

MFP Controller Print Controller
API_SIM_VerR

MFP Controller Kernel Program
A0P00Y0-2100-G00-00 CDEF

MFP Controller Print Controller Font
0000

MFP Controller SubSet

MFP Controller Print Controller Demo Page
A7PU0Y0-3E00-G00-00

A92ES1E012DA

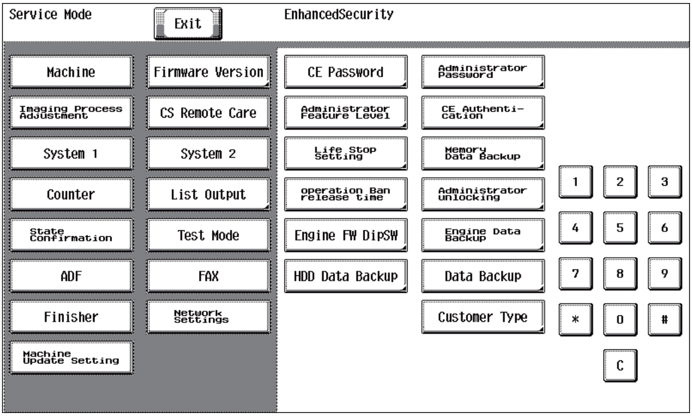
8.2 CE Authentication function

- The service engineer uses a CE password for verifying his or her identity as service engineer, as he or she attempts to use the functions available from the Service Mode. Specific keys must first be entered before carrying out this authentication procedure.

8.2.1 Setting the CE Authentication function

1. Call the Service Mode to the screen.
See P.10

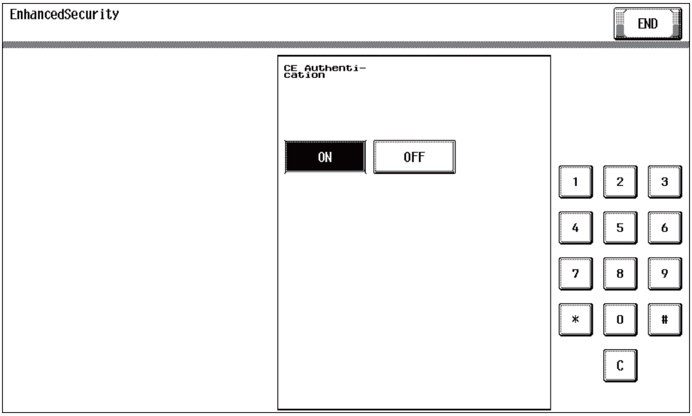
2. Press the following keys in this order to display the Enhanced Security screen:
Stop → 0 → Clear



A92ES1E004DA

3. Touch [CE Authentication].

4. Touch [ON] and [END].



A92ES1E005DA

8.3 Administrator Password function

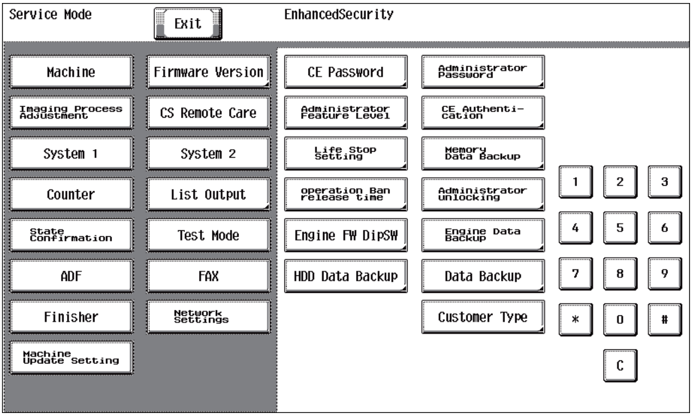
- This function is used when the administrator sets the administrator password. It also allows a new administrator password to be set without requiring the entry of the currently set administrator password. It is therefore used when the administrator forgets the administrator password.

NOTE

- **If the administrator password is temporarily changed by the service engineer, never fail to have the administrator change the administrator password accordingly.**

8.3.1 Setting the administrator password

1. Call the Service Mode to the screen.
   See P.10
2. Press the following keys in this order to display the Enhanced Security screen:
   Stop → 0 → Clear



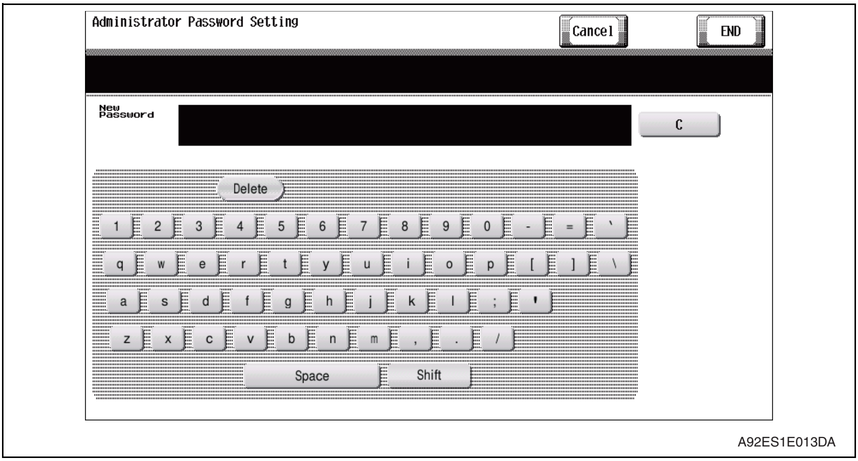
A92ES1E004DA

3. Touch [Administrator Password].

4. Enter the default value “1234567812345678” as the new password from the keyboard on the screen. Then, touch [END].

NOTE

- **Use the default value “1234567812345678” as the password used only temporarily.**



A92ES1E013DA

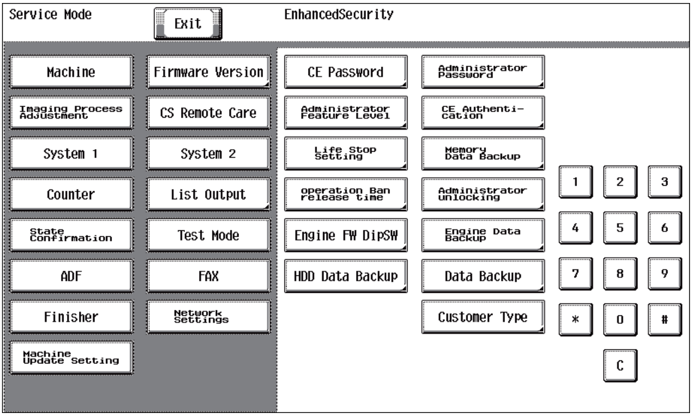
5. Enter the new administrator password (the default value “1234567812345678”) once again and touch [END].
6. Get the administrator of the machine to access the Administrator Settings using the default password. Then, have him or her select the following functions in this order and change the default password: [Administrator Settings] → [Security Settings] → [Administrator Password].

8.4 CE Password function

- The CE password function is used to change the CE password to call the Service Mode to the screen.

8.4.1 Setting the CE password

1. Call the Service Mode to the screen.
   See P.10
2. Press the following keys in this order to display the Enhanced Security screen:
   Stop → 0 → Clear



A92ES1E004DA

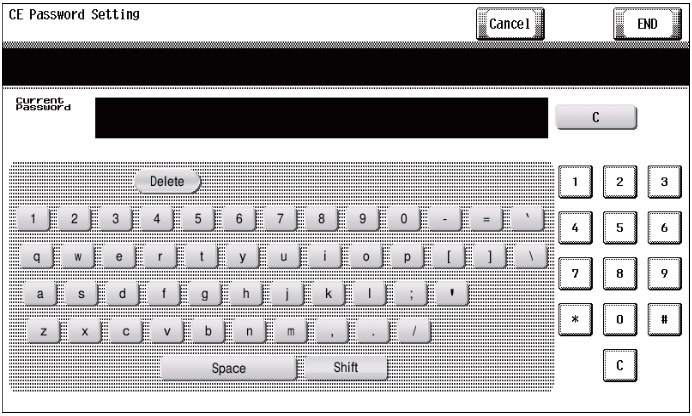
3. Touch [CE Password].
4. Type the currently used CE password from the keyboard shown on the display and touch [END].

NOTE

- **If there is a mismatch in the CE password between that currently set and that just entered, the machine displays a message telling that the CE password entered is wrong. Enter the correct one.**
- **Each time a wrong CE password is entered, the CE password illegal access count is incremented by one.**
  When the access to the Service Mode has been successful with the correct CE password entered, the CE password illegal access count is cleared and reset to 0.

- **When “ON” is set for Enhanced Security Mode, the machine is set into an access lock state if a wrong CE password is entered a predetermined number of times. Then, access to the Service Mode cannot be made until the access lock state is released.**

  For the procedure to release the access lock state, see P.12.



A92ES1E006DA

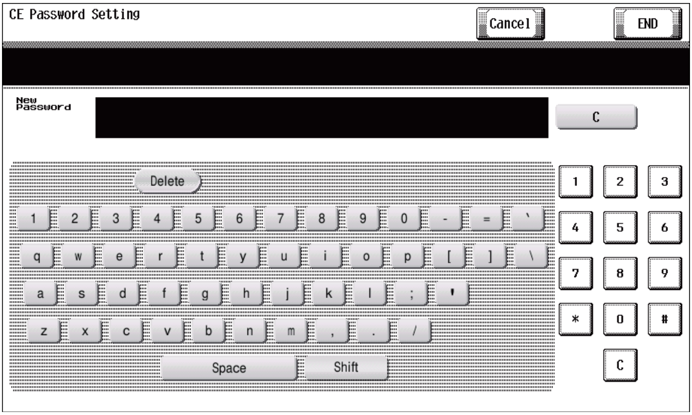
5. Type the password to be newly used from the keyboard shown on the display and touch [END].

NOTE

- **When [Password Rules] is set to "Enable" for [Administrator Settings] → [Security Settings] → [Security Details], the machine does not accept any new password that contains only the same character or that is the same as the previous password.**

  Also, when the number of password characters is lower than the minimum number of characters (initial value: 12 characters) as set out under [Set Minimum Password Length] in the [Password Rules], a new password will not be able to be set.
- **The CE password should be set at a value which is not the initial value and which is difficult to guess.**
- **Quitting the Service Mode after the new password has been set will validate the setting of the new password.**

- **NEVER forget the CE password. When forgetting the CE password, call responsible person of KM.**



A92ES1E007DA

6. Retype the new CE password and touch [END].

NOTE

- **If there is a mismatch in the CE password between that typed first and that just typed, the machine displays a message telling that the CE password entered is wrong. In this case, set the CE password once again.**

Characters and symbols to be used for the CE password
• Numeric characters: 0 to 9 • Alpha characters: upper and lower case letters • Symbols: !, #, $, %, &, ’, (,), *, ,, -, ., /, :, ;, <, =, >, ?, @, [, \,], ^, _, ‘, {, l, }, ~, + • Special character (98 characters) Selectable from among a total of 191 characters

NOTE

- **Depending on the main unit’s marketing area setting and language setting, it may not be possible to set or input special characters from the control panel. However, it is possible to make such settings or inputs through the PC, using the PageScope Web Connection etc. Therefore, please note that if special characters are set as the password using the PC, it would not be possible to input them on the control panel, and they may therefore not be used for the password.**

8.5 Initialization function

- The initialization function resets the current settings for various functions to the default values.
- **Since all subsequent data will be cleared, execute "Data Clear" function with care. Once Data Clear has been executed, be sure to again designate the settings of items whose data has been cleared.**
  (For the functions to be set in Administrator Settings, have the administrator make the settings again.)
- **After resetting the data or having the administrator make the settings again, confirm that the MFP is a properly operation status by referring to the Installation Check List or User's Guide.**

A. Items cleared by Clear All Data function

Item		Details
Service Mode/Administrator Settings	CE password	CE password is reset to "9272927292729272".
	Enhanced Security Mode	Enhanced Security Mode is set to [OFF].
	Administrator password	Administrator password is reset to "1234567812345678".
	Password Rules *1	Password Rules is set to [Disable].
	User Authentication	User Authentication is set to [OFF], Public User is set to [ON], and the following setting is set to "Restrict." • User Name List • Print without Authentication • Print Simple Auth.
	User Box Administrator Setting	User Box Administrator Setting is set to [Restrict].
	HDD Encryption Setting	HDD Encryption Setting function is set to [OFF].
	Overwrite HDD Data	Overwrite HDD Data is set to [OFF].
	Prohibited Functions When Authentication Error	Prohibited Functions When Authentication Error is set to [Mode1].
	Confidential Documents Access Method	Confidential Documents Access Method is set to [Mode1]. (Linked to Prohibited Functions When Authentication Error)
	FTP server function	The following function is permitted. • Print Data Capture • Acquisition of VCM count data
	Release Time Settings	Release Time Settings is set to [5 min.].
	Audit Log Settings	Audit Log Settings is set to [No].
	TCP Socket setting	TCP Socket setting is set to [No].
	Network Setting	The currently set network settings (DNS Server setting, IP Address setting and SMTP Server setting) is cleared and reset to the default setting.
	SSL-compliant protocol settings	Makes the protocol not complying with SSL.
	System Auto Reset	System Auto Reset is set to [1 min.].
	Daylight Saving Time	Daylight Saving Time is set to [No].
	Time Adjustment Setting (NTP)	Time Adjustment Setting is set to [OFF].

Item		Details
Others	SSL certificate (PageScope Web Connection)	Deletes the currently set SSL certificate.
	SSL encryption strength (PageScope Web Connection)	Deletes the SSL certificate to thereby clear the SSL encryption strength.
	Clearing the network setting (PageScope Web Connection)	Network settings are cleared at PageScope Web Connection.
	User registration data	All information on the user registered with the machine is deleted.
	Account track registration data	All information on the account track registered with the machine is deleted.
	Use Box registration data/files	All information on the box registered with the machine and files saved in the box are deleted.
	Secure Print Document ID/ Password/File	All information on Secure Print Document registered with, and files saved in, the machine are deleted.
	One-Touch Registration Data	All is deleted.
	Time/date data	Varies corrected data, if the time-of-day data is corrected due to, for example, the daylight saving time.
	Registering and Changing Address by the user	Change by the user is enabled of destination registration.

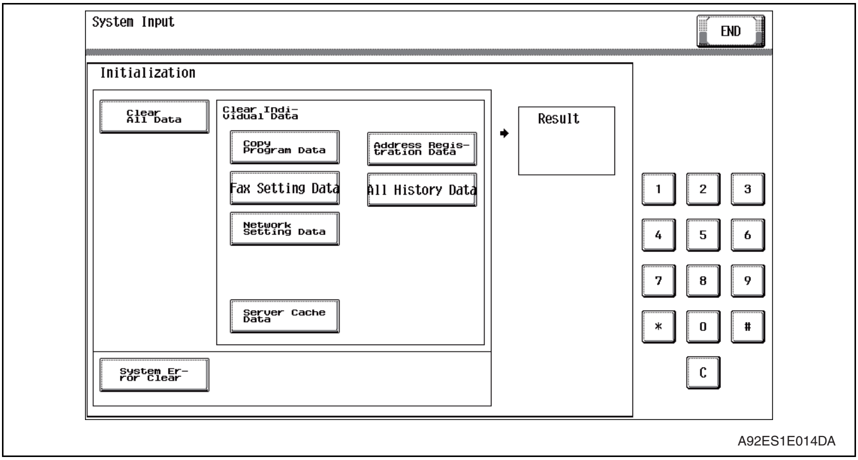
*1: If the Enhanced Security Mode is set to “ON” again after setting the Password Rules OFF, the Password Rules will be set ON with its initial value (minimum of 12 characters).

B. Items cleared by Clear Individual Data (Network Setting Data)

Item		Details
Administrator Settings	FTP server function	The following function is permitted. • Print Data Capture • Acquisition of VCM count data
	Network Setting	The currently set network settings (DNS Server setting, IP Address setting and SMTP Server setting) is cleared and reset to the default setting.
	SSL-compliant protocol settings	Makes the protocol not complying with SSL.
Others	SSL certificate (PageScope Web Connection)	Deletes the currently set SSL certificate.
	SSL encryption strength (PageScope Web Connection)	Deletes the SSL certificate to thereby clear the SSL encryption strength.

8.5.1 Initialize method

1. Call the Service Mode to the screen.
   See P.10
2. Touch [System 1].
3. Touch [Initialization].
4. Select [Clear All Data] or the clear item in [Clear Individual Data] and press the Start key.



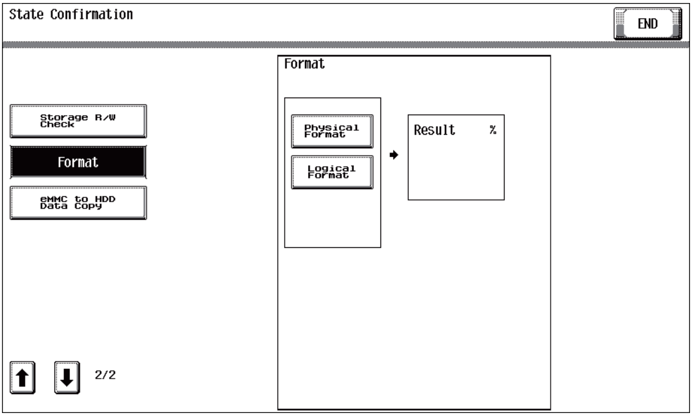
5. When “OK” is displayed, turn off the main power switch and turn it on again more than 10 seconds after.

NOTE
When the Clear All Data function has been executed, be sure to make the following settings again.

- **Since the CE password is reset to the default value, be sure to set once again a CE password that meets the requirements of the Password Rules.**
- **Since the administrator password is reset to the default value, be sure to have the administrator of the machine set once again an administrator password that meets the requirements of the Password Rules.**
- **If you leave the site with the Service Mode setting screen being displayed, unauthorized changes could occur for any set values. When you finish the setting of Service Mode, or if you have to leave the site by necessity when the Service Mode has been set, be sure to touch [Exit] to the main screen.**
- **Since the Enhanced Security Mode is reset to “OFF,” be sure to have the administrator set the Enhanced Security Mode to “ON.”**

8.6 HDD Format

- **Do not perform HDD format carelessly, as performing HDD format clears the following data. Whenever HDD format is executed, be sure to make the settings again for the types of data that have been reset. (For the functions available from Administrator Settings, have the administrator make the settings again.)**
- **After resetting the data or having the administrator make the settings again, confirm that the MFP is a properly operation status by referring to the Installation Check List or User's Guide.**



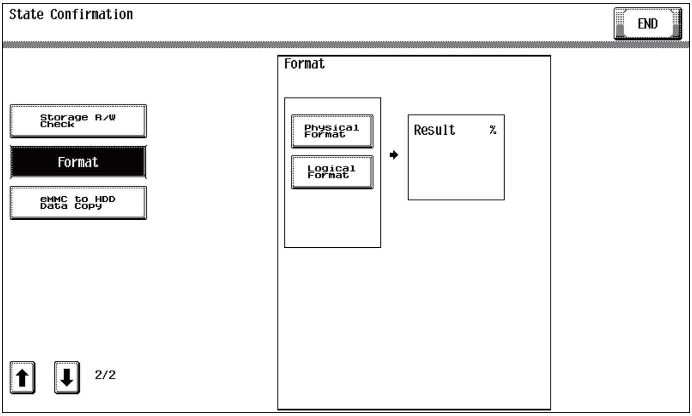
A92ES1E015DA

A. Items cleared by HDD format

Item		Details
Administrator Settings	Enhanced Security Mode	Set to [OFF]
	User Authentication	Set to [OFF]
	Account Track Authentication	Set to [OFF]
	User Name List	Set to [OFF]
	Print Without Authentication	Set to [Restrict]
	Print Simple Auth.	Set to [Restrict]
	User Box Administrator Setting	Set to [Restrict]
	SSL-compliant protocol settings	Makes the protocol not complying with SSL.
Others	User registration data	All information on the user registered with the machine is deleted.
	Account track registration data	Deletes all account track-related data that has been registered.
	Use Box registration data/files	All information on the box registered with the machine and files saved in the box are deleted.
	Secure Print Document ID/ Password/File	All information on Secure Print Document registered with, and files saved in, the machine are deleted.
	Destination recipient data files	All is deleted.
	Audit log	Deletes the audit log.

8.6.1 HDD format execution procedure

1. Call the Service Mode to the screen.
   See P.10
2. Touch [State Confirmation].
3. Touch [Memory/Storage Adjustment].
4. Touch [↓].
5. Touch [Format].
6. Touch [Physical Format] or [Logical Format] and press the Start key.



A92ES1E015DA

7. HDD format is automatically terminated as soon as it is completed.
8. Turn off the main power switch and turn it on again more than 10 seconds after.

8.7 HDD installation setting

- HDD installation setting sets whether the hard disk is installed or not.

- **Changing the HDD installation setting from “Installed” to “Not Installed” will clear the following types of data. Do not do that carelessly.**
  If the HDD installation setting is made again, be sure to make the settings again for those that have been changed. (Have the administrator make the settings again for the setting items of Administrator Settings.)

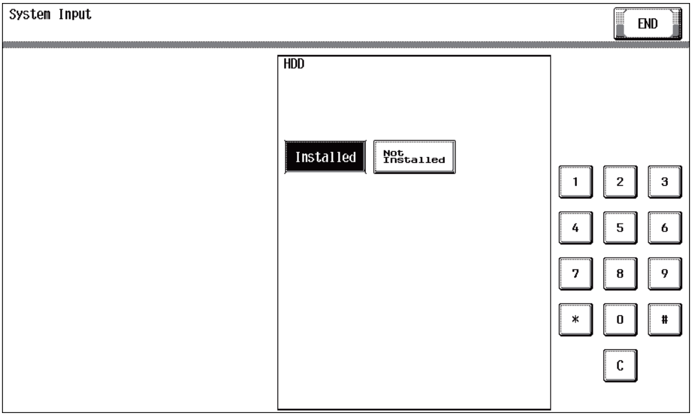
Item		Details
Administrator Settings	Enhanced Security Mode	Enhanced Security Mode is set to [OFF].
	User Authentication	User Authentication is set to [OFF], Public User is set to [ON], and the following setting is set to “Restrict.” • User Name List • Print without Authentication • Print Simple Auth.
Box functions		It is not possible to use.

NOTE

- **If the HDD installation setting is set to “Not Installed”, make sure to informs users that this machine is not guaranteed by the ISO15408 evaluation.**
- **If the HDD installation setting is changed to “Not Installed” and then back to “Installed” again, reusing the original hard disk will allow image files stored in the box or secure print documents to be used. Note, however, that all boxes become Public.**

8.7.1 HDD installation setting procedure

1. Call the Service Mode to the screen.
   See P.10
2. Touch [System 2].
3. Touch [HDD].
4. Touch [Installed] or [Not Installed].



A92ES1E009DA

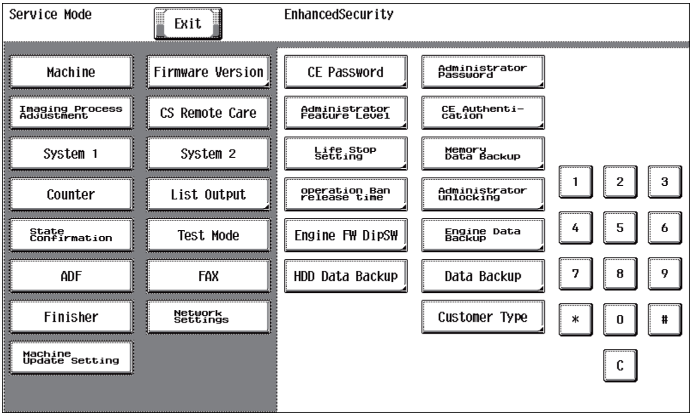
5. Touch [END] and exit the Service Mode.

8.8 Operation ban release time setting

- This function is used to set the period of time to be elapsed before the access lock state is released.
- When the access lock release operation is performed, the machine measures the period of time set with this function and releases the access lock state after the lapse of the set period of time.

8.8.1 Operation ban release time setting procedure

1. Call the Service Mode to the screen.
   See P.10
2. Press the following keys in this order to display the Enhanced Security screen:
   Stop → 0 → Clear

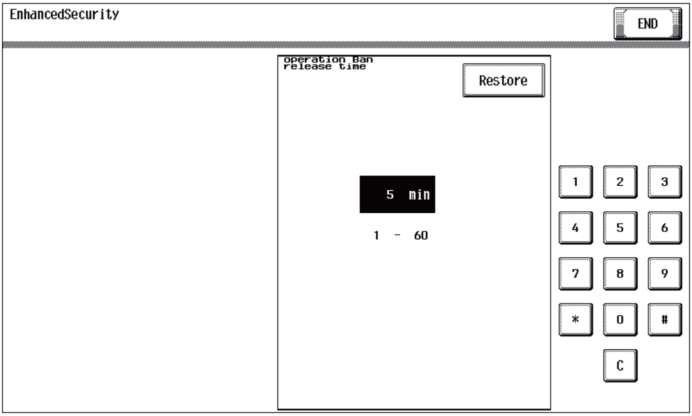


A92ES1E004DA

3. Touch [Operation Ban release time].
4. Enter the time from the 10-key pad and touch [END].

NOTE

- **The setting time ranges from 1 to 60 min. (default value: 5 min.).**
  If the Enhanced Security Mode has been set to "ON," however, the value that can be set should be at least 5 min.



Operation Ban release time
5 min
1 - 60

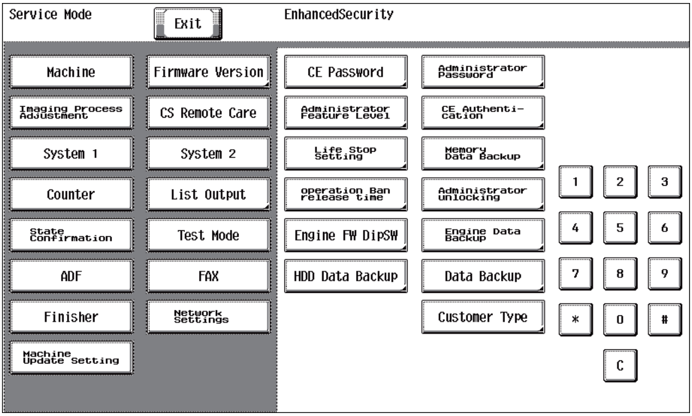
A92ES1E016DA

8.9 Administrator Unlocking function

- When Administrator authentication using the Administrator password is set into an access lock state, this function may be used to release the access lock state.
- The access lock state for the Administrator password authentication can generally be released by turning OFF and ON the main power switch and upon the lapse of the period of time to be elapsed before the access lock state is released. This function, however, overrides these events, allowing the access lock state to be released regardless of these events.

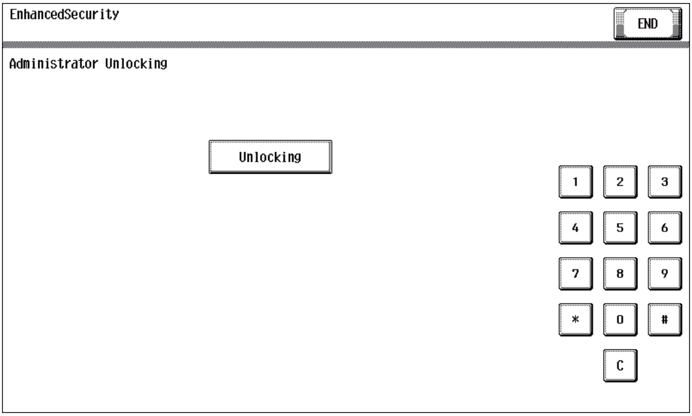
8.9.1 Administrator Unlocking function procedure

1. Call the Service Mode to the screen.
   See P.10
2. Press the following keys in this order to display the Enhanced Security screen:
   Stop → 0 → Clear



A92ES1E004DA

3. Touch [Administrator Unlocking].
4. Touch [Unlocking].



A92ES1E017DA

5. Check that “OK” appears on the screen and then touch [END].

9. Overwrite All Data function

- The Overwrite All Data function overwrites and deletes all data saved in all areas of the HDD and resets all passwords stored in the memory region on the MFP board or the eMMC board to the default settings. It can be used when the machine is to be discarded or use of a leased machine is terminated at the end of the leasing contract, thereby properly blocking leaks of data.

9.1 Overwrite All Data procedure

- The Overwrite All Data function can be set by the following.
  [Administrator Settings] → [Security Settings] → [Storage Management Settings] → [Overwrite All Data]
- For the details of Overwrite All Data procedure, see the User's Guide Security Operations.

9.2 Items to be cleared by Overwrite All Data

- **If the administrator of the machine executes Overwrite All Data by mistake, all items that have been cleared must be set or registered again.**
  (For the items to be set in Administrator Settings, be sure to have the administrator perform the setting and registration procedures again.)

9.2.1 Items cleared by Overwrite All Data

Item		Contents
Administrator Settings	Encryption key	The currently set encryption key is cleared.
	Administrator Password	The currently set password is cleared and reset to the default setting.
	Password Rules *1	Password Rules is set to [Disable].
	Network Settings	The currently set network settings (DNS Server setting, IP Address setting and SMTP Server setting) is cleared and reset to the default setting.
	Daylight Saving Time	Daylight Saving Time is set to [No].
	Time Adjustment Setting (NTP)	Time Adjustment Setting is set to [OFF].
	Password for FW Update (USB)	The current password set for FW Update (USB) is cleared.
Others	SSL certificate (PageScope Web Connection)	Deletes the currently set SSL certificate.
	SSL encryption strength (PageScope Web Connection)	Deletes the SSL certificate to thereby clear the SSL encryption strength.
	SSL-compliant protocol settings	Makes the protocol not complying with SSL.
	User registration data	All information on the user registered with the machine is deleted.
	Account track registration data	Deletes all account track-related data that has been registered.
	Use Box registration data/files	All information on the box registered with the machine and files saved in the box are deleted.
	Secure Print Document ID/ Password/File	All information on Secure Print Document registered with, and files saved in, the machine are deleted.
	ID & print files	All ID & print files are deleted.

Item		Contents
Others	Image Data File	The following data is deleted: • Image files other than secure print documents, ID & print files and user box files • Data files left in the HDD data space, used as image files and not deleted through the general deletion operation • Temporary data files generated during print image file processing
	Destination data files	All destination data is deleted, including e-mail addresses and telephone numbers.
	Time/date data	Varies corrected data, if the time-of-day data is corrected due to, for example, the daylight saving time.
	Memory data backup area *	Clears all data that has been backed up.

*1: If the Enhanced Security Mode is set to "ON" again after setting the Password Rules OFF, the Password Rules will be set ON with its initial value (minimum of 12 characters).

* Memory data backup area

- The data saved in the memory region on the MFP board is stored in the backup area at regular intervals or through manual processing.
- The data saved in the memory region on the MFP board is subjected to an abnormality check through comparison made against the backed up data when the main power switch is turned on or upon updating of data.

10. Firmware rewriting

10.1 Outline

- There are two ways to update the firmware: One is by directly connecting with the main body using the USB memory device, and the other is by downloading over a network using the Internet ISW (Machine Update Setting).

10.2 USB memory

NOTE

- **USB memory must be connected with the main power switch off.**

10.2.1 Preparation

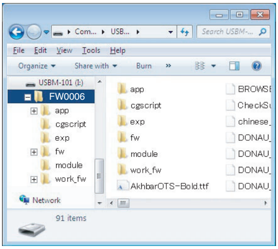
- Conditions for USB memory which can be used for updating the firmware are as follows:
  - USB flash memory compatible with the USB (1.1/2.0/3.0) interface.
    The speed is limited to USB2.0 specifications even if using a device that supports USB3.0.
  - The USB memory is formatted in FAT32 format.
  - No security functions such as encryption and password lock have been added (or the USB memory allows its security functions to be turned OFF).
  - We recommend that you use a memory device with no more than 32 GB of capacity.
  - USB flash memory that appears as multiple drives on a computer cannot be used.

10.2.2 Procedure

- A digital signature is provided to the firmware.
  Confirm the digital signature as follows.
  Right click the acquired exe file to display the property screen.
  Select [Digital Signatures] → [Details] → [General], check that Konica Minolta, Inc. is displayed in Name of the signer field; and select [View Certificate] → [General], check that the signing time is within the validated date of the certificate.

1. Uncompress the firmware file.

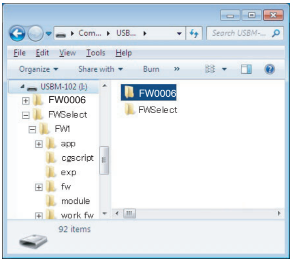
2. Connect the USB to the PC, and copy the extracted data [FW0006] to the root directory of the USB memory.



A92ES1C018DA

NOTE

- **More than one firmware data with a single model or multiple models can be stored in the USB memory.**
  In this case, copy the firmware data to the USB memory according to the following procedures.
  1. **Make the folder named "FWSelect" (case-sensitive) to the root directory of the USB memory.**
  2. **Make a folder with any folder name (one byte alphameric characters, maximum 40 characters) under "FWSelect" folder, and store the firmware data to the folder.**



USBM-102 (I:)
FW0006
FWSelect
FW1
app
cgscript
exp
fw
module
work fw

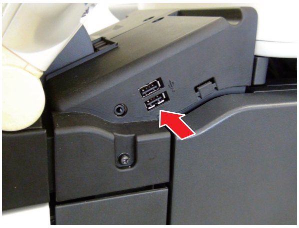
92 items

FW0006
FWSelect

A92ES1C019DA

3. Turn OFF the main power switch.

4. Connect the USB memory containing the firmware into the USB port on the right side of the operation panel.



A92ES1C020DA

NOTE

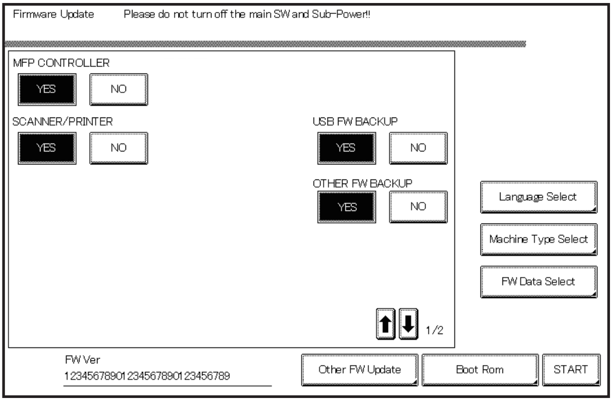
- **USB memory must be connected with the main power switch off.**

5. Turn ON the main power switch while pressing the Stop key.

NOTE

- **When [Administrator Settings] → [Security Settings] → [USB Connection Permission setting] → [External Memory (Service)] → [FW Update] is set to "Restrict", a message "It is limited by the administrator." will appear, and update of the firmware cannot be executed.**
- **When [Administrator Settings] → [Security Settings] → [FW Update (USB) Perm. Sett.] is set to "Password Priority", it requires to input a password after confirming with the administrator.**

6. Control panel shows F/W items to be updated, and select the particular type of F/W to be updated. (Select [YES].)



Firmware Update Please do not turn off the main SW and Sub-Power!!

MFP CONTROLLER
[✓ YES] NO

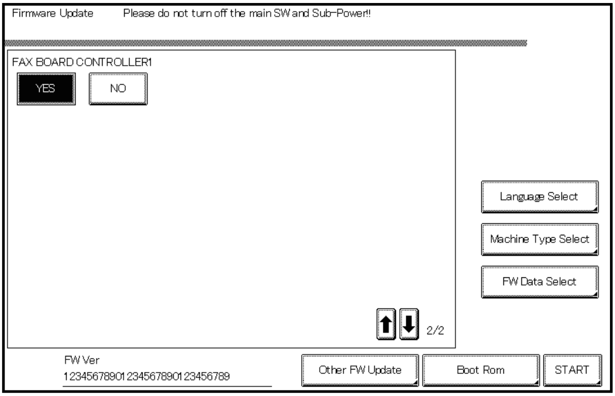
SCANNER/PRINTER
[✓ YES] NO

USB FW BACKUP
[✓ YES] NO

OTHER FW BACKUP
[✓ YES] NO

FW Ver
12345678901 2345678901 23456789

A92ES1C021DA



Firmware Update Please do not turn off the main SW and Sub-Power!!

FAX BOARD CONTROLLER1
[✓ YES] NO

FW Ver
12345678901 2345678901 23456789

A92ES1C025DA

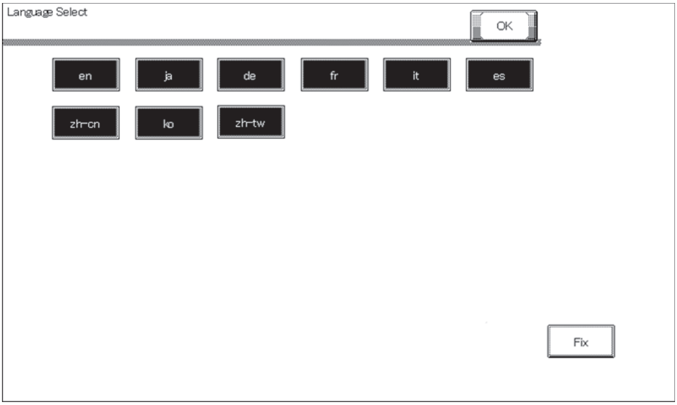
F/W to be updated	Appropriate board	Remark
MFP CONTROLLER	eMMC board (eMMC)	-
SCANNER/PRINTER	MFP board (MFPB)	-
FAX BOARD CONTROLLER1	FAX board (FAXB)	FK-517 is mounted

NOTE

- **Unless one of the keys on the control panel is touched, firmware is automatically updated after 30 seconds when the main power switch is turned on.**
- **When the BootRom file is in the firmware data, [BootRom] key is displayed. Touching the key updates data.**
- **If either or both of the SCB file and power sub CPU file are contained within the firmware data, the [Other FW Update] key displays. Press the key to update.**

- **When more than one firmware are stored in step 1, touching [FW Data Select] enables selection. (Data of other models cannot be selected.)**
  At this time, the data marked with an asterisk on the upper-left side of the data selection screen is the firmware data in the "FW0006" folder in the USB memory device.

7. Touch the [Language Select].
8. On the Language Select screen, select a language to be displayed on the LCD area of the control panel, then touch [Fix].



A92ES1C022DA

NOTE

- **The language selected on this screen is displayed on the Language Selection screen of Utility.**
- **Up to 9 languages are selectable. However, Japanese and English are essential options.**

9. Touch [OK] to go back to the firmware update selection screen.
10. Touch [START]. (At this time, the Start key starts blinking red.)
11. Check that the control panel shows the message indicating that the data has been rewritten correctly ([Downloading Completed]). (The Start key lights blue.)
12. Turn OFF the main power switch.
13. Remove the USB memory device.
14. Turn ON the main power switch.
15. Call the Service Mode to the screen.
16. Select [Firmware Version].
17. Make sure if the version of firmware is updated.

10.2.3 Action when data transfer fails

- If “NG” appears on the control panel, indicating that rewriting has been unsuccessful (in which case the Start key lights up red), take the following steps.

1. Perform the data rewriting procedure again.
2. If the procedure is abnormally terminated, change the USB memory for a new one and try another rewriting sequence.
3. If the procedure is still abnormally terminated, change the board that has caused “NG” and carry out data rewriting procedure.

F/W to be updated	Appropriate board	Remark
MFP CONTROLLER	eMMC board (eMMC)	-
SCANNER/PRINTER	MFP board (MFPB)	-
FAX BOARD CONTROLLER1	FAX board (FAXB)	FK-517 is mounted

10.2.4 Entering the machine type information

- When MFP board is replaced, it is necessary to enter the machine type information.
- Refer to the following procedures to enter the machine type information.

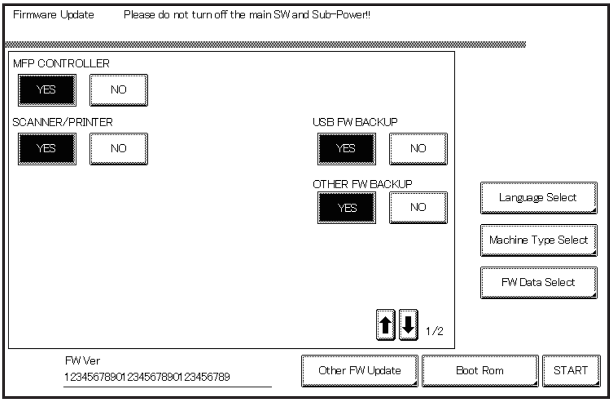
A. Procedure

1. Insert the USB memory to the USB port.
2. Turn ON the main power switch while pressing the Stop key.

NOTE

- **When [Administrator Settings] → [Security Settings] → [USB Connection Permission setting] → [External Memory (Service)] → [FW Update] is set to “Restrict”, a message “It is limited by the administrator.” will appear, and update of the firmware cannot be executed.**
- **When [Administrator Settings] → [Security Settings] → [FW Update (USB) Perm. Sett.] is set to “Password Priority”, it requires to input a password after confirming with the administrator.**

3. Touch [Machine Type Select].



Firmware Update Please do not turn off the main SW and Sub-Power!!

MFP CONTROLLER: YES

SCANNER/PRINTER: YES

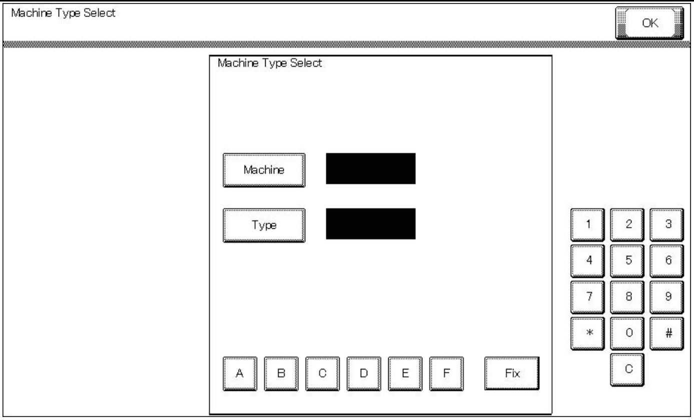
USB FW BACKUP: YES

OTHER FW BACKUP: YES

FW Ver 1234567890123456789012345678

A92ES1C021DA

4. Enter [Machine] and [Type] information according to the following table. Then touch [Fix].



A92ES1C023DA

First four digits of the serial number	A92E	A92F	A92G
[Machine]	A	A	A
[Type]	1	2	F1

5. Touch [OK], and turn OFF the main power switch.

11. FAX function (only when the fax kit is mounted as optional equipment)

NOTE

- **When the user use the machine with the facsimile function, it is necessary to install and setting the optional FAX kit FK-517 properly by the service engineer.**

11.1 Installing/setting procedure of the FAX kit

11.1.1 Install procedure

1. Turn OFF the power switch and unplug the power cord from the power outlet.
2. Connect the supplied USB cable and harness to the fax kit. As for the harness, insert the connector on the side where the blue cable tie is attached.
3. For C3851FS: Remove the rear left cover. (Two screws)
   For C3851/C3351: Remove the rear left cover. (One screw)
4. Remove the filter from the back of the main body.
5. Remove the rear cover. (Four screws)
6. Remove the knockout from the rear cover.
7. Remove the left cover. (Two screws)
8. Remove the screw.
9. Remove the shield plate while withdrawing the mounting plate for the HDD. (11 screws)
10. Attach the fax kit by fitting the tab. (Two supplied screws)
11. Attach the fax kit while pushing it.
12. Connect the USB cable and harness to the MFP board.
13. Fit the USB cable and harness into the wire saddle.
14. To install the covers and other parts removed in steps 3 to 9, reverse the removal procedure.

11.1.2 Connecting the modular cable

1. Connect the supplied modular cable to the LINE port.
   If the user is connected with a key telephone system or a private branch exchange (PBX), do not connect the modular cable to where other than an analog line.

11.1.3 Affixing the labels

1. Affix the supplied label (Super G3 label).
2. Affix the supplied name plate label.

11.1.4 Configuration procedures

A. Setting the FAX

1. Plug the power cord into the power outlet and turn ON the power switch.
2. Display the Service Mode screen.
3. Touch “System 2.”
4. Touch “Option Board Status.”
5. Touch “Set” of FAX (circuit 1).
6. Touch “END” and touch “Exit.”
7. Turn OFF and ON the power switch.
   When displayed the Service Mode screen, be sure to turn OFF the power after exiting the Service Mode screen and wait for 10 seconds or more before turning ON.
8. Display the Service Mode screen.
9. Touch “System 1.”
10. Touch “Marketing Area.”

11. Touch “Fax Target.”
12. Use the [-] or [+] key to select the Target Area (Refer to the list below).

Country code setting for FAX			
U.S.	US	Poland	EU* (PL)
Canada	CA	Taiwan	TW
Germany	DE	Australia	AU
U.K.	EU* (GB)	New Zealand	NZ
France	EU* (FR)	Hong Kong	HK
Switzerland	EU* (CH)	Malaysia	MY
Netherlands	EU* (NL)	Singapore	SG
Belgium	EU* (BE)	South Africa	ZA
Austria	EU* (AT)	China	CN
Norway	EU* (NO)	Korea	KR
Sweden	EU* (SE)	Argentina	AR
Finland	EU* (FI)	Brazil	BR
Ireland	EU* (IE)	Vietnam	VN
Denmark	EU* (DK)	Philippines	PH
Spain	EU* (ES)	Russia	RU
Portugal	EU* (PT)	Saudi Arabia	SA
Italy	EU* (IT)		

NOTE

- **Set OT for countries other than the ones listed above.**

* Select the appropriate country code according to the dial system used in the installation place. For DTMF, select “EU,” and for dial pulse, select “each destination country code.”

13. Touch “END” twice.
14. Touch “FAX.”
15. Touch “Initialization.”
16. Touch “Fax Function Parameter” and “Communication Journal Data.”
17. Touch “Yes.”
18. Touch “Yes.”
19. Touch “END.”
20. Touch “Exit” on the Service Mode screen.
21. Perform the sending and receiving tests between the Machine and either the store which offers the service or the local retailer, to check that it can be operated normally.

B. Caution when performing dial transfer

After setting the country code, dialing operations may be selected after the switchboard dial tone is detected depending on the destination. In this case, depending on the switchboard connected to the machine and the type of dial tone received from the switchboard, dialing operations may not be available.
If that happens, you may be able to avoid the problem with the following setting.

(1) Turn the Dial Tone Detection function OFF

1. Display the Service Mode screen.
2. Touch “FAX.”
3. Touch “NetWork.”
4. Touch “Network Setting 2.”

5. Touch “OFF” of Dial Tone Detection.
6. Touch “END.”
7. Touch “Exit” on the Service Mode screen.

Use of this manual should be strictly supervised to avoid disclosure of confidential information.