



KONICA MINOLTA

**SERVICE MANUAL**

SECURITY FUNCTION

---

# **bizhub**

## **C360/C280/C220**

for PKI Card System

This Service Manual (Ver. 1.02) describes bizhub C360/bizhub C280/  
bizhub C220 PKI Card System Control Software  
(MFP Controller: A0ED0Y0-0100-GM0-31).





# Revision history

After publication of this service manual, the parts and mechanism may be subject to change for improvement of their performance.

Therefore, the descriptions given in this service manual may not coincide with the actual machine.

When any change has been made to the descriptions in the service manual, a revised version will be issued with a revision mark added as required.

Revision mark:

- To indicate clearly a section revised, show  to the left of the revised section.  
A number within  represents the number of times the revision has been made.
- To indicate clearly a section revised, show  in the lower outside section of the corresponding page.  
A number within  represents the number of times the revision has been made.

## NOTE

Revision marks shown in a page are restricted only to the latest ones with the old ones deleted.

- When a page revised in Ver. 2.0 has been changed in Ver. 3.0:  
The revision marks for Ver. 3.0 only are shown with those for Ver. 2.0 deleted.
- When a page revised in Ver. 2.0 has not been changed in Ver. 3.0:  
The revision marks for Ver. 2.0 are left as they are.

2010/07	1.02	—	Revised
2010/06	1.01	—	Revised
2010/06	1.00	—	Issue of the first edition
Date	Service manual Ver.	Revision mark	Descriptions of revision

# CONTENTS

## Security function

1.	Overview .....	1
2.	Compliance with the ISO15408 standard.....	1
3.	Data to be protected.....	1
4.	Precautions for operation control .....	1
5.	Checking the firmware version number.....	3
5.1	Security authentication firmware version number.....	3
6.	Accessing the Service Mode.....	3
6.1	Access method to the Service Mode.....	3
6.2	Access lock of Service Mode.....	5
6.2.1	Access lock release procedure .....	5
7.	Enhancing the security function .....	6
7.1	Details of settings .....	6
7.2	Security enhancing procedure.....	6
7.2.1	Making and checking the service settings .....	6
7.2.2	Requests to the administrator .....	11
8.	Service Mode functions.....	12
8.1	Firmware Version.....	12
8.1.1	Checking the firmware version number.....	12
8.2	CE Authentication function .....	13
8.2.1	Setting the CE Authentication function.....	13
8.3	Administrator Password function .....	14
8.3.1	Setting the administrator password.....	14
8.4	CE Password function.....	16
8.4.1	Setting the CE password.....	16
8.5	Initialization function .....	19
8.5.1	Initialize method .....	21
8.6	HDD Format.....	22
8.6.1	HDD format execution procedure.....	23
8.7	HDD installation setting .....	24
8.7.1	HDD installation setting procedure .....	24
8.8	Operation ban release time setting.....	25
8.8.1	Operation ban release time setting procedure.....	25
8.9	Administrator Unlocking function .....	26
8.9.1	Administrator Unlocking function procedure .....	26
9.	Overwrite All Data function.....	27

---

9.1	Overwrite All Data procedure .....	27
9.2	Items to be cleared by Overwrite All Data .....	27
9.2.1	Items cleared by Overwrite All Data.....	27
10.	Firmware rewriting .....	28
10.1	Outline .....	28
10.2	USB memory .....	28
10.2.1	Preparation .....	28
10.2.2	Procedure .....	28
10.2.3	Action when data transfer fails.....	31
11.	Setup procedure for PKI card system .....	32
12.	Installation of the loadable driver .....	32
13.	FAX function.....	33
13.1	Installing/setting procedure of the FAX kit .....	33
13.1.1	Install procedure .....	33
13.1.2	Setting procedure .....	34

## 1. Overview

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

## 2. Compliance with the ISO15408 standard

The security functions offered by this machine comply with ISO15408/IEC15408 (level: EAL3).

## 3. Data to be protected

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

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

- Encrypted document transmitted to the machine using a dedicated printer driver and an IC card from the client PC and saved in the machine
- Image files which have been scanned for transmission to a user mail address through email (S/MIME)

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

- Encrypted document
- Scanned image files
- Image files other than Encrypted document
- Image files of a job in the queue state other than Scanned image 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

## 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. Operating conditions for the IC card and IC card reader**

The machine supports the following types of IC card and IC card reader.

- The types of IC cards supported by the machine are the Common Access Card (CAC) and Personal Identity Verification (PIV).
- The type of IC card reader supported by the machine is AU-211P.

**D. Network connection requirements for the machine**

If the LAN is to be connected to an outside network, no unauthorized attempt to establish connection from the external network should be permitted.

<To achieve effective security>

- If the LAN, in which the machine is installed, is connected to an outside network, install a firewall or similar network device to block any access to the machine from the outside network and make the necessary settings.

**E. Machine maintenance control**

When the service engineer performs maintenance service jobs for the machine, he or she should check the firmware version number and the checksum value, and make sure that the system has not been altered.

**F. 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, is 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.

## 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 number and the checksum value.
- 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.28 for the method of how to re-write the firmware.](#)

### 5.1 Security authentication firmware version number

	MFP Controller Ver.	Check Sum
bizhub C360/C280/C220	A0ED0Y0-0100-GM0-31	111A

[Refer to P.12 for the method of checking the firmware version.](#)

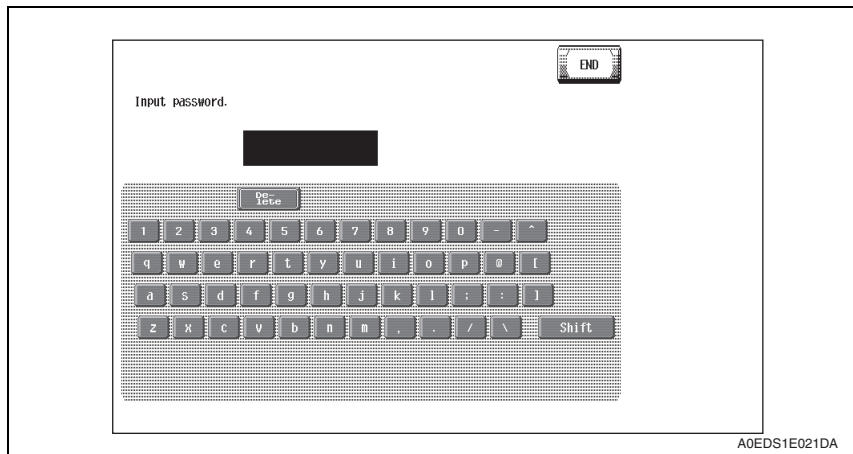
## 6. Accessing the Service Mode

### 6.1 Access method to the Service Mode

1. Press the Utility/Counter key.
2. Touch [Meter Count].
3. Touch [Check Details] on Meter Count display.
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].**

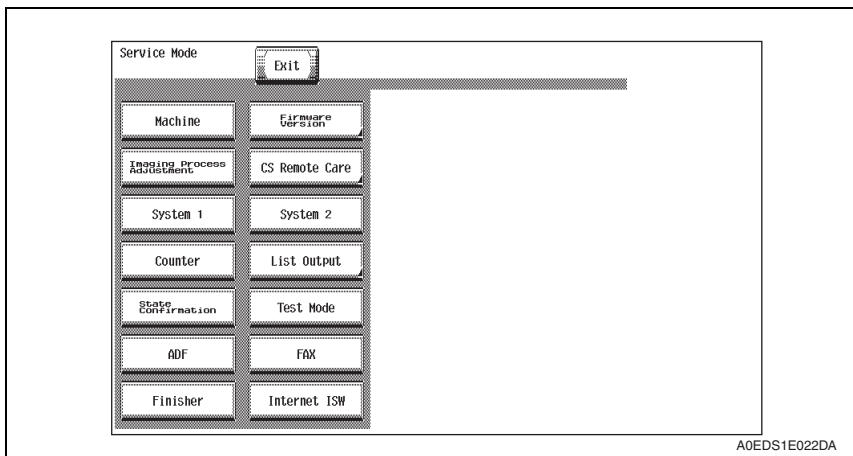


#### NOTE

- **The CE password entered is displayed as “\*.”**
- **NEVER forget the CE password. When forgetting the CE password, call responsible person of KMBT.**

- 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 "Mode 2" is set for [Prohibited Functions When Authentication Error] as accessed through [Administrator Settings] → [Security Settings] → [Security Details], 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.5.
- 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 sub power switch; 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 press [Exit] to the basic screen.

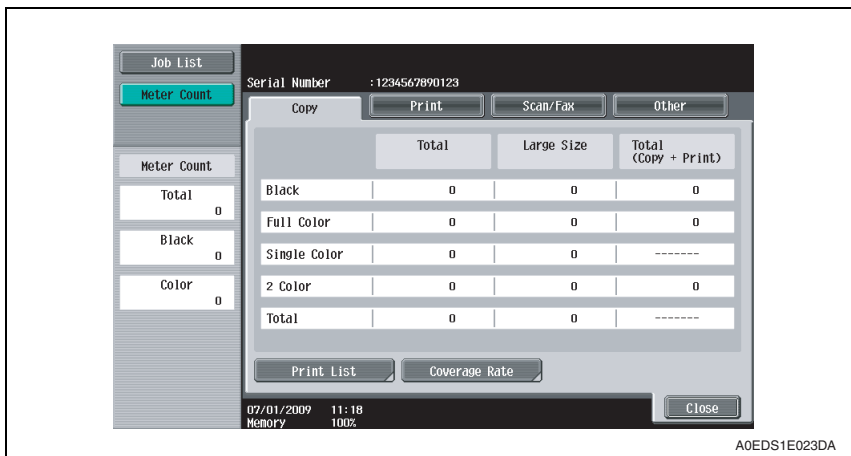


## 6.2 Access lock of Service Mode

- 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 sub power switch/main power switch and turn it on again more than 10 seconds after.
2. Press the Utility/Counter key.
3. Touch [Meter Count].
4. Touch [Check Details].
5. Touch [Coverage Rate].



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.25

## 7. Enhancing the security function

### 7.1 Details of settings

Item	Setting/Check	Default Setting
CE Authentication	ON	OFF
CE Password	Set arbitrarily.	92729272
Internet ISW	Check the setting of OFF	OFF
HDD installation setting	Check the setting of Installed.	Installed
CS Remote Care	Execute RAM Clear	-

**NOTE**

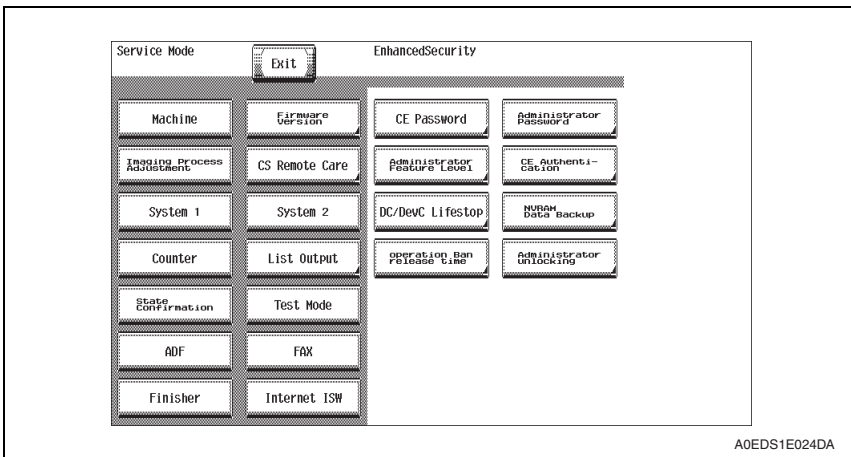
- The CE Password must be set to any value other than the default one.
- If fax functions are to be used, check that the fax kit has been mounted and set up properly.

[See P.33](#)

### 7.2 Security enhancing procedure

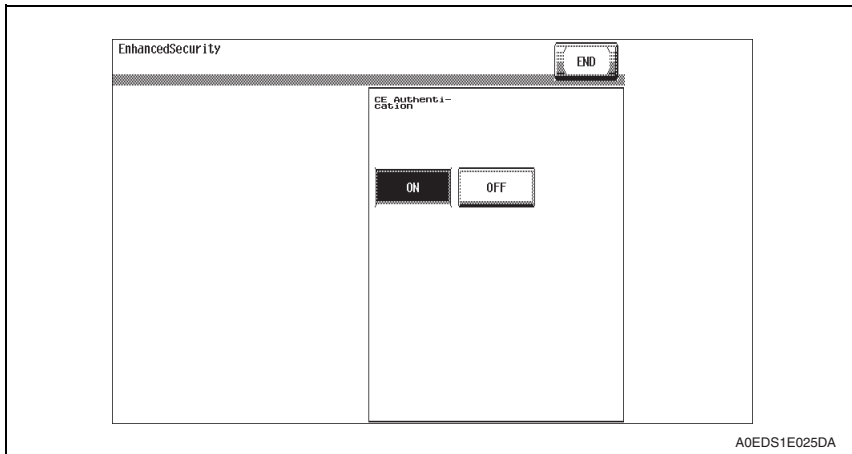
#### 7.2.1 Making and checking the service settings

1. Call the Service Mode to the screen.  
[See P.3](#)
2. Press the following keys in this order to display the Enhanced Security screen:  
Stop → 0 → Clear



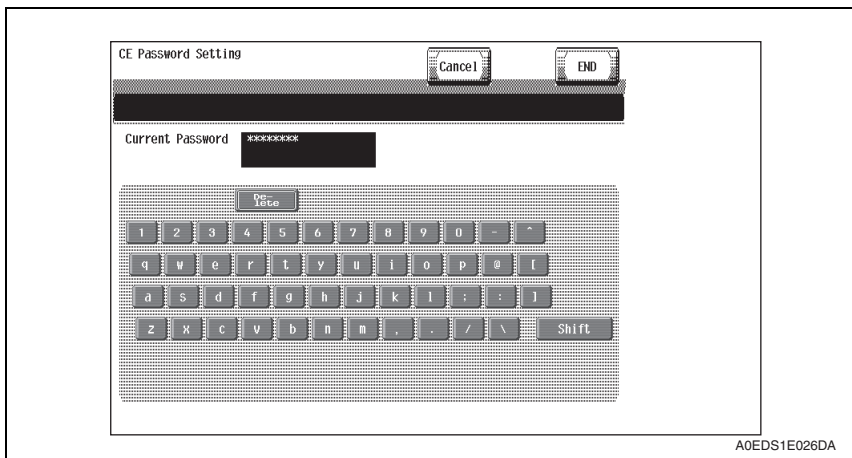
3. Touch [CE Authentication].

4. Touch [ON].



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

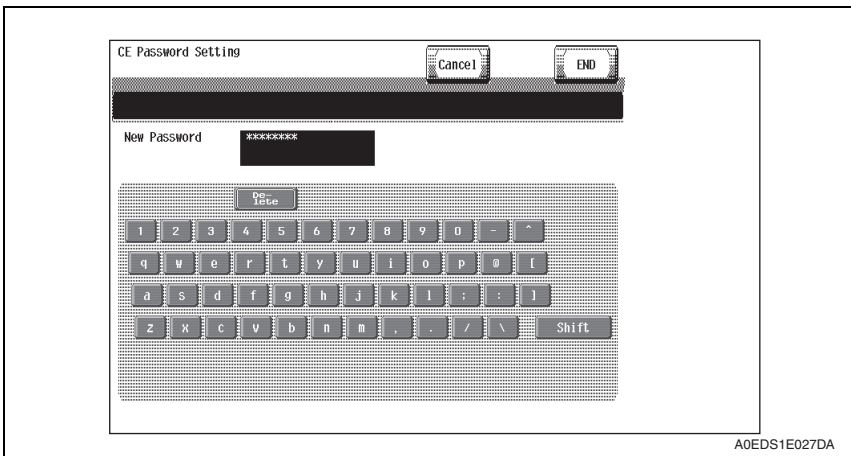
6. The default setting is "92729272." Using the keyboard shown on the display, enter "92729272" in Current Password and touch [END].



- 7. From the keyboard shown on the display, enter a new 8-digit password and touch [END].

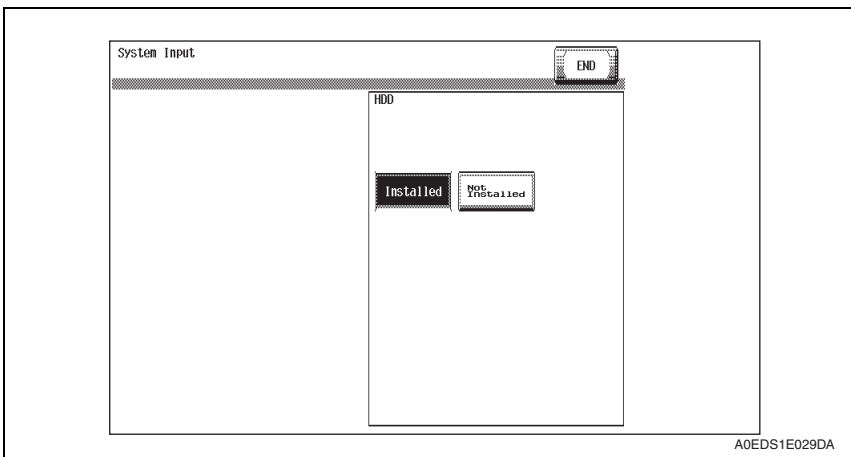
**NOTE**

- **Be sure to change the CE password.**
- **Set any value other than the default one for the CE Password.**
- **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 KMBT.**



A0EDS1E027DA

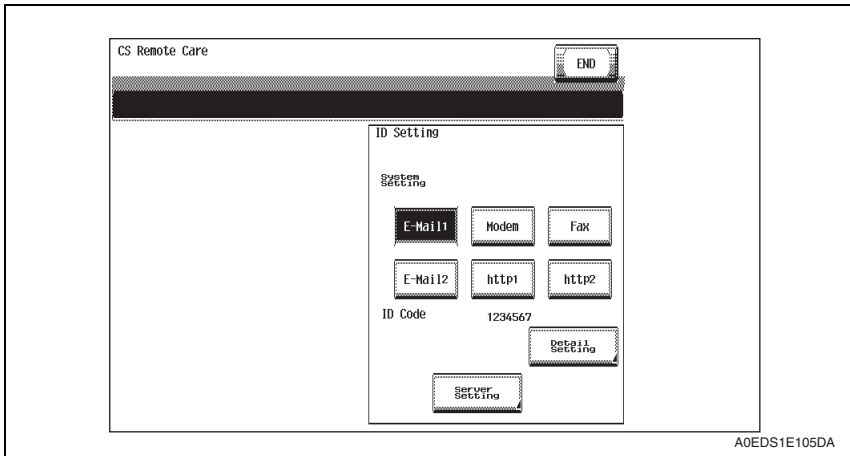
- 8. Type the new CE password again and touch [END].
- 9. Touch [System 2].
- 10. Touch [HDD] and check that "Installed" is selected.



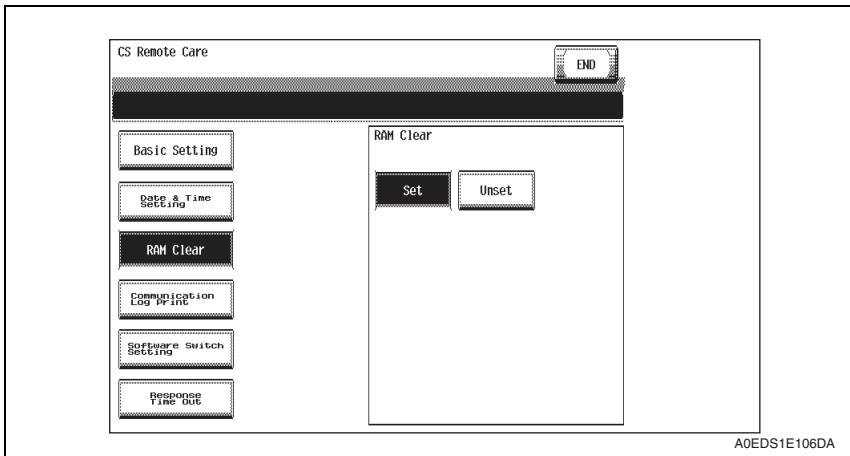
A0EDS1E029DA

- 11. Touch [END].
- 12. Touch [CS Remote Care].

- 13. If CS Remote Care has been set, [Detail Setting] appears on the display.  
Touch [Detail Setting].



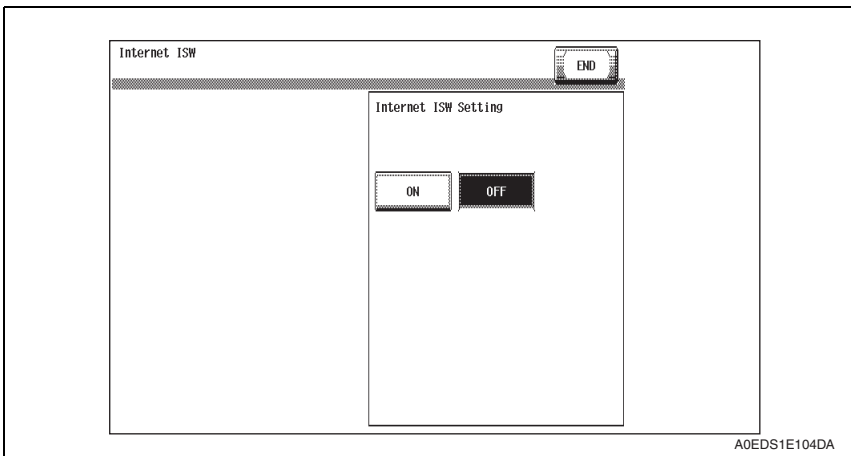
- 14. Touch [RAM Clear].
- 15. Touch [Set] and [END].



- 16. Touch [END] to display the Service Mode screen.

17. Touch [Internet ISW].

18. Touch [Internet ISW Set] and check that "OFF" is selected.

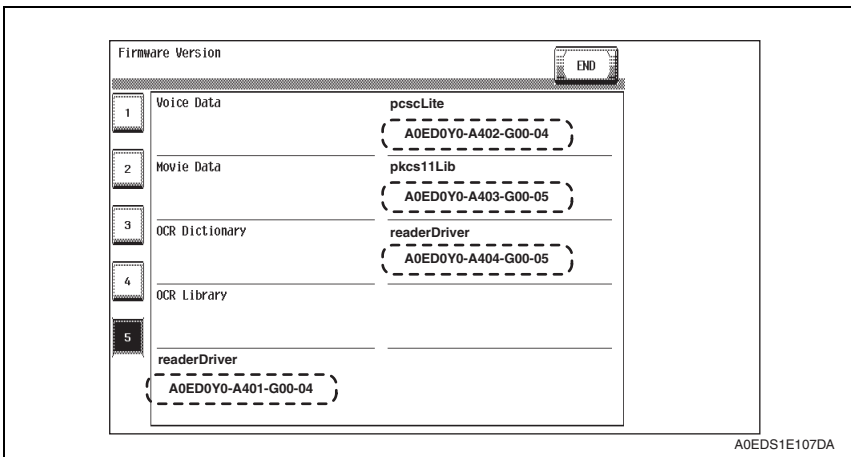


19. Touch [END].

20. Touch [Firmware Version].

21. Touch [5].

22. Make sure with the administrator that the version number of "readerDriver", "pcscLite", "pkcs11Lib" and "pkcs11Cfg" are the applicable version for this machine.



23. Touch [End].

24. Exit the Service Mode.

### 7.2.2 Requests to the administrator

- 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 "External Server (Active Directory only)" is set.	Not authenticated
Prohibit Functions When Auth. Error	Check that Prohibited Functions When Authentication Error has been set to [Mode2] by the administrator of the machine.	Mode 1
PSWC Settings	Check that "OFF" is set.	ON
OpenAPI Access Setting	Check that "Restrict" is set.	Allow
TCP Socket	Check that "OFF" is set.	ON
FTP Server Setting	Check that "OFF" is set.	ON
SNMP v1/v2c Setting	Check that Write setting is set to "Invalid".	Valid
SNMP v3(IP)	Check that "OFF" is set.	ON

#### NOTE

- If the administrator of the machine registers a new Encryption Key be sure first to perform [Physical Format] by accessing [Service Mode] → [State Confirmation] → [HDD Format].

# 8. Service Mode functions

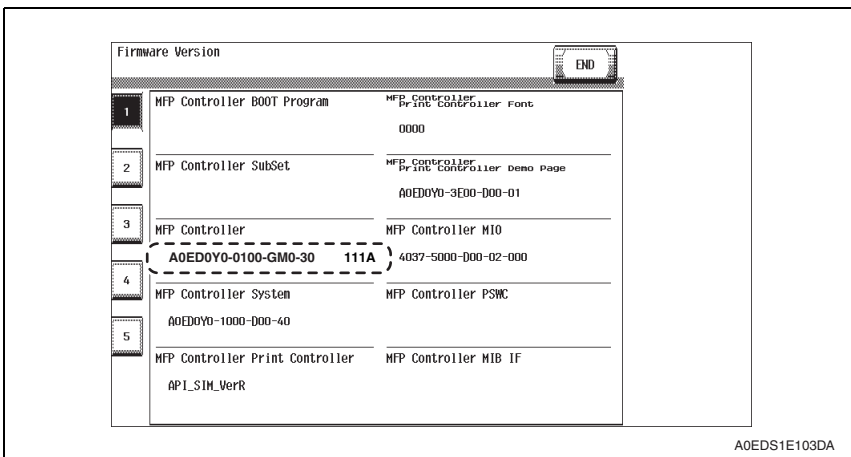
- The Service Mode is used to set various service functions.

## 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 firmware version number of the MFP Controller and the checksum value against the security authentication version.

### 8.1.1 Checking the firmware version number

1. Call the Service Mode to the screen.  
[See P.3](#)
2. Touch [Firmware Version].
3. Check the Firmware version number of MFP Controller and the checksum value using firmware version number.



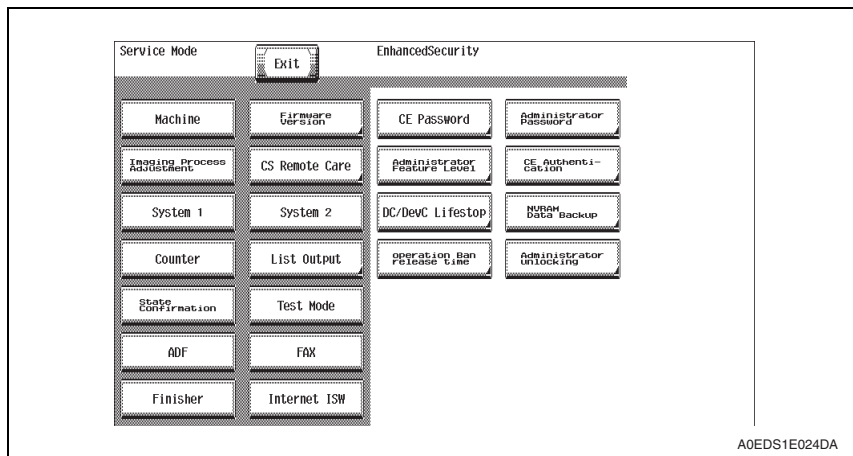


## 8.2 CE Authentication function

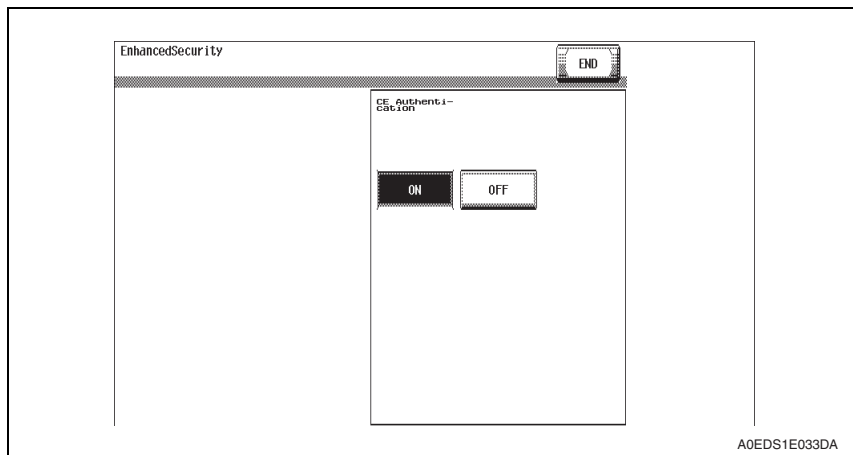
- The service engineer uses an 8-digit CE password for verifying his or her identity as service engineer, as he or she attempts to use the functions available from the Service Mode. Specific keys must first be entered before carrying out this authentication procedure.

### 8.2.1 Setting the CE Authentication function

- Call the Service Mode to the screen.  
[See P.3](#)
- Press the following keys in this order to display the Enhanced Security screen:  
Stop → 0 → Clear



- Touch [CE Authentication].
- Touch [ON] and [END].



### 8.3 Administrator Password function

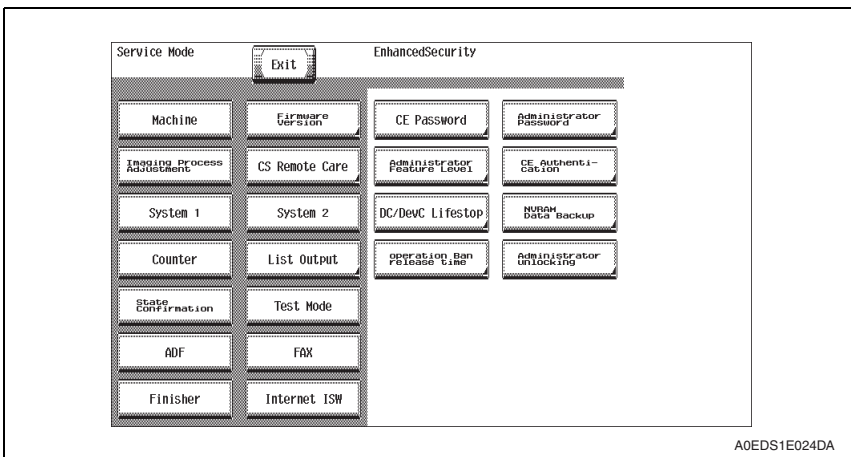
- This function is used when the administrator sets the administrator password. It also allows a new administrator password to be set without requiring the entry of the currently set administrator password. It is therefore used when the administrator forgets the administrator password.

#### 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.3](#)
2. Press the following keys in this order to display the Enhanced Security screen:  
Stop → 0 → Clear

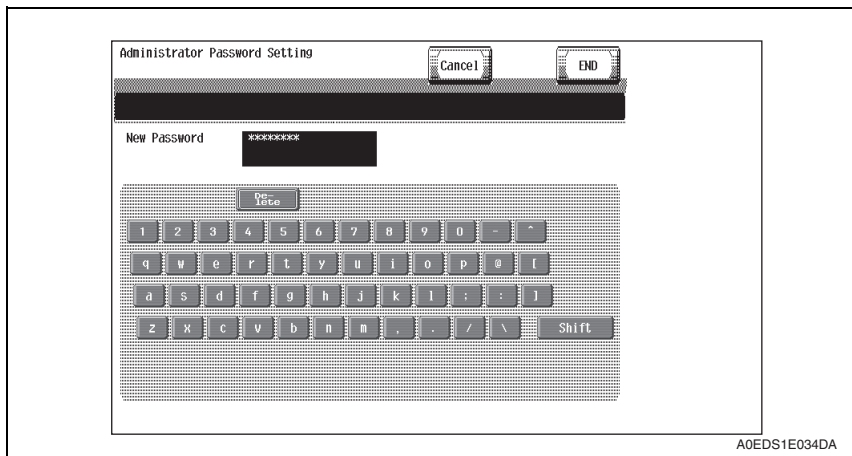


3. Touch [Administrator Password].

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.



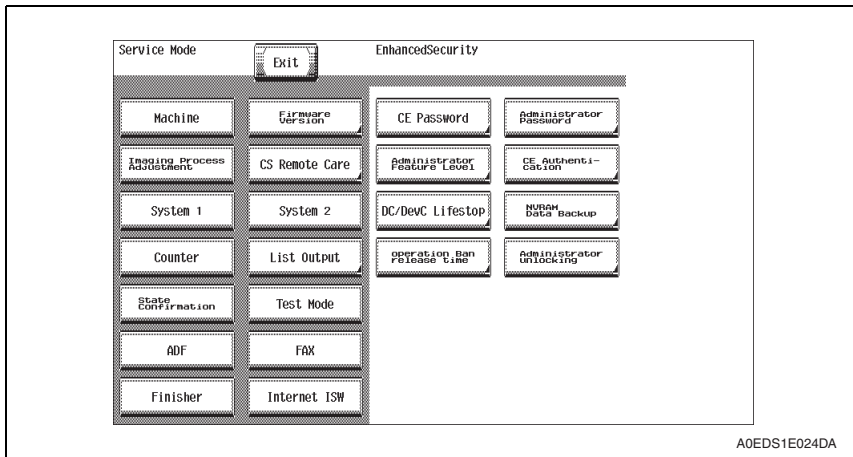
5. Enter the new Administrator Password (the default value “1234567812345678”) once again and touch [END].
6. Get the Administrator of the machine to access the Administrator Settings using the default password. Then, have him or her select the following functions in this order and change the default 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.3](#)
2. Press the following keys in this order to display the Enhanced Security screen:  
Stop → 0 → Clear



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

**NOTE**

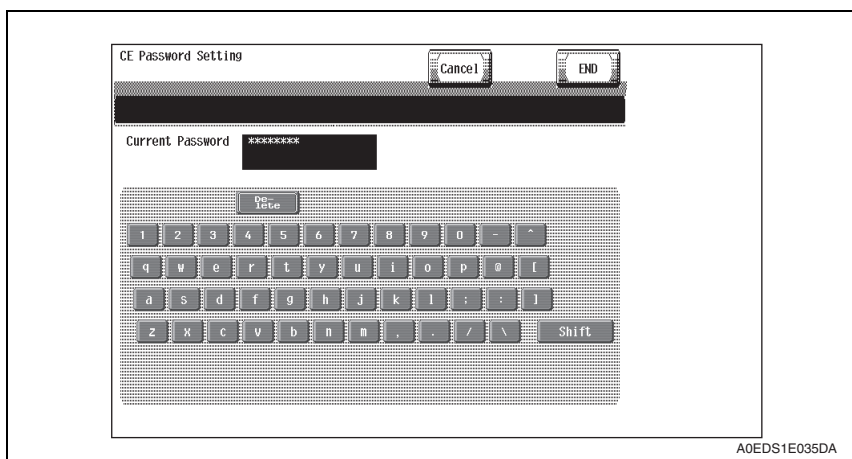
- If there is a mismatch in the CE Password between that currently set and that just entered, the machine displays a message telling that the CE Password entered is wrong. Enter the correct one.
- Each time a wrong CE password is entered, the CE password illegal access count is incremented by one.

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 "Mode 2" is set for [Prohibited Functions When Authentication Error] as accessed through [Administrator Settings] → [Security Settings] → [Security Details], 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.

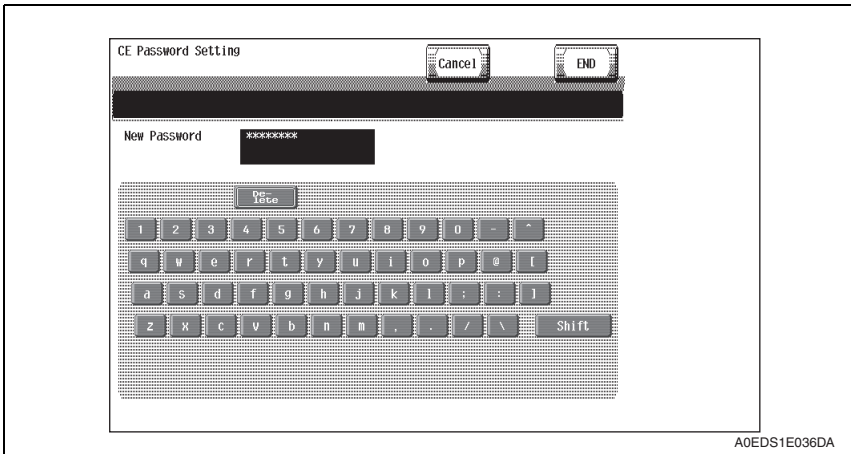
[For the procedure to release the access lock state, see P.5.](#)



- 5. Type the 8-digit password to be newly used from the keyboard shown on the display and touch [END].

**NOTE**

- For the CE Password, set a value other than the default.
- 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 KMBT.



- 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
<ul style="list-style-type: none"> <li>• Numeric characters: 0 to 9</li> <li>• Alpha characters: upper and lower case letters</li> <li>• Symbols: !, #, \$, %, &amp;, ', (, ), *, ,, -, ., /, :, ;, &lt;, =, &gt;, ?, @, [, \, ], ^, _ , ` , {,  , }, ~, +</li> </ul> Selectable from among a total of 93 characters

## 8.5 Initialization function

- The Data Clear 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 “92729272.”
	Administrator password	Administrator password is reset to “1234567812345678.”
	HDD Encryption Setting	HDD Encryption Setting function is set to OFF.
	Temporary Data Overwrite Setting	Temporary Data Overwrite Setting is set to [OFF].
	Prohibit Functions When Auth. Error	Prohibit Functions When Auth. Error is set to [Mode2].
	Secure Documents Access Method	Secure Documents Access Method is set to [Mode2]. (Linked to Prohibit Functions When Auth. Error)
	FTP server function	The following function is permitted. <ul style="list-style-type: none"> <li>• Print Data Capture</li> <li>• Acquisition of VCM count data</li> </ul>
	Release Time Settings	Release Time Settings is set to [5 min.].
	Audit Log Settings	Audit Log Settings is set to [No].
	SNMP v1/v2c	Write Setting of the SNMP v1/v2c Setting is set to “Invalid.”
	SNMP v3	SNMP v3 Setting is set to “OFF.”
	WebDAV server password	WebDAV server password is reset to the default value (sysadm).
	TCP Socket Settings	TCP Socket setting is set to [OFF].
	Network Setting	The currently set network settings (DNS Server setting, IP Address setting, SMTP Server setting, NetWare Setting, NetBIOS setting and AppleTalk Printer Name setting) is cleared and reset to the default setting.
	SSL-compliant protocol settings	All are set to OFF.
System Auto Reset	System Auto Reset is set to [1 min.].	
OpenAPI Settings	Access Setting is set to [Allow].	
PSWC Setting	PSWC Setting is set to [ON].	

Item		Details
Others	SSL certificate (PageScope Web Connection)	Deletes the currently set SSL certificate.
	SSL encryption strength (PageScope Web Connection)	Deletes the currently set SSL encryption strength setting.
	Administrator Password Change via Network (PageScope Web Connection)	Enables a change of the Administrator password made over the network.
	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/ S/MIME certificate data	All is deleted.
	Change made by the user of destination registration	Change by the user is enabled of destination registration.

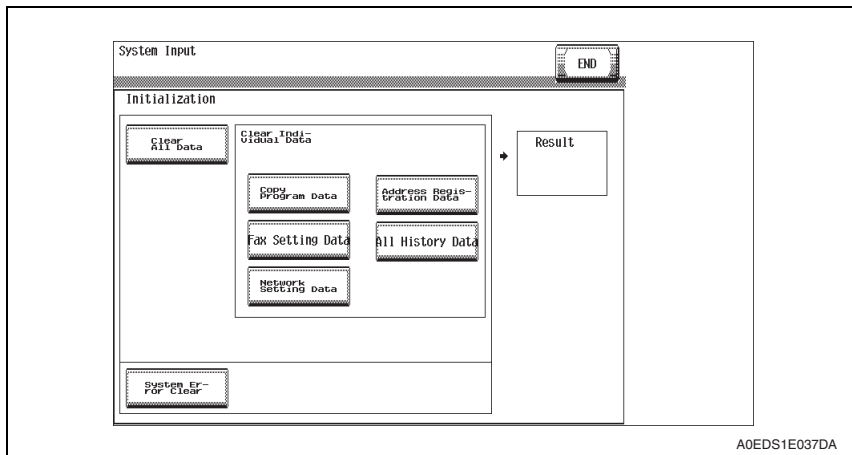
**B. Items cleared by Clear Individual Data (Network Setting Data)**

Item		Details
Administrator Settings	FTP server function	The following function is permitted. <ul style="list-style-type: none"> <li>• Print Data Capture</li> <li>• Acquisition of VCM count data</li> </ul>
	SNMP v1/v2c	Write Setting of the SNMP v1/v2c Setting is set to "Enable."
	SNMP v3	Security Level Setting of the SNMP v3 Setting is set to "auth-password/priv-password."
	SNMP password v3	SNMP password v3 is reset to the default value (MAC address).
	WebDAV server password	WebDAV server password is reset to the default value (sysadm).
	Network Setting	The currently set network settings (DNS Server setting, IP Address setting, SMTP Server setting, NetWare Setting, NetBIOS setting and AppleTalk Printer Name setting) is cleared and reset to the default setting.
	SSL-compliant protocol settings	All are set to OFF.
Others	SSL certificate (PageScope Web Connection)	Deletes the currently set SSL certificate.
	SSL encryption strength (PageScope Web Connection)	Deletes the currently set SSL encryption strength setting.



### 8.5.1 Initialize method

1. Call the Service Mode to the screen.  
See P.3
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.

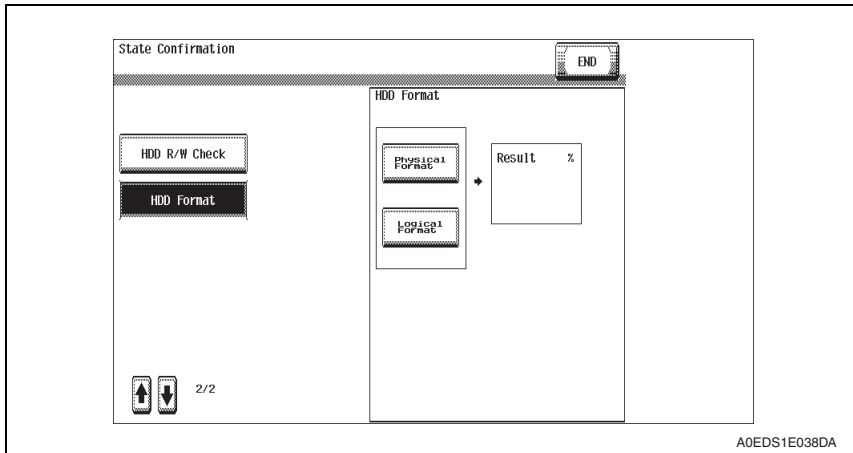
- Since the CE Password is reset to the default value, be sure to set once again a CE Password that meets the requirements of the Password Rules.
- Since the Administrator Password is reset to the default value, be sure to have the administrator of the machine set once again an Administrator Password that meets the requirements of the Password Rules.
- Since the SNMP Password v3 is reset to the default value (MAC address), be sure to have the administrator of the machine set once again a 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 press [Exit] to the main screen.

When the Clear Individual Data (Network Setting Data) function has been executed, be sure to make the following settings again.

- Since the SNMP Password v3 is reset to the default value (MAC address), be sure to have the administrator of the machine set once again a password that meets the requirements of the Password Rules.

### 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.



#### A. Items cleared by HDD format

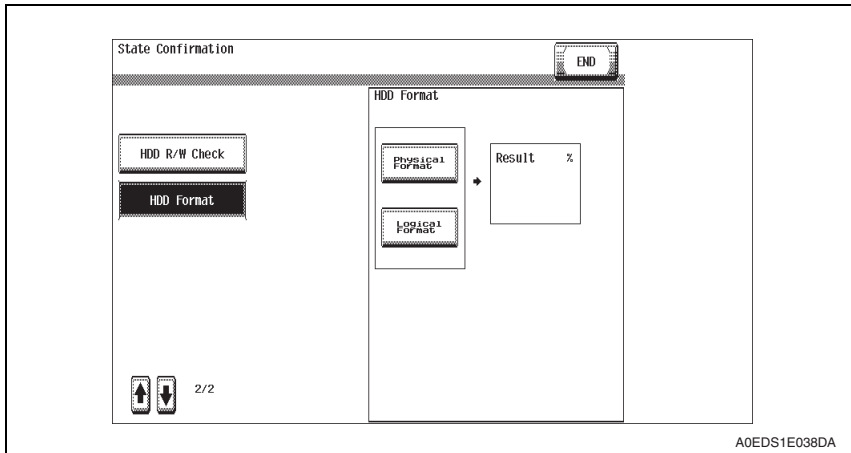
Item	Details
Encrypted document	Deletes all encrypted document saved in encrypted document user box.
External server	Deletes the currently set external server.
Loadable driver	Deletes the currently set loadable driver.

#### NOTE

- Performing HDD format deletes the loadable device driver installed in the machine. When the HDD format is performed, make sure to reinstall the loadable device driver to the machine. For details of the reinstallation procedure of the loadable device driver, see the following page.  
[See P.32](#)

### 8.6.1 HDD format execution procedure

1. Call the Service Mode to the screen.  
[See P.3](#)
2. Touch [State Confirmation].
3. Touch [Memory/HDD Adj.].
4. Touch [↓].
5. Touch [HDD Format].
6. Touch [Physical Format] or [Logical Format] and press the Start key.



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

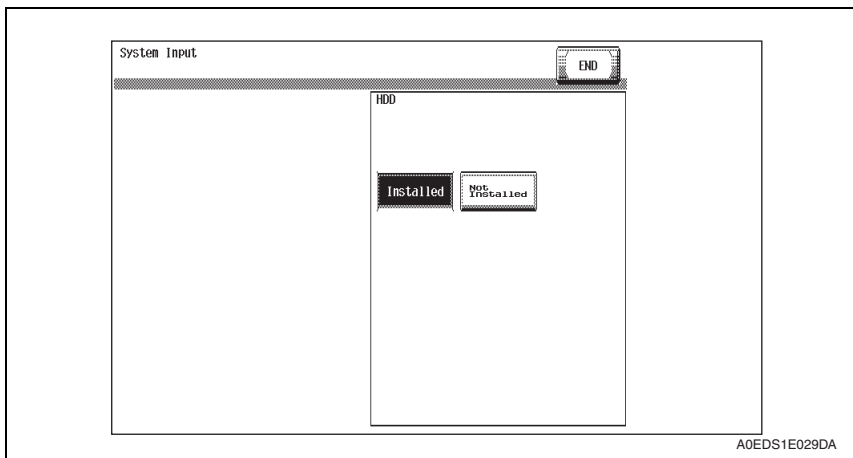
- HDD installation setting sets whether the hard disk is installed or not.

### NOTE

- **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.3](#)
2. Touch [System 2].
3. Touch [HDD].
4. Touch [Installed] or [Not Installed].



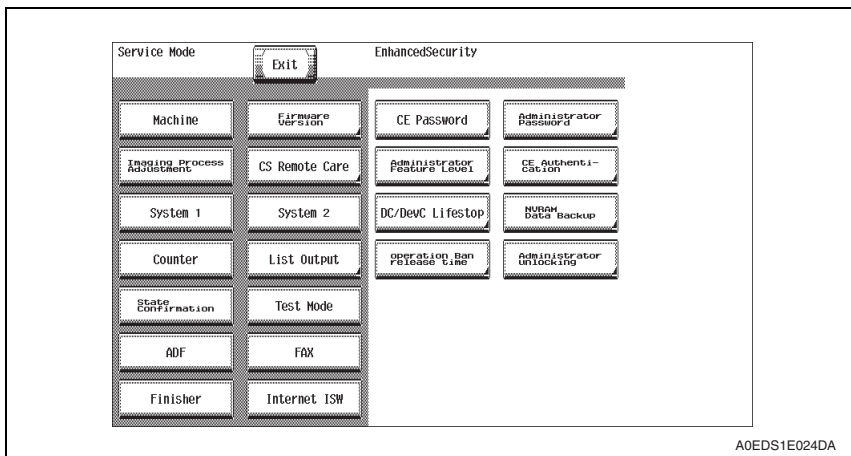
5. Touch [END] and exit the Service Mode.

### 8.8 Operation ban release time setting

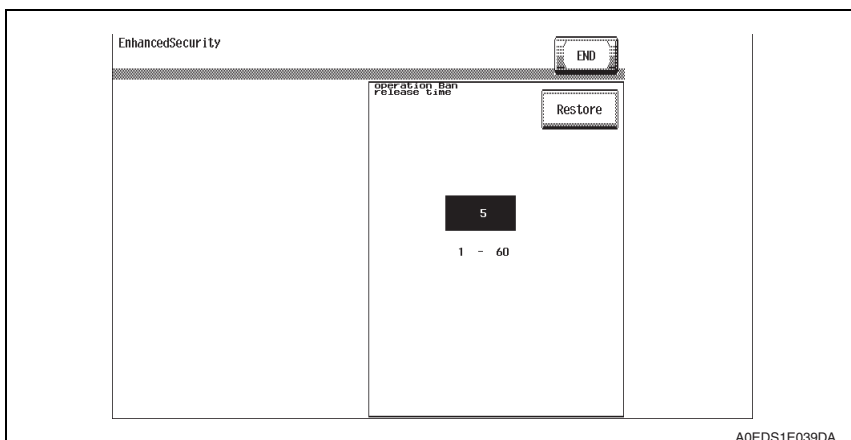
- This function is used to set the period of time to be elapsed before the access lock state is released.
- When the access lock release operation is performed, the machine measures the period of time set with this function and releases the access lock state after the lapse of the set period of time.

#### 8.8.1 Operation ban release time setting procedure

1. Call the Service Mode to the screen.  
[See P.3](#)
2. Press the following keys in this order to display the Enhanced Security screen:  
Stop → 0 → Clear



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

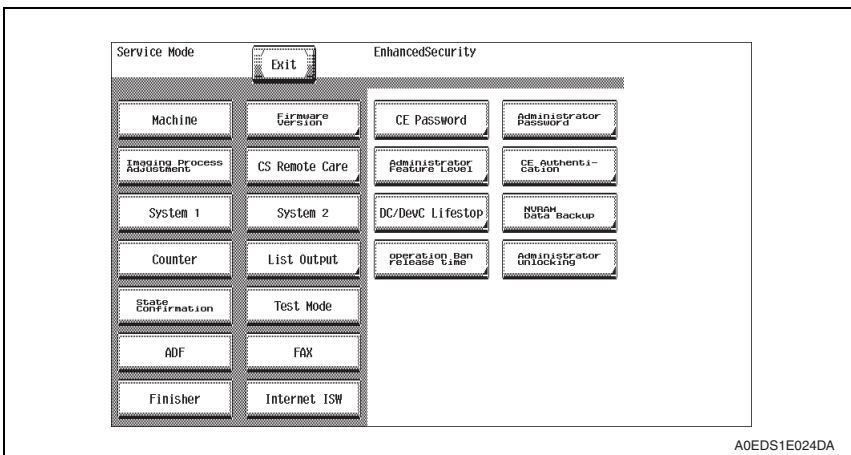


## 8.9 Administrator Unlocking function

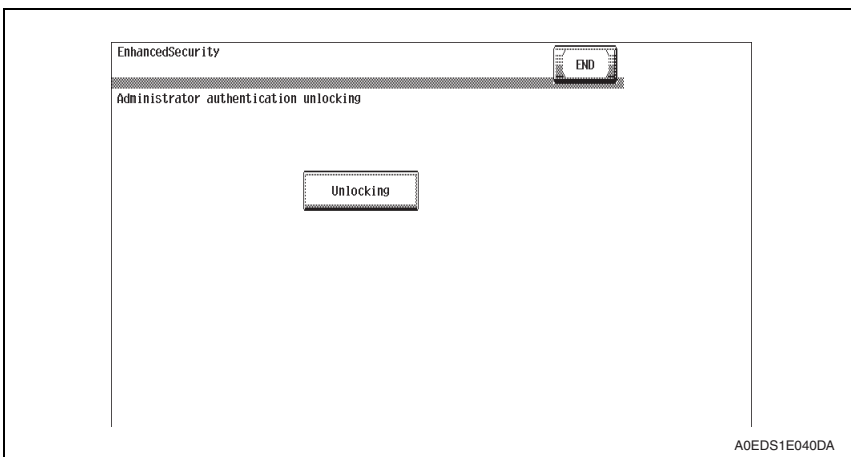
- When Administrator authentication using the Administrator password is set into an access lock state, this function may be used to release the access lock state.
- The access lock state for the Administrator password authentication can generally be released by turning OFF and ON the main power switch 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.3](#)
2. Press the following keys in this order to display the Enhanced Security screen:  
Stop → 0 → Clear



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



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 NVRAM 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] → [HDD 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	All setting items in administrator settings are cleared.
Encrypted document	Deletes all encrypted document saved in encrypted document user box.
Scanned image files	Deletes all Scanned image files
Image Data File	The following data is deleted: <ul style="list-style-type: none"> <li>• Image files other than Encrypted document</li> <li>• Image files of jobs in job queue state other than Scanned image files</li> <li>• Data files left in the HDD data space, used as image files and not deleted through the general deletion operation</li> <li>• Temporary data files generated during print image file processing</li> </ul>
S/MIME certificate	Deletes the currently set S/MIME certificate
Loadable driver	Deletes the currently set loadable driver.
NVRAM data backup area *	Clears all data that has been backed up.

\* NVRAM data backup area

- The data saved in NVRAM is stored in the backup area at regular intervals or through manual processing.
- The data saved in NVRAM 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.

#### NOTE

- **When rewriting the firmware, it is necessary to execute the following steps to rewrite the firmware.**  
**The BootROM rewriting and the loadable device driver/OCR dictionary installing should be executed as necessary depend on the firmware type or usage environment.**
  1. Touch [BootRom] in the firmware update item display, and touch [START].
  2. Check the message "BootRom Update completed successfully", and touch [OK].
  3. Rewrite the firmware data.
  4. Select [Service Mode] → [System 2] → [Data Install], and update the movie data to the new version.
  5. Select [Service Mode] → [System 2] → [Software Switch Setting].
  6. Touch [Switch No.] and enter "25" with the ten-key pad.
  7. Touch [HEX Assignment] and enter "20" with the ten-key pad.
  8. Touch [Fix].
  9. Turn OFF and ON the main power switch and sub power switch.
  10. Install the loadable device driver as occasion demands.
  11. Install the OCR dictionary data for the searchable PDF as occasion demands.

### 10.2 USB memory

#### 10.2.1 Preparation

- Conditions for USB memory which can be used for updating the firmware are as follows:
  - Without security function added (security function can be turned off)
  - Memory with 1 GB to 2 GB are recommended (One with 4 GB or more may not operate)
  - Corresponds to USB 2.0
  - Formatted with FAT32 type

#### 10.2.2 Procedure

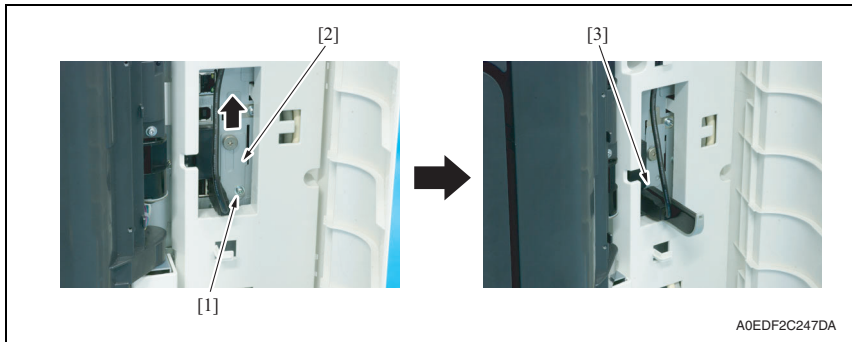
1. Connect the USB to the PC, and copy the firmware data to the USB memory.

#### NOTE

- **The firmware data to be updated must be copied to the root directory with the file name "A0EDFW. tar."**
  - **More than one firmware data with a single model or multiple models can be stored in the USB memory. (Maximum of fifteen files)**  
**When storing more than one firmware data, make a folder with a name "(model code) FW" ("A0EDFW" for this machine) right under the root directory.**  
**(File names can be set arbitrarily)**
  - **When making a folder and storing more than one firmware data, it is also necessary to copy the firmware data "A0EDFW. tar" to the root directly.**
2. Turn OFF the main power switch and the sub power switch.
  3. Remove the screw [1].

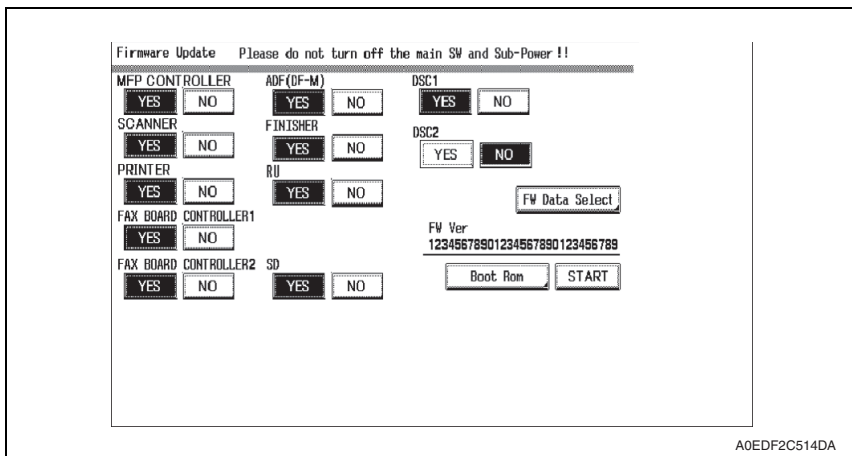


- 4. Lift up the cover [2] of the USB port.
- 5. Insert the USB memory device to the USB port [3] for service.



**NOTE**

- USB memory must be connected with the main power switch/sub power switch off.
  - When updating the firmware, use the USB port for the service. It cannot be updated when connected to another USB port.
- 6. Turn ON the main power switch and the sub power switch.
  - 7. Control panel shows F/W items to be updated, and select the particular type of F/W to be updated. (Select [YES].)



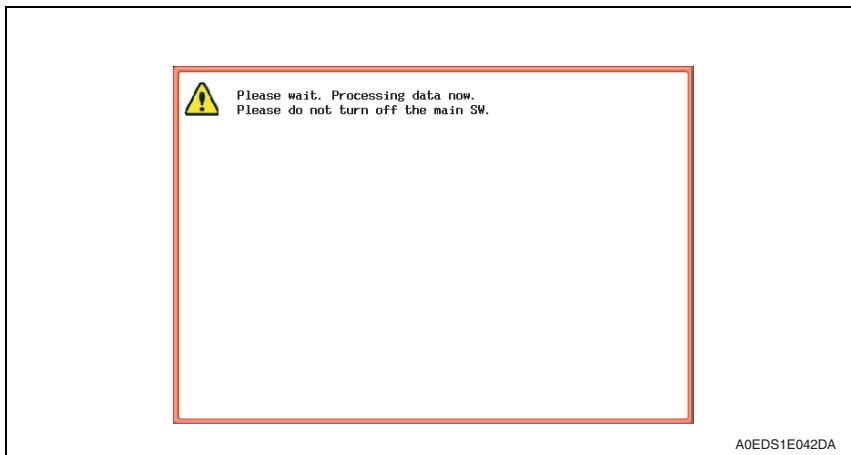
F/W to be updated	Appropriate board	Remark
MFP CONTROLLER	MFP board (MFPB)	
SCANNER	MFP board (MFPB)	
PRINTER	Printer control board (PRCB)	
FAX BOARD CONTROLLER1	Fax board (Main)	Only when the FK-502 is mounted
FAX BOARD CONTROLLER2	Fax board (Sub)	Only when the FK-502 is mounted
ADF (DF-M)	DF control board (DFCB)	
FINISHER	FNS control board (FSCB)	Only when the FS-527/529 is mounted
RU	Transfer control board (TRCB)	
SD	SD drive board (SDDB)	Only when the SD-509 is mounted
DSC1	DSC board	Only when the SC-507 is mounted
DSC2	Not used	

**NOTE**

- **Unless one of the keys on the control panel is pressed, firmware is automatically updated after 30 seconds when the main power switch/sub power switch is turned on.**
  - **When the BootRom file is in the firmware data, [RootRom] key is displayed. Pressing the key updates data.**
  - **When more than one firmware are stored in step 1, pressing [FW Data Select] enables selection. (Data of other models cannot be selected.) (Data with \* at the left top of data selection screen will be the default data copied to the root directly in the USB memory.)**
8. Press the [START]. (At this time, the Start key starts blinking red.)
  9. Check that the control panel shows the message indicating that the data has been rewritten correctly ([Downloading Completed]). Check also the check sum value ([Check Sum #####]) shown on the control panel. (The Start key lights blue.)
  10. Turn OFF the main power switch and the sub power switch.
  11. Remove the USB memory device, and fix the cover of the USB port using a screw.
  12. Turn ON the main power switch and the sub power switch.

**NOTE**

- **When turning the main power switch ON for the first time after the firmware is updated, data may sometimes be internally updated. In that case, the following message will be displayed. Never turn the main power switch OFF until either the serial number input screen or the trouble code screen is displayed.**



13. Call the Service Mode to the screen.
14. Select [Firmware Version].
15. 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	MFP board (MFPB)	
SCANNER	MFP board (MFPB)	
PRINTER	Printer control board (PRCB)	
FAX BOARD CONTROLLER1	Fax board (Main)	Only when the FK-502 is mounted
FAX BOARD CONTROLLER2	Fax board (Sub)	Only when the FK-502 is mounted
ADF (DF-M)	DF control board (DFCB)	
FINISHER	FNS control board (FSCB)	Only when the FS-527/529 is mounted
RU	Transfer control board (TRCB)	
SD	SD drive board (SDDB)	Only when the SD-509 is mounted
DSC1	DSC board	Only when the SC-507 is mounted
DSC2	Not used	

## 11. Setup procedure for PKI card system

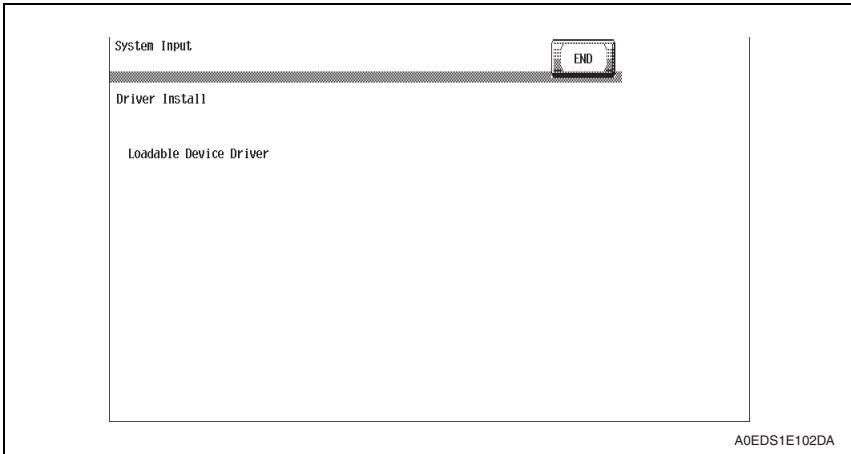
- After rewriting the firmware to the PKI card system, it is necessary to perform some setting to operate the PKI system.  
For details of the setting procedure, see “PKI card system setup instructions” and perform appropriate settings.

## 12. Installation of the loadable driver

- The loadable driver is updated using the USB memory.

### A. Procedure

1. Prepare a USB memory on which the driver data of the loadable device to be used was written.
2. Turn OFF the main/sub power switch.
3. Insert the USB memory to the USB port of the machine.
4. Turn ON the main/sub power switch.
5. Call the Service Mode to the screen.
6. Touch [System 2] → [Driver Install].



7. Touch [SET] to start installing the data.
8. Check that the control panel shows the message indicating that the data has been installed correctly.
9. Turn OFF the main power switch.
10. Remove the USB memory from the USB port.

## 13. FAX function

### NOTE

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

### 13.1 Installing/setting procedure of the FAX kit

#### 13.1.1 Install procedure

1. Turn off the machine and unplug the power cord from the power outlet.
2. Remove the mounting bracket from the PCI expansion board (four screws).
3. Remove the cover from the back of the machine as shown in the illustration (four screws).
4. Remove the plate as shown below (12 screws).
5. Remove the hard disk and its mounting bracket together from the machine (two screws).
6. Disconnect the two connectors from the hard disk.
7. Mount the PCI expansion board on the hard disk mounting bracket (four screws removed in step 2).
8. Connect the two connectors removed in step 6 to the hard disk.
9. Connect the PCI expansion board connector to the machine and screw the mounting bracket (two screws removed in step 5).
10. Reinstall the plate that has been removed in step 4 (12 screws).
11. Reinstall the cover that has been removed in step 3 (four screws).
12. Remove the cover from the right side of the machine as shown in the illustration (four screws).
13. If the machine does not have the paper feed cabinet installed, remove the indicated knockout using nippers.
14. Remove the left shield cover (six screws).
15. Check to make sure that SW2 on the FAX control board is set to "LINE-1."
16. Insert the FAX kit into the left socket and tighten the two shoulder screws.
17. Reinstall the cover removed in step 12 (four screws).
18. Open the door of the cover installed in step 17.
19. Connect the modular cable.
20. Route the modular cable as shown in the illustration below.
21. Close the door of the cover.

**13.1.2 Setting procedure****A. Setting the FAX (circuit 1)**

1. Plug the power cord into the power outlet and turn on the machine.
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."
7. Touch "System 1."
8. Touch "Marketing Area."
9. Touch "Fax Target."
10. Use the or key to select the Target Area (Refer to the list below).

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

**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."

11. Touch "END" twice.
12. Touch "FAX."
13. Touch "Initialization."
14. Touch "Fax Function Parameter" and "Communication Journal Data."
15. Touch "Yes."
16. Touch "Yes."
17. Touch "END."
18. Touch "Exit" on the Service Mode screen.

**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.
8. Turn OFF and ON the Main Power Switch.

**C. Affixing the labels**

1. Affix the label furnished with the kit to the position shown below.
2. Affix the label (Super G3 label) furnished with the machine to the position shown below.

**D. Setting the FAX (circuit 2)**

1. Plug the power cord into the power outlet and turn on the machine.
2. Display the Service Mode screen.
3. Touch "System 2."
4. Touch "Option Board Status."
5. Touch "Set" of FAX (circuit 2).
6. Touch "END."
7. Touch "FAX."
8. Touch "Line2."
9. Touch "Initialization."
10. Touch "Fax Function Parameter."
11. Touch "Yes."
12. Touch "Yes."
13. Touch "END."
14. Touch "Exit" on the Service Mode screen.
15. Turn OFF and ON the Main Power Switch.
16. 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.

**E. 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 "Line2."
4. Touch "NetWork."
5. Touch "Network Setting 2."
6. Touch "OFF" of Dial Tone Detection.
7. Touch "END."
8. Touch "Exit" on the Service Mode screen.
9. Turn OFF and ON the Main Power Switch.





KONICA MINOLTA

© 2009 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC.

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

Printed in Japan  
DDA0ED-C-SE1