KONICA MINOLTA

SERVICE MANUAL

SECURITY FUNCTION

bizhub C3110

This Service Manual (Ver. 1.01) describes:
TOE Name: bizhub C3110/ineo+ 3110 Control Software
(Controller Firmware: A6DT30G0116-999)

2014. 10
Ver. 1.01

KONICA MINOLTA, INC.

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 △1 to the left of the revised section.
  A number within △1 represents the number of times the revision has been made.

- To indicate clearly a section revised, show ▲1 in the lower outside section of the corresponding page.
  A number within ▲1 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.

2014/10	1.01	-	Revised
2014/06	1.00	-	Issue of the draft edition
Date	Service manual Ver.	Revision mark	Descriptions of revision

CONTENTS

Security function

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].
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 stored in the machine and made available for use by its users are protected while the machine is being used.

- Image files stored in the HDD by secured job
- Image files stored as “Personal” in the HDD by scan to HDD
- Image files stored in the HDD by ID & Print

The following data are also counted among the assets to be protected:

- Password

- User passwords and secured job passwords stored in the HDD and CE passwords, administrator passwords and SNMP passwords stored in the memory area on the MFP board

- Encryption Key

- Encryption Key to be registered in the memory area on the MFP board

- User identification information

- User identification information stored in the HDD

- IC card information

- User IC card information stored in the HDD

- Trusted channel setting data

- Trusted channel setting data stored in the memory area on the MFP board

The following types of data stored in the HDD and memory area on the MFP board are protected when use of a leased machine is terminated at the end of the leasing contract or the machine is to be discarded.

- Image files stored in the HDD by secured job
- Image files stored as “Personal” in the HDD by scan to HDD
- Image files stored in the HDD by ID & Print
- Image files of a job in the queue
- Any image files stored in the HDD data space other than the Secured Job files, files stored as “Personal” by Scan to HDD, and ID & Print 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
- CE passwords, Administrator passwords, SNMP passwords, Encryption Key, trusted channel setting data, and machine setting data stored in the memory area on the MFP board
- User identification information, user IC card information, user passwords and secured job passwords stored in the HDD

This machine offers the SSL function as a data protection method to ensure confidentiality of images (Scan to HDD files) transmitted and received over the network.

When transmitting and receiving highly confidential image data (Secured job files, Scan to HDD files, ID & Print files) among different pieces of IT equipment within an office LAN, the machine carries out communications with the correct destination via reliable paths or through anti-sniffing measures, assuming an office environment that responds to most stringent security requirements.

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 who sets up and services the machine should produce his or her identification card to the administrator of the machine and let the administrator confirm identity of the service engineer.
- 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.
- Do not leave the machine for a long time with the service mode display. When finishing the setting procedure in service mode, terminate the service mode as soon as possible.

C. Operating conditions for the IC card and IC card reader

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

IC card type	IC card reader
TypeA	AU-201/SCL-010
Felica IDm	AU-201/SCL-010
HID Prox	AU-201H * North America only

- SCL-010 is not covered by certification of ISO15408.

D. Machine maintenance control

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

E. 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.

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.
- If the firmware version/revision number of this machine is different from numbers shown in the list below, it will be necessary to re-write to the following certified firmware version.
  Refer to P.16 for the method of how to re-write the firmware.

5.1 Security authentication firmware version number

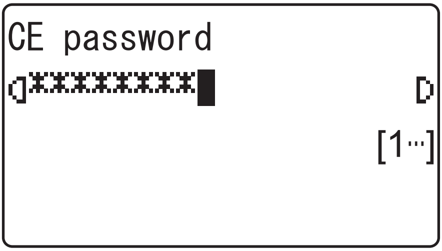
Firmware type	Version
Controller firmware	A6DT30G0116-999

Refer to P.8 for the method of checking the firmware version.

6. Accessing the Service Mode

6.1 Access method to the Service Mode

1. Select [UTILITY] and press the Select key.
2. Press the following keys in this order:
   Stop/Reset → 0 → 0 → Stop/Reset → 0 → 1
3. Enter the CE password (the default CE password is set to “92729272”).
4. Press the Select key.



CE password

****

[1…]

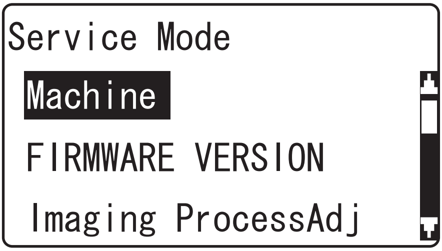
A6DTS1E001DA

NOTE

- **The CE password entered is displayed as “∗.”**
- **NEVER forget the CE password. When forgetting the CE password, contact Konica Minolta.**
  If the CE password is forgotten, replacement of the MFP board will initialize the setting values and turn “OFF” the Enhanced Security mode. Be sure to have the administrator set the Enhanced Security mode back to “ON” again.
- **Access to the Service Mode through the CE Password is restricted by up to 3 times.**
  If the CE password illegal access count exceeds 3 times, the machine is then set into an access lock state, so that further access to the Service Mode is disabled until unlocking the access lock.
  To unlock the access lock state, it is nessesary to restart the machine while by turning the main power switch OFF and ON.

- **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.**

5. The Service Mode screen will appear.



Service Mode

Machine

FIRMWARE VERSION

Imaging ProcessAdj

A6DTS1E002DA

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 the Stop/Reset key and log-out from the Service Mode.**

7. Enhancing the security function

- Perform the Enhanced Security Mode procedures while making checks of installation checklist in User's Guide [Security Operations].
- 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 Security enhancing procedure

7.1.1 Making and checking the service settings

- Resetting the CE password to meet the requirements of the password rules before executing the security enhancing procedure.
  See P.12

7.1.2 Requests to the administrator

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

Item	Setting/Check	Default Setting
Password Rules	Set to ON.	OFF
Administrator Password	Check that the password meets the requirements of the Password Rules.	12345678
Encryption Key	Set the Encryption Key.	OFF
User Authentication	Set to [Device] (Card Authentication + Password]).	OFF
Certificate for SSL	Register the self-signed certificate for SSL communications.	No setting
Enhanced Security Mode	Set to ON.	OFF

7.1.3 Functions whose settings are changed by Enhanced Security Mode

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

Function Name	Default Setting	When Enhanced Security mode is set to [ON]
Public User Access • To permit use by a public user having no user registration.	Restrict	Restrict (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)
User Name List • To display the list key for User names on user authentication screen.	OFF	OFF (not to be changed)
SSL • To set whether to encrypt access by SSL.	OFF	ON (not to be changed)
SSL Encryption Strength • To set the SSL encryption strength for the SSL encryption communication.	AES-256,3DES, RC4-128,DES, RC4-40	AES-256/3DES (not to be changed to one containing strength lower than AES/3DES)
FTP Server • To set whether to use FTP server function or not.	Enable	Disable (Selection can be made between [Enable] and [Disable])
SNMPv1/v2c • To use when changing Write setting.	Read/Write enable	Only Read is enabled (not to be changed)
SNMP v3 Security Level and auth-password/priv-password • To set the security level for the Reading/ Writing Authority User which is used for SNMP v3.	Auth-password/ Priv-password	auth-password/priv-password (Selection can be made between [auth-password] and [auth-password/priv-password])
Administrator Password Change Via Network (Pagescope Web Connection)	Enabled	Restrict
Telnet	OFF	OFF (not to be changed)

NOTE

- **Turning ON the Enhanced Security Mode does not enable the ID & Print function. To protect image files, be sure to have the administrator enable ID & Print function manually.**

8. Service Mode functions

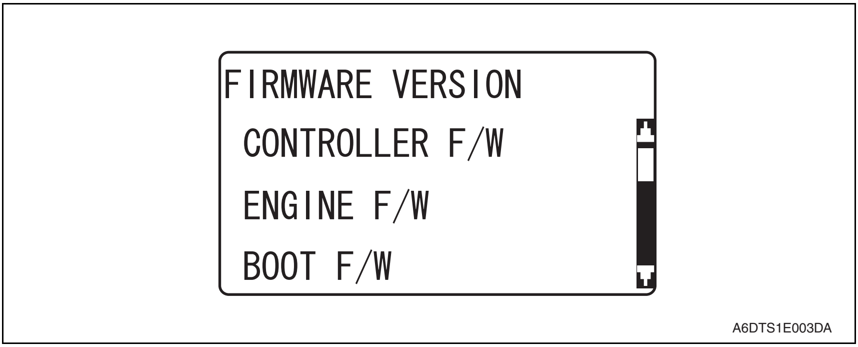
- The Service Mode is used to set various service functions.

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 [CONTROLLER F/W] against the security authentication version.

8.1.1 Checking the firmware version number

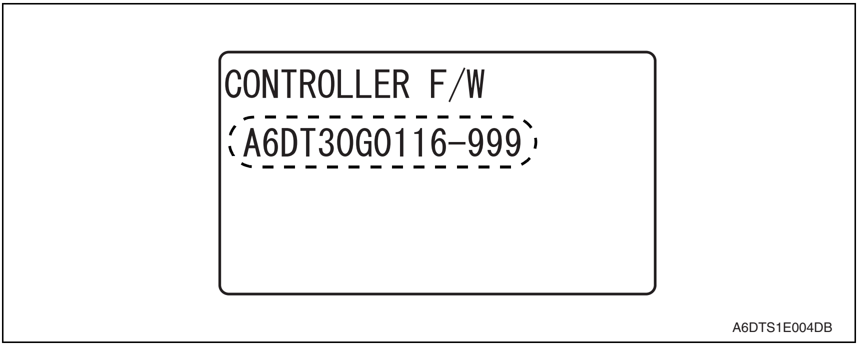
1. Call the Service Mode to the screen.
   See P.4
2. Select [FIRMWARE VERSION] and press the Select key.



FIRMWARE VERSION
CONTROLLER F/W
ENGINE F/W
BOOT F/W

A6DTS1E003DA

3. Check the Firmware version number of [CONTROLLER F/W] using firmware version number.

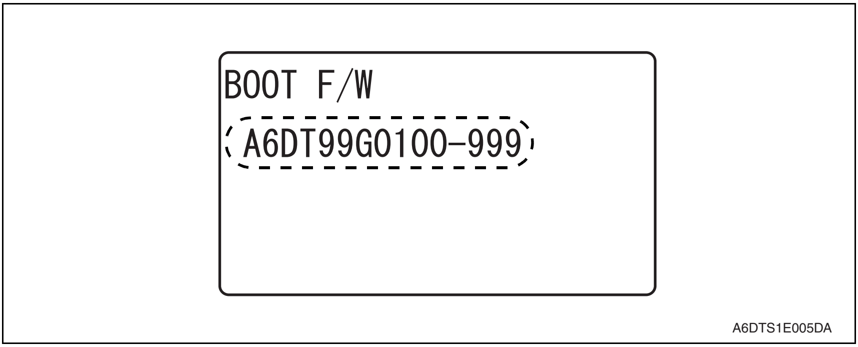


CONTROLLER F/W
A6DT30G0116-999

A6DTS1E004DB

NOTE

- **Check that the version of [BOOT F/W] is “A6DT99G0100-999”.**
- **If the version of [BOOT F/W] does not match, the service engineer will stop this setting and contact Konica Minolta.**



BOOT F/W
A6DT99G0100-999

A6DTS1E005DA

4. Press the Stop/Reset key.

8.2 Administrator Password function

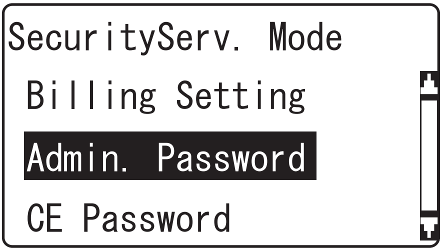
- This function is used when the administrator sets the administrator password. It also allows a new administrator password to be set without requiring the entry of the currently set administrator password. It is therefore used when the administrator forgets the administrator password.

NOTE

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

8.2.1 Setting the administrator password

1. Call the Service Mode to the screen.
   See P.4
2. Press the following keys in this order to display the SecurityServ. Mode screen:
   Back → 2 → 2 → 2 → 0 → 0
3. Select [Admin. Password] and press the Select key.

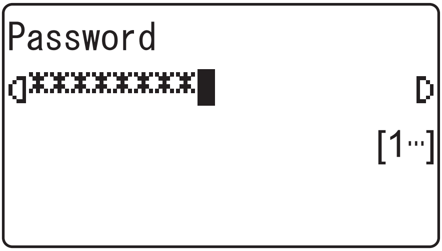


A6DTS1E006DA

4. Enter the default value “12345678” as the new password. Then, press the Select key.

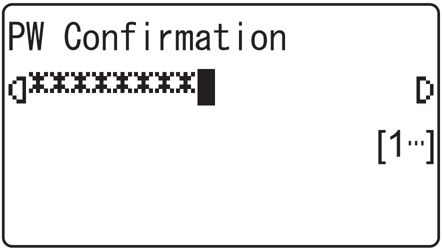
NOTE

- **Use the default value “12345678” as the password used only temporarily.**



A6DTS1E007DA

5. Enter the new administrator password (the default value “12345678”) once again and press the Select key.



PW Confirmation

[********█]

[1…]

A6DTS1E008DA

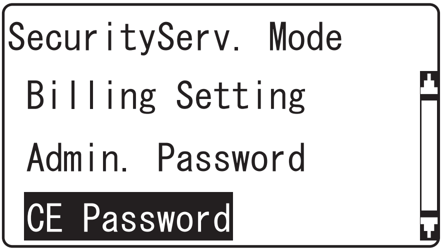
6. Get the administrator of the machine to access the Administrator Settings using the default password. Then, have him or her select the following functions in this order and change the default password: [Administrator Settings] → [Security Settings] → [Admin. Password].

8.3 CE Password function

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

8.3.1 Setting the CE password

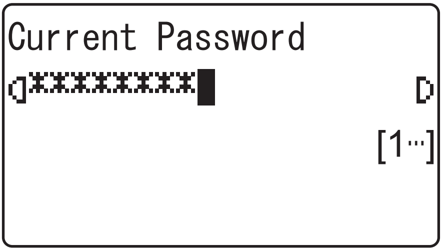
1. Call the Service Mode to the screen.
   See P.4
2. Press the following keys in this order to display the SecurityServ. Mode screen:
   Back → 2 → 2 → 2 → 0 → 0
3. Select [CE Password] and press the Select key.



SecurityServ. Mode
Billing Setting
Admin. Password
CE Password

A6DTS1E009DA

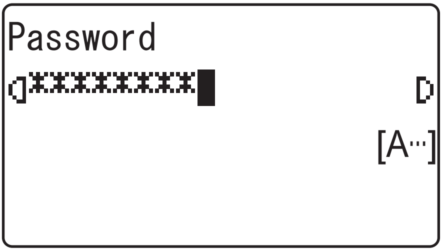
4. Enter the CE password set currently and press the Select key.



Current Password
****
[1…]

A6DTS1E010DA

5. Enter an 8-digit CE password to be newly used and press the Select key.

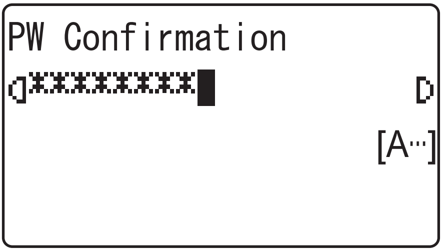


Password

[********]

A6DTS1E011DA

6. Re-enter the 8-digit CE password to be newly used and press the Select key.



PW Confirmation

[********]

A6DTS1E012DA

NOTE

- **The machine does not accept any new password that contains only the same character, consists of less than 8 digits, or that is the same as the previous password.**
- **For the CE Password, set a value other than the default.**
- **NEVER forget the CE password. When forgetting the CE password, contact Konica Minolta.**
  If the CE password is forgotten, replacement of the MFP board will initialize the setting values and turn "OFF" the Enhanced Security mode. Be sure to have the administrator set the Enhanced Security mode back to "ON" again.

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, }, ~, +, SPACE Selectable from among a total of 94 characters * The symbol "'" cannot be selected.

9. Data erase function

- The data erase function (Overwrite All Data/Restore All) overwrites and deletes all data saved in all areas of the HDD, and resets all passwords stored in the memory area on the MFP 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 Data erase procedure

- For the details of data erase procedure, see the User's Guide Security Operations.

9.2 Items to be cleared by data erase function

- **If the administrator of the machine executes data erase function 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.)

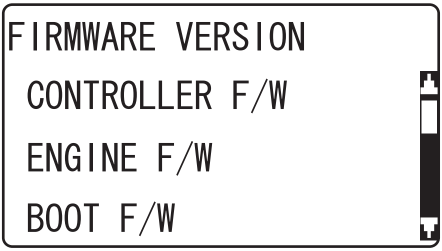
Items of data cleared	Description	Method
Enhanced Security Mode	Set to [OFF]	Overwrite All Data HDD Format RESTORE ALL
User registration data	Deletes all user-related data that has been registered	Overwrite All Data HDD Format
IC card registration data	Deletes all IC card-related data that has been registered	Overwrite All Data HDD Format
Secured Job Password/ file	Deletes all Secured Job-related information and files saved	Overwrite All Data HDD Format
Scan to HDD file	Delete all files stored as Personal by Scan to HDD	Overwrite All Data HDD Format
ID & Print file	Deletes all ID & Print files	Overwrite All Data HDD Format
Image files	• Image files saved other than the Secured Job files, files stored as Personal by Scan to HDD, and ID & Print files • Image files of jobs in job queue state • Remainder data files, used as image files and not deleted through only the general deletion operation • Temporary data files generated during print image file processing	Overwrite All Data HDD Format
Administrator Password	Clears the currently set password, resetting it to the factory setting	RESTORE ALL
SNMP Password	Clears the currently set password, resetting it to the factory setting (MAC address)	RESTORE ALL
SSL certificate	Deletes the currently set SSL certificate	Overwrite All Data HDD Format RESTORE ALL
Network Setting	Clears the currently set network settings (DNS Server setting, IP Address setting, and NetBIOS setting), resetting it to the factory setting	RESTORE ALL
Machine setting data	Deletes the machine setting data	RESTORE ALL

Items of data cleared	Description	Method
Trusted channel setting data	Deletes the trusted channel setting data	RESTORE ALL

10. Firmware rewriting

10.1 Checking the current firmware version

1. Call the Service Mode to the screen.
   See P.4
2. Select [FIRMWARE VERSION] and press the Select key.
3. Select the firmware to be updated and check the current version.



FIRMWARE VERSION
CONTROLLER F/W
ENGINE F/W
BOOT F/W

A6DTS1E003DA

10.2 Firmware upgrading procedure by USB memory device

10.2.1 Preparations for firmware upgrading

A. System requirements

- PC equipped with a USB port
- USB memory device

B. Saving the firmware data into the USB memory device

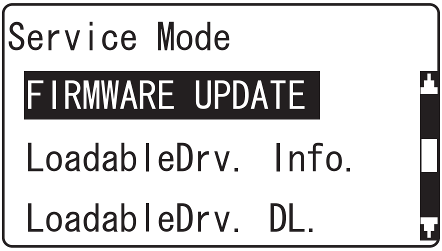
1. Save the firmware data in appropriate space in the PC.
2. Connect the USB memory device to the PC.
3. Create a “firmware” folder immediately under the drive of the USB memory device.
4. Copy the firmware data (***.prn) in the firmware folder created in step 3.

NOTE

- **Be sure to save the firmware data in “drive:/firmware/***.prn.”**
- **This machine can display up to 20 files of firmware data during upgrading.**

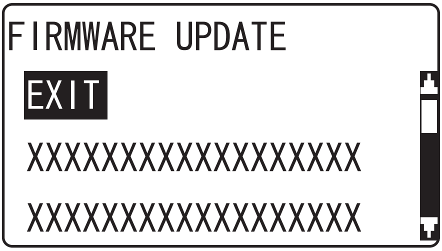
C. How to write firmware data

1. Turn the main power switch ON.
2. Connect the USB memory device to this machine.
3. Call the Service Mode to the screen.
   See P.4
4. Select [FIRMWARE UPDATE] and press the Select key.



A6DTS1E013DA

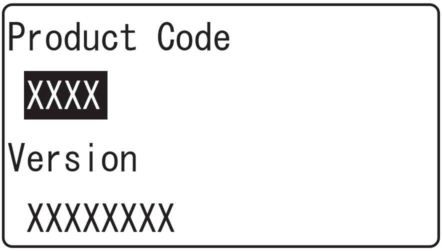
5. A list of firmware data in the USB memory device will be displayed.



A6DTS1E014DA

NOTE

- **Before upgrading firmware, use [Check Setting] to check that the firmware data is correct.**

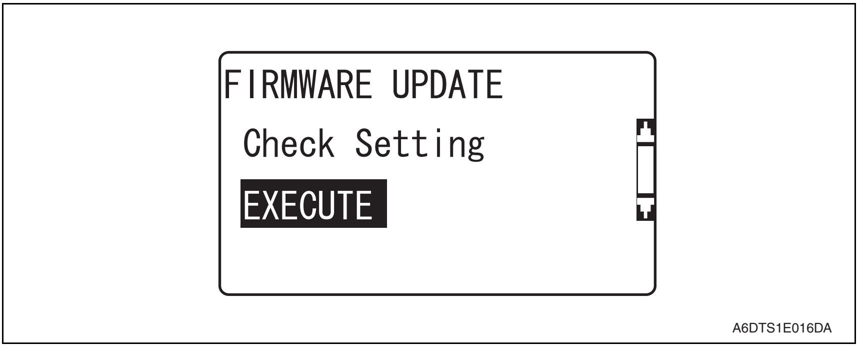


Product Code
XXXX
Version
XXXXXXXX

A6DTS1E015DA

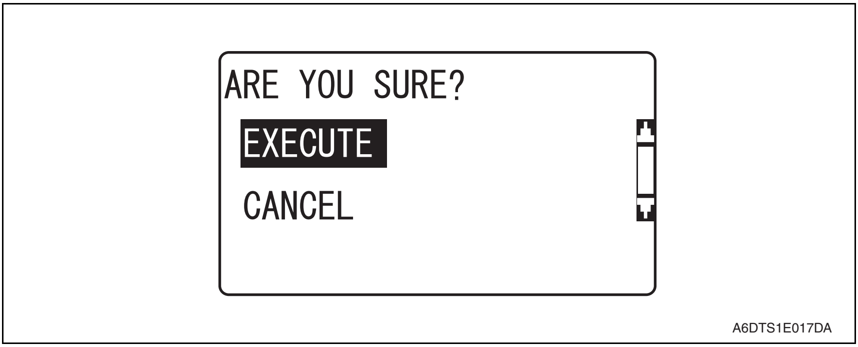
6. Press the Back key.

7. Select the specific firmware data to be upgraded and press the Select key.
8. Select [EXCUTE] and press the Select key.



FIRMWARE UPDATE
Check Setting
EXECUTE

9. Select [EXCUTE] and press the Select key.



ARE YOU SURE?
EXECUTE
CANCEL

10. The firmware upgrading procedure starts.

NOTE

- **NEVER turn OFF the power of the printer during firmware upgrading.**
- **NEVER disconnect the USB memory device from this machine during the firmware upgrading procedure.**

11. This machine is automatically restarted as soon as the firmware is upgraded correctly.

NOTE

- **At the time of firmware rewriting, check that there is no trouble code displayed.**
- **At the time of firmware rewriting, contact Konica Minolta when any trouble occurred.**

12. Remove the USB memory device from this machine.

11. Loadable driver downloading

11.1 Outline

- When using the machine with user authentication by the IC card, the loadable driver must be downloaded to the machine to use the IC card reader.

11.2 Downloading procedure

11.2.1 Preparations for loadable driver downloading

A. System requirements

- PC equipped with a USB port
- USB memory device

B. Confirmation of Digital Signature

- To ensure integrity of the data file, confirm the digital signature using the property of the provided loadable driver.

C. Saving the loadable driver data into the USB memory device

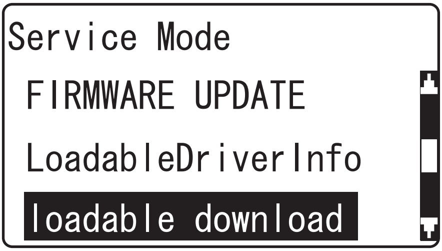
1. Save the loadable driver data in appropriate space in the PC.
2. Connect the USB memory device to the PC.
3. Create a “firmware” folder immediately under the drive of the USB memory device.
4. Copy the loadable driver (***.tar) in the firmware folder created in step 3.

NOTE

- **Be sure to save the firmware data in “drive:/firmware/***.tar.”**

11.2.2 How to download loadable driver data

1. Turn the main power switch ON.
2. Call the Service Mode to the screen.
   See P.4
3. Connect the USB memory device to this machine.
4. Select [loadable download] and press the Select key.



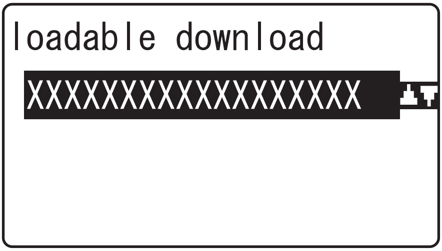
```
Service Mode
 FIRMWARE UPDATE
 LoadableDriverInfo
 loadable download
```

A6DTS1E018DA

bizhub C3110

Security Function

5. The loadable driver data list in the USB memory device will be displayed.

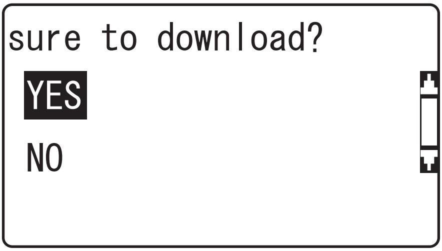


loadable download

XXXXXXXXXXXXXXXXXX

A6DTS1E019DA

6. Select the loadable driver data to be downloaded, and press the Select key.
7. Select [YES] and press the Select key.



sure to download?

YES

NO

A6DTS1E020DA

8. The loadable driver downloading procedure starts.

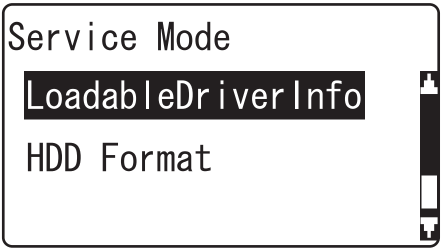
NOTE

- **NEVER disconnect the USB memory device from this machine during the loadable driver downloading procedure.**

9. A message will appear on the screen to prompt you to restart this machine, so turn off the main power switch.
10. Remove the USB memory device from this machine.
11. Turn the main power switch ON.

11.2.3 Checking the loadable driver version

1. Turn the main power switch ON.
2. Call the Service Mode to the screen.
   See P.4
3. Select [LoadableDriverInfo] and press the Select key.

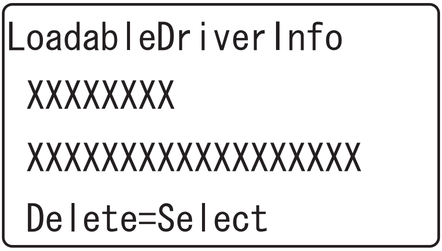


Service Mode
LoadableDriverInfo
HDD Format

A6DTS1E021DA

4. Check the following versions for each type of card.

- Felica:A3GN0Y0A502G0000
- TypeA :A3GN0Y0A502G0000
- HID-Prox:A3GN0Y0A00G00000



LoadableDriverInfo
XXXXXXXX
XXXXXXXXXXXXXXXXXX
Delete=Select

A6DTS1E022DA

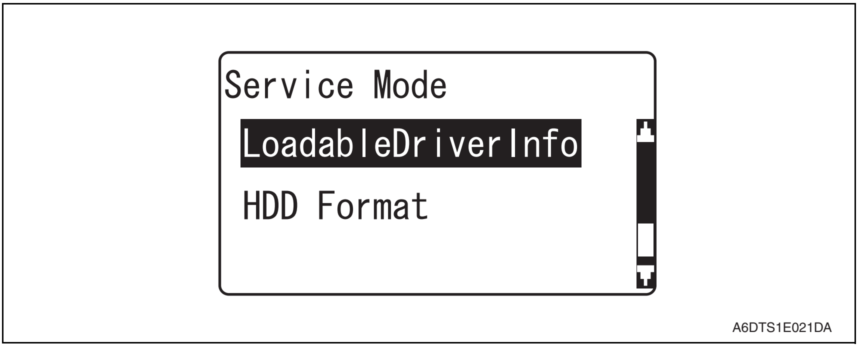
NOTE

- **When downloading the loadable driver of Felica or TypeA, since the versions of loadable drivers for both Felica and TypeA are same, when holding the card to be registered over a card reader, a message showing that the card has failed to be authenticated indicates that the loadable drive has been downloaded successfully. If no message appears, download the loadable driver of the type of card to be registered again.**

5. Press the Back key.

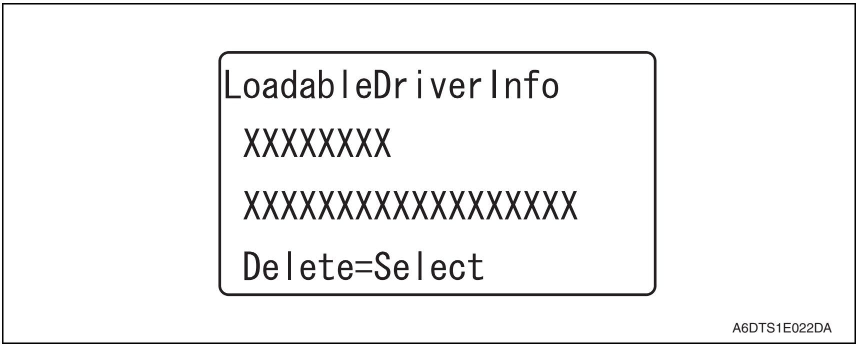
11.3 Deleting procedure

1. Turn the main power switch ON.
2. Call the Service Mode to the screen.
   See P.4
3. Select [LoadableDriverInfo] and press the Select key.



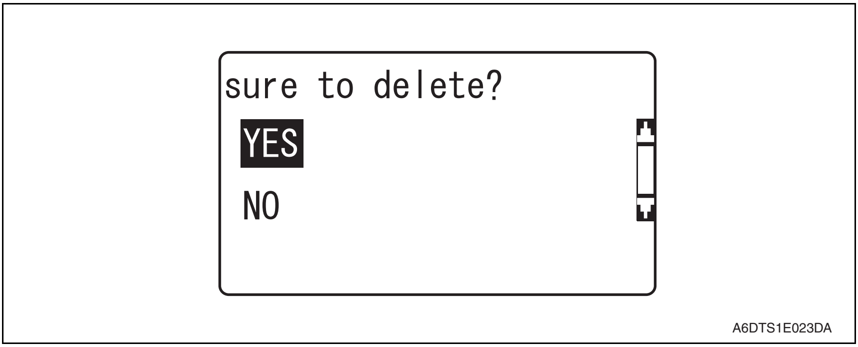
Service Mode
LoadableDriverInfo
HDD Format

4. Press the Select key.



LoadableDriverInfo
XXXXXXXX
XXXXXXXXXXXXXXXXXX
Delete=Select

5. Select [YES] and press the Select key on the confirmation screen.



sure to delete?
YES
NO

6. Restart this machine following the message on the control panel.

KONICA MINOLTA

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