Fingerprint Identification System

Owner's Manual



Model : LAFP10-R
LAFP10-S



CAUTION

RISK OF ELECTRIC SHOCK
DO NOT OPEN



CAUTION:TO REDUCE THE RISK OF ELECTRIC SHOCK
DO NOT REMOVE COVER (OR BACK)
NO USER-SERVICEABLE PARTS INSIDE
REFER SERVICING TO QUALIFIED SERVICE PERSONNEL.



This lightning flash with arrowhead symbol within an equilateral triangle is intended to alert the user to the presence of uninsulated dangerous voltage within the product's enclosure that may be of sufficient magnitude to constitute a risk of electric shock to persons.



The exclamation point within an equilateral triangle is intended to alert the user to the presence of important operating and maintenance(servicing) instructions in the literature accompanying the product.

FCC (Federal Communications Commission)

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technical for help.

WARNING: This equipment may generate or use radio frequency energy. Changes or modifications to this equipment may cause harmful interference unless the modifications are expressly approved in the instruction manual. The user could lose the authority to operate this equipment if an unauthorized change or modification is made.

This device complies with Part 15 of the FCC`s Rules. Operation is subject to the following two Conditions:
1. This device may not cause harmful interference, and
2. This device must accept ant interference received, including interference that may cause undesirable operation.

- A suitable conduit entries, knock-outs or glands shall be provided in the cable entries of this product in the end user.
- **Caution:**Danger of explosion if battery is incorrectly replaced. Replaced only with the same or equivalent type recommended by the manufacturer.
  Dispose of used batteries according to the manufacturer's instructions.

- Holes in metal, through which insulated wires pass, shall have smooth well rounded surfaces or shall be provided with brushings.

Warning: Do not install this equipment in a confined space such as a bookcase or similar unit.

Warning: Wiring methods shall be in accordance with the National Electric Code, ANSI/NFPA 70.

Warning: This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Warning: To reduce a risk of fire or electric shock, do not expose this product to rain or moisture.

Caution: This installation should be made by a qualified service person and should conform to all local codes.

Caution: To avoid electrical shock, do not open the cabinet. Refer servicing to qualified personnel only.

Caution: The apparatus should not be exposed to water (dripping or splashing) and no objects filled with liquids, such as vases, should be placed on the apparatus.

To disconnect power from the mains, pull out the mains cord plug. When install the product, ensure that the plug is easily accessible.



Disposal of your old appliance

1. When this crossed-out wheeled bin symbol is attached to a product it means the product is covered by the European Directive 2002/96/EC.
2. All electrical and electronic products should be disposed of separately from municipal waste stream via designated collection facilities appointed by the government or the local authorities.
3. The correct disposal of your old appliance will help prevent potential negative consequences for the environment and human health.
4. For more detailed information about disposal of your old appliance, please contact your city office, waste disposal service or the shop where you purchased the product.
5. EEE Compliance with Directive.

Hereby, LG. declares that this LAFP10 is in compliance with the essential requirements and other relevant provisions of directive 1999/5/EC.

CE This product is manufactured to comply with EMC Directive 2004/108/EC and Low Voltage Directive 2006/95/EC.

European representative :

This class [B] digital apparatus complies with Canadian ICES-003 Get appareil numerique de la classe [B] est conforme a la norme NMB-003 du canada.

Important Safety Instructions

1. **Read these instructions.** - All these safety and operating instructions should be read before the product is operated.
2. **Keep these instructions.** - The safety, operating and use instructions should be retained for future reference.
3. **Heed all warnings.** - All warnings on the product and in the operating instructions should be adhered to.
4. **Follow all instructions.** - All operating and use instructions should be followed.
5. **Do not use this apparatus near water.** - For example: near a bath tub, wash bowl, kitchen sink, laundry tub, in a wet basement; near a swimming pool; etc.
6. **Clean only with dry cloth.** - Unplug this product from the wall outlet before cleaning. Do not use liquid cleaners.
7. **Do not block any ventilation openings. Install in accordance with the manufacturer's instructions.** - Slots and openings in the cabinet are provided for ventilation, to ensure reliable operation of the product, and to protect it from overheating. The openings should never be blocked by placing the product on a bed, sofa, rug or other similar surface. This product should not be placed in a built-in installation such as a bookcase or rack unless proper ventilation is provided and the manufacturerís instructions have been adhered to.
8. **Do not install near any heat sources such as radiators, heat registers, stoves, or other apparatus (including amplifiers) that produce heat.**

Important Safety Instructions

9. **Do not defeat the safety purpose of the polarized or grounding-type plug. A polarized plug has two blades with one wider than the other. A grounding type plug has two blades and a third grounding prong. The wide blade or the third prong are provided for your safety. If the provided plug does not fit into your outlet, consult an electrician for replacement of the obsolete outlet.**

10. **Protect the power cord from being walked on or pinched particularly at plugs, convenience receptacles, and the point where they exit from the apparatus.**

11. **Only use attachments/accessories specified by the manufacturer.**

12. **Use only with the cart, stand, tripod, bracket, or table specified by the manufacturer, or sold with the apparatus. When a cart is used, use caution when moving the cart/apparatus combination to avoid injury from tip-over.**



13. **Unplug this apparatus during lightning storms or when unused for long periods of time.**

14. **Refer all servicing to qualified service personnel. Servicing is required when the apparatus has been damaged in any way, such as power-supply cord or plug is damaged, liquid has been spilled or objects have fallen into the apparatus, the apparatus has been exposed to rain or moisture, does not operate normally, or has been dropped.**

Glossary



LAFP10
Fingerprint Identification System

■ **Admin, Administrator**
- As a user who can enter into the terminal menu mode, he can register/modify/delete terminal users and change the operating environment by changing settings.
- If there is no administrator for a terminal, anyone can change the settings. In this regard, it is recommended to register at least one administrator.
- Caution is required with registration and operation because an administrator has the right to change critical environmental settings of the terminal.

■ **1 to 1 Verification**
- A user's verification fingerprint (template) is compared to the user's enrollment fingerprint (template) previously registered. The terminal performs 1:1 matches against the user's enrolled template until a match is found.
- It is called 1 to 1 Verification because only the fingerprint registered in the user's ID or card is used for comparison.

■ **1 to N Identification**
- The terminal performs matches against multiple fingerprints (templates) based solely on fingerprint information.
- Without the user's ID or card, the user's fingerprint is compared to fingerprints previously registered.

■ **I-Capture (Intelligent Capture)**
- Reinforces detection capability for residual fingerprints (fingerprints left on a sensor window due to sweat or contaminants on a finger) and automatically adjusts sensor settings to detect good-quality fingerprints regardless of the conditions (dry or wet) of the fingerprints.

■ **Authentication level**
- Depending on the fingerprint match rate, it is displayed from 1 to 9. Authentication is successful only if the match rate is higher than the set level.
- The higher the Authentication level, the higher the security. However, it requires a relatively high match rate, so Authentication is vulnerable to failure.
- 1:1 Level: Authentication level used for 1:1 verification.
- 1:N Level: Authentication level used for 1:N identification.

■ **Authentication method**
- Various kinds of authentication including FP (fingerprint) authentication, PW (password) authentication, RF (card) authentication, or a combination of these methods.
- Ex) FP|PW: fingerprint or password authentication; password is used for authentication if fingerprint authentication fails.

■ **Function keys**
- [F1], [F2], [F3], [F4], [ENTER] are used, and they are used for direct authentication and each key represents each authentication mode.

Contents

1. Before using 10
1.1. Safety precautions 10
1.2. Terminal description 12
1.3. Screen description 13
1.4. Voice information 14
1.5. Buzzer sound 14
1.6. LED signal 14
1.7. Correct fingerprint registrationm and input methods 15

2. Introduction 17
2.1. Features 18
2.2. Configuration 19

3. Configuration settings 20
3.1. Check items before device configuration settings 20
3.1.1. Entering menu 20
3.1.2. Changing setting parameters 21
3.1.3. Saving device configuration settings 22
3.2. Menu configuration 23
3.3. User account 24
3.3.1. User registration 24
3.3.1.1. '1. FP' registration 25
3.3.1.2. '2. ID&PW' registration 27
3.3.1.3. '3. FPIPW' registration 28
3.3.1.4. '4. FP&PW' registration 29
3.3.1.5. '5. RF' registration 30
3.3.1.6. '6. RFIFP' registration 31
3.3.1.7. '7. RF&FP' registration 32
3.3.1.8. '8. RFIPW' registration 33
3.3.1.9. '91. RF&PW' registration 34
3.3.1.10. '92. ID&FPIRF&FP' registration 35
3.3.1.11. '93. ID&PWIRF&PW' registration 36
3.3.2. Deleting User 37
3.3.3. Modifying User 38
3.3.3.1. '1. FP' user 38
3.3.3.2. '2. ID&PW' user 39
3.3.3.3. '3. FPIPW' , '4. FP&PW' user 39
3.3.3.4. '5. RF' user 40
3.3.3.5. '6. RFIFP' , '7. RF&FP' , '92. ID&FPIRF&FP' user 40
3.3.3.6. '8. RFIPW' , '91. RF&PW' , '93. ID&PWIRF&PW' user 40
3.3.4. Administrator registration 41
3.3.5. Delete All Users 42
3.4. Network settings 43
3.4.1. Terminal ID 43
3.4.2. Connection mode 43
3.4.3. Connection method 44
3.4.4. IP address 44
3.4.5. Subnet mask 44
3.4.6. Gateway 45
3.4.7. Server IP 45
3.4.8. Server port 45
3.5. Option settings 46
3.5.1. Application mode 46

Contents

3.5.2. Option settings for authentication 47
3.5.2.1. Settings for ID display when authentication is successful 47
3.5.2.2. Settings for only card authentication 48
3.5.2.3. 1:N authentication settings 48
3.5.3. Doorlock 49
3.5.3.1. Door opening time 49
3.5.3.2. Door status monitor 49
3.5.3.3. Door open alarm 50
3.5.4. Volume 50
3.5.4.1. Voice 50
3.5.4.2. Buzzer volume 50
3.5.4.3. Case open alarm 51
3.5.5. Current time 51
3.5.6. Other 51
3.5.6.1. LCD Backlight On/Off 51
3.6. Terminal information view 52
3.7. Extra functions 53
3.7.1. Terminal lock 53
3.7.2. Read card number 53
3.8. Device settings 54
3.8.1. Function key 54
3.8.2. Card reader 55
3.8.2.1. Card reader type setting 55
3.8.2.2. Card reader format setting 55
3.8.3. Fingerprint sensor 56
3.8.3.1. 1:1 verification level 56
3.8.3.2. 1:N identification level 56
3.8.3.3. Intelligent-Capture 56
3.8.4. Wiegand output 57
3.8.5. System configuration 58
3.8.5.1. User ID length 58
3.8.5.2. Language 58
3.8.6. Terminal initialization 59
3.8.6.1. Configuration settings initialization 59
3.8.6.2. Authentication record initialization 59
3.8.6.3. Factory default initialization 59
4. How to use 60
4.1. Access control application 60
4.1.1. Authentication mode 60
4.1.2. [1:1] fingerprint authentication 61
4.1.3. [1:N] fingerprint authentication 62
4.1.4. Password authentication 63
4.1.5. Card authentication 64
4.1.6. User ID group authentication 65
4.1.7. Multiple fingerprint authentication 66
4.2. Time & Attendance control 67
4.2.1. Authentication mode 67
4.2.2. Expansion of working mode by multi-key function 68
4.3. For using as meal management system 69
4.3.1. Meal Classification 69
4.3.2. [1:1] Fingerprint authentication 70
4.3.3. [1:N] Fingerprint authentication 70
4.3.4. Password authentication 70
4.3.5. Card authentication 70
4.3.6. User ID group authentication 70
4.3.7. Allowing multiple authentication 71

1. Before using

1.1. Safety precautions

☐ Under no circumstances will Union Community be responsible for accidents or damages caused by inappropriate use of the product caused by not referring to the user manual.

⚠Warning

⊘ Handling with wet hands or allowing liquid to flow into it is not advised.



It may cause an electric shock or damage.

⊘ Do not disassemble, repair, or modify the terminal at discretion.



It may cause an electric shock, fire or damage.

⊘ Do not place a fire source near the terminal.



It may cause a fire.

⊘ Keep out of reach of children.



It may cause an accident or damage.

⚠ Safety

If the above warnings are ignored, it may result in death or serious injury.

⚠ Cautions

If the above cautions are ignored, it may result in property loss or human injury.

⊘ The sign is a “Prohibition”

Ⓘ The sign is that user should keep the manual

1. Before using

⚠Cautions

Avoid using insecticide or flammable spray near the terminal.

It may result in deformation or color change.



Avoid high humidity or dust.

The terminal may be damaged.



Avoid severe temperature changes.

The terminal may be broken.



Avoid using water, benzene, thinner, or alcohol for cleaning.

It may cause an electric shock or fire.



Do not place a magnet close to the terminal.

The terminal may break down or malfunction.



Avoid impacts or using sharp objects on the terminal.

The terminal may be damaged and broken.



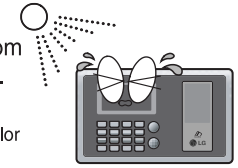
Do not contaminate the fingerprint input area.

Fingerprints may not be well recognized.

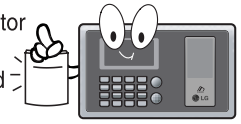


Keep away from direct sunlight.

It may cause deformation or color change.



Read the operator manual, any damage caused due to misuse will be the user's liability.



1. Before using

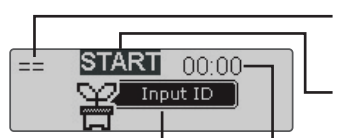
1.2. Terminal description



No	item		description
❶	LCD		Display character message for all the operations
❷	Key pad	F1 F2 F3 F4	[F1] : Start, [F2] : Leave, [F3] : Outside work, [F4] : Come back
		1 2 3 4 5 6 7 8 9	Input digits (1~9)
		0	Enter '0' or LCD menu scroll
		*	Terminal menu setting (Enter into menu mode for terminal menu setting when pressed over 2 seconds)
		#	- Clear typo when entering settings - Move up to higher menu - Use when escaping from menu setting
❸	Enter, Call	Enter	Use after entering the settings when configuring the terminal environment
		Call	Visitors use this to ring the interphone bell
❹	Micro phone		Convey visitor's voice to door phone
❺	LED Lamp		Show operation status like power supply, Lock status and card contact
❻	Fingerprint input window		Fingerprint input
❼	IRED sensor		Person's approach makes it automatically turn on button LED and LCD window with ID input screen
❽	Card input area		Card input
❾	Speaker		Voice output

1. Before using

1.3. Screen description



== Connected to network server
→← Disconnected to network server

Access mode display in case of access control (F1, F2, F3, F4)
T&A mode display in case of time & attendance control (START, LEAVE, OUT, BACK, NORMAL)

Current time

Information message



- Initial screen.



- Waiting for a user's ID to be input.



- Fingerprint input.



- When a non-registered user ID is entered.
- When connection mode is SN and 1:N identification is tried even though there is no user allowed for 1:N identification.



- Password input.



- Successful authentication.



- Authentication failed.



- Terminal program is in upgrade. (Power must not turn off when this message is displayed.)



- There is no user registered on the terminal or no connection to the server, so it is trying to connect.



- Waiting for a reply from the server for authentication.



- A registered user tried authentication at that time when access is not allowed.



- There is no response from the server during the authentication process.
- Network to server is disconnected during the authentication process.



- Terminal is locked.
- It is not mealtime in case of meal control mode.

1. Before using

1.4. Voice information

“Please enter your fingerprint”	Enter fingerprint using the fingerprint input window
“You are authorized”	Successful authentication
“Please try again”	Authentication failed

1.5. Buzzer sound

“ppig”	When a button is pressed or a card is being read. When fingerprint input is completed and user is allowed to take off his fingertip
“ppibig”	Authentication is failed or wrong user fingerprint input happened.
“ppiriririck”	Waiting for fingerprint input
“ppiririck”	Authentication is successful or settings for the current user are completed.

1.6. LED signal

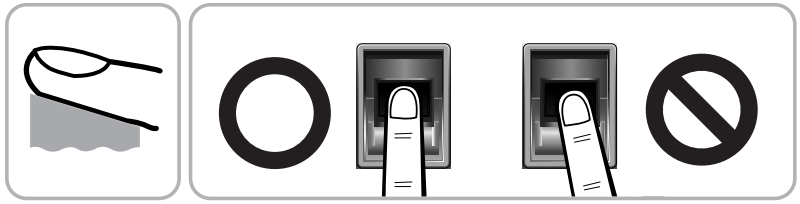
POWER LED : Power on/off
DOOR LED : Door open/close
CARD LED : Card contact

1. Before using

1.7. Correct fingerprint registration and input methods

☐ Correct fingerprint registration methods

Place your index finger on the window just as you do with a finger stamp.Finger tip touching is not an appropriate registration or input method. Make sure the center of your finger touches the window.



☐ Use your index finger, if possible.

As usual, the index finger guarantees an accurate and stable fingerprint input.

☐ Check if your fingerprint is unclear or damaged.

It is tricky to recognize fingerprints on dry, wet, unclear, or injured fingers. Use another finger in this case.



1. Before using

1.7. Correct fingerprint registration and input methods

□ Cautions about fingerprint condition

Depending on the user's fingerprint condition, some fingerprints may not be used or may cause an inconvenience.

- If the fingerprint is damaged or very unclear, then it cannot be recognized. Please use a password instead in this case.
- When a finger is dry, breathe on the finger for smooth operation.
- For kids, it may be tricky or impossible to use the terminal because their fingerprints are too small or very unclear. It is recommended to register their fingerprints every six months.
- For the elderly, it may not be possible to register their fingerprints if there are too many fine lines on the fingerprints.
- If fingerprints are very unclear, it may be convenient if you register 2~3 fingerprints.
- It is recommended that you register more than 2 fingerprints.

2. Introduction

2.1. Features

☐ **Access control system using LAN**
- Communication between the unit and authentication server is done through a UTP cable and TCP/IP protocol, so an existing LAN can be used as it is. It guarantees network-based administration and monitoring as well as easy expansion, high reliability, and higher speed.

☐ **Convenient auto sensing function**
- Simple authentication process without any key input simple fingerprint touching is sufficient.

☐ **Simple authentication using fingerprints**
- Fingerprint authentication technology prevents users from forgotten password or card, stolen key or card, etc., which is one of good ways to improve security level.

☐ **High processing capacity of terminal and server**
- There is not any limit on management of user's access information in case that access server is used. Even in standalone operation by using local terminal, it is possible to manage fingerprint authentication of more than 8,000 users (in optional case).

☐ **Various information messages**
- It ensures easy fingerprint recognition because voice and LCD window information are provided during the authentication process. In addition, the backlight installed in the LCD window helps with easy key operation in the dark.

☐ **Door phone**
- Easy visitor identification and convenient response.

☐ **Various and flexible access controls**
- No risk of rent, forgery, or loss of keys or cards.
- Perfect control by assigning different security clearances to each user or group.
- Flexibility provided by allowing limited time for entry/exit.
- Low maintenance.
- No need to issue visitor card for visitor.

2. Introduction

2.1. Features

□ Various applications including access control, time & attendance, etc.

- Various operation modes depending on the terminal menu settings.

□ Enhanced security with detection of fake finger

- Adopted detection technology of fake finger enhances security level.

□ Various registration and authentication methods

- There are a total of 11 registration and authentication methods (4 methods if the card reader is not installed), so you are required to select one method before registering users and an administrator.

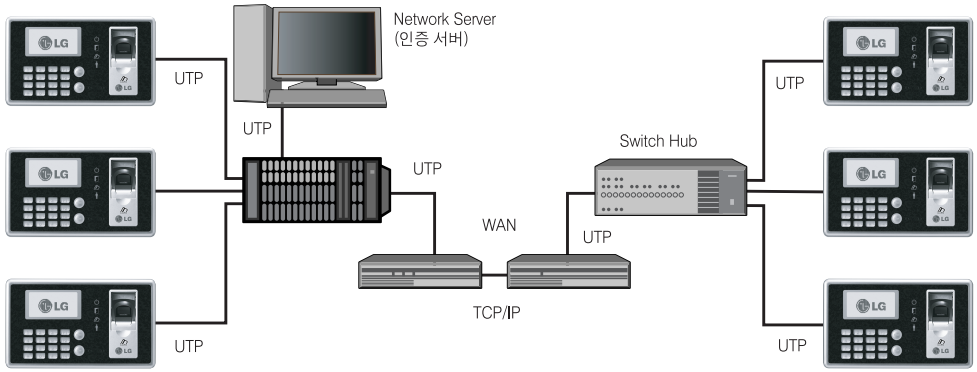
registration	registration and authentication method
FP	Fingerprint registration. Fingerprint authentication.
ID&PW	Password registration. Password authentication after ID input.
FP|PW	Fingerprint and password registration. Fingerprint or password authentication.
FP&PW	Fingerprint and password registration. Password authentication after fingerprint authentication.
RF	Card registration. Card authentication
RF|FP	Card and fingerprint registration. Card or fingerprint authentication
RF&FP	Card and fingerprint registration. Fingerprint authentication after card authentication.
RF|PW	Card and password registration. Card or password authentication.
RF&PW	Card and password registration. Password authentication after card authentication.
ID&FP|RF&FP	Card and fingerprint registration. Fingerprint authentication after ID input or fingerprint authentication after card authentication.
ID&PW|RF&PW	Card and password registration. Password authentication after ID input or password authentication after card authentication.

※ RF defines '125KHz Proximity Card' or '13.56MHz Smart Card'.

2. Introduction

2.2. Configuration

☐ Network configuration



☐ Standalone configuration



3. Configuration settings

3.1. Check items before device configuration settings

3.1.1. Entering menu

The following screen appears when **[*] is pressed for over 2 sec.**

1. User
2. Network
3. Option
4. Terminal Info
5. Ext Function
6. Device

- Press [0] to view menus not shown in the LCD window.
- Press a number key in order to go submenu. The following administrator authentication allows for entry of submenu.

<Input Admin ID>
ID : 0001

- Press [ENTER] after entering the administrator's ID, and the administrator authentication is processed according to the previous setting such as fingerprint authentication or password authentication. If the authentication succeeds, submenu screen appears.

※ Administrator authentication is required only once for all in main menu, so all other menus are accessible until he/she completely exits from the main menu.

3. Configuration settings

3.1.2. Changing setting parameters

To change setting parameters, press [#] to delete old values and input new values.

Press [0] to see menus not shown in the LCD window, and press the corresponding number to select a menu.

Press [ENTER] for confirmation of setting parameter or to move to the next setting, and press [#] to move to upper menus.

Hold [#] for over 2 sec. to cancel the current setting and move to the upper menu.

3. Configuration settings

3.1.3. Saving device configuration settings

Press [#] in the main menu to save device configuration settings.
The following screen appears:



Save?
[Y=1/N=2] : _

Press [1] to save changes.
If not, press [2].



If there are no changes in device configuration settings, it goes out of this setting mode without going through the above screen.

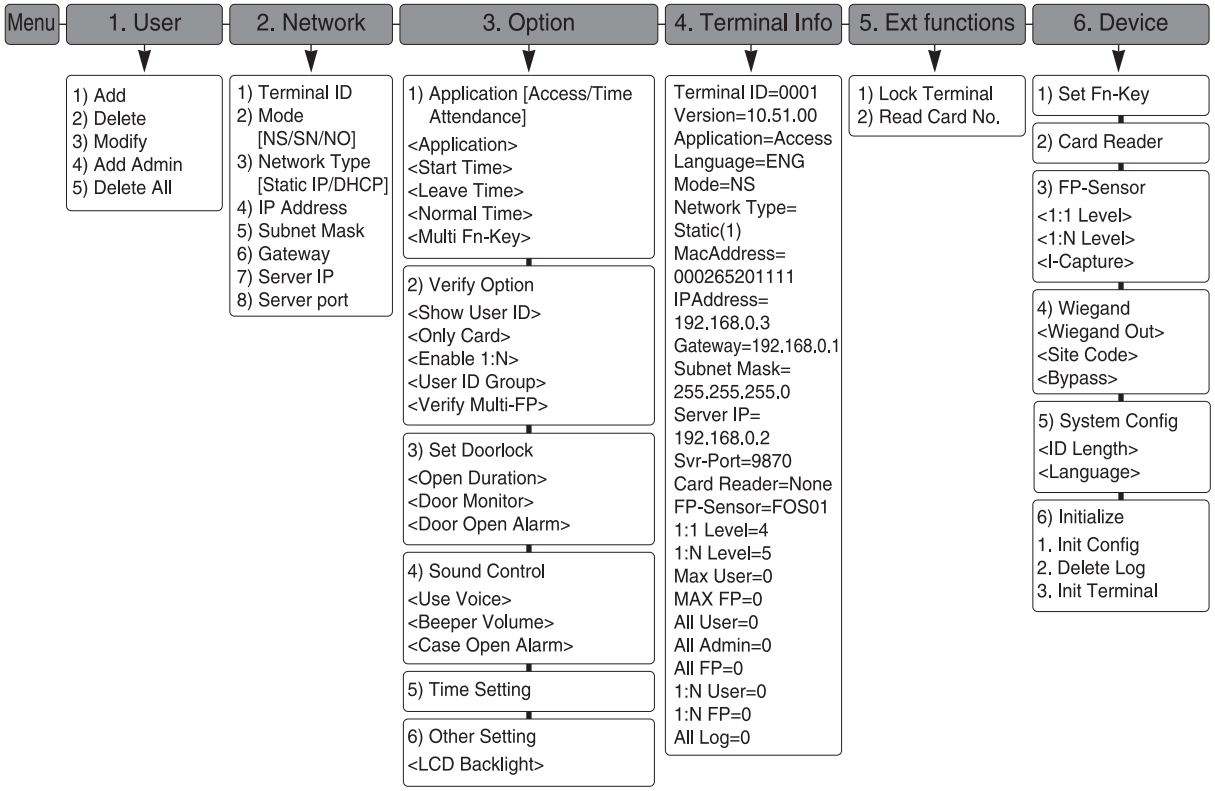


If there is no input for a certain period of time while changing the device configuration settings, the setting process finishes. If there are changes in device configuration settings, the above screen “Save?” appears. If not, it goes out of this setting mode and the initial screen appears.

3. Configuration settings

3.2. Menu configuration

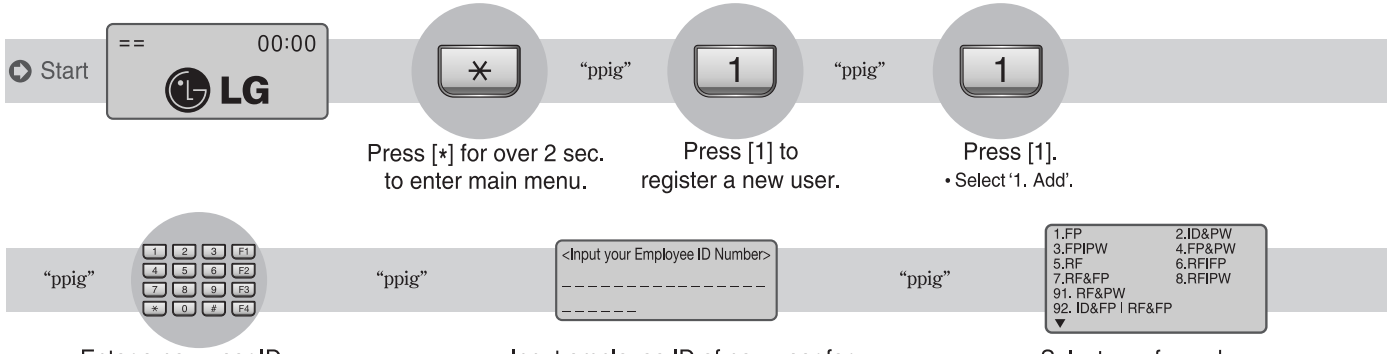
□ Press [*] for over 2 sec. to enter the menu.



3. Configuration settings

3.3. User account

3.3.1. User registration



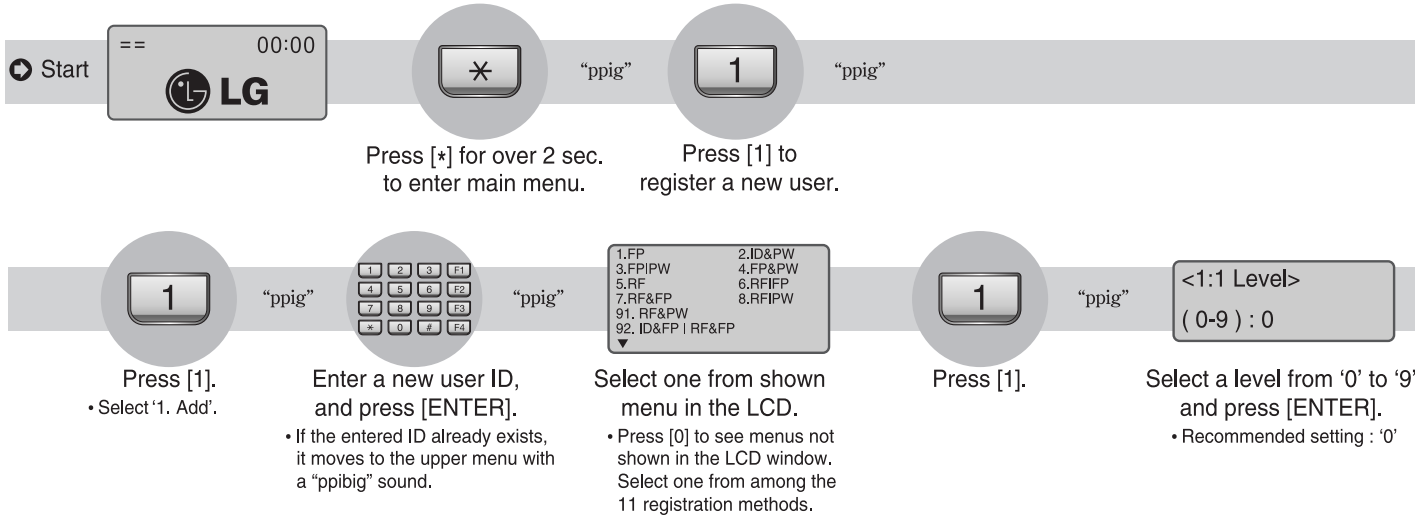
※ ID basically consists of four digits and is changable from two digits to eight digits at ‘3.8.5.1 User ID length’.

※ Employee ID can be available as User ID for more than 8 digits of User ID or using English Employee ID (Maximum 20 digits).
※ When using Employee ID number as User ID, User ID can be input in the terminal only if Employee ID Number consists of numbers only.

3. Configuration settings

3.3.1.1. ‘1. FP’ registration

□ Fingerprint registration and fingerprint authentication.



3. Configuration settings



Select '0' or '9' and press [ENTER].

- The default is '0'. To enable 1:N authentication, it should be set to '1'.

Since red light is on in fingerprint input window, hold the finger for about 3 sec. on the sensor until light is off.

Place the same finger again on the sensor since red light flickers - red light is off and on.

- If succeeds, it ends.
- If fails, it returns to the '1. Add' screen.

※ **1:1 Level :** A Different authentication level can be assigned to respectively different users. If the authentication level for a user is set to '0', the authentication level for the terminal is changed, the applied authentication level for all users respectively set to '0' is simultaneously changed.

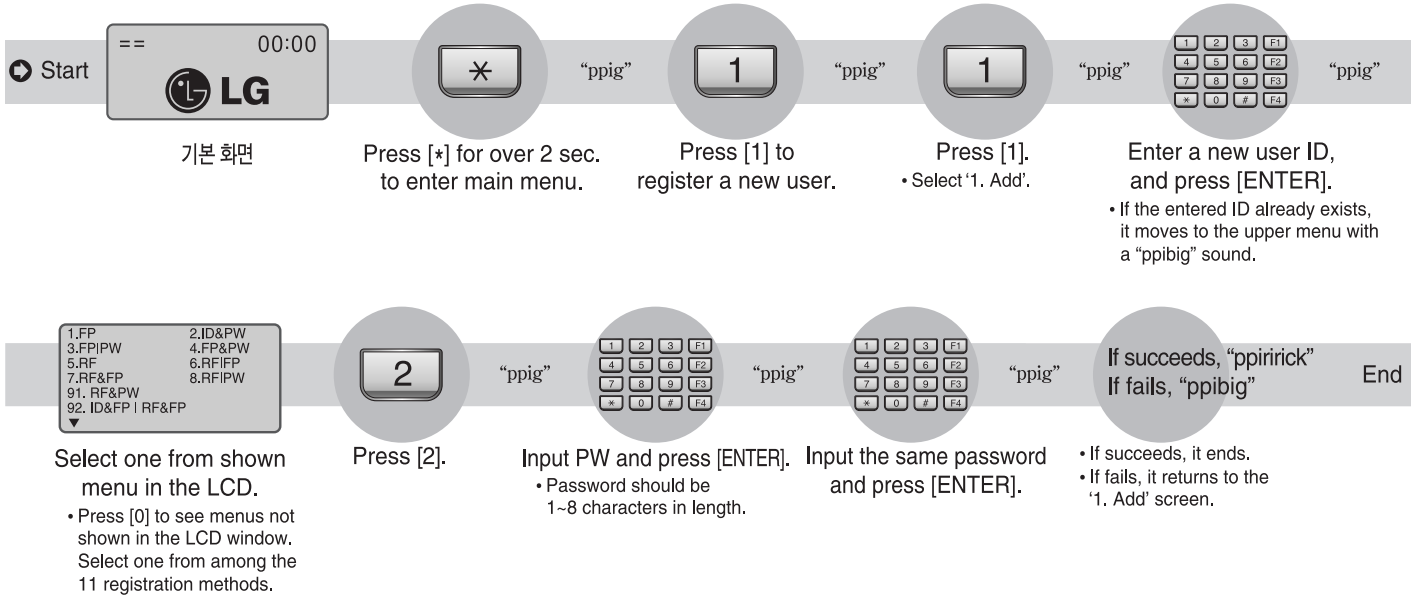
※ **Enable 1:N :** In case that there are not many users or for the convenience of a specific user, a fingerprint only without ID can be used for authentication. For authentication without ID, it shall be set to '1'. For authentication with ID, it shall be set to '0'.

※ **Add FP :** A "ppiriririck" buzzer sound rings twice and a light on the fingerprint sensor turns on. Place a finger onto the fingerprint input window and wait for 2~3 seconds until the light turns off and the fingerprint is saved.Please note that the same fingerprint must be inputted twice. To enter the same fingerprint again, remove the finger from the window and place the same finger again onto the window. If registration succeeds, a "ppiririck" buzzer sound rings. Then, it returns to the "1.Add" screen. If the fingerprint image is not in good conditions or there is no input in the window for 10 seconds after the fingerprint sensor light turns on, it returns to the "1. Add" screen with a failure buzzer sound "ppibig". In case that the fingerprint to be registered is in bad conditions, repeat to try the registration process more than 2 or 3 times or register other fingerprint. For remarkably few people having fingerprints in bad conditions which are not properly accepted for registration process, it is recommended to use a password for authentication.

3. Configuration settings

3.3.1.2. '2. ID&PW' registration

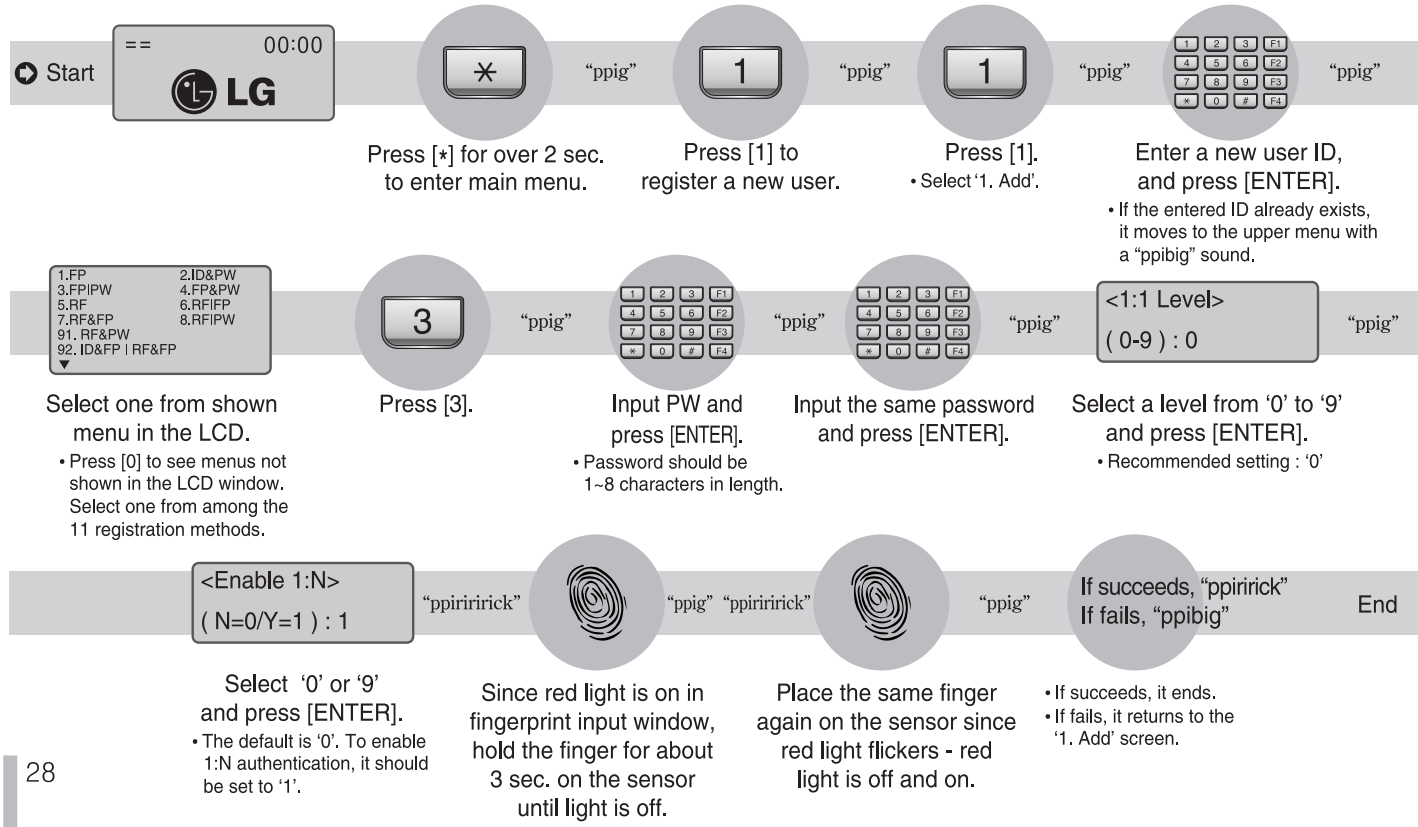
□ Password registration and password authentication for a user.



3. Configuration settings

3.3.1.3. '3. FP|PW' registration

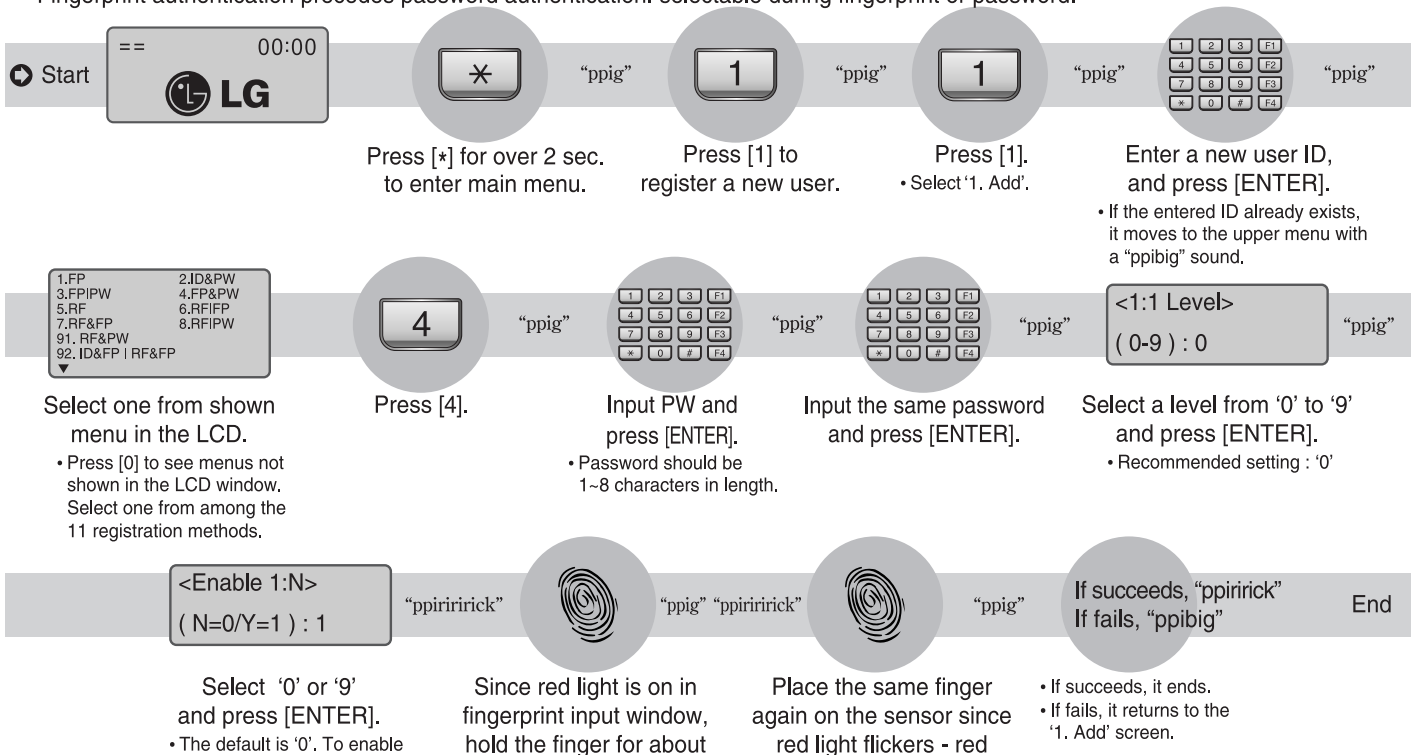
□ After both fingerprint and password are registered, authentication method is selectable during fingerprint or password.



3. Configuration settings

3.3.1.4. '4. FP&PW' registration

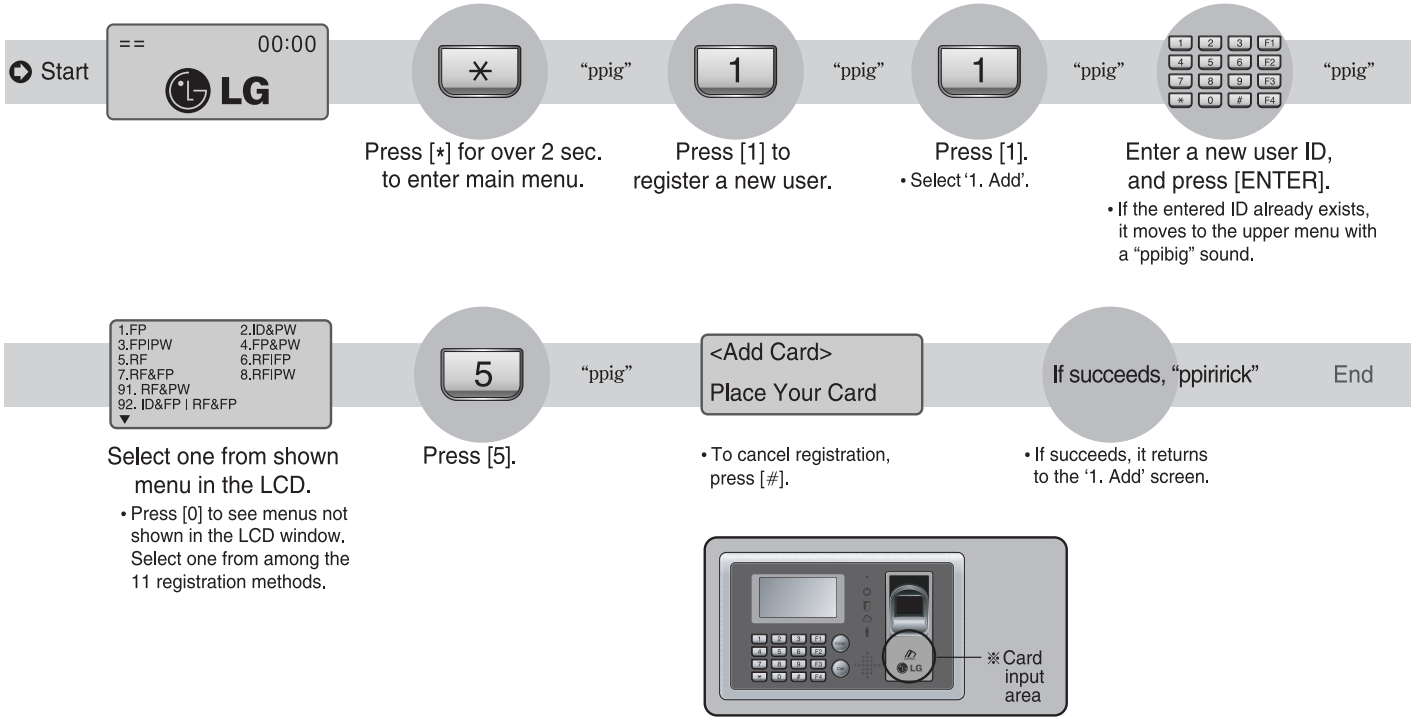
□ After both fingerprint and password are registered, fingerprint authentication and password authentication should be done for access. Fingerprint authentication precedes password authentication. selectable during fingerprint or password.



3. Configuration settings

3.3.1.5. '5. RF' registration

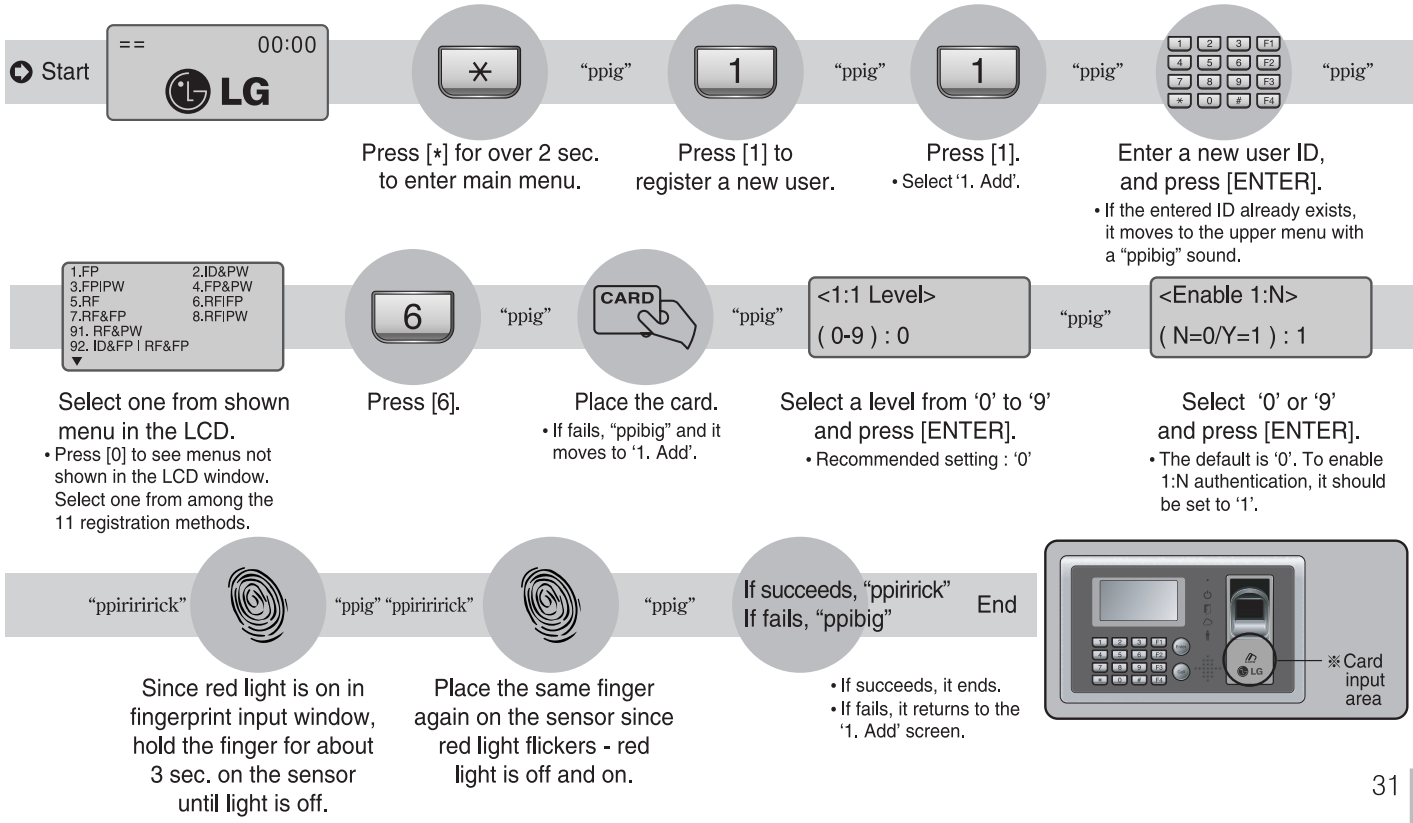
□ Card registration and card authentication.



3. Configuration settings

3.3.1.6. '6. RF|FP' registration

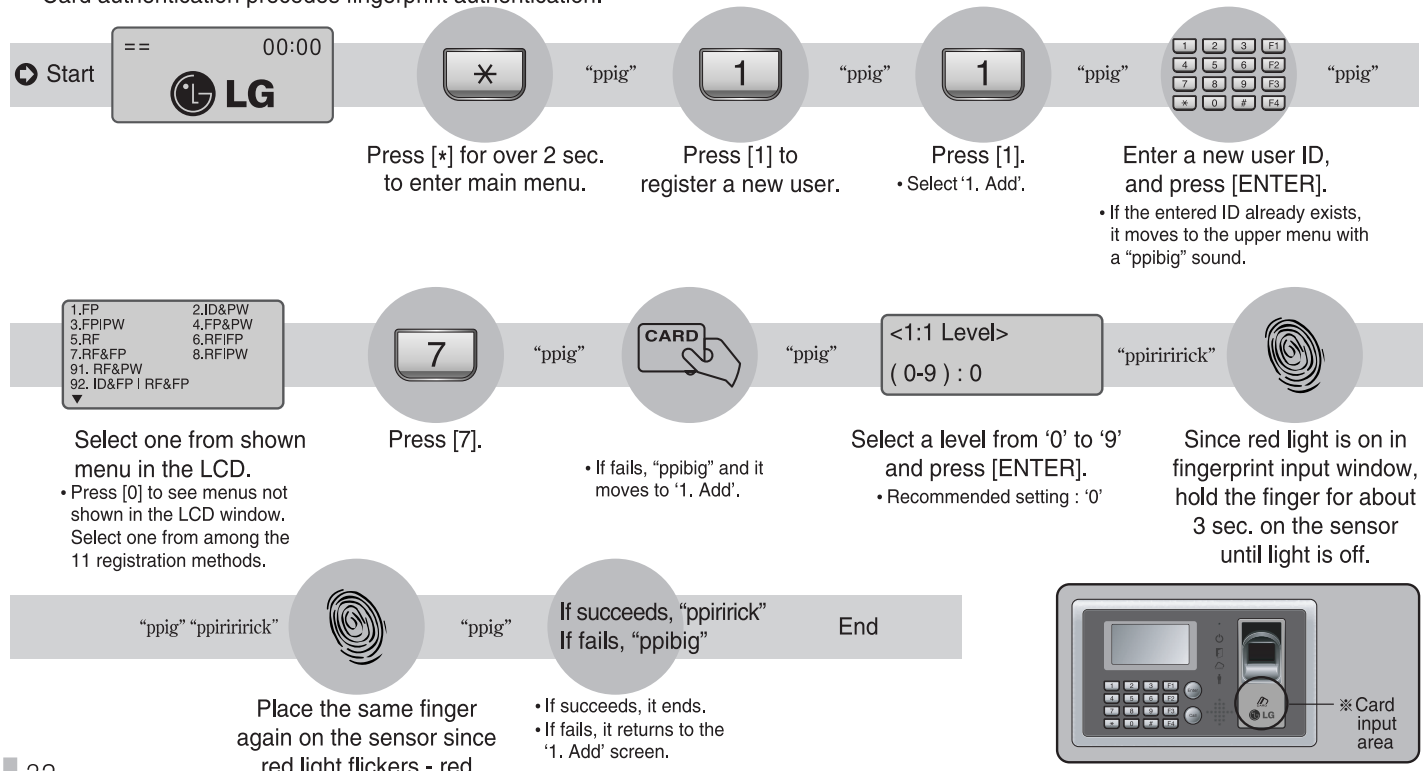
□ After both card and fingerprint are registered, authentication method is selectable during card or fingerprint.



3. Configuration settings

3.3.1.7. '7. RF&FP' registration

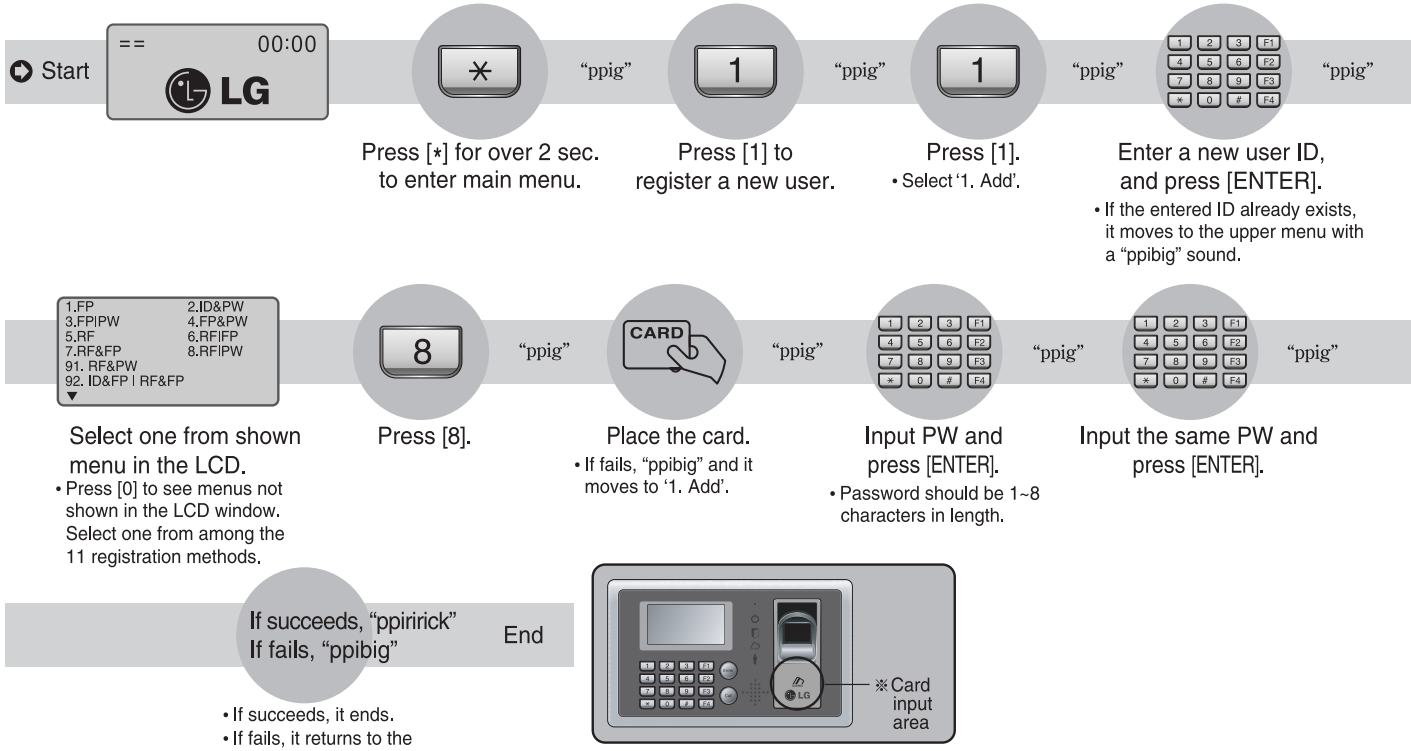
☐ After both card and fingerprint are registered, card authentication and fingerprint authentication should be done for access.
Card authentication precedes fingerprint authentication.



3. Configuration settings

3.3.1.8. '8. RF|PW' registration

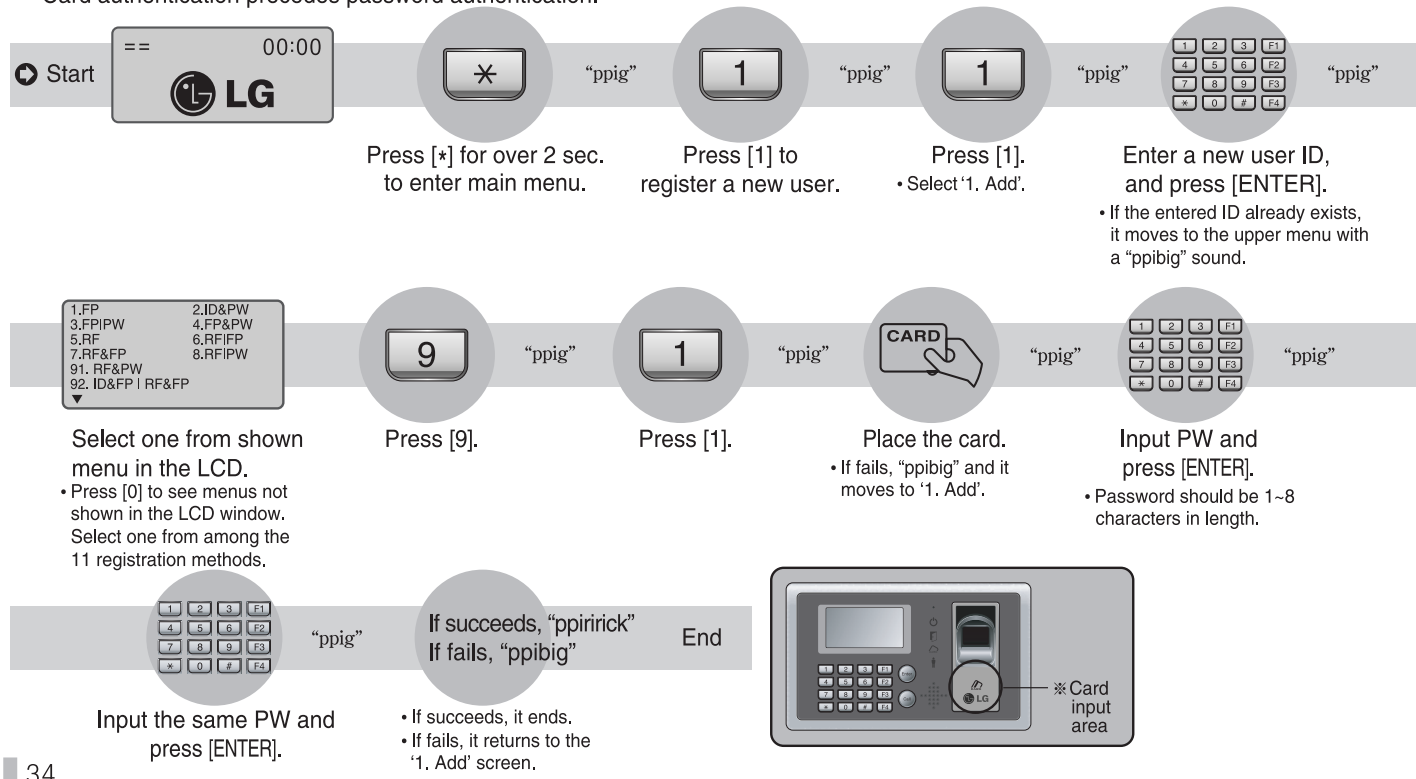
□ After both card and password are registered, authentication method is selectable during card or password.



3. Configuration settings

3.3.1.9. '91. RF&PW' registration

□ After both card and password are registered, card authentication and password authentication should be done for access. Card authentication precedes password authentication.

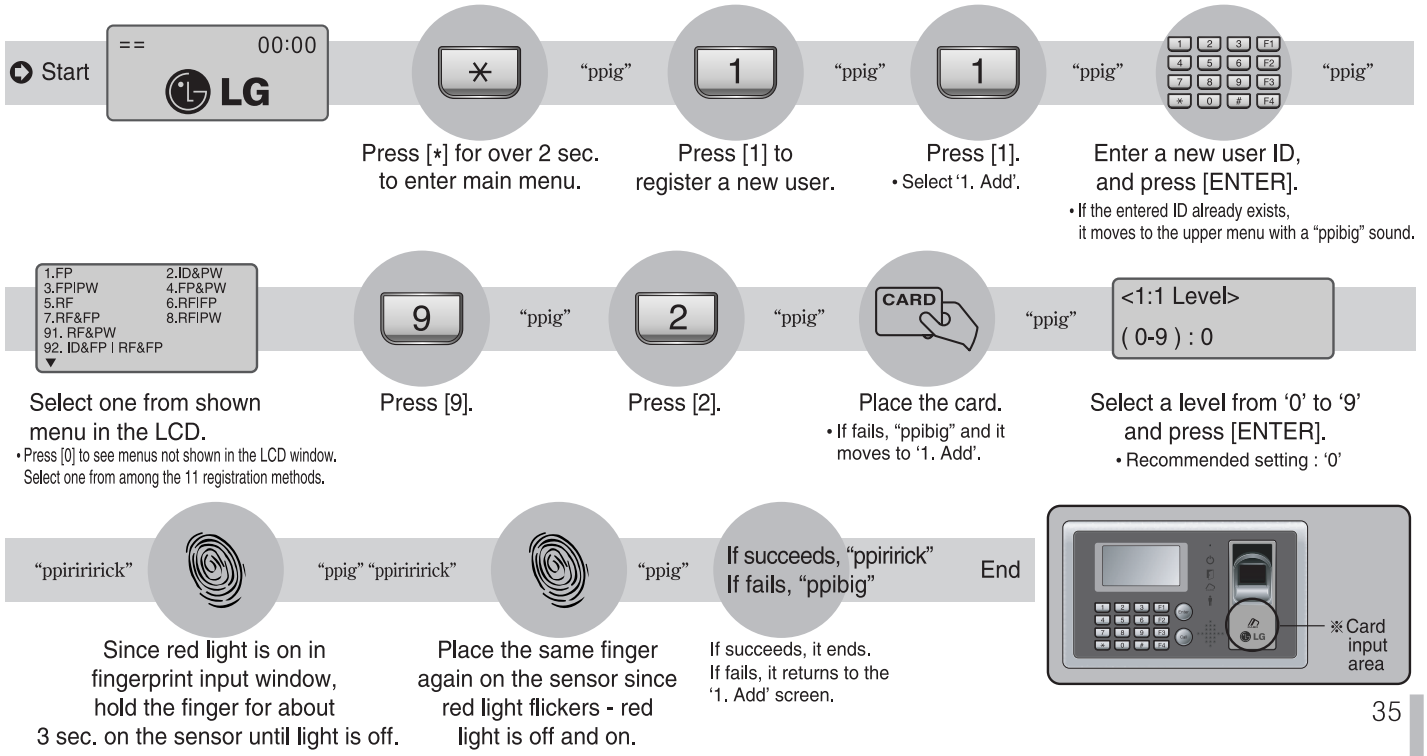


3. Configuration settings

3.3.1.10. '92. ID&FP|RF&FP' registration

☐ After both card and fingerprint are registered, authentication method is selectable during ID and fingerprint authentication or card and fingerprint authentication.

☐ If a user feels difficult in inputting ID, a card can be used instead of ID input for authentication.

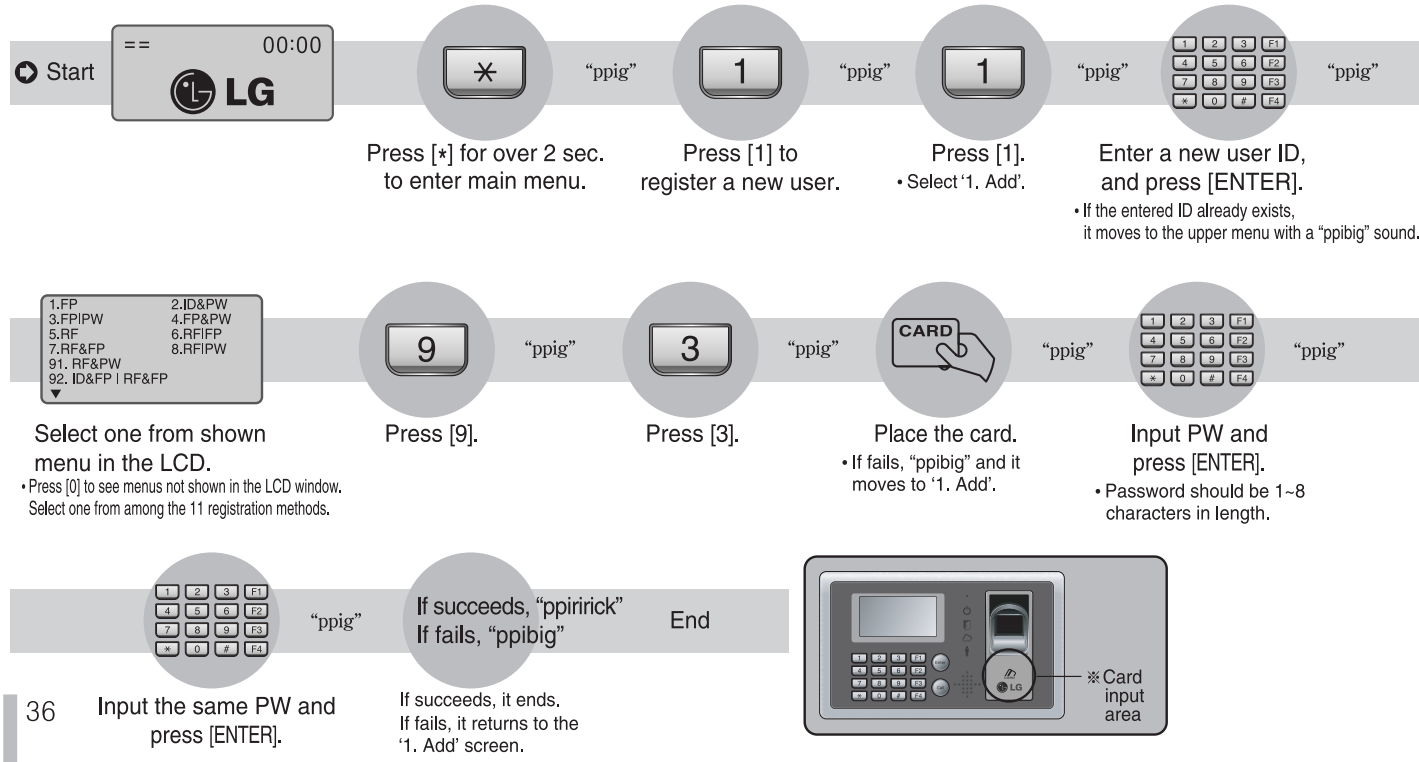


3. Configuration settings

3.3.1.11. '93. ID&PW|RF&PW' registration

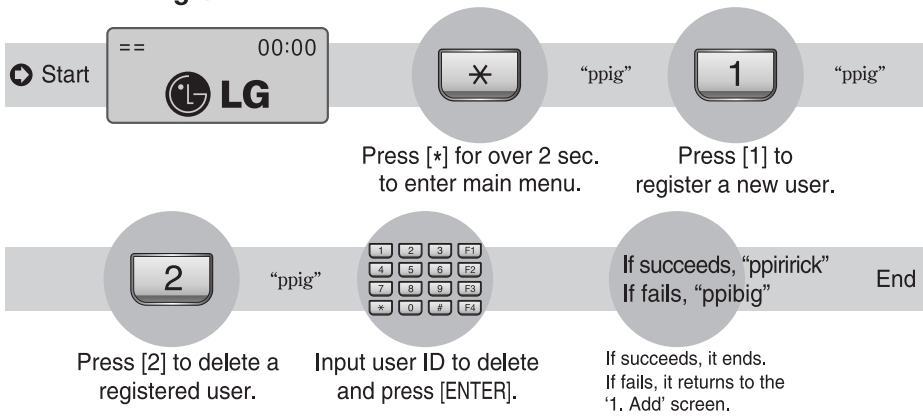
☐ After both card and password are registered, authentication method is selectable during ID and password authentication or card and password authentication.

☐ If a user feels difficult in inputting ID, a card can be used instead of ID input for authentication.



3. Configuration settings

3.3.2. Deleting User



※ After entering the user ID to be deleted, press [ENTER]. All the information about the user in the local terminal is deleted together with a "ppiririck" buzzer sound. However, the information about the user is still stored in the server. To completely delete this information, the data in the server should be deleted.

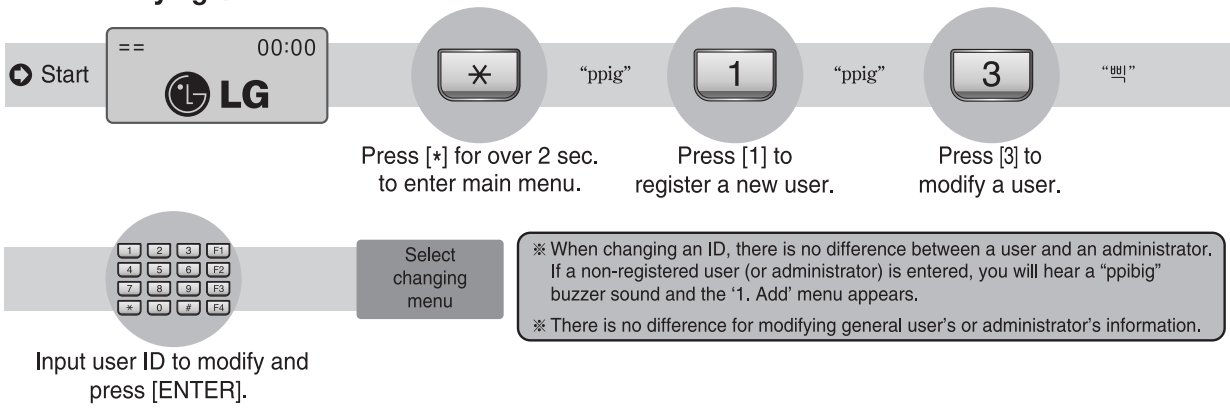
※ If a non-registered user ID is entered, '2.Delete' appears together with a "ppibig" sound.

1. Add
2. Delete
3. Modify
4. Add Admin
5. Delete All

※ Caution is required when deleting a user or an administrator as there is no differential procedure for deleting their information. Also, carefully note that user's information stored just in the local terminal-not in the server-is not recoverable after deletion is completely done.

3. Configuration settings

3.3.3. Modifying User



3.3.3.1. '1. FP' user

1. 1:1 Level
2. Add FP

<1:1 Level>
(0-9) : 0

<Add FP>
Input Your FP

Default screen ⇨ [*] ⇨ [1] ⇨ [3] ⇨ [ID]+[ENTER] ⇨ [Select changing menu]

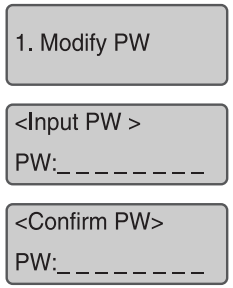
- To change the authentication level, press [1]. To add a fingerprint to the corresponding ID, press [2].
- A maximum of 5 fingerprints can be added to an ID. If there is an attempt to add more than 5 fingerprints, a "ppibig" buzzer sound rings when [2] is pressed.
- 'Fingerprint registration' user

1) When modifying 1:1 authentication level is selected.
   - Recommended setting : '0'
   - To change this value, press the [#] to delete the current value and enter the new value.

2) When registering additional fingerprints is selected.
   - This is same as 'Add FP' in 3.3.1.1. '1. FP' registration. The same fingerprint must be inputted twice.
   - If additional fingerprint registration succeeds, a "ppiririck" buzzer sound rings. If not, a "ppibig" buzzer sound rings and the '1. Add' menu appears.

3. Configuration settings

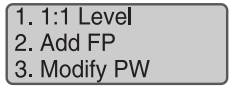
3.3.3.2. '2. ID&PW' user



Default screen ➔ [*] ➔ [1] ➔ [3] ➔ [ID]+[ENTER] ➔
[Select changing menu]

- To modify a password, press [1].
  - Input password. Password should be 1~8 characters in length.
  - Press [ENTER] after inputting the password.
  - Input the same password once more for confirmation.
    Press [ENTER] to confirm the password.
- To cancel this operation, press [#].
- If password modification succeeds, a "ppiririck" buzzer sound rings.
  If not, a "ppibig" buzzer sound rings and the
  "1. Add" menu appears.

3.3.3.3. '3. FP|PW', '4. FP&PW'user



Default screen ➔ [*] ➔ [1] ➔ [3] ➔ [ID]+[ENTER] ➔
[Select changing menu]

- Press [1] to modify the 1:1 Level (refer to '3.3.3.1').
- Press [2] to register additional fingerprints
  (refer to '3.3.3.1').
- Press [3] to modify password (refer to '3.3.3.2').
- To cancel, press [#].

3.3.3.4. ‘5. RF’ user

1. Change Card

Change Card>
Place Your Card

Default screen ➪ [*] ➪ [1] ➪ [3] ➪ [ID]+[ENTER] ➪ [Select changing menu]

- To change the card, press [1].
- To cancel, press [#].
- If a user places the card close to the unit, a “ppiririck” buzzer sound in case of successful modification rings and the ‘1. Add’ menu appears.

3.3.3.5. ‘6. RF|FP’, ‘7. RF&FP’, ‘92. ID&FP|RF&FP’ user

1. 1:1 Level
2. Add FP
3. Change Card

Default screen ➪ [*] ➪ [1] ➪ [3] ➪ [ID]+[ENTER] ➪ [Select changing menu]

- Press [1] to modify the 1:1 Level (refer to ‘3.3.3.1’).
- Press [2] to register additional fingerprints (refer to 3.3.3.1).
- Press [3] to change the card (refer to ‘3.3.3.4’).
- To cancel, press [#].

3.3.3.6. ‘8. RF|PW’, ‘91. RF&PW’, ‘93. ID&PW|RF&PW’ user

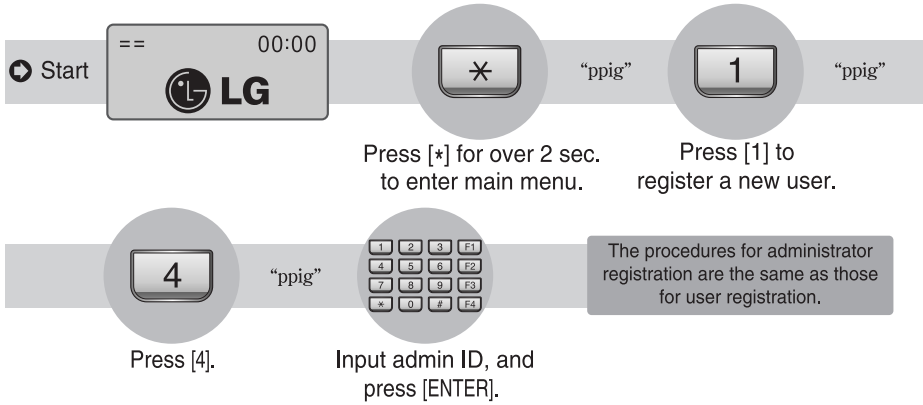
1. Modify PW
2. Change Card

Default screen ➪ [*] ➪ [1] ➪ [3] ➪ [ID]+[ENTER] ➪ [Select changing menu]

- Press [1] to modify password (refer to ‘3.3.3.2’).
- Press [2] to change the card (refer to ‘3.3.3.4’).
- To cancel, press [#].

3. Configuration settings

3.3.4. Administrator registration

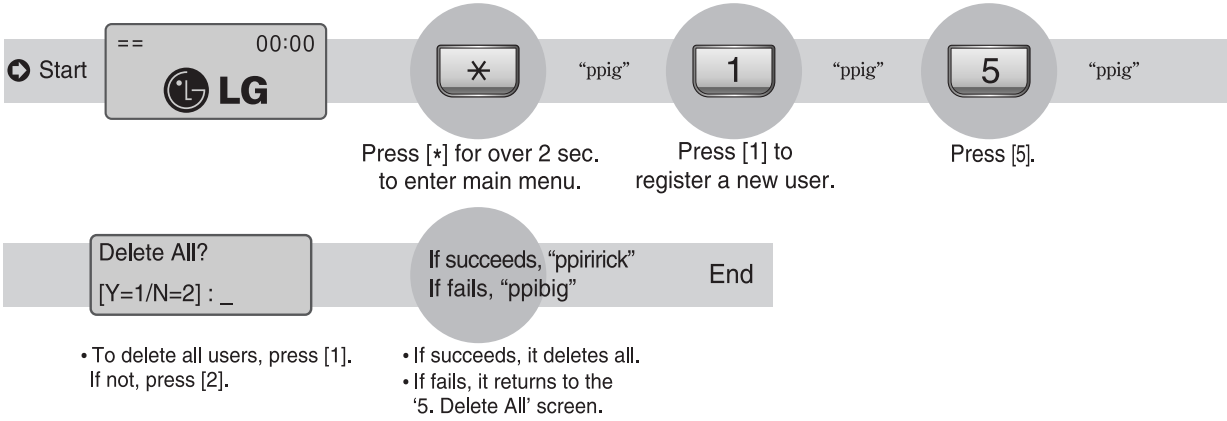


※ ID basically consists of four digits and is changable from two digits to eight digits at '3.8.5. System configuration setting'.

※ Be careful to register new administrator as the registered administrator can change the terminal configuration settings including registration/modification/deletion of user information.

3. Configuration settings

3.3.5. Delete All Users



※ Special care is required because all user accounts including the administrator are deleted with this operation.

3. Configuration settings

3.4. Network settings

□ In the main menu, press [2] to select '2.Network' to see the following screen.
When this setting is done, press [ENTER] to move to the next setting.

3.4.1. Terminal ID

<Terminal ID>
ID: 00000001

• Press [ENTER] to move to the next setting.

Default screen ➔ [*] ➔ [2]

- This ID is unique for each terminal and used by an authentication server to distinguish each terminal. The default is '00000001'.
- It should be identical to the door ID set in the server program and its length should be 1~8 characters.
- If the terminal ID is '1000', enter [1][0][0][0] in sequence. If it is '0001', enter only '1'.

3.4.2. Connection mode

Mode [NS/ SN/ NO]
(0-2) : 0

• Press [ENTER] to move to the next setting.

Default screen ➔ [*] ➔ [2] ➔ [ENTER]

- This defines where the priority for authentication is between the local terminal and network server, and the default is '0' (NS). There are three different modes as follow:

mode	button	description
NS	[0]	If the local terminal is properly connected to network server, authentication is done in the server. In case of disconnection between local terminal and network server due to network troubles or others, it is done in the local terminal.
SN	[1]	Even though the local terminal is properly connected to network server, the authentication is done in the local terminal and its result is transmitted to network server in real time. However, if the user ID entered for 1:1 authentication does not exist in the local terminal, the relevant authentication is tried in network server.
NO	[2]	The authentication operation is done only in network server.

3. Configuration settings

3.4.3. Connection method

Network Type:0 0:Static 1:DHCP

- Press [ENTER] to move to the next setting.

Default screen ➪ [*] ➪ [2] ➪ [ENTER] ➪ [ENTER]

- Press [0] for Static IP, the default is '0'.
- Press [1] for DHCP.
- For static IP settings, refer to '3.4.4. IP address', '3.4.5. Subnet mask' and '3.4.6. Gateway'. In case of dynamic IP, there is no need for additional settings.

3.4.4. IP address

<IP Address> 192.168.0.3

- Press [ENTER] to move to the next setting.

- Press [#] to delete an old IP and enter the new IP.
- If the IP address is '210.98.100.50', enter as below:
  [2] [1] [0] [9] [8] [*] [1] [0] [0] [5] [0]

3.4.5. Subnet mask

<Subnet Mask> 255.255.255.0

- Press [ENTER] to move to the next setting.

- Press [#] to delete an old value and enter the new value.
- If the subnet mask is '255.255.255.0', enter as below:
  [2] [5] [5] [2] [5] [5] [2] [5] [5] [0]

3. Configuration settings

3.4. Network settings

3.4.6. Gateway

<Gateway>
192.168.0.1

- Press [ENTER] to move to the next setting.

- Press [#] to delete an old value and enter the new value.
- If the gateway IP address is '210.98.100.1', enter as below:
  [2] [1] [0] [9] [8] [*] [1] [0] [0] [1]

3.4.7. Server IP

<Server IP>
192.168.0.2

- Press [ENTER] to move to the next setting.

- Press [#] to delete an old value and enter the new value.
- If the sever address is '210.98.100.121', enter as below:
  [2] [1] [0] [9] [8] [*] [1] [0] [0] [1] [2] [1]

3.4.8. Server port

<Server port>
Num : 2201

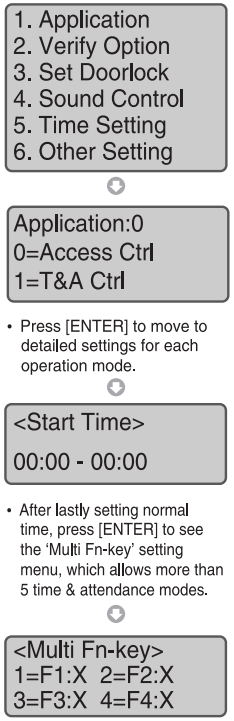
- After the network setting is completely done, press [ENTER] to return to the main menu.

- Press [#] to delete an old value and enter the new value.
- As the port number of the authentication server, the default is '2201'. Special care is required when changing this number because the corresponding number in the server should also be changed with the same number.
- If the server port is '2201', enter as below:
  [2] [2] [0] [1]

3. Configuration settings

3.5. Option settings

3.5.1. Application mode



Default screen ➪ [*] ➪ [3] ➪ [1]

- The default is '0=Access Ctrl'
- For access control application, set as '0'. For time & attendance, set as '1'.
- Access control
  - There are no detailed settings under access control application here. It moves to the upper menu.
- Time attendance control
  - By setting up those default times regarding Start/Leave/Out/Back, the terminal display mode after authentication can be automatically changed to programmed time & attendance mode. In addition, by using multi-Fn key, over 40 sub modes of time & attendance can be defined.
  - If time setting is not necessary, set as '00:00-00:00'
  - To change the start time from '00:00~00:00' to '06:00~09:59', press [#] to delete the existing setting time, and enter [0] [6] [0] [0] [0] [9] [5] [9] in sequence.
  - As long as no other function button is pressed during the setting time, it operates in start time mode. Even if the authentication for outside work (Out) happens by pressing [F3] function key, the terminal display mode after the authentication of outside work is automatically changes to start time mode, which is very convenient for users in time & attendance mode.
  - After setting <start time>, set <leave time> and <normal time> in the same manner. Note that each time must not overlap. Ex.)start time : '06:00~09:59', leave time : '17:00~22:00' and normal time : '10:00~16:59'.
- Multi Fn-key
  - Default setting: all 'X'
  - This menu is useful when more than 5 time & attendance modes are necessary.
  - When setting as 'X' : each function key represents a specific working mode such as F1=Start, F2=Leave, F3=Outside work (out) and F4=Back. When a function key is pressed, authentication mode is changed to the corresponding working mode.
  - When setting as 'O' : a mode is defined by the combination of a function key and a number key such as 'F3+1'. For example, if the setting is 1=F1: X 2=F2: X 3=F3: X 4=F4: O, 14 different working modes can be defined according to user input such as [ENTER]: normal, [F1]: start, [F2]: leave, [F3]: outside work(out), and [F4]+'0' ~ [F4]+'9'.
  - The O/X setting can be changed by pressing the corresponding number key. After setting is completed, press [ENTER] to move to the upper menu.

3. Configuration settings

3.5.2. Option settings for authentication

1. Application
2. Verify Option
3. Set Doorlock
4. Sound Control
5. Time Setting
6. Other Setting

Default screen ➔ [*] ➔ [3] ➔ [2]

- To set the basic option for authentication, press [2].

3.5.2.1. Settings for ID display when authentication is successful

<Show User ID>
(N=0/Y=1):0

- Press [ENTER] to move to the next setting.

- Default setting : '0'
- If it is set to the default setting '0', only the 'Success' message is displayed. If it is set to '1', user ID is displayed in the LCD window when authentication is successful as shown below:
  (Ex.) OK! <0001>

3.5.2.2. Settings for only card authentication

<Only Card>
(N=0/Y=1):0

- Press [ENTER] to move to the next setting.

Default screen ➔ [*] ➔ [3] ➔ [2] ➔ [ENTER]

- Default setting : '0'
- Even if a user is registered to be authenticated with a card & password or a card & fingerprint, if it is set to '1', a user can get access to an area through the relevant terminal only by using a card.
- This function is useful at building entrance door - among other places of a building with several installed terminals - where there is frequent entrance and exit and there is no need for severe access control.

3. Configuration settings

3.5.2.3. 1:N authentication settings

<Enable 1:N>
(N=0/Y=1):0

Default screen ➔ [*] ➔ [3] ➔ [2] ➔ [ENTER] ➔ [ENTER]

- Default setting : '1'.
- This enables fingerprint authentication without inputting a user ID or placing a card. For your information, even if a user is registered to be authenticated with 1:N authentication, only 1:1 authentication is allowed in the terminal if this is set to '0'.
- In cases that ID input or fingerprint authentication after placing a card - when card input replaces ID input - is unavoidably needed, it should be set to '0'.
- The followings are detailed settings about whether 1:N authentication is allowed or not.

<User ID Group>
(N=0/Y=1):0

■ When 1:N authentication is allowed as setting of '1'

- Default setting : '0'.
- If this setting is set to '1', inputting fore part of ID digits stands for a specific group, which speeds up 1:N authentication by searching for same fingerprint only among the specific group. This faster matching speed is very useful in case that over 1,000 users are registered.
- If it is set to '1', as mentioned above, fingerprint matching is executed only among the user group starting with the same fore part of ID digits. If it is set to '0', inputted numbers is considered just as user's ID and only 1:1 authentication is executed.
- For example, when a user ID is a 4-digit number and '12' is inputted for authentication, if it is set to '1', 1:N authentication is performed among user IDs '1200'~'1299'. If it is set to '0', 1:1 authentication only for user ID No. 12 is performed.

<Verify Multi-FP>
(N=0/Y=1):0

■ When 1:N authentication is not allowed as setting of '0'

- Default setting : '0'.
- If it is set to '1', for successful authentication, all registered fingerprints should be authenticated after ID (or card) input.
- This is used when a high security level is required for special areas. If a user of 'ID 0001' has 3 fingerprints registered to the unit, all 3 fingerprints should be authenticated after ID input.
- The authentication sequence for the 3 fingerprints does not matter in this case, but whole authentication fails if a single fingerprint is not successfully authenticated.

• After the setting is completely done, press [ENTER] to move to the upper menu.

3. Configuration settings

3.5.3. Doorlock

1. Application
2. Verify Option
3. Set Doorlock
4. Sound Control
5. Time Setting
6. Other Setting

Default screen ➔ [*] ➔ [3] ➔ [3]

- Press [3] for door settings.

3.5.3.1. Door opening time

<Open Duration>
(00-30):03

- After this setting is completely done, press [ENTER] to move to the next setting.

Default screen ➔ [*] ➔ [3] ➔ [3]

- Default setting : '03' (unit: sec.)
- This is used to set the door opening time after authentication is successfully done. This means the door opening time only for strike type but is not applicable to dead bolt type or auto door.
- If this is set to '00', the door control in access control mode is out of control. Therefore, '00' setting may be possible only for time & attendance mode, where there is no need for lock control.

3.5.3.2. Door status monitor

<Door Monitor>
[0/1=NO/2=NC]:0

- Once the setting is completely done, Press [ENTER] to move to the next setting

Default screen ➔ [*] ➔ [3] ➔ [3] ➔ [ENTER]

- Default setting : '0'
- '0' setting is for no monitoring, '1' setting is for dead bolt type or auto door and '2' setting is for strike type.
- When this is set to '1' or '2', the door status through connected terminal is periodically transmitted to the server.

button	description
[0]	NW - No monitoring
[1]	NO - Dead bolt type or auto door (In case that lock monitoring pin is low when the door is locked)
[2]	NC - Strike type (In case that lock monitoring pin is high when the door is locked)

3. Configuration settings

3.5.3.3. Door open alarm

<Door Open Alarm>
(00-30):00

Default screen ➔ [*] ➔ [3] ➔ [3] ➔ [ENTER] ➔ [1] or [2] ➔ [ENTER]

- Default setting : '00'
- For smoothly operation of this setting, the relevant lock should be the lock type to be able to monitor whether the door is open or closed and its monitoring pin should properly be connected to the terminal. The previously mentioned setting for monitoring door status should be set to '1' or '2' for this operation.

- Once the setting is completely done, press [ENTER] to move to the upper menu.

3.5.4. Volume

1. Application
2. Verify Option
3. Set Doorlock
4. Sound Control
5. Time Setting
6. Other Setting

Default screen ➔ [*] ➔ [3]

- Press [4] for volume settings.

3.5.4.1. Voice

<Use Voice>
(N=0/Y=1):1

Default screen ➔ [*] ➔ [3] ➔ [4]

- Default setting : '1'
- To make voice information about terminal control available, set it to '1'. If not, set it to '0'.

- Press [ENTER] to move to the next setting.

3.5.4.2. Buzzer volume

<Beeper volume>
(0-2):1

Default screen ➔ [*] ➔ [3] ➔ [4] ➔ [ENTER]

- Default setting : '1'
- This is for the terminal buzzer volume. If this is set to '0', there is no buzzer sound. '1' setting means low volume and '2' means high volume.

- Press [ENTER] to move to the next setting.

3.5.4.3. Case open alarm

<Case Open Alarm>
(N=0/Y=1):1

- After this setting is completely done, press [ENTER] to move to the next setting.

Default screen ➔ [*] ➔ [3] ➔ [4] ➔ [ENTER] ➔ [ENTER]

- Default setting : '1'
- An alarm sounds if the terminal case is damaged or opened. For this setting, VIRDI 4000 series have case open sensor installed.

3.5.5. Current time

<Time Setting>
20090925211806

- Press [ENTER] to check that the current time is updated and move to the upper menu.

Default screen ➔ [*] ➔ [3] ➔ [5]

- This is to set the terminal current time. The above example represents the year 2009, month 9, date 25, hour 21, min. 18, and sec. 06. To change it, delete the old numbers with the [#] button before adding the new numbers.

3.5.6. Other

1. Application
2. Verify Option
3. Set Doorlock
4. Sound Control
5. Time Setting
6. Other Setting

Default screen ➔ [*] ➔ [3] ➔ [6]

- Press [6] for other settings.

3.5.6.1. LCD Backlight On/Off

<LCD Backlight>
(0=Off/1=On):

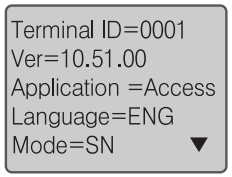
- After the setting is completely done, press [ENTER] to move to the upper menu.

Default screen ➔ [*] ➔ [3] ➔ [6]

- Default setting : '0'.
- This is to set LCD backlight. If it is set to '1', LCD backlight is on all the times. On the other hand, if it is set to '0', the LCD backlight is normally off and keypad operation or placing a card makes the backlight on. Since it has passed 10 seconds after relevant operation is done, backlight becomes off.

3. Configuration settings

3.6. Terminal information view



Default screen ➔ [*] ➔ [4]

• Press [0] to scroll up and down the screen.

item	description
Terminal ID	Terminal ID
Version	Terminal firmware version
Application	Terminal application mode (Access/T&A)
Language	Language for text and voice of the LCD screen
Mode	Connection mode between terminal and network server
Network type	Network connection type (static IP/DHCP)
Mac address	Terminal ethernet hardware address
IP address	Terminal IP address
Gateway	Terminal gateway address
Subnet mask	Terminal subnet mask address
Server IP	IP address of network server connected to the terminal
Svr-port	Port number of network server program
Card Reader	Card reader type
FP-Sensor	Fingerprint sensor type
1:1 Level	Identification level for 1:1 authentication
1:N Level	Identification level for 1:N authentication
Max User	Maximum user capacity to be able to be registered to a terminal
Max FP	Maximum fingerprint capacity to be able to be registered to a terminal. For example, if there are 100 registered users and two fingerprints per user are registered, it means a total of 200 fingerprints is registered.
All User	Number of current users registered to a terminal including administrators
All Admin	Number of administrators registered to a terminal
All FP	Number of fingerprints currently registered to a terminal
1:N User	Number of users for 1:N authentication
1:N FP	Number of fingerprints for 1:N authentication
All Log	Authentication records stored in a terminal

3. Configuration settings

3.7. Extra functions

□ In the main menu, press [5] to select '5.Ext function' and the following screen appears:

```
1. Lock Terminal
2. Read Card No.
```

3.7.1. Terminal lock

```
<Lock?>
(N=0/Y=1):0
```

Default screen ⇨ [*] ⇨ [5] ⇨ [1]

- Default setting '0' : Releasing terminal lock
  '1' : Setting terminal lock
- An administrator in local terminal ? not by server program - can directly set up or release the terminal lock to the local terminal. If it is set to '1', the terminal is locked and nobody is accessible to the specific area through locked terminal until the administrator unlocks the terminal.
- For this setting, 'Allow admin to access' in terminal configuration of server program should be permitted.

- After the setting is completely done, press [ENTER] to move to the upper menu.

3.7.2. Read card number

```
Place Your Card
```

Default screen ⇨ [*] ⇨ [5] ⇨ [2]

- This is an extra function which is not related to terminal configuration settings. By using this function, an administrator can read the card number when she/he places a card to the terminal mounted with card reader, in order to register the placed card to server. If this LCD screen pops up and then an administrator places a card to the terminal, the card number shows in the LCD screen.

- To exit from this setting, press [#] to move to the upper menu.

3. Configuration settings

3.8. Device settings

□ In the main menu, press [6] to select '6. Device', and the following screen asking for a password appears:

<Input PW>
PW : _ _ _ _ _ _ _ _

Default screen ➪ [*] ➪ [6]

- In the most of cases, There is no need for modifying the device settings after installation. Therefore, be careful not to modify the device settings without any obvious reasons.
- This previously set password from factory is to call administrator's attention, which is fixed one and should not be changed.
- Input '084265' as the previously set password and press [ENTER] to show the detailed setting items.

3.8.1. Function key

<Key On/Off>
1=F1 : O 2=F2 : O
3=F3 : O 4=F4 : O
5=ENT : O 6=FP : O

- After the setting is completely done, press [ENTER] to move to the upper menu.

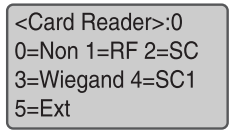
Default screen ➪ [*] ➪ [6] ➪ '084265'+[ENTER] ➪ [1]

- Default setting : all 'O'
- This is to enable or disable the function keys. 'O' means enabling the function key and 'X' means disabling the function key. Whenever the number conformed to a function key in this setting is pressed, this setting is changed between 'O' and 'X'.
- In this setting, 1 conforms to [F1], 2 conforms to [F2], 3 is for [F3] and 4 is for [F4]. For example, if an administrator presses [1] one time in this setting and [F1] key is disabled - [X], a user can not enter into start mode by pressing [F1] key button as [F1] key is disabled.
- Additionally, if only [F1] or [F2] is set to 'O', the terminal can be used in either always start or always leave mode.
- 6 (FP) is used for setting detection function of fake finger.

3. Configuration settings

3.8.2. Card reader

3.8.2.1. Card reader type setting

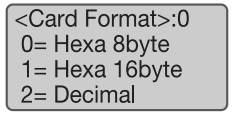


- After the setting is completely done, press [Ent] to move to the next menu.

Default screen ➡ [*] ➡ [6] ➡ '084265'+[Ent] ➡ [2]

- Default setting : '0'
- This is to set the card reader mounted in a terminal. Refer to the followings for correct setting:
  - '0' : No card reader
  - '1' : Low-frequency RF Card reader mounted
  - '2' : High-frequency smart card reader
  - '3' : Wiegand card reader like HID card module
  - '4' : Other smart RF reade
  - '5' : External card reader
- If a card reader is mounted into a terminal and the above setting is correctly done, when [F1]~[F4] or [Ent] is pressed, the authentication mode is changed and 1:1 fingerprint authentication is ready for operation - in this case, 1:N fingerprint authentication is not performed except for auto sensing setting.

3.8.2.2. Card reader format setting



- After the setting is completely done, press [Ent] to move to the upper menu.

- Default setting : '0'
- Set up format of data from card reader
  - 0: Hexa data value with 8byte
  - 1: Hexa data value with 16byte
  - 2: Decimal data value

3. Configuration settings

3.8.3. Fingerprint sensor

3.8.3.1. 1:1 verification level

1:1 level
(1-9):4

- Press [ENTER] to move to the next setting.

Default screen ➔ [*] ➔ [6] ➔ '084265'+[ENTER] ➔ [3]

- Default setting : '4'.
- This is to set 1:1 matching security level for a terminal between the fingerprint captured from fingerprint input window and the relevant fingerprint stored in a terminal. The higher 1:1 matching level means the higher security. But possibility of authentication failure is getting higher as higher matching rate is required.
- For an example of 1:1 authentication with ID input, if inputted ID number is '1234', there is authentication process between the fingerprint captured from fingerprint input window and the fingerprint associated with ID '1234' in a terminal.

3.8.3.2. 1:N identification level

1:N Level
(3-9):5

- Press [ENTER] to move to the next setting.

Default screen ➔ [*] ➔ [6] ➔ '084265'+[ENTER] ➔ [3] ➔ [ENTER]

- Default setting : '5'
- This is to set 1:N authentication security level between the fingerprint captured from fingerprint input window and all the fingerprints in a terminal which are allowed for 1:N authentication.
- For your information, 1:N authentication level is not set for respective user but only for a terminal.

3. Configuration settings

3.8.3.3. Intelligent-Capture

<I-Capture>
(N=0/Y=1):1

- After the setting is completely done, press [ENTER] to move to the upper menu.

Default screen ➪ [*] ➪ [6] ➪ '084265'+[ENTER] ➪ [3] ➪ [ENTER] ➪ [ENTER]

- Default setting : '1'
- This adjusts the sensor settings automatically to enhance good fingerprint detection capability by reducing bad influences from humid fingers and/or residual fingerprints which are left on a sensor window due to sweat and/or contaminants on fingertip.
- If it is set to '0', fingerprint capturing time gets shorter but its authentication rate for dry or wet finger becomes lower.
- If it is set to '1', fingerprint capturing time becomes longer than that of above '0' setting but its authentication rate gets higher. Therefore, '1' setting is recommended.

3.8.4. Wiegand output

Wiegand Out:0
0=None 1=26bit
2=34bit

<Site Code>
(0-255):000

- After the setting is completely done, press [ENTER] to move to the upper menu.

Default screen ➪ [*] ➪ [6] ➪ '084265'+[ENTER] ➪ [4]

- Default setting : '0'
- If Wiegand output from the local terminal is needed for external access controller with Wiegand input, an administrator can set this setting as '1' or '2'.
  - In case of '1' setting, "site code [1 byte] and user ID [2 bytes]" are transmitted through Wiegand output port. User ID should be set as less than 4 digits.
  - In case of '2' setting, "site code [1 byte] and user ID [3 bytes]" are transmitted through Wiegand output port. User ID should be set as less than 7 digits.
- This setting is not related to external Wiegand reader.
- In cases of '1' or '2' settings, the below-mentioned site code should be set.
  - Default setting : '000'.
  - An administrator can assign the site code of from 0 to 255 which is transmitted together with a user ID.

3. Configuration settings

3.8.5. System configuration

```
1. Set Fn-Key
2. Card Reader
3. FP-Sensor
4. Wiegand
5. System Config
6. Initialize
```

Default screen ➔ [*] ➔ [6] ➔ '084265'+[ENTER] ➔ [5]

3.8.5.1. User ID length

```
<ID Length>
(2-8):4
```

- Press [ENTER] to move to the next setting.

Default screen ➔ [*] ➔ [6] ➔ '084265'+[ENTER] ➔ [5]

- Default setting : '4'
- This ID length can be 2~8 digits and should be the same as that of ID registered in the server program. If the ID registered in the server program is '000075', input '6'.
- With modifying this ID length shorter than before during normal operation after installation, an administrator may not be able to be authenticated and enter into main menu if she/he has longer ID length, compared to the modified ID length. Therefore, be careful to give serious consideration before modifying the ID length.

3.8.5.2. Language

```
<Language>:1
0=KOR 1=ENG
2=JPN 3=ESP
4=POR 5=CHN
```

- After the setting is completely done, press [ENTER] to move to the upper menu.

Default screen ➔ [*] ➔ [6] ➔ '084265'+[ENTER] ➔ [5] ➔ [ENTER]

- Default setting : '1' (English)
- Voice output languages are as follow, '0': Korean, '1': English, '2': Japanese, '3': Spanish, '4': Portuguese and '5': Chinese.
- LCD characters correspond to the assigned language.

3. Configuration settings

3.8.6. Terminal initialization

1. Init Config
2. Delete Log
3. Init Terminal

Default screen ➔ [*] ➔ [6] ➔ '084265'+[ENTER] ➔ [6]

- To initialize configuration settings, press [1]. To initialize the record, press [2]. To factory default settings, press [3].

3.8.6.1. Configuration settings initialization

<Init Config>
[Y=1 / N=2] :

- After this configuration setting initialization is successfully done, it moves to the upper menu together with a 'ppiririck' buzzer sound.

Default screen ➔ [*] ➔ [6] ➔ '084265'+[ENTER] ➔ [6] ➔ [1]

- To initialize configuration settings, press [1]. If not, press [2].
- All the configuration settings except for Mac (physical) address are initialized; user's information and authentication records are not deleted.

※If this configuration settings initialization is done, the language for voice output and display characters is changed to English. If you need to set as other language, refer to '3.8.5.2. Language'.

3.8.6.2. Authentication record initialization

<Delete All Log>
[Y=1 / N=2] :

- After this configuration setting initialization is successfully done, it moves to the upper menu together with a 'ppiririck' buzzer sound.

Default screen ➔ [*] ➔ [6] ➔ '084265'+[ENTER] ➔ [6] ➔ [2]

- To initialize the log data, press [1]. If not, press [2].
- All the log data related to authentication are deleted; configuration settings and user's information are not deleted.

3.8.6.3. Factory default initialization

<Init Terminal>
[Y=1 / N=2] :

- After this configuration setting initialization is successfully done, it moves to the upper menu together with a 'ppiririck' buzzer sound.

Default screen ➔ [*] ➔ [6] ➔ '084265'+[ENTER] ➔ [6] ➔ [3]

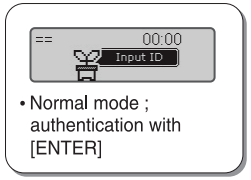
- To initialize everything to factory default, press [1]. If not, press [2].
- Except for the Mac (physical) address stored in the terminal, all configuration settings, user's information and authentication records (log data) are deleted, which becomes same as factory default.
- If this factory default initialization is done, the language for voice output and display characters is changed to English. If you need to set as other language, refer to '3.8.5.2. Language'.

4. How to use

4.1. Access control application

□ Default screen ➪ [*] ➪ [3] Option ➪ [1] Application ➪ [0] for access control application

4.1.1. Authentication mode



• Normal mode ; authentication with [ENTER]



• F1 mode ; authentication with [F1]



• F2 mode ; authentication with [F2]



• F3 mode ; authentication with [F3]



• F4 mode ; authentication with [F4]

• Fingerprint authentication

- Fingerprint authentication in the corresponding mode by pressing a relevant function key; [Enter], [F1], [F2], [F3] and [F4]. Fingerprint authentication through auto sensing without pressing any keys. This authentication is performed in the current mode displayed in the screen.

• Password authentication

- After inputting the user ID and changing the authentication mode by pressing the corresponding function key, input the password for authentication.

• Card authentication after the following settings are done : menu ➪ '6.Device' settings ➪ '2.Card reader' ➪ <Card Reader> is set to [1] or over

- Pressing the function key changes just authentication mode. For card authentication, press the corresponding function key and then place the card close to the terminal.

4. How to use

4.1.2. [1:1] fingerprint authentication

□ When auto sensing is running, input '0001' if the user ID is '0001' and then place your finger close to the fingerprint sensor. The light on the fingerprint input window turns on to detect the fingerprint and the authentication result is displayed on the LCD window.

□ If the user ID is '0001', input '0001' and press the function key. Voice information like "please enter your fingerprint" follows. When a fingerprint is inputted, the authentication result is displayed on the LCD window. is entered, the authentication result will be displayed on the LCD window.



If the user ID is '0001', input '1' or '0001' and press the function key.



Place your finger close to the input window when you hear the voice message "Please enter your fingerprint". Do not remove your finger until you hear a "ppig" buzzer sound.



If authentication is successfully done, a success message is displayed on the LCD together with a voice message "You are authorized". The door d LED turn on and door relay runs.The default screen appears after 1~2 seconds. The door LED turns off and door relay is back again after the door open setting time has elapsed.

□ The following error message appears together with a voice message "Please try again".



• In case of authentication failure



• Non-registered user ID



• During the authentication request to the authentication server, network trouble occurred or network line was disconnected.

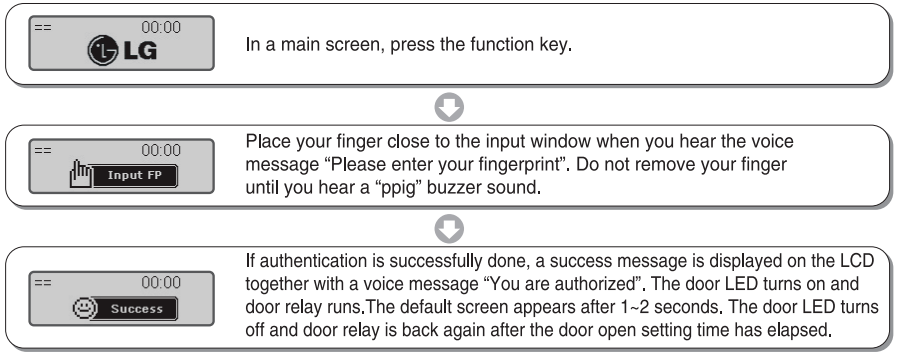
4. How to use

4.1.3. [1:N] fingerprint authentication

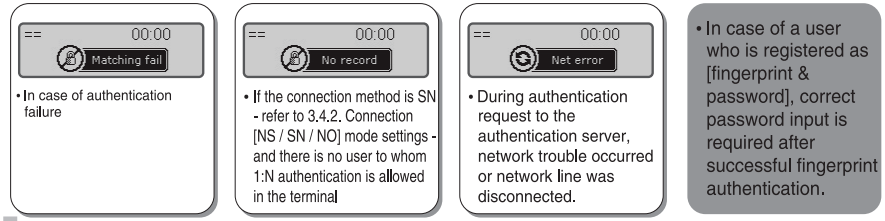
□ This authentication is allowed only for users who are registered as 1:N authentication setting.

□ If a user places his/her finger close to the fingerprint sensor when auto sensing is running, the light on the fingerprint input window turns on to detect the fingerprint and the authentication result is displayed on the LCD window.

□ When you press the function key, voice information like “please enter your fingerprint” follows. When a fingerprint is inputted, the authentication result is displayed on the LCD window.



□ Error message : The following error message appears together with a voice message “Please try again”



4. How to use

4.1.4. Password authentication

□ If the user ID is '0001', input '0001' and press the function key. The terminal waits for the user password to be inputted after a "ppiriririck" buzzer sound. Input the relevant password and press [ENTER]. The authentication result appears on the LCD.



If the user ID is '0001', enter '0001' and press the function key.



The terminal waits for the user password to be inputted after a "ppiriririck" buzzer sound. Input the relevant password and press [ENTER]. For security reason, the password is displayed as '*' on the LCD screen, not actual numbers.



If authentication is successfully done, a success message is displayed on the LCD together with a voice message "You are authorized". The door LED turns on and door relay runs.The default screen appears after 1~2 seconds. The door LED turns off and door relay is back again after the door open setting time has elapsed.

□ Error message: An error message appears together with the voice message "Please try again"



• In case of authentication failure



• Non-registered user ID



• During authentication request to the authentication server, network trouble occurred or network line was disconnected.

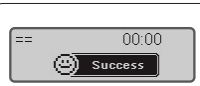
4. How to use

4.1.5. Card authentication

☐ In case of a user who is registered as [RF], [RF|FP] or [RF|PW], place the card close to the terminal in main screen. After a “ppig” buzzer sound, the authentication result appears on the LCD.



Place your card close to the terminal. It makes a “ppig” buzzer sound.



If authentication is successfully done, a success message is displayed on the LCD together with a voice message “You are authorized”. The door LED turns on and door relay runs.The default screen appears after 1~2 seconds. The door LED turns off and door relay is back again after the door open setting time has elapsed.

☐ Error message : An error message appears together with the voice message “Please try again”



Non-registered card



During authentication request to the authentication server, network trouble occurred or network line was disconnected.

☐ In case of a user who is registered as [RF&FP] or [ID&FP | RF&FP], place the card close to the terminal in main screen. After a “ppig” buzzer sound, the following fingerprint authentication screen appears:



When the light on the fingerprint input window turns on together with the voice message “Please enter your fingerprint”, enter your fingerprint and hold it there until you hear a “ppig” buzzer sound.

☐ In case of a user who is registered as [RF&PW] or [ID&PW | RF&PW], place the card close to the terminal in main screen. After a “ppig” buzzer sound, the following fingerprint authentication screen appears:



After a “ppiriririck” buzzer sound, the terminal waits for the user password to be inputted. Enter password and press [ENTER].

4. How to use

4.1.6. User ID group authentication

- User ID group authentication is performed just among users grouped with same first digit and/or above of user ID - at least one digit. This authentication can conveniently be used if there are too many users and the matching time for 1:N authentication takes too long. In the menu, set as below: 3. Option ⇨ 2. Verify option ⇨ Enable 1:N ⇨ <User ID Group>=1.
- For your information, refer to the followings on how to use this authentication in more details, If the relevant ID for a user is '1234', enter only '12' for this authentication. This matching is performed just among users having IDs of from '1200' to '1299' , starting with '12'. If the ID is '0012', enter '0012' or '00' for authentication.



If the user ID is '1234', enter '1', '12' or '123' and then press the function key.



When the light on the fingerprint input window turns on together with the voice message "Please enter your fingerprint", enter your fingerprint and hold it there until you hear a "ppig" buzzer sound.

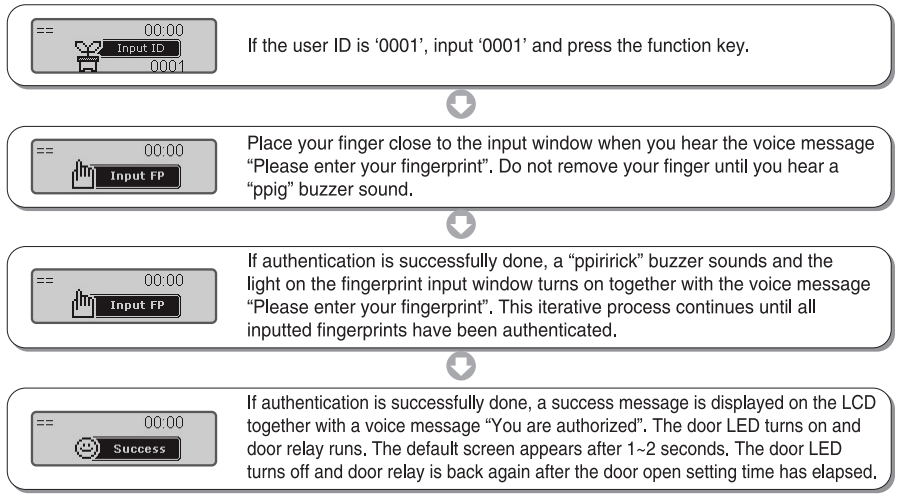


If authentication is successfully done, a success message is displayed on the LCD together with a voice message "You are authorized". The door LED turns on and door relay runs.
The default screen appears after 1~2 seconds. The door LED turns off and door relay is back again after the door open setting time has elapsed.

4. How to use

4.1.7. Multiple fingerprint authentication

- For a door where higher security is required, multiple fingerprints captured from more than two persons are assigned to a single ID for access to the specific door. The door opens only when all the registered fingerprints are successfully authenticated. In the menu, set as below: 3. Option ➪ 2. Verify option ➪ <Enable 1:N>=0 ➪ <Verify Multi-FP>=1.
- For example, if the ID '0001' is registered with three different fingerprints, all three fingerprints must be authenticated for access after ID input. A single authentication failure in mid course results in overall failure and the whole authentication process should be restarted. This iterative process continues until all three fingerprints are authenticated.



- Error message is same as that of [1:1] authentication.

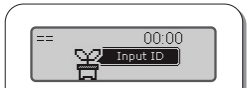
4. How to use

4.2. Time & Attendance control

□ Default screen ➪ [*] ➪ [3] Option ➪ [1] Application ➪ [1] T&A (Time Attendance) settings

□ If start and leave time for employees are fixed, set <start time>, <leave time> and <normal time> to reduce user input errors.

4.2.1. Authentication mode



• Normal mode; authentication with [ENTER]



• Start mode; authentication with [F1]



• Leave mode; authentication with [F2]



• Outside work mode; authentication with [F3]



• Return mode; authentication with [F4]

• Fingerprint authentication

- Press the function key which is related to specific T & A mode.If the function key is not used and authentication process is done in auto sensing, the current mode on the screen is working for authentication.

• Password authentication

- After inputting the user ID and changing the authentication mode by pressing the corresponding function key, input the password for authentication.

• Card authentication after the following settings are done: menu (“6.Device” settings ➪ “2.Card reader ” ➪ <Card Reader> is set to [1] or over. Pressing the function key changes just authentication mode. For card authentication, press the corresponding function key and then place the card close to the terminal.

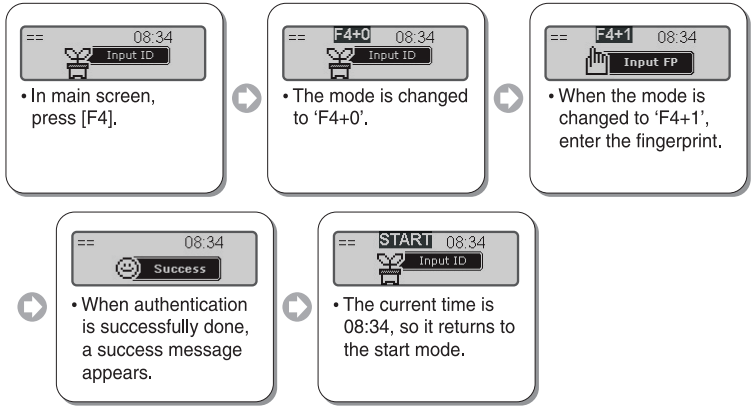
- After authentication is done, working mode returns to the mode - start, leave or normal - previously set as time frames but if no mode is set for the specific time period, the previous authentication mode is maintained.

• [1:1] fingerprint authentication : Same as ‘4.1.2.’. [1:N] fingerprint authentication : Same as ‘4.1.3.’. Password authentication : Same as ‘4.1.4.’ Card authentication : Same as ‘4.1.5.’. User ID group authentication : Same as ‘4.1.6.’

4. How to use

4.2.2. Expansion of working mode by multi-key function

- If more than 5 working modes - start, leave, outside work (out), return (back) and normal - are required, it can be expanded up to 41 modes.
- After setting Menu ➪ 3.Option ➪ 1.Application ➪ [1] T&A, set more than one key to 'O' in <Multi Fn-key> setting. The keys set to 'X' are not applied in this multi-key function.
- As a mode is defined as a function key plus a number key, press a number key after pressing the function key for authentication. In the server program, authentication mode is displayed as a function key plus a number key like 'F3+1'.
- For example, when [F4] is set to [O] and <start time> is set to '07:00~09:30', if a fingerprint user tries for authentication in 'F4+1'mode,



4. How to use

4.3. For using as meal management system

□ Default screen ⇨ [*] ⇨ [3] Option ⇨ [1] Application ⇨ [2] Setting up to meal

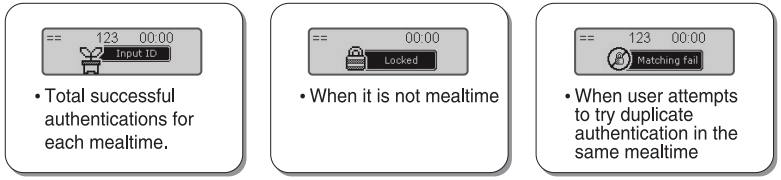
□ When setting up meal management, a user must input at least one mealtime because the terminal is locked except for mealtime.

□ Each user can authenticate only once for each meal and multiple authentications are not allowed, but multiple authentications by using [ENTER] key are allowed.

□ If multiple authentications should not be allowed under any circumstances, go to
Default screen ⇨ [*] ⇨ [6] Device settings ⇨ [1] Function key ⇨ Setting up to Ent=[X] at <KeyOn/Off>.

4.3.1. Meal Classification

□ Function key is used as manipulating key for authentication and can only classify meal based on mealtime without mode classification. The number placed in the upper center of screen displays the number of authentications for each mealtime.



- In case of authentication by fingerprint, authentication is available by auto sensing function without pressing Enter or function key.
- For password authentication Input user ID and function key and press password
- For card authentication
  (ex:Default screen ⇨ [*] ⇨ [6] Device settings ⇨ [3] Card reader ⇨ <Card Reader>= more than 1)
  Punch card for authentication

4.3.2. [1:1] Fingerprint authentication

□ Same as 4.1.2. but [ENTER] key is not available

4.3.3. [1:N] Fingerprint authentication

□ Same as 4.1.3. but [ENTER]

4.3.4. Password authentication

□ Same as 4.1.4. but [ENTER] key is not available

4.3.5. Card authentication

□ Same as 4.1.5. but [ENTER] key is not available

4.3.6. User ID group authentication

□ Same as 4.1.6. but [ENTER] key is not available

4. How to use

4.3.7. Allowing multiple authentications

□ Default screen ➪ [ENTER] ➪ [6] Device settings ➪ [1] Function key ➪ Must be setting as Ent=[O] on <Key On/Off>
(For initializing, edit is not needed since default setting value is [O], but it needs to be checked if it is not working.)

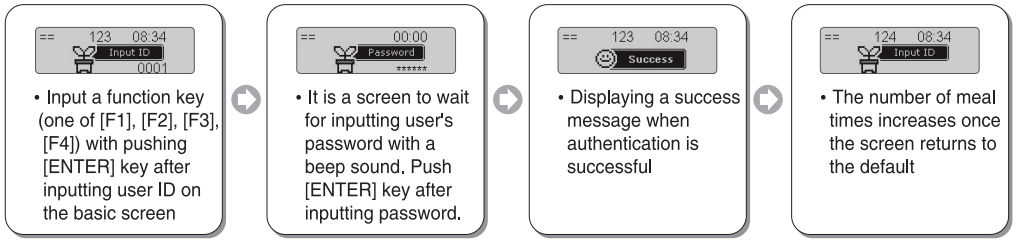
□ For multiple fingerprint authentications



□ For multiple card user authentications



□ For multiple password authentications





P/N : MFL62730801