Smart/RF Card Authentication System

Owner's Manual

Model : LACT10-R
LACT10-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 LACT10 is in compliance with the essential requirements and other relevant provisions of directive 1999/5/EC.

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.**

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

LACT10

Smart/RF Card Authentication System

■ Admin, Administrator

- As a user who can enter into the terminal menu mode, he/she 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, so 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 fingerprint recognition unit.

■ Authentication Method

- Various kinds of authentication including RF(card) authentication, PW (password) authentication or a combination of these methods
  Ex) RFIPW : card or password authentication; ID&password is used for authentication if card is not used.

■ Function keys

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

■ [NS] / [SN] / [NO] Mode

- [NS] Mode : When there is a live connection to the server, authentication is done through the server. If not, it is done through the terminal.
- [SN] Mode: Even though there is a live connection to the server, authentication is done through the terminal and the result is forwarded to the server in real time. However, in the case of 1:1 authentication, if the entered user ID is not registered in the server, authentication is done through the server.
- [NO] Mode : Even though a user is registered in the terminal, authentication is done through the server in any event.

Contents

1. Before use 10
1.1. Safety precautions 10
1.2. Terminal description 12
1.3. Button description 12
1.4. Screen description 13
1.5. LCD Icon during operation 14
1.6. Voice information during operation 14
1.7. Buzzer sound during operation 14

2. Introduction 15
2.1. Features 15
2.2. Configuration 16
2.2.1. Network configuration 16
2.2.2. Standalone configuration 16
2.3. Specifications 17

3. Environment settings 18
3.1. Check items before setting the environment 18
3.1.1. Entering menu 18
3.1.2. Change settings 19
3.1.3. Save environment settings 20
3.2. Menu configuration 21
3.3. User account 22
3.3.1. User registration 22
3.3.1.1. “1. RF”registration 23
3.3.1.2. “2. ID&PW”registration 24
3.3.1.3. “3. RF|PW”registration 25
3.3.1.4. “4. RF&PW”registration 26
3.3.1.5. “5. ID&FP|RF&FP”registration 27
3.3.2. Delete User 28
3.3.3. Modify User 29
3.3.3.1. “1. RF”user 30
3.3.3.2. “2. ID&PW”user 31
3.3.3.3. “3.RF|PW”, “4.RF&PW”, “5.ID&PW|RF&PW”user 32
3.3.4. Administrator registration 33
3.3.5. Delete All Users 34
3.4. Network settings 35
3.4.1. Terminal ID settings 35
3.4.2. Connection [NS/SN/NO] mode settings 36
3.4.3. Connection method settings 37
3.4.4. IP address settings 38
3.4.5. Subnet mask settings 39
3.4.6. Gateway settings 40
3.4.7. Server IP settings 41
3.4.8. Server port settings 42
3.5. Option settings 43
3.5.1. Application mode settings 43
3.5.1.1. [0] Access Control 27 43
3.5.1.2. [1] Time Attendance control 43
3.5.1.3. [2] Meal (Cafeteria) Service control 44

Contents

3.5.2. Authentication method settings 45
3.5.2.1. Settings for ID display when authentication is successful 45
3.5.2.2. Auto enter key setting 45
3.5.2.3. Settings for card only authentication 45
3.5.3. Door settings 46
3.5.3.1. Door opening time settings 46
3.5.3.2. Door status monitor 46
3.5.3.3. Door open alarm settings 47
3.5.4. Volume settings 47
3.5.4.1. Voice settings 47
3.5.4.2. Buzzer volume settings 47
3.5.5. Current time settings 48
3.5.6. Other Setting 48
3.5.6.1. LCD Backlight On/Off settings 48
3.5.6.2. LCD Brightness settings 48
3.5.6.3. Display Time settings 48
3.6. Terminal information view 49
3.7. Extended functions 50
3.7.1. Terminal lock settings 50
3.7.2. Read card number 50
3.7.3. Interfacing with sensor for fire detection 50
3.8. Device settings 51
3.8.1. System configuration settings 51
3.8.1.1. User ID length settings 51
3.8.1.2. Language settings 51
3.8.2. Function key settings 52
3.8.3. Card reader settings 52
3.8.4. Wiegand output settings 53
3.8.5. Terminal initialization 54
3.8.5.1. Settings initialization 54
3.8.5.2. Authentication record initialization 54
3.8.5.3. Factory initialization 54
4.How to use the terminal 55
4.1. Access control 55
4.1.1. Authentication mode 55
4.1.2. Card authentication 56
4.1.3. Password authentication 57
4.2. Time Attendance control 58
4.2.1. Authentication mode 58
4.2.2. Card authentication 58
4.2.3. Password authentication 58
4.2.4. Working mode expansion using multi-key authentication 59
4.3. Meal control 60
4.3.1. Meal classification 60
4.3.2. Card authentication 60
4.3.2. Password authentication 60

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 unit.

It may cause an electric shock, fire or damage.

Do not place a fire source near the unit.

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 insecticides or flammable sprays near the unit.

It may result in deformation or color change.

Avoid high humidity or dust.

The unit may be damaged.

Avoid severe temperature changes.

The unit 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 unit.

The unit may break down or malfunction.

Avoid impacts or using sharp objects on the unit.

The unit 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 operators manual, any damage caused due to misuse will be the user's liability.

1. Before using

1.2. Terminal description

1.3. Button description

Function key	Access mode	T&A mode	Cafeteria mode
F1	F1	Start	Menu 1
F2	F2	Leave	Menu 2
F3	F3	Outside	Menu 3
F4	F4	Return	Menu 4

Function key	Description
0	Input number '0' value or Menu scroll button
Ent	Enter menu after pressing over 2sec
Del	Change setting. Move to upper menu. Return to normal mode

1. Before using

1.4. Screen description

- Initial screen.

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

- Password input.

- Authentication is successful.

- Authentication is failed.

- Entered a non-registered user ID.
- Connection method is [SN] and 1:N identification is accessed even though there is no user allowed for 1:N identification.

- A registered user tried. authentication twice time during same menu time when terminal is cafeteria mode.

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

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

- Ready status for card data input.

- A registered user tried. authentication when entry/exit is not allowed.

- Waiting for server authentication.

- Terminal is locked.
- A registered user tried authentication when Cafeteria time is not allowed.

- Terminal program upgrade. (Power switch should not be turned off when this message is displayed.)

1. Before using

1.5. LCD Icon during operation

Network status	: LAN cable is not connected.
	: LAN cable is connected, but server is not connected.
	: Server is connected.
Door status	: Door Close
	: Door Open
Card input	: Displayed 1sec after card data is read

1.6. Voice information during operation

"You are authorized"

Authentication is successful.

"Please try again"

Authentication is failed.

1.7. Buzzer sound during operation

Confirmation Tone (One beep)

When a button is pressed or a card is being read.

Error Tone (Two short beeps)

Authentication failed or wrong user input.

Beeping

Waiting for fingerprint input

Confirmation Tone
(Three short beeps)

Authentication successful or settings for the current user are completed

2. Introduction

2.1. Features

□Access control system using LAN.

- Communication between the terminal and authentication server is done through d 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.

□Simple and fast authentication process.

□High capacity of terminal and server.

- There is no limit on user registration for the server, and the terminal itself can store up to 20,000 card user.

□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.

□Various and flexible Access controls.

- Perfect control by assigning different security clearances to each user or group
- Provides flexibility by allowing limited time for entry/exit.

□Various applications including Access, T&A, Cafeteria management.

- Various operation modes depending on the terminal menu settings.

□Various registration and authentication methods

- There are a total of 5 registration and authentication methods, so you are required to select one method before registering users and an administrator.

RF	Card registration, Card authentication
ID&PW	Password registration, Password authentication
RF|PW	Card and password registration, Card or password authentication.
RF&PW	Card and password registration, Password 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

2.2.1. Network configuration

2.2.2. Standalone configuration

2. Introduction

2.3. Specifications

Item	SPEC	REMARK
CPU	32Bit RISC CPU	
MEMORY	8M SDRAM	
	2M FLASH (Default)	User: 10,000 / Log: 20,000
	4M FLASH (Option)	User: 20,000 / Log: 98,000
Authentication speed	< 0.2 sec.	
Communication Port	TCP/IP, Wiegand In&Out	
	RS-232, RS-485, 2 Relay	
Temperature / Humidity	-10 ~ 50 / Lower than 90% RH	
LCD	128 X 64 Graphic LCD	
SIZE	140 X 89 X 28 mm	
AC / DC Adapter	INPUT : Universal AC 100 ~ 220V	
	OUTPUT : DC 12V (Option : DC 24V)	
	UL, CSA, CE Approved	
Card Reader	RF Card Reader (LACT10-R)	EM Card, 125kHz
	Smart Card Reader (LACT10-S)	ISO 14443 A-type, 13.56MHz

3. Environment settings

3.1. Check items before setting the environment

3.1.1. Entering menu

The following screen appears when the [ENT] button is pressed for over 2 sec.

1. User
2. Network
3. Option

- Press [0] to view menus not shown in the LCD window.
- If a number corresponding to the menu required is pressed (ex. [1] for user account), the following screen for administrator authentication appears.

<Input Admin ID>
ID : 0001

- Press [ENT] 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 authentication is successful, sub-menus of the menu chosen appear.

※Administrator authentication is required only once, so all menus are accessible until he exits from the menus altogether.

3. Environment settings

3.1.2. Change settings

To change settings, press the [DEL] button 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 [ENT] for settings verification or to move to the next setting, and press the [DEL] button to move to upper menus.

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

3.1.3. Save environment settings

Press the [DEL] button in the main menu to save environment settings and the following screen appears

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

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

If there are no changes made to the settings, "Save?" does not appear, and the initial screen appears.

If there is no input for a certain period of time while setting the environment, the settings process will finish. If there are changes made to the settings, "Save?" appears. If not, it does not appear and the initial screen appears.

3. Environment settings

3.2. Menu configuration

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

3. Environment settings

3.3. User account

3.3.1. User registration

3. Environment settings

3.3.1.1. “1. RF” registration

□ Fingerprint registration and fingerprint authentication.

3.3.1.2. “2. ID&PW” registration

□ Password registration and password authentication for a user.

3. Environment settings

3.3.1.3. “3. RFIPW” registration

□ Card and password registration, card or password authentication.

3. Environment settings

3.3.1.4. “4. RF&PW” registration

□ Card and password registration, card and password authentication.

3. Environment settings

3.3.1.5. “5. ID&PWIRF&PW” registration

□ RF-Card and password registration, ID input and password authentication or card and password authentication.

※ After Card registration (refer to “1. RF” registration), password registration (refer to “2. ID&PW” registration) follows.

※ In this case, a card is used instead of ID for authentication. This is helpful to users who have difficulty inputting their ID.

3.3.2. Delete User

- After entering the user ID to delete, press [ENT] you will hear three short beeps and all the information about the user is deleted. However, the information is still stored in the server. To completely delete this information, the data in the server shall also have to be deleted.
- If a non-registered user ID is entered, °∞2.Delete°± appears together with an error tone.
- Caution is required when deleting a user or an administrator. The user just registered in the unit (not in the server) is not recoverable, so special care is required.

3. Environment settings

3.3.3. Modify User

3. Environment settings

3.3.3.1. “1.RF” user

3. Environment settings

3.3.3.2. “2.ID&PW” user

Enter the user's ID to Modify, and press [Ent].
• When changing an ID, there is no difference between a user and an administrator.
If a non-registered user (or administrator) is entered, you will hear an error tone and the "1. Add" menu appears.

Press the [1] button to change the passwords.
• To change passwords, press [1].
To cancel it, press [DEL].

Press [Ent] to input the password.

Input the same password once more for verification.
• Press [ENT] to confirm the password.
If the password change is successful, you will hear three short beeps if not, you will hear an error tone and the "1. Add" menu appears.

3. Environment settings

3.3.3.3. “3.RFIPW” , “4.RF&PW” , “5.ID&PWIRF&PW” user

3. Environment settings

3.3.4. Administrator registration

3.3.5. Delete All Users

3. Environment settings

3.4. Network settings

In the main menu, press [2] to select "2.Network" to see the following screen. When the setting is chosen, press [Ent] to move to the next setting.

1. User registration
2. Network settings
3. Option settings

3.4.1. Terminal ID settings

Press [Ent] for over 2 sec. to enter main menu.

Press [2] to network settings.

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]. Press [ENT] to move to the next setting.

3. Environment settings

3.4.2. Connection [NS / SN / NO] mode settings

NS mode : '0', SN mode : '1',
NO mode : '2'

- This defines the authentication method between the terminal and network server, and the default is '1' (SN). Each authentication method is described below
  - NS mode: select [0]. When there is a live connection to the server, authentication is done through the server. If not, it is done through the terminal.
  - SN mode: select [1]. Even though there is a live connection to the server authentication is done through the terminal and the result is forwarded to the server in real time. However, in the case of 1:1 authentication, if the entered user ID is not registered in the server, authentication is done through the server.
  - NO mode: select [2]. Even though a user is registered in the terminal, authentication is done through the server in any event.
- Depending on the number of terminals, the number of users, or network conditions, each different mode can be used flexibly, but if there are more than 10 terminals connected to the server for simultaneous authentication or there are frequent network problems, it is recommended to use SN authentication (setting '1').
- Press [ENT] to move to the next setting.

3. Environment settings

3.4.3. Connection method settings

Press [0] for Static IP.
Press [1] for DHCP.

- The default is '0' (Static IP). If a fixed IP is assigned to the unit in a network, press [0]. If there is a DHCP server in the network to which the unit is connected, press [1].
- Press [ENT] to move to the next setting.

※For Static IP (0), refer to 3.4.4. IP address, 3.4.5. Subnet mask and 3.4.6. Gateway. For DHCP, skip those sections.

3. Environment settings

3.4.4. IP address settings

Press [Del] 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] [0] [9] [8] [1] [0] [0] [5] [0]
- Press [ENT] to move to the next setting.

3. Environment settings

3.4.5. Subnet mask settings

Press [Del] 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]
- Press [ENT] to move to the next setting.

3. Environment settings

3.4.6. Gateway settings

3. Environment settings

3.4.7. Server IP settings

Press [Del] 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] [ENT] [1] [0] [0] [1] [2] [1]
- Press [ENT] to move to the next setting.

3. Environment settings

3.4.8. Server port settings

Press [Del] to delete an old value and enter the new value.

- As the port number of the authentication server, the default is '9870'. Special care is required when changing this number because the corresponding number in the server should also be changed.
- If the server port is '9870', enter as below - [2] [2] [0] [1]
- Once the network setting is complete, press [Ent] to return to the main menu.

3. Environment settings

3.5. Option settings

3.5.1. Application mode settings

1. Application
2. Verify Option
3. Set Door lock

<Application>:0
0=Access Ctrl
1=T&A Ctrl 2=Meal Ctrl

• Press [Ent] to move to detailed settings for each operation mode.

<Start Time>
00:00 - 00:00

• After lastly setting normal time, press [Ent] to see the 'Multi Fn-key' setting menu, which allows more than 5 time & attendance modes.

<Multi Fn-key>
1=F1:X 2=F2:X
3=F3:X 4=F4:X

Default screen ➡ [Ent] ➡ [3] ➡ [1]

- The default is '0=Access Ctrl'
- For access control application, set as '0'. For time & attendance, set as '1'.

3.5.1.1. [0] Access Control

- No more detailed settings. It moves to the upper menu.

3.5.1.2. [1] 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 [Del] 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 [Ent]: 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 [Ent] to move to the upper menu.

3.5.1.3. [2] Meal (Cafeteria) Service control

<Breakfast>
00:00-00:00

• Press [Ent] to see <Without Limit> menu setting after setting all the menu time.

<Without Limit>
(N=0/Y=1):0

<식권프린터 사용>
(N=0/Y=1) : 0

- If time setting is not necessary, Set as '00:00-00:00'.
- If <Breakfast> time is set from 07:00 to 09:00, all authentication data is recorded as <breakfast>.
- After setting <Breakfast> time, continue to set <Lunch>, <Dinner>, <Supper> and <Snack> with same manner. If some menu is not necessary, set as '00:00-00:00'.
- Each menu time shall not be overlapped. User can authenticate only one time during same menu time.
- If user has to authenticate more than one time, he/she has to authenticate fingerprint after <Ent> button is pressed.
- 'Terminal Locked' message will be displayed during an interval time between each <Menu> setting time. Nobody can authenticate until the terminal is locked except entering a menu mode.

3. Environment settings

3.5.2. Option settings for authentication

1. Application
2. Verify Option
3. Set Doorlock

Default screen ➡ [Ent] ➡ [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 [Ent] 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. Auto enter key setting

<Auto Enter Key>
(N=0/Y=1):0

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

Default screen ➡ [Ent] ➡ [3] ➡ [2] ➡ [Ent]

- Default setting : ‘0’
- If it is set to the default setting '0', a user should input ID and push [F1]~[F4], [Ent] or go through fingerprint verification.
  If it is set to [1], for a example, a user who uses password inputs ID, which goes for authentication process without pushing any function key.
  The authentication mode is the currently setting mode.

3.5.2.3. Settings for card only authentication

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

- Once the setting is complete, press [ENT] to move to the upper menu.

Default screen ➡ [Ent] ➡ [3] ➡ [2] ➡ [Ent]

- Default setting : ‘0’
- Even for a user who is registered to be authenticated with a card & PW / card & fingerprint, he/she only needs to use a card if this option is set to '1'.
  This option is usually used when there are may terminals installed at the building entrance door where user entry/exit is frequent and the security level is relatively low.

3.5.3. Doorlock

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

Default screen ➡ [Ent] ➡ [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 [Ent] to move to the next setting.

Default screen ➡ [Ent] ➡ [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 [Ent] to move to the next setting

Default screen ➡ [Ent] ➡ [3] ➡ [3] ➡ [Ent]

- 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. Environment settings

3.5.3.3. Door open alarm

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

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

Default screen ➡ [Ent] ➡ [3] ➡ [3] ➡ [Ent] ➡ [1] or [2] ➡ [Ent]

- 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.

3.5.4. Volume

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

Default screen ➡ [Ent] ➡ [3]

- Press [4] for volume settings.

3.5.4.1. Voice

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

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

Default screen ➡ [Ent] ➡ [3] ➡ [4]

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

3.5.4.2. Buzzer volume

<Beeper volume>
(0-2):1

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

Default screen ➡ [Ent] ➡ [3] ➡ [4] ➡ [Ent]

- 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.

3. Environment settings

3.5.5. Current time

<Time Setting>
20090925211806

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

Default screen ➡ [Ent] ➡ [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 [Del] button before adding the new numbers.

3.5.6. Other

4. Sound Control
5. Time Setting
6. Other Setting

Default screen ➡ [Ent] ➡ [3] ➡ [6]

- Press [6] for other settings.

3.5.6.1. LCD Backlight On/Off

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

- Press [Ent] to move to the next setting

Default screen ➡ [Ent] ➡ [3] ➡ [6]

- Default setting : ‘0’.
- This is for LCD backlight on/off settings. If it is set to the default setting '0', LCD backlight is normally off. Only in cases that a user operates with keypad or card, LCD backlight goes on and after the working operation is done, it goes off in about 10 seconds. If it is set to '1', it always stays on.

3.5.6.2. LCD Brightness settings

<LCD Brightness>
(0-2):1

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

Default screen ➡ [Ent] ➡ [3] ➡ [6] ➡ [Ent]

- Default setting : ‘1’.
- This is for LCD brightness level setting menu. The higher setting value is for high brightness.

3.5.6.3. Display Time settings

<Display Time> : 1
0=20:30 1=PM 8:30

- Once the setting is complete, press [Ent] to move to the upper menu.

Default screen ➡ [Ent] ➡ [3] ➡ [6] ➡ [Ent] ➡ [Ent]

- Default setting : ‘1’.
- If it is set to the default setting '0', time is displayed as below.
  [07/08/25 21:30]
  If it is set to the default setting '1', time is displayed as below.
  [07/08/25 PM 9:30]

3.6. Searching Terminal info

Terminal ID=0001
Ver=10.00.01
Application=Access
Language=ENG Mode=SN

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

Default screen ➔ [Ent] ➔ [4]

- In the main menu, press [4] to select "4.Terminal info" and the following screen appears where all the environmental settings are displayed:

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. Environment 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 settings

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

- Once the setting is complete, press [ENT] to move to the upper menu.

Default screen ➡ [Ent] ➡ [5] ➡ [1]

- Default setting '0' : Releasing terminal lock
  '1' : Setting terminal lock
- Instead of a server program, an administrator can directly set up a terminal lock for a terminal.
  If it is set to '1', the terminal is locked and nobody can pass the door until an administrator unlocks the terminal.
- For this function, 'administrator entering OK' shall be checked in the terminal option of the server program.

3.7.2. Read card number

```
Place Your Card
```

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

Default screen ➡ [Ent] ➡ [5] ➡ [2]

- As an auxiliary function regardless of the terminal environmental settings,
  a terminal with a card reader can read the card number to register the card to a server.
  When the card is read by the terminal, the card number is displayed on the LCD window.

3.7.3. Interfacing with sensor for fire detection

```
<Fire detection Check>
[0/1=NO/2=NC]:0
```

- After setting the value, please press [Ent] and then move on upper menu

Default screen ➡ [Ent] ➡ [5] ➡ [3]

- Default setting '0'
- In terminal, it detects the connected sensor for fire detection.
  And then it transmits the connected server

3. Environment settings

3.8. Device settings

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

• Enter '084265' as the setting password and press [Ent] to view the detailed setting items.

Default screen ➡ [Ent] ➡ [6]

- A device setting is an option that is not necessary to change after installation, so it is recommended not to change it except when it is really required.
- This setting password is just for user information, so it cannot be changed.

3.8.1. System configuration settings

```
1. System Config
2. Set Fn-Key
3. Card Reader
```

Default screen ➡ [Ent] ➡ [6] ➡ '084265'+[Ent] ➡ [1]

- Press [1] for system settings.

3.8.1.1. User ID length settings

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

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

Default screen ➡ [Ent] ➡ [6] ➡ '084265'+[Ent] ➡ [1]

- Default setting: '4'
- This can be 2~8 digits and shall be the same as the ID registered in the server program. If the ID registered in the server program is '000075', enter 6.
- Special care is required when reducing the number of digits during normal operation because an administrator may not be able to be authenticated when he wants to enter menus due to the reduced number of digits.

3.8.1.2. Setting language

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

Default screen ➡ [Ent] ➡ [6] ➡ '084265'+[Ent] ➡ [1] ➡ [Ent]

- Default setting: '1'(English)
- This setting menu output voice message by designated language, '0': Korean, '1':English, '2':Japanese, '3':Spanish, '4':Portuguese, '5':Chinese.
- LCD characters correspond to the assigned language.

3.8.2. Function key settings

```
<Key On/Off>
1=F1 : O    2=F2 : O
3=F3 : O    4=F4 : O
5=Ent : O
```

• Once the setting is complete, press [Ent] to move to the upper menu.

Default screen ➔ [Ent] ➔ [6] ➔ '084265'+[Ent] ➔ [2]

- Default setting: all '0'
- This is for enabling/disabling the function keys. '0' is 'enable' and 'X is 'disable.
  Whenever a function key is pressed, it toggles between O/X.
- 1 is for [F1], 2 is for [F2], 3 is for [F3], 4 is for [F4], and 5 is for [Ent].
  If F1 becomes X by pressing [1], you can not change to start mode even if you press [F1].
- Additionally, if only [F1] or [F2] is set to '0', the terminal can be used in either always start or always leave mode.

3.8.3. Card reader settings

```
<Card Reade>:0
0=RF/SC
1=Wiegand
```

Default screen ➔ [Ent] ➔ [6] ➔ '084265'+[Ent] ➔ [2]

- This is the setting for the card reader connected to a terminal. This shall be set to 0 except in the following cases:.
- '0': 125KHz card or 13.56MHz card
- '1': Additional card reader is connected through wiegand interface.
  (EX: HID reader)

```
<Card Format >:0
0=Hexa 8byte
1=Hexa 16byte
2=Decimal
```

• Once the setting is complete, press [Ent] to move to the upper menu.

If it is set to the default setting '0', it is possible to set <Card Format> to change card number display format.

- Default setting: '0'
- '0': Displayed 8 digit number of 16 antilogarithm → A5CBEF12
  '1': Displayed 8 digit added behind of 8 digit number of 16 antilogarithm → A5CBEF1200000000
  '2': Displayed 10 digit number of 10 antilogarithm → 0317705125

```
<Dummy mode>
(N=0/Y=1) : 0
```

• After setting the value, please press [Ent] and then move on upper menu

- Default setting: '0'
- When it set up Dummy mode, it transmits card data with connected device from RS-232 by reading the card to terminal.

* In terminal, it does not deal with card data

3.8.4. Wiegand output settings

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

Default screen ➡ [Ent] ➡ [6] ➡ '084265'+[Ent] ➡ [4]

- Default setting: '0'
- When this is set to [1], 'Site code + user ID' is sent to the Wiegand port of the terminal when authentication is done.
  It can be used only for systems where there is a lock controller and the controller is operated by a Wiegand input.
  This is usually set to [0].
- If it is set to '1', user ID shall be shorter than 4 digits because 'Site code [1 byte] + user ID [2 bytes]' is transferred.
- If it is set to '2', user ID shall be shorter than 7 digits because 'Site code [1 byte] + user ID [3 bytes]' is transferred.

※ This is not effective when a Wiegand-type card reader is used, and set the following site code when the setting is higher than '1'

<Site code>
(0-255) : 000

- Default setting: '0'
- This is only available when Wiegand Out is set to '1' or '2'.
  Enter the site code (0-255) to be sent to the Wiegand port together with the user ID

• Once the setting is complete, press [Ent] to move to the upper menu.

3.8.5. Terminal initialization

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

Default screen➡ [Ent] ➡ [6] ➡ '084265'+[Ent] ➡ [5]

- Press [1] for settings initialization,
  press [2] for authentication record initialization,
  press [3] for factory initialization.

3.8.5.1. Settings initialization

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

• If initialization is successful three short beeps will be heard and the screen will go to the upper menu

Default screen➡ [Ent] ➡ [6] ➡ '084265'+[Ent] ➡ [5] ➡ [1]

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

※ If the settings are initialized, the language of the voice and menus becomes English. If you need to set other language ("6. Set Device" → "5. System Config" → <Language>: set to 0~4)

3.8.5.2. Authentication record initialization

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

Default screen➡ [Ent] ➡ [6] ➡ '084265'+[Ent] ➡ [5] ➡ [2]

- To initialize the record, press [1]. If not, press [2].
- Deletes all logs related to authentication, but settings and users are not deleted.
  Once initialization is done successfully, it moves to the upper menu together with a beeping sound

3.8.5.3. Factory initialization

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

• Once initialization is done successfully, the terminal is rebooted after three short beeps.

Default screen➡ [Ent] ➡ [6] ➡ '084265'+[Ent] ➡ [5] ➡ [3]

- To Factory Default settings, press [1]. If not, press [2].
- Except for the Mac (physical) address stored in the terminal, all settings, users and log information are deleted for the factory default.

※ If the settings are initialized, the language of the voice and menus becomes English. If you need to set other language ("6. Set Device" → "5. System Config" → <Language>: set to 0~4)

4. How to use the terminal

4.1. Access control

Default screen ➡ [Ent] ➡ [3]Option ➡ [1]Application ➡ [0]Access control settings

4.1.1. Authentication mode

Normal mode;
authentication with [Ent]

F1 mode;
authentication with [F1]

F2 mode;
authentication with [F2]

F3 mode;
authentication with [F3]

F4 mode;
authentication with [F4]

- Card authentication
  Before place the card, change the authentication mode by pressing the corresponding function key.
  or place the card for authentication.

- Password authentication
  After entering the user ID and changing the authentication mode by pressing the corresponding function key,
  enter the password for authentication.

4.1.2. Card authentication

For a user who is registered as [RF], [RF|FP], or [RF|PW], when placing the card close to the default screen, a beep sound will be heard and the authentication result appears on the LCD.

If you place your card close to the unit, you will hear a beep.

If authentication is successful, you will see a success message on the LCD together with the voice message "You are authorized". The door open icon and the card icon turn on LCD. The default screen appears after 1~2 sec., and the door is closed when the door open setting time has elapsed.

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

Non-registered card used.

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

For a user who is registered as [RF&FP] or [ID&FP | RF&FP], when placing the card close to the default screen, a beep will be heard and 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 beep.

4.1.3. Password authentication

If the user ID is "0001", enter "0001" and press the function key. You will hear a beeping sound and the terminal waits for the user password to be input. Enter the password and press [Ent], and the authentication result appears on the LCD.

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

You will hear a beeping sound and the terminal waits for the user password to be input.
Enter the password and press [ENT].
(The password is displayed as <*> on the LCD screen, rather than the actual numbers.)

If authentication is successful, you will see a success message on the LCD together with the voice message "You are authorized". The door open icon and the card icon turn on LCD. The default screen appears after 1~2 sec., and the door is closed when the door open setting time has elapsed.

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

Password authentication failed.

Non-registered user ID entered.

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

4.2. Time Attendance control

Default screen ➔ [Ent] ➔ [3]Option ➔ [1]Application ➔ [1]T&A (Time Attendance) settings

If the start/leave time is fixed, set <start time>, <leave time>, and <normal time> to reduce user input errors.

4.2.1. Authentication mode

Normal mode; authentication with [Ent]

Start mode;
authentication with [F1]

Leave mode;
authentication with [F2]

Leave mode;
authentication with [F2]

Outside work mode;
authentication with [F3]

- Card authentication
  Before place the card, change the authentication mode by pressing the corresponding function key, or place the card for authentication.
- Password authentication
  After entering the user ID and changing the authentication mode by pressing the corresponding function key, enter the password for authentication.
- Working mode after authentication depends on <start time>, <leave time>, and <normal time> settings.
  The previous authentication mode is maintained if no mode is set for a specific time period.

4.2.2. Working mode expansion using multi-key authentication

- Same as 4.1.2.

4.2.3. Password authentication

- Same as 4.1.3.

4.2.4. Working mode expansion using multi-key authentication

- If more than 5 working modes such as start, leave, outside work, return, and general are required, it can be expanded up to 41 modes.
- After **Default screen ➔ [Ent] ➔ [3]Option ➔ [1]Application ➔ [1]T&A (Time Attendance) settings** set more than one key to '0'. However, the keys set to 'X' are not the case.
- Because a mode is defined with a number key, enter a number key after entering the function key for authentication. In the server program, authentication mode is "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 authentication "F4+1"mode

4.3. Meal control

Default screen➔ [Ent] ➔ [3]Option ➔ [1]Application ➔ [2] Meal settings

- If the terminal is set for meal control, as the terminal is in "lock setting!" status during other time frames except for the meal times previously set, at least more than one time frame as meal time should be set for meal control usage.
- Basically, a single authentication is allowed for each meal per user but double authentication is also possible **Default screen➔ [Ent] ➔ [3]Option ➔ [1]Application ➔ [2] Meal settings ➔ <Without Limit>**

4.3.1. Meal classification

- In meal control, the function key is just an operation key for authentication. There is just meal classification with a meal time frame - there is no mode classification. The number shown in the LCD screen means the number of authentication for a specific meal time period.

Total number of successful authentication is displayed.

Not in meal time period

In case that a user tries double authentication during the same meal time period

4.3.2. Card authentication

- Same as 4.1.2., but [Ent] cannot be used as a function key.

4.3.3. Password authentication

- Same as 4.1.3., but [Ent] cannot be used as a function key.

LG

P/N : MFL62731801