AC-2100 Plus User Guide

Version Eng-1.00

<Revison History>

Version	Date	Description	Firmware Version
1.00	2016-12-01	-Initial Release	10.61.00-000.00

<Glossary>

- Admin (Administrator)
  - A user who can enter into the terminal menu mode, who has the authority to register / modify / delete the terminal's user and change the operating environment through setting change.
  - If there is no administrator registered on the terminal, **it is recommended to register at least one administrator** since anyone can enter the terminal menu and change the setting.
  - The administrator has the right to change the important environment settings of the fingerprint recognition device, so it requires special care in registration and operation.

- 1:1 Verification (1 to 1, Verification)
  - It is the method to authenticate fingerprints with a user ID or card.
  - It is called 1: 1 verification because it compares only the fingerprint of the user registered in the user ID or card.

- 1:N Identification (1 to N, Identification)
  - It is the method to find the user by fingerprint only.
  - It is called 1: N authentication because it is the method to find the same fingerprint as the input fingerprint among fingerprints registered without user ID or card input.

- Authentication level
  - This is the level used for fingerprint authentication. It is displayed in steps 1 ~ 9 according to the degree of fingerprint matching. Authentication must be successful if the match between two fingerprints is higher than the set authentication level.
  - The higher the authentication level is, the higher the security is.
    Nevertheless, as it relatively requires the higher match rate, the probability of authentication failure is higher when authenticating.
  - 1:1 authentication level: Authentication level used for 1:1 verification
  - 1:N authentication level: Authentication level used for 1:N Identification

- Authentication Method
  - This represents the various types of authentication including FP (Fingerprint) authentication, RF (Card) authentication or a combination of each method.
    Ex) Card or FP: Authentication with card of fingerprint.

- Function Keys
  - It is [F1], [F2], [F3] and [F4] keys, which can enter the menu and change the mode of office start or leave.

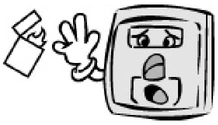
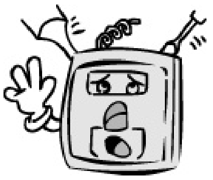
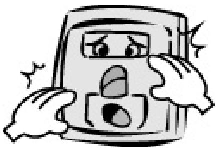
- LFD (Live Finger Detection): Anti-imitation fingerprint function
  - This function allows the input of only real fingerprints and blocks the input of imitation fingerprints produced using rubber, paper, film and silicone.

Table of Contents

1. Before Use

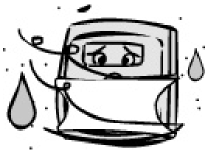
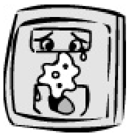
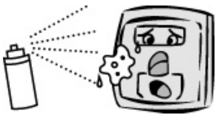
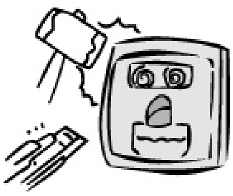
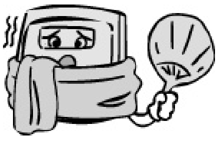
1.1. Safety Precautions

- Warning

Do not handle the unit with wet hands and do not allow liquid to flow into or on it. -> It may cause an electric shock and damage. 	Do not place a fire source near the unit. -> It may cause a fire. 
Do not disassemble, repair, or modify the unit. -> It may cause an electric shock, fire or damage. 	Keep out of children's reach. -> It may cause an accident or damage. 

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

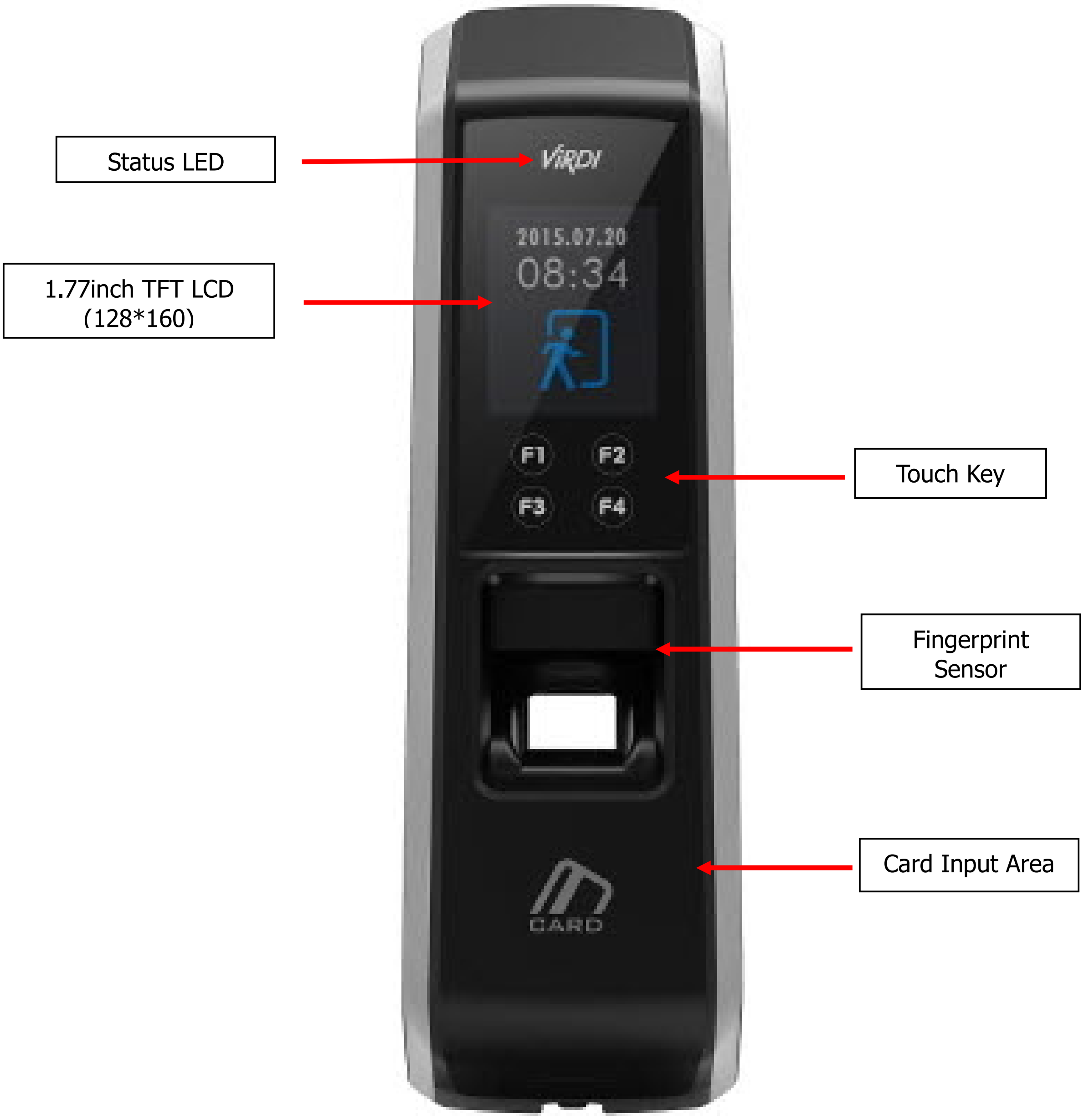
- Cautions

Keep away from direct sunlight. -> It may cause mal-function, deformation or change the color of the unit. 	Avoid high humidity or dust. ->고장의 위험이 있습니다. 
Avoid using water, benzene, thinner, or alcohol for cleaning the unit. -> It may cause an electric shock or fire. 	Do not place a magnet near the unit. -> The unit may break down or malfunction.
Avoid getting the fingerprint input area dirty. -> It may prevent the unit from recognizing the fingerprint. 	Avoid using insecticides or flammable sprays near the unit. -> It may result in the deformation or change the color of the unit. 
Avoid impact or using sharp objects on the unit. -> The unit may get damaged and broken. 	Avoid installing the unit in a place where temperature changes severely. -> It may cause the unit to malfunction. 

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

※ We are not responsible for accidents or damages caused by not using them as described in this manual.

1.2. Terminal Description



1.3. Button for operation

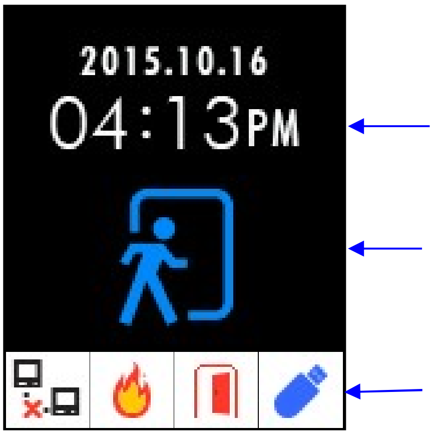
F1	- Change from main screen to **[Attend]** mode. - Move up or increase **[↑]** button in the menu mode.
F2	- Change from main screen to **[Leave]** mode - Move down or decrease **[↓]** button in the menu mode.
F3	- Change from main screen to **[Outdoor]** mode - When pressing for more than 2 seconds, enter the menu mode - Used to enter [**ENT**] or move left [←] in the menu mode. When pressing it for more than 2 seconds, it is used to **[ESC]** button: **[ESC~]**
F4	- Change from main screen to **[Return]** mode. When pressing it again, **[Return]** mode is changed into **[Access]** mode. - Used to enter **[Enter]** or move right **[→]** in the menu mode. When pressing it for more than 2 seconds, it is used to **[ENT]** button: **[F4~]**

1.4. During operation, *ViRDI* Logo LED is displayed as below.

ViRDI	Power	Blue	On: Normal
ViRDI	Door	Green	On: Door Open Off: Door Close
ViRDI	Alarm	Red	Off: Normal Flickering: Open lid, Lock controller communication error

※ LED turns on at the same time depending on the situation.

1.5. Screen display during operation



Shows the current time

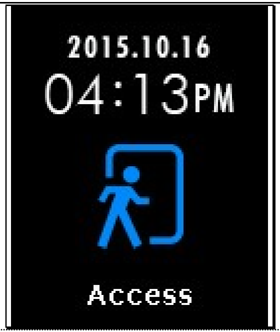
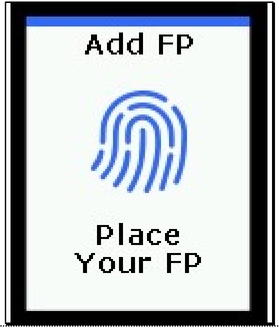
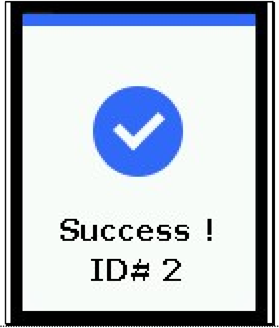
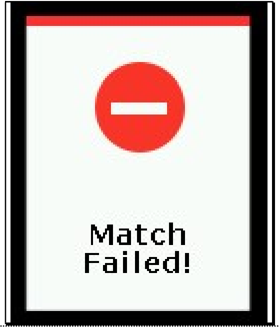
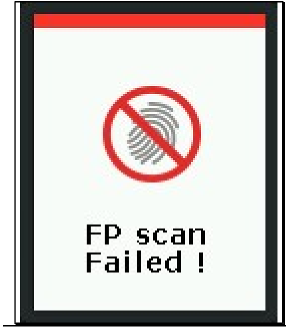
When access control, shows **[Access]** mode. (F1, F2, F3, F4, Access)
When TNA, shows **[Attend/Leave]** mode.
(Attend, Leave, Outdoor, Return)

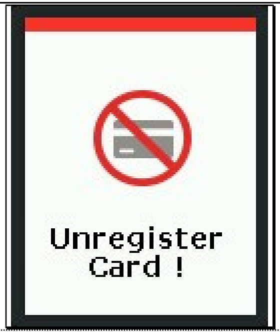
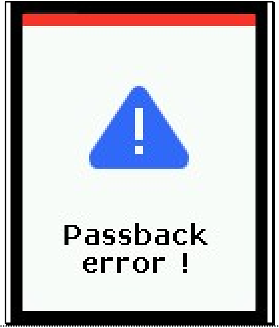
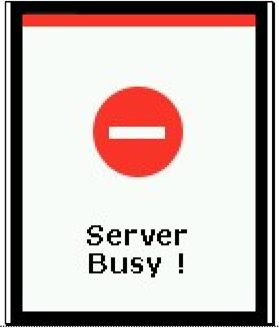
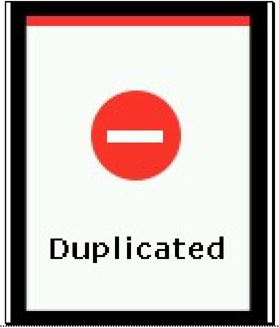
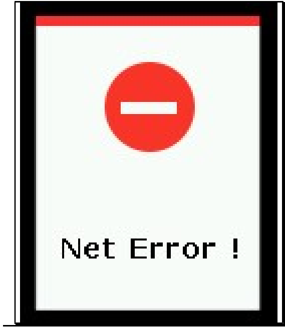
Shows the status icon and **[Access]** mode.

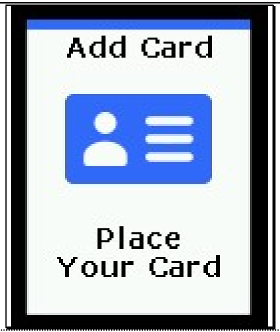
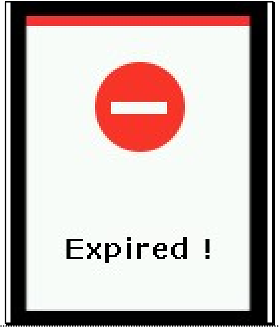
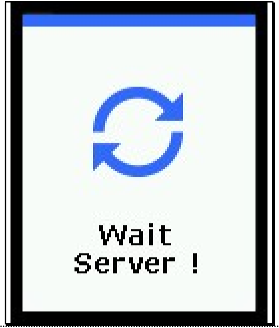
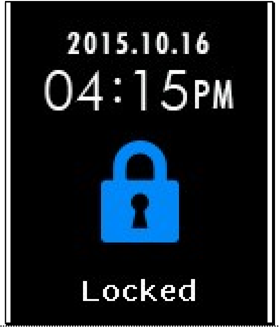
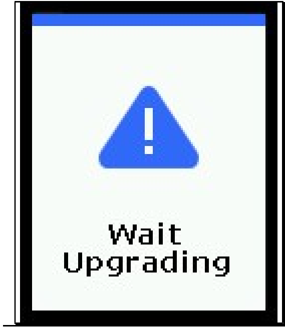
1.5.1 Icons

① Fire Detection	🔥	A fire is detected by the fire detection sensor. (When connecting the fire detection sensor)
② Door Status	🚪	Doors open (Forced to open door or door open continuously)
③ Server Connection Status	🖧 🖧	LAN cable is not connected. Only link is connected.
④ USB Connection	🔌	USB is connected.

1.5.2 Message Information

	- The default screen of AC-2100 (Plus)
	- The fingerprint is being input or ready.
	- When authentication is successful.
	- When authentication fails.
	- When fingerprint input fails. - When your finger is taken off too early before your fingerprint is entered.

 Unregister Card !	- When an unregistered card is entered. - When 1:N Authentication is attempted under the condition that authentication priority is SN and there is no user who has been allowed for 1:N Authentication
 Passback error !	- When anti-pass back is in error.
 Server Busy !	- When the server cannot handle since there are too many authentication requests from terminal.
 Duplicated	- When the terminal is set to [**Meal Management**] and users attempt more than 2 times authentication in the same meal time.
 Net Error !	- When there is no response from the server during authentication attempt - When the network is disconnected during authentication attempt to the server

 Add Card Place Your Card	- When the card input is ready
 Expired !	- When the card is registered but its authentication is attempted even if it is not the access control time.
 Wait Server !	- When the terminal waits for a response after requesting authentication to the server.
 2015.10.16 04:15PM Locked	- When the terminal is locked - When the meal management is set in the non-meal time.
 Wait Upgrading	- When the terminal program is upgraded (Do not power off the terminal when this message is displayed)

1.6. Voice guide during operation

Operation	Voice guide
When the fingerprint is entered	Please enter your fingerprint.
When authentication is successful	You are authorized.
When authentication fails	Please try again.

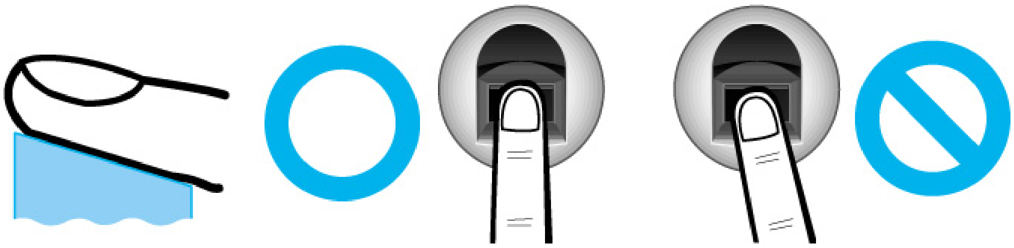
1.7. Buzzer guide during operation

Ppik	When button or card is operated	-If the button is pressed or if the terminal reads the card -If your finger may be taken off because your fingerprint has been successfully entered.
Ppibik	When failure	If authentication fails or the user’s input is wrong
Ppiriririk	When input is ready	When it is notified that fingerprint input is ready
Ppiririk	When success	When authentication is successful or if the current user finishes settings

1.8. How to register and enter the correct fingerprint

- How to correctly register the fingerprint

  Enter your fingerprint as if you take a thumbprint by using your forefinger if possible.
  The fingerprint cannot be correctly registered and entered only by your fingertips.
  Please touch the center of fingerprint on the fingerprint input section.

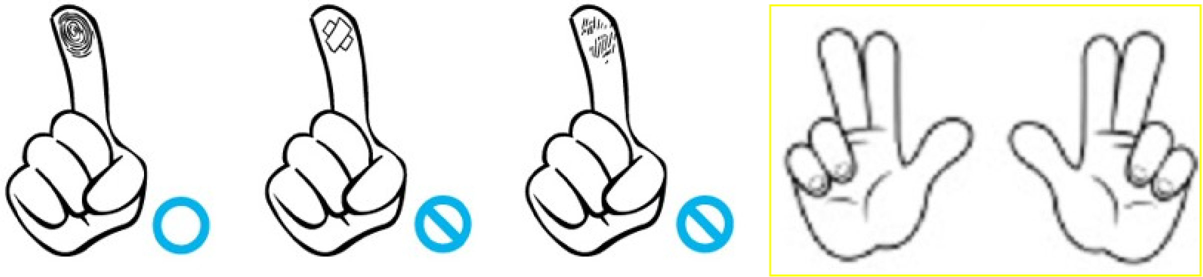


- Please enter the fingerprint of forefinger if possible.

  When using your forefinger, you can enter your fingerprint correctly or safely.

- Make sure that the fingerprint is unclear or wounded.

  Too dry, wet, blurry or wounded fingerprints are difficult to recognize. In this case, the fingerprint of another finger should be registered



- Precautions depending on your fingerprint status

  The availability of the fingerprint may vary depending on your fingerprint status.

  - This product consists of a fingerprint recognition system and cannot recognize the damaged or unclear fingerprints. They should be registered with a password.

  - **If your hands are dry, you can blow it out** to operate it more smoothly.

  - For children, too small or unclear fingerprints may be difficult or impossible to use. They need to register a new fingerprint every six months.

  - For seniors, the fingerprint with too many lines may not be registered.

  - It is recommended that you will register more than 2 fingerprints if possible.

  - In order to increase the fingerprint authentication rate, it is recommended to use six of ten fingers as the picture above. (Both thumbs, forefingers, middle finger)

2. Product Description

2.1. Product Features

● **Access Control system with the network (LAN)**

- The fingerprint reader communicates with the authentication server using a UTP cable and TCP/IP protocol. This terminal can be applied to the existing LAN network and has easy expandability. It ensures a fast speed by **10/100 Mbps Auto Detect** and facilitates management and monitoring via the network.

● **Convenient Auto Sensing function**

- The authentication function can be simply operated by entering the fingerprint without separate keys entered.

● **Simple Identification via fingerprint**

- By using the biometrics (Fingerprint recognition technology), it can prevent when the user forgets the password and the loss or theft of cards or keys and it can enhance the security of identification since it uses the fingerprint.

● **Convenient Information Message with LCD and voice**

- The information message is voiced or displayed on the LCD display for each operation to receive certification so that you can easily input. In particular, thanks to a built-in backlight for the LCD display, you can easily identify the screen and operate keys in the dark room.
- The voice is stored in the memory and it can be changed to a desired voice from the server.

● **Provide the diverse and flexible access control feature**

- Easy to use it without the risk of rental, counterfeit and loss of your key or card
- Provide the complete access control function by granting access authority for user groups
- Provide the flexibility of access control by allowing the access time restrictedly
- Economical maintenance and development costs compared to other access control devices
- Remove the inconvenience that visitors are registered in the management office and then separate cards are issued.

● **Can be used as various operating system such as crime prevention, access, attendance, and meals**

- Support various operating methods according to the operation method setting of terminal menu.

● **Large processing capacity of server**

- When the terminal information is managed by server, it can be processed almost infinitely.
-

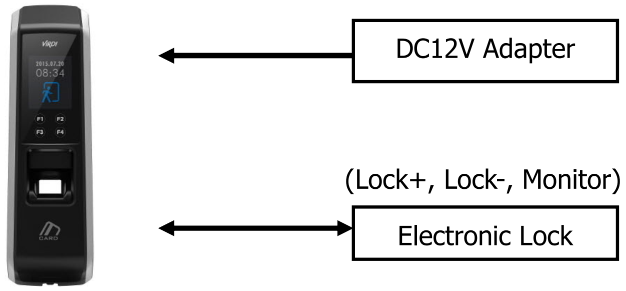
- **Provide the printer interlocking feature**
  - Whenever authentication, it provides the feature that the authentication information can be printed via the printer.

- **Provide various registration and authentication method**
  - There are a total of four registration and authentication methods for general users. Before registering users or administrators, you should determine how to register and authenticate.

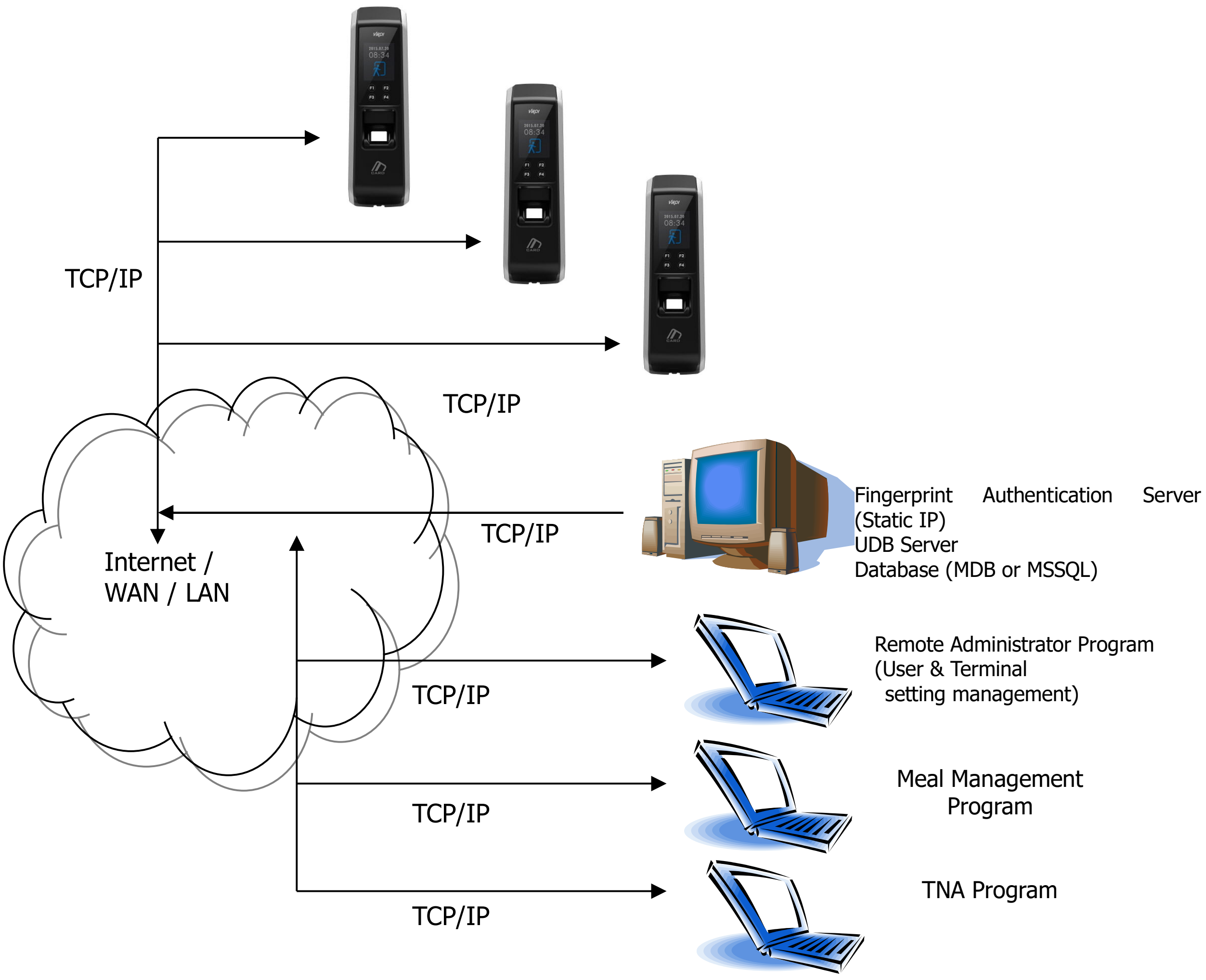
FP	Fingerprint Registration Fingerprint Authentication
Card	Card Registration Card Authentication
Card or FP	Card and Fingerprint Registration Card or Fingerprint Authentication
Card and FP	Card and Fingerprint Registration Card Authentication and then Fingerprint Authentication

2.2. Configuration Diagram

2.2.1. Standalone Use (Access)



2.2.2. Connect the PC server (Access, TNA, Meal Management)



2.3. Product Specification

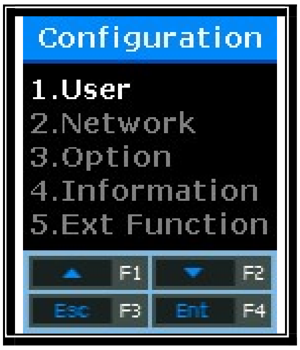
Category	SPEC	REMARK
CPU	32 bits RISC CPU(400MHz)	
MEMORY	64M SDRAM	
	32M NOR FLASH 128M NAND FLASH	1,500 User 1,500 Finger 10,000 Log
Fingerprint Sensor	Optical	
Authentication Speed	Less than 1 second	
Scan Area / Resolution	12.6 * 14.8mm / 500 DPI	
FRR / FAR	0.1% / 0.0001%	
Communication Port	TCP/IP	Authentication server communication
	RS-232	Printer
	RS-485	External device communication
	Wiegand In/Out	Card Reader or External device communication
Temperature / Humidity	-20 ~ 60 / Lower than 90% RH	
LCD	1.77" Color LCD	
SIZE	58mm(W) * 191mm(H) * 62mm(D)	
AC / DC Adapter	INPUT : Universal AC 100 ~ 250V	
	OUTPUT: DC 12V (Option : DC 24V)	
	UL, CSA, CE Approved	
Card Reader	Smart Card Reader	14443A type, 13.56MHz

3. Environment Setting

3.1. Before Environment Setting

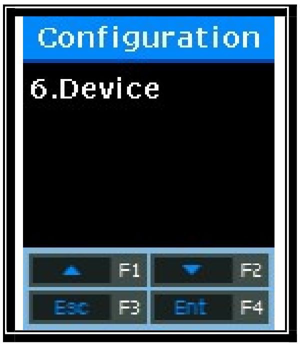
3.1.1. Menu

When pressing **[F3]** button for more than 2 seconds, the administrator authentication screen will be displayed.


Configuration

1.User
2.Network
3.Option
4.Information
5.Ext Function

Select the menu you want to change by using **[↑](F1)** and **[↓](F2)** buttons, and press **[ENT](F4)** button to go to the submenu.

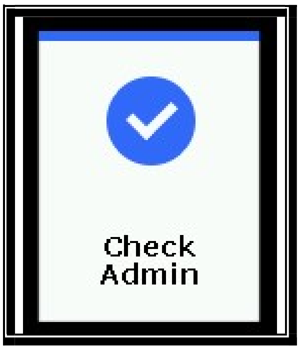

Configuration

6.Device

The description of function buttons such as **[F1]**, **[F2]**, **[F3]**, and **[F4]** is in numerical order on the bottom of the screen as shown above. Go up and down the screen, you can press **[ENT](F4)** button to select the desired menu, or press **[ESC](F3)** for more than 2 seconds to return to the upper menu.

3.1.2. Admin Authentication

After entering menu, the screen is displayed as below.



The administrator is verified by either card of fingerprint depending on the authentication method. Upon successful authentication, the screen goes to the following menu.

※ **The administrator authentication menus is displayed only when there is any registered administrator.** Once it is authenticated to enter the menu mode, you can access to all menus until you escape completely from the main menu.

3.1.3. Modify Settings

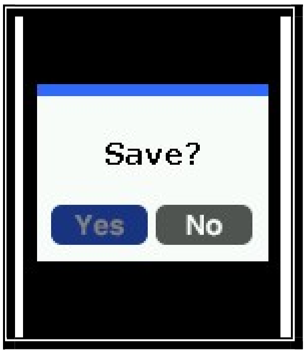
Modify the existing settings by pressing **[↑][↓]** buttons.
If the set value is more than 2 digits, press **[←][→]** buttons to move to the place that you want to change and press **[↑][↓]** buttons to change the value up or down.

Press **[ENT]** button to check the set value or go to next setting.
If you want to cancel during the setting and move to the upper menu, press **[ESC]** button for more than 2 seconds.

If only **[←][↑][↓][→]** buttons are displayed except **[ESC]** and **[ENT]** buttons, **[ESC]** is enabled by pressing **[F3]** for more than 2 seconds, and **[ENT]** by pressing **[F4]** for more than 2 seconds.

3.1.4. Set the environment and save

After changing settings, press **[ESC]** button on the main menu screen to save the changes, and the following screen will be displayed.



Select **[Yes]** button to save modifications, **[No]** button to cancel modifications, and then press **[ENT]** button. If there is any modified information, the terminal will be rebooted.

- If there is no change information, the screen goes out from the environment setting menu without the "**Save?**" process.

- If no data is input in the main menu for a certain time during changing environment setting, the screen will exit from the environment setting menu. In this case, if there is any change in the menu, the screen performs the "**Save?**" process. If there is no change in the menu, the screen goes to the main screen without saving changes.

3.2. Menu Configuration

1. User	1. Add User 2. Delete 3. Modify 4. Add admin 5. Delete All	
2. Network	1. Terminal ID	<Terminal ID > <Auth Mode>:NS/SN/NO/SO
	2. Terminal Net	<Net Type> <Terminal IP> <Subnet Mask> <Gateway>
	3. Server Net	<Server Type> <Server IP> <Server Port>
3. Option	1. Application	<WorkMode> 1. Access 2. T&A 3. Cafeteria
		When setting to Access <F1 Time> <F2 Time> <F3 Time> <F4 Time> <Access Time> <Multi Fn-Key> <Use Printer> <Use Key>
		When setting to T&A < Attend> <Leave > < Out> < In> <Access Time> <Multi Fn-Key> <Use Printer> <Use Key>

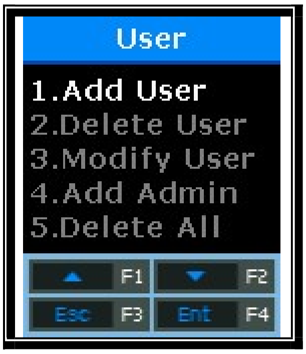
		When setting to Cafeteria <Breakfast> <Lunch> <Dinner> <Supper> <Snack> <No Limit> <Use Printer> <Use Key>
	2. Verify	<Show User> <Only Card> <Use TOC> <Blocking Time> <Global Block> <NetErr TimeOut>
	3. Doorlock	<Open Duration> <Open Alarm>
	4. Sound	<Voice> <Beep> <Case Open>
	6. Time	<Sync Time> <Calendar> <System Time> <Time Display>
	6. RS485 Set	<RS485 ID>

4. Terminal Info	Version	Firmware version of the terminal
	WorkMode	Terminal operating modes (T&A + security/T&A/food service)
	Language	Language setting
	Auth Mode	Authentication priority
	1:1 Level	Authentication level applied when 1:1 authentication
	1:N Level	Authentication level applied when 1:N authentication
	Terminal Id	Terminal ID
	Net Type	Network connection methods (Static IP/DHCP)
	Terminal IP	Terminal IP address
	Gateway	Terminal Gateway address
	Subnet Mask	Terminal Subnet Mask address
	Server Type	Network server connection mode setting
	Server IP	IP address of the network server connected to the terminal
	Server Port	Port number of the network server program
	MAC Address	Terminal MAC address
	Card Ver	Card reader module firmware version
	Card Format	Card data display format
	All User	The total number of users registered in the terminal, including administrators
	All Admin	The number of administrators registered in the terminal
	Max User	The maximum number of users who can be registered in the terminal
	All FP	The total number of fingerprints saved in the terminal
	Max FP	The maximum number of fingerprints that can be registered in the terminal
	All Log	The number of the authentication result saved in the terminal
	Max Log	The maximum number of the authentication results that can be save in the terminal
	Serial Num	Display serial number
5. Ext Function	1. Lock Term	<Lock Term>
	2. Read Card	<Read Card>

	3. Monitor	<Monitor 1> <Monitor 2>
	4. Duress FP	<Duress FP>
6. Devicev	1. Sys Config	<ID Length> <Language>
	2. Card Format	<Card Reader> <Card Format>
	3. FP-Sensor	<1:1 Level> <1:n Level> <LFD Level> <Check FP>
	4. Wiegand	<Wiegand Out>
	5. Initialize	<Init Config> <Delete Log> <Init Terminal> <DB Backup>
	6.Ext Device	<External Device> <Local AntiPB> <Auth Mode> <Lock Ctrl>

3.3. User Management

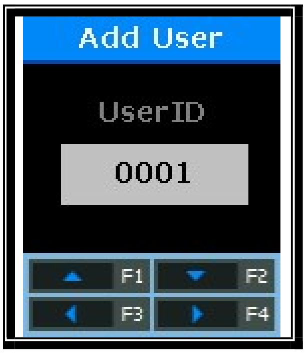
Select **[1. User]** on the main menu, and the following screen will appear.



Press **[↑][↓]** buttons to select the menu you want to change, and press **[ENT]** button.

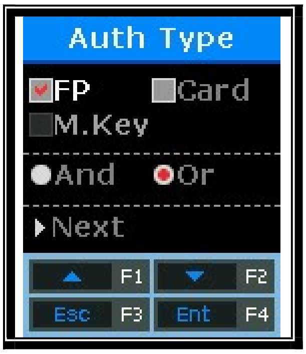
3.3.1 Add User

Select **[F3~]** → **[1. User]** → **[1. Add User]** on the main screen, and the following screen will be displayed



Enter the ID of the new user you want to register, and press **[F4]** button long.

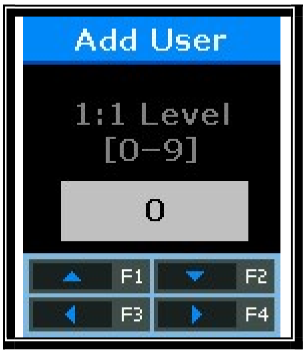
When registering, the available user ID is automatically displayed on the LCD so that you can register it conveniently. If necessary, you can change the ID by using function keys. If the other user has been already registered in the entered ID, the message of “Duplicated User ID” with “Fail” buzzer is displayed on the LCD and then the screen goes to the upper menu. If the entered ID is not registered, the following authentication type selection screen appears.



By using **[↑][↓]** buttons,
select the authentication type and **[And]** or **[Or]**, and press **[Next]** button

3.3.1.1. Add FP

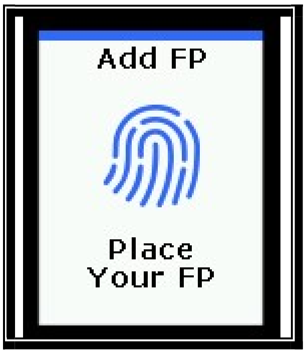
Register the fingerprint and authenticate by fingerprint.



Default Setting: '0'

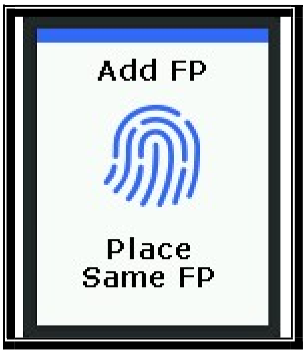
This screen is available to determine the authentication level for each user to be registered. By changing this value, the different authentication level may be set for each registered user.
If this value is set to '0', the 1:1 Level set in the terminal is used instead of the user-specific authentication level.

After finishing setting, select **[ENT]** button to move to the next setting.



Add your fingerprint referring "1.8 How to register and enter the correct fingerprint" in pg.13.

When the fingerprint sensor is on, place your finger on the fingerprint input window. When "Ppik" buzzer sounds, wait for 2~3 seconds until the light turns off and take your fingers off. When the first fingerprint is successfully entered, the message "Please try again." is displayed. And then register the same fingerprint once again.


Add FP

Place
Same FP

Enter the same fingerprint once again.

It should be noted that when entering the second fingerprint after entering the first fingerprint, you must take off your finger from the fingerprint input window and then enter the second fingerprint again. When the registration is completed, select **[Add FP]**. If it fails, the screen returns to the **[1. User]** screen.

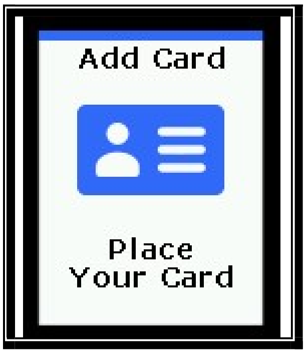
Below is the LCD message during registration process.

Register Success!	When registration is successful
Fail!	When registration fails
	If the fingerprint image is unclear, or if no fingerprint is entered for ten seconds after the FP sensor lights off
Duplicated FP!	If the fingerprint registered already is registered again

If registration fails even if you try to repeat 2-3 times depending on the correct fingerprint registration method, it is recommended to authenticate by using the card.

3.3.1.2. Add Card

Register only card and authenticate by the card.


Add Card

Place Your Card

Place the card to register on the fingerprint window. To cancel the registration and exit, select [**ESC**] button.

When the registration is completed, select [**Add FP**] about whether to register the additional cards. If it fails, the screen returns to [**1. Add User**] menu.

The following shows the notice message during registration.

Register Success!	When the registration succeeds
Fail!	When the registration fails
Duplicated Card!	If the registered card is registered again

3.3.1.3. Fingerprint or Card registration

Register the user with card and fingerprint and then authenticate with card or fingerprints when authenticating.

To register the user, please register the fingerprint (refer the fingerprint registration) and then card (refer the card registration).

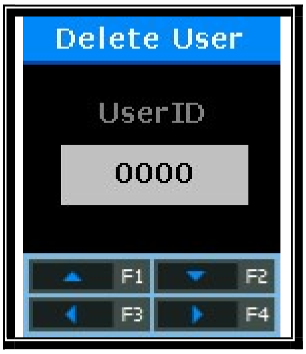
3.3.1.4. Fingerprint and Card registration

Register the user with card and fingerprint and it requests to authenticate with card and then with fingerprint.

To register the user, please register the fingerprint (refer the fingerprint registration) and then card (refer the card registration).

3.3.2. Delete User

Select [**F3~**] → [**1. User**] → [**2. Delete**] on the main screen, and the following screen is displayed.


Delete User

UserID

0000

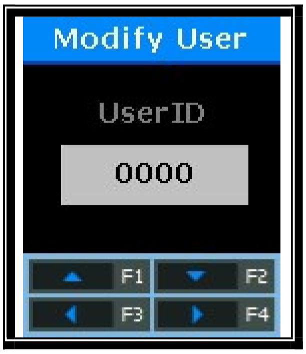
Enter the new user ID to delete and press [**F4**] button long.

Enter the user ID to delete from the registered users of the terminal and press [**F4**] long, the success buzzer sounds and then all the information will be deleted from the terminal. However, the data deletion from the terminal doesn't mean the data deletion from the server. To delete the data permanently, it must be deleted from the server as well.
If the ID of an unregistered user is entered, the message of "Unregister" with "Fail" buzzer is displayed on the LCD and then the screen goes to [1. User] menu.

Please note that it will not be possible to recover if you delete the user registered in the terminal only because it is not registered in the network server.

3.3.3. Modify User

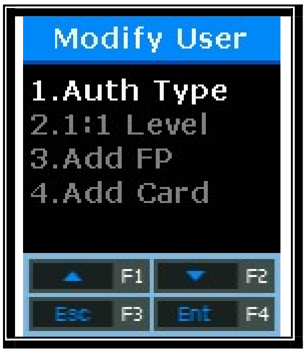
Select [**F3~**] → [**1. User**] → [**3. Modify User**] on the main screen, and the following screen is displayed.



Enter the user ID to modify and press [**ENT**] button long.

Both general users and administrators can be changed without distinction. If the ID of an unregistered user (or administrator) is entered, the message of "Unregister" with fail buzzer is displayed on LCD and then screen goes to [**1. User**] menu.

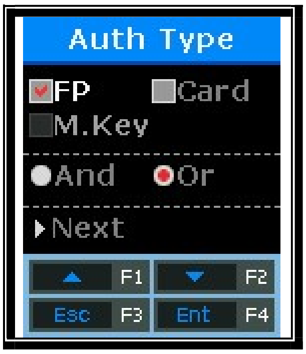
The changeable items of users are different according to the user authentication method and are classified as below.



Select [**1. Auth Type**] to change the authentication method; [**2.1:1 Level**] to modify the authentication level; [**3. Add FP**] to add fingerprint in the relevant ID; [**4. Add Card**] to add the cards.

※ Up to 10 fingerprints/cards per ID can be registered. If you try to register more than 10 fingerprints/cards, when selecting [**3. Add FP**] or [**4. Add Card**], "Fail" buzzer sounds and the message of "User FP/Card Full!" is displayed on the LCD.

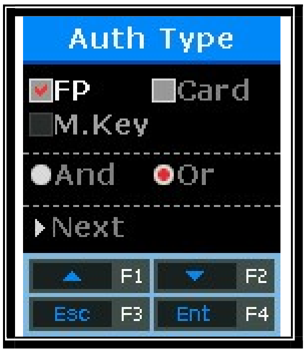
[1] Auth Type



By using [↑][↓] button, select the authentication method and [**And**] or [**Or**] and then [**Next**] button.

To modify, select the authentication type referring p.27~p.29 in [**3.3.1.1**]~[**3.3.1.4**].

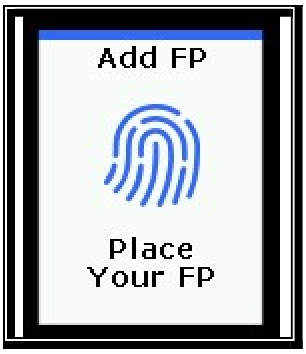
[2] 1:1 Level



Recommended Setting: '0'

To modify, enter the new setting value.
If this value is set as '0', 1:1 level set in the terminal is used instead of the user-specific authentication level.

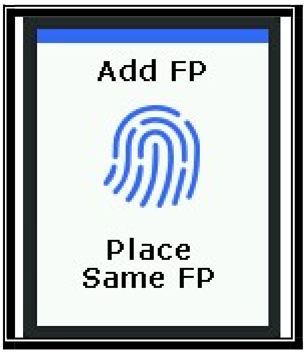
[3] Add FP



Refer "1.8 How to register and enter the fingerprint" in pg.13.

When the fingerprint sensor lights on, place your finger on the fingerprint input window. When "Ppik" buzzer sounds, wait for about 2~3 seconds until the light turns off, and lift your finger.
When the first fingerprint is successfully entered, the message of "Please try again" is

displayed. Enter the same fingerprint twice.



Add FP

Place
Same FP

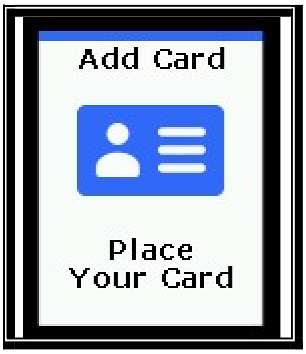
Enter the same fingerprint once again.

Please note if you enter the first fingerprint and then enter the second fingerprint, you should remove your finger and enter it on the fingerprint input window. When the fingerprint addition is complete, select whether or not to register the additional fingerprints. If fail, return to [**3. Modify User**] screen.

Below is the LCD message during the registration.

Register Success!	When registration is successful
Fail!	When registration fails
	If the fingerprint image is unclear, or if no fingerprint is entered for ten seconds after the FP sensor lights off
Duplicated FP!	If the fingerprint registered already is registered again
User FP Full!	If ten fingerprints have been registered in the relevant ID

[4] Add Card



Add Card

Place
Your Card

To cancel the registration, select [**ESC**] button.

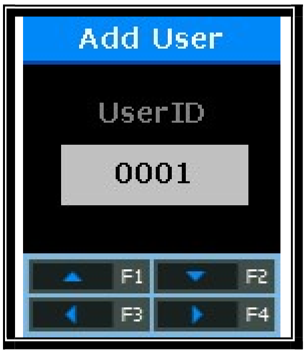
When placing your card on the LCD, the successful buzzer sounds and the newly entered card number is added.
If card change fails, the "Fail" buzzer sounds and the screen returns to the [**3. Modify**] menu.

Below is the LCD message during the registration.

Register Success!	When registration is successful
Fail!	When registration fails
Duplicated Card!	If the card registered already is registered again
User Card Full!	If ten fingerprints have been registered in the relevant ID

3.3.4. Add Admin

Select [**F3~**] → [**1. User**] → [**4. Add Admin**] on the main screen, the screen below is displayed.



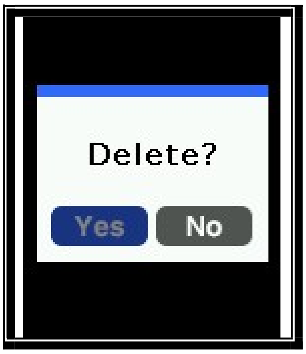
Enter the Admin ID to register and select [**F4**] button long.

※ Since then, the admin registration process is same as the general user registration.

Only the registered user as administrator has the authority to change the operation environment of the terminal and register/modify/delete all the information of the saved users in the terminal.
Therefore, special attention is required for the registration of the terminal administrators.

3.3.5. Delete All Users

Select [**F3~**] → [**1. User**] → [**5. Delete All**] on the main screen, and the screen below is displayed.



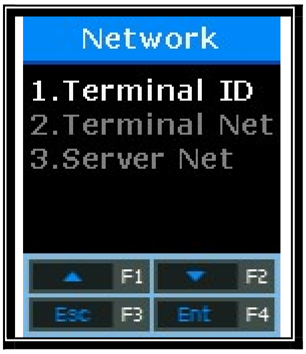
Select [**1**] to delete all users and [**2**] to cancel.

After requesting reconfirmation, **all users including administrators are immediately deleted**. **Before using this function, special attention is required**.

After successful deletion, the successful buzzer occurs and then the screen returns to [**1. User**] menu.

3.4. Network

Select [**2. Network**] on the main menu, and the screen below is displayed.

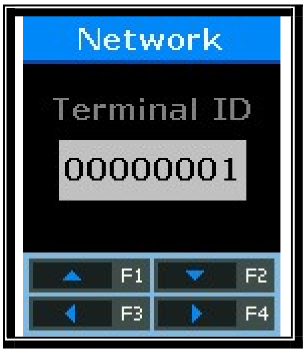


Press [↑][↓] buttons to select the menu to change, and press [**ENT**] button.

3.4.1. Terminal ID

Select [**F3~**] → [**2. Network**] → [**1. Terminal ID**] on the main screen, and the screen is displayed

3.4.1.1. Terminal ID



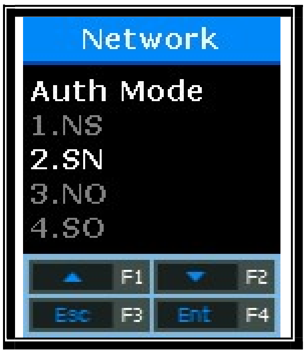
Terminal ID

00000001

This ID is the unique ID used to allow the server to identify the terminal. The default value is '00000001'. Default setting: '00000001'

This ID must match the door ID set to the server program and is entered as an 8-digit number. Press [**ENT**] button long, and go to the next menu.

3.4.1.2. Auth Mode [NS / SN / NO / SO] setting



Network

Auth Mode

1.NS

2.SN

3.NO

4.SO

Select [**1**] for **NS**, [**2**] for **SN**,
[**3**] for **NO**, and [**4**] for **SO**.
Default Setting: [**2.SN**]

This menu is to determine the authentication priority between the terminal and the network, the default is [**2. SN**], and the authentication method in each mode operates as follows.

NS	If the terminal is connected to the server, authentication is attempted from the server. If the terminal is disconnected from the server due to a network failure, etc., authentication is attempted from the terminal.
SN	Even if the terminal is connected to the server, authentication is attempted from the terminal. The authentication result is sent to the server in real time. However, if the entered user is not registered in the terminal, authentication is attempted from the server. (If there is any fingerprint user in the terminal, the 1:N fingerprint authentication is not performed in the server.)
NO	Even if the user is registered in the terminal server, authentication is performed through the server only.
SO	Only users registered in the terminal are authenticated. If the terminal is connected to the server, the authentication result is sent to the server in real time.

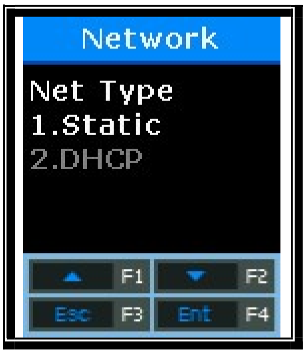
The authentication priority may be set flexibly depending on the situation such as the number of terminals connected to the server, the number of authenticated users, or network failure. However, if more than 10 terminals are connected to the server and so concurrent authentication is often attempted, or if network failure often occurs, it is recommended to attempt SN authentication (set to '2').

After entering correctly, press [**ENT**] button, and the screen will go to the upper menu.

3.4.2. IP setting

Select [**F3~**] → [**2. Network**] → [**2. Terminal Net**] on the main screen, and the following screen is displayed.

3.4.2.1. Connection Method Setting



Network

Net Type
1.Static
2.DHCP

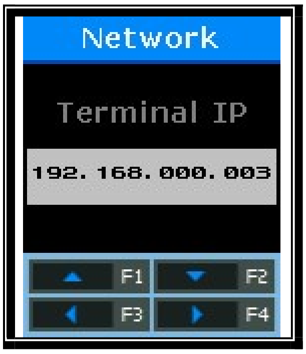
Select [**1**] if Static IP is assigned, and select [**2**] to set IP using DHCP.
Default Setting: [**1. Static**]

This refers about how to connect terminal to network. The default value is [**1. Static**]. Select [**1**] when using the Static IP assigned from the connected network, and select [**2**] when using the IP assigned from the DHCP server which exists in the connected network.

After entering correctly, press [**ENT**] button for next setting.

※ If the net type is set to [**1. Static**], you should set "3.4.2.2 Terminal IP setting", "3.4.2.3 Subnet Mask Setting", Subnet Mask setting", "3.4.2.4 Gateway setting" in each. However, if the connection method is set to [**2. DHCP**], the setting is unnecessary and omitted.

3.4.2.2. Terminal IP Setting



Network

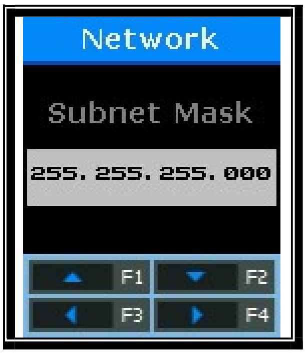
Terminal IP

192. 168. 000. 003

Press [←][→] buttons to move to the digit to change, and press [↑][↓] buttons to change the numbers.
Default Setting: "192.168.000.003"

Set the IP to be assigned in the terminal.
After entering correctly, press [**F4**] button for next setting.

3.4.2.3. Subnet Mask Setting



Network

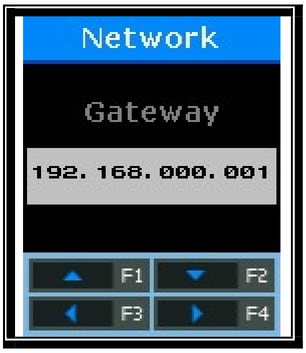
Subnet Mask

255. 255. 255. 000

Press [←][→] buttons to move to the digit to change, and press [↑][↓] buttons to change the numbers.
Default Setting: "255.255.255.000

Set the subnet mask of the network connected to terminal.
After entering correctly, press [**F4**] button long to move to the next setting.

3.4.2.4. Gateway Setting



Network

Gateway

192. 168. 000. 001

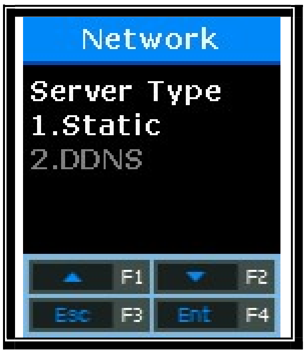
Press [←][→] buttons to move to the digit you want to change, and press [↑][↓] buttons to change the numbers.
Default Setting: "192.168.000.001"

Enter the gateway IP address of the network connected with terminal.
After entering correctly, press [**F4**] button long to move to the upper menu.

3.4.3. Server Setting

Select [**F3~**] → [**2. Network**] → [**3. Server Net**] on the main screen, and the following screen is displayed.

3.4.3.1. Server type setting


Network

Server Type
1.Static
2.DDNS

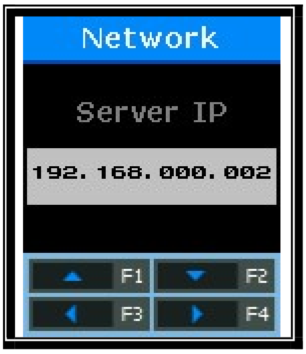
Select [**1**] if Static IP is assigned, and select [**2**] to set IP using DDNS.
Default Setting: [**1. Static**]

This is the way that the terminal is connected to the network.
Select [**1. Static**] when using the Static IP assigned from the connected network, and select [**2. DDNS**] when using the IP assigned from the DDNS server.

After entering correctly, press [**ENT**] button to move to the next setting.

※ If the connection method is set to[**1. Static IP**], the following procedures such as "3.4.3.2. Sever IP Setting" and "3.4.3.3. Server Port Setting" should be set respectively. However, if the connection method is set to '2. DDNS', DDNS ID needs to be additionally set and so "4.4.3.4. DDNS ID Setting" is added.

3.4.3.2. Server IP setting


Network

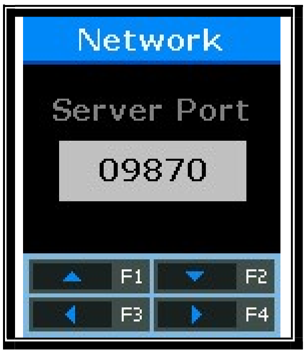
Server IP

192. 168. 000. 002

Press [←][→] buttons to move to the digit to change, and press [↑][↓] buttons to change the numbers.
Default Setting: "192.168.000.002"

Set the IP address of the network server for the terminal to access.
After entering correctly, press [**F4**] button long to move to next setting.

3.4.3.3. Server Port Setting

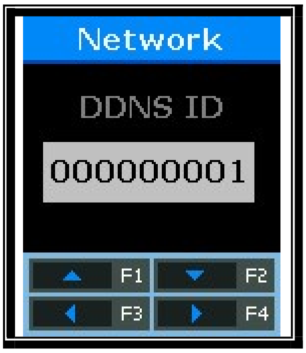


09870

Press [←][→] button to move to the digit to change, and press [↑][↓] button to change numbers.
Default Setting: "09870"

Set the port of the network server for the terminal to access.
After entering correctly, press [**F4**] button to move to upper menu.

3.4.3.4. DDNS ID Setting



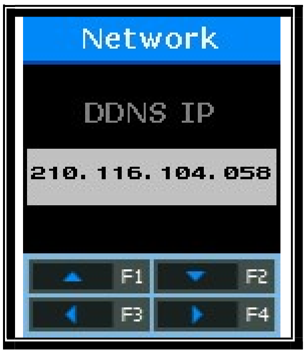
000000001

Press [←][→] buttons to move to the digit you want to change, and press [↑][↓] buttons to change the numbers.
Default Setting: "000000001"

This is the setting only when the server connection method is set to [**2. DDNS**].
Set DDNS ID of the DDNS server connected to the terminal.

After entering correctly, press [**F4**] button to move to the next setting.

3.4.3.5. DDNS IP Setting



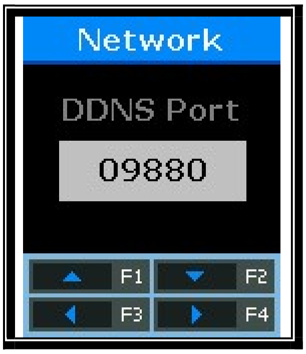
DDNS IP

210. 116. 104. 058

Press [←][→] buttons to move to the digit you want to change, and press [↑][↓] buttons to change the numbers.
Default Setting: "210.116.104.058"

Set the IP Address of the network server to be connected with the terminal.
After entering correctly, press [**F4**] button long to move to the next setting.

3.4.3.6. DDNS Port Setting



DDNS Port

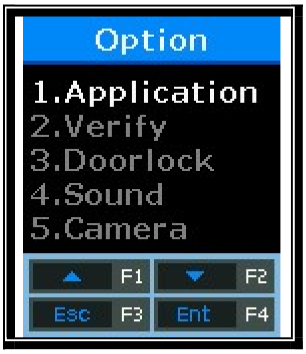
09880

Press [←][→] buttons to move to the digit you want to change, and press [↑][↓] buttons to change the numbers.
Default Setting: "09880"

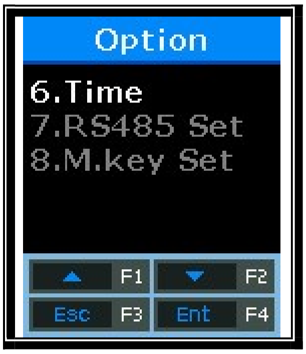
Set the server port to be connected with the terminal.
After entering correctly, press [**F4**] button long to move to the upper menu

3.5. Option Setting

Select [**3. Option**] in the main menu, and the screen is displayed below.

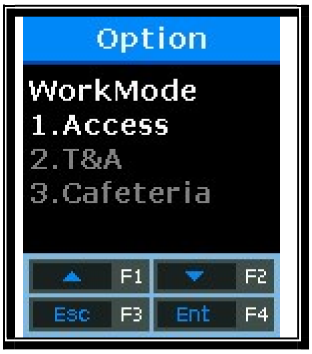


Press [↑][↓] buttons to select the menu to change, and press [**ENT**] button.



3.5.1. WorkMode Setting

Select [**F3~**] → [**3. Option**] → [**1. WorkMode**] in the main screen, and the following screen is displayed.



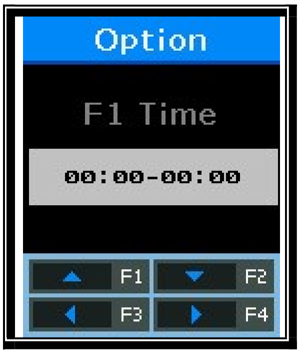
Set the workmode that you want to set.
Default setting: [**1. Access**]

This is to set the work mode of the terminal. Select [**1. Access**] for simple access control; [**2. T&A**] for T&A control; and [**3. Cafeteria**] for Food Service management.

After selecting, press [**ENT**] button to move to the detail setting menu depending on each work mode.

3.5.1.1 When setting [**1. Access**] or [**2. T&A**]

By setting the default time for each T&A mode, after authentication, the terminal display mode can be changed into the set T&A mode.



If time setting is unnecessary, set the time as '00:00-00:00'.

This is to set the default attendance time. Press [←][→] buttons to move to the digit to change, and press [↑][↓] buttons to change the numbers.

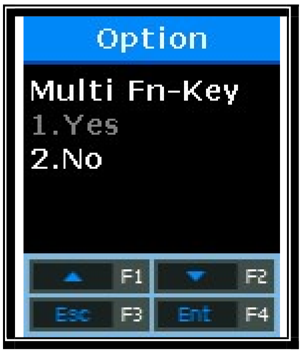
Within the set time zone, the Attend mode is always displayed if another function key is not pressed. Even if the Leave mode is authenticated by pressing [F2] button, the terminal display mode is automatically turned into the Leave after authentication. Therefore, it is convenient to manage T&A.

After <F1 Time>, set <F2 Time>, <F3 Time>, <F4 Time>, and <Access Time> in the same way. As shown below, each time zone must be set not to overlap each other.

(Ex) F1 Time=06:00~09:59, F2 Time=17:00~22:00

<F1 Time> 06:00~09:59	<F2 Time> 17:00~22:00

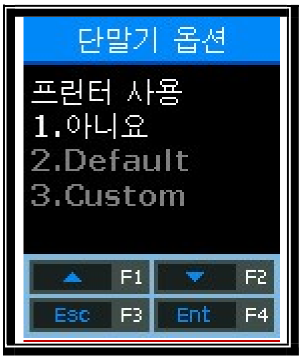
And press [ENT] button, and the screen below is displayed.



Default Setting: [**2. No**]

At least five authentication mode may be set if necessary. Whether to use function keys of F5~F6 is determined by using F1~F3 keys. When setting [1. Yes], press F1(F2, F3) mode once more, it will change into F5(F6, F7) mode.

Press [**ENT**] button and the screen is displayed as below.



단말기 옵션

프린터 사용

1.아니요

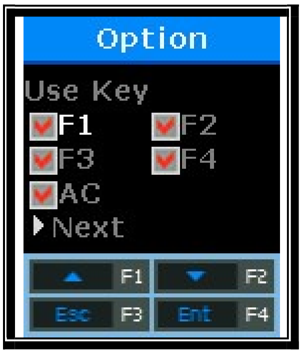
2.Default

3.Custom

Default Setting: [**1. No**]

This is the menu about whether to print the authentication result by printer or not. When setting [**1. No**] or [**2. Default**], if the authentication succeeds, terminal ID, user ID, date, and authentication mode are printed in the printer connected with RS232 port. The used printer is "SRP-350" Serial Type model.

For next setting, press [**ENT**] button and this screen is displayed.



Option

Use Key

☑F1 ☑F2

☑F3 ☑F4

☑AC

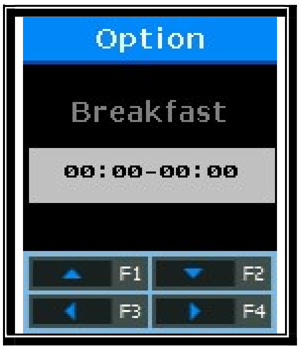
▶Next

Default Setting: All [**V**]

Set whether to use each function key. When setting to [**V**], it means that the authentication mode may be changed when pressing the function key. When setting Blank, the authentication mode is not changed in spite of pressing the key. When this mode is used only for [**Attend**] or [**Leave**], it is available by unchecking other function keys.

After selecting the set value, press [**ENT**] button, and all authentication settings are finished and the screen moves to the upper menu.

3.5.1.2. When setting [**3. Cafeteria**]



Option

Breakfast

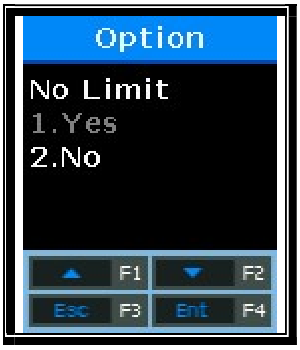
00:00-00:00

If time setting is unnecessary,
it is set to '00:00-00:00'.

This is to set the breakfast time. Breakfast is unconditionally authenticated within the set time zone.
After setting the breakfast time, set <**Lunch**>, <**Dinner**>, <**Supper**>, and <**Snack**> in order in the same way. The unused meal time is set to '00:00-00:00'.

Each time zone must be set not to overlap each other. When the time is not set to the food time zone, the terminal displays "Locked!" message. As the terminal is locked, all inputs are blocked except for access to the menu mode.

When <**Snack**> is set, the menu to check whether to duplicate authentication is displayed.



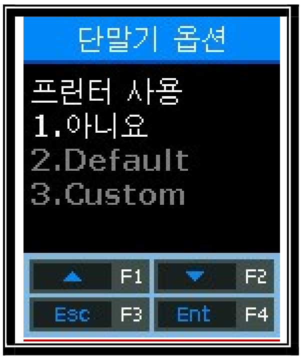
Option

No Limit
1.Yes
2.No

Default Setting: '2. No'

If the mode is set to 'No', authentication is once allowed within the same meal time zone. When attempting authentication again, the "Duplicated!" message is displayed and the authentication fails.

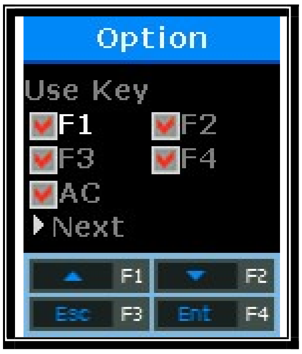
For next setting, press [**ENT**] button and the printer setting screen is displayed.



Default Setting: '1. No'

This is the menu whether to print the authentication result by printer. When setting '1' or '2', if the authentication succeeds, terminal ID, user ID, date and authentication mode are printed from the printer connected with RS232 port.
The printer to use is "SRP-350" Serial Type model.

For next setting, press [**ENT**] button and the screen is displayed below.



Default: All 'V'

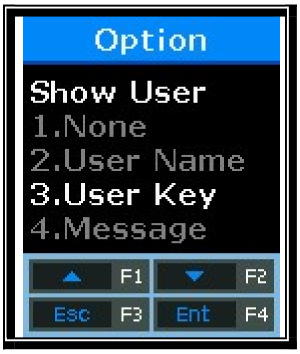
Set whether to use each function key. When setting to 'V', it means that the authentication mode may be changed when pressing the function key. When setting to Blank, the authentication mode is not changed in spite of pressing the key. When this mode is used only for [**Attend**] or [**Leave**], it is available by unchecking other function keys.

After selecting the set value, press [**ENT**] button, and all authentication settings are finished and the screen moves to the upper menu.

3.5.2. Authentication method setting

Select [**F3~**] → [**3. Option**] → [**2. Verify**] on the main screen, and the following screen will appear.

3.5.2.1. Set whether to display IP when successful authentication

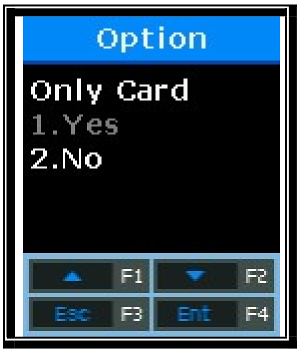


Default Setting: '2. User Name'

- '1': Displays the authenticated user ID.
- '2': Displays the user name in LCD screen. If there is no user name, the user ID is displayed. But it shows Max 16 letters for English, Max 8 letters for Korean.
- '3': Displays the employee number entered when registering the user. But it shows Max 20 letters for English, Max 10 letters for Korean.
- '4': Displays the message entered when registering the user. But it shows Max 16 letters for English, Max 8 letters for Korean.

(Caution)
* User name and message are set in server. For output, the user information must be downloaded.
* User name and message must be set to the same language as the terminal language.
(Example) OK! <0001>
For next setting, press [**ENT**] button.

3.5.2.2. Set whether to permit authentication using card only

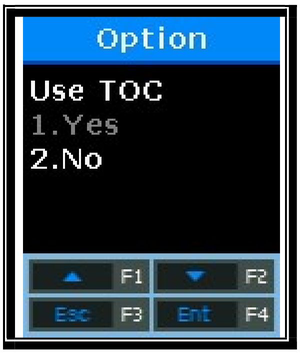


Default Setting: '2.No'

This option makes it possible to authenticate by using card only without fingerprint. Even if the user is registered in FP and Card, he/she can be authenticated by using card only in the terminal that this option is set to '1'.

After selecting the set value, press [**ENT**] button, and the screen will go to the upper menu.

3.5.2.3. To authenticate only using the information saved in the Smart Card


Option

Use TOC

1.Yes

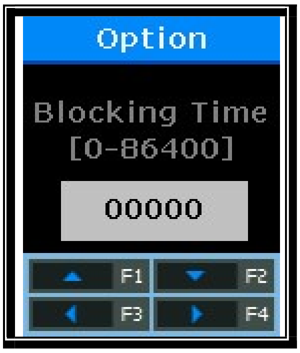
2.No

Default Setting: '2.No'

This option makes it possible to authenticate by using only the user information and fingerprint without user download. In order for this option to work, you must have a SC card reader installed and set it as a fingerprint card terminal.

After selecting the set value, press [**ENT**] button, and the screen will go to the upper menu.

3.5.2.4. Blocking Time Setting


Option

Blocking Time
[0-86400]

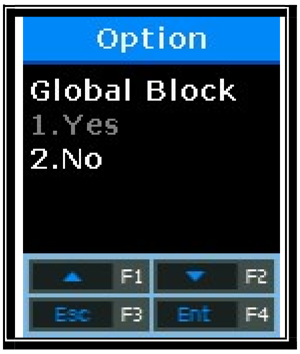
00000

Default Setting: 00000 (Unit: Second)

This option is to prohibit the user from re-authenticating within the set time. There is no limit when the mode is set to '0'. However, if it is set to the greater value than '0', re-authentication cannot be permitted until the time lapses more than the set time after successful authentication.

After selecting the set value, press [**ENT**] button, and the screen will go to the upper menu.

3.5.2.5. Global Block Setting

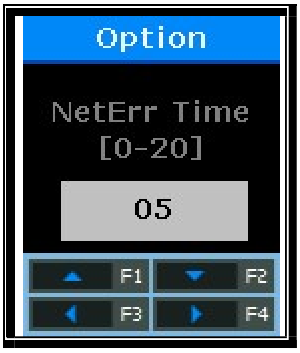


Default Setting: '2.No'

This option is to prohibit the user from authenticating within the short time. After successful authentication, the terminal function is blocked during the previous blocking time setting.

After selecting the set value, press [**ENT**] button, and the screen will go to the upper menu.

3.5.2.6. NetErr TimeOut – Network Error Time Setting (Second)



Default Setting: '05'

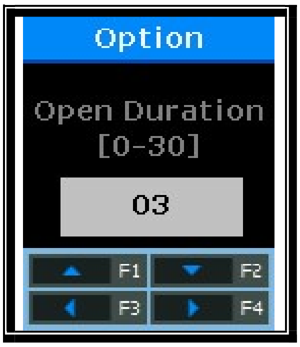
In the server authentication mode, if the network error time is set, the time to wait for authentication can be set.
For example, if the error time is set to 5 seconds, when the user does not receive any response from the server for 5 seconds after authentication request, an error message comes out. (However, the user is processed as authentication failure.)

After selecting the set value, press [**ENT**] button, and all authentication settings will be finished and the screen will move to the upper menu.

3.5.3. Door Setting

Select [**F3~**] → [**3. Option**] → [**3. Doorlock**] on the main screen, and the following screen is displayed.

3.5.3.2. Door Open Time Setting



Option

Open Duration
[0-30]

03

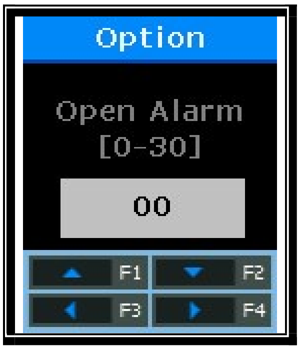
Default setting: '03'(Unit: Second)

This option is to specify the time when after authentication through the terminal, the door is opened and then closed. Strike type means the time when if opening the door after authentication, the door is automatically locked again. In the case of Dead Bolt type and Auto Door, the door will work regardless of the value.

If the mode is set to '00', it is impossible to control the door. '00' must be set only when the door is not connected to Lock.

After selecting the set value, press [**F4**] button to move to the next setting.

3.5.3.3 Door Open Alarm Setting



Option

Open Alarm
[0-30]

00

Default Setting: '00'

This option allows the terminal to check the time when the door is open. If the door is open over the set time (minimum 5 seconds to maximum 30 seconds), an alarm occurs. When the time is set to '00', no alarm occurs. Even if the time is set to 01~04, an alarm starts to sound after the lapse of at least 5 seconds.

The door must be closed within the set time. But, it may not be closed due to unforeseen circumstances. The alarm allows users to check the cause that the door is unclosed and take any action so that the door can be closed normally.

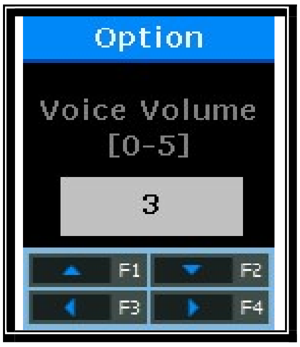
To use this function, the lock must have the function to monitor whether the door is open or close. The monitoring pin of the lock must be also connected to the terminal. To check whether the door is open or close, the mode must be set to '2' or '3'.

After selecting the set value, press [**F4**] button long, and the screen will finish all the setting of the door and move to the upper menu.

3.5.4. Volume Setting

Select [**F3**~] → [**3. Option**] → [**4. Volume**] on the main screen, and the following screen is displayed.

3.5.4.1. Voice Volume Setting



Option

Voice Volume
[0-5]

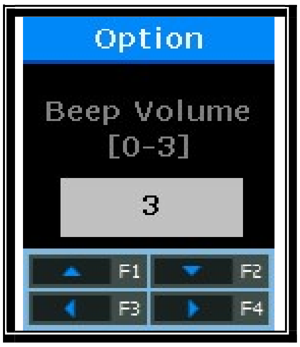
3

Default Setting: '3'

This option is to set the volume during voice guidance. If the volume is set to '0', the voice message does not come out.

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

3.5.4.2. Buzzer Volume Setting



Option

Beep Volume
[0-3]

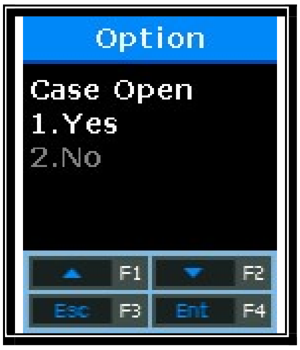
3

Default Setting: '3'

This option is to set the terminal buzzer volume. The buzzer occurs silent for '0', small volume for '1', and large volume for '3'.

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

3.5.4.3. Case Open Alarm Setting



Option

Case Open
1.Yes
2.No

Default Setting: [**1. Yes**]

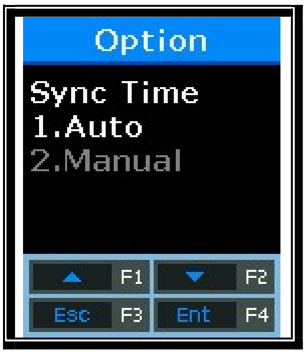
This option is to set whether an alarm occurs when the terminal case is open. The alarm occurs for '1' and it does not occur not for '2'.

After selecting the set value, press [**ENT**] button, and the screen will go to the upper menu.

3.5.5. Current Time Setting

Select [**F3**~] → [**3. Option**] → [**6. Time Display**] and the screen below is displayed.

3.5.5.1. Time Synchronization Setting

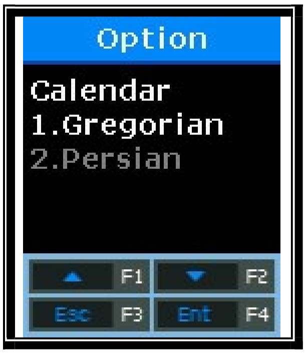


Default Setting: [**1. Auto**]

This option is to set how to synchronize the current time of the terminal with the server time. Set to [**1. Auto**] to automatically synchronize with server time, and set to [**2. Manual**] to manually synchronize with server time.

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

3.5.5.2. Calendar Setting

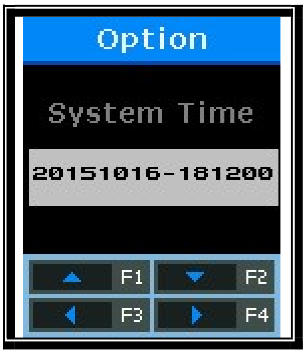


Default Setting: [**1. Gregorian**]

This option is to set how to display the current date in the terminal. The date is generally set to [**1. Gregorian**], but [**2. Persian**] when using the Persian calendar specially.

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

3.5.5.3. Time Setting


Option

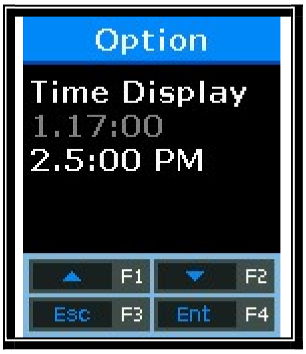
System Time

20151016-181200

The current time of the terminal is displayed in the order of "2009:Year, 08:Month, 01:Day, 21:Hour, 18:Min, 06:Sec". To modify, move to the desired position using [←][→] buttons, and modify the existing values using [↑][↓] buttons.

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

3.5.5.4. Time Display Setting


Option

Time Display

1.17:00

2.5:00 PM

Default Setting: '2.05:00 PM'

This option is how to display the current time of the terminal. When setting to '1', the time is displayed to the 24-hour time. When setting to '2', the time is displayed by separating with AM/PM.

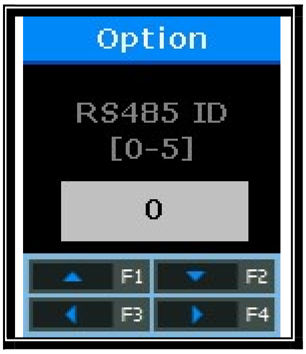
After selecting the set value, press [**ENT**] button, and the screen will go to the upper menu.

3.5.6. RS485 Setting

Select [**F3**~] → [**3. Option**] → [**7. RS485 Set**] → [**ENT**] on the main screen, and the following screen is displayed.

3.5.6.1. RS485 Setting

This option is to set RS485 ID in order to work together with RS485 device.



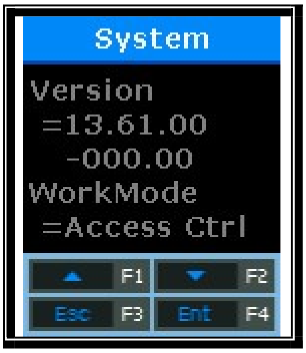
RS485 ID
[0-5]
0

Press [↑][↓] buttons to select the ID value, and press [**ENT**] button.
Default Setting: '0'

After selecting the set value, press [**ENT**] button, and the screen will go to the upper menu.

3.6. Terminal Information Inquiry

Select [**3. Information**] on the main menu, and the following screen is displayed.



Version
=13.61.00
-000.00
WorkMode
=Access Ctrl

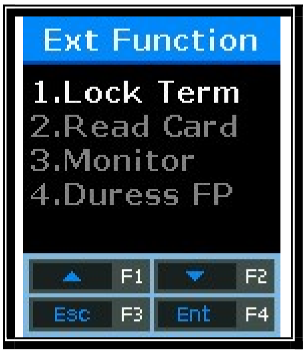
All the environmental settings of the terminal can be checked in order.

Press [↑][↓] buttons and scroll them up and down, and you can in order check the settings in the following table.

Version	Terminal firmware version
WorkMode	Terminal operating modes (T&A + security/T&A/food service)
Language	Language setting
Auth mode	Authentication priority
1:1 Level	Authentication level applied when 1:1 authentication
1:n Level	Authentication level applied when 1:n authentication
Terminal Id	Terminal ID
Net Type	Network connection methods (Static IP/DHCP)
Terminal IP	Terminal IP address
Gateway	Terminal gateway address
Subnet Mask	Terminal subnet mask address
Server Type	Network server connection mode setting
Server IP	IP address of the network server connected to the terminal
Server Port	Port number of the network server program
MAC Addr	Terminal MAC address
Card Ver	Card reader module firmware version
Card Format	Card data display format
All User	The total number of users registered in the terminal, including administrators
All Admin	The number of administrators registered in the terminal
Max User	The maximum number of users who can be registered in the terminal
All FP	The total number of fingerprints saved in the terminal
Max FP	The maximum number of fingerprints that can be registered in the terminal
All Log	The number of the authentication results saved in the terminal
Max Log	The maximum number of the authentication results that can be saved in the terminal
Serial Num	Terminal serial number

3.7. Additional Function (Extra Function)

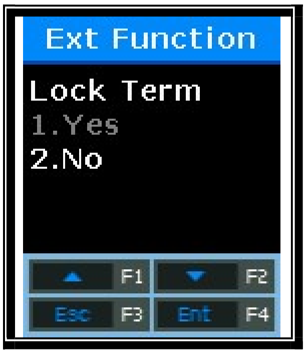
Select [**5. Ext Function**] on the main menu, and the following screen is displayed.



Press [↑][↓] buttons to select the menu you want to change, and press [**ENT**] button.

3.7.1. Terminal Lock Setting

Select [**F3**~] → [**5. Ext Function**] → [**1. Lock Term**] on the main screen, and the following screen is displayed.



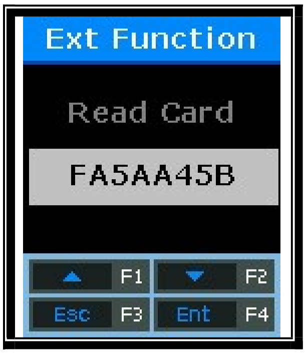
Default Setting: [**2. No**] (Unlock Terminal)

This function allows the administrator to directly lock or unlock the terminal without the server program. If it is set to '1', nobody can access the office until the administrator releases the set.

After selecting the set value, press [**ENT**] button, and the screen will go to the upper menu.

3.7.2. Card number inquiry

Select [**F3**~] → [**5. Ext Function**] → [**2. Read Card**] on the main screen, and the following screen is displayed.


Ext Function

Read Card

FA5AA45B

This is an additional function regardless of the terminal environment setting. In the case of the terminal that the card reader is added, the card number can be checked for card registration via the server. Place the card on this screen, and the card number will be displayed on the LCD.

To exit the card read, press [**ESC**] button to move to the upper menu.

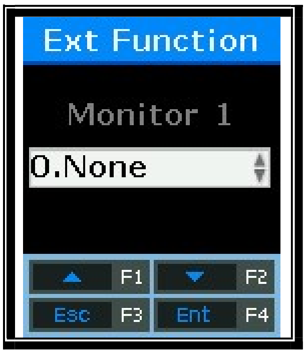
3.7.3. Monitor Input Port Setting

This option acts to connect the sensor to the terminal input port, and send a notice message to the server when the status is changed.

Select [**F3**~] →[**5. Ext Function**] →[**3. Monitor**] on the main screen, and the following screen will appear.

(Caution) DM2 is a currently unused spare port. Before using the relevant function, check the required ports and install.

3.7.3.1. Monitor 1 Input Port Setting


Ext Function

Monitor 1

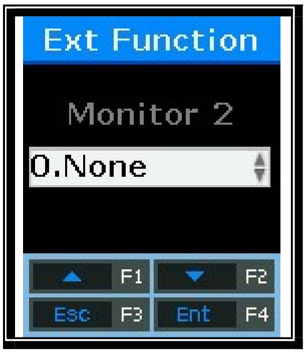
0.None

Set when connecting an external contact to DM0.
(When using a motor lock, set to 1 or 2.)
Default Setting: '0.None'

- '0.None': When nothing is connected
- '1.NO' or '2.NC': When the open door status monitoring pin is connected
- '3.Fire NO' or '4.Fire NC': When the fire detection sensor is connected
- '5.Panic NO' or '6.Panic NC': When the panic situation detection sensor is connected
- '7.EMC NO' or '8.EMC NC': When the emergency detection sensor is connected
- '9.Ctrler Out': When the authentication result is sent to the external controller
  (Connect the RED LED of controller to DM0 or DM1 through the board has the TR. Set the relevant pin to '9. Ctrler Out'. Wiegand Out must be set.)

For next setting, press [**ENT**] button.

3.7.3.2. Monitor 2 Input Port Setting


Ext Function

Monitor 2

0.None

Set when connecting an external contact to DM1.
(When using a motor lock, set to 1 or 2.)
Default Setting: '0.None'

- '0.None': When nothing is connected
- '1.NO' or '2.NC': When the open door status monitoring pin is connected
- '3.Fire NO' or '4.Fire NC': When the fire detection sensor is connected
- '5.Panic NO' or '6.Panic NC': When the panic situation detection sensor is connected
- '7.EMC NO' or '8.EMC NC': When the emergency detection sensor is connected
- '9.Ctrler Out': When the authentication result is sent to the external controller
  (Connect the RED LED of controller to DM0 or DM1 through the board has the TR. Set the relevant pin to '9. Ctrler Out'. WiegandOut must be set.)

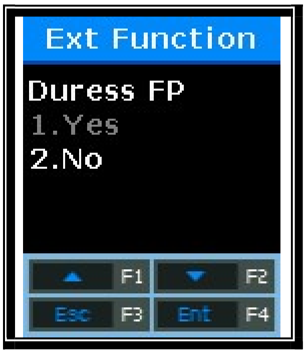
After selecting the set value, press [**ENT**] button, and the screen will go to the upper menu.

3.7.4. Duress FP Setting

Select [**F3**~] →[**5. Ext Function**] →[**4. Duress FP**] on the main screen, and the following screen is displayed.

3.7.4.1 Duress FP Alarm

This function allows the users to use an alarm when the duress fingerprint is entered.



Ext Function

Duress FP

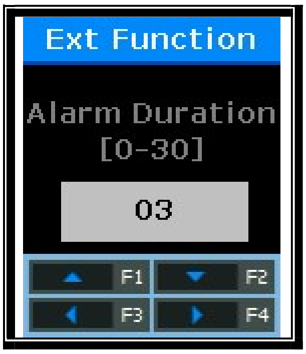
1.Yes

2.No

Set whether to use the duress fingerprint alarm.
Default Setting: '2.No'

The default setting is [**2. No**]'. When it is set to [**1. Yes**], if the pre-registered fingerprint is authenticated, the 'L2' Pin will output the DC12V. If any emergency detection device such as a siren is connected to this Pin, it will operate.

If <**Duress FP**> is set to [**1. Yes**], the menu for setting the time corresponding to 12V will appear.



Ext Function

Alarm Duration
[0-30]

03

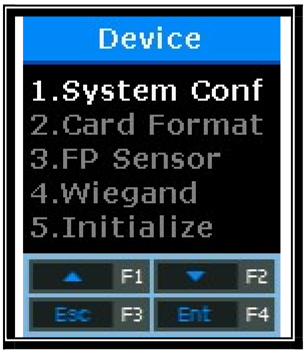
Default Setting: '03' (Unit: Second)

To modify, Press [←][→] buttons to move to the desired position, and press [↑][↓] buttons to change the existing value.

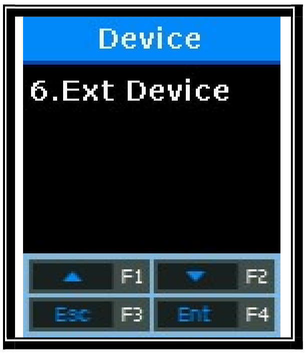
After selecting the set value, press [**ENT**] button, and the screen goes to the upper menu.

3.8. Device Setting

Select [**6. Device**] on the main menu, and the following screen is displayed.



Press [↑][↓] buttons to select the menu to change, and press [**ENT**] button.

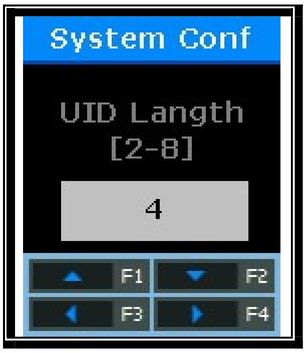


Most of device settings are the option that does not need to change after installation. It is recommended that they are not changed unless there is any clear purpose.

3.8.1. System Configuration

Select [**F3**~] → [**6. Device**] → [**1. System Conf**] on the main screen, and the following screen is displayed.

3.8.1.1. User ID Digits Setting



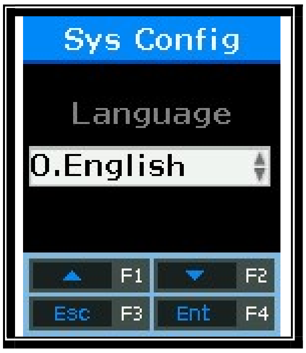
UID Langth
[2-8]
4

Default Setting: '4'

This is the part for setting the length of user ID. The length of user ID can be set from 2 to 8 digits. It should be equal to the length of ID registered in the server program. If the 6-digit ID of '000075' is registered in the server program, the mode is set to '6'.

After setting, press [**ENT**] button to move to the upper menu.

3.8.1.2. Language Setting



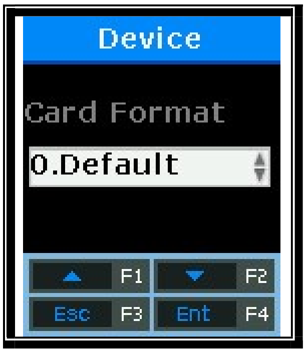
Language
0.English

Default Setting: [**0. English**]

If the language setting is changed, the voice message and the message on the LCD are changed into the set language.

3.8.2. Card Reader Format Setting

Select [**F3~**] → [**6. Device**] → [**2. Card Format**] on the main screen, and the following screen is displayed.



Card Format
0.Default

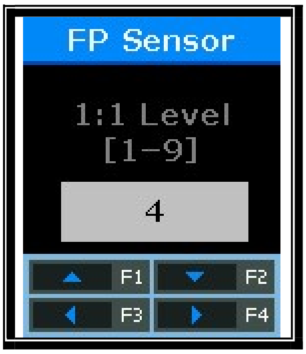
Default Setting: [**0. Default**]

This option is to specify the format that displays the read card number. When setting to Hexa, the format is displayed to the hexadecimal number. When setting to Decimal, the format is displayed to the decimal number. In the device equipped with the RF (low frequency) card reader, if the mode is set to [**4. Format 5**] and it reads EM Card, the card number is displayed to the hexadecimal number of 10byte.

3.8.3. Fingerprint sensor Setting

Select [**F3**~] → [**6. Device**] → [**3. FP Sensor**] on the main screen, and the following screen is displayed.

3.8.3.1. 1:1 Level Setting



FP Sensor

1:1 Level
[1-9]

4

Default Setting: '4'

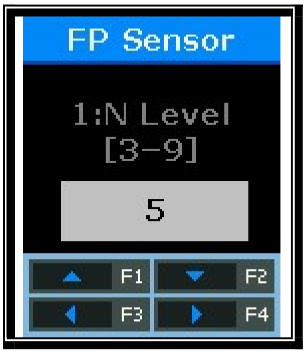
This option is to set the match degree with the same fingerprint when comparing the fingerprint on the fingerprint input window with the user fingerprint saved in the database. The higher authentication level may ensure the higher security. But it requires the relatively high concordance rate. When authenticating User ID, it high likely to deny authentication.

In case of 1:1 Authentication Level, if the ID entered to the authentication level that underwent the authentication process with the ID input is '1234', this option finds the fingerprint registered to the ID of '1234' from the terminal database and compares it with the fingerprint on the fingerprint input window.

However, in case of 1:1 authentication, if the 1:1 authentication level of users is not set to '0' (using the terminal authentication level), the 1:1 authentication level of users is applied.

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

3.8.3.2. 1:N Level Setting



FP Sensor

1:N Level
[3-9]

5

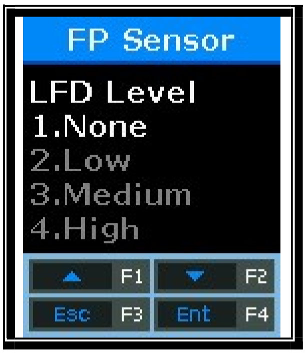
Default Setting: '5'

This option is to set the authentication level using the fingerprint only without ID input. This option is used to find the fingerprint matched by comparing the fingerprint on the fingerprint input window with the user fingerprint saved in the database.

In case of 1:N authentication, the user-specific authentication level is not set. Therefore, authentication is always based on the terminal authentication level.

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

3.8.3.3. LFD Setting

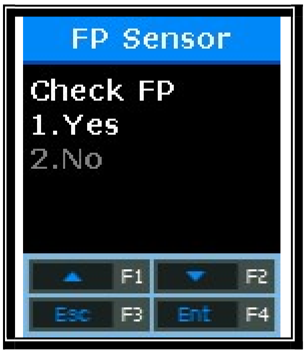


Default Setting: [**1. None**]

This option is to set the LFD level that can prevent fake fingerprints from entering. The higher LFD level may ensure the higher function that prevents the input of fake fingerprints made of rubber, paper, film, and silicon. However, too dry fingerprints may not be entered even when entering actual fingerprints.

After selecting the set value, press [**ENT**] button, and the screen will go to the upper menu.

3.8.3.4. Similar Fingerprint Registration Limit Setting

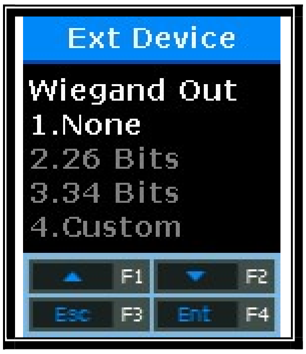


Default Setting: [**1. Yes**]

If the mode is set to [**1. Yes**], this option acts to check whether a new fingerprint is the same as the pre-registered fingerprint, and to prevent the same fingerprint from being registered as the ID of another user.

3.8.4. Wiegand Output Setting

Select [**F3**~] → [**6. Device**] → [**4. Wiegand**] on the main screen, and the following screen is displayed.

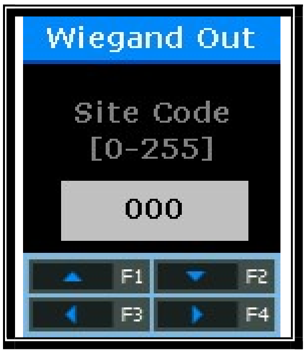


Default Setting: [**1. None**]

This option is used only when the terminal is equipped with a separate controller operated by Wiegand input. After authentication, the following types of data are sent to the Wiegand port of the terminal.

1.None	General case. The Wiegand Out port is not used.
2.26bit	"Site code [1 byte] + User ID [2 bytes]" are transferred. User ID should be set to the 4-digit or less number. Example) SiteCode:045, UID:6543 → 1 00101101 0001 1001 10001111 0
3.34bit	"Site code [1 byte] + User ID [3 bytes]" are transferred. User ID should be set to the 7-digit or less number. However, if User ID is 8 digits, Site code is ignored and only "User ID [4 bytes]" is transferred. Example) SiteCode:001, UID:123456 → 0 00000001 00000001 11100010 01000000 0
4.Custom	This is the user-defined setting that is available only in the server. Only checking is possible in the terminal.

※ This option is unrelated to use the Wiegand type card reader. If the mode is set to '2' or '3', the following site code is set.

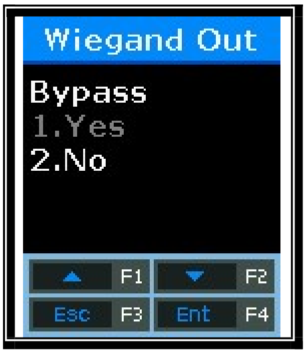


Default Setting: '000'

This option is available only when Wiegand Out is set to '2' or '3'. The site code to send to Wiegand port including User ID is set to the value of 0~255.

After selecting the set value, press [**F4**] button, and the screen will go to the upper menu.

3.8.4.1. Bypass Setting

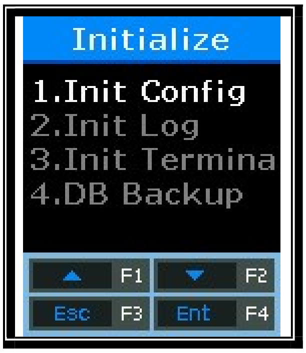


Default Setting: [**2. No**]

This option is available when the Wiegand card reader is used.
When the mode is set to [**1. Yes**], the card information entering to 'Wiegand in' is bypassed to 'Wiegand Out'.

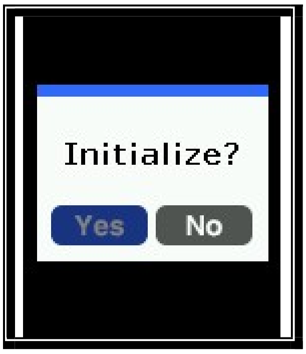
3.8.5. Terminal Initialization

Select [**F3~**] → [**6. Device**] → [**5. Initialize**] on the main screen, and the following screen is displayed.



Select [1] to initialize the set value; [2] to initialize the authentication records; [3] to initialize the factory; and [4] to use the UDL10 to back up the DB.

3.8.5.1. Setting Value Initialization

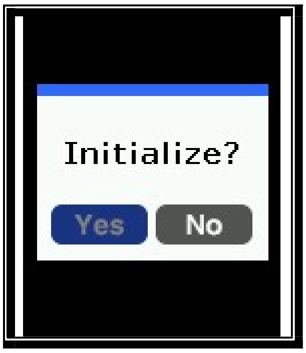


Select [**1**] to initialize, and [**2**] to cancel.

This option initializes all settings of the terminal except for the MAC (physical) addresses and serial numbers saved in the terminal. But, users and authentication records are not deleted.

When initialization is successfully completed, the "Ppiririck" beep occurs and the screen moves to the upper menu.

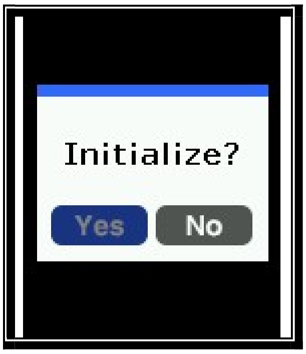
3.8.5.2. Authentication Log Initialization



Select [1] to initialize, and [2] to cancel.

This option deletes all authentication related logs except for set values and users.
When initialization is successfully completed, the "Ppiririck" beep occurs and the screen moves to the upper menu.

3.8.5.3. Factory Initialization

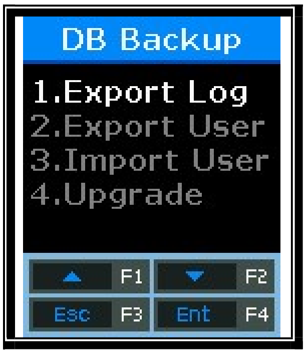


Select [1] to initialize, and [2] to cancel.

This option deletes all authentication related logs except for set values and users.
When initialization is successfully completed, the "Ppiririck" beep sounds and the screen moves to the upper menu.

3.8.5.4. UDL(USB Data Loger) backup

- If the UDL10 has the USB memory card is inserted, the mode moves to the sub-menu. If USB is not inserted, the warning message of 'Not Detected Memory' is displayed.



DB Backup

1.Export Log
2.Export User
3.Import User
4.Upgrade

DB Backup Menu.

✓ Export Log

- Used when the log data saved in the AC2200 terminal is exported to USB.
- Data is saved with a file name of LOG.DAT in the place of [**USB top-level**] folder → [**AC2200**] folder → [**00000000** (8-digit terminal ID)] folder → [**LOG**] folder".
- Only log data can be saved, except for photos.

✓ Export User

- Used when the user data saved in the AC2200 terminal is exported to USB.
- Data is saved with a file name of USER.DAT in the unisuser folder.
- The number of exported users can be checked on the LCD.

✓ Import User

- Used when the user data (USER.DAT) saved in USB is imported into the terminal.
- The firmware file is 'ac2200.bin'. To upgrade, it must be saved with a file name of ac2200.bin in the [**AC2200**] folder.
- The size of imported data can be checked on the LCD.

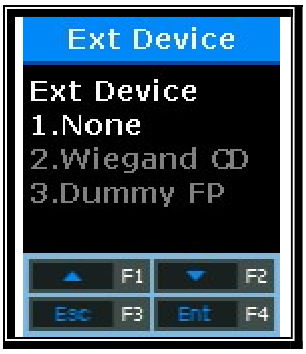
✓ Upgrade

- Used when upgrading the terminal firmware by using the firmware data (ac2200.bin) saved in the USB.
- The firmware file is 'ac2200.bin'. To upgrade, it must be saved with a file name of ac2200.bin in the AC2200 folder.
- The size of imported data can be checked on the LCD.

Caution!!
When removing the USB or powering off the terminal during upgrading, the product may not work properly. Special caution is required.

3.8.6. External Device Setting

Select [**F3**~] → [**6. Device**] → [**6. Ext Device**] on the main screen, and the following screen is displayed

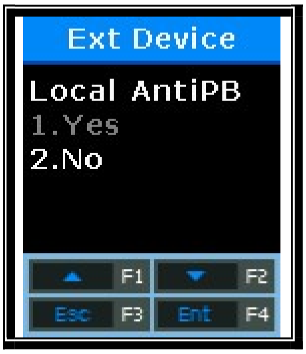

Ext Device

Ext Device
1.None
2.Wiegand CD
3.Dummy FP

Default Setting: [**1. None**]

This option is available when connecting the Slave Reader using the card or fingerprint to the terminal in order to use as a secondary authentication device. The mode is set to '2' when connecting the Wiegand card reader, and '3' when connecting the SR100.

For the next setting, press [**ENT**] button.

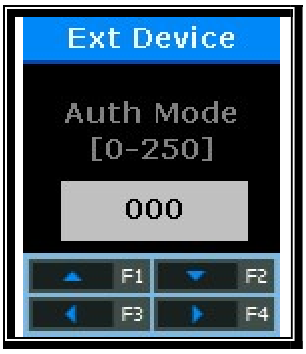

Ext Device

Local AntiPB
1.Yes
2.No

Default Setting: [**2. No**]
When setting to [**1. Yes**], it checks Anti-Pass back in the terminal.

This screen is displayed only when <Ext Device> is set to '2' or '3'.
This option is used to allow only authorized users to access and leave the office. To this end, the terminal and Slave Reader are installed to both the inside and outside of the door. Only users who access the office by authentication via the terminal can leave the office by authentication via the Slave Reader. When setting [**1. Yes**], the server authentication is unavailable. The device checks whether Pass back is valid in the authentication order between the terminal and the Slave Reader.

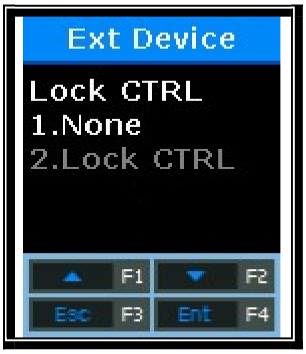
Press [**ENT**] button to move to the next setting.



Default Setting: '0'

This option is to set the authentication (T&A) mode saved from the Slave Reader. If the device is set to '0', it is saved as the current authentication mode; saved to F1 when '1', F2 when '2', Access when '3', F3 when '4', and F4 when '5'.

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



Default Setting: [**1. None**]

This screen is displayed only when <Ext Device> is not set to '3'.
When connecting an external device of LC010 to the terminal, the mode is set to [**2. Lock Ctrl**]. When the terminal interlocks with MCP040, RS485 ID must be set.

4. How to Use Terminal

4.1. When operating to [**1. Access**]

- Set [**Menu**] → [**3. Option**] → [**1. Application**] → [**1. Access**]

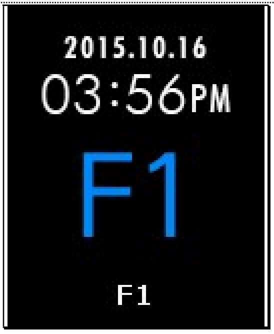
4.1.1. Authentication Mode

- Press function keys, change to the desired authentication mode such as F1, F2, F3, F4, and then perform authentication. When perform authentication without pressing function keys specially, the mode is automatically authenticated to the access mode.

- Authentication Method
  - F1 Authentication: Press [**F1**] key to change to the F1 mode, and then perform authentication. Authentication is performed without changing the mode within the time zone set to the Attend time.
  - F2 Authentication: Press [**F2**] key to change to the F2 mode, and then perform authentication. Authentication is performed without changing the mode within the time zone set to the Leave time.
  - F3 Authentication: Press [**F3**] key to change to the F3 mode, and then perform authentication.
  - F4 Authentication: Press [**F4**] key to change to the F4 mode, and then perform authentication.
  - Access Authentication:
  - Press twice [**F4**] key or press [**F4**] key long to change to the access mode, and then perform authentication. Or, perform authentication without changing the mode within the time zone set to the access time.

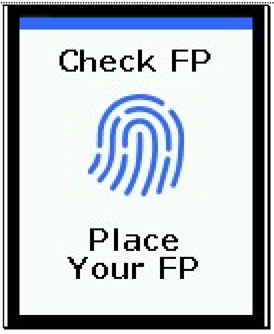
4.1.2. Authentication with fingerprint

▶ After changing the authentication mode by pressing function keys, place your finger on the fingerprint sensor. Then, the authentication result receiving the fingerprint will appear on the LCD with a voice message.



At the alert status, press [**F1**] key to change the authentication mode to ‘F1’.

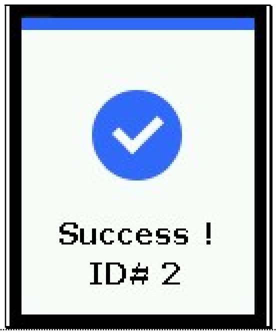
▼



Check FP

Place
Your FP

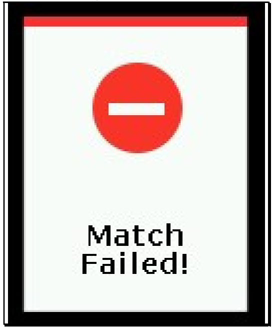
Place your finger on the fingerprint sensor, and the white light is on the fingerprint input window. Keep your finger until the white light is off with a beep sound.



Success !
ID# 2

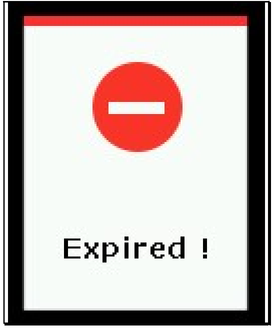
If your fingerprint is successfully authenticated, the voice message of "You are authorized" comes out and a success message is displayed on the LCD.

※ Error Message: The following messages will appear with the voice message of "Place try again".



Match
Failed!

When authentication fails

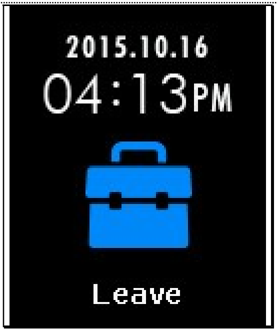


Expired !

When the fingerprint is registered but its authentication is attempted out of the access control time

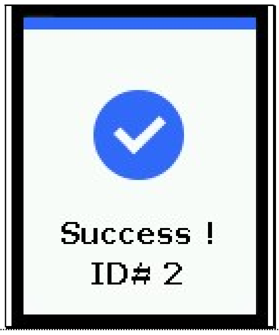
4.1.3. Authentication with card

▶ For users who have registered to [**Card**] or [**FP or Card**], place the card on the main screen, and the beep sound will occur and the authentication result will be displayed on the LCD.


2015.10.16
04:13PM
Leave

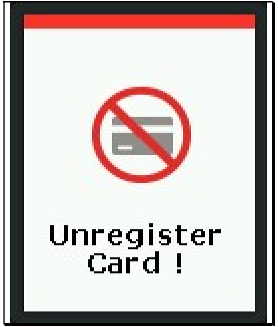
Press [**F2**] key to change the authentication mode to Leave.

▼

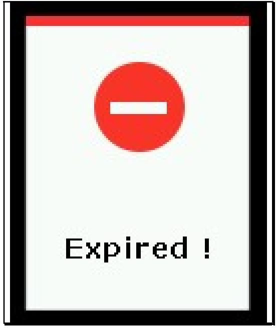

Success !
ID# 2

If your fingerprint is successfully authenticated, the voice message of "You are authorized" comes out and a success message is displayed on the LCD.

Error Message: The following messages will appear with the voice message of "Please try again".


Unregister
Card !

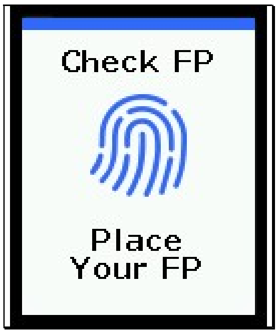
When a unregistered card is entered


Expired !

When the card is registered but its authentication is attempted out of the access control time

▶ For users who are registered with the [FP and Card]

Place the card on the main screen, and the "beep" sounds. The fingerprint cannot be authorized without going through the following fingerprint input process.



When the lamp is on the fingerprint input window with the voice message of "Please enter your fingerprint", enter your fingerprint and keep your finger until the "beep" sound occurs.

4.2. When operating [2. T&A]

- Set [**Menu**] → [**3. Option**] → [**1. Application**] → [**2. T&A**]

- If you set <**Attend**> and <**Leave**> under the condition that the attend time is constant, even if authentication is attempted without pressing [**F1**] or [**F2**] keys, the fingerprint is authenticated to 'Attend' within the time zone set to 'Attend' and to 'Leave' within the time zone set to 'Leave'. Therefore, users can reduce the T&A input error.

4.2.1. Authentication Mode

- Press function keys to change the authentication mode to Attend, Leave, Outdoor, Return, and Access, and then perform authentication with each authentication mode.

- Authentication Method
  - Attend Authentication: Press [**F1**] key to change to the attend mode, and then perform authentication. Authentication is performed without changing the mode within the time zone set to the Attend time.
  - Leave Authentication: Press [**F2**] key to change to the leave mode, and then perform authentication. Authentication is performed without changing the mode within the time zone set to the Leave time.
  - Outdoor Authentication: Press [**F3**] key to change to the outdoor mode, and then perform authentication.
  - Return Authentication: Press [**F4**] key to change to the return mode, and then perform authentication.
  - Access Authentication: Press twice [**F4**] key or press [**F4**] key long to change to the access mode, and then perform authentication. Or, perform authentication without changing the mode within the time zone set to the access time.

4.2.2. Fingerprint Authentication

- Press the function key to change the T&A mode.
- Enter your fingerprint

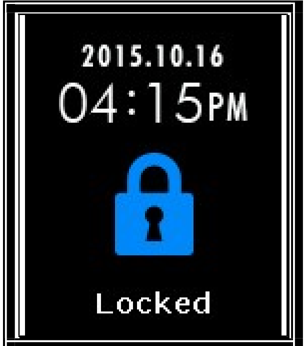
4.2.3. Authentication with Card

- Press the function key to change the T&A mode
- Place the card on the terminal

4.3. When operating to [**2. Cafeteria**]

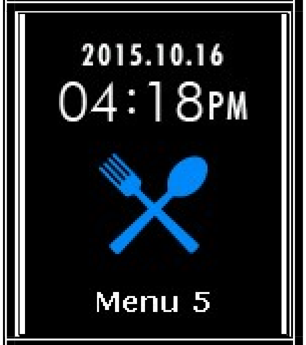
- Set to [**Menu**] → [**3. Option**] → [**1. Application**] → [**3. Cafeteria**]
- When the mode is set to the food service control, the terminal is locked in the time other than meal times. The meal time must be set to more than one meal per person.

- Displayed LCD



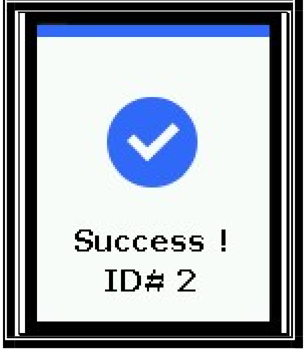
2015.10.16
04:15PM
Locked

When it is not the meal time
(No authentication attempt)



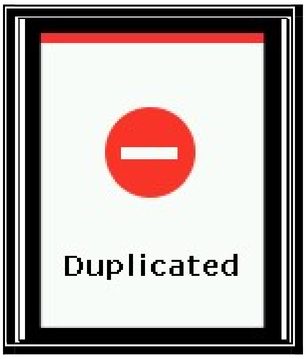
2015.10.16
04:18PM
Menu 5

The default screen during the meal time



Success !
ID# 2

If the authentication is successful



When the mode is set to "Not-allowed Duplicate Authentication Unallowable", if the authentication is again attempted after successful authentication, a duplicate authentication error is displayed.

- When authenticating with the fingerprint
  Enter the fingerprint to receive authentication.

- When authenticating with the card
  Enter the card to receive authentication.

- When attempting authentication without pressing the menu key, it is automatically authenticated to [**Menu 1**].