AC-2100 User Guide

Version Eng-1.12

< Revison History>

Version	Date	Description	Firmware Version
1.00	2009-08-20	Initial Release	10.51.00
1.01	2009-10-29	Change the menu key - Menu : F2~ → F3~	10.51.01~
1.02	2010-03-08	<Multi Fn-Key > added (P.34) <Print Out> added (P.35) <Time Sync> added (P.42)	10.51.03~
1.03	2010-04-05	<F3 Time>, <F4 Time> added (P.34) <Template On Card> added (P.36)	10.51.03-000.03 ~
1.04	2010-04-20	Add 12=Danish in <Language> (P.47)	10.51.04-000.00 ~
1.05	2010-10-05	Add 13=Russian in <Language> (P.47) <Blocking Time> added (P.37)	10.51.06-000.00 ~ 10.51.06-000.01 ~
1.06	2010-11-25	Add 14=French, 15=Farsi <Language> (P.48)<Calendar> added (P.42) Add 3.Message in <Show User ID> (p36)	10.51.06-000.04 ~ 10.51.06-000.05 ~
1.07	2011-04-06	<Key On/Off> menu added (p34) '4.Format 5' added on<Card Format> (p47)	10.51.07-000.00 ~ 10.51.07-000.02 ~
1.08	2011-08-09	4. Wireless Lan menu added on 2. Network (p31) 6.External Device menu added on 6. Device (p51)	**30**.51.08.000.01 ~ (Only apply to higher than H/W version 30)
1.09	2011-09-30	'16=Srpski' (Serbian) added on <Language> (p46) '3.FireNO, 4.FireNC, 5.PanicNO, 6.PanicNC, 7=Emergency NO 8=Emergency NC' added on <Alarm Sensor2> (p45)	10.51.07-000.03 ~ 10.51.07-000.04 ~
1.10	2013-04-01	UDL (USB Data Loger) function added (p52)	3x.51.10-000.00 ~ (Only apply to higher than H/W version 3x)
1.11	2014-06-18	3.7.3.2. Sensor Monitor 2 Input port setting 3.5.2.5. Global Blockin setting 3.5.2.6. NetErr TimeOut 3.5.7. RS485 ID Set(setting) 3.8.6. External Device setting	30.51.10_000.02 30.51.08-000.06 30.51.10.000.11
1.12	2014-07-17	3.3.4. "To change" -> "To register" contents modification	

< Terminology Description >

- Admin, Administrator
  - As a user who can access using terminal menu mode, the administrator has rights to change the operating environment through registration/modification/deletion of terminal users.
  - In case no registered administrator is available, anyone can access the terminal menu to change a particular setting. **Therefore, it is recommended to have at least one administrator.**
  - As the administrator has rights to change important environment setting of fingerprint recognition device, special caution is required during registration and operation.

- 1:1 Authentication (1 to 1, Verification)
  - This is a method that authenticates fingerprint after entering user ID or card
  - This method is called 1:1 authentication because the fingerprint of a user registered in a user ID or card.

- 1:N Authentication (1 to N, Identification)
  - This is a method that searches a corresponding user only with fingerprint.
  - This method is called 1:N authentication because it searches the identical fingerprint from the registered fingerprints without user ID or card input.

- Authentication Level
  - This is a level used during fingerprint authentication. 1~9 levels are available for display according to the level of fingerprint correspondence. The correspondence level of two fingerprints during authentication must be higher than the authentication level in the setting.
  - A higher authentication level provides a higher security level. However, a relatively higher correspondence rate may lead to a higher authentication failure rate.
  - 1:1 authentication level: Authentication level used during 1:1 authentication
  - 1:N authentication level: Authentication level used during 1:N authentication

- Authentication Method
  - This represents the various types of authentication methods formed with combination of FP (fingerprint) authentication and RF (card) authentication.
    Example) Card or FP: Authentication with card or fingerprint

- Function Key
  - [F1], [F2], [F3] and [F4] keys are available. These keys allow a user to enter the menus or change modes such as office start/leave.

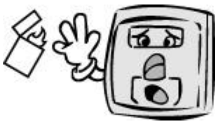
- LFD (Live Finger Detection): Imitation Fingerprint Prevention Function
  - This function allows the input of only real fingerprints and blocks the input of imitation fingerprints produced using rubber, paper, film and silicone.

Table of Contents

1. Check before Device Use

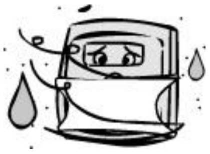
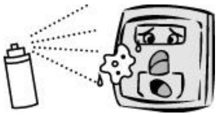
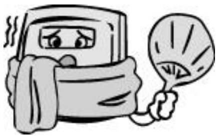
1.1. Cautions for Safety

- Warning

Do not operate the device with wet hand, and do not let liquid such as water to flow into the device. -> It may cause device failure or electric shock.	Do not place the device near fire. -> It may cause fire. 
Do not disassemble, repair or modify the device without permission. -> It may cause device failure, electric shock or fire.	Do not let children play with the device. -> It may cause children safety accident or device failure.

- If displayed instructions are not followed, it may cause death or serious injury of a user.

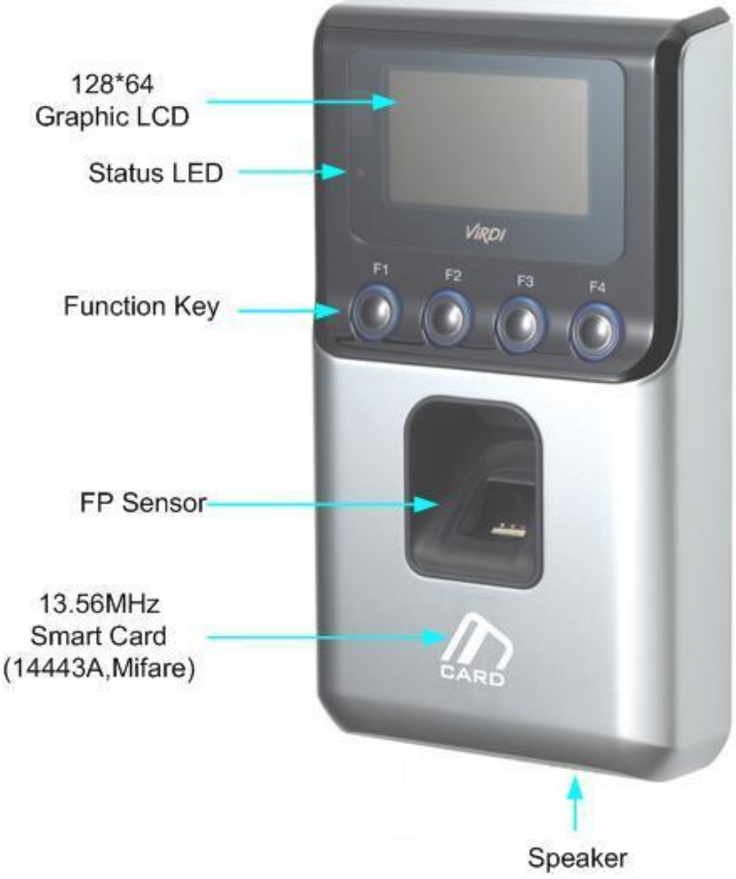
- Caution

Do not expose the device to direct sunlight. -> It may cause malfunction, deformation and discoloration of the device.	Do not install the device in a humid or dusty location. -> It may cause device malfunction. 
Do not spray water for cleaning the device. Do not wipe the device with benzene, thinner or alcohol. -> It may cause electric shock or fire.	Do not place the device near magnets. -> It may cause device failure or malfunction.
Do not contaminate the fingerprint input area. -> Fingerprint may not be properly recognized.	Do not spray pesticide or flammable liquid on the device. -> It may cause deformation and discoloration. 
Do not apply impact on the device. Do not let a sharp object touch the device. -> It may damage the device leading to device failure.	Do not install the device in a place with a large variation of temperature. -> It may cause device failure. 

- If displayed instructions are not followed, it may cause injury of a user or property damage.

※ We are not reliable for the accidents and damages caused by not following the user guide.

1.2. Terminal Component Name



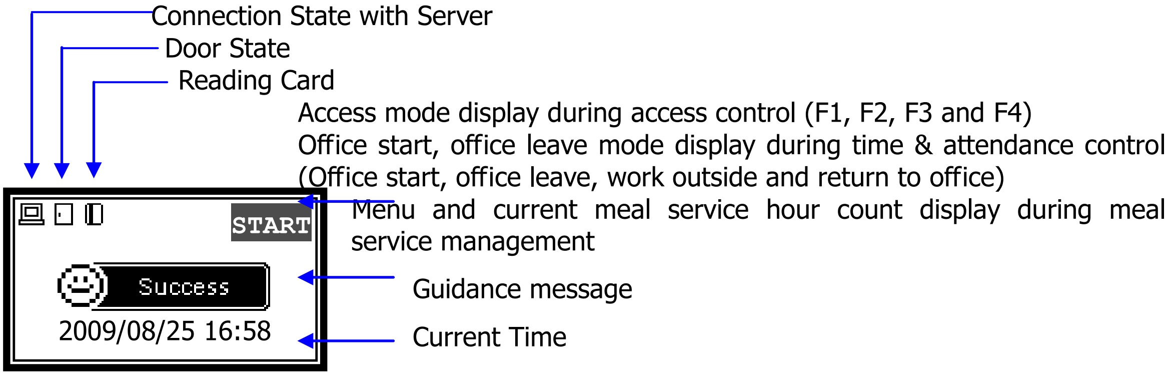
1.3. Information on Button Required during Operation

F1	- Change to office start mode - At menu mode, used as [ESC] or move to left [←] button, used as [ESC] button if pressed down for longer then 2 seconds: [ESC~]
F2	- Change to office leave mode - At menu mode, used as move up or increase **[↑]** button
F3	- Change to work outside mode - Entry to menu mode if pressed down for longer than 2 seconds [F3~] - At menu mode, used as move down or decrease **[↓]** button
F4	- Change to return to office/access mode - At menu mode, used as [ENT] or move to right [→] button used as [ENT] button if pressed down for longer than 2 seconds: [F4~]

1.4. Information on LED Signal Displayed during Operation

●	Power source	Red	Light on: Normal Light on and off: Cover open
●	Door	Green	Light on: Door open Light off: Door closed

1.5. Information on Screen Displayed during Operation



Connection State with Server

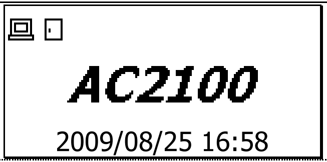
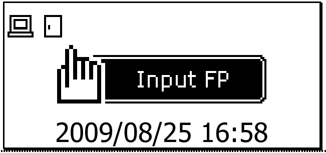
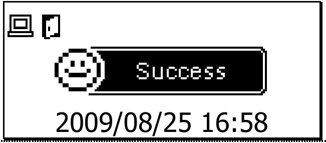
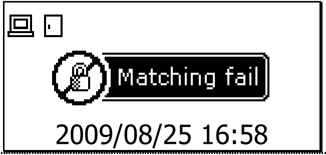
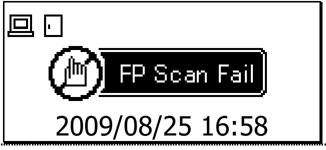
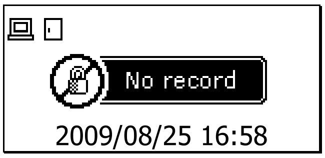
Door State

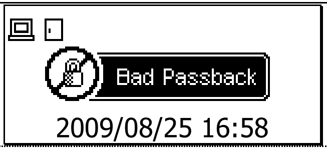
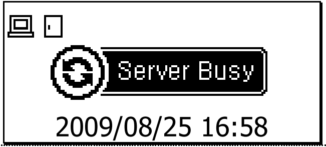
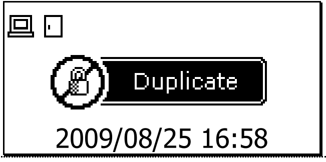
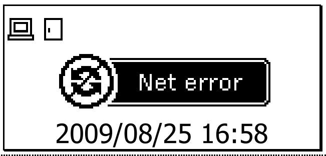
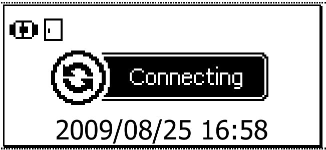
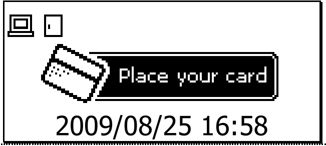
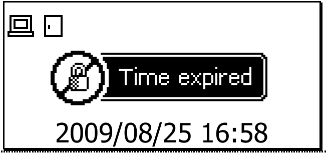
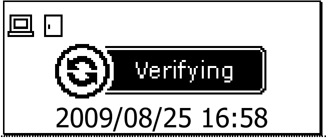
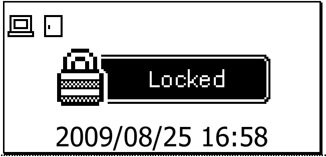
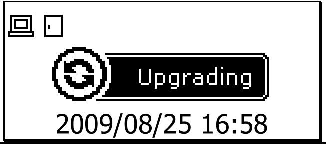
Reading Card

Access mode display during access control (F1, F2, F3 and F4)
Office start, office leave mode display during time & attendance control (Office start, office leave, work outside and return to office)
Menu and current meal service hour count display during meal service management

Guidance message

Current Time

 AC2100 2009/08/25 16:58	- Default screen of AC2100
 Input FP 2009/08/25 16:58	- Under fingerprint input or waiting for fingerprint input
 Success 2009/08/25 16:58	- Authentication success
 Matching fail 2009/08/25 16:58	- Authentication failure
 FP Scan Fail 2009/08/25 16:58	- Fingerprint input failure In case the finger is removed too early before the fingerprint is entered
 No record 2009/08/25 16:58	- Unregistered card input - In case 1:N authentication is attempted when authentication priority is SN and a user with 1:N authentication permission is not available in the terminal

 Bad Passback 2009/08/25 16:58	- Passback failure
 Server Busy 2009/08/25 16:58	- In case processing is difficult during server authentication because too many authentication requests are made from the terminal
 Duplicate 2009/08/25 16:58	- In case the same user attempts authentication more than twice during the same meal service hour when the terminal is set and used as meal service management
 Net error 2009/08/25 16:58	- In case the server is not responding during authentication attempt to the server - In case network is disconnected during authentication attempt to the server
 Connecting 2009/08/25 16:58	- In case connection attempt continues because no registered user is available in the terminal and connection to the server cannot be made
 Place your card 2009/08/25 16:58	- Waiting for card input
 Time expired 2009/08/25 16:58	- In case authentication is attempted with proper registration during the time when access is not permitted
 Verifying 2009/08/25 16:58	- Waiting for response after authentication attempt to the server
 Locked 2009/08/25 16:58	- In case terminal is in lock state - In case it is not meal service hour when setting as meal service management
 Upgrading 2009/08/25 16:58	- When upgrading terminal program (Do not switch off terminal power while this message is displayed.)

1.6. Information on LCD Icon Displayed during Operation

Server connection state	⊣⊢ : LAN cable not connected ⊞ : LAN cable connected but not connected to server program 🖳 : Connected to server program

Door open/closed	□ : Door closed ◪ : Door open
Reading card	◧ : Disappears 1 second after a card is read

1.7. Information on Voice Message Issued during Operation

Operation	Voice guidance
Fingerprint input	Please enter your fingerprint.
Authentication success	You are authorized.
Authentication failure	Please try again.

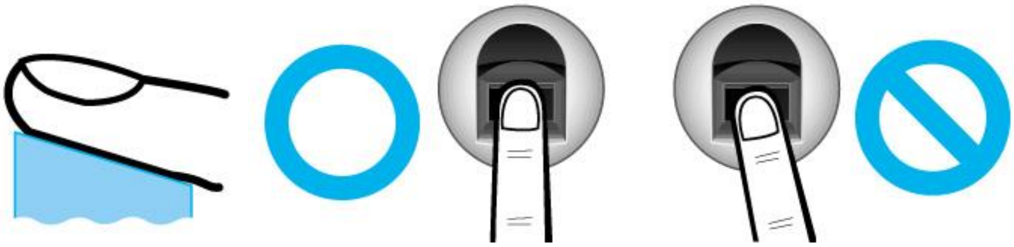
1.8. Information on Buzzer Sound Issued during Operation

ppik	Alarm sound during button or card operation	In case button is pressed or card is read In case finger can be removed after fingerprint input is completed
ppibik	Failure	In case authentication fails or user input is wrong
ppiriririk	Waiting for input	When informing that the system is waiting for fingerprint input
ppiririk	Success	In case authentication succeeds or the setting of a current user is completed

1.9. Proper Fingerprint Registration and Input Method

- Proper fingerprint input method

If possible, use the index finger and enter fingerprint as if you are making a thumbprint. Just touching a finger to the fingerprint input window is not the proper way for registration/input. The proper way is to touch the center of fingerprint on the fingerprint input window.



- If possible, use the fingerprint of the index finger for input.

  With the index finger, a more accurate and stable fingerprint can be entered.

- Check whether the fingerprint is clear or it has wound.
  Too dry or wet fingerprint, blurred fingerprint and fingerprint with wound are difficult to recognize. In such a case, use the fingerprint of a different finger for registration.

- Cautions according to the conditions of user's fingerprint

  A fingerprint may not be usable or may be inconvenient to use depending on the conditions of fingerprint.

  - This product is a fingerprint recognition system. If a fingerprint is damaged or weak, it cannot be used. If that happens, use a password for operation.

  - **If your hand is too dry, breathe into it** for a while to ensure smooth operation.

  - In case of children, fingerprint may be too small or weak to use. It is necessary to register the fingerprint every six months.

  - In case of seniors, registration may be difficult if fingerprint has excessive fine wrinkles.

  - It is recommended to register at least 2 fingerprints.

2. Product Introduction

2.1. Product Features

- **Access control system using network (LAN)**
  - As communication between fingerprint recognition device and authentication server is done using UTP cable and TCP/IP protocol, existing local area network can be used for good scalability. **10/110 Mbps auto detect** provides fast speed and allows easy management and monitoring through a network.

- **Convenient auto sensing function**
  - Authentication operation requires only fingerprint input without additional key input.

- **Simple authentication using fingerprint**
  - The use of fingerprint recognition technology, one of biometrics technologies, prevents loss of password, card, key or theft. As fingerprint is used, the security level of authentication is substantially increased.

- **Convenient guidance message using LCD and voice**
  - Using voice and LCD display window, every authentication operation is processed with guidance message. Especially, the built-in backlight of LCD display window allows for easy screen identification and key operation even in dark areas. As voice is saved in the memory, making change to a desired voice is possible at the server.

- **Provides various and flexible access control methods**
  - Convenient to use while preventing lending, forgery and loss of key or card
  - Provides perfect access control function by granting access rights for each user group
  - Provides flexibility in access control by granting limited access hour
  - Provides low maintenance and development cost compared to other access control devices
  - Removes inconvenience of obtaining additional card from management office for visitors

- **Applied in various operation systems such as crime prevention, access, time & attendance and meal service**
  - Supports various operation systems according to operation method setting of the terminal menu

- **Sufficient processing capacity of server**
  - In case of managing information of accessed people using the server,

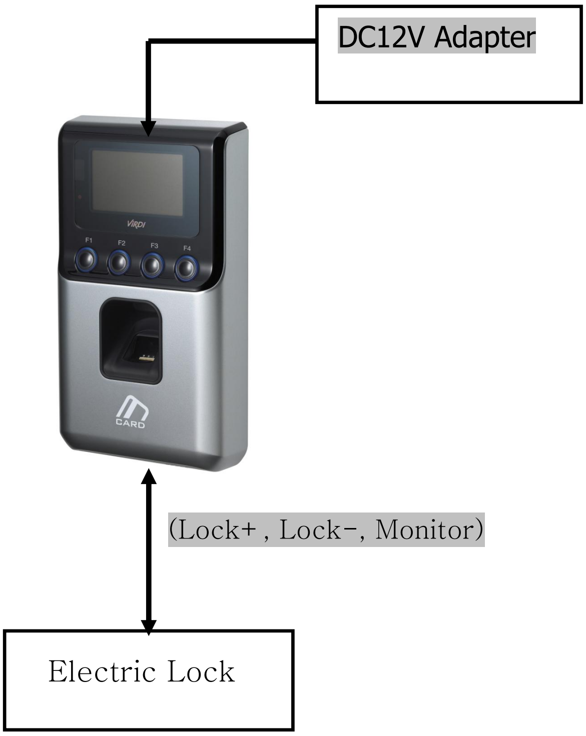
nearly limitless processing is possible.

- **Provides various registration and authentication methods**
  There are 4 registration and authentication methods available for general users. The registration and authentication method must be chosen before registering a user or administrator.

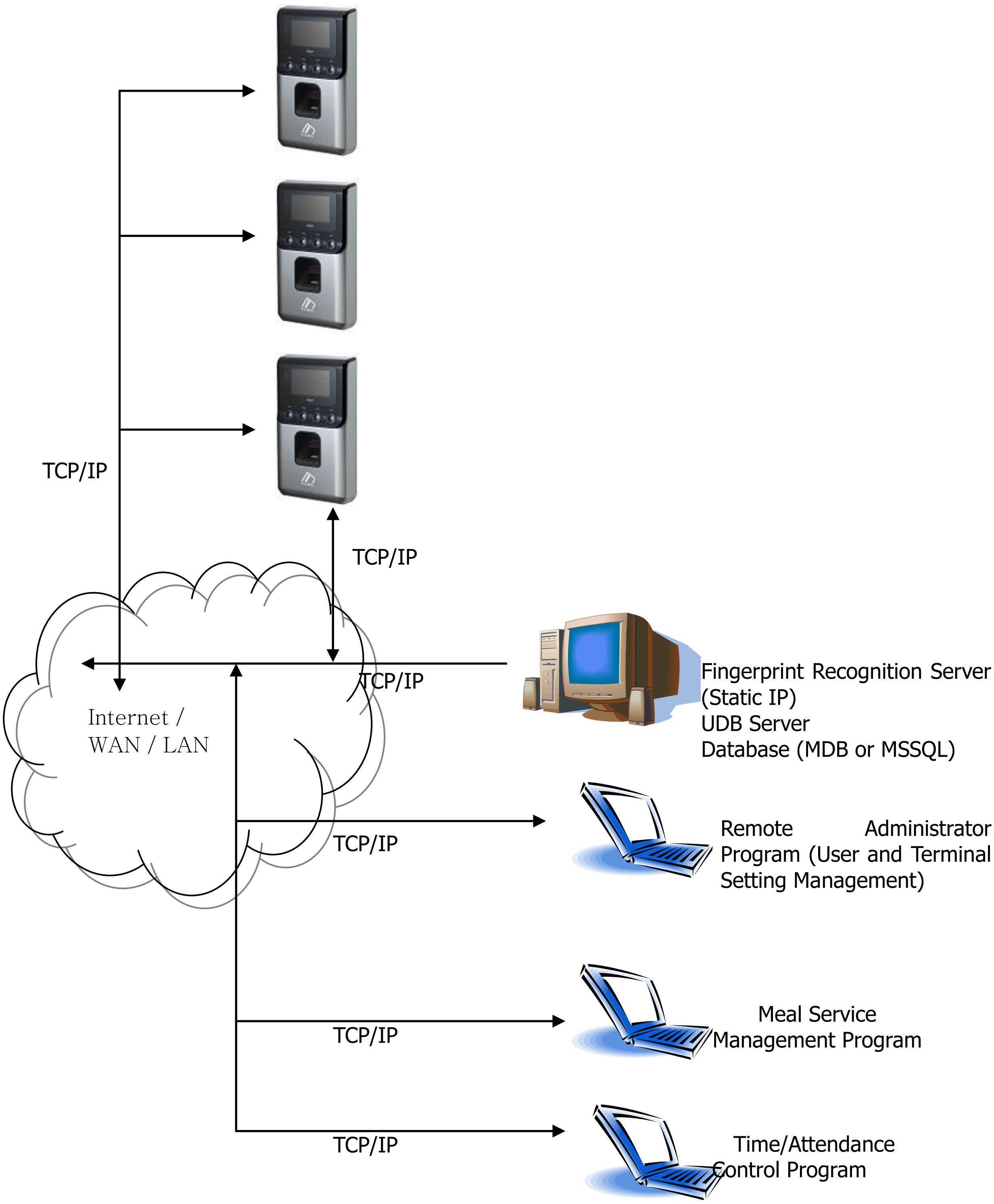
FP	Fingerprint registration Fingerprint authentication
RF	Card registration Card authentication
RF|FP	Card and fingerprint registration Card or fingerprint authentication
RF&FP	Card and fingerprint registration Fingerprint authentication after card authentication

2.2. Configuration Figure

2.2.1. Independent Use (Access)



2.2.2. Connection with PC server (Access, Time & Attendance and Meal Service Management)



2.3. Product Specifications

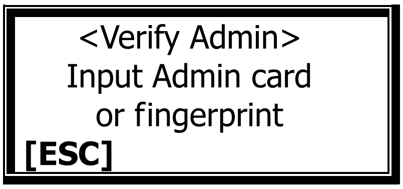
Classification	Specification	Remarks
CPU	32Bit RISC CPU(266MHz)	
MEMORY	8M SDRAM	
	4M FLASH	100 User 100 Finger 5,119 Log
Fingerprint Sensor	Optical	
Authentication Speed	Within 1 second	
Scan Area / Resolution	13 * 15mm / 500 DPI	
FRR / FAR	0.1% / 0.001%	
Communication Port	TCP/IP	Authentication server communication
	RS-232	Meal service printer
	RS-485	External device communication
	Wiegand In/Out	Card reader or external device communication
Temperature / Humidity	-20 ~ 50 / Lower than 90% RH	
LCD	128 X 64 Graphic LCD	
SIZE	92.3mm * 169.9mm * 39.5mm	
AC / DC Adapter	INPUT : Universal AC 100 ~ 250V	
	OUTPUT : DC 12V (Option : DC 24V)	
	UL, CSA, CE Approved	
Card Reader	Smart Card Reader	A-type, 13.56MHz
Option	Door phone	

3. Environment Setting

3.1. Items to Check before Setting Environment

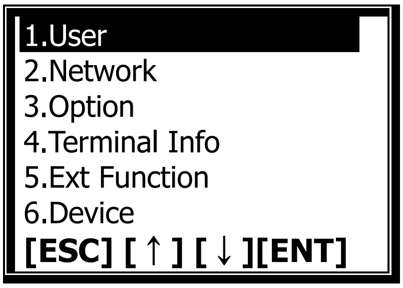
3.1.1. Entering Menu

If [F3] button is pressed for longer than 2 seconds, the following administrator authentication screen is displayed.



<Verify Admin>
Input Admin card
or fingerprint
[ESC]

If administrator authentication with card or fingerprint according to the registered authentication method succeeds, the system enters the menu as shown below.



1.User
2.Network
3.Option
4.Terminal Info
5.Ext Function
6.Device
[ESC] [↑] [↓][ENT]

F1 F2 F3 F4

After selecting a desired menu with **[↑]**(F2) and **[↓]**(F3) button, press [**ENT**](F4) button to enter the lower menu.

The description of F1, F2, F3 and F4 button functions are displayed in order at the bottom of the screen as shown in the above figure. Move up and down and make selection by pressing [ENT](F4). The system can transfer to the upper menu by pressing [ESC](F1).

※ The administrator authentication is displayed only when there is a registered administrator. Authentication is required only once during entry to the menu. Access rights to all menus are valid until the system leaves completely from the main menu.

3.1.2. Modifying Setting Values

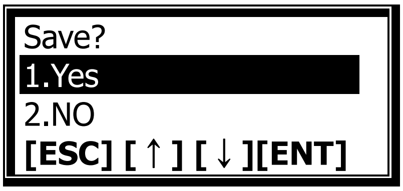
Setting values can be modified by pressing **[↑][↓]** button.
If a setting value is longer than 2 digits, move to the location of a digit to change by pressing **[←][→]** button and change the value by pressing **[↑][↓]** button.

After checking the setting value, press [ENT] button to continue setting.
To move to the upper menu during setting, press [ESC] button.

In case that the **[←][↑][↓][→]** buttons are the only buttons displayed ([ESC] and [ENT] buttons are not displayed), pressing down [F1] button for longer than 2 seconds replaces [ESC] button function while pressing down [F4] button for longer than 2 seconds replaces [ENT] button.

3.1.3. Saving after Completion of Environment Setting

To save the modified setting values, press [ESC] button in the main menu screen. Then, the following screen is displayed.



Save?
1.Yes
2.NO
[ESC] [↑] [↓][ENT]

After selecting [1.Yes] to save the modified setting values or [2. No] to cancel them, press [ENT] button.

- ➢ If no modification was made, the system leaves from the environment setting menu without the above "Save?" process.

- ➢ If there is no input value for a certain period of time during environment setting change, the system leaves from the environment setting menu. If a modification was made in such a case, "Save?" process shows up. If no modification was made, the system moves directly to the default screen.

3.1.4. Procedures to Enter Menu without Administrator Authentication

In case fingerprint authentication cannot be made because administrator password or card registered in the terminal is lost or no administrator is available, use the following procedures to enter the menu.

① Open the terminal cover.

② While the cover is open, set No. 4 dip switch of the board to the ON state.

③ Press down [F3] button for longer than 2 seconds to enter the menu. If you press [F4] button at the administrator authentication screen, "ppiririck" buzzer sound is heard and the system enters a selected menu.

- ➢ After the completion of setting value modification, **be sure to set No. 4 dip switch back to the OFF state.**

3.2. Menu Configuration

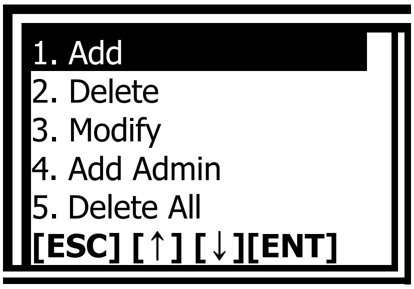
1.User	1. Add 2. Delete 3. Modify 4. Add admin 5. Delete All	
2.Network	1. Terminal ID	<Terminal ID> <Verify Mode>:NS/SN/NO/SO
	2.IP Address	<Network Type> <IP Address> <Subnet Mask> <Gateway>
	3. Server IP	<Server IP> <Server Port>
3.Option	1. Application	<Application> 0. Access Ctrl 1.T&A Ctrl 2.Meal Ctrl
		When setting as 0 or 1 <Start Time> <Leave Time> <Access Time>
		2.When setting as Meal Ctrl <Breakfast> <Lunch> <Dinner> <Supper> <Snack> <Without Limit>
	2. Verify Option	<Show User ID> <Only Card> <Template On Card> <Blocking Time>
	3. Set Doorlock	<Open Duration> <Door Monitor> <Door Open Alarm>
	4. Sound Control	<Voice Volume> <Beeper Volume> <Case Open Alarm>
	5. LCD Setting	<LCD Backlight> <LCD Light Ctrl>
	6. Time Setting	<Time Sync> <Calendar> <Time Setting>

4.Terminal Info	T-ID=0001 Ver=10.50.00 Application=Access Language=ENG Verify Mode=SN Network Type=Static Mac-Address=000265101234 IP Address=192.168.0.3 Gateway=192.168.0.1 Subnet Mask=255.255.255.0 Server IP=192.168.0.2 Svr-Port=2201 Card Reader=RF|SC|Wiegand CDR Version= Card Format=0 1:1 Level=3 1:N Level=4 All Admin=0 All User=0 Max User=100 1:N User=0 1:N FP=0 MAX 1:N FP=100 All FP=0 MAX FP=100 All Log=0 Max Log=5,119	
5.Ext Function	1. Lock Terminal 2. Read Card No.	
	3. Sensor Monitor	<Alarm Sensor1> <Send On/Off?> <Alarm Sensor2> <Send On/Off?>
6.Device	1. System Config	<ID Length> <Language>
	2. Card Reader	<Card Reader> <Card Format>
	3. FP-Sensor	<1:1 Level> <1:N Level> <LFD> <Check SameFP>
	4. Wiegand	<Wiegand Out>
	5. Initialize	1. Init Config 2. Delete Log 3. Init Terminal

3.3. User Control

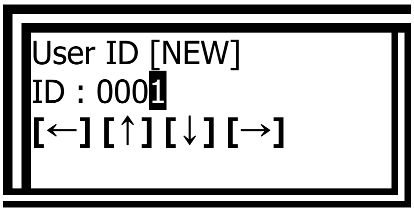
3.3.1. User Registration

If “1.User” in the main menu is selected, the following screen is displayed.



1. Add
2. Delete
3. Modify
4. Add Admin
5. Delete All
[ESC] [↑] [↓][ENT]

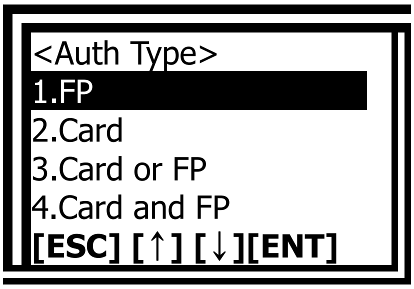
To register a new user, select “1.Add”.



User ID [NEW]
ID : 0001
[←] [↑] [↓] [→]

Enter the ID of a new user to be registered and press down [F4] button for a longer period of time.

The IDs that are allowed for registration are automatically shown on the screen during registration, thus allowing for a more convenient registration process. An ID can be changed using function keys. If an entered ID is already registered, the LCD message “Already registered ID” is displayed and a buzzer sound for failure is heard. Afterwards, the system moves to the upper menu. In case of an unregistered ID, the following authentication method selection screen is displayed.

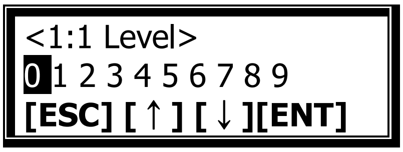


<Auth Type>
1.FP
2.Card
3.Card or FP
4.Card and FP
[ESC] [↑] [↓][ENT]

After selecting one of 4 authentication methods using **[↑][↓]** button, press [ENT] button.

3.3.1.1. Registration with “1.FP”

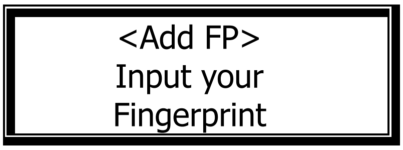
Both registration and authentication are made using fingerprint.
◆ At default screen [F3~]→ [1.User] → [1.Add] → User ID [F4~] → [1.FP] → Select 1:1 authentication level [ENT] → Enter fingerprint → Reenter the same fingerprint ◆


<1:1 Level>
0 1 2 3 4 5 6 7 8 9
[ESC] [↑] [↓][ENT]

Recommended setting: '0'

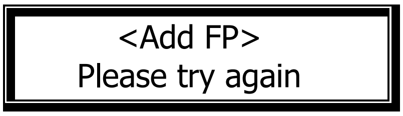
This menu determines the authentication level for each user to be registered. The authentication level for each registered user can be set differently by changing this value.
If this value is set as '0', authentication is done using 1:1 authentication level set at the terminal rather than the authentication level for each user.

After the completion of setting, press [ENT] button to continue setting.


<Add FP>
Input your
Fingerprint

Enter fingerprint by referring to "1.9. Proper Fingerprint Registration and Input Method"

When the fingerprint sensor is lighted, touch the fingerprint input window with the finger. When "ppik" buzzer sound is heard, wait for 2~3 seconds until the light is turned off and remove the finger.
If the first fingerprint input succeeds, reenter the same fingerprint after the "Please try again" message (shown below) is displayed.


<Add FP>
Please try again

Reenter the same fingerprint.

Be sure to note that you must remove the finger from the fingerprint input window before you make the second fingerprint input attempt. When registration is completed, the system returns to "1.Add" selection screen. Up to 3 trials can be done should the registration fail.

The following are the LCD guidance messages displayed during the registration process.

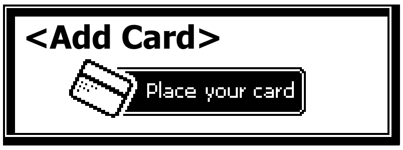
Registration Completed!	In case of authentication success
Registration Failed!	In case of authentication failure
Fingerprint registration failed!	In case fingerprint image quality is poor or no fingerprint input is entered within 10 seconds after fingerprint sensor is lighted
Already registered FP	In case a user attempts to register an already registered fingerprint

If a proper fingerprint registration method fails after 2~3 trials, the use of card is recommended.

3.3.1.2. Registration with "2. Card"

Both registration and authentication are made only using card.

◆ At default screen [F3~]→ [1.User] → [1.Add] → User ID [F4~] → [2.Card] → Card reading ◆



<Add Card>

Place your card

Place a card to be registered. To cancel registration and escape, press [ESC] button.

When registration is completed, the system returns to "1. Add". Up to 3 trials can be made should the registration fail.

The following are the LCD guidance messages displayed during the registration process.

Registration Completed!	In case of authentication success
Registration Failed!	In case of authentication failure
Already registered card	In case a user attempts to register an already registered card

3.3.1.3. Registration with "3. Card or FP"

A user is registered with card and fingerprint. Authentication is done using card or fingerprint.

◆ At default screen [F3~] → [1.User] → [1.Add] → User ID [F4~] → [3.Card or FP] → Card reading → 1:1 authentication level [ENT] → Enter fingerprint → Reenter the same fingerprint ◆

For the registration process of a user, fingerprint registration (Refer to Registration with "1. FP") is done after card registration is completed (Refer to Registration with "2.Card").

3.3.1.4. Registration with "4. Card and FP"

A user is registered using card and fingerprint. Fingerprint authentication is also required after card authentication is completed.

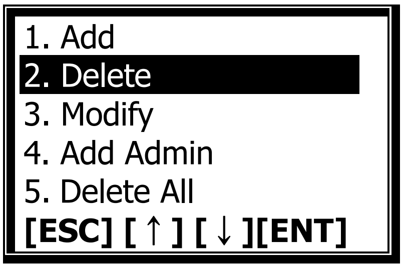
◆ At default screen [F3~] → [1.User] → [1.Add] → User ID [F4~] → [4.Card and FP] → Card reading → 1:1 authentication level [ENT] → Enter fingerprint → Reenter the same fingerprint ◆

For the registration of a user, fingerprint registration (Refer to Registration with "1. FP") is done after card registration is completed (Refer to Registration with "2.Card").

3.3.2. User Deletion

◆ At default screen [F3~] → [1.User] → [2.Delete] → User ID [F4~] ◆

If "1.User" is selected by pressing [1] button in the main menu, the following screen is displayed.



Select [2.Delete] to delete a user.

This is an item that deletes a user registered in the terminal. After entering the ID of a user to be deleted, press down [F4] button for a longer period of time. Afterwards, the buzzer sound for success is heard and user information is deleted from the terminal. Note that deleting information from the terminal does not delete the information in the server. To completely delete information, you must also delete the information in the server.

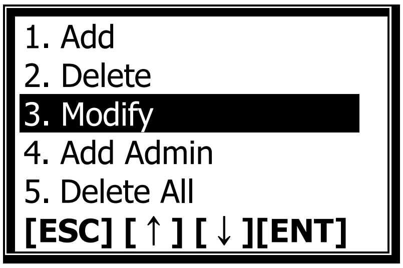
If the ID of an unregistered user is entered, the LCD message "Unregistered ID" is displayed and the buzzer sound for failure is heard. Afterwards, the system moves to the menu at the time of selecting "2. User Deletion".

Be sure to note that general user and administrator are not distinguished when deleted. Also, note that user information cannot be recovered in case of deleting a user who is registered only in the terminal but not in the network server.

3.3.3. User Change

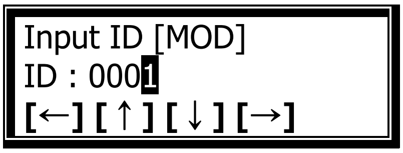
◆ At default screen [F3~] → [1.User] → [3.Modify] → User ID [F4~] → Select information to modify → Modify user information ◆

Select "1.User" at the main menu.



1. Add
2. Delete
3. Modify
4. Add Admin
5. Delete All
[ESC] [↑] [↓][ENT]

Select [3.Modify] to modify a user.



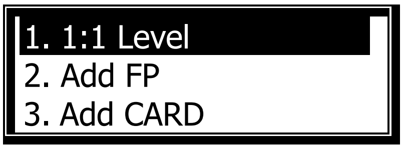
Input ID [MOD]
ID : 0001
[←] [↑] [↓] [→]

After entering the ID of a user to be modified, press down [ENT] button for a longer period of time.

Modification can be made without distinguishing general user and administrator. If the ID of an unregistered user (or administrator) is entered, the LCD message "Unregistered ID" is displayed and the buzzer sound for failure is heard. Afterwards, the system moves to the menu at the time of selecting "1.Add".

Items that can be modified vary according to the authentication method of a user. They are classified as shown below.

3.3.3.1. User Registered with "1.FP"

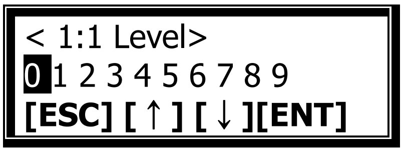


1. 1:1 Level
2. Add FP
3. Add CARD

Select [1] to modify authentication level, [2] to add fingerprint to the corresponding ID and [3] to add card.

※ Up to 10 fingerprints can be registered in one ID. If registration exceeding 10 fingerprints is attempted by selecting [2], the buzzer sound for failure is heard and "Excess of the limit" message is displayed on the LCD screen.

[1] In case of selecting 1:1 level change

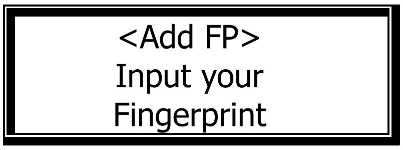


< 1:1 Level>
0 1 2 3 4 5 6 7 8 9
[ESC] [↑] [↓][ENT]

Recommended setting: '0'

To change it, enter a new setting value.

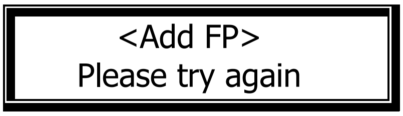
[2] In case of selecting Add FP



<Add FP>
Input your
Fingerprint

Enter fingerprint by referring to “1.9. Proper Fingerprint Registration and Input Method”

When the fingerprint sensor is lighted, place the finger on the fingerprint input window. If the “ppik” buzzer sound is heard, wail for 2~3 seconds until the light is switched off, and then remove the finger.
If the first fingerprint input attempt succeeds, the “Please try again” message (shown below) is displayed. Then, reenter the same fingerprint.



<Add FP>
Please try again

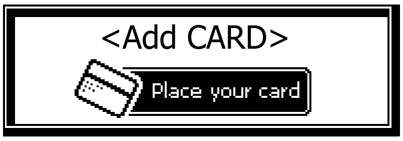
Reenter the same fingerprint.

Be sure to note that you must remove the finger from the fingerprint input window before you make the second fingerprint input attempt. When registration is completed, the system returns to “1.Add” selection screen. Up to 3 trials can be done should the registration fail.

The following are the LCD messages displayed during the registration process.

Modification Completed!	In case of registration success
Modification Failed!	In case of registration failure
Fingerprint registration failed!	In case fingerprint image quality is poor or no fingerprint input is entered within 10 seconds after fingerprint sensor is lighted
Already registered FP	In case of trying to register an already registered fingerprint
Excess of the limit	In case 10 fingerprints are already registered in the corresponding ID

[3] In case of selecting Add CARD



<Add CARD>
Place your card

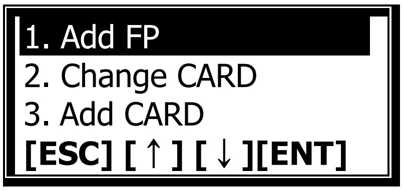
Press [ESC] button to cancel registration.

After the card is placed, the buzzer sound for success is heard and a newly entered card number is added.
If more than 3 card change trials fail, the buzzer sound for failure is heard and the system returns to “1. Add” selection screen.

The following are the LCD messages displayed during the registration process.

Modification Completed!	In case of registration success
Modification Failed!	In case of registration failure
Already registered card	In case of trying to register an already registered card
Excess of the limit	In case 10 cards are already registered in the corresponding ID

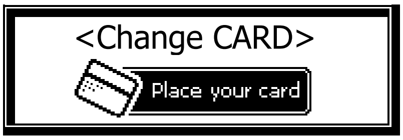
3.3.4.2. User Registered with "2.Card"



Select [1] to add fingerprint, [2] to change card and [3] to add card.

[1] In case of selecting Add FP: Refer to [2] In case of selecting Add FP of 3.3.3.1.

[2] In case of selecting Change CARD

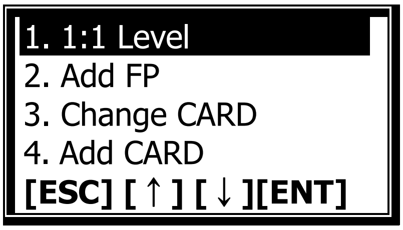


Press [ESC] button to cancel change.

After the card is placed, the "Processing is completed." voice message is heard and the card number of a user is changed to the newly entered card. If card change trial fails more than 3 times, the buzzer sound for failure is heard and the system returns to "1.Add" selection screen.

[3] In case of selecting Add CARD: Refer to [3] In case of selecting Add CARD of 3.3.3.1.

3.3.4.3. User Registered with "3. CARD or FP" , "4.CARD and FP"



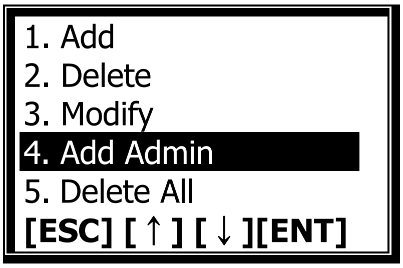
Select [1] to change authentication level, [2] to add fingerprint to the corresponding ID, [3] to change card number and [4] to add card

[1] In case of selecting 1:1 Level change: Refer to [1] In case of selecting authentication level change of 3.3.3.1.
[2] In case of selecting Add FP: Refer to [2] In case of selecting Add FP of 3.3.3.1.
[3] In case of selecting Change CARD: Refer to [2] In case of selecting Change CARD of 3.3.3.2.
[4] In case of selecting Add CARD: Refer to [3] In case of selecting Add CARD of 3.3.3.1.

3.3.4. Administrator Registration

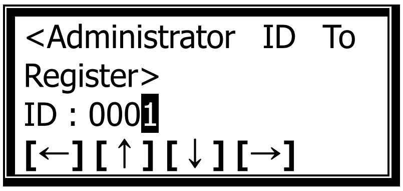
◆ At default screen [F3~] → [1.User] → [4.Add Admin] → Administrator ID [F4~] ◆

Select "1.User" at the main menu.



1. Add
2. Delete
3. Modify
4. Add Admin
5. Delete All
[ESC] [↑] [↓][ENT]

Select [4.Add Admin] to register an administrator.



<Administrator ID To Register>
ID : 0001
[←] [↑] [↓] [→]

After entering the ID of an administrator to change, press down [F4] button for a longer period of time.

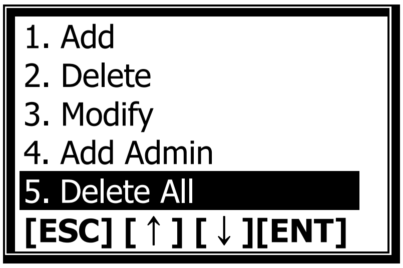
※ Administrator registration processes beyond this point are identical to general user registration processes.

A user registered as an administrator can change terminal's operation environment. An administrator can register/modify/delete information of all users saved in the terminal, therefore, caution should be exercised for terminal's administrator registration.

3.3.5. All User Deletion

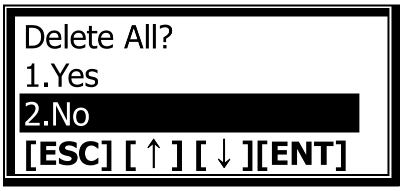
◆ At default screen [F3~] → [1.User] → [5.Delete All] ◆

Select "1.User" at the main menu.



1. Add
2. Delete
3. Modify
4. Add Admin
5. Delete All
[ESC] [↑] [↓][ENT]

Select [5] to delete all users.



Delete All?
1.Yes
2.No
[ESC] [↑] [↓][ENT]

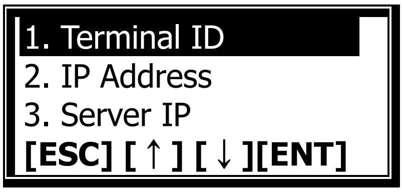
Select [1] to delete all users and [2] to cancel deletion.

After selecting “1.Yes” to answer the above confirmation question, **all users including administrators are deleted. Therefore, special caution needs to be taken before using this function.**

When the deletion process is completed, the buzzer sound for success is heard and the system returns to menu at the time of selecting “1.Add”.

3.4. Network Setting

If “2.Network” is selected at the main menu, the following screen is displayed.



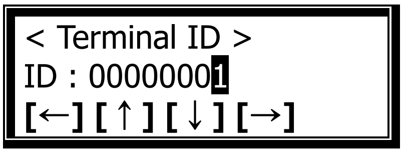
1. Terminal ID
2. IP Address
3. Server IP
[ESC] [↑] [↓][ENT]

Select [1] to change terminal ID, [2] to change IP setting and [3] to change server IP.

3.4.1. Terminal ID

◆ At default screen [F3~] → [2.Network] → [1.Terminal ID] ◆

3.4.1.1. Terminal ID

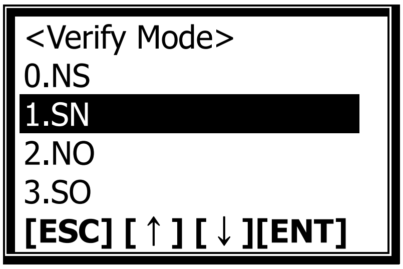


< Terminal ID >
ID : 00000001
[←] [↑] [↓] [→]

This ID is a unique ID used by the authentication server to distinguish the terminals. The default value is ‘00000001’.

This value must be identical to the ID of a door set at the server program. An 8-digit number is entered. Press down [ENT] button for a longer period of time to move to the next menu.

3.4.1.2. Authentication Priority [NS / SN / NO / SO] Setting



<Verify Mode>
0.NS
1.SN
2.NO
3.SO
[ESC] [↑] [↓][ENT]

Select [0] for NS,
[1] for SN,
[2] for NO,
and [3] for SO.

This is an item that determines the authentication priority between a terminal and the network server. The default value is '1.SN'. Authentication procedures for each mode are shown below.

NS	If the server is connected, authentication is processed at the server. If the server is disconnected due to network failure, authentication is processed at the terminal.
SN	Even if the server is connected, authentication is processed at the terminal and the authentication result is sent to the server in real-time. But if an entered user is not registered in the terminal, authentication is processed at the server. (In case of 1:N fingerprint authentication, server authentication is not attempted.)
NO	Even if a user is registered in the terminal, authentication is always processed at the server.
SO	Only a user registered in the terminal is authenticated. If the server is connected, the authentication result is sent in real-time.

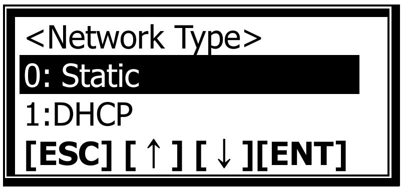
It can be set flexibly according to various considerations such as the number of terminals connected to the server, the number of users to be authenticated or the frequency of network failure occurrence. However, in case the number of authentication trials is high because more than 10 terminals are connected to the server or in case network failure occurs frequently, SN authentication ('1' setting) is recommended.

After carefully entering the input value, press [ENT] button to move to the upper menu.

3.4.2. IP Setting

◆ At default screen [F3~] → [2.Network] → [2.IP Address] ◆

3.4.2.1. Connection Type Setting



```
<Network Type>
0: Static
1:DHCP
[ESC] [↑] [↓][ENT]
```

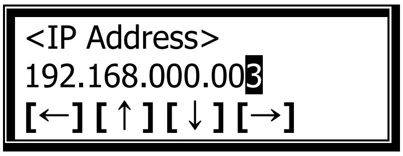
Select [0] to acquire static IP and [1] to acquire dynamic IP.

This item selects a type for connecting a terminal to a server. The default value is '0' (Static IP).
Select [0] if a static IP is acquired from the connected server and [1] if a dynamic IP is acquired from the DHCP server existing in the network.

After carefully entering the input value, press [ENT] button to continue setting.

※ If the connection type is set as static IP (0), the following 3.4.2.2. IP address, 3.4.2.3. Subnet mask and 3.4.2.4. Gateway need to be set. However, a dynamic IP does not require these setting processes.

3.4.2.2. IP Address Setting



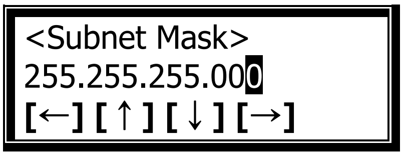
```
<IP Address>
192.168.000.003
[←] [↑] [↓] [→]
```

After moving to the position of a digit to change using [←][→] button, change the value using [↑][↓] button.

IP address assigned to the terminal is set.

After carefully entering the value, press down [F4] button for a longer period of time to continue setting.

3.4.2.3. Subnet Mask Setting



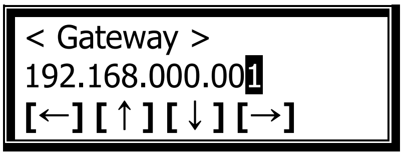
```
<Subnet Mask>
255.255.255.000
[←] [↑] [↓] [→]
```

After moving to the position of a digit to change using [←][→] button, change the value using [↑][↓] button.

The subnet mask of the network which the terminal is connected to is set.

After carefully entering the value, press down [F4] button for a longer period of time to continue setting.

3.4.2.4. Gateway Setting



< Gateway >
192.168.000.001
[←] [↑] [↓] [→]

After moving to the position of a digit to change using [←][→] button, change the value using [↑][↓] button.

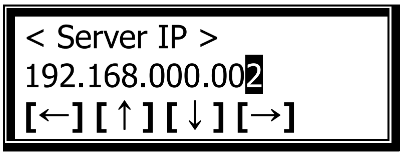
The gateway IP address of the network which the terminal is connected to is entered.

After carefully entering the value, press down [F4] button for a longer period of time to continue setting.

3.4.3. Server IP Setting

◆ At default screen [F3~]→ [2.Network] → [3.Server IP] ◆

3.4.3.1. Server IP Setting



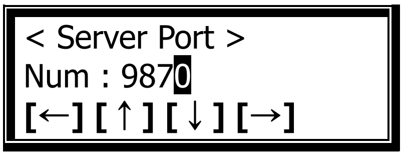
< Server IP >
192.168.000.002
[←] [↑] [↓] [→]

After moving to the position of a digit to change using [←][→] button, change the value using [↑][↓] button.

The IP address of the network server which the terminal is connected to is designated.

After carefully entering the value, press [F4] button for a longer period of time to continue setting.

3.4.3.2. Server Port Setting



< Server Port >
Num : 9870
[←] [↑] [↓] [→]

After moving to the position of a digit to change using [←][→] button, change the value using [↑][↓] button.

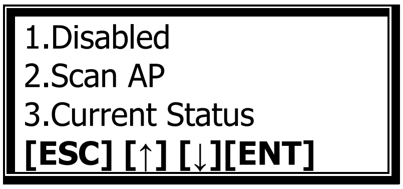
This is an item that enters the port of the authentication server. The default port value of the authentication server is '9870'. Note that if this value is changed, the value at the server program must also be changed.

After carefully entering the value, press down [F4] button for a longer period of time to move to the upper menu.

3.4.4. Wireless LAN Setting

◆ On the basic screen [F3~]→ [2.Network] → [4.Wireless LAN] ◆

3.4.4.1. Setting to use wireless LAN



1.Disabled
2.Scan AP
3.Current Status
[ESC] [↑] [↓][ENT]

Default: 1. Disabled

This menu only appears if WiFi module is inserted, and it sets up whether a terminal uses wired LAN or wireless LAN.
You can modify whether you use it or not by pressing the key'1', and you can use wireless LAN only if it is set as 'Enabled'
To use wired LAN, it should be set as 'Disabled'

3.4.4.2. Search for AP

◆ On the basic screen [F3~]→[2.Network]→[4.Wireless LAN]→[2.Scan AP] ◆

It searches for AP nearby. Once it displays AP nearby on the screen after searching, select one to connect by pressing [↑] or [↓] button and press [F4] button. Then choose applicable encryption method for selected AP and press [F4]. Once you input password on the screen, wireless LAN setting will be completed.

3.4.4.3. Search for status

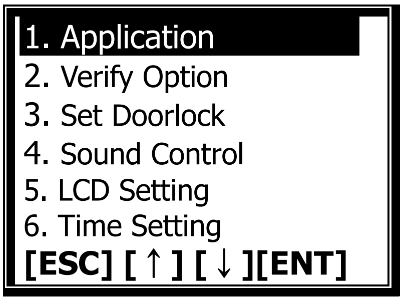
◆ On the basic screen [F3~]→[2.Network]→[4.Wireless Lan]→[3.Current Status] ◆

It shows AP connecting wireless LAN and current connection status.

3.5. Option Setting

3.5.1. Application Setting

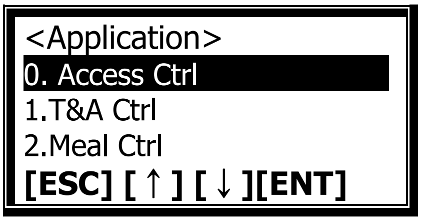
If [3.Option] is selected at the main menu, the following screen is displayed.



1. Application
2. Verify Option
3. Set Doorlock
4. Sound Control
5. LCD Setting
6. Time Setting
[ESC] [↑] [↓][ENT]

Select [1] to set the operation mode of the terminal.

◆ At default screen [F3~] → [3.Option] → [1. Application] ◆



<Application>
0. Access Ctrl
1.T&A Ctrl
2.Meal Ctrl
[ESC] [↑] [↓][ENT]

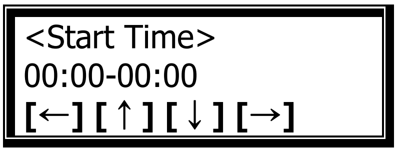
A desired operation mode can be set and the default value is '0' (Access Ctrl).

This item selects the operation mode of the terminal. Select '0' for operation as simple access control, '1' for operation as time & attendance control and '2' for operation as meal service management.

After making the selection, press [ENT] button to enter the sub-setting menu of each operation type.

3.5.1.1 In case of Setting as "[0. Access Ctrl]" or "[1.T&A Ctrl]"

This item sets the default setting hour of each time & attendance mode. It is possible to set terminal display mode to be automatically changed to time & attendance mode in setting after the completion of authentication.



<Start Time>
00:00-00:00
[←] [↑] [↓] [→]

If time setting is not required, it is set to '00:00-00:00'.

This item sets the default office start time. After moving to the position of the time to change using [←][→] button, change the value using [↑][↓] button.

Unless other function buttons are pressed, office start time mode is always displayed during the time period in setting. Even if authenticated as office leave mode by pressing [F2] button, the mode is switched back to office start mode after authentication is completed to provide convenience in the time & attendance control.

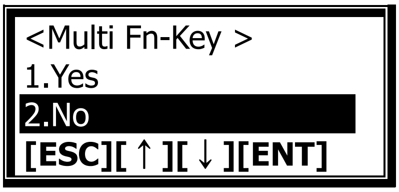
After setting <Start Time>, the identical method is used to set <Leave Time>,

<F3 Time>, <F4 Time> and <Access Time>. As shown in the following example, these hours must be overlapped.

(Example) Start Time=06:00~09:59, Leave Time=17:00~22:00

<Start Time>	<Leave Time>
06:00~09:59	17:00~22:00

Press [ENT] button to continue setting.

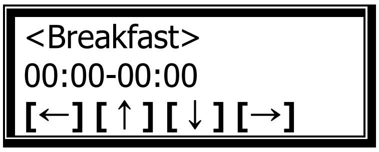


<Multi Fn-Key >
1.Yes
2.No
[ESC][↑][↓][ENT]

Default Setting: '2.No'

This is the setting for using more than 5 authentication modes. It is the menu to make for F5~F7 by using F1~F3. If '1.Yes' is selected, F1(F2, F3) on F1 mode(F2, F3) is pressed again, it changes to F5(F6, F7) mode.

3.5.1.2. In case of Setting as "[2.Meal Ctrl]"



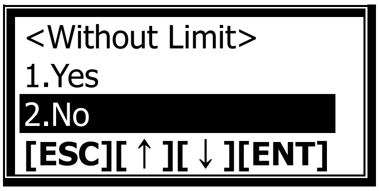
<Breakfast>
00:00-00:00
[←] [↑] [↓] [→]

In case time setting is not required, it is set to '00:00-00:00'.

This item sets the breakfast hour. Authentication is done as breakfast during this hour.
After the completion of breakfast hour setting, the identical method is used to set <Lunch>, <Dinner>, <Supper> and <Snack>. 00:00-00:00 is set for meals that are not used.

Each of the meal hours must not be overlapped. For the hours not set for meal service, "Locked!" message is displayed on the terminal and all inputs except entry to menu mode are blocked just as in terminal lock mode.

In case the setting is made up to <Snack>, the menu that determines whether to allow duplicated authentication is displayed as shown below.

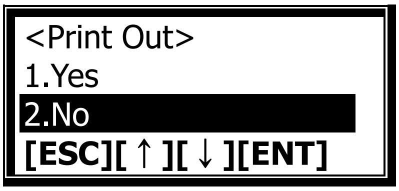


<Without Limit>
1.Yes
2.No
[ESC][↑][↓][ENT]

Default setting: '2.No'

If it is set to No, only one authentication is allowed during a given meal service hour. If the second authentication trial is attempted, authentication fails and "Duplicated!" message is displayed.

Press [ENT] button to continue setting.



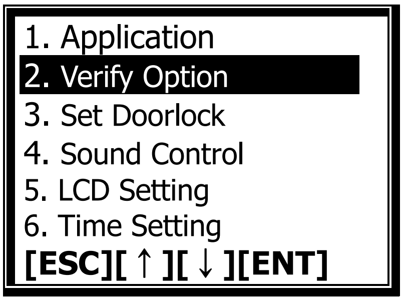
<Print Out>
1.Yes
2.No
[ESC][↑][↓][ENT]

Default setting: '2.No'

This menu is to set up if the authentication result is needed for printing. If you set up '1', the printer connected by RS232 prints out terminal ID, user ID, date and time and authentication mode. The compatible printer is "SPR-350" Serial model.

3.5.2. Authentication Method Setting

If [3.Option] is selected at the main menu, the following screen is displayed.

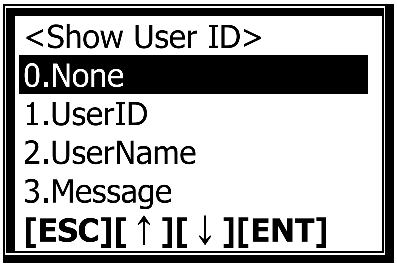


1. Application
2. Verify Option
3. Set Doorlock
4. Sound Control
5. LCD Setting
6. Time Setting
[ESC][↑][↓][ENT]

Select [2.Verify Option] to set the default authentication method of the terminal.

3.5.2.1. ID Display Option Setting upon Authentication Success

◆ At default screen [F3~] → [3.Option] → [2.Verify Option] ◆



<Show User ID>
0.None
1.UserID
2.UserName
3.Message
[ESC][↑][↓][ENT]

Default setting: '0'

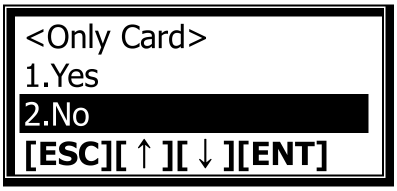
If the default setting '0' is used, only the authentication result message is displayed upon authentication success. If it is set to '1', the ID of an authenticated user is displayed on the LCD screen as shown below. If it is set to '2', the user's name is displayed on the LCD screen. However, if the user's name is not available, the ID is displayed instead. If it is set to '3', the user's

message is displayed on the LCD screen. However, if the user's message is not available, the ID is displayed instead.
(Example) OK!<0001>

Press [ENT] button to continue setting.

3.5.2.2. Setting to Determine Whether to Allow Authentication Only using Card

◆ At default screen [F3~] → [3.Option] → [2.Verify Option] → [ENT] ◆



```
<Only Card>
1.Yes
2.No
[ESC][↑][↓][ENT]
```

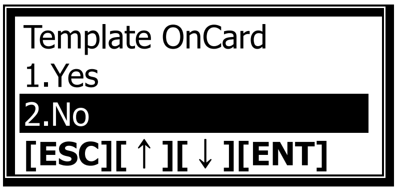
Default setting: '2.No'

This option allows authentication only using card without fingerprint input. In case this option is set to '1' in the terminal, only card authentication is done even if authentication with both CARD and FP is registered.

Press [ENT] button to continue setting.

3.5.2.3. Authentication option only with the stored info in Smart Card

◆ At default screen [F3~] → [3.Option] → [2.Verify Option] → [ENT] → [ENT] ◆



```
Template OnCard
1.Yes
2.No
[ESC][↑][↓][ENT]
```

Default setting: '2.No'

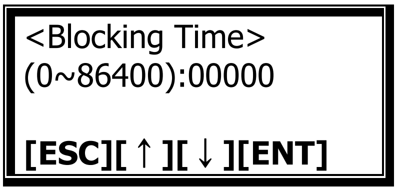
This option allows identifying only with user info and fingerprint stored in the card and it does not require user info to be downloaded to the terminal. For the option, terminal must have Smart Card reader module and set up as '1. Yes' in <Template OnCard> menu

Press [ENT] button to continue setting.

3.5.2.4. Blocking Time Setting

◆ At default screen [F3~] → [3.Option] → [2.Verify Option] → [ENT] →

[ENT] → [ENT] ◆


```
<Blocking Time>
(0~86400):00000

[ESC][↑][↓][ENT]
```

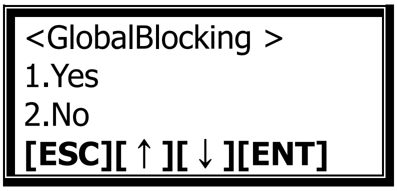
Default setting: 00000 (Unit: Second)

This function prevents a same user from getting authenticated again within a certain time. If the value is set for '0', there is no use but if it is greater than '0', the re-authentication will be permitted only after the time.

After selecting a setting value, press [ENT] button to finish authentication method setting and move to the upper menu.

3.5.2.5. Global Blocking setting

◆ In the basic window, [F3~] → [3.Option] → [2.Verify Option] → [ENT] → [ENT] → [ENT] → [ENT]

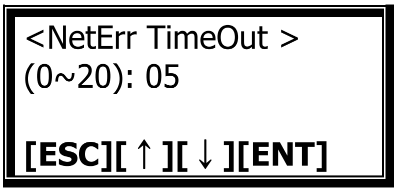

```
<GlobalBlocking >
1.Yes
2.No
[ESC][↑][↓][ENT]
```

Basic setting : '2.No'

It is the function to prevent for the user to authorize in short time. It blocks the terminal for the specific time after authorization success
If you click [ENT] button after selecting the setting value, it is moved to the next menu.

3.5.2.6. NetErr TimeOut – Network error time setting (Sec)

◆ In the basic window, [F3~] → [3.Option] → [2.Verify Option] → [ENT] → [ENT] → [ENT] → [ENT] → [ENT]


```
<NetErr TimeOut >
(0~20): 05

[ESC][↑][↓][ENT]
```

Basic setting: 5sec

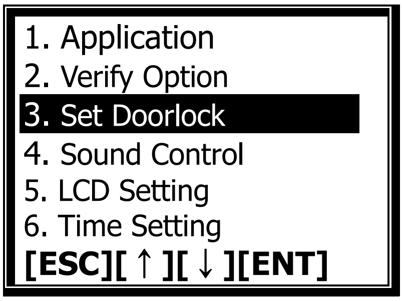
In the server authorization mode, if you set the network error time, you can

set authorization waiting time.
For example, if you set network error time as 5 seconds, the error message appear when there is no response for 5 seconds in the user authorization. (But, the user is considered to be failed to authorize).

If you click [ENT] button after selecting the set value, all the authorization method setting is finished and it is moved to the upper menu.

3.5.3. Door Setting

If [3.Option] is selected at the main menu, the following screen is displayed.



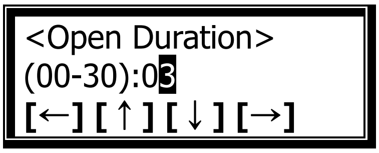
1. Application
2. Verify Option
3. Set Doorlock
4. Sound Control
5. LCD Setting
6. Time Setting

[ESC][↑][↓][ENT]

Select [3.Set Doorlock] for door setting.

3.5.3.1. Door Open Duration Setting

◆ At default screen [F3~] → [3.Option] → [3.Set Doorlock] ◆



<Open Duration>
(00-30):03
[←] [↑] [↓] [→]

Default setting: '03' (Unit: Second)

This option sets the duration of time until the door is locked again after the door is opened through authentication success in the terminal. Strike type represents a time when the door is locked again automatically after the door is opened through authentication success. In case of dead bolt type and automatic door, the door operates regardless of these setting values.

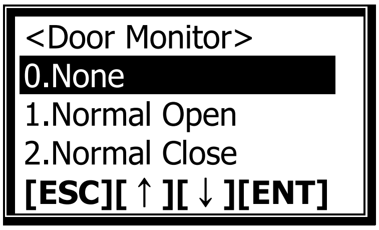
`

If it is set to '00', door control is not possible. Use '00' setting only when the lock is not connected.

After selecting a setting value, press down [F4] button for a longer period of time to continue setting.

3.5.3.2. Door Open Status Check

◆ At default screen [F3~] → [3.Option] → [3.Set Doorlock] → [F4~] ◆



```
<Door Monitor>
0.None
1.Normal Open
2.Normal Close
[ESC][↑][↓][ENT]
```

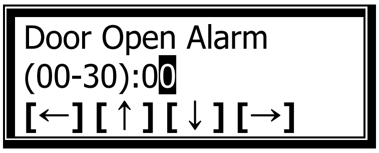
Default setting: '0'

- '0.None': In case door status is not checked
- '1.Normal Open': In case of dead bolt type or automatic door
  (In case lock monitoring is open when the door is locked)
- '2.Normal Close': In case of strike type
  (In case lock monitoring is close when the door is locked)

Select '0' for no setting, '1' for dead bolt type or automatic door and '2' for strike type. In case it is set to '1' or '2', information of the door connected to the terminal is sent to the server periodically.

After selecting a setting value, press [ENT] button to continue setting.

3.5.3.3 Door Open Alarm Setting



```
Door Open Alarm
(00-30):00
[←] [↑] [↓] [→]
```

Default setting: '00'

The terminal checks how long the door is opened. This function issues an alarm if the door is opened for a duration that exceeds the time in setting (Min. 5seconds ~Max. 30 seconds).
If it is set to '00', an alarm is issued. Even if it is set to 01~04, an alarm is issued after at least 5 seconds are elapsed.

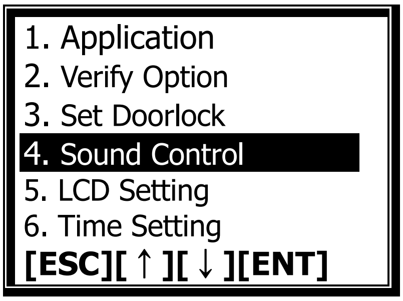
The door should be locked within the time in setting but the door may not be locked due to unforeseen circumstances. In such a case, an alarm is issued to determine the cause of a problem and take the necessary measures to ensure normal door operation.

To use this function, the lock must have a monitoring function that checks the opening/locking of the door. Also, the monitoring pin of the lock must be connected to the terminal. In addition, the door open state check in the previous item must be set to '1' or '2' in order to set this function.

After selecting a setting value, press down [F4] button for a longer period of time to continue setting. Afterwards, all settings for the door are completed and the system moves to the upper menu.

3.5.4. Volume Setting

If [3.Option] is selected at the main menu, the following screen is displayed.

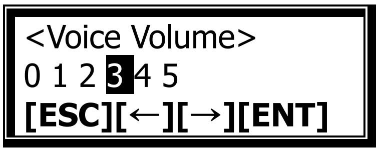


```
1. Application
2. Verify Option
3. Set Doorlock
4. Sound Control
5. LCD Setting
6. Time Setting
[ESC][↑][↓][ENT]
```

Select [4.Sound Control] to set volume.

3.5.4.1. Voice Volume Setting

◆ At default screen [F3~] → [3.Option] → [4.Sound Control] ◆



```
<Voice Volume>
0 1 2 3 4 5
[ESC][←][→][ENT]
```

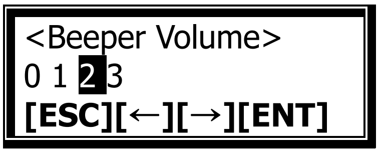
Default setting: '3'

This option sets the volume level during voice guidance. If it is set to '0', voice message is not issued.

Press [ENT] button to continue setting.

3.5.4.2. Buzzer Volume Setting

◆ At default screen [F3~] → [3.Option] → [4.Sound Control] → [ENT] ◆



```
<Beeper Volume>
0 1 2 3
[ESC][←][→][ENT]
```

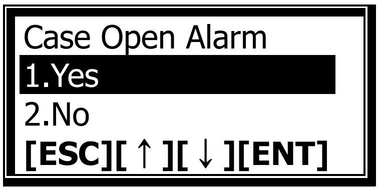
Default setting: '2'

This option sets the volume level of the terminal buzzer. If it is set to '0', no buzzer sound is heard. '1' produces low buzzer sound while '3' produces high buzzer sound.

Press [ENT] button to continue setting.

3.5.4.3. Cover Open Alarm Setting

◆ At default screen [F3~] → [3.Option] → [4.Sound Control] → [ENT] → [ENT] ◆



Case Open Alarm
1.Yes
2.No
[ESC][↑][↓][ENT]

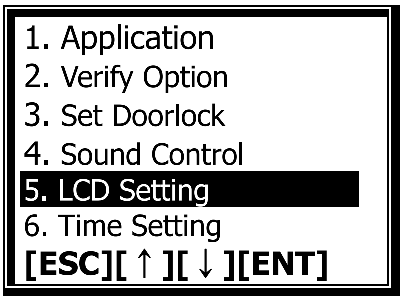
Default setting: '1.Yes'

This option determines whether to issue a warning after the terminal cover is opened. An alarm is issued for '1' setting and no warning for '2' setting.

After selecting a setting value, press [ENT] button to move to the upper menu.

3.5.5. LCD Setting

If "3.Option" is selected at the main menu, the following screen is displayed.

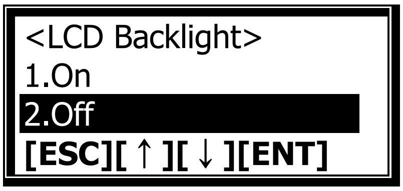


1. Application
2. Verify Option
3. Set Doorlock
4. Sound Control
5. LCD Setting
6. Time Setting
[ESC][↑][↓][ENT]

Select [5] to set LCD.

3.5.5.1. On/Off Setting of LCD Backlight

◆ At default screen [F3~] → [3.Option] → [5.LCD Setting] ◆



<LCD Backlight>
1.On
2.Off
[ESC][↑][↓][ENT]

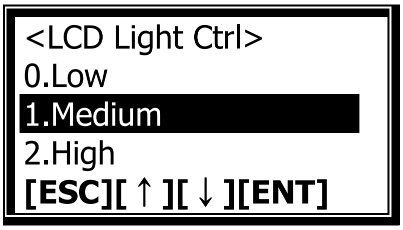
Default setting: '2.Off'

This option sets the on/off state of the terminal LCD backlight.
If it is set to '1.On', the LCD backlight is always on. If it is set to '2.Off', the LCD backlight is off except during key or card operation. The light is switched off

automatically about 10 seconds after a key or card operation is completed.

Press [ENT] button to continue setting.

3.5.5.2. LCD Brightness Setting



```
<LCD Light Ctrl>
0.Low
1.Medium
2.High
[ESC][↑][↓][ENT]
```

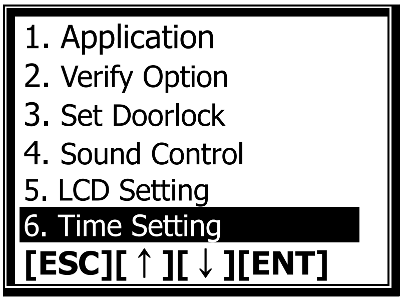
Default setting: ‘1’

This option sets the brightness of the terminal LCD light. Select ‘0’ for dim light and ‘2’ for bright light.

After selecting a setting value, press [ENT] button to move to the upper menu.

3.5.6. Time Setting

If “3.Option” is selected at the main menu, the following screen is displayed.

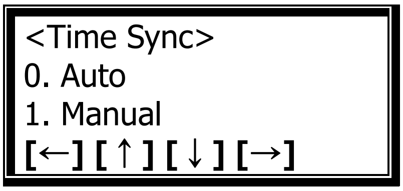


```
1. Application
2. Verify Option
3. Set Doorlock
4. Sound Control
5. LCD Setting
6. Time Setting
[ESC][↑][↓][ENT]
```

Select [6] to set the current time.

3.5.6.1. Time Synchronization

◆ At default screen [F3~] → [3.Option] → [6.Time Setting] ◆



```
<Time Sync>
0. Auto
1. Manual
[←] [↑] [↓] [→]
```

Default Setting: ‘0. Auto’

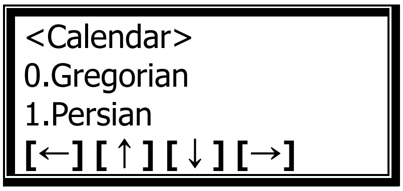
This menu is to set up the terminal time synchronization with the Server. ‘0.

Auto' is to set the time synchronization automatically and '1. Manual' is to set manually.

Press [ENT] button to continue setting.

3.5.6.2. Calendar

◆ At default screen [F3~] → [3.Option] → [6.Time Setting] → [ENT] ◆



```
<Calendar>
0.Gregorian
1.Persian
[←] [↑] [↓] [→]
```

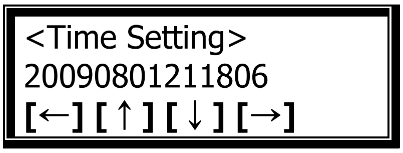
기본설정: '0.Gregorian'

This menu is to set up the terminal calendar. If it is set to '1.Persian' , Persian calendar is displayed on the LCD screen.

Press [ENT] button to continue setting.

3.5.6.3. Current Time Setting

◆ At default screen [F3~] → [3.Option] → [6.Time Setting] → [ENT]] → [ENT] ◆



```
<Time Setting>
20090801211806
[←] [↑] [↓] [→]
```

The current time of the terminal is displayed and the time in the above example shows 2009:year, 08:month, 01:day, 21:hour, 18:minute, 06:second. To make time change, move to a desired position by pressing **[←][→]** button and increase/decrease the value by pressing **[↑][↓]** button.

If [F4] button is pressed down for a longer period of time, the current time of the terminal is changed and the system moves to the upper menu. To cancel the input, press down [F1] button for a longer period of time to leave from the current menu.

3.5.7. RS485 ID Set(Setting)

◆ In basic window, [F3~] → [3.Option] → [7.RS485 ID Set] → [ENT]

It is the menu setting RS485 ID to connect with MCP040.

```
RS485 ID Set
0 1 2 3 4 5 6 7
[ESC][↑][↓][ENT]
```

After selecting ID value by clicking [↑][↓] button, click [ENT] button.

3.6. Terminal Information Inquiry

◆ At default screen [F3~] → [4.Terminal Info] ◆

If "4.Terminal Info" is selected at the main menu, the following screen is displayed. All environment setting values can be checked in order.

```
T-ID=0001
Ver=10.50.00
Application=Access
Language=ENG
Verify Mode=SN
Network Type=Static
[ESC][↑][↓]
```

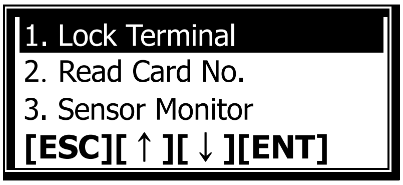
The setting values in the following table can be checked in order by scrolling up and down using [↑][↓] key.

T-ID	Terminal ID
Ver	Firmware version of terminal
Application	Terminal operation mode (time & attendance + crime prevention/time & attendance/meal service)
Language	Language setting
Verify Mode	Authentication priority
Network Type	Network type distinction (static IP/dynamic IP)
Mac-Address	Ethernet hardware address of terminal
IP Address	IP address of terminal
Gateway	Gateway address of terminal
Subnet Mask	Subnet mask address of terminal
Server IP	IP address of network server connected to terminal
Svr-Port	Port number of network server program
Card Reader	Card reader type (RF|SC|Wiegand or SmartCard)
CDR Version	Card reader module firmware version
Card Format	Card data display type
1:1 Level	Authentication level used in 1:1 authentication

1:N Level	Authentication level used in 1:N authentication
All Admin	The number of administrators registered in a terminal
All User	The total number of users including administrators registered in a terminal
Max User	The maximum number of users allowed for registration in a terminal (100)
1:N User	The total number of users allowed for 1:N authentication
1:N FP	The total number of fingerprints allowed for 1:N authentication
MAX 1:N FP	The maximum number of fingerprints allowed for registration in a terminal (100) In case there are 50 registered users and each of them registered 2 fingerprints, the total number of registered fingerprints is 100.
All FP	The total number of fingerprints saved in a terminal
MAX FP	The maximum number of fingerprints allowed for registration in a terminal (100)
The Number of Authentication Records	The number of authentication results saved in a terminal
The Maximum Number of Authentication Records	The maximum number of authentication results that can be saved in a terminal (5,119)

3.7. Extra Function

If "5.Ext Function" is selected in the main menu, the following screen is displayed.

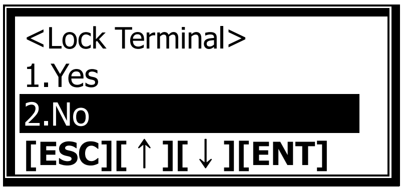


1. Lock Terminal
2. Read Card No.
3. Sensor Monitor
[ESC][↑][↓][ENT]

After selecting a menu to change by pressing [↑][↓] key, press [ENT] button.

3.7.1. Terminal Lock Setting

◆ At default screen [F3~] → [5. Ext Function] → [1. Lock Terminal] ◆

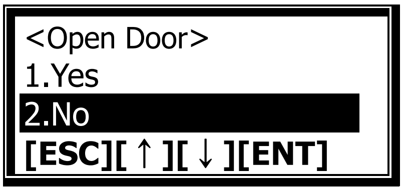


<Lock Terminal>
1.Yes
2.No
[ESC][↑][↓][ENT]

Default setting '1': Terminal lock set
'2': Terminal lock cancel

This function allows the administrator to set or cancel the terminal's locking from the terminal rather than by the server program. If it is set to '1', locking state is set in and no one can access the door until the administrator cancels the setting.

▶ In case terminal locking time is set in the server, the following menu is displayed to allow the administrator to open the door temporarily.



```
<Open Door>
1.Yes
2.No
[ESC][↑][↓][ENT]
```

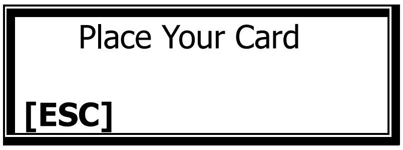
If '1.Yes' is selected, the door opens.

※ To use this function, **"Allow administrator access" item must be checked** in the terminal option of the server program.

After selecting a setting value, press [ENT] button to move to the upper menu.

3.7.2. Card Number Inquiry

◆ At default screen [F3~] → [5. Ext Function] → [2.Read Card No.] ◆



```
    Place Your Card

[ESC]
```

This is an additional function that is not related to the environment setting of the terminal. A terminal with card reader can read a card number to allow card registration at the server. If a card is placed while this screen is displayed, the card number is displayed on the LCD screen.

Press [ESC] button to leave from the card reading menu and move to the upper menu.

3.7.3. Sensor Monitor Input Port Setting

3.7.3.1. Sensor Monitor 1 Input Port Setting

This function sends an alarm message to the server by detecting fire or heat through the detection sensors connected to the input port of the terminal.

◆ At default screen [F3~] → [5. Ext Function] → [3.Sensor Monitor] ◆

```
<Sensor Monitor1>
0.None
1.Normal Open
2.Normal Close
[ESC][↑][↓][ENT]
```

Default setting '0': Port state is not checked.
'1': If port state becomes 1, state information is sent to the server.
'2': If port state becomes 0, state information is sent to the server.

If it is set to '1' or '2', state information is sent to the server when the state value of Door_Monitor_0 port is changed. In such a case, the pre-set pop-up message saved in the server is displayed.
The sensor monitor1 port uses the same port as the door monitor pin. Therefore, if Menu→3.Option→3.Set Doorlock→<Door Monitor> is set to '1' or '2', this port is set to '0.None' under any conditions.

If <Sensor Monitor1> is set to '1' or '2', the menu to select port state transmission option is displayed. Port state information can be sent to the server only once when the port state becomes "On" or whenever the port state is changed.

```
<Send On/Off?>
1.Yes
2.No
[ESC][↑][↓][ENT]
```

If it is set to default setting '2.No', port state information is sent only when the port state becomes "On".
If it is set to '1.Yes', port state information is sent to the server whenever the port state is changed.

Press [ENT] button to continue setting.

3.7.3.2. Sensor Monitor 2 Input Port Setting

Set up when Door_Monitor_1 port is connected to a sensor of fire detection or emergency detection.

```
<Sensor Monitor1>
0.None
1.Normal Open
2.Normal Close
3.Fire NO
[ESC][↑][↓][ENT]
```

Default '0': It doesn't check port status.

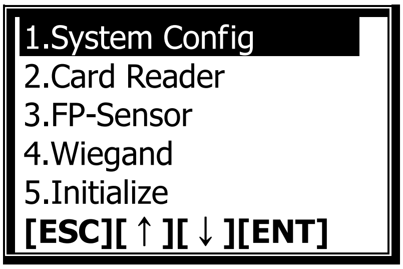
- '0.None': If nothing is connected
- '1. Normal Open' or '2. Normal Close': If sensor defined in sever is connected
- '3.Fire NO' or '4.Fire NC': If fire detection sensor is connected
- '5.Panic NO' or '6.Panic NC': If panic situation detection sensor is connected

- '7.Emergency NO' or '8.Emergency NC': If emergency detection sensor
  is connected
- '9.ControllerOut': When sending the result to the controller
  → Set up NO/NC as per status of input pin when detecting.

If fire detection (3 or 4) is set, connected gate will be open and the alarm will go off while detecting fire sensor.
After selecting setting value, press [ENT] button to move to the upper menu.

3.8. Device Setting

If "6.Device" is selected at the main menu, the following screen is displayed.



1.System Config
2.Card Reader
3.FP-Sensor
4.Wiegand
5.Initialize
[ESC][↑][↓][ENT]

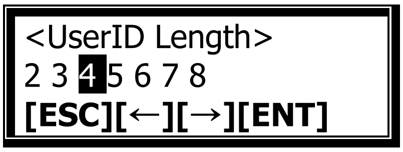
After selecting a menu to change by pressing [↑][↓] key, press [ENT] button.

In most cases, device settings do not require change after installation. Therefore, it is recommended not to change them during operation without any particular reason for doing so.

3.8.1. System Configuration

3.8.1.1. User ID Digit Setting

◆ At default screen [F3~] → [6.Device] → [1.System Config] ◆



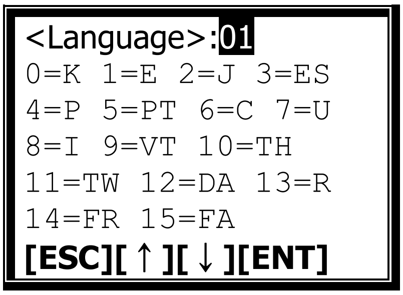
<UserID Length>
2 3 4 5 6 7 8
[ESC][←][→][ENT]

Default setting: '4'

This option sets the length of user ID. A user ID consisting of 2~8 digits is allowed and it must be of identical length to the one registered in the server program. If a 6-digit ID '000075' is registered in the server program, this item is set to 6.

After selecting a setting value, press [ENT] button to move to the upper menu.

3.8.1.2. Language Setting



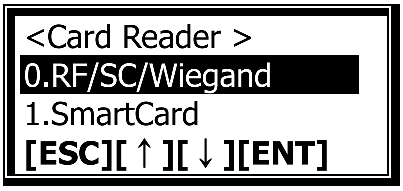
<Language>:01
0=K 1=E 2=J 3=ES
4=P 5=PT 6=C 7=U
8=I 9=VT 10=TH
11=TW 12=DA 13=R
14=FR 15=FA
[ESC][↑][↓][ENT]

Default setting: '1=EN'
0=Korean, 1= English, 2=Japanese,
3=Spanish, 4=Polish, 5=Portuguese,
6=Chinese, 7=Arabic, 8=Italian,
9=Vietnamese,10=Thai,11=Taiwanese,
12=Danish,13=Russian,14=French, 15=Farsi

If the language setting is changed, messages displayed on the screen are expressed using the changed language.

3.8.2. Card Reader Setting

◆ At default screen [F3~] → [6.Device] → [2.Card Reader] ◆

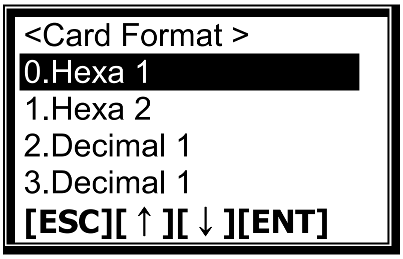


<Card Reader >
0.RF/SC/Wiegand
1.SmartCard
[ESC][↑][↓][ENT]

Default setting: '0'

This option selects a card reader type. It is set to the default value '0' in case of a low frequency card or when reading the serial number of smart card. It is set to '1' in case of reading data from a specific block of smart card. The server sets the detailed card format.

▶ If the card reader type is set to '0', the card number display type can be changed by selecting <Card Format>.



<Card Format >
0.Hexa 1
1.Hexa 2
2.Decimal 1
3.Decimal 1
[ESC][↑][↓][ENT]

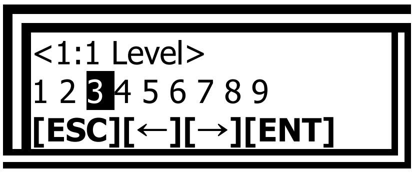
Default setting: '0'

This menu designates a type for displaying a card number that was read. Hexa setting displays using hexadecimal numbers while Decimal setting displays using decimal numbers.

3.8.3. Fingerprint Sensor Setting

3.8.3.1. 1:1 Level Setting

◆ At default screen [F3~] → [6.Device] → [3.FP Sensor] ◆


<1:1 Level>
1 2 3 4 5 6 7 8 9
[ESC][←][→][ENT]

Default setting: '3'

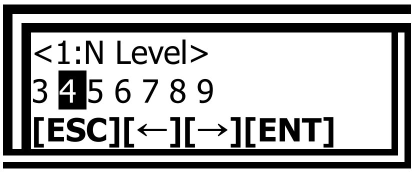
When comparing the users' fingerprints saved in the terminal database with the fingerprint in the fingerprint input window, this function sets the level of correspondence that can be considered as the identical fingerprint. A higher authentication level provides a higher security level. However, a higher security level may lead to a higher authentication denial rate.

In case of 1:1 authentication level, this function is used to locate the fingerprint registered with ID '1234' from the terminal database and compare it with the fingerprint entered in the fingerprint input window if the ID entered with authentication level used in case authentication and processed along with ID input is '1234'.

However, in case of 1:1 authentication, user's authentication level is followed if user's 1:1 authentication level was not set to '0' (terminal's authentication level used).

Press [ENT] button to continue setting.

3.8.3.2. 1:N Level Setting


<1:N Level>
3 4 5 6 7 8 9
[ESC][←][→][ENT]

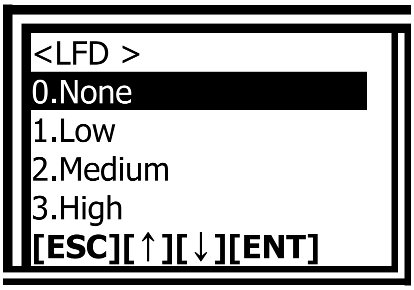
Default setting: '4'

This is the menu that sets the authentication level in case of using only fingerprint input without ID input.
This function is used to locate the corresponding fingerprint by comparing the fingerprint entered in the fingerprint input window with the fingerprints saved in the terminal database.

In case of 1:N authentication level, setting authentication level for each user is not allowed and terminal's authentication level is used as basis.

Press [ENT] button to continue setting.

3.8.3.3. LFD Setting



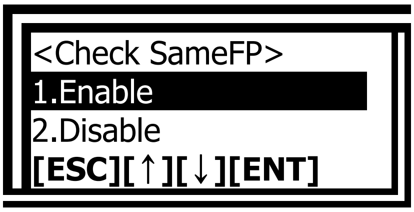
<LFD >
0.None
1.Low
2.Medium
3.High
[ESC][↑][↓][ENT]

Default setting: '0.None'

This menu sets the LFD level that can prevent the input of imitation fingerprints. A higher LFD level strengthens the function for preventing the input of imitation fingerprints made using materials such as rubber, paper, film and silicone. However, a higher LFD level may also prevent the input of real fingerprints if they are too dry.

After selecting a setting value, press [ENT] button to continue setting.

3.8.3.4. Similar Fingerprint Registration Restriction Setting



<Check SameFP>
1.Enable
2.Disable
[ESC][↑][↓][ENT]

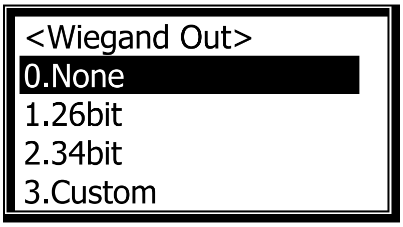
Default setting: '1.Enable'

If this menu is set to '1.Enable', a checking is performed during the registration process to determine whether a new fingerprint is already registered. This prevents the same fingerprint from being registered again as a new user ID.

After selecting a setting value, press [ENT] button to continue setting.

3.8.4. Wiegand Output Setting

◆ At default screen [F3~] → [6.Device] → [4.Wiegand] ◆



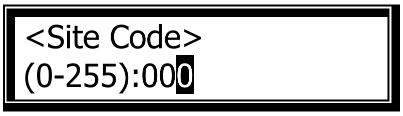
<Wiegand Out>
0.None
1.26bit
2.34bit
3.Custom

Default setting: '0'

This function is used only in case that an additional controller operated by Wiegand input is installed. After authentication is completed, the data in the following types are sent to the Wiegand port of the terminal.

0.None	This is a general case and Wiegand out port is not used.
1.26bit	As "Sitecode[1byte] + User ID[2bytes]" is sent, the user ID is set using less than 4 digits. Transmission example) For SiteCode:045, UID:6543 → 1 00101101 0001 1001 10001111 0
2.34bit	As "Sitecode[1byte] + User ID[3bytes]" is sent, the user ID is set using less than 7 digits. However, if the user ID consists of 8 digits, Sitecode is ignored and only "User ID[4bytes] is sent. Transmission example) SiteCode:001, UID:123456 → 0 00000001 00000001 11100010 01000000 0
3.Custom	As a setting made through user definition, this setting can be set only at the server. You can only check it at the terminal.

※ It has nothing to do with the use of a Wiegand type card reader. If it is set to '1' or '2', the following site code value is set.



```
<Site Code>
(0-255):000
```

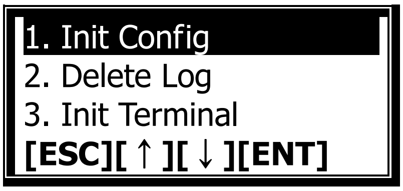
Default setting: '000'

This option can be used when the above Wiegand out is set to '1' or '2'. Enter a designated value between 0~255 in a site code to send to the Wiegand port along with a user ID.

After entering a setting value, press down [F4] button for a longer period of time to move to the upper menu.

3.8.5. Terminal Initialization

If [5.Initialize] is selected after selecting "6.Device" at the main menu, the following selection menu is displayed.

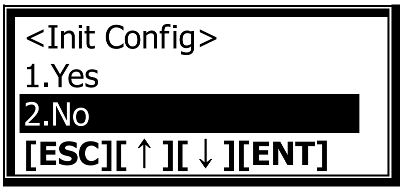


```
1. Init Config
2. Delete Log
3. Init Terminal
[ESC][↑][↓][ENT]
```

Select [1] to initialize setting values,
[2] to initialize authentication records,
and [3] for factory reset.

3.8.5.1. Setting Value Initialization

◆ At default screen [F3~] → [6.Device] → [5.Initialize] → [1.Init Config] ◆



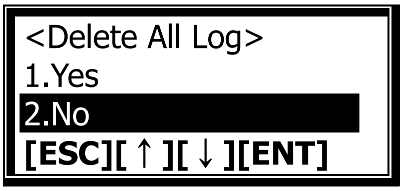
Select [1] to initialize,
and [2] to cancel.

All terminal’s setting values except MAC (physical) address are initialized but the users and authentication records are not deleted.

If initialization is completed successfully, “ppiririck” buzzer sound is heard and the system moves to the upper menu.

3.8.5.2. Authentication Record Initialization

◆ At default screen [F3~] → [6.Device] → [5.Initialize] → [2. Delete Log] ◆

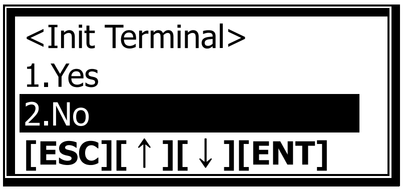


Select [1] to initialize,
and [2] cancel.

All authentication-related logs are deleted but the setting values and users are not deleted.
If initialization is completed successfully, “ppiririck” buzzer sound is heard and the system moves to the upper menu.

3.8.5.3. Factory Reset

◆ At default screen [F3~] → [6.Device] → [5.Initialize] → [3. Init Terminal] ◆

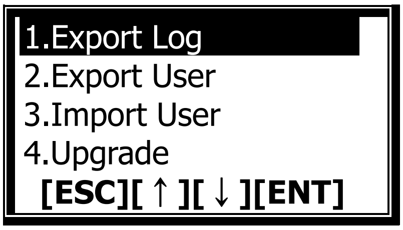


Select [1] to initialize,
and [2] to cancel.

All data are deleted and the terminal enters into a factory reset state.
If initialization is completed successfully, the buzzer sound for success is heard and the terminal is rebooted.

3.8.5.4. UDL (USB Data Loger) Backup

◆ On the basic screen, [F3~] → [6.Device] → [5.Initialize] → [4.DB Backup] ◆
- If USB memory card is inserted, it enters lower menu, and if USB is not inserted, 'Not detected Memory' of warning message will be shown.



1.Export Log
2.Export User
3.Import User
4.Upgrade
[ESC][↑][↓][ENT]

DB Backup Menu

✓ Export Log
  - This menu is for exporting saved log data on AC2100 to USB.
  - Location of data is USB Top Folder -> AC2100 Folder -> 00000000 (8 digits of terminal ID) Folder -> Saved as a file name of LOG.DAT on LOG Folder

✓ Export User
  - This menu is for exporting saved user data on AC 2100 to USB.
  - Location of data is USB Top Folder -> Saved as a file name of USER.DAT on AC2100
  - Numbers of exported users will be shown on the bottom of the screen.

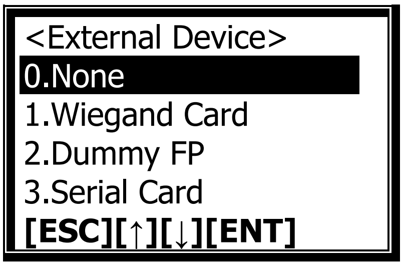
✓ Import User
  - This menu is for importing saved user data (USER.DAT) on USB to a terminal.
  - The user file (USER.DAT) to be imported should be saved as a file name of USER.DAT on AC 2100 folder.
  - Imported data size will be shown on the bottom of the screen.

✓ Upgrade (Firmware upgrade)
  - This menu is for upgrading terminal's firmware by using saved firmware data (ac21w.bin) on USB.
  - The related firmware file is 'ac21w.bin' and it should be saved as a file name of ac21w.bin on AC2100 Folder in order to upgrade.
  - Imported data size will be shown on the bottom of the screen.

(Caution)
If USB memory is removed, or terminal is turned off during upgrading, it might cause abnormal operation of the product.

3.8.6. External Device Setting

◆ On the basic screen [F3~] → [6.Device] → [6.External Device] ◆

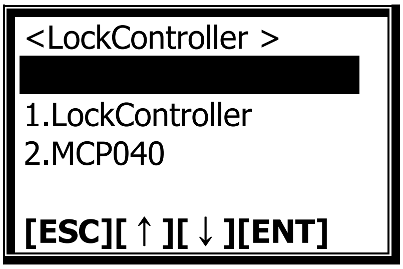


<External Device>
0.None
1.Wiegand Card
2.Dummy FP
3.Serial Card
[ESC][↑][↓][ENT]

Default: '0.None'

It is set when using the slave reader which uses the card or fingerprint to the terminal as the supplementary authorization device. It is set '1' when connecting Wiegand card reader. And it is set '2' when connecting SR100. And it is set '3' when using the card number sending function of RS232.

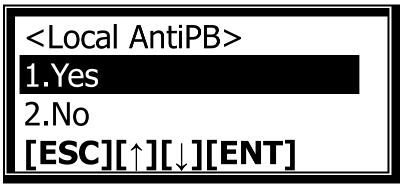
Click [ENT] button for the next setting.



<LockController >
1.LockController
2.MCP040
[ESC][↑][↓][ENT]

Basic setting: '0.None'

It only appears when the <External device> is set '0'.
Set '1.LockController' when connecting external device LC010. Set '2.MCP040' when connecting MCP040. Be sure to set RS484 ID when connecting MCP040.



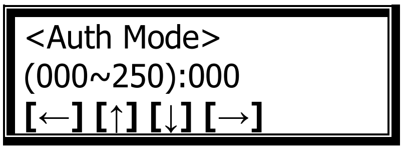
<Local AntiPB>
1.Yes
2.No
[ESC][↑][↓][ENT]

Default: '2.No'
If it is set as '1.Yes',
Anti-Passback will be checked in a terminal.

It appears only if <External Device> is set as '1' or '2'.
It is used if a terminal and a slave reader are installed on both inside and outside of a gate, and set up as letting only those users who have clocked in by the terminal clock out by the slave reader.

If it is set as '1.Yes', server authentication is not possible to use. It will check if valid passback or not by authentication order between the terminal and the slave reader.

Press [ENT] button to do the next setting.



```
<Auth Mode>
(000~250):000
[←] [↑] [↓] [→]
```

Default: '0'
Slave

If it is authenticated on slave reader, authentication (T&A) mode to be saved will be set up.
If 0 is set, it will be saved as current authentication mode of a terminal.
If '1', it will be saved as F1, if '2', it will be saved as F2, if '3', it will be saved as Access, if '4', it will be saved as F3, and if '5', it will be saved as F4.

4. How to Use Terminal

4.1. In Case of Operating as [0.Access Ctrl]

- Set as Menu → 3.Option → 1. Application → [0.Access Ctrl]

4.1.1. Authentication Mode

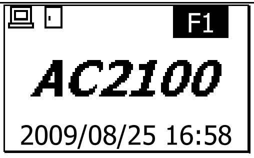
- Authentication is done after changing to a desired authentication mode such as F1, F2, F3 and F4 by pressing the function keys. In case of authenticating without pressing any function key, authentication with access mode is done automatically.

- Authentication method
  F1 authentication: Authentication is done after changing to F1 mode by pressing [F1] key.
  For hours set as office start time, authentication is done without mode change.
  F2 authentication: Authentication is done after changing to F2 mode by pressing [F2] key.
  For hours set as office leave time, authentication is done without mode change.
  F3 authentication: Authentication is done after changing to F3 mode by pressing [F3] key.
  F4 authentication: Authentication is done after changing to F4 mode by pressing [F4] key.
  Access authentication: Authentication is done after changing to access mode by pressing [F4] key or authentication is done without mode change for hours not set as office start/leave

time.

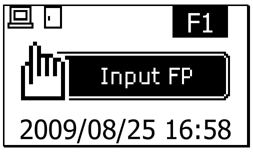
4.1.2. Authentication Using Fingerprint

▶ After changing the authentication mode by pressing a function key, place the finger on the fingerprint sensor. Afterwards, the fingerprint is entered and the authentication is displayed on the LCD screen along with a voice message.


F1
AC2100
2009/08/25 16:58

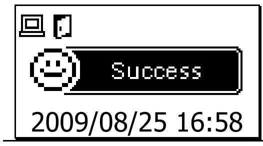
Change authentication mode to 'F1' by pressing [F1] key in the alert state.

▼


F1
Input FP
2009/08/25 16:58

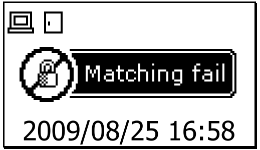
When you place the finger on the fingerprint sensor, the fingerprint input window is lighted in red along with ppik" sound. Leave the finger until the light is switched off.

▼

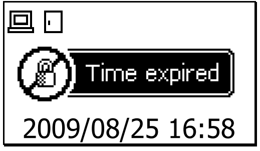

Success
2009/08/25 16:58

Upon authentication success, the voice message "You are authorized" is heard and the success message is displayed on the LCD screen.

※ Error message: The following message along with the voice message "Try it again" is displayed.


Matching fail
2009/08/25 16:58

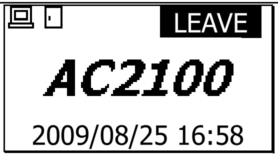
In case of authentication failure


Time expired
2009/08/25 16:58

In case of trying to authenticate during a time not allowed for access even though the registration is valid

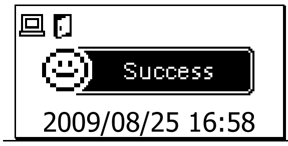
4.1.3. Authentication Using Card

▶ If a user registered with [Card] or [Card or FP] places the card on the default screen, "ppik" sound is heard and authentication result is displayed on the LCD screen.


LEAVE
AC2100
2009/08/25 16:58

Change authentication mode to office leave mode by pressing [F2] key.

▼

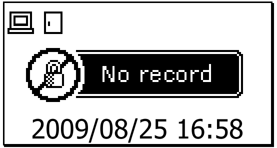


Success

2009/08/25 16:58

Upon authentication success, the voice message “You are Authorized” is heard and the authentication success message is displayed on the LCD screen.

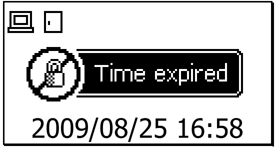
※ Error message: The following message along with the voice message “Please try again” is displayed.



No record

2009/08/25 16:58

In case entering an unregistered card

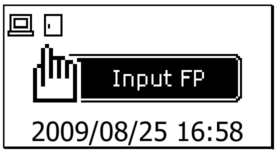


Time expired

2009/08/25 16:58

In case of trying to authenticate during a time not allowed for access even though the registration is valid

▶ If a user registered with [Card and FP] places the card on the default screen, “ppik” sound is heard and the following additional fingerprint input procedure is required for authentication.



Input FP

2009/08/25 16:58

The fingerprint input window is lighted along with the voice message “Please enter your fingerprint”. Enter fingerprint and leave it until “ppik” sound is heard.

4.2. In Case of Operating as [1.T&A Ctrl]

- Set as Menu → 3.Option → 1. Application → [1.T&A Ctrl]

- In case office start/leave time is fixed, setting of <Start Time> and <Leave Time> enables authentication as start office during start office hour and as leave office during office leave hour without pressing [F1] or [F2] key. Being as such, it reduces the input error regarding the user’s time & attendance.

4.2.1. Authentication Mode

- Authentication is done with each of the authentication modes after changing to start office, leave office, work outside, return to office and access modes by pressing the function keys.

- Authentication method

Start office authentication: Authentication is done after changing to start office mode by pressing [F1] key.
Authentication is done without mode change during hours set as start office time.

Leave office authentication: Authentication is done after changing to leave office mode by pressing [F2] key.
Authentication is done without mode change during hours set as leave office time.

Work outside authentication: Authentication is done after changing to work outside mode by pressing [F3] key.

Return to office authentication: Authentication is done after changing to return to office mode by pressing [F4] key.

Access authentication: Authentication is done after changing to access mode by pressing [F4] key or authentication is done without mode change for hours not set as office start/leave time.

4.2.2. Fingerprint Authentication

- Change time & attendance mode by pressing the function keys.
- Enter fingerprint.

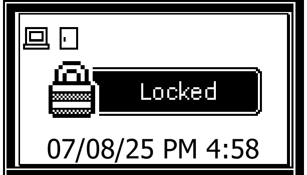
4.2.3. Authentication Using Card

- Change time & attendance mode by pressing the function keys.
- Place card.

4.3. In Case of Operating as [2.Meal Ctrl]

- Set as Menu → 3.Option → 1. Application setting → [2.Meal Ctrl]
- If set as meal service management, the terminal enters into a lock state except during meal service time. Therefore, at least one meal service time must be entered.

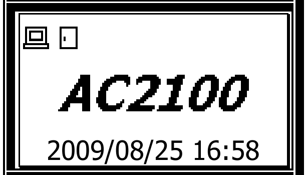
- Display Screen



Locked

07/08/25 PM 4:58

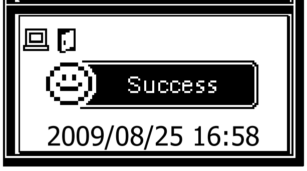
In case it is not meal service time (Authentication attempt not allowed)



AC2100

2009/08/25 16:58

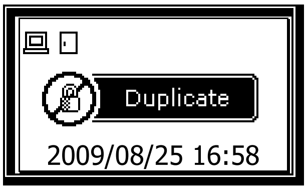
Default screen during meal service time



Success

2009/08/25 16:58

In case of authentication success



Duplicate

2009/08/25 16:58

If setting does not allow duplicated authentication, duplicated authentication trial error is displayed for the authentication attempt after a successful authentication

- In case of fingerprint authentication
  Authentication is done by entering a fingerprint.

- In case of card authentication
  Authentication is done by placing a card.

- In case of attempting authentication without pressing the menu selection key, authentication is done automatically with [Menu 1].