# VIRDI 4000 User Guide

Version eng-1.06

UNION COMMUNITY

# < Glossary>

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

- 1 to 1 Verification
  - A user's fingerprint is compared to the user's fingerprint in his ID or card.
  - It is called 1 to 1 Verification because only the fingerprint registered in the user's ID or card is used for comparison.

- 1 to N Identification
  - Many stored fingerprints are used for comparison.
  - Without the user's ID or card, the user's fingerprint is compared to fingerprints previously registered

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

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

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

- Function keys

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

# Table of Contents

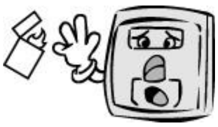
**< Glossary>........................................ 2**
**Table of Contents ........................................ 3**
**1. Before use........................................ 5**
**1.1. Safety precautions ........................................ 5**
**1.2. Terminal description ........................................ 6**
**1.4. Screen (during operation) description ........................................ 7**
**1.5. Voice information during operation........................................ 8**
**1.6. Buzzer sound during operation ........................................ 8**
**1.7. LED signal during operation ........................................ 8**
**1.8. Correct fingerprint registration and input methods........................................ 9**
**2. Introduction ........................................ 11**
**2.1. Features ........................................ 11**
**2.2. Configuration........................................ 13**
2.2.1. Network configuration........................................ 13
2.2.2. Standalone configuration........................................ 13
**2.3. Specifications........................................ 14**
**3. Environment settings........................................ 15**
**3.1. Check items before setting the environment........................................ 15**
3.1.1. Entering menu ........................................ 15
3.1.2. Change settings ........................................ 15
3.1.3. Save environment settings ........................................ 16
**3.2. Menu configuration ........................................ 17**
**3.3. User account........................................ 20**
3.3.1. User registration........................................ 20
3.3.2. Delete User ........................................ 25
3.3.3. Modify User ........................................ 25
3.3.4. Administrator registration........................................ 29
3.3.5. Delete all users........................................ 29
**3.4. Network settings ........................................ 30**
3.4.1. Terminal ID settings........................................ 30
3.4.2. Connection [NS / SN / NO] mode settings........................................ 30
3.4.3. Connection method settings........................................ 31
3.4.4. IP address settings........................................ 31
3.4.5. Subnet mask settings ........................................ 31
3.4.6. Gateway settings........................................ 32
3.4.7. Server IP settings ........................................ 32
3.4.8. Server port settings ........................................ 32
**3.5. Option settings........................................ 33**
3.5.1. Application mode settings........................................ 33
3.5.2. Authentication method settings........................................ 35
3.5.3. Door settings ........................................ 37
3.5.4. Volume settings........................................ 39
3.5.5. Current time settings ........................................ 40
3.5.6. Other setting........................................ 40
**3.6. Terminal information view ........................................ 41**
**3.7. Extended functions........................................ 42**

3.7.1. Terminal lock settings .......... 42
3.7.2. Read card number .......... 42
**3.8. Device settings .......... 43**
3.8.1. Function key settings .......... 43
3.8.2. Card reader settings .......... 43
3.8.3. Fingerprint sensor settings .......... 44
3.8.4. Wiegand output settings .......... 45
3.8.5. System configuration settings .......... 46
3.8.6. Terminal initialization .......... 47
**4. How to use the terminal .......... 48**
**4.1. Access control .......... 48**
4.1.1. Authentication mode .......... 49
4.1.2. [1:1] fingerprint authentication .......... 49
4.1.3. [1:N] fingerprint authentication .......... 51
4.1.4. Password authentication .......... 52
4.1.5. Card authentication .......... 53
4.1.6. User ID group authentication .......... 54
4.1.7. Multiple fingerprint authentication .......... 55
**4.2. Time attendance control .......... 55**
4.2.1. Authentication mode .......... 56
4.2.2. [1:1] fingerprint authentication .......... 56
4.2.3. [1:N] fingerprint authentication .......... 56
4.2.4. Password authentication .......... 57
4.2.5. Card authentication .......... 57
4.2.6. User ID group authentication .......... 57
4.2.7. Working mode expansion using multi-key authentication .......... 57
**4.3. For meal management ..........** 오류! 책갈피가 정의되어 있지 않습니다.
4.3.1. Melal Type .......... **오류! 책갈피가 정의되어 있지 않습니다.**
4.3.2. [1:1] Fingerprint Authentication**오류! 책갈피가 정의되어 있지 않습니다.**
4.3.3. [1:N] Fingerprint Authentication**오류! 책갈피가 정의되어 있지 않습니다.**
4.3.4. Password Authentication .......... 59
4.3.5. Authentication with card .......... 59
4.3.6. Group Authenciation using User ID .......... 59
4.3.7. Duplicate Authentication Enable**오류! 책갈피가 정의되어 있지 않습니다.**

# 1. Before use

## 1.1. Safety precautions

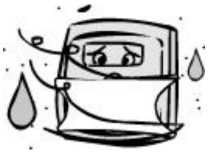
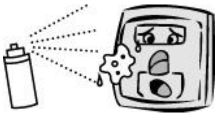
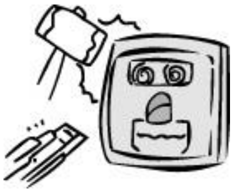
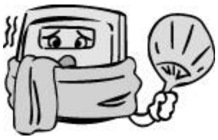
- Warning

| | | | |
|---|---|---|---|
| Handling with wet hands or allowing liquid to flow into it is not advised.<br>-> It may cause an electric shock or damage. | | Do not place a fire source near the unit.<br>-> It may cause a fire. |  |
| Do not disassemble, repair, or modify the unit.<br>-> It may cause an electric shock, fire or damage. | | Keep out of reach of children.<br>-> It may cause an accident or damage. | |

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

-

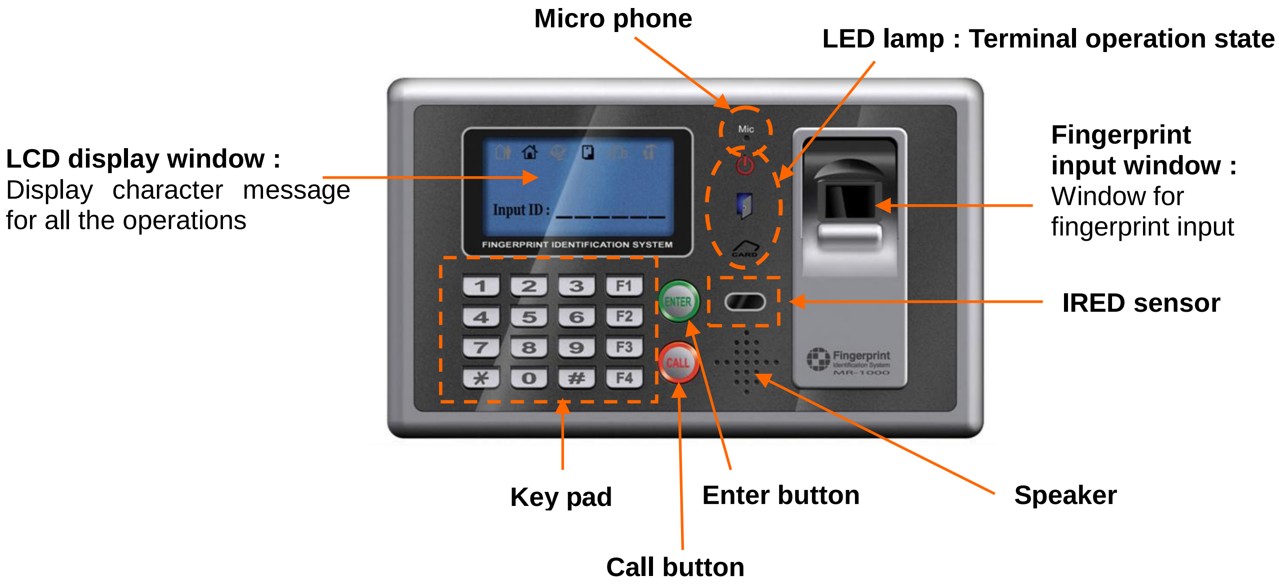
- Cautions

| | | | |
|---|---|---|---|
| Keep away from direct sunlight<br>-> It may cause deformation or color change. | | Avoid high humidity or dust ->The unit may be damaged. |  |
| Avoid using water, benzene, thinner, or alcohol for cleaning<br>-> It may cause an electric shock or fire. | | Do not place a magnet close to the unit.<br>-> The unit may break down or malfunction. | |
| Do not contaminate the fingerprint input area.<br>-> Fingerprints may not be well recognized. | | Avoid using insecticides or flammable sprays near the unit.<br>-> It may result in deformation or color change. |  |
| Avoid impacts or using sharp objects on the unit.<br>-> The unit may be damaged and broken. |  | Avoid severe temperature changes<br>-> The unit may be broken. |  |

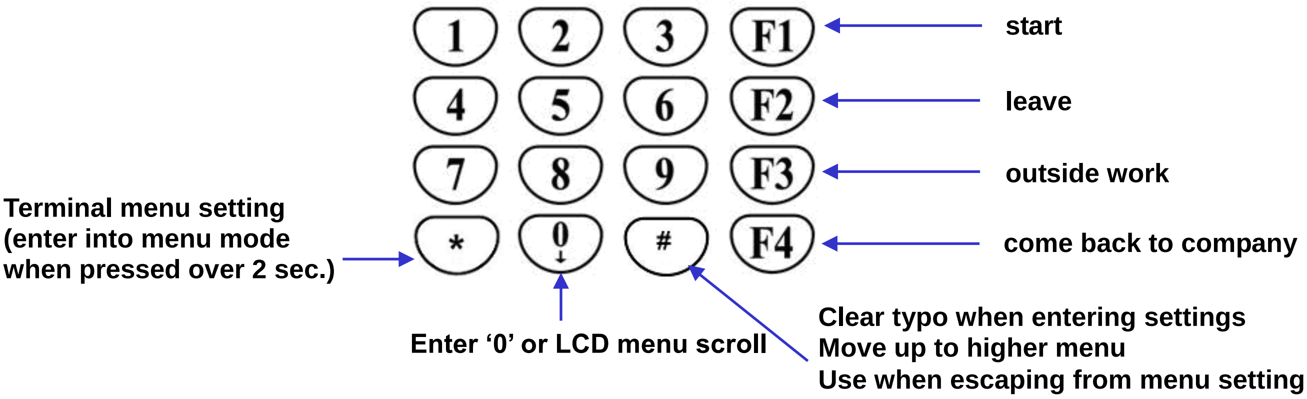
- If the above cautions are ignored, it may result in property loss or human injury.

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

## 1.2. Terminal description


Micro phone
LED lamp : Terminal operation state
LCD display window : Display character message for all the operations
Fingerprint input window : Window for fingerprint input
IRED sensor
Key pad
Enter button
Speaker
Call button
Mic
Input ID : ______
FINGERPRINT IDENTIFICATION SYSTEM
1 2 3 F1 4 5 6 F2 7 8 9 F3 * 0 # F4
ENTER
CALL
CARD
Fingerprint Identification System MR-T000

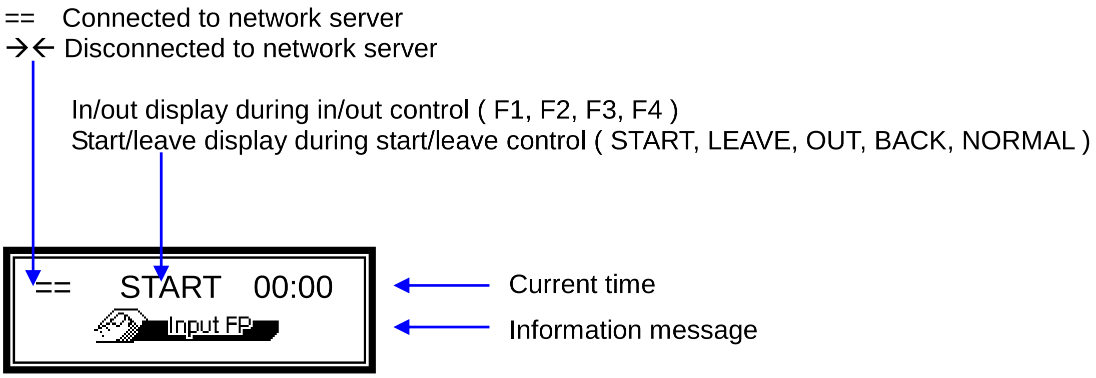
### Button description


1 2 3 F1
4 5 6 F2
7 8 9 F3
* 0 # F4
start
leave
outside work
come back to company
Terminal menu setting (enter into menu mode when pressed over 2 sec.)
Enter '0' or LCD menu scroll
Clear typo when entering settings
Move up to higher menu
Use when escaping from menu setting

Use after entering the settings when configuring the terminal environment

Visitors use this to ring the interphone bell

## 1.3. Screen (during operation) description



== Connected to network server

→← Disconnected to network server

In/out display during in/out control ( F1, F2, F3, F4 )

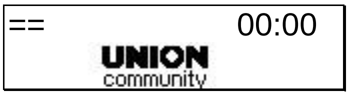
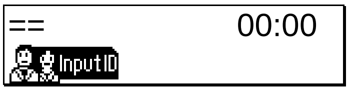
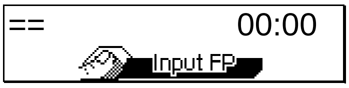
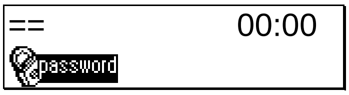
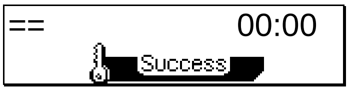
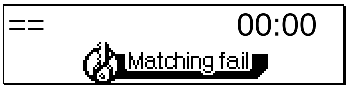
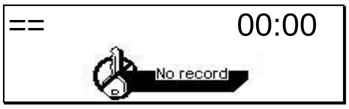
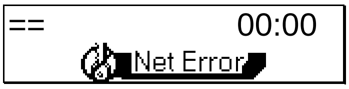
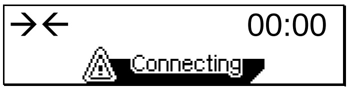
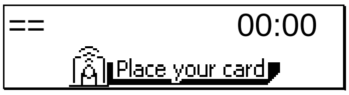
Start/leave display during start/leave control ( START, LEAVE, OUT, BACK, NORMAL )

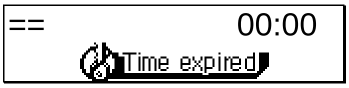
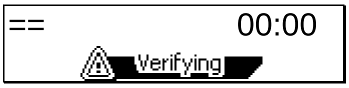
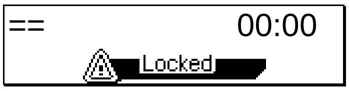
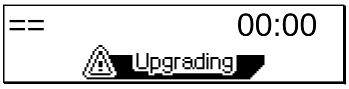
== START 00:00

Input FP

Current time

Information message

| | |
|---|---|
| <br>== 00:00<br>UNION community | - Initial screen |
| <br>== 00:00<br>Input ID | - Waiting for a user's ID to be input |
| <br>== 00:00<br>Input FP | - Fingerprint input |
| <br>== 00:00<br>password | - Password input |
| <br>== 00:00<br>Success | - Authentication successful |
| <br>== 00:00<br>Matching fail | - Authentication failed |
| <br>== 00:00<br>No record | - Entered a non-registered user ID<br>- Connection method is SN and 1:N identification is accessed even though there is no user allowed for 1:N identification |
| <br>== 00:00<br>Net Error | - There is no response from the server during the authentication process.<br>- Network to server is disconnected during the authentication process. |
| <br>→← 00:00<br>Connecting | - There is no user registered on the terminal or no connection to the server, so it is trying to connect. |
| <br>== 00:00<br>Place your card | - Waiting for card to be input |

| | |
|---|---|
|  == 00:00<br>Time expired | - A registered user tried authentication when entry/exit is not allowed. |
|  == 00:00<br>Verifying | - Waiting for a reply from the server for authentication |
|  == 00:00<br>Locked | - Terminal is locked<br>- No meal time even though the unit is set to meal control mode |
|  == 00:00<br>Upgrading | - Terminal program upgrade (Power switch should not be turned off when this message is displayed.) |

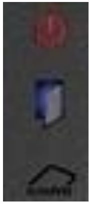
## 1.4. Voice information during operation

| | |
|---|---|
| "Please enter your fingerprint" | Enter fingerprint using the fingerprint input window |
| "You are authorized" | Authentication successful |
| "Please try again" | Authentication failed |

## 1.5. Buzzer sound during operation

| | |
|---|---|
| "ppig" | When a button is pressed or a card is being read<br>When fingerprint input is completed, allowing the user to remove his fingerprint |
| "ppibig" | Authentication failed or wrong user input |
| "ppiriririck" | Waiting for fingerprint input |
| "ppiririck" | Authentication successful or settings for the current user are completed |

## 1.6. LED signal during operation



POWER LED : Power on/off

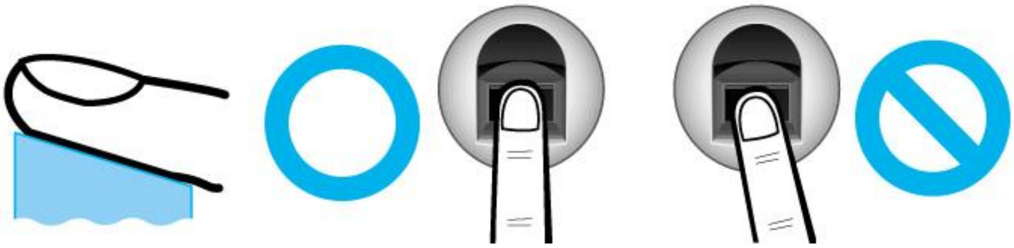
DOOR LED : Door open/close

CARD LED : Card contact

## 1.7. Correct fingerprint registration and input methods

- Correct fingerprint registration methods

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



- Use your index finger.

  The index finger guarantees an accurate and stable fingerprint input.

- Check if your fingerprint is unclear or damaged.
  It is tricky to recognize fingerprints on dry, wet, unclear, or injured fingers. Use another finger in this case.

- Cautions about fingerprint condition

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

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

# 2. Introduction

## 2.1. Features

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

- Convenient Auto Sensing function
  - Simple authentication process without any key input; simple fingerprint touching is sufficient.

- Simple authentication using fingerprints
  - Due to Biometrics fingerprint recognition technology, it is not necessary to carry a password, card, or key, etc., or to worry about robbery. This improves the level of security.

- High capacity of terminal and server
  - There is no limit on fingerprint registration for the server, and the unit itself can store up to 8,000 fingerprints.

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

- Door phone
  - Easy visitor identification and convenient response.

- Various and flexible Access controls
  - No risk of rent, forgery, or loss of keys or cards
  - Perfect control by assigning different security clearances to each user or group
  - Provides flexibility by allowing limited time for entry/exit
  - Low maintenance and development costs compared to other units
  - No need to issue a visitor card to a visitor

- Various applications including entry/exit, start/leave, meal counting, etc.
  - Various operation modes depending on the terminal menu settings

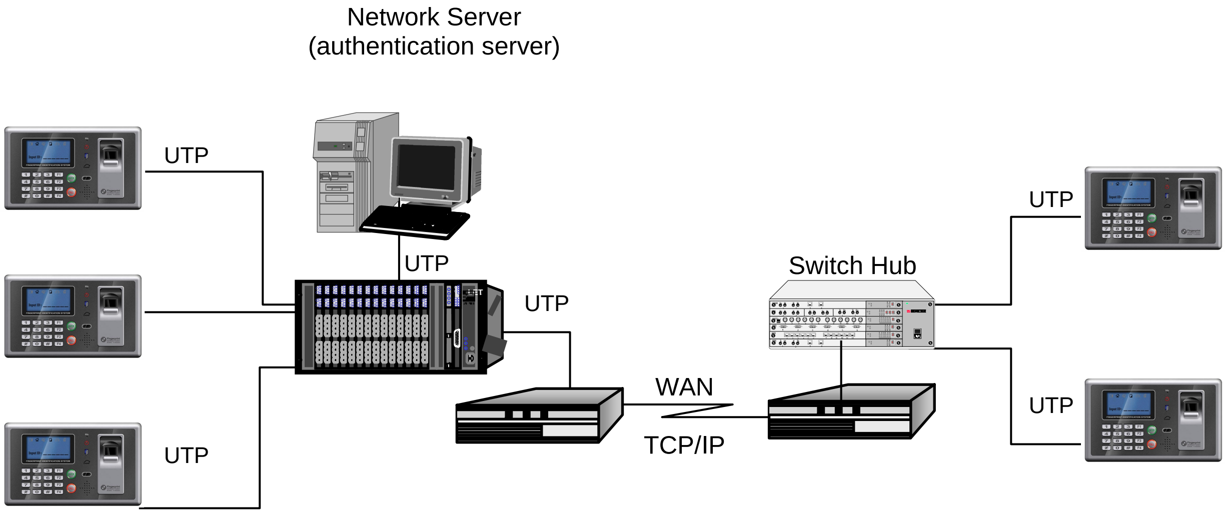
- Various registration and authentication methods
  - There are a total of 11 registration and authentication methods (4 methods

if the card reader is not installed), so you are required to select one method before registering users and an administrator.

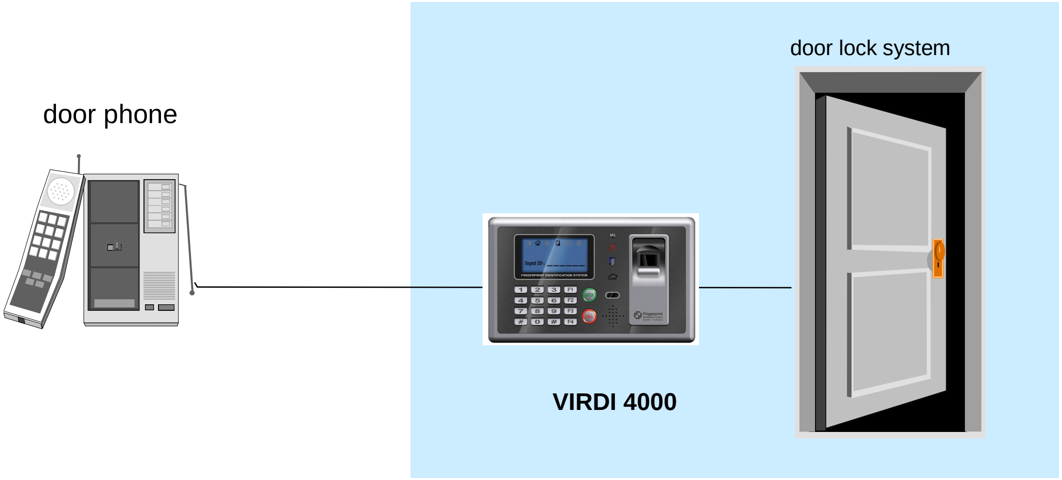
| | |
|---|---|
| FP | Fingerprint registration<br>Fingerprint authentication |
| ID&PW | Password registration<br>Password authentication |
| FP\|PW | Fingerprint and password registration<br>Fingerprint or password authentication |
| FP&PW | Fingerprint and password registration<br>Password authentication after fingerprint authentication |
| RF | Card registration<br>Card authentication |
| RF\|FP | Card and fingerprint registration<br>Card or fingerprint authentication |
| RF&FP | Card and fingerprint registration<br>Fingerprint authentication after card authentication |
| RF\|PW | Card and password registration<br>Card or password authentication |
| RF&PW | Card and password registration<br>Password authentication after card authentication |
| ID&FP\|RF&FP | Card and fingerprint registration<br>Fingerprint authentication after ID input or fingerprint authentication after card authentication |
| ID&PW\|RF&PW | Card and password registration<br>Password authentication after ID input or password authentication after card authentication |

## 2.2. Configuration

### 2.2.1. Network configuration



### 2.2.2. Standalone configuration



## 2.3. Specifications

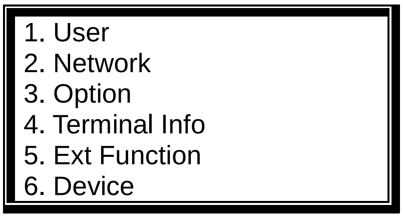
| ITEM | SPEC | REMARK |
|---|---|---|
| CPU | 32Bit RISC CPU | |
| MEMORY | 8M SDRAM | |
| | 4M FLASH (Default) | 3,440 fingerprints |
| | 8M FLASH (Option) | 8,080 fingerprints |
| Fingerprint sensor | Optical | |
| Authentication speed | <1 sec. | |
| Scan Area / Resolution | 12.9 * 15.2mm / 500 DPI | |
| FRR / FAR | 0.1% / 0.001% | |
| Communication Port | TCP/IP, RS-232, Wiegand | |
| | RS-485 (Option) | |
| Temperature / Humidity | -10 ~ 50 /<br>Lower than 90% RH | |
| LCD | 128 X 64 Graphic LCD | |
| SIZE | 181 X 109 X 43 mm | |
| AC / DC Adapter | INPUT : Universal AC 100 ~ 250V | |
| | OUTPUT : DC 12V (Option : DC 24V) | |
| | UL, CSA, CE Approved | |
| Option | RF Card Reader | EM Card, 125kHz |
| | Smart Card Reader | A-type, 13.56MHz |
| | Door phone | |

# 3. Environment settings

## 3.1. Check items before setting the environment

### 3.1.1. Entering menu

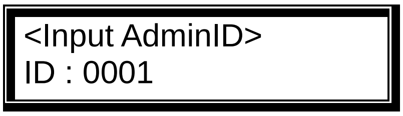
The following screen appears when [*] is pressed for over 2 sec.



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

Press [0] to view menus not shown in the LCD window.

If a number corresponding to the menu required is pressed (ex. [1] for user account), the following screen for administrator authentication appears:



<Input AdminID>
ID : 0001

Press [ENTER] after entering the administrator’s ID, and the administrator authentication is processed according to the previous setting such as fingerprint authentication or password authentication. If authentication is successful, sub-menus of the menu chosen appear

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

### 3.1.2. Change settings

To change settings, press the [#] button to delete old values and input new values.

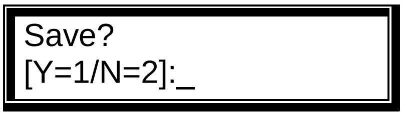
Press [0] to see menus not shown in the LCD window, and press the corresponding number to select a menu.

Press [ENTER] for settings verification or to move to the next setting.

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

### 3.1.3. Save environment settings

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



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

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

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

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

## 3.2. Menu configuration

| | | |
|---|---|---|
| 1. User | 1. Add<br>2. Delete<br>3. Modify<br>4. Add Admin<br>5. Delete All | |
| 2. Network | 1) Terminal ID<br>2) Mode [NS/SN/NO]<br>3) Network Type [Static IP/DHCP]<br>4) IP Address<br>5) Subnet Mask<br>6) Gateway<br>7) Server IP<br>8) Server port | |
| 3. Option | 1. Application [Access/Time Attendance] | <Application><br><Start Time><br><Leave Time><br><Normal Time><br><Ticket Printer><br><Multi Fn-Key> |
| | 2. Verify Option | <Show User ID><br><Auto Enter Key><br><Only Card><br><Enable 1:N ><br><User ID Group><br><NetErr TimeOut> |
| | 3. Set Doorlock | <Open Duration><br><Door Monitor><br><Door Open Alarm> |
| | 4. Sound Control | <Use Voice><br><Beeper Volume><br><Case Open Alarm> |
| | 5. Time Setting | |
| | 6. Other Setting | <LCD Backlight><br><Display Time><br><Time Setting><br><Fire Sensor> |

| | | |
|---|---|---|
| 4. Terminal Info | Terminal ID=0001<br>Version=10.41.00<br>Application=Access<br>Language=ENG<br>Mode=NS<br>Network Type= Static(1)<br>Mac-Address=000265201111<br>IP Address=192.168.0.3<br>Gateway=192.168.0.1<br>Subnet Mask=255.255.255.0<br>Server IP=192.168.0.2<br>Svr-Port==2201<br>Card Reader=None<br>FP-Sensor=FOS02<br>1:1 Level=4<br>1:N Level=5<br>Max User=0<br>MAX FP=0<br>All User=0<br>All Admin=0<br>All FP=0<br>1:N User=0<br>1:N FP=0<br>All Log=0 | |
| 5. Ext functions | 1. Lock Terminal<br>2. Read Card No. | |
| 6. Device | 1. Set Fn-Key | |
| | 2. Card Reader | |
| | 3. FP-Sensor | <1:1 Level><br><1:N Level><br><LFD><br><Similarfingerprint check> |
| | 4. Wiegand | <Wiegand Out><br><Site code><br><Bypass> |
| | 5. System Config | <ID Length><br><Language> |
| | 6. Initialize | 1. Init Config<br>2. Delete Log<br>3. Init Terminal |

| | | |
|---|---|---|
| | 7. External device | < External device ><br><Local AntiPB><br><Auth Mode> |

## 3.3. User account

### 3.3.1. User registration

Press the [1] button in the main menu to select “1.User”, and the following screen appears:

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

Press [1] to register a new user.

```
User ID [NEW]
ID : _ _ _ _
```

Enter a new user ID, and press [ENTER].

If the entered ID is not new, you will hear a “ppibig” sound and it moves to the upper menu. If not, the following authentication method selection screen appears:

```
1.FP           2.ID&PW
3.FP|PW        4.FP&PW
5.RF           6.RF|FP
7.RF&FP        8.RF|PW
91. RF&PW
92. ID&FP | RF&FP
▼
```

Press [0] to see menus not shown in the LCD window. Select one from among the 11 registration methods.

#### 3.3.1.1. “1. FP” registration

fingerprint registration and fingerprint authentication

◆ [ENTER] → [1] → [1] → User ID [ENTER] → [1] → 1:1 Level [ENTER] → Enable 1:N [ENTER] → Input FP → Input same FP ◆

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

Recommended setting: ‘0’

A different authentication level can be assigned to each different user.
If this is set to ‘0’, the identification level set for the terminal is used instead of the identification level assigned to each user. When the 1:1 verification level of the terminal is changed, all user identification levels set to ‘0’ are changed.

Press [ENTER] to move to the next setting.

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

The default is ‘1’, but it shall be set to ‘1’ to enable 1:N authentication.

If there are not many users or for the convenience of a specific user, a fingerprint alone can be used for authentication, without ID.
For authentication without ID, it shall be set to ‘1’. For authentication with ID, it shall be set to ‘0’.

Press [ENTER] to enter fingerprints.

<Add FP>
Input Your FP

You will hear a “ppiriririck” buzzer sound twice and a light on the fingerprint sensor will turn on. Place a finger onto the fingerprint input window and wait for 2~3 sec. until the light turns off and the fingerprint is saved.

To enter a second fingerprint, remove the previous finger completely from the window to improve the authentication rate.

If you hear a “ppiririck” buzzer sound, registration is successful. It returns to the “1.Add” screen. If the fingerprint image is not so good or there is no input in the window for 10 sec. after the fingerprint sensor light turned on, it returns to the “1. Add” screen with a failure buzzer sound “ppibig”.

Repeat the above procedures 2~3 times by complying with the correct fingerprint registration methods. If it eventually fails, it is recommended to use a password for authentication.

### 3.3.1.2. “2. ID&PW” registration

Password registration and password authentication for a user

◆ [ENTER] → [1] → [1] → User ID [ENTER] → [2]
→ Input PW [ENTER] → Input same PW [ENTER] ◆

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

Input password. Password should be 1~8 characters in length.

Press [ENTER] to input the password.

**<Confirm PW >**
**PW : _ _ _ _ _ _ _ _ _**

Input the same password once more for verification.

If you hear a “ppiririck” buzzer sound, registration is successful. If they are different, you will hear a “ppibig” buzzer sound indicating failure and the “1.Add” menu screen appears.

### 3.3.1.3. “3. FP|PW” registration

Fingerprint and password registration, and fingerprint or
password authentication

◆ [ENTER] → [1] → [1] → User ID [ENTER] → [3] → Input PW [ENTER]
→ Input same PW [ENTER] → 1:1 Level [ENTER] → Enable 1:N [ENTER]
→ Input FP → Input same FP ◆

After fingerprint registration (refer to ① “1. FP” registration), password registration (refer to ② “2. ID&PW” registration) follows.

If you hear a “ppiririck” buzzer sound, registration is successful. If they are different, you will hear a “ppibig” buzzer sound indicating failure and the “1. Add” menu appears.

### 3.3.1.4. “4. FP&PW” registration

Fingerprint and password registration, and fingerprint and password authentication

◆ [ENTER] → [1] → [1] → User ID [ENTER] → [4] → Input PW [ENTER]
→ Input same PW [ENTER] → 1:1 Level [ENTER] → Enable 1:N [ENTER]
→ Input FP → Input same FP ◆

After fingerprint registration (refer to ① “1.FP” registration), password registration (refer to ② “2. ID&PW” registration) follows.

### 3.3.1.5. “5. RF” registration

Card registration and card authentication

◆ [ENTER] → [1] → [1] → User ID [ENTER] → [5] → Place the card ◆

**<Add Card>**
**Place Your Card**

To cancel registration, press the [#] button.

If a user places the card close to the unit, a “ppiririck” buzzer sound (registration is successful) will be heard and the “1. Add” menu appears.

### 3.3.1.6. “6. RF|FP” registration

Card and fingerprint registration, and card or fingerprint authentication

◆ [ENTER] → [1] → [1] → User ID [ENTER] → [6] → Place the card
→ 1:1 Level [ENTER] → Enable 1:N [ENTER]
→ Input FP → Input same FP ◆

After card registration (refer to ⑤ “5. RF” registration), fingerprint registration refer to ① “1. FP” registration.) follows.

### 3.3.1.7. “7. RF&FP” registration

Card and fingerprint registration, and card and fingerprint authentication

◆ [ENTER] → [1] → [1] → User ID [ENTER] → [7] → Place the card
→ 1:1 Level [ENTER] → Input FP → Input same FP ◆

After card registration (refer to ⑤ “5. RF” registration), fingerprint registration refer to ① “1. FP” registration.) follows.

### 3.3.1.8. “8. RF|PW” registration

Card and password registration, and card or password authentication

◆ [ENTER] → [1] → [1] → User ID [ENTER] → [8]
→ Place the card → Input PW [ENTER] → Input the PW ◆

After card registration (refer to ⑤ “5. RF” registration), password registration (refer to ② “2. ID&PW” registration) follows.

### 3.3.1.9. “91. RF&PW” registration

Card and password registration, and card and password authentication

◆ [ENTER] → [1] → [1] → User ID [ENTER] → [9][1]
→ Place the card → Input PW [ENTER] → Input same PW [ENTER] ◆

After card registration (refer to ⑤ “5. RF” registration), password registration (refer to ② “2. ID&PW” registration) follows.

### 3.3.1.10. “92. ID&FP|RF&FP” registration

Card and fingerprint registration, ID and fingerprint authentication or card and fingerprint authentication

.

◆ [ENTER] → [1] → [1] → User ID [ENTER] → [9][2]
→ Place the card → 1:1 Level [ENTER] → Input FP → Input same FP ◆

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

After card registration (refer to ⑤ “5. RF” registration), fingerprint registration (refer to ① “1. FP” registration) follows.

#### 3.3.1.11. “93. ID&PW|RF&PW” registration

RF card and password registration, ID input and password authentication or card and password authentication

◆ [ENTER] → [1] → [1] → User ID [ENTER] → [9][3]
→ Place the card → Input PW [ENTER] → Input same PW [ENTER] ◆

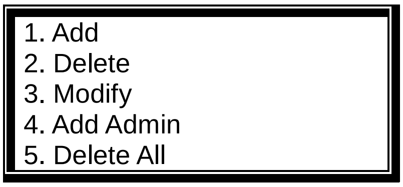
In this case, a card is used instead of ID for authentication. This is helpful to users who have difficulty inputting their ID.

After Card registration (refer to ⑤ “5. RF” registration), password registration (refer to ② “2. ID&PW” registration) follows.

### 3.3.2. Delete User

◆ [ENTER] → [1] → [2] → User ID [ENTER] ◆

In the main menu, press [1] to select “1.User”, and the following screen appears:



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

To select delete user, press [2].

After entering the user ID to delete, press [ENTER], and all the information about the user is deleted together with a “ppiririck” buzzer sound. However, the information is still stored in the server. To completely delete this information, the data in the server shall also have to be deleted.

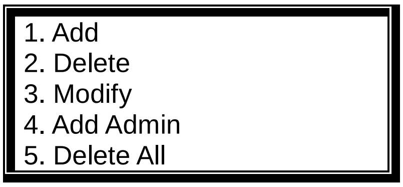
If a non-registered user ID is entered, “2.Delete” appears together with a “ppibig” sound.

Caution is required when deleting a user or an administrator. The user just registered in the unit (not in the server) is not recoverable, so special care is required.

### 3.3.3. Modify User

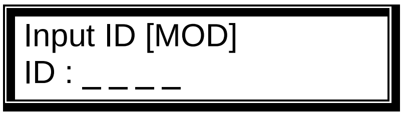
◆ [ENTER] → [1] → [3] → User ID [ENTER] → Select changing menu → change value ◆

In the main menu, press [1] to select “1. User” to see the following screen:



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

To Modify a user, press [3].



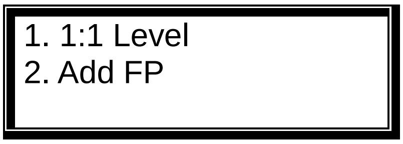
Input ID [MOD]
ID : _ _ _ _

Enter the user’s ID to Modify, and press [ENTER].

When changing an ID, there is no difference between a user and an administrator.
If a non-registered user (or administrator) is entered, you will hear a “ppibig” buzzer sound and the “1. Add” menu appears.

### 3.3.3.1. “1. FP” user

If a user’s fingerprint is already registered, changing the identification level or additional fingerprint registration is possible.

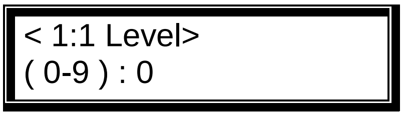


1. 1:1 Level
2. Add FP

To change the authentication level, press [1]. To add a fingerprint to the corresponding ID, press [2].

※ A maximum of 5 fingerprints can be added to an ID. If there is an attempt to add more than 5 fingerprints, a “ppibig” buzzer sound will be heard when the user presses [2].

[1] When Verification level change is selected

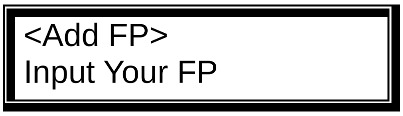


< 1:1 Level>
( 0-9 ) : 0

Recommended setting: ‘0’

To change settings, enter the new settings.

[2] When register additional fingerprints is selected



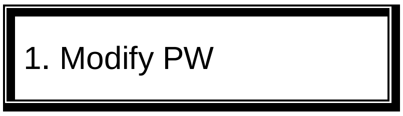
<Add FP>
Input Your FP

You will hear a “ppiriririck” buzzer sound twice and a light on the fingerprint sensor will turn on. Place a finger onto the fingerprint input window and wait for 2~3 sec. until the light turns off and the fingerprint is saved.

If you hear a “ppiririck” buzzer sound, registration is successful. It returns to the “1.Add” screen. If the fingerprint image is not so good or there is no input in the window for 10 sec. after the fingerprint sensor light turned on, it returns to the “1. Add” screen with a failure buzzer sound “ppibig”.

### 3.3.3.2. “2.ID&PW” user

when a user wants to change his/her password



1. Modify PW

To change passwords, press [1]. To cancel it, press [#].

Press the [1] button to change the passwords

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

Input password. Password should be 1~8 characters in length.

Press [ENTER] to input the password.

```
<Confirm PW>
PW:_ _ _ _ _ _ _ _
```

Input the same password once more for verification.

Press [ENTER] to confirm the password.

If the password change is successful, you will hear a “ppiririck” buzzer sound. If not, you will hear a “ppibig” buzzer sound and the “1. Add” menu appears.

### 3.3.3.3. “3.FP|PW”, “4.FP&PW” user

```
1. 1:1 Level
2. Add FP
3. Modify PW
```

Press the [1] button to change the 1:1 Level (refer to “3.3.3.1”)
Press the [2] button to register additional fingerprints (refer to “3.3.3.1”)
Press the [3] button to change passwords (refer to “3.3.3.2”).
To cancel, press the [CLR] button.

### 3.3.3.4. “5.RF” user

```
1. Change Card
```

To change the card, press [1].
To cancel, press the [#] button.

Press the [1] button to change the card.

```
<Change Card>
Place Your Card
```

To cancel, press the [#] button.

If a user places the card close to the unit, a “ppiririck” buzzer sound (Modification is successful) will be heard and the “1. Add” menu appears.

### 3.3.3.5. “6.RF|FP”,”7.RF&FP”,”92.ID&FP|RF&FP” user

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

Press [0] to see menus not shown in the LCD window.
To cancel, press the [#] button.

Press the [1] button to change the 1:1 Level (refer to “3.3.3.1”).
Press the [2] button to register additional fingerprints (refer to “3.3.3.1”).
Press the [3] button to change the card (refer to “3.3.3.4”).

### 3.3.3.6. “8.RF|PW”,”91.RF&PW”,”93.ID&PW|RF&PW” user

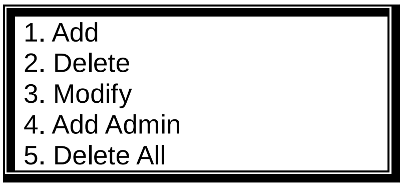
1. Modify PW
2. Change Card

Press the [1] button to change passwords (refer to “3.3.3.2”).
Press the [2] button to change the card (refer to “3.3.3.4”).
To cancel, press the [#] button.

### 3.3.4. Administrator registration

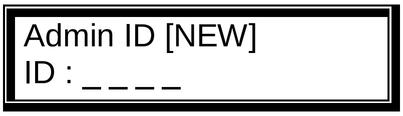
◆ [ENTER] → [1] → [4] → Admin ID [ENTER] ◆

In the main menu, press [1] to select “1.User”, and select [0] to see the following screen:



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

For administrator registration, press [4].



Admin ID [NEW]
ID : _ _ _ _

Enter the administrator ID to register and press [ENTER].

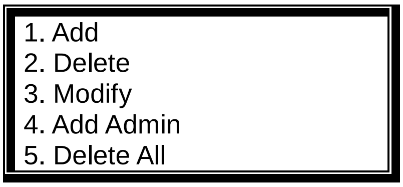
※ The procedures for administrator registration are the same as for user registration.

Only an administrator can change the terminal operation environment and register/change/delete user information stored in the unit, so special care is required when registering an administrator.

### 3.3.5. Delete all users

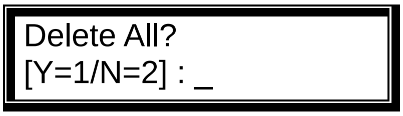
◆ [ENTER] → [1] → [5] ◆

In the main menu, press [1] to select “1. User”, and select [0] to see the following screen:



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

To delete all users, press [5].



Delete All?
[Y=1/N=2] : _

To delete all users, press [1]. If not, press [2].

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

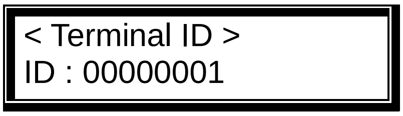
When this operation is successful, you will hear a “ppiririck” buzzer sound and the “1. Add” menu appears.

## 3.4. Network settings

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

### 3.4.1. Terminal ID settings

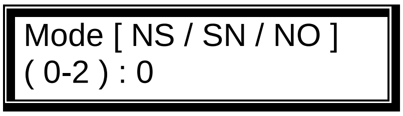
◆ [ENTER] → [2] ◆



```
< Terminal ID >
ID : 00000001
```

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

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



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

NS mode: ‘0’, SN mode: ‘1’,
NO mode: ‘2’

This defines the authentication method between the terminal and network server, and the default is ‘0’ (NS). Each authentication method is described below:

- NS mode: select [0]. When there is a live connection to the server, authentication is done through the server. If not, it is done through the terminal.

- SN mode: select [1]. Even though there is a live connection to the server authentication is done through the terminal and the result is forwarded to the server in real time.
  However, in the case of 1:1 authentication, if the entered user ID is not registered in the server, authentication is done through the server.

- NO mode: select [2]. Even though a user is registered in the terminal, authentication is done through the server in any event.

- SO mode: select [3]. When there is a live connection to the server, authentication is done through the server. If not, it is done through the terminal.
Depending on the number of terminals, the number of users, or network conditions, each different mode can be used flexibly, but if there are more than

10 terminals connected to the server for simultaneous authentication or there are frequent network problems, it is recommended to use SN authentication (setting ‘1’).

Press [ENTER] to move to the next setting.

### 3.4.3. Connection method settings

◆ [ENTER] → [2] → [ENTER] → [ENTER] ◆

```
Network Type:0
0:Static   1:DHCP
```

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

The default is ‘0’ (Static IP). If a fixed IP is assigned to the unit in a network, press [0]. If there is a DHCP server in the network to which the unit is connected, press [1].

Press [ENTER] to move to the next setting.

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

### 3.4.4. IP address settings

```
< IP Address >
192.168.   0.   3
```

Press [#] to delete an old IP and enter the new IP.

If the IP address is ‘210.98.100.50’, enter as below:

[2] [1] [0] [9] [8] [*] [1] [0] [0] [5] [0]

Press [ENTER] to move to the next setting.

### 3.4.5. Subnet mask settings

```
<Subnet Mask>
255.255.255.   0
```

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

If the subnet mask is ‘255.255.255.0’, enter as below:

[2] [5] [5] [2] [5] [5] [2] [5] [5] [0]

Press [ENTER] to move to the next setting.

### 3.4.6. Gateway settings

```
<Gateway>
192.168.   0.   1
```

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

If the gateway IP address is ‘210.98.100.1’, enter as below:

[2] [1] [0] [9] [8] [*] [1] [0] [0] [1]

Press [ENTER] to move to the next setting.

### 3.4.7. Server IP settings

```
< Server IP >
192.168.   0.   2
```

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

If the sever address is “210.98.100.121”, enter as below:

[2] [1] [0] [9] [8] [*] [1] [0] [0] [1] [2] [1]

Press [ENTER] to move to the next setting.

### 3.4.8. Server port settings

```
< Server port >
Num : 2201
```

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

As the port number of the authentication server, the default is ‘2201’. Special care is required when changing this number because the corresponding number in the server should also be changed.

If the server port is ‘2201’, enter as below:

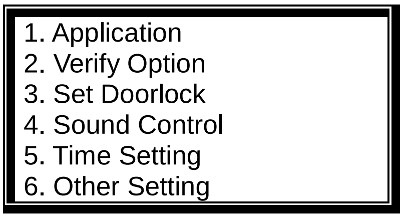
[2] [2] [0] [1]

Once the network setting is complete, press [ENTER] to return to the main menu.

## 3.5. Option settings

### 3.5.1. Application mode settings

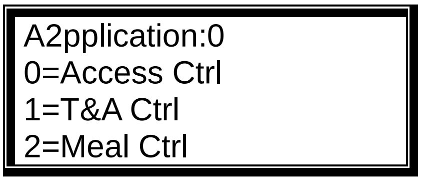
In the main menu, press [3] to select “3. Option” and following screen appears:



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

To set the basic operation mode of a terminal, press [1].

◆ [ENTER] → [3] → [1] ◆



```
A2pplication:0
0=Access Ctrl
1=T&A Ctrl
2=Meal Ctrl
```

The default is ‘0’ (Access Ctrl).

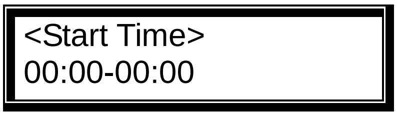
For simple Access control, set to ‘0’. for Time Attendance control, set to ‘1’.
for Meal management control to set ‘2’.
Press [ENTER] to move to detailed settings for each operation mode.

3.5.1.1. [0]: Access Control

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

3.5.1.2. [1]: Time Attendance control

Default time can be set to Start/Leave/Out/Back. After authentication, the terminal display mode can be automatically changed to programmed operation mode. If <multi-key authentication> is set as the operation mode, over 40 sub modes can be defined.



```
<Start Time>
00:00-00:00
```

If time setting is not necessary, set as ‘00:00-00:00’.

To change the start time from ‘00:00~00:00’ to ‘06:00~09:59’, press [CLR] to delete the existing setting time, and enter [0][6][0][0][0][9][5][9] in sequence.

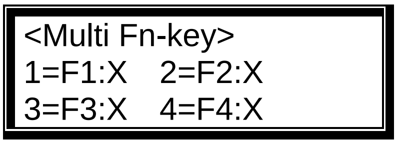
As long as no other function button is pressed during the setting time, it operates in start time mode. Even if it is set to outside work, the terminal display mode automatically changes to start mode, so authentication is convenient.

After setting <start time>, set <leave time> and <normal time> in the same manner. Each time shall not overlap.

Ex.)start time:06:00~09:59, leave time:17:00~22:00, normal time:10:00~16:59

| < Start Time > | < Leave Time > | < Normal Time > |
|---|---|---|
| 06:00~09:59 | 17:00~22:00 | 10:00~16:59 |

After setting normal time, press [ENTER] to see the “Multi Fn-key” setting menu, which allows more than 5 working modes.



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

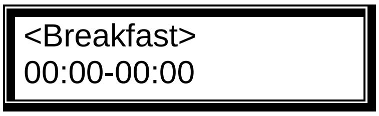
Default setting: all ‘X’

This menu is useful when more than 5 working modes are necessary.

- X setting: each function key represents a working mode such as F1=Start, F2=Leave, F3=Outside work, and F4=Back. When a function key is pressed, authentication mode changes to the corresponding working mode.
- O setting: a mode is defined by the combination of a function key and a number key such as “F3+1”.
  (Ex.) If the setting is 1=F1: X   2=F2: X   3=F3: X   4=F4: O, 14 different working modes can be defined according to user input such as [ENTER]: normal, [F1]: start, [F2]: leave, [F3]: outside work,  and [F4]+‘0’~[F4]+‘9’.

The O/X setting can be changed by pressing the corresponding number key. After setting is completed, press [ENTER] to move to the upper menu.

### 3.5.1.3. [2] Set as Meal Management



```
<Breakfast>
00:00-00:00
```

’00:00-00:00’ for Time setting not needed

If the time is set to Breakfast, authentication will be made as breakfast on appointed time.
After the Breakfast setting, same method can be applied for <Lunch>, <Dinner>, <Supper>, <Snack>. Set 00:00-00:00 For unused meal.

Each timezone need to be set so that they do not overlap each other. Within the time set, user can authenticate only once, If user need to proceed duplicate verification, press [ENTER] during Card or FP authentication

[Lock Set] will be displayed, if meal time setting has not made, and all input will be blocked except menu as same as terminal locking mode.

After setting up <Snack>, then <ENT>, <Without Limit> menu will appear

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

Default Setting: '0'

If duplicate authentication limits set to '0'. Duplication can be made by 'F4' key during authentication.

. If you do not want to duplicate authentication limits, set to '1'

Press [ENT] after the above setting, It will move to <Ticket Printer> setting

```
Ticket printer
(N=0/Y=1):0
```

Default Setting: '0'

Whether to set the RS232-1 printer as food stamps interlocking set to '1'. SRP-350 will print Terminal ID, User ID, Date, Meal ticket number, Menu will be printed.

### 3.5.2. Authentication method settings

In the main menu, press [3] to select "3. Option" and the following screen appears:

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

To set the default authentication method, press [2].

#### 3.5.2.1. Settings for ID display when authentication is successful

◆ [ENTER] → [3] → [2] ◆

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

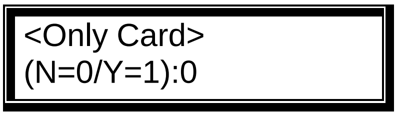
Default setting: '0'

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

Press [ENTER] to move to the next setting.

### 3.5.2.2. Settings for card only authentication

◆ [ENTER] → [3] → [2] → [ENTER] ◆



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

Default setting: ‘0’

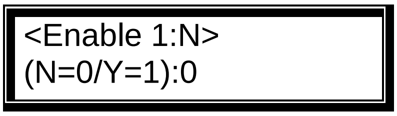
Even for a user who is registered to be authenticated with a card & PW / card & fingerprint, he/she only needs to use a card if this option is set to ‘1’.

This option is usually used when there are may terminals installed at the building entrance door where user entry/exit is frequent and the security level is relatively low.

Press [ENTER] to move to the next setting.

### 3.5.2.3. 1:N authentication settings

◆ [ENTER] → [3] → [2] → [ENTER] → [ENTER] ◆



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

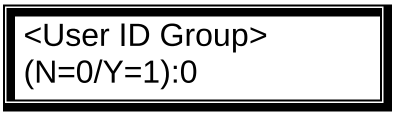
Default setting: ‘1’

This enables fingerprint authentication without a user ID or card. Even if a user is registered to be authenticated with 1:N authentication, only 1:1 authentication is allowed with the terminal if this is set to ‘0’.

If ID input or fingerprint authentication after card input (when card input replaces ID input) is required, it should be set to ‘0’.

The following are detailed settings for 1:N authentication.

① When 1:N authentication is set to ‘1’



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

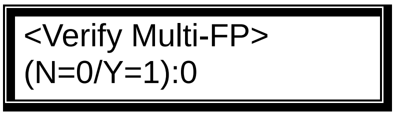
Default setting: ‘0’

Treat first digits of the ID as a group for authentication, so 1:N authentication can be processed much faster when over 1,000 users are registered.

If it is set to ‘1’, fingerprint authentication is performed for users starting with the entered ID. If it is set to '0', treat entered numbers as a user ID and try user fingerprint and 1:1 authentication for the corresponding ID

Ex.) when a user ID is a 4-digit number and '12' is entered for authentication, if it is set to '1', 1:N authentication is performed for user IDs '1200'~'1299'. If it is set to '0', 1:1 authentication is performed on user ID 12 with his/her fingerprint.

② When 1:N authentication is set to '0'


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

Default setting: '0'

For successful authentication, all registered fingerprints shall be authenticated after ID (or card) input.

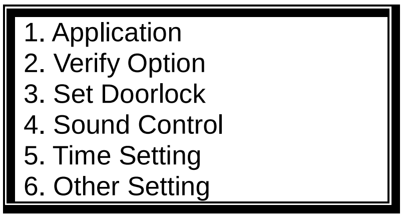
This is used when a high security level is required for special areas. If a user of 'ID 0001' has 3 fingerprints registered to the unit, all 3 fingerprints shall be authenticated after ID input.

The authentication sequence for the 3 fingerprints does not matter in this case, but authentication fails if a single fingerprint is not successfully authenticated

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

### 3.5.3. Door settings

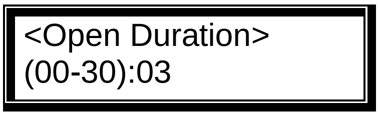
In the main menu, press [3] to select "3. Option" and the following screen appears:


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

Press [3] for door settings.

#### 3.5.3.1. Door opening time settings

◆ [ENTER] → [3] → [3] ◆


<Open Duration>
(00-30):03

Default setting: '03' (unit: sec.)

This is used to set the door opening time after authentication is successful. For the strike type, this means the door opening time. For the dead bolt type or auto door, this time is not effective.

If this is set to ‘00’, the door is out of control, so it may be set to ‘00’ only for the start/leave time period.

Once the setting is complete, press [ENTER] to move to the next setting.

### 3.5.3.2. Door status monitor

◆ [ENTER] → [3] → [3] → [ENTER] ◆

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

Default setting: ‘0’

- ‘0’: NW – no check
- ‘1’: NO – Dead Bolt Type or auto door
  (Lock monitoring is On when the door is locked)
- ‘2’: NC - Strike Type
  (Lock monitoring is Off when the door is locked)

‘0’ is for no check, ‘1’ is for dead bolt type or auto door; ‘2’ is for strike type. When this is set to ‘1’ or ‘2’, the door condition connected to the terminal is sent to the server periodically.

Once the setting is complete, Press [ENTER] to move to the next setting.

### 3.5.3.3 Door open alarm settings

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

Default setting: ‘00’

The terminal checks if the door has been open for more than setting time(5sec~30sec). If so, it makes an alarm sound.
If this is set to ‘00’, there is no alarm sound.

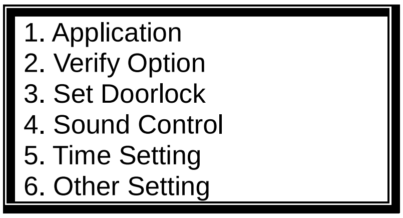
This alarm helps the relevant person check what has caused the problem in a timely manner and eliminate the problem.

For this function, the lock shall be able to monitor whether the door is open or closed and its monitoring pin shall be connected to the terminal. The door open check shall be set to ‘1’ or ‘2’ for this operation.

Once the setting is complete, press [ENTER] to move to the upper setting.

### 3.5.4. Volume settings

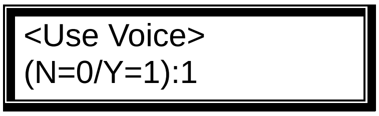
In the main menu, press [3] to select “3. Option”, and the following screen appears:



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

Press [4] for volume settings.

#### 3.5.4.1. Voice settings

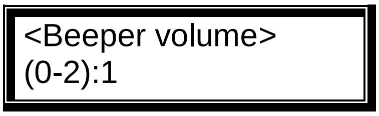


```
<Use Voice>
(N=0/Y=1):1
```

Default setting: ‘1’

To make voice information available, set it to ‘1’. If not, set it to ‘0’.
Press [ENTER] to move to the next setting.

#### 3.5.4.2. Buzzer volume settings



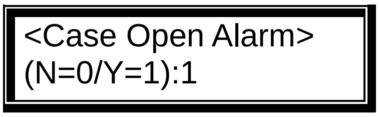
```
<Beeper volume>
(0-2):1
```

Default setting: ‘1’

This controls the terminal buzzer volume. If this is set to ‘0’, there is no buzzer sound. ‘1’ means low volume, and ‘2’ means high volume.

Press [ENTER] to move to the next setting.

#### 3.5.4.3. Case open alarm settings



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

Default setting: ‘0’

If the terminal case is damaged or opened, an alarm will sound. It works only when the case open sensor is installed.

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

### 3.5.5. Current time settings

◆ [ENTER] → [3] → [5] ◆

In the main menu, press [3] to select “3. Option”. Press [5] to see the following screen:

```
<Time Setting>
20060401211806
```

This is for the terminal current time. The above example represents the year 2006, month 04, date 01, hour 21, min. 18, and sec. 06. To change it, delete the old numbers with the [#] button before adding the new numbers.

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

### 3.5.6. Other setting

In the main menu, press [3] to select “3.Option”. Press [6] to see the following screen:

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

Press [6] for other settings.

#### 3.5.6.1. LCD Backlight On/Off settings

◆ [ENTER] → [3] → [6] ◆

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

Default setting : ‘0’

This is for LCD backlight on/off settings.

If it is set to the default setting [0], LCD backlight is normally off. Only in cases that a user operates with keypad or card, LCD backlight goes on and after the working operation is done, it goes off in about 10 seconds.

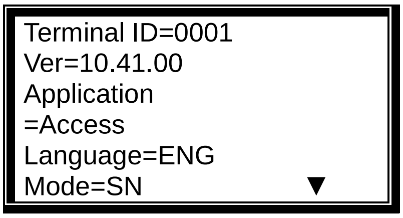
If it is set to ‘1’, it always stays on.

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

## 3.6. Terminal information view

◆ [ENTER] → [4] ◆

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



```
Terminal ID=0001
Ver=10.41.00
Application
=Access
Language=ENG
Mode=SN              ▼
```

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

| | |
|---|---|
| Terminal ID | Terminal ID |
| Version | Terminal firmware version |
| Application | Terminal application mode (Access/T&A) |
| Language | Language for text and voice of the LCD screen |
| Mode | Connection mode between terminal and network server |
| Network type | Network connection type (fixed IP/variable IP) |
| Mac Address | Terminal Ethernet hardware address |
| IP address | Terminal IP address |
| Gateway | Terminal Gateway address |
| Subnet mask | Terminal Subnet Mask address |
| Server IP | IP address of network server connected to the terminal |
| Svr-port | Port number of network server program |
| Card Reader | Connected card reader type |
| FP-Sensor | Connected fingerprint sensor type |
| 1:1 Level | Identification level for 1:1 authentication |
| 1:N Level | Identification level for 1:N authentication |
| Max User | Max. number of users registered to a terminal |
| Max FP | Max. number of fingerprints registered to a terminal. For example, if there are 100 registered users and two fingerprints are registered for each user, then there is a total of 200 fingerprints registered |
| All User | Number of current users registered to a terminal including administrators |
| All Admin | Number of administrators registered to a terminal |
| All FP | Number of fingerprints currently registered to a terminal |

| | |
|---|---|
| 1:N User | Number of users for 1:N authentication |
| 1:N FP | Number of fingerprints for 1:N authentication |
| All Log | Authentication records stored in a terminal |

## 3.7. Extended functions

In the main menu, press [5] to select “5.Ext function”. And the following screen appears:

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

### 3.7.1. Terminal lock settings

◆ [ENTER] → [5] → [1] ◆

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

Default setting ‘0’: terminal lock clear
‘1’: terminal lock set

Instead of a server program, an administrator can directly set up a terminal lock for a terminal. If it is set to ‘1’, the terminal is locked and nobody can pass the door until an administrator unlocks the terminal.

※ For this function, ‘administrator entering OK’ shall be checked in the terminal option of the server program.

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

### 3.7.2. Read card number

◆ [ENTER] → [5] → [2] ◆

```
Place Your Card
```

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

To exit from the card reader, press [CLR] to move to the upper menu.

## 3.8. Device settings

In the main menu, press [6] to select “6. Device”, and the following screen asking for the setting password appears:

Device settings is an option that is not necessary to change after installation, so it is recommended not to change it except when it is really required.

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

This setting password is just for user information, so it cannot be changed.

Enter “084265” as the setting password and press [ENTER] to view the detailed setting items.

### 3.8.1. Function key settings

◆ [ENTER] → [6] → ‘084265’ [ENTER] → [1] ◆

```
<Key On/Off>
1=F1:0   2=F2:0
3=F3:0   4=F4:0
5=Ent:O   6=FP:O
```

Default setting: all ‘O’

This is for enabling/disabling the function keys. ‘O’ is ‘enable’ and ‘X’ is ‘disable’. Whenever a function key is pressed, it toggles between O/X.

1 is for [F1], 2 is for [F2], 3 is for [F3], 4 is for [F4], 5 is for [ENTER], and 6 is for the fingerprint sensor’s Auto Sensing. If F1 becomes X by pressing [1], you can not change to start mode even if you press [F1].

Additionally, if only [F1] or [F2] is set to ‘O’, the terminal can be used in either always start or always leave mode.

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

### 3.8.2. Card reader settings

◆ [ENTER] → [6] → ‘084265’ [ENTER] → [2] ◆

```
Card Reader:0
0=Non 1=RF 2=SC
3=Wiegand 4=SC1
5=Ext
```

Default setting: ‘0’

This is the setting for the card reader connected to a terminal. This shall be set to ‘0’ except in the following cases:

- ‘0’: no card reader
- ‘1’: a low-frequency RF Card reader is installed
- ‘2’: a high-frequency smart card reader is installed
- ‘3’: a Wiegand-type card reader is installed (ex.: HID...)
- ‘4’: a new version of the smart RF reader is installed
- ‘5’: an external card reader is installed

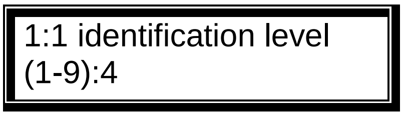
If this is set to a number other than 0 and [F1]~[F4] or [ENTER] is pressed, only the authentication mode is changed and 1:N fingerprint authentication is not performed. However, 1:N authentication is performed only for auto sensing.

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

3.8.3. Fingerprint sensor settings

3.8.3.1. 1:1 verification level settings

◆ [ENTER] → [6] → ‘084265’ [ENTER] → [3] ◆


1:1 identification level
(1-9):4

Default setting: ‘4’

This sets the matching rate between the fingerprints input and the fingerprints stored in the database of a terminal. The higher the level, the higher the security, but the possibility of authentication failure is higher.

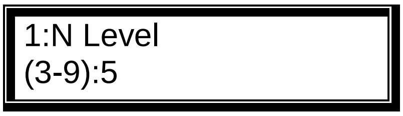
1:1 identification level is an authentication level setting menu used when authentication is performed together with an ID. If the entered ID is ‘1234’, the fingerprint registered with the ID ‘1234’ is retrieved from the database to compare the two fingerprints.

However, in the case of 1:1 authentication, if a user’s 1:1 level is not set to [0] (1:1 level of the terminal is used), the user’s 1:1 level is used.

Press [ENTER] to move to the next setting.

3.8.3.2. 1:N identification level settings

◆ [ENTER] → [6] → ‘084265’ [ENTER] → [3] → [ENTER] ◆


1:N Level
(3-9):5

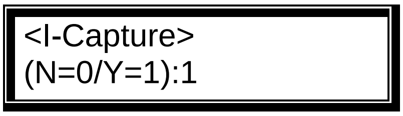
Default setting: ‘5’

This sets the identification level when authentication is performed without ID input.
An entered fingerprint is compared to all the fingerprints in the database for which 1:N authentication is allowed.

For 1:N authentication, the identification level is not set for each user, so the terminal authentication level is basically used.

Press [ENTER] to move to the next setting.

3.8.3.3. Intelligent-Capture settings


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

Default setting: ‘1’

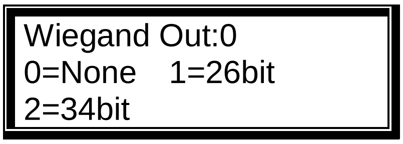
This adjusts the sensor settings automatically to enhance detection capability regardless of residual fingerprints (fingerprints left on a sensor window due to sweat or contaminants on a finger) or fingerprint humidity.

- If it is set to ‘0’, fingerprint authentication time is shorter, but the success rate is lower for dry or wet fingerprints.
- If it is set to ‘1’, it takes about 0.5~1 sec. longer compared to when it is set to ‘0’, but the success rate is higher, so ‘1’ is recommended.

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

3.8.4. Wiegand output settings

◆ [ENTER] → [6] → ‘084265’ [ENTER] → [4] ◆


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

Default setting: ‘0’

When this is set to ‘1’, “Site code + user ID” is sent to the Wiegand port of the terminal when authentication is done. It can be used only for systems where there is a lock controller and the controller is operated by a Wiegand input. This is usually set to ‘0’.

- If it is set to ‘1’, user ID shall be shorter than 4 digits because “Site code [1 byte] + user ID [2 bytes]” is transferred.
- If it is set to ‘2’, user ID shall be shorter than 7 digits because “Site code [1 byte] + user ID [3 bytes]” is transferred.

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

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

Default setting: ‘000’

This is only available when Wiegand Out is set to ‘1’ or ‘2’. Enter the site code (0-255) to be sent to the Wiegand Port together with the user ID.

```
<Bypass>
(0=Off/1=On):1
```

Default setting: ‘1’

In case of Wiegand card input, '1' is set to output Wiegand card value and '0' is set to output configured format above.

* In case of fingerprint users, they will be outputted in configured format though Bypass is set to '1'.

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

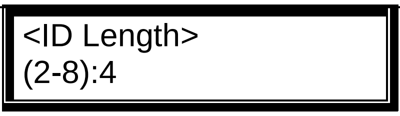
### 3.8.5. System configuration settings

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

Press [5] for system settings.

#### 3.8.5.1. User ID length settings

◆ [ENTER] → [6] → ‘084265’ [ENTER] → [5] ◆



<ID Length>
(2-8):4

Default setting: ‘4’

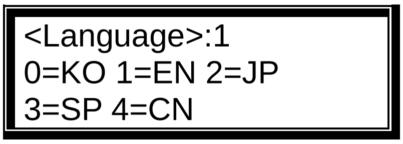
This can be 2~8 digits and shall be the same as the ID registered in the server program. If the ID registered in the server program is ‘000075’, enter 6.

Special care is required when reducing the number of digits during normal operation because an administrator may not be able to be authenticated when he wants to enter menus due to the reduced number of digits.

Press [ENTER] to move to the next setting.

### 3.8.1.2. Language settings

◆ [ENTER] → [6] → ‘084265’ [ENTER] → [5] → [ENTER] ◆



<Language>:1
0=KO 1=EN 2=JP
3=SP 4=CN

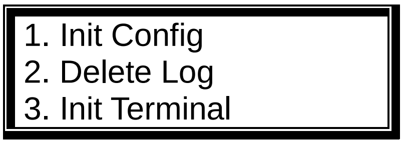
Default setting: ‘1’ (English)

Voice information languages follow these settings: ‘0’: Korean, ‘1’: English, ‘2’: Japanese, ‘3’: Spanish, ‘4’: Chinese
‘0’ ~ ‘2’: LCD characters also correspond to the language.
‘3’ ~ ‘4’: LCD characters are in English.

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

### 3.8.6. Terminal initialization

In the main menu, press [6] to select “6. Device”, and then press [6] to select “6. Initialize” and the following screen appears:



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

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

### 3.8.6.1. Settings initialization

◆ [ENTER] → [6] → ‘084265’ [ENTER] → [6] → [1] ◆

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

To initialize settings, press [1]. If not, press [2].

All the settings except Mac (physical) address are initialized, but the user and authentication records are not deleted.

※ If the settings are initialized, the language of the voice and menus becomes English. If you need to set other language
(“6. Set Device”→ “1. System Config” → <Language>: set to 0~4)

Once initialization is done successfully, it moves to the upper menu together with a “ppiririck” buzzer sound.

3.8.6.2. Authentication record initialization

◆ [ENTER] → [6] → ‘084265’ [ENTER] → [6] → [2] ◆

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

To initialize the record, press [1].
If not, press [2].

Deletes all logs related to authentication, but settings and users are not deleted. Once initialization is done successfully, it moves to the upper menu together with a “ppiririck” buzzer sound.

3.8.6.3. Factory initialization

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

To Factory Default settings, press [1]. If not, press [2].

Except for the Mac (physical) address stored in the terminal, all settings, users and log information are deleted for the factory default.

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

Once initialization is done successfully, the terminal is rebooted after a “ppiririck” buzzer sound.

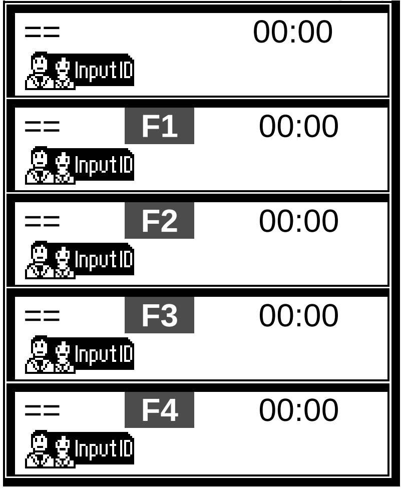
# 4. How to use the terminal

## 4.1. Access control

- Menu “3.Option” → “1.Application” → [0] Access control settings

### 4.1.1. Authentication mode

- Authentication mode display screen



Normal mode; authentication with [ENTER]

F1 mode; authentication with [F1]

F2 mode; authentication with [F2]

F3 mode; authentication with [F3]

F4 mode; authentication with [F4]

- Fingerprint authentication
  Press the function key for authentication with the corresponding mode.
  If the function key is not used and authentication is done using Auto Sensing, the current authentication mode on the screen is used.

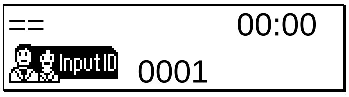
- Password authentication
  After entering the user ID and changing the authentication mode by pressing the corresponding function key, enter the password for authentication.

- When a card is used together (i.e., menu → "6.Device" settings → "3.Card reader" → when <Card Reader> is set to over 1)
  When entering the function key, only the authentication mode is changed instead of entering into fingerprint authentication, so change the authentication mode by pressing the corresponding function key to enter the card.

### 4.1.2. [1:1] fingerprint authentication

▶ During auto sensing, if the user ID is '0001', enter '0001', and then place your finger close to the fingerprint sensor. The light on the fingerprint input window will turn on to detect the fingerprint and the authentication result will be displayed on the LCD window.

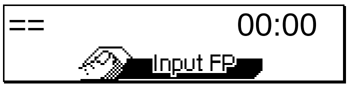
▶ If the user ID is '0001', enter '0001' and press the function key. The light on the fingerprint input window will turn on together with voice information. When a fingerprint is entered, the authentication result will be displayed on the LCD window.



== 00:00
Input ID 0001

If the user ID is ‘0001’, enter ‘1’ or ‘0001’ and press the function key.

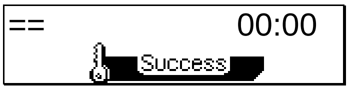
▼



== 00:00
Input FP

Place your finger close to the input window when the light on the fingerprint input window turns on together with the voice message “Please enter your fingerprint”. Do not remove your finger until you hear a “ppig” buzzer sound.

▼

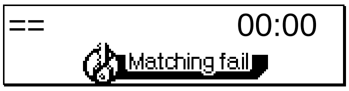


== 00:00
Success

If authentication is successful, a success message will be displayed on the LCD together with a voice message “You are authorized”. The door relay and LED turn on.

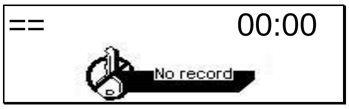
The default screen appears after 1~2 sec., and the door relay and LED turn off when the door open setting time has elapsed.

※ Error message: An error message appears together with a voice message “Please try again”.



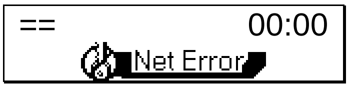
== 00:00
Matching fail

Authentication failed.



== 00:00
No record

Non-registered user ID entered.



== 00:00
Net Error

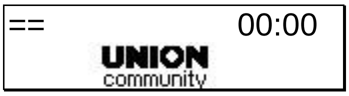
During the authentication request to the authentication server, network trouble occurred or the line is disconnected.

### 4.1.3. [1:N] fingerprint authentication

This authentication is only allowed for a user to whom 1:N authentication is allowed during registration.

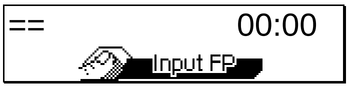
▶ During Auto Sensing, if a user places his/her finger close to the fingerprint sensor, the light on the fingerprint input window will turn on to detect the fingerprint and the authentication result will be displayed on the LCD window.

▶ In the default screen, press the function key and the light on the fingerprint input window will turn on together with a voice message "Please enter your fingerprint". When a fingerprint is entered, the authentication result will be displayed on the LCD window.


== 00:00
UNION community

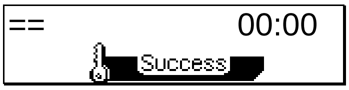
In the default screen, press the function key.

▼


== 00:00
Input FP

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

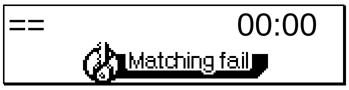
▼


== 00:00
Success

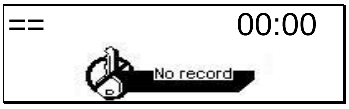
If authentication is successful, you will see a success message on the LCD together with the voice message "You are authorized". The door relay and LED turn on.

The default screen appears after 1~2 sec., and the door relay and LED turn off when the door open setting time has elapsed.

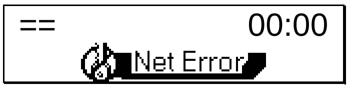
※ Error message: An error message appears together with the voice message "Please try again".


== 00:00
Matching fail

Authentication failed.


== 00:00
No record

If the connection method is SN and there is no user to whom 1:N authentication is allowed in the terminal.

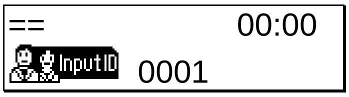

== 00:00
Net Error

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

▶ In the case of a user who is registered with [fingerprint & password], password input is required for successful authentication after fingerprint authentication is successful.

### 4.1.4. Password authentication

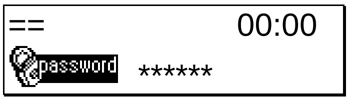
▶ If the user ID is “0001”, enter “0001” and press the function key. You will hear a “ppiriririck” buzzer sound and the terminal waits for the user password to be input. Enter the password and press [ENTER], and the authentication result appears on the LCD.



== 00:00
InputID 0001

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

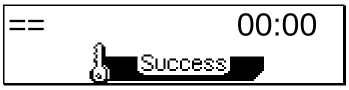
▼



== 00:00
password ******

You will hear a “ppiriririck” buzzer sound and the terminal waits for the user password to be input. Enter the password and press [ENTER].
(the password is displayed as ‘*’ on the LCD screen, rather than the actual numbers.)

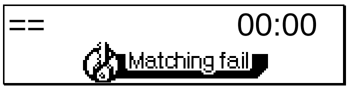
▼



== 00:00
Success

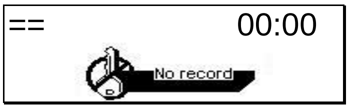
If authentication is successful, you will see a success message on the LCD together with the voice message “You are authorized”. The door relay and LED turn on.
The default screen appears after 1~2 sec., and the door relay and LED turn off when the door open setting time has elapsed.

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



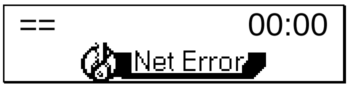
== 00:00
Matching fail

Password authentication failed.



== 00:00
No record

Non-registered user ID entered.

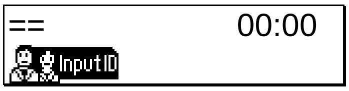


== 00:00
Net Error

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

### 4.1.5. Card authentication

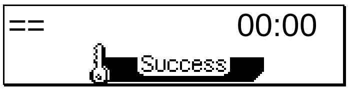
▶ For a user who is registered as [RF], [RF|FP], or [RF|PW], when placing the card close to the default screen, a "ppig" buzzer sound will be heard and the authentication result appears on the LCD.



== 00:00
Input ID

If you place your card close to the unit, you will hear a "ppig" buzzer sound.

▼

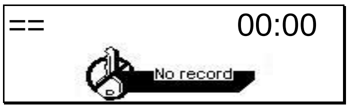


== 00:00
Success

If authentication is successful, you will see a success message on the LCD together with the voice message "You are authorized". The door relay and LED turn on.

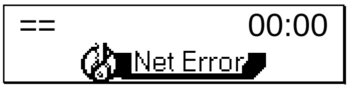
The default screen appears after 1~2 sec., and the door relay and LED turn off when the door open setting time has elapsed.

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



== 00:00
No record

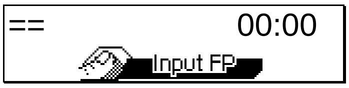
Non-registered card used.



== 00:00
Net Error

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

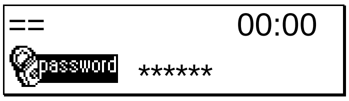
▶ For a user who is registered as [RF&FP] or [ID&FP | RF&FP], when placing the card close to the default screen, a "ppig" buzzer sound will be heard and the following fingerprint authentication screen appears:



== 00:00
Input FP

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

▶ For a user who is registered as [RF&PW] or [ID&PW | RF&PW], when placing the card close to the default screen, a "ppig" buzzer sound will be heard and the following fingerprint authentication screen appears:



== 00:00
password ******

A "ppiriririck" buzzer sound will be heard and the unit waits for the user password to be input. Enter password and press [ENTER].

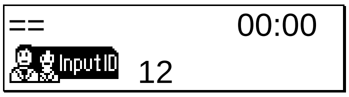
### 4.1.6. User ID group authentication

Authentication is done with the first digits (at least one digit) of the user ID instead of all the digits of the user ID. It is more convenient than 1:1 authentication. This is used when 1:N cannot be used because there are too many users or when 1:N authentication is too slow.

In the menu, set as below:

3. Option settings → 2. Authentication method settings → <1:N authentication>=1 → <ID group authentication >=1

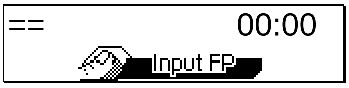
For example, for a user whose ID is ‘1234’, enter only ‘12’ for authentication, then only the fingerprints of users starting with ‘12’ (1200~1299 users) are searched. If the ID is ‘0012’, enter ‘0012’ or ‘00’ for authentication.



== 00:00

Input ID 12

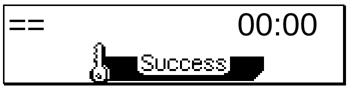
If the user ID is ‘1234’, enter ‘1’, ‘12’, or ‘123’, and then press the function key.



== 00:00

Input FP

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



== 00:00

Success

If authentication is successful, you will see a success message on the LCD together with the voice message “You are authorized”. The door relay and LED turn on.

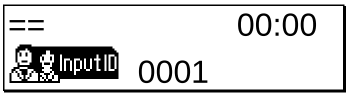
The default screen appears after 1~2 sec., and the door relay and LED turn off when the door open setting time has elapsed.

### 4.1.7. Multiple fingerprint authentication

For a door to which a higher level of security is required, multiple fingerprints from more than 2 people are assigned to a single ID. The door opens only when all the registered fingerprints are authenticated.
In the menu, set as below:
3. Option setting → 2. Authentication method settings → <1:N authentication >=0 → < multiple fingerprint authentication >=1

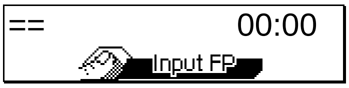
For example, if the ID ‘0001’ is registered with 3 fingerprints, all 3 fingerprints must be authenticated after ID input to enter through the door. A single failure in the middle renews the authentication process. This iterative process continues until all 3 fingerprints are authenticated.

▶ If the user ID is ‘0001’, enter ‘1’ or ‘0001’ and press the function key. The light on the fingerprint input window turns on together with the voice message “Please enter your fingerprint.” (during auto sensing, fingerprint input alone is sufficient). When a fingerprint is entered, the authentication result will be displayed on the LCD window.


== 00:00
Input ID 0001

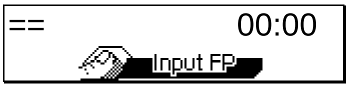
If the user ID is ‘0001’, enter ‘0001’ and press the function key.

▼


== 00:00
Input FP

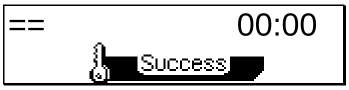
When the light on the fingerprint input window turns on together with the voice message “Please enter your fingerprint”, enter your fingerprint and hold it there until you hear a “ppig” buzzer sound.

▼


== 00:00
Input FP

If authentication is successful, you will hear a “ppiririck” buzzer sound and the light on the fingerprint input window turns on together with the voice message “Please enter your fingerprint”. This iterative process continues until all entered fingerprints have been authenticated.

▼


== 00:00
Success

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

※ Error message: the same as the error with [1:1] authentication

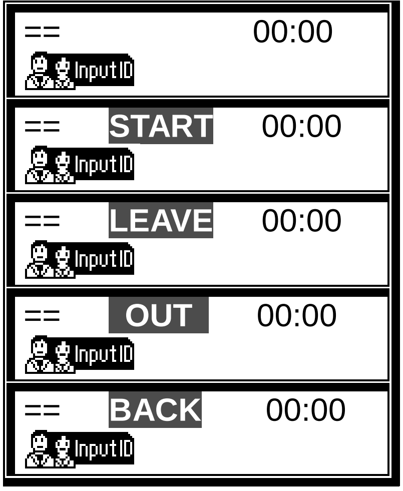
### 4.2. Time attendance control

- Menu “3.Option” → “1.Application” → [1] T&A (Time Attendance) settings

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

### 4.2.1. Authentication mode

- Authentication mode display screen



Normal mode; authentication with [ENTER]

Start mode; authentication with [F1]

Leave mode; authentication with [F2]

Outside work mode; authentication with [F3]

Return mode; authentication with [F4]

- Fingerprint authentication
  Press the function key for working mode authentication.
  If the function key is not used and authentication is done with Auto Sensing, the current authentication mode on the screen is used.

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

- When a card is used together (i.e., Menu → 6.Device settings → 3. Card reader → when <Card Reader> is set to over 1)
  When entering the function key, only the working mode is changed instead of entering into fingerprint authentication, so change the working mode by pressing the corresponding function key to enter the card.

- Working mode after authentication depends on <start time>, <leave time>, and <normal time> settings. The previous authentication mode is maintained if no mode is set for a specific time period.

### 4.2.2. [1:1] fingerprint authentication

- the same as 4.1.2.

### 4.2.3. [1:N] fingerprint authentication

- the same as 4.1.3.

4.2.4. Password authentication

- the same as 4.1.4.

4.2.5. Card authentication

- the same as 4.1.5.

4.2.6. User ID group authentication

- the same as 4.1.6.

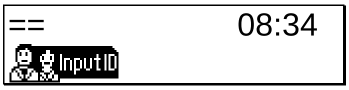
4.2.7. Working mode expansion using multi-key authentication

- If more than 5 working modes such as start, leave, outside work, return, and general are required, it can be expanded up to 41 modes.

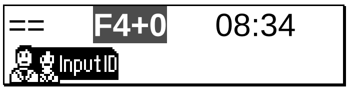
- After setting Menu → 3.Option → 1.Application → [1] T&A, in <Multi Fn-key>, set more than one key to 'O'. However, the keys set to 'X' are not the case.

- Because a mode is defined with a number key, enter a number key after entering the function key for authentication. In the server program, authentication mode is "F3+1".

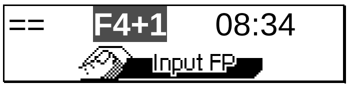
- For example, when [F4] is set to [O] and <start time> is set to '07:00~09:30', if a fingerprint user tries authentication "F4+1"mode,



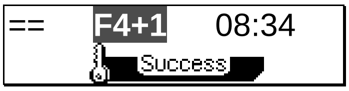
In the default screen, press [F4].



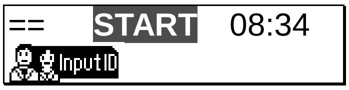
The mode is changed to "F4+0".
Press [1].



When the mode is changed to "F4+1", enter the fingerprint.



When authentication is successful, a success message appears.



The current time is 08:34, so it returns to the start mode.

## 4.3. For meal management

- Menu → 3. Option Setting → 1. Operation method setting → [2]Meal setting

- 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.

- If duplication authentication enable option is set to '1', duplication authentication can be unlimited. If it is set to '0', an individual user is authenticated once in each meal and duplication authentication is unavailable. However, the user can use duplication authentication function with [ENTER] key.

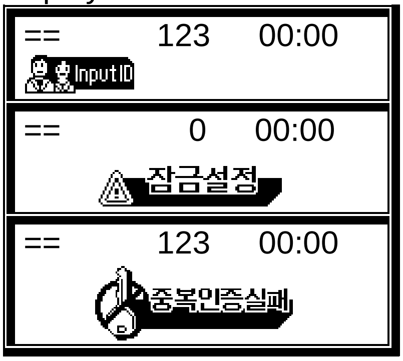
.

- If duplication authentication always needs to be unavailable, duplication authentication enable option is set to '0', and then move to Menu -> 6. device setting -> 1. Function key setting -> set Ent=[X] in <Key On/Off>. As a result, duplication authentication function with [ENTER] key is not available.

### 4.3.1. Meal Type

- In meal service management, function key runs as operation key for authentication. The number on the top of LCD screen displays only the count of authentication during relevant meal service.

- Display Screen



== 123 00:00
Input ID

== 0 00:00
잠금설정

== 123 00:00
중복인증실패

Display the total count of authentication success during each meal service period

In case that other than meal service time

In case that an user attempts to re-authenticate during same meal service time period

- If authentication is made by fingerprint, auto sensing function makes it done without using authentication with function key or function key itself.

- Authentication with password
For authentication, after entering user ID, press function key and password

- In case that authentication is made along with a card (Menu -> 6. device setting -> 3. card reader -> <Card Reader>= more than 1), enter card to proceed.

4.3.2. [1:1] Fingerprint authentication

- Though it is identical to 4.1.2., [ENTER] key cannot be used in function key 4.1.2.

4.3.3. [1:N] Fingerprint authentication

- Though it is identical to 4.1.3., [ENTER] key cannot be used in function key.

4.3.4. Password authentication

- Though it is identical to 4.1.4., [ENTER] key cannot be used in function key.

4.3.5. Authentication with card

- Though it is identical to 4.1.5., [ENTER] key cannot be used in function key.

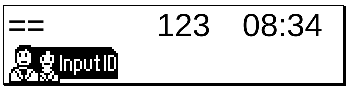
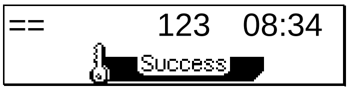
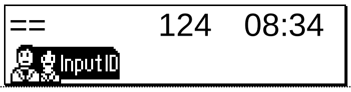
4.3.6. Group Authentication using User ID

- Though it is identical to 4.1.6., [ENTER] key cannot be used in function key.

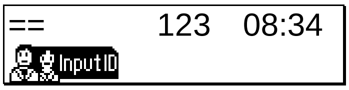
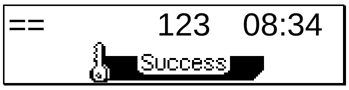
4.3.7. Duplicate Authentication Enable

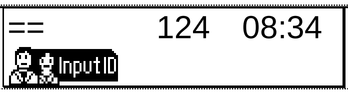
- Menu -> 6. Device setting -> 1. Function key setting -> In <Key On/Off>, Ent=[0] must be set. (For initialization, as default setting value is [0], it does not need to be changed. However, if it does not work properly, checking is necessary)

- In case that duplication authentication by fingerprint users

| | |
|---|---|
|  == 123 08:34<br>InputID | In the main screen, enter fingerprint while pressing [ENTER] button. |
|  == 123 08:34<br>Success | Success message is displayed upon authentication success |
|  == 124 08:34<br>InputID | The number of meal count increases when returning to the main screen. |

-In case that duplication authentication by card users

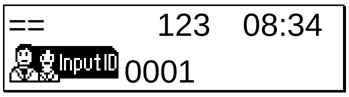
| | |
|---|---|
|  == 123 08:34<br>InputID | In the main screen, enter card while pressing [ENTER] button. |
|  == 123 08:34<br>Success | Success message is displayed upon authentication success |



```
==          124   08:34
InputID
```

The number of meal count increases when returning to the main screen.

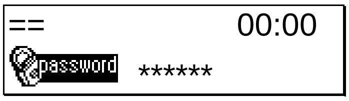
- In case that duplication authentication by password users



```
==          123   08:34
InputID 0001
```

In the main screen, after enter user ID, enter one of function keys ([F1], [F2], [F3], and [F4]) while pressing [ENTER] button

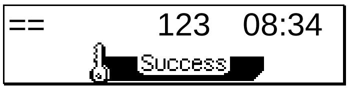
▼



```
==                00:00
password  ******
```

"Birririk" sound is heard and user's password input screen is displayed. After entering password, press [ENTER] button.

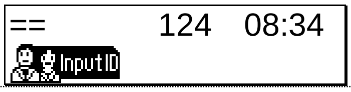
▼



```
==          123   08:34
        Success
```

Success message is displayed upon authentication success

▼



```
==          124   08:34
InputID
```

The number of meal count increases when returning to the main screen.