

# VIRDI 4000™ User's Manual

---

Version eng-1.02



**UNION**  
COMMUNITY

---

Copyright 2006 By UNION COMMUNITY Co., Ltd.

## Disclaimer

Information in this document is provided in connection with UNION COMMUNITY products. No license, express or implied, by estoppels or otherwise, to any intellectual property rights is granted by this document. Except as provided in UNION COMMUNITY's Terms and Conditions of Sale for such products, UNION COMMUNITY assumes no liability whatsoever, and UNION COMMUNITY disclaims any express or implied warranty, relating to sale and/or use of UNION COMMUNITY products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right.

UNION COMMUNITY products are not intended for use in medical, life saving, life sustaining applications, or other applications in which the failure of the UNION COMMUNITY product could create a situation where personal injury or death may occur. Should Buyer purchase or use UNION COMMUNITY products for any such unintended or unauthorised application, Buyer shall indemnify and hold UNION COMMUNITY and its officers, employees, subsidiaries, affiliates, and distributors harmless against all claims, costs, damages, and expenses, and reasonable attorney fees arising out of, directly or indirectly, any claim of personal injury or death associated with such unintended or unauthorised use, even if such claim alleges that UNION COMMUNITY was negligent regarding the design or manufacture of the part.

UNION COMMUNITY reserves the right to make changes to specifications and product descriptions at any time without notice to improve reliability, function, or design. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." UNION COMMUNITY reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them.

Please contact UNION COMMUNITY, local UNION COMMUNITY sales representatives or local distributors to obtain the latest specifications and do this before placing your product order.

## About UNION COMMUNITY

With regard to any fingerprint-related issues, UNION COMMUNITY is always in readiness to find out well fitted solutions, depending on customers' requirements and needs.

As a leading provider of fingerprint core technology, UNION COMMUNITY has set up wide variety of fingerprint product lines from fingerprint OEM modules to several choices of fingerprint finished products including access control, time & attendance, door lock, PC peripherals, safety box, etc, that incorporate UNION COMMUNITY's groundbreaking biometrics technology. Based on its proprietary algorithm, its own

sensor and in-house one-stop processing capability regarding hardware, software, product design, etc., our services to government sector and various commercial sectors like security, construction and enterprise are in full swing through fast problem-solving approach to meet market trends or demands. As a result, UNION COMMUNITY exports its market-proven fingerprint products to over 40 countries including Japan, USA, Europe and China.

As the biggest and the most promising company in the commercial sector of biometrics industry in Korea, UNION COMMUNITY was awarded "Korean World-class Product Award" for its excellent performance by Minister of Commerce, Industry and Energy in December 2005.

To be the world-class company in biometrics field, UNION COMMUNITY and all the members continue to do all-out efforts for the world-best quality product, creation of new paradigm and customers' satisfaction through accumulated expertise and working experience from various reference sites and versatile hardware & software development.

#### About This Manual

This is an introduction to operation of VIRDI 4000 series supplied by UNION COMMUNITY. This manual describes how to do user registration in local terminal, terminal settings, network settings, etc. The purpose of this manual is to provide instructions on using VIRDI 4000 series and troubleshooting minor problems.

## < Glossary >

### ● Admin, Administrator

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

### ● 1 to 1 Verification

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

### ● 1 to N Identification

- The terminal performs matches against multiple fingerprints (templates) based solely on fingerprint information.
- Without an 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.
- Example: 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 are for direct authentication. Each key represents each authentication mode.

## Table of Contents





<b>&lt; Glossary&gt;</b> .....	<b>4</b>
<b>Table of Contents</b> .....	<b>6</b>
<b>1.1. Safety Precautions</b> .....	<b>8</b>
<b>1.3. Screen (during operation) Description</b> .....	<b>10</b>
<b>1.4. Voice Information During Operation</b> .....	<b>11</b>
<b>1.5. Buzzer Sound During Operation</b> .....	<b>11</b>
<b>1.6. LED Signal During Operation</b> .....	<b>11</b>
<b>1.7. Correct fingerprint registration and input methods</b> .....	<b>12</b>
<b>2.1. Features</b> .....	<b>14</b>
2.2.1. Network configuration.....	16
2.2.2. Standalone configuration .....	16
<b>3.1. Check items before device configuration settings</b> .....	<b>18</b>
3.1.1. Entering menu .....	18
3.1.2. Changing setting parameters .....	18
3.3.1. User registration .....	22
3.3.3. Modifying User .....	27
3.3.5. Delete All Users.....	30
3.4.1. Terminal ID settings .....	31
3.4.2. Connection [NS / SN / NO] mode settings.....	31
3.4.3. Connection method settings .....	32
3.4.4. IP address settings .....	32
3.4.5. Subnet mask settings .....	32
3.4.6. Gateway settings.....	33
3.4.7. Server IP settings .....	33
3.4.8. Server port settings .....	33
3.5.1. Application mode settings.....	34
3.5.2. Option settings for authentication .....	35
3.5.3. Doorlock settings.....	38
3.5.4. Volume settings .....	39
3.5.5. Current time settings .....	40
3.5.6. Other setting.....	41
<b>3.7. Extra functions</b> .....	<b>43</b>
3.7.1. Terminal lock settings .....	43
3.7.2. Read card number.....	43
<b>3.8. Device settings</b> .....	<b>44</b>
3.8.1. Function key settings.....	44
3.8.2. Card reader settings .....	45
3.8.3. Fingerprint sensor settings .....	46
3.8.4. Wiegand output settings .....	48
3.8.5. System configuration settings.....	48
3.8.6. Terminal initialisation .....	49
<b>4. How to use the terminal</b> .....	<b>51</b>
<b>4.1. Access control application</b> .....	<b>51</b>
4.1.1. Authentication mode .....	51
4.1.2. [1:1] fingerprint authentication .....	52
<b>4.2. Time &amp; Attendance control</b> .....	<b>57</b>

VIRDI 4000™ User's Manual	7
4.2.1. Authentication mode .....	57
4.2.2. [1:1] fingerprint authentication .....	58
4.2.3. [1:N] fingerprint authentication.....	58
4.2.4. Password authentication .....	58
4.2.5. Card authentication .....	58
4.2.6. User ID group authentication.....	58
4.2.7. Expansion of working mode by multi-key function .....	58

# 1. Before use






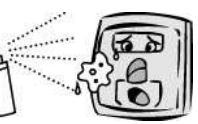
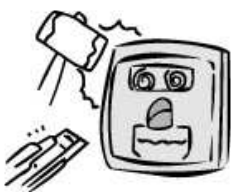
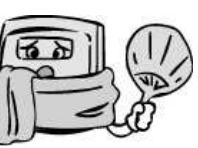
## 1.1. Safety Precautions

### ● Warnings

<p>Handling with wet hands or allowing liquid to flow into it is prohibited. -&gt; It may cause an electric shock or damage.</p>		<p>Do not place a fire source near the terminal. -&gt; It may cause a fire.</p>	
<p>Do not disassemble, repair, or modify the terminal at your discretion. -&gt; It may cause an electric shock, fire or damage.</p>		<p>Keep out of reach of children. -&gt; It may cause an accident or damage.</p>	

- If the above warning is ignored, it may result in death or serious injury.

### ● Cautions

<p>Keep away from direct sunlight -&gt; It may cause deformation or a change of colour.</p>		<p>Avoid high humidity or dust -&gt; The terminal may be damaged.</p>	
<p>Avoid using water, benzene, thinner, or alcohol for cleaning -&gt; It may cause an electric shock or fire.</p>		<p>Do not place a magnet close to the terminal. -&gt; The terminal may break down or malfunction.</p>	
<p>Do not contaminate the fingerprint input area. -&gt; Fingerprints may not be recognised very well.</p>		<p>Avoid using insecticide or flammable spray near the terminal. -&gt; It may result in deformation or a change of colour.</p>	
<p>Avoid impacts or using sharp objects on the terminal. -&gt; The terminal may be damaged and broken.</p>		<p>Avoid severe temperature changes -&gt; The terminal may be broken.</p>	

- 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 without referring to the user manual.



1.2. Terminal Description

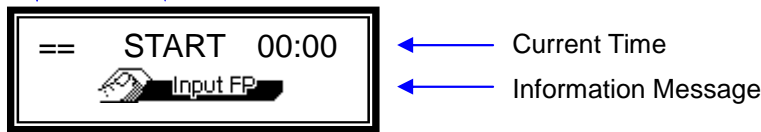


No.	item	description	
①	LCD	Display messages for all the operations.	
②	Key Pad	[F1], [F2], [F3], [F4]	[F1] : Start, [F2] : Leave, [F3] : Outside Work, [F4] : Return
		[1] ~ [9]	Input digits (1~9).
		[0]	Enter '0' or LCD menu scroll.
		[*]	Terminal menu setting (Enter into menu mode for terminal menu setting when pressed and held for over 2 seconds).
		[#]	- Clear typo when entering settings. - Move up to higher menu. - Use when escaping from menu setting.
③	Enter, Call	[ENTER]	Use after entering the settings when configuring the terminal environment.
		[CALL]	Visitors use this to ring the interphone bell.
④	Microphone	Convey visitor's voice to door phone.	
⑤	LED Lamp	Show operation status like Power Supply, Lock Status and Card Contact.	
⑥	Fingerprint Input Window	Fingerprint input.	
⑦	IRED Sensor	Person's approach automatically turns on button LED and LCD window with ID input screen.	
⑧	Card Input Area	Card input.	
⑨	Speaker	Voice output.	





1.3. Screen (during operation) Description

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

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



	- Initial screen.
	- Waiting for a user's ID to be input.
	- Fingerprint input.
	- Password input.
	- Successful authentication.
	- Authentication failed.
	- When a non-registered user ID is entered.
	- When connection mode is SN and 1:N identification is tried - even though there's no user allowed for 1:N identification.
	- There is no response from the server during the authentication process.
	- Network to server is disconnected during the authentication process.
	- There is no user registered on the terminal, or no connection to the server, so it's trying to connect.
	- Waiting for card to be input.

	- A registered user tried authentication at a time when access is not allowed.
	- Waiting for a reply from the server for authentication.
	- Terminal is locked. - It is not a mealtime - when in meal control mode.
	- Terminal program is in upgrade mode. <b>(power must not be turned off while this message is displayed).</b>

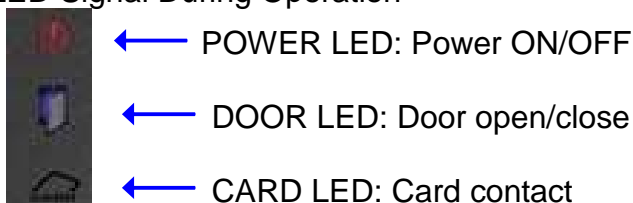
#### 1.4. Voice Information During Operation

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

#### 1.5. Buzzer Sound During Operation

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

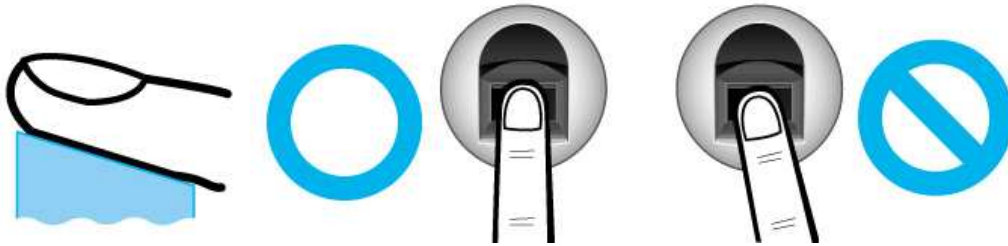
#### 1.6. LED Signal During Operation



## 1.7. Correct fingerprint registration and input methods

- Correct fingerprint registration method

Place your index finger on the window just as you would with a finger stamp. Touching with a fingertip is not an appropriate registration or input method. Make sure the centre of your finger touches the window.



- Use your index finger, if possible.

The index finger guarantees an accurate and stable fingerprint input.

- Check if your fingerprint is clear and undamaged. It is tricky to recognise prints from dry, wet, unclear, or injured fingers. If this is the case, use another finger.



- Cautions about fingerprint condition

The condition of a user's fingerprint could affect its usefulness and may cause it to be unrecognized.

- If the fingerprint is damaged or unclear, it will not be recognised. In this case, please use a password instead.
- When a finger is dry, breathe on the finger for a smooth operation.

- For kids, it may be tricky or impossible to use the terminal because their fingerprints are too small or undeveloped. It is recommended you 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's more convenient to register 2~3 fingerprints.
- It is recommended you register more than 2 fingerprints.

## 2. Introduction

### 2.1. Features

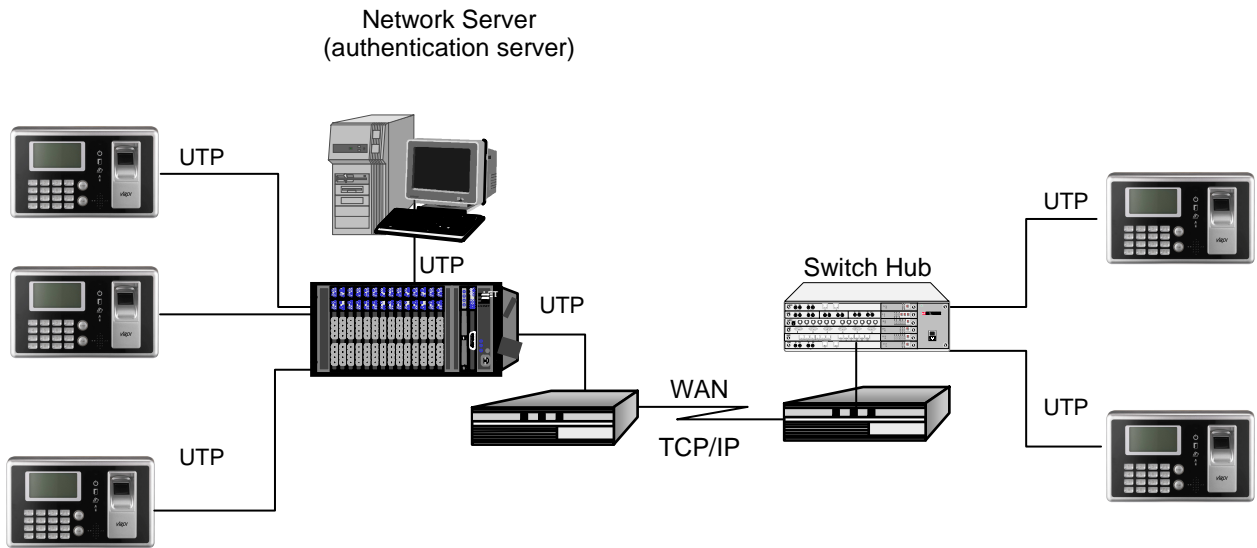
- Access control system using LAN
  - Communication between the unit and authentication server is done via a UTP cable and TCP/IP protocol, so an existing LAN can be used as it is. It guarantees network-based administration and monitoring as well as easy expansion, high reliability, and higher speed.
- Convenient Auto Sensing function
  - Simple authentication process without any key input; simple fingerprint touching is sufficient.
- Simple authentication using fingerprints
  - Fingerprint authentication technology protects users from forgotten passwords or cards, stolen keys or cards, etc., which is a good way to improve security levels.
- High processing capacity of terminal and server
  - There is not any limit on management of users' access information in cases where an access server is used. Even in standalone operation, by using the local terminal, it is possible to manage fingerprint authentication of more than 8,000 users (in optional cases).
- Various information messages
  - 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 when it's dark.
- Door phone
  - Easy visitor identification and convenient response.
- Various and flexible access controls
  - No risk of loaning, forgery, or loss of keys or cards.
  - Perfect control by assigning different security clearances to each user or group.
  - Flexibility provided by allowing limited time for entry/exit.
  - Low maintenance.
  - No need to issue cards for visitors.
- Various applications including access control, time & attendance, meal control, etc.
  - Various operation modes depending on the terminal menu settings.

- Enhanced security with detection of fake fingerprints
  - Adopted detection technology of fake finger enhances security levels.
- Various registration and authentication methods
  - There are a total of 11 registration and authentication methods (4 methods if the card reader is not installed). You are required to select one method before registering users and an administrator.

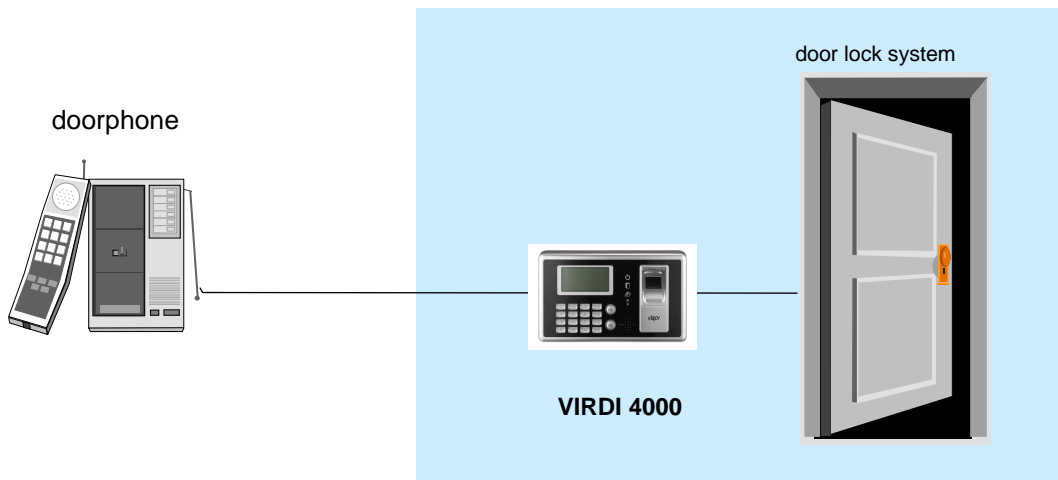
FP	Fingerprint registration. Fingerprint authentication.
ID&PW	Password registration. Password authentication after ID input.
FP/PW	Fingerprint and password registration. Fingerprint or password authentication.
FP&PW	Fingerprint and password registration. Password authentication after fingerprint authentication.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

## 2.2. Configuration

### 2.2.1. Network configuration



### 2.2.2. Standalone configuration





## 2.3. Specification

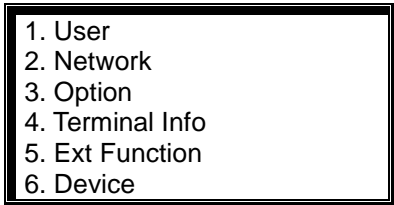
Item	Specification	Remarks
CPU	32-Bit RISC CPU	
Memory	8M SDRAM	
	4M Flash (Default)	6,880 fingerprints
	8M Flash (Option)	16,160 fingerprints
Fingerprint Sensor	Optical	
Authentication Speed	<1 second	
Scan Area / Resolution	12.9 * 15.2mm / 500 DPI	
FRR / FAR	0.1% / 0.001%	
Communication Port	TCP/IP, RS-232, Wiegand	
	RS-485 (Option)	
Temperature / Humidity	-10°C ~ +50°C Lower than 90% RH	
LCD	128 x 64 Graphic LCD	
Dimensions	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. Device Configuration Settings

### 3.1. Check items before device configuration settings.

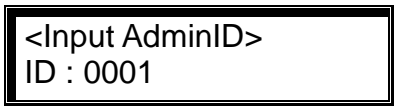
#### 3.1.1. Entering menu

The following screen appears when [\*] is pressed and held for over 2 seconds.



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

Press a numeric key to move to a submenu. The following administrator authentication allows for entry into submenu.



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

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

#### 3.1.2. Changing setting parameters

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

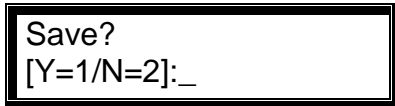
Press [0] to see menus not shown in the LCD window, and press the corresponding numeric key to select a menu.

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

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

### 3.1.3. Saving device configuration settings

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



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

- If there are no changes in device configuration settings, it moves out from this setting mode without displaying the above screen.
- If there is no input for a certain period of time, while changing the device configuration settings, the setting process finishes. If there are changes in device configuration settings, the above screen "Save?" appears. If not, it moves out from this setting mode and the initial screen appears.

3.2. Menu configuration

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

<p>4. Terminal Info</p>	<p>Terminal ID=0001                  Version=10.51.00                  Application=Access                  Language=ENG                  Mode=NS                  Network Type= Static(1)                  Mac-Address=000265201111                  IP Address=192.168.0.3                  Gateway=192.168.0.1                  Subnet Mask=255.255.255.0                  Server IP=192.168.0.2                  Svr-Port==2201                  Card Reader=None                  FP-Sensor=FOS01                  1:1 Level=4                  1:N Level=5                  Max User=0                  MAX FP=0                  All User=0                  All Admin=0                  All FP=0                  1:N User=0                  1:N FP=0                  All Log=0                  DipSwitch=000000</p>	
<p>5. Ext functions</p>	<p>1. Lock Terminal                  2. Read Card No.                  3. Fire Sensing Check</p>	
<p>6. Device</p>	<p>1. Set Fn-Key</p>	
	<p>2. Card Reader</p>	
	<p>3. FP-Sensor</p>	<p>&lt;1:1 Level&gt;                  &lt;1:N Level&gt;                  &lt;I-Capture&gt;                  &lt;Similar FP check&gt;</p>
	<p>4. Wiegand</p>	<p>&lt;Wiegand Out&gt;                  &lt;Site Code&gt;                  &lt;Bypass&gt;</p>
	<p>5. System Config</p>	<p>&lt;ID Length&gt;                  &lt;Language&gt;</p>
	<p>6. Initialise</p>	<p>1. Init Config                  2. Delete Log                  3. Init Terminal</p>

### 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 already exists, it moves to the upper menu with a “ppibig” sound. If not, selection screen for the following authentication method 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 amongst the 11 registration methods.

##### 3.3.1.1. “1. FP” registration

Fingerprint registration and fingerprint authentication

- ◆ [\*] → [1] → [1] → User ID [ENTER] → [1] → 1:1 Level [ENTER]  
→ Enable 1:N [ENTER] → Input FP → Input the same FP again ◆

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

Recommended setting: '0'

Different authentication levels can be assigned to different users. If the authentication level for a user is set to '0', the authentication level for the terminal is changed, the applied authentication level for all users set to '0' is simultaneously changed.

Press [ENTER] to move to the next setting.

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

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

When there are not many users, or for the convenience of a specific user, a fingerprint only without ID can be used for authentication. For authentication without ID, it shall be set to '1'. For authentication with ID, it should be set to '0'.

Press [ENTER] to enter fingerprints.

```
<Add FP>
Input Your FP
```

A “ppiririck” buzzer sound rings twice and a light on the fingerprint sensor turns on. Place a finger onto the fingerprint input window and wait for 2~3 seconds until the light turns off and the fingerprint is saved.

Please note that the same fingerprint must be input twice. To enter the same fingerprint again, remove the finger from the window and place the same finger again onto the window.

If registration succeeds, a “ppiririck” buzzer sound rings. Then, it returns to the “1.Add” screen. If the fingerprint image is not in good condition or there is no input in the window for 10 seconds after the fingerprint sensor light turns on, it returns to the “1. Add” screen with a failure buzzer sound “ppibig”.

If the fingerprint to be registered is in bad condition, try to repeat the registration process 2 or 3 times or register another fingerprint. For the remarkably few people having fingerprints in bad condition, which are not properly accepted for the registration process, 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.

- ◆ [\*] → [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 confirmation.

If registration succeeds, a “ppiririck” buzzer sound rings. Then, it returns to the “1.Add” screen. If they are different, a “ppibig” buzzer sound indicates failure rings and the “1.Add” menu screen appears.

#### 3.3.1.3. “3. FP/PW” registration

After both fingerprint and password are registered, authentication method is selectable as either fingerprint or password.

- ◆ [\*] → [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 ◆

As mentioned above, password registration (refer to ② “2. ID&PW” registration) precedes fingerprint registration (refer to ① “1. FP” registration).

#### 3.3.1.4. “4. FP&PW” registration

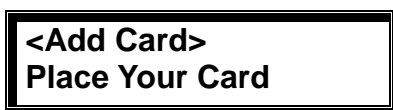
After both fingerprint and password are registered, fingerprint authentication and password authentication are needed for access. Fingerprint authentication precedes password authentication.

- ◆ [\*] → [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 ◆

#### 3.3.1.5. “5. RF” registration

Card registration and card authentication.

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



To cancel registration, press the [#] button.

If a user places the card close to the unit, a “ppiririck” buzzer sounds on successful registration. “1. Add” menu appears.

#### 3.3.1.6. “6. RF/FP” registration

After both card and fingerprint are registered, authentication method is selectable as either card or fingerprint.

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



Card registration (refer to ⑤ “5. RF” registration) precedes fingerprint registration (refer to ① “1. FP” registration).

#### 3.3.1.7. “7. RF&FP” registration

After both card and fingerprint are registered, card authentication and fingerprint authentication are needed for access. Card authentication precedes fingerprint authentication.

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

Card registration (refer to ⑤ “5. RF” registration) precedes fingerprint registration (refer to ① “1. FP” registration).

#### 3.3.1.8. “8. RF/PW” registration

After both card and password are registered, authentication method is selectable as either card or password.

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

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

#### 3.3.1.9. “91. RF&PW” registration

After both card and password are registered, card authentication and password authentication are needed for access. Card authentication precedes password authentication.

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

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

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

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

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

If a user finds it difficult to input their ID, a card can be used instead of ID

input for authentication.

Card registration (refer to ⑤ “5. RF” registration) precedes fingerprint registration (refer to ① “1. FP” registration).

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

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

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

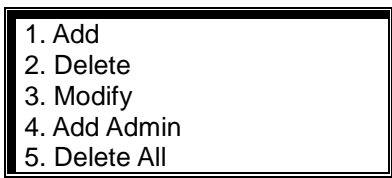
If a user feels difficult in inputting ID, a card can be used instead of ID input for authentication.

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

### 3.3.2. Deleting User

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

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



To delete user, press [2].

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

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

Caution is required when deleting a user or an administrator as there is not any different procedure for deleting their information. Also, note carefully that user’s information stored just in the local terminal – not in the server – is not recoverable after deletion is complete.

### 3.3.3. Modifying User

- ◆ [\*] → [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].

There is no difference for modifying a general user's or administrator's information.

#### 3.3.3.1. "1. FP" user

For users who registered only their fingerprints for access, they can modify 1:1 authentication level and add other fingerprints.

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's an attempt to add more than 5 fingerprints, a "ppibig" buzzer sound rings when [2] is pressed.

[1] When modifying 1:1 authentication level is selected.

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

Recommended setting: '0'

To change this value, press the [#] to delete the current value and enter the new value.

[2] When registering additional fingerprints is selected.

<Add FP >
Input Your FP

This is same as 'Add FP' in 3.3.1.1. "1. FP" registration. The same fingerprint must be input twice.

If additional fingerprint registration succeeds, a "ppiririck" buzzer sounds. If not, a "ppibig" buzzer sounds and the "1. Add" menu appears.

### 3.3.3.2. "2.ID&PW" user

When a user wants to change their password.

1. Modify PW

To modify a password, press [1]. To cancel this operation, press [#].

Press the [1] button to modify the password.

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

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

Press [ENTER] after inputting the password.

<Confirm PW>  
PW: \_ \_ \_ \_ \_

Input the same password once more for confirmation.

Press [ENTER] to confirm the password.

If password modification succeeds, a "ppiririck" buzzer sounds. If not, a "ppibig" buzzer sounds 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 [0] to see menus not shown in the LCD window.

To cancel, press the [CLR] button.

Press the [1] button to modify 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 modify password (refer to "3.3.3.2").

### 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 "ppirrick" buzzer sounds if the modification is successful 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 modify 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 modify password (refer to "3.3.3.2").

Press the [2] button to change the card (refer to "3.3.3.4").

### 3.3.4. Administrator registration

◆ [\*] → [1] → [4] → Admin 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
---

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 those for user registration.

Make sure to register the new administrator as the registered administrator. The registered administrator can change the terminal configuration settings, including registration/modification/deletion of user information.

### 3.3.5. Delete All Users

◆ [\*] → [1] → [5] ◆

In the main menu, press [1] to select "1. User". Using the button [0], you can scroll through the hidden menu.

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 succeeds, a "ppiririck" buzzer sounds 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 this setting is done, press [ENTER] to move to the next setting.

#### 3.4.1. Terminal ID settings

◆ [\*] → [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' and NO mode: '2'

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

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

Depending on the number of terminals, number of users, or network conditions,

each mode can be used flexibly. 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

◆ [\*] → [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 static IP is assigned to the terminal from present network system, press [0]. If there is a DHCP server in network system from which a dynamic IP is assigned to the terminal, press [1].

Press [ENTER] to move to the next setting.

※ For Static IP settings, refer to '3.4.4. IP address', '3.4.5. Subnet mask' and '3.4.6. Gateway'. For dynamic IP, there's no need for additional settings.

### 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 server 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.

The default port number of the authentication server 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]
```

After the network setting is complete, press the [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].

◆ [\*] → [3] → [1] ◆

```

Application:0
0=Access Ctrl
1=T&A Ctrl
  
```

The default is '0=Access Ctrl'.

For Access Control application, set as '0'. For Time & Attendance, set as '1'.

Press [ENTER] to move to detailed settings for each operational mode.

##### 3.5.1.1. [0]: Access Control

There are no detailed settings under Access Control application. Moves to the upper menu.

##### 3.5.1.2. [1]: Time Attendance control

By setting up the default times relating to Start/Leave/Out/Back, the terminal display mode, after authentication, can be automatically changed to program time & attendance. In addition, by using the multi-Fn keys, over 40 sub modes of Time & Attendance 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. If the authentication for "not at work" (Out) happens by pressing [F3] function key, the terminal display mode after the authentication of "not at work" automatically changes to start time mode, which

is very convenient when using time & attendance mode.

After setting <start time>, set <leave time> and <normal time> in the same manner. Note that each time must not overlap.

Example: start time:06:00~09:59, leave time:17:00~22:00 and normal time:10:00~16:59

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

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

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

Default setting: all 'X'

This menu is useful when more than 5 time & attendance modes are necessary.

- When setting as X: each function key represents a specific working mode such as F1=Start, F2=Leave, F3=Not at work (out) and F4=Back. When a function key is pressed, authentication mode changes to the corresponding working mode.
- When setting as O: a mode is defined by the combination of a function key and a number key such as “F3+1”. For example, if the setting is 1=F1: X 2=F2: X 3=F3: X 4=F4: O, 14 different working modes can be defined according to user input such as [ENTER]: normal, [F1]: start, [F2]: leave, [F3]: not at work (out), and [F4]+'0'~[F4]+'9'.

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

### 3.5.2. Option settings for authentication

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 basic option for authentication, press [2].

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

◆ [\*] → [3] → [2] ◆

<Show User ID> (0-2):0
---------------------------

Default setting: '0'

If set to the default setting '0', only the "Success" message is displayed. When set to '1', the user ID is displayed in the LCD window when authentication is successful; as shown below. When set to '2', the user name appears in the LCD window when authentication is successful; as shown below.

Example: OK! &lt;0001&gt;

Example: Smith, you are authorised.

Press [ENTER] to move to the next setting.

## 3.5.2.2. Settings for card authentication only.

◆ [\*] → [3] → [2] → [ENTER] ◆

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

Default setting: '0'

If a user is registered to be authenticated with a Card & Password, or a Card & Fingerprint, and if set to '1', they can only get access to an area, via the relevant terminal, by using a card.

This function is useful at a building entrance door – and other positions in a building with several installed terminals - where there is frequent entry and exit and no need for high security access control.

Press [ENTER] to move to the next setting.

## 3.5.2.3. 1:N authentication settings

◆ [\*] → [3] → [2] → [ENTER] → [ENTER] ◆

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

Default setting: '1'

This enables fingerprint authentication without inputting a user ID, or using a card. For your information, even if a user is registered to be authenticated with

1:N authentication, only 1:1 authentication is allowed in the terminal if this is set to '0'.

In cases when ID input or fingerprint authentication after placing a card – when card input replaces ID input – is unavoidably needed, it should be set to '0'.

The following are detailed settings about whether 1:N authentication is allowed or not.

① When 1:N authentication is allowed if set to '1'

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

Default setting: '0'

If set to '1', the first part of the User ID input stands for a specific group. This speeds up 1:N authentication by searching for fingerprints only amongst that specific group. This faster matching speed is very useful when there are over 1,000 users registered.

If set to '1', as mentioned above, fingerprint matching is only executed amongst the User Group starting with the same first part of User ID. If set to '0', numbers input are considered just as the User's ID and only 1:1 authentication is executed.

For example, when a user ID is a 4-digit number and '12' is input for authentication, if set to '1', 1:N authentication is performed amongst user ID's '1200'~'1299'. If set to '0', 1:1 only authentication for User ID No. 12 is performed.

② When 1:N authentication is not allowed set to '0'.

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

Default setting: '0'

If set to '1', for successful authentication, all registered fingerprints should be authenticated after ID (or card) input.

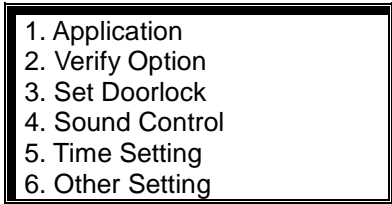
This is used when a higher security level is required for special areas. If a user of 'ID 0001' has 3 fingerprints registered to the unit, all 3 fingerprints should be authenticated after ID input.

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

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

### 3.5.3. Doorlock settings

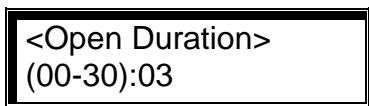
In the main menu, press [3] to select "3. Option" and the following screen appears:



Press [3] for door settings.

#### 3.5.3.1. Door opening time settings.

◆ [\*] → [3] → [3] ◆



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

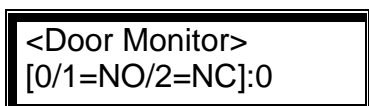
This is used to set the door opening time after authentication is successful. This only applies to the door opening time for strike type locks and not applicable to dead bolt type locks or automatic doors.

If set to '00', the door in access control mode is not controlled. Therefore, the '00' setting is only possible for time & attendance mode, where there's no need for lock control.

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

#### 3.5.3.2. Door status monitor

◆ [\*] → [3] → [3] → [ENTER] ◆



Default setting: '0'

- '0': NW – No monitoring
- '1': NO – Dead bolt type lock or automatic door
- '2': NC - Strike type lock

'0' setting is for no monitoring, '1' setting is for dead bolt type locks or

automatic doors and '2' setting is for strike type locks. When set to '1' or '2', the door status, via connected terminal, is periodically transmitted to the server.

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

### 3.5.3.3 Door open alarm settings

◆ [Fn] → [3] → [3] → [ENTER] → [ENTER] ◆

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

Default setting: '00'

The terminal checks if the door has been left open for longer than this setting time – from 5 seconds minimum to 30 seconds maximum. Opening for longer than this setting time sounds an alarm. If set to '00', there is no alarm sound. If set from '01' to '04', there is no alarm sounded until the door has been open for at least 5 seconds.

There could be an unexpected problem which prevents the door from closing. In such cases, this alarm helps the relevant personnel (administrators) check what has caused the problem and eliminate it.

For a smooth operation, the relevant lock should be a type capable of monitoring whether the door is open or closed. The lock monitoring output should be properly connected to the terminal. The previously mentioned setting for monitoring door status should be set to '1' or '2' for this operation.

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

### 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 enable voice control information from the terminal, set to '1'. If not, set 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 sets the terminal buzzer volume. When set to '0', there is no buzzer sound. '1' setting means low volume and '2' means high volume.

Press [ENTER] to move to the next setting.

#### 3.5.4.3. Case open alarm settings

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

Default setting: '1'

An alarm sounds if the terminal case is damaged or opened. For this setting, the VIRDI 4000 series have a case open sensor installed.

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

#### 3.5.5. Current time settings

◆ [\*] → [3] → [5] ◆

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

```
<Time Setting>
20060401211806
```

This sets 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.

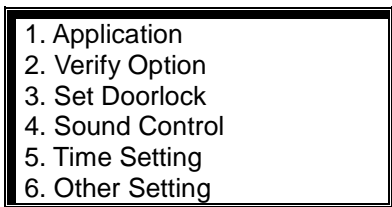
Press [ENTER] to check that the current time is updated and move to the upper



menu.

### 3.5.6. Other setting

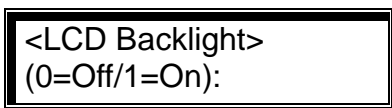
In the main menu, press [3] to select "3.Option". Press [6] to see the following screen:



Press [6] for other settings.

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

◆ [\*] → [3] → [6] ◆



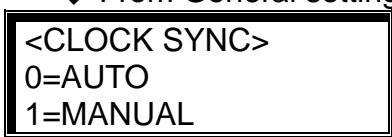
Default setting : '0'

This sets the LCD backlight. If set to '1', the LCD backlight is on all the times. However, if set to '0', the LCD backlight is normally off and a keypad operation or placing a card turns the backlight on. After 10 seconds have passed with no relevant terminal operation, backlight turns off.

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

#### 3.5.6.2 Clock Sync

◆ From General setting: [\*] → [3] → [6] → [ENTER] → [ENTER]



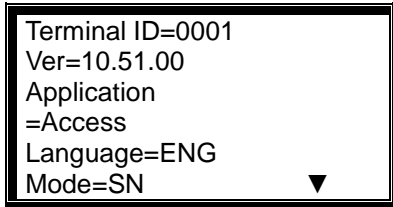
Default setting : '0'

If set to '0', Time is synchronised with the connected server.  
If set to '1', Time from terminal is activated by the RTC.

## 3.6. Terminal information view

◆ [\*] → [4] ◆

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



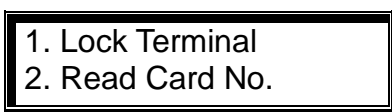
Press [0] to scroll up and down the screen.

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 (static IP/dynamic 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	Card reader type.
Card Reader Version	Card reader firmware version.
FP-Sensor	Fingerprint sensor type.
1:1 Level	Identification level for 1:1 authentication.
1:N Level	Identification level for 1:N authentication.
Max User	Maximum user capacity to be able to be registered to a terminal.
Max FP	Maximum fingerprint capacity that can be registered to a terminal. For example, if there are 100 registered users and two fingerprints per user are registered, it means a total of 200 fingerprints are 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.
Dip Switch	Dip Switch setting status in a terminal.

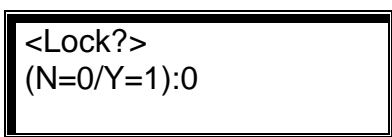
### 3.7. Extra functions

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



#### 3.7.1. Terminal lock settings

◆ [\*] → [5] → [1] ◆



Default setting '0': Releasing terminal lock  
'1': Setting terminal lock

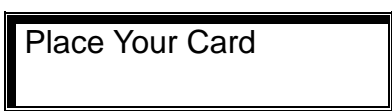
An administrator at a local terminal – not by server program – can directly set up or release the terminal lock of a local terminal. If set to '1', the terminal is locked and nobody can access specific areas via the locked terminal until the administrator unlocks it.

※ For this setting, 'Allow admin to access' in terminal configuration of server program should be permitted.

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

#### 3.7.2. Read card number

◆ [\*] → [5] → [2] ◆



This is an extra function which is unrelated to terminal configuration settings. By

using this function, an administrator can read a card number when it is placed on the terminal mounted card reader. This is to register the placed card with the server. When this LCD screen pops up and an administrator places a card on the terminal, the card number shows in the LCD screen.

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

### 3.7.3. Fire Sensing Link

◆ [\*] → [5] → [3] ◆

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

Default setting: '0'

Linking a Fire Sensor with the terminal. On sensing a fire, send a fire-sensing signal to switch the door to open.

After setting, press [Enter] to upper menu.

## 3.8. Device settings

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

In most cases there is no need to modify the device settings after installation. Therefore, be careful not to modify the device settings without any obvious reasons.

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

This previously factory set password is to call administrator's attention, and is fixed and should not be changed.

Input '084265' as the previously set password and press [ENTER] to show the detailed setting items.

### 3.8.1. Function key settings

◆ [\*] → [6] → '084265' [ENTER] → [1] ◆

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

Default setting: all '0'

This is to enable or disable the function keys. 'O' means enabling the function key and 'X' means disabling the function key. Whenever the number conforming to a function key in this setting is pressed, the setting is changed from 'O' to 'X'.

In this setting, 1 is for [F1], 2 is for [F2], 3 is for [F3] and 4 is for [F4]. For example, if an administrator presses [1] once in this setting the [F1] key is disabled - [X], a user cannot enter into start mode by pressing the [F1] key button as the [F1] key is now disabled.

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

6 is used for setting detection function for fake fingerprints.

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

### 3.8.2. Card reader settings

#### 3.8.2.1. Card reader type setting

◆ [\*] → [6] → '084265' [ENTER] → [2] ◆

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

Default setting: '0'

This is to set the card reader mounted in a terminal. Refer to the followings for correct setting:

- '0': No card reader
- '1': Low-frequency RF Card reader mounted
- '2': High-frequency smart card reader
- '3': Wiegand card reader, such as HID card module
- '4': Other smart RF reader
- '5': External card reader

If a card reader is mounted within a terminal and the above setting is correctly done, when [F1]~[F4] or [ENTER] is pressed, the authentication mode is changed and 1:1 fingerprint authentication is ready for operation - in this case, 1:N fingerprint authentication is not performed except for the auto sensing setting.

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

### 3.8.2.2 Card Reader format setting

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

Default setting: '0'

Set card data format from card reader.

- 0: Hexadecimal data, process with 8byte data value.
- 1: Hexadecimal data, process with 16byte data value.
- 2: Process with Decimal data value.

### 3.8.3. Fingerprint sensor settings

#### 3.8.3.1. 1:1 verification level settings for a terminal

◆ [\*] → [6] → '084265' [ENTER] → [3] ◆

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

Default setting: '4'

This is to set 1:1 matches the security level for a terminal between the fingerprint captured from the fingerprint input window and the relevant fingerprint stored in a terminal. The higher the 1:1 matching level, the higher the security. But there's a possibility of authentication failures increasing when higher matching rate are required.

For an example of 1:1 authentication with ID input, if inputted ID number is '1234', there is authentication process between the fingerprint captured from the fingerprint input window and the fingerprint associated with ID '1234' in a terminal.

For your information, if a user's 1:1 authentication level is set to '0' – refer to 3.3.1.1. "1. FP" registration, 1:1 matching process for the user is performed according to the 1:1 authentication level (1:1 level of a terminal) assigned through "3.8.4.1. 1:1 authentication level for a terminal". If a user's 1:1 authentication level is set to another level, except for '0', the 1:1 matching process for the user is performed according to their own 1:1 level.

Press [ENTER] to move to the next setting.

#### 3.8.3.2. 1:N identification level settings

◆ [\*] → [6] → '084265' [ENTER] → [3] → [ENTER] ◆

1:N Level  
(3-9):5

Default setting: '5'

This is to set the 1:N authentication security level between the fingerprint captured from the fingerprint input window and all fingerprints in a terminal which are allowed for 1:N authentication.

For your information, 1:N authentication level is not set for respective users but only for a terminal.

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 to automatically enhance good fingerprint detection capability by reducing bad influences coming from humid fingers and/or residual fingerprints which are left on a sensor window due to sweat and/or contaminants on fingertip.

- If it is set to '0', fingerprint capturing time is shorter but the authentication rate for dry or wet finger becomes lower.
- If it is set to '1', fingerprint capturing time becomes longer than that of the '0' setting but the authentication rate increasing. Therefore, a '1' setting is recommended.

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

### 3.8.3.4. LFD Label Setting

<LFD>  
(0-3):0

Default setting: '0'

When setting the fake fingerprint level to 0, security levels are comparably low. If 3, security level is the highest.

After input set value [ENTER] to upper menu.

## 3.8.4. Wiegand output settings

◆ [\*] → [6] → '084265' [ENTER] → [4] ◆

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

Default setting: '0'

The default setting is '0'. If Wiegand output from the local terminal is needed for external access controller with Wiegand input, an administrator can set this setting as '1' or '2'.

- In case of '1' setting, "site code [1 byte] and user ID [2 bytes]" are transmitted through Wiegand output port. User ID should be set as less than 4 digits.
- In case of '2' setting, "site code [1 byte] and user ID [3 bytes]" are transmitted through Wiegand output port. User ID should be set as less than 7 digits.

- ※ This setting is not related to external Wiegand reader.
- ※ In cases of '1' or '2' settings, the below-mentioned site code should be set.

<Site Code>
(0-255):000

Default setting: '000'

An administrator can assign the site code, from 0 to 255, which is transmitted together with a user ID.

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

<Bypass>
0=Off
1=Wiegand
2=Terminal

Default setting: '0'

1. Data input Wiegand data is printed as wiegand
2. Input card data from terminal is printed as wiegand

## 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 configuration settings.



## 3.8.5.1. User ID length settings

◆ [\*] → [6] → '084265' [ENTER] → [5] ◆

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

Default setting: '4' digits

This ID length can be 2~8 digits and should be the same as that of ID registered in the server program. If the ID registered in the server program is '000075', input 6.

Modifying the ID length to be shorter than before, during normal operation after installation, an administrator may not be able to be authenticated and enter into main menu if they have a longer ID length, compared to the newly modified ID length. Therefore, serious consider the implications of modifying the ID length.

Press [ENTER] to move to the next setting.

## 3.8.1.2. Language settings

◆ [\*] → [6] → '084265' [ENTER] → [5] → [ENTER] ◆

<Language>:1 0=KO 1=EN 2=JP 3=SP 4=CN 5=AR 6=IT 7=VT 8=TA 9=PO
--

Default setting: '1' (English)

Voice message are set from this menu.

'0':Korean, '1':English, '2':Japanese, '3':Spanish, '4':Chinese, '5':Arabic,  
 '6':Italian, '7':Vietnamese, '8':Thai '9':Polish.

If 0~3, Language from LCD will be displayed as Korean, English, Japanese, Spanish. If 4~9, voice message will be English.

Voice output languages are as follow, '0': Korean, '1': English, '2': Japanese, '3': Spanish, '4': Chinese and '5':Arabic.

'0'~'2': LCD characters correspond to the assigned language.

'3'~'5': LCD characters are English.

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

## 3.8.6. Terminal initialisation

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

### 3.8.6.1. Configuration settings initialisation

◆ [\*] → [6] → '084265' [ENTER] → [6] → [1] ◆

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

To initialise configuration settings, press [1]. If not, press [2].

All the configuration settings except for Mac (physical) address are initialised; users' information and authentication records are not deleted.

※ If this configuration settings initialisation is done, the language for voice output and display characters change to English. If you need to set as another language, refer to the following: “6. Set Device” → “1. System Config” → <Language>: set to 0~4”

After this configuration setting initialisation is successfully done, it moves to the upper menu together with a “success” buzzer sound.

### 3.8.6.2. Authentication record initialisation

◆ [\*] → [6] → '084265' [ENTER] → [6] → [2] ◆

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

To initialise the log data, press [1].  
 If not, press [2].

All the log data related to authentication is deleted; configuration settings and users' information are not deleted.

After this initialization is successfully done, it moves to the upper menu together with a “success” buzzer sound.

### 3.8.6.3. Factory default initialisation

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

To initialise everything to factory default, press [1]. If not, press [2].

Except for the Mac (physical) address stored in the terminal, all configuration

settings, users' information and authentication records (log data) are deleted, which is factory default.

- ※ If this factory default initialisation is done, the language for voice output and display characters change to English. If you need to set as another language, refer to the following: "6. Set Device" → "5. System Config" → <Language>

After this initialisation is successfully done, the terminal is rebooted with a "success" buzzer sound.






## 4. How to use the terminal

### 4.1. Access control application

- Menu "3.Option" → "1.Application" → [0] for access control application

#### 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]

※ In the access control application, the authentication process mainly happens in normal mode by pressing the 'Enter' button, or using auto sensing without pressing any keys. For more detailed operation on the access control application, an administrator can specify F1, F2, F3 and F4 modes at their discretion as F1, F2, F3 and F4 modes are not set as fixed modes.

- Fingerprint authentication

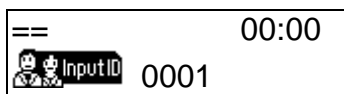
Fingerprint authentication to a corresponding mode; by pressing one of the function keys: 'Enter', F1, F2, F3 and F4.

Fingerprint authentication through auto sensing; without pressing any keys. This authentication is performed in the mode displayed on the screen.

- Password authentication  
After inputting the user ID, and changing the authentication mode by pressing the corresponding function key, input the password for authentication.
- Card authentication after the following settings are done: menu → “6.Device” settings → “3.Card reader” → <Card Reader> is set to [1] or over  
Pressing the function key changes just the authentication mode. For card authentication, press the corresponding function key and then place the card close to the terminal.

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

- ▶ When auto sensing is running, input ‘0001’ if the user ID is ‘0001’ and then place your finger close to the fingerprint sensor. The light on the fingerprint input window turns on to detect the fingerprint and the authentication result is displayed on the LCD window.
- ▶ If the user ID is ‘0001’, input ‘0001’ and press the function key. Voice information such as, ‘please enter your fingerprint’ follows. When a fingerprint is input, the authentication result is displayed on the LCD window.



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



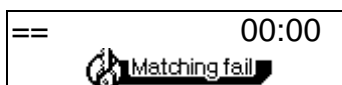
Place your finger close to the input window when you hear the voice message “Please enter your fingerprint”. Do not remove your finger until you hear a “ppig” buzzer sound.



If authentication is successfully done, a success message is displayed on the LCD together with a voice message “You are authorised”. The door LED turn on and door relay runs.

The default screen appears after 1~2 seconds. The door LED turns off and door relay releases after the door open setting time has elapsed.

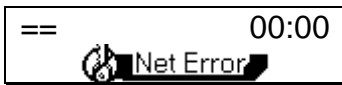
- ※ Error message: The following error message appears together with a voice message “Please try again”.



In case of authentication failure.



Non-registered user ID.



During the authentication request to the authentication server, a network problem occurred or the network was disconnected.

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

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

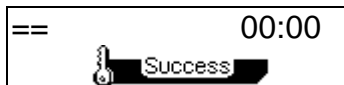
- ▶ If a user places their finger close to the fingerprint sensor when auto sensing is running, the light on the fingerprint input window turns on to detect the fingerprint and the authentication result is displayed on the LCD window.
- ▶ When you press the function key, voice information like 'please enter your fingerprint' follows. When a fingerprint is input, the authentication result is displayed on the LCD window.



In the main screen, press the function key.

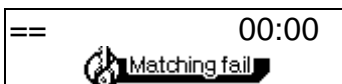


Place your finger close to the input window when you hear the voice message "Please enter your fingerprint". Do not remove your finger until you hear a "ppig" buzzer sound.



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

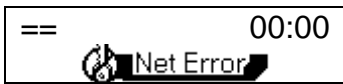
※ Error message: The following error message appears together with a voice message "Please try again".



In case of authentication failure



If the connection method is SN – refer to 3.4.2. Connection [NS / SN / NO] mode settings - and there is no user to whom 1:N authentication is allowed in the terminal.

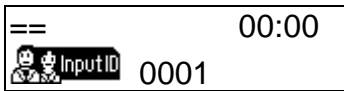


During authentication request to the authentication server, a network problem occurred or the network was disconnected.

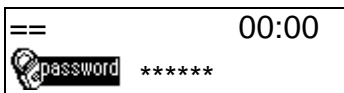
- ▶ In case of users who are registered as [fingerprint & password], the correct password input is required after successful fingerprint authentication.

#### 4.1.4. Password authentication

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



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



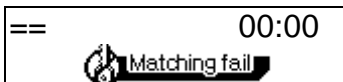
The terminal waits for the user password to be input after which a "ppiririck" buzzer sounds. Input the relevant password and press [ENTER]. For security reasons, the password is displayed as '\*' on the LCD screen, not the actual numbers.



If authentication is successful, a success message is displayed on the LCD together with a voice message "You are authorised". The door LED turns on and door relay runs.

The default screen appears after 1~2 seconds. The door LED turns off and door relay releases after the door open setting time has elapsed.

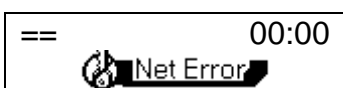
- ※ Error message: An error message appears together with the voice message "Please try again".



In case of authentication failure.



Non-registered user ID.



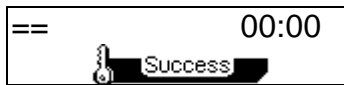
During authentication request to the authentication server, a network problem occurred or the network was disconnected.

4.1.5. Card authentication

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



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



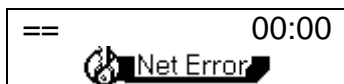
If authentication is successful, a success message is displayed on the LCD together with a voice message “You are authorised”. The door LED turns on and door relay runs.

The default screen appears after 1~2 seconds. The door LED turns off and door relay releases after the door open setting time has elapsed.

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



Non-registered card.



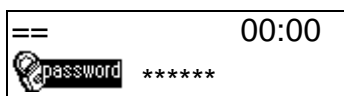
During authentication request to the authentication server, a network problem occurred or the network line disconnected.

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



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

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



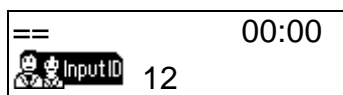
After a “ppirirrick” buzzer sound, the terminal waits for the user password to be input. Enter password and press [ENTER].

#### 4.1.6. User ID group authentication

User ID group authentication is performed from among users grouped with the same first digit and/or above user ID – at least one digit. This authentication can be conveniently used if there are lots of users and the matching time for 1:N authentication takes too long. In the menu set, as below: 3. Option settings → 2. Authentication method settings → <1:N authentication>=1 → <ID group authentication >=1.

For information, refer to the following on how to use this authentication in more detail.

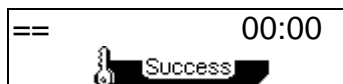
If the relevant ID for a user is 1234, enter only 12 for this authentication. The matching is performed from users having IDs of 1200 to 1299; all starting with 12. If the ID is “0012”, enter “0012” or “00” for authentication.



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



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



If authentication is successful, a success message is displayed on the LCD together with a voice message “You are authorised”. The door LED turns on and door relay runs.

The default screen appears after 1~2 seconds. The door LED turns off and door relay releases after the door open setting time has elapsed.

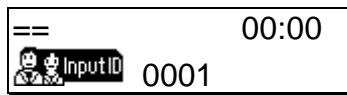
#### 4.1.7. Multiple fingerprint authentication

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

For example, if the ID “0001” is registered with three different fingerprints, all three fingerprints must be authenticated for access after ID input. A single authentication failure in mid course results in overall failure and the whole authentication process should be restarted. This iterative process continues until all three fingerprints are authenticated.



▶ If the user ID is “0001”, input “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.” - when auto sensing runs, fingerprint only input is sufficient for authentication. When a fingerprint is input, the authentication result is displayed on the LCD window.



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



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



If authentication is successful, a “ppiririck” buzzer sounds and the light on the fingerprint input window turns on together with the voice message “Please enter your fingerprint”. This process is re-iterated until all fingerprints have been input and authenticated.



If authentication is successful, a success message is displayed on the LCD together with a voice message “You are authorised”. The door LED turns on and door relay runs.

The default screen appears after 1~2 seconds. The door LED turns off and door relay releases after the door open setting time has elapsed.

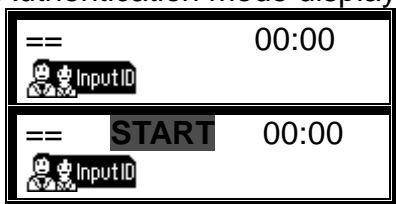
※ Error message is same as that of [1:1] authentication.

#### 4.2. Time & Attendance control

- Menu “3.Option” → “1.Application” → [1] T&A (Time Attendance) settings
- If start and leave time for employees are fixed, set <start time>, <leave time> and <normal time> to reduce user input errors.

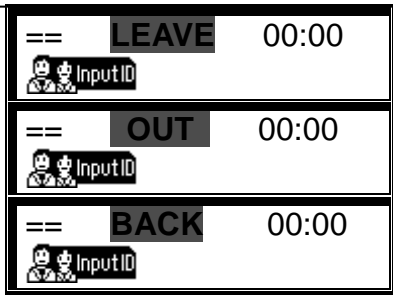
##### 4.2.1. Authentication mode

- 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 which related to specific T & A mode.

If the function key is not used, and authentication process is done in auto sensing, the current mode on the screen works for authentication.

- Password authentication

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

- Card authentication after the following settings are done: menu "6.Device" settings "3.Card reader" (<Card Reader>) is set to [1] or over.

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

- After authentication is done, the working mode returns to the one – start, leave or normal - previously set in the time frames. If no mode is set for the specific time period, the previous authentication mode is maintained.

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

- Same as 4.1.2.

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

- Same as 4.1.3.

#### 4.2.4. Password authentication

- Same as 4.1.4.

#### 4.2.5. Card authentication

- Same as 4.1.5.

#### 4.2.6. User ID group authentication

- Same as 4.1.6.

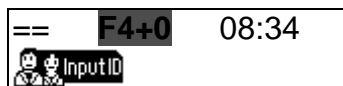
#### 4.2.7. Expansion of working mode by multi-key function

- If more than 5 working modes - start, leave, not in work (out), return (back) and normal - are required, it can be expanded up to 41 modes.

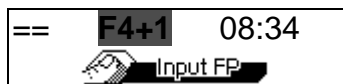
- After setting Menu → 3.Option → 1.Application → [1] T&A, set more than one key to 'O' in <Multi Fn-key> setting. The keys set to 'X' are not applied in this multi-key function.
- As a mode is defined as a function key plus a number key, press a number key after pressing the function key for authentication. In the server program, authentication mode is displayed as a function key plus a number key like "F3+1".
- For example, when [F4] is set to [O] and <start time> is set to "07:00~09:30", if a fingerprint user tries for authentication in "F4+1" mode,



In main 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.