Access Controller NAC-3000R

Terminal User Manual

NITGEN
biometric solutions

FCC NOTICE

THIS DEVICE COMPLIES WITH PART 15 OF THE FCC RULES.
OPERATION IS SUBJECT TO THE FOLLOWING TWO CONDITION:
(1) THIS DEVICE MAY NOT CAUSE HARMFUL INTERFERENCE, AND
(2) THIS DEVICE MUST ACCEPT ANY INTERFERENCE RECEIVED, INCLUDING INTERFERENCE THAT MAY CAUSE UNDERSIRED OPERATION.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communication. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures :

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit difference from that to which the receiver is connected.
- Consult the dealer of an experienced radio/TV technician for help.

NOTE : The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user’s authority to operate the equipment.

CAUTION : Changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

Table of Contents

Chapter 1 Before You Start

Chapter 2 Environment Setup

Chapter 3 How to Use the Terminal

Chapter 1
Before You Start

1.1 About the product

■ Overview

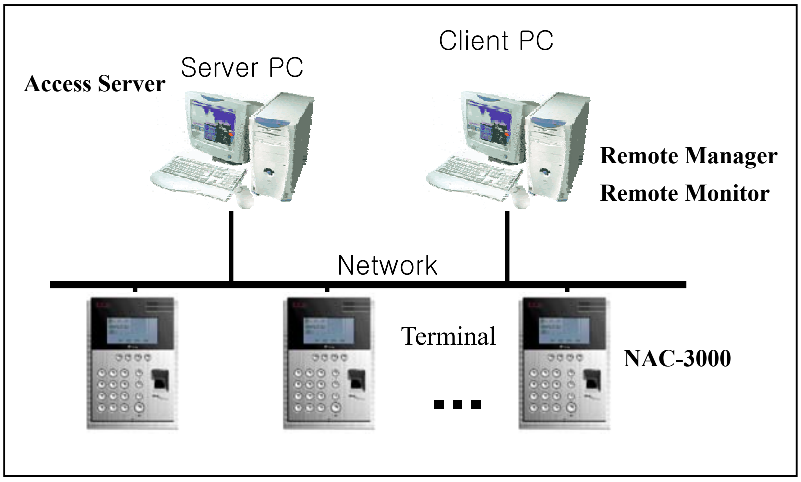
Biometric systems are recently used in various authentication systems. They are increasingly used not only in environments that require high level of security but also in many other places because they are convenient and economical. Among various biometric systems, the fingerprint recognition system takes up most of the market because it is easy to use as well as economical and capable of developing various types of applications. NITGEN, a global leader in the fingerprint recognition industry, provides various fingerprint authentication solutions such as PC security, knowledge management, vaulting service, access control, electronic approval, and financial payment. NITGEN actively responds to customer needs through continuous research, development and quality management.

The NITGEN access control system is an advanced product in which core technologies of NITGEN recognized worldwide such as fingerprint recognition algorithm, optical sensors, embedded design technology, and software application technology are organically combined and optimized. In addition, unlike other existing access control systems that use passwords or ID cards only, it is free from such risks as loss of password and abuse or duplication of card, providing excellent convenience and security. It is designed to maximize operational efficiency, enabling integrated monitoring and systematic management of terminals which have been operated independently on a remote location via the network.

The NITGEN access control system can use various combinations of RF card, password and fingerprint authentication. Designed to meet both universal uses and specific uses, it can be used in various customer environments including enterprises and government agencies due to such convenient built-in features as group ID, short ID, 1:N authentication, interphone and voice instruction.

This manual describes how to use NITGEN’s access control terminal (NAC-3000R).

System configuration



Component	Main Featt ·es
Server PC	1. Server software: Access Sever 2. Terminal communication and log data collection 3. User information and log database 4. Performing authentication
Client PC	1. Client software: Remote Manager/Remote Monitor 2. User registration and management 3. Monitoring terminal status and events
Terminal (NAC-3000R)	1. Performing user authentication 2. Door control

You can use all features with the NITGEN access control terminal (NAC-3000R) only. If you use it with the management programs (Access Server, Remote Manager and Remote Monitor) in network environment, you can manage a number of terminals more easily and efficiently. You can use the server and client software in one PC.

1.2 Features and specifications

■ Product features

The NITGEN access control system (NAC-3000R) has the following features:

① Control and manage access of a large number of people.

② Combine several authentication types
(fingerprint, password, and RF card).

③ Control multiple access control terminals via the network.

④ Manage remote systems easily (running server and client PCs independently).

⑤ Provide various additional features including user access lookup and interphone.

⑥ Real-time monitoring of access status.

⑦ Access control by period and time.

⑧ SDK (Software Developer's Kit) is provided for development of various applications such as time & attendance (not supplied).

⑨ High speed 1:N authentication is available.

⑩ Enhanced user convenience (short ID/group ID authentication and Auto-on).

■ System specifications (when connected with the server)

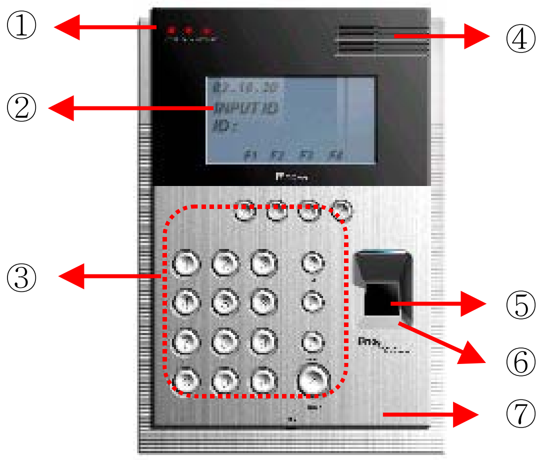
Section	Content
Access terminal	Connection allowed up to 255 terminals
Remote management	Simultaneous server access up to 8
Number of users to register	5,000 users (2 fingerprints per 1 user) 10,000 users (1 fingerprint per 1 user)
Network	10 Mbps, TCP/IP
Authentication type	Fingerprint, password and RF card (optional)
Authentication speed	Less than 1 second (1:1 authentication) 1:N mode : average 2.5 seconds(1,000FP, Server) average 2 seconds(500FP, Terminal) average 1 second(300FP, Terminal) PentiumⅣ 1GHz, 512MB RAM

■ Terminal specifications

Section		Content
Display	Size	128 * 64 Dots LCD
	Language	English, Korean
Sensor	Model	OPP01
	Type	Optical
	Resolution	500 DPI
	Additional	Auto on / Latent Image Check
Authentication	Speed	1:1 mode: T < 1sec. 1:N mode -Avg. 2.5sec(1,000FP, Server) -Avg. 2sec (500FP, Terminal) -Avg. 1sec (300FP, Terminal) ※PentiumⅣ 1GHz, 512MB RAM
	Algorithm	FRR: 0.1 % or less, FAR: 0.001 % or less

Number of users to register	Terminal	2,000 users (2 FP per 1 user) 4,000 users (1 FP 1 user)
Communication	TCP/IP	10 base-T Ethernet
	RS-232C	Max 115200 bps (optional)
	Wiegand	26 bit, 34 bit mode(output only) ※ID Length : 4digit
Size	Case	135 (W)*45 (L)*202.5 (H) mm
	Bracket	102.4(W)*26.6(L)*157.5(H) mm
Supported doors	Deadbolt / Strike / EM Lock / Auto door	
Power	Adaptor	Input: AC 100 V ~ 240 V, 50/60 Hz Output: DC 12 V, 3 A
Additional features	Interphone	MIC and Speaker included
	Voice instruction (English / Korean)	
	Alarm Buzzer	
	Downloading Logo / Firmware	
	Variable ID length (4 ~ 15 digit)	
Option	UPS (2.9Ah)	
	RF Module (HID)	
Temperature	Operation	-20℃ ~ 60℃ (With no icing or condensation)
	Stroage	-20℃ ~ 65℃
Humidity	Operation	25% ~ 85% RH
	Stroage	15% ~ 90% RH

1.3 Product details



A. LED lamps: They indicates the terminal operation status. The below table shows what they mean from the left:

Lamp	Operation Status	Color
Power	Power status. The LED is on while the power is supplied.	Red
Door	Open/close status of the door. The LED is on while the door is open.	Green
Network	Network connection status. The LED is on while connected to the network.	Green

② LCD screen: It displays menus and options for all operations.

③ Keypad: It is used to enter user ID or set up environment. For each key description, please see the following table:

Keys	Description
0 ~ 9	Number keys.
< >	Direction keys. Move the cursor up and down when selecting menu items.
Enter	Press this key to complete such operation as ID input or environment setup.
Cancel	Delete the entered numbers one by one, or move to the upper-level of the menu.
Call	A guest can use it to talk to someone inside with the interphone.
Menu	Set or modify the settings.
F1 ~ F4	Define time & attendance features: arriving, leaving, going out for outside duty and coming back from outside duty. You can freely set the function keys in accordance with the requirements of the related software.

④ Speaker: For voice instruction, interphone communication, and alarms.

⑤ Fingerprint input sensor: Put the fingerprint here.

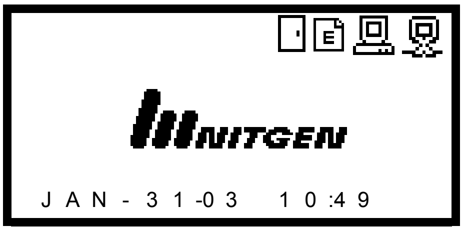
⑥ Auto-On switch: No keyboard operation is required. Fingerprint is automatically read in when placing the finger on the fingerprint input sensor.

⑦ Microphone: It is connected to the internal interphone.

1.4 LCD screen

■ Initial screen

The initial screen of the terminal is as below. The icons in the upper part of the LCD screen indicate the status of the terminal. The logo in the middle of the screen can be defined by the manager, and current date and time are displayed at bottom.



■ Initial screen

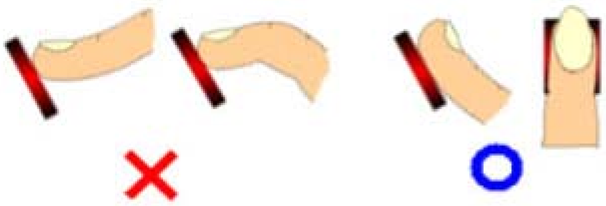
The below table describes the icons in the LCD screen.

Icon	Description
▯	The door is connected to the door lock device.
▯	The door is open after the user authentication is validated.
E	The display language is English.
가	The display language is Korean.
▦	Terminal mode SO (Stand Alone): All operations take place in the terminal alone.
🖥	NS (Network Server): Authentication is done in the server.
▦	NL (Network Local): Authentication is done in the terminal and the log is saved in the server.
🖥	The terminal is connected to the server.
🖥	The terminal is not connected to the server.

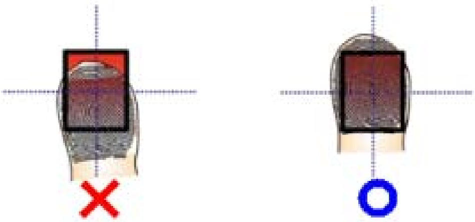
1.5 How to input fingerprint

When you enroll and authenticate user fingerprint, do the followings to avoid authentication error:

B. Press your finger evenly to maximize the input area. If we say the weakest push as 0%, and the strongest push as 100%, apply 50~70% of force.



② Make sure that the core of the fingerprint is at the center of the fingerprint input window. In general, the core of the fingerprint is on the same line as the lunula of the fingernail. So locate the lunula of the fingernail at the center of the fingerprint input window.



1.6 Authentication types

With the NITGEN access control system, you can use fingerprints, passwords, and RF cards (optional) for authentication. Depending on customer environment, you can use one of the following authentication types as you need.

■ **Fingerprint authentication**

Use fingerprints to validate access authentication with the following types:

- 1:1 authentication

  In this mode, enter a pre-registered ID first and then a fingerprint. The enrolled fingerprint corresponding to the ID will be compared to the entered fingerprint on a 1:1 basis. The 1:1 authentication type takes a short time regardless of the number of users. There is no need to make any special settings in the system. After entering the ID, enter the fingerprint to perform authentication.

- 1:N authentication

  Only enrolled fingerprints are used for authentication. Though the authentication procedure is simple, this method will take a little longer than the 1:1 authentication if there are many users. There is no need to make any special settings in the system.

- Short ID (SID) authentication

  The user ID can be 4 – 15 digits long depending on the initial setting. This method simplifies ID input procedure. Instead of entering the entire registered ID, you can enter only the first part of the ID for authentication. For example, if the user ID is 1234 567, enter 12 only and then the fingerprint. Then the system will perform 1:N authentication for all Ids that start with 12xxxxx. There is no need to make any special settings in the system.

• Group authentication

For group authentication, you can specify a group ID of 1 – 4 digits long for each user group. You will enter a group ID and a fingerprint for authentication. For example, you can use the unit number for public housing like an apartment as a group ID. You can specify a group ID when you register a user. Unlike other methods, **you must enter the group ID, and then press F1 before entering the fingerprint** to perform group authentication.

- **Password authentication**

A password of 4 – 8 digits long is used to validate access authentication. You can use this method in such a special case as when the fingerprints are damaged.

- **RF card authentication (optional)**

The RF card of a user is used to identify the user. You can register the RF card number to the system in advance to provide against loss or theft of the RF card.

Chapter 2
Environment Setup

2.1 Menu configuration

■ Features

The terminal menu is configured as follows. You can use this menu to set the initial environment, register users, and set the fingerprint recognition device and the network. You can use the menu button on the terminal keypad.

For more information on how to register, modify and delete users, and check the version, please refer to Chapter 3.

Menu	Command
User Manager	1. Register User 2. Modify User 3. Delete User 4. Delete All
FP Option	1. Sensor Option 2. Secu. Level 3. Latent Check 4. Sensor Timeout 5. Auto-On Check
UI Option	1. Language 2. Voice 3. Button Beep
Door Option	1. Open Duration 2. Warn. Duration
System Option	1. Encryption 2. Log 3. RF Card 4. Wiegand 5. Function Mode 6. Terminal Mode 7. Time Setting

Gate Permit	1. Date 2. Time [From] 3. Time [To]
Network	1. Terminal ID 2. TCP/IP 3. N/W Timeout
Information	1. # of User 2. F/W Version
Factory Ini.	1. DB Format 2. FP Number 3. ID Length

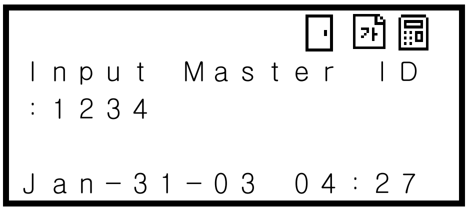
■ Master authentication

When you install the terminal for the first time, you can set the environment without master authentication. But after the master has been registered, you should pass master authentication to change the terminal settings with menu.

⚠ In standalone mode without the network connection, the first registered user will be the master. For more information on how to register users, refer to "Register users" in Chapter 3. When you register the first user, the default user type becomes Master.

⚠ In network environment, you can choose either Normal or Master for the first registered user. In other words, the registration procedure of the first user is the same with other normal procedure.

If you press the menu button to show the menu, the following screen will appear for master authentication. Enter the Master ID and proceed with the pre-defined authentication type (fingerprint, password and RF) to display the menu.

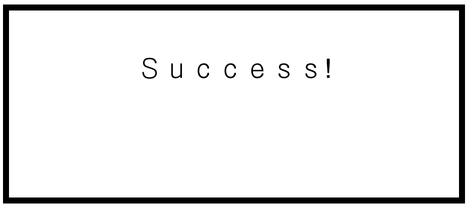


```
Input Master ID
:1234

Jan-31-03 04:27
```

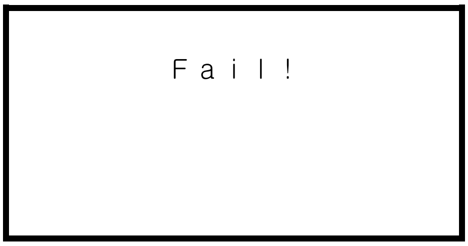
■ Result screen

If you succeed, the following message will appear, followed by the menu screen.



Success!

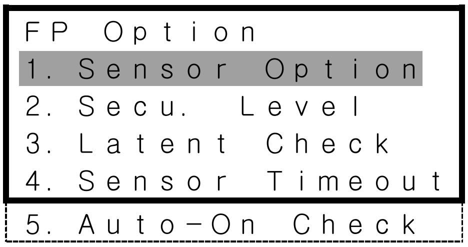
If you fail, the following message will appear and you will go back to the initial screen. This failure message means that the changes you made have not been applied.



Fail!

2.2 Fingerprint Option

Use this menu to set the operation environment of the fingerprint input sensor. It has the following 5 submenus. Move to the submenu you want to choose with the direction keys and press the Enter key.



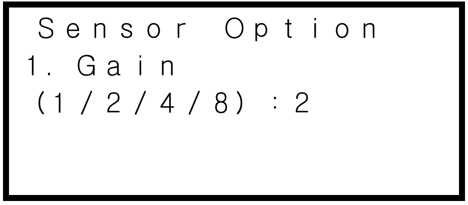
```
FP Option
1. Sensor Option
2. Secu. Level
3. Latent Check
4. Sensor Timeout
5. Auto-On Check
```

■ Sensor Option

Set the sensor options to get a clear fingerprint image. The sensor option values are the internal settings of the CMOS image sensor. You can set gain, brightness and contrast. The defaults of Gain, Brightness and Contrast are 2, 40 and 20 respectively.

⚠ These values can largely affect the fingerprint recognition performance because they are very sensitive. So it is highly recommended that default values be used without any modification if possible.

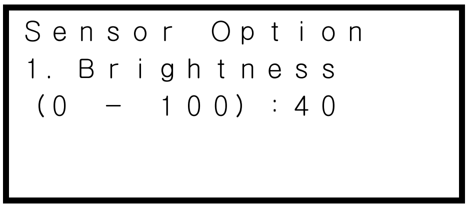
- Gain (1 / 2 / 4 / 8)



```
 Sensor Option
1. Gain
 (1/2/4/8) : 2
```

Enter a gain value and press the Enter key. Then the brightness setup screen will appear.

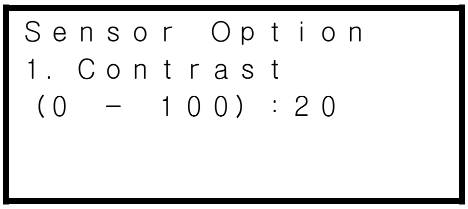
- Brightness (0~100)



```
Sensor Option
1. Brightness
 (0 - 100) :40
```

Enter a brightness value and press the Enter key. Then contrast setup screen will appear.

- Contrast (0~100)



```
Sensor Option
1. Contrast
 (0 - 100) :20
```

⚠ If the recognition performance is decreased because it is very dry (i.e. in winter), adjust Brightness between 20 and 30 (recommendation: 20).

⚠ If the recognition performance is decreased because it is very wet (i.e. in summer), adjust Brightness between 50 and 80 (recommendation: 60).

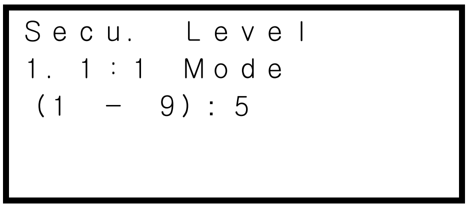
- **Security Level**

Specify security level if you use fingerprint authentication. You can choose a level between 1 and 9. The greater the number is, the higher the security level is. You can specify security levels for **1:1 mode** and **1:N mode** separately to use the system more efficiently. In general, set the **1:N mode** security level higher than the **1:1 mode** one.

> ⚠ If a high level of security is required, you will need to specify a high security level. But a high security level can increase the false rejection rate (fail to authenticate the right person) depending on the status of the fingerprint. In contrast, a low security level may increase the false acceptance rate (allow authentication for the wrong person).

- 1:1 mode

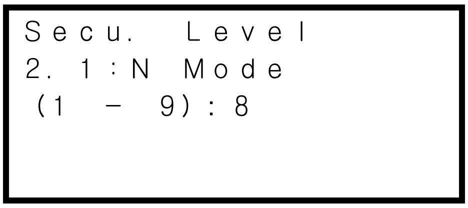
In this mode, you should input ID first and then your fingerprint. The enrolled fingerprint corresponding to the ID will be compared to the entered fingerprint on a 1:1 basis. So you can set lower security level in this mode than in 1:N mode without degrading security.



```
Secu. Level
1. 1:1 Mode
 (1 - 9): 5
```

- 1:N mode

  In this mode, you need to input fingerprint only without ID. It is recommended to set a higher security level in this mode than in 1:1 mode. The default is 8.

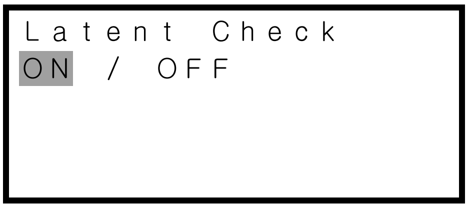


```
Secu. Level
2. 1:N Mode
(1 - 9):8
```

⚠ In the 1:N mode, if you set the security level too low, the false acceptance rate may increase, resulted in degrading security. On the other hand, if you set it too high, the false rejection rate may increase, resulted in inconvenience.

■ Latent Check

It prevents recognition error possibly caused by latent fingerprint image in the fingerprint input window because of sweat or sebum. The initial setting is 『**ON**』. Move to the value you want to choose with the direction keys and press the Enter key.

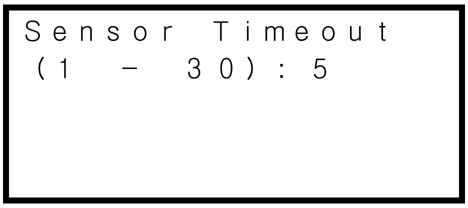


```
Latent Check
ON / OFF
```

⚠ This feature can increase security but it may slow down authentication time. So if high level of security is required, you can use this feature. But you'd better not use this feature in an environment where convenience and quickness are more important (i.e. when used for attendance management).

■ Sensor Timeout (1 ~ 30 seconds)

Set the timeout of fingerprint input. The LED blinks and the terminal waits for fingerprint input during the specified seconds. After that time, the LED will be turned off. The default is 『**5** 』. Use the number keys to enter the value and press the Enter key.

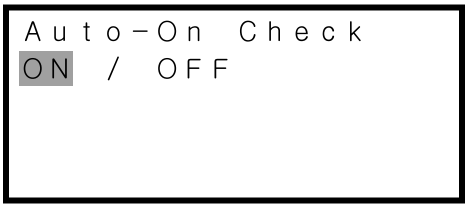


```
Sensor Timeout
(1 - 30): 5
```

Auto-On Check

Auto-On check is an automatic finger detection function. If someone place finger on the sensor, it detects finger and simuates pressing Enter Key.

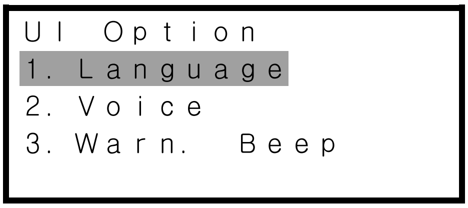
The initial setting is 『**ON**』. Move to the value you want to choose with the direction keys and press the Enter key.



```
Auto-On Check
ON / OFF
```

2.3 UI (User Interface) Option

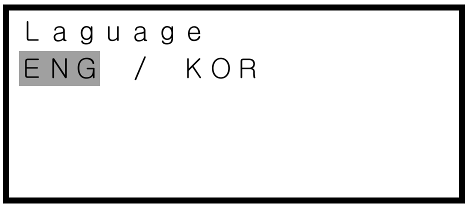
Use this menu to set the user environment such as display language, voice instruction and alarm. The following three submenus are provided. Move to the submenu you want to choose with the direction keys and press the Enter key.



```
UI Option
1. Language
2. Voice
3. Warn. Beep
```

■ Language

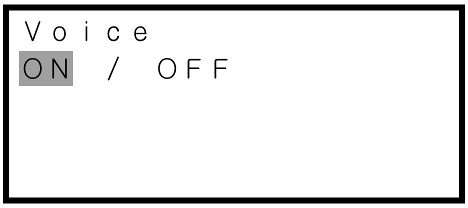
Select either ENG (English) or KOR (Korean) to set the language for LCD screen display. Move to the value you want to choose with the direction keys and press the Enter key.



```
Laguage
ENG / KOR
```

■ Voice

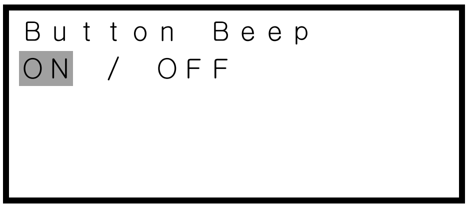
Provide voice instruction on how to use the terminal for fingerprint authentication. Move to the value you want to choose with the direction keys and press the Enter key.



```
Voice
ON / OFF
```

■ Button Beep

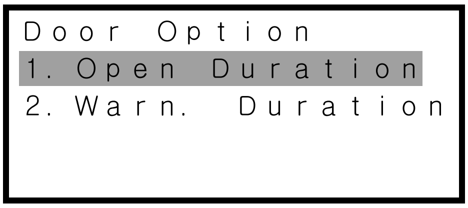
Decide whether to use button beep. Move to the value you want to choose with the direction keys and press the Enter key.



Button Beep
ON / OFF

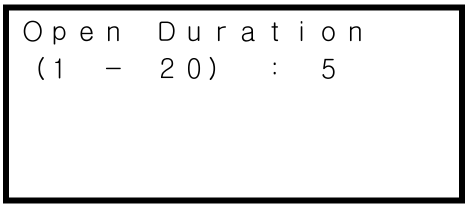
2.4 Door Option

Use this menu to set the door open and close behaviors operated by the terminal. Move to the submenu you want to choose with the direction keys and press the Enter key.



■ Open Duration

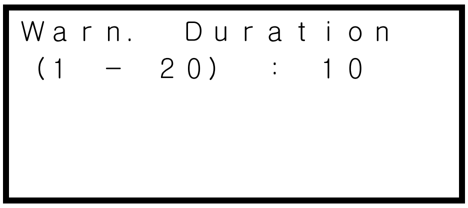
Specify how long the door will be open after user authentication is validated. You can specify a value between 1 and 20. Use the number keys to enter the value and press the Enter key.



```
Open Duration
 (1 - 20) : 5
```

■ Warning Duration

It gives an alarm if the door is still open after the specified time elapses. If the alarm sounds, check why the door is not closed and take necessary steps to make sure that the door closes normally. Specify a value between 1 and 20, **but it should be greater than the door open time.** Use the number keys to enter the value and press the Enter key.

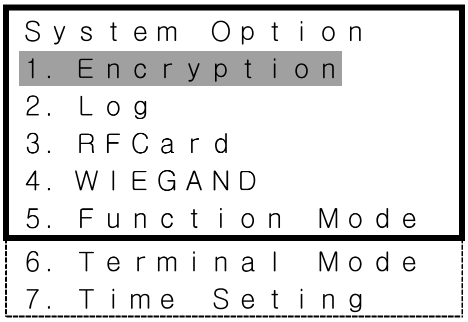


```
Warn. Duration
 (1 - 20) : 10
```

⚠ These features may not work in some types of doors.

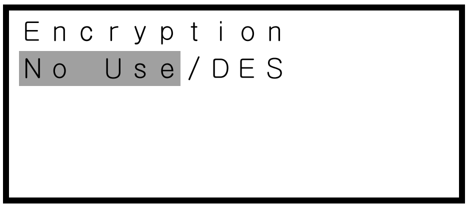
2.5 System Option

Use this menu to set the terminal system. The following 7 submenus are provided. Move to the submenu you want to choose with the direction keys and press the Enter key.



■ Encryption

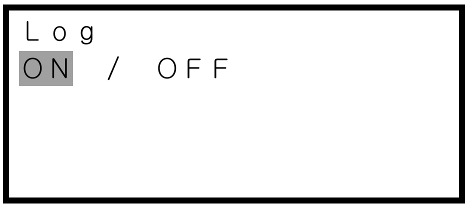
Decide whether to encrypt incoming and outgoing content of terminal in network communication. Move to the value you want to choose with the direction keys and press the Enter key.



⚠ If you use encryption, security and system stability will be enhanced. On the other hand, it will take longer to perform encryption and decryption.

■ Log

Decide whether to save access information. If the terminal is connected to the network, access information is transferred to the server in real-time, whereas if it is in standalone mode without network connection, information is saved within the terminal. Move to the value you want to choose with the direction keys and press the Enter key.

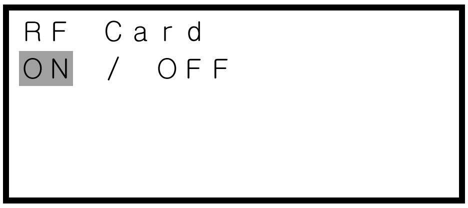


```
Log
ON / OFF
```

⚠ You can save up to 3,000 latest events in a terminal.

■ RF Card

Decide whether to use RF card for user authentication. Move to the value you want to choose with the direction keys and press the Enter key.

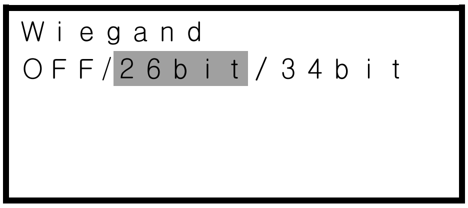


```
RF Card
ON / OFF
```

⚠ RF is optional. If the terminal is not equipped with RF module, this feature is not available.

■ Wiegand

Decide whether to use wiegand protocol for transmission authentication result and user ID to sever.

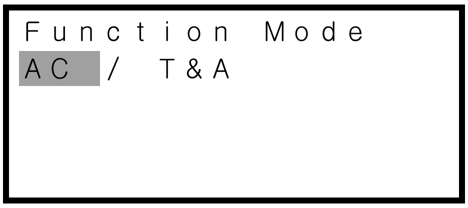


```
Wiegand
OFF/26bit/34bit
```

⚠ Wiegand communication works only if the length of user ID is 4 digit.

■ Function Mode

Set the function keys of the keypad (F1 ~ F4) either for access control (AC) or for time & attendance (T&A). If you choose 『**AC**』, F1 will be used for group authentication. If you choose 『**T&A**』, function keys from F1 to F4 will be used for time & attendance - arriving, leaving, going out for outside duty and coming back from outside duty (inter-operating with the time & attendance software is required). Move to the value you want to choose with the direction keys and press the Enter key.



```
Function Mode
AC / T&A
```

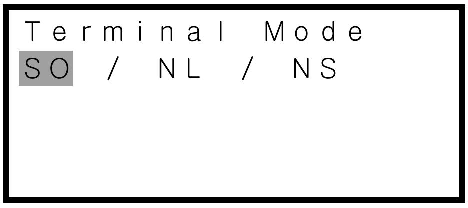
Terminal mode

The terminal can be used in one of the following three modes. Move to the value you want to choose with the direction keys and press the Enter key.

- **SO** (Standalone Only):
  One terminal is used independently. All settings such as user registration, deletion, and access control are performed in the terminal alone. Event log information is saved within the terminal.
- **NL** (terminal authentication):
  User authentication is done by the terminal while various log events are sent to the server in real-time instead of being saved within the terminal.

- **NS** (server authentication):
  User authentication is done by the server.

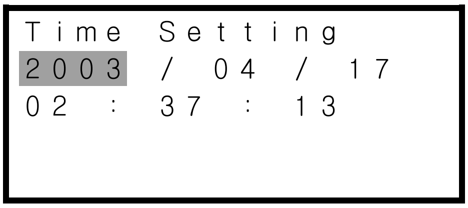
Please refer to the authentication modes described above and choose the proper one.



```
Terminal Mode
SO / NL / NS
```

■ Time Setting

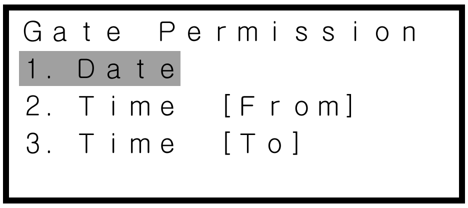
Set the current date and time to be displayed in the LCD screen. Use the number keys to enter the date and time. When you enter the year and press the Enter key, the cursor moves to "month," and so on (year → month → day → hour → minute → second). Use the 24 hour format for hour setting.



```
Time Setting
2003 / 04 / 17
02 : 37 : 13
```

2.6 Gate Permission

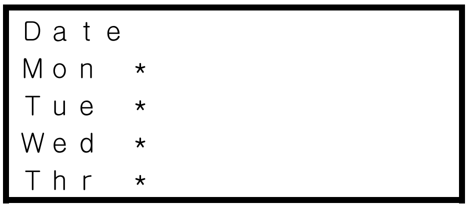
Use this menu to set the permission time of the access control system. The following three submenus are provided.



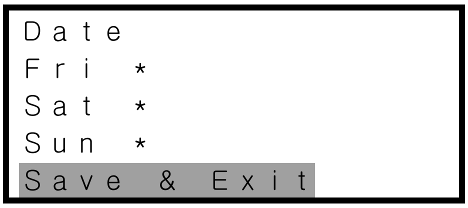
```
Gate Permission
1. Date
2. Time [From]
3. Time [To]
```

■ Date

Specify days of the week when the terminal is enabled. By default, all days of the week are checked with 『*』. The terminal is enabled on the day with the mark . Use the direction keys to move to the day and press the Enter key to set the availability. If you press the Enter key on an enabled day with the check mark, it becomes disabled. Keep in mind that access is prohibited on disabled days.



```
Date
Mon *
Tue *
Wed *
Thr *
```

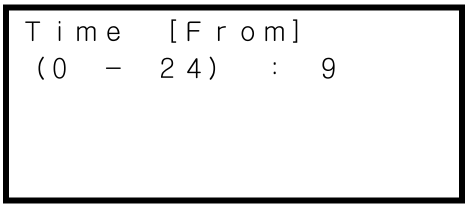


```
Date
Fri *
Sat *
Sun *
Save & Exit
```

When you complete the setting, select 『Save & Exit』.

■ Time [From]

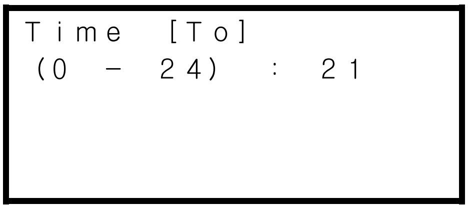
Set the start time of the day when the terminal begins to work. For example, if you want to use the terminal from 9 am to 9 pm, set the start and end times respectively as follows. Use the number keys to enter the value and press the Enter key.



```
Time [From]
 (0 - 24) : 9
```

■ Time [To]

Set the end time of the day when the terminal stops to work. Use the number keys to enter the value and press the Enter key.



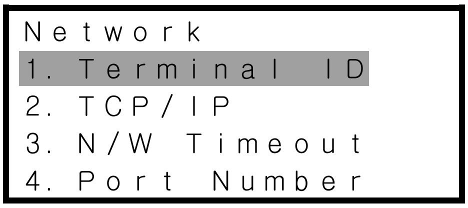
```
Time [To]
 (0 - 24) : 21
```

⚠ If you restrict access time, user access is allowed only within the specified time frame. But the authentication can be enabled by the terminal master who has the authority to change the time restriction setting with menu.

⚠ If you want to specify the time expending two days such as from 1 pm today to 2 am the next day, set the start time as 13 and the end time as 2.

2.7 Network

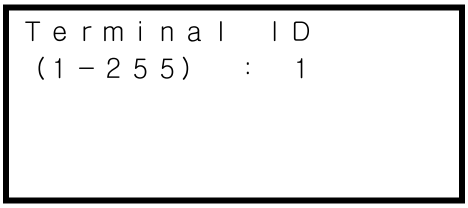
Use this menu to set the network environment to connect the terminal to the network. The following four submenus are provided. Move to the submenu you want to choose with the direction keys and press the Enter key.



```
Network
1. Terminal ID
2. TCP/IP
3. N/W Timeout
4. Port Number
```

■ Terminal ID

Set a unique ID for the terminal. Considering that several terminals can be connected to the server via the network, make sure that the ID matches the one specified in the management program.



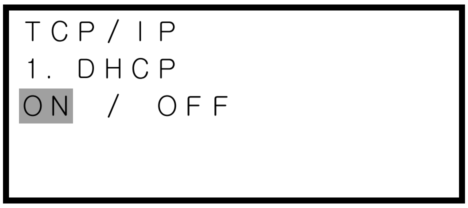
```
Terminal ID
 (1-255)  :  1
```

■ TCP/IP

Set TCP/IP of the terminal.

① DHCP

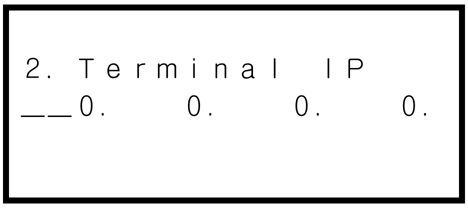
You can decide whether to use DHCP that automatically assigns IP addresses to network clients. If you choose to use DHCP by selecting 『**ON**』, you can skip step ② and ③.



```
TCP/IP
1. DHCP
ON / OFF
```

② Terminal IP

An IP address consists of 4 numbers and each of the number has 3 digits. Entering all 3 digits for a number will move the cursor to the next field so that you can start to enter the next number. But you should press the Enter key to move to the next field if a number has less than 3 digits.

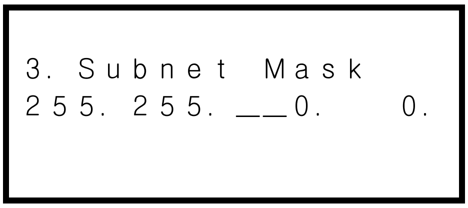


```

2. Terminal IP
__0.   0.   0.   0.
```

③ Subnet Mask

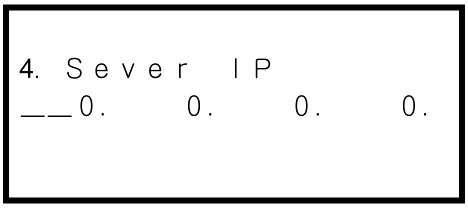
The first two numbers of Subnet Mask are fixed as 255.255. Enter the rest numbers with the same way as you enter the terminal IP address.



```
3. Subnet  Mask
255. 255. __0.    0.
```

④ Server IP

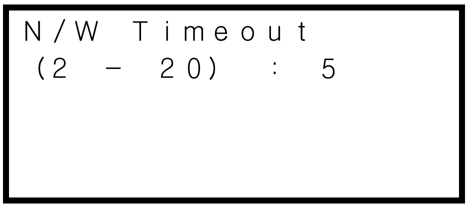
Enter the server IP address with the same way as you enter the terminal IP address.



```
4. Sever  IP
__0.    0.    0.    0.
```

■ Network Timeout

When the terminal communicates with the server via the network, it will be assumed that the network connection is disabled if there is no response within the specified time. You can specify a value between 2 and 20. If the network environment is not stable, start with 5 seconds and then increase the value gradually.

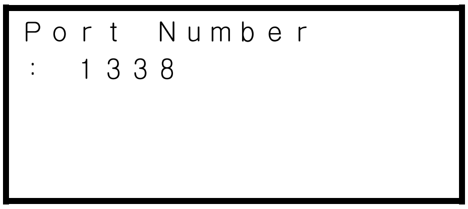


```
N/W  Timeout
 (2  -  20)  :  5
```

⚠ If the server communication cycle is too short, it may cause too much communication burden on the networking. If it is too long, the real-time monitoring system may not work well. So set the value properly for your environment.

■ Port Number

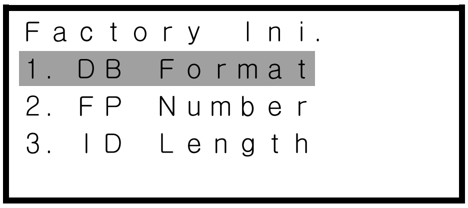
Set the port number for when the terminal communicates with the server via the network. You can specify a value between 1 and 65535.



```
Port Number
:  1338
```

2.8 Factory Initialization

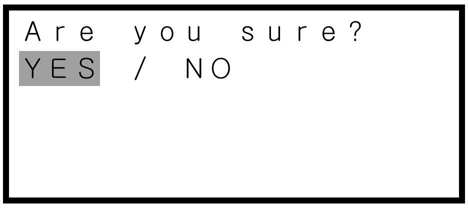
Use this menu to initialize the current settings to factory defaults. To use『FP Number』or『ID Length』, you must delete all users because they are not available if there is left any one registered user.



```
Factory Ini.
1. DB Format
2. FP Number
3. ID Length
```

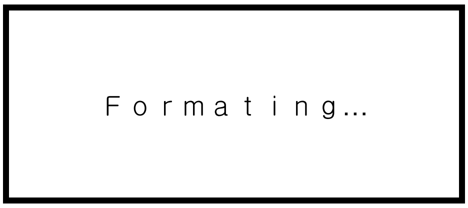
■ DB Format

Format the flash memory where user information is stored and the memory where log information is stored. If you select DB Format, the following message appears.



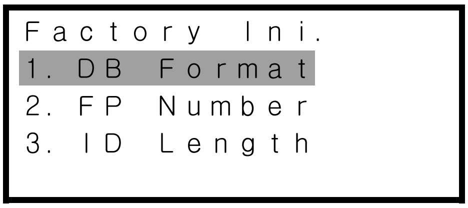
```
Are you sure?
YES / NO
```

Choose "YES" to start formatting. The following message will appear, showing you that formatting is in progress.



```
Formating...
```

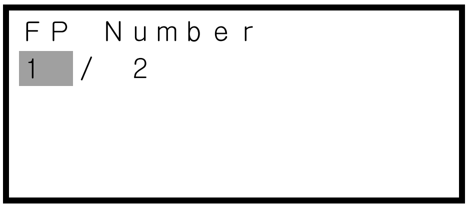
When formatting is complete, you will return to the initial screen.



```
Factory Ini.
1. DB Format
2. FP Number
3. ID Length
```

■ Fingerprint Number

Choose the number of fingerprints you can enroll for each user ID. Move to the value you want to choose with the direction keys and press the Enter key.

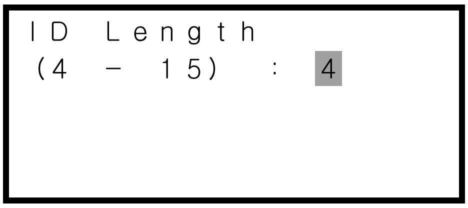


```
FP Number
1 / 2
```

⚠ If you choose 1, you can register up to 4,000 users, and if you choose 2, you can register up to 2,000 users.

■ ID Length

Specify the user ID length between 4 and 15.



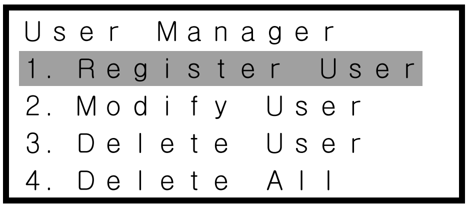
```
ID Length
(4 - 15) : 4
```

⚠ You can't change the ID length if there is left any one registered user.

Chapter 3
How to Use the Terminal

3.1 User Manager

Use this menu to manage the database where user information is stored. You can access this menu only through master authentication. (Refer to "Master authentication" in Chapter 2.) Four submenus are provided: Register User, Modify User, Delete User and Delete All. Move to the submenu you want to choose with the direction keys and press the Enter key.



```
User Manager
1. Register User
2. Modify User
3. Delete User
4. Delete All
```

⚠ If the terminal mode is NL or NS, only 『Register User』 will be displayed on the screen. The other features are available only in the server.

■ **Register User**

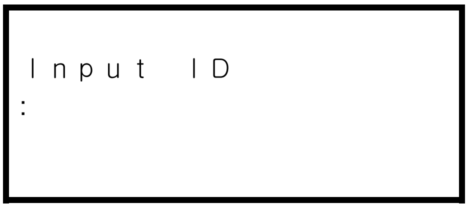
Register users who will use the access control system. User information will be stored in the database. After you pass master authentication, use the following procedure to register users.

⚠In SO terminal mode, user registration is performed in the terminal. In NL or NS terminal mode, it is done in the terminal or the server. In the NL or NS mode, however, you can register users as long as the network works well. If the terminal is disconnected, you can't register users.

⚠If you want to change the SO terminal mode to NL or NS, you must delete the entire users in the terminal database and re-register.

① Input ID

If you choose Register User, the below screen will appear so that you can input a user ID. Enter an ID and press the Enter key. If an identical ID already exists, an error message will appear and you will go back to the previous menu.



```
 Input ID
:
```

⚠ To modify the ID during the input process, use the Cancel button. Pressing the Cancel button will delete numbers one by one if there are any numbers entered. If there's nothing, you will return to the upper-level menu.

② Input Group ID

When you finish Input ID process, the next Group ID screen will appear so that you can specify the group where the user belongs to. If you do not want to use the group ID, press the

Enter key to move to the next step. Input a group ID in 4 or less digits, and press the Enter key.

```
Inpur Group ID
0
```

⚠ If you did not select group ID in the initial environment setup, the group ID input step will be skipped.

③ User Type

Choose Normal or Master user type. Use the direction keys to make a choice, and press the Enter key to finalize the setting.

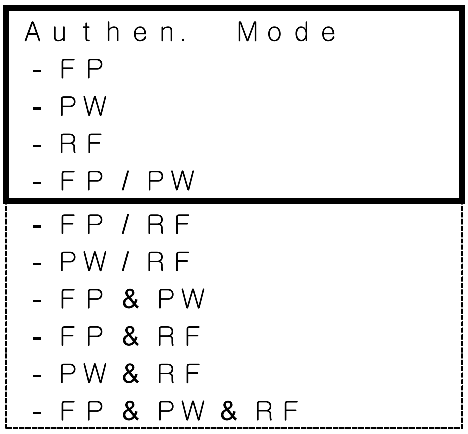
- Normal: Normal users do not have the privilege to manage the terminal. They will have the access privilege only after they pass authentication.

- Master: As terminal managers, master users have door access privilege and can manage the user database and set the environment with corresponding menu items. You can specify master users up to 8.

```
User Type
Normal/Master
```

④ Authentication Mode

Choose one of user authentication modes - fingerprint, password, RF card and several combinations of the three. Move to the value you want to choose with the direction keys and press the Enter key.



```
Authen.  Mode
 - FP
 - PW
 - RF
 - FP / PW
 - FP / RF
 - PW / RF
 - FP & PW
 - FP & RF
 - PW & RF
 - FP & PW & RF
```

⚠ If you did not select RF when you setup the system, any authentication modes including RF will not be displayed in the screen.

- **How to use the authentication modes**

※Legend: FP (fingerprint), PW (password), RF (RF card), Enter(↵)

“/” (OR combination), “&” (AND combination)

Classification	Descripti n
FP	Authenticate by fingerprint only. ① ID + fingerprint (1:1 authentication) ② fingerprint input (1:N authentication)

PW	Authenticate by password only. ① ID + ↵+ PW + ↵
RF	Authenticate by RF card only. ① RF
FP/PW	Authenticate by fingerprint or password. Try fingerprint first. If you input the ID first and fails in the fingerprint authentication, you can try password authentication. But if you fail in the fingerprint authentication without ID input, you can't try password authentication and authentication fails. ① ID + FP (if FP fails, try PW +↵) ② FP (if FP fails, authentication fails)
FP/RF	Authenticate by fingerprint or RF card. Try fingerprint first. If you input the ID first and fails in the fingerprint authentication, you can try RF card authentication. But if you fail in the fingerprint authentication without ID input, you can't try RF card authentication and authentication fails. ① ID + FP (if FP fails, try RF) ② FP (if FP fails, authentication fails) ③ RF
PW/RF	Authenticate by password or RF card. ① RF ② ID + ↵+ PW + ↵(if PW authentication fails, try RF)
FP&PW	Authenticate by fingerprint and password. You should succeed in both.

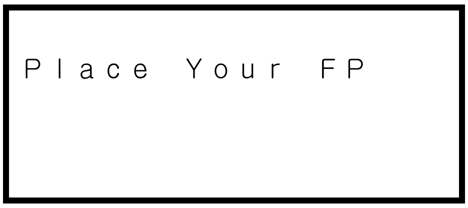
	① FP + PW + ↵ ② ID + FP + PW + ↵
FP&RF	You should succeed in both fingerprint and RF card. The following three methods are available. ① RF + FP ② FP(1:N authentication) + RF ③ ID + FP + RF
PW&RF	You should succeed in both password and RF card. ① RF + PW + ↵ ② ID + ↵+ PW + ↵+ RF
FP&PW&RF	You should succeed in fingerprint, password and RF card. ① FP + PW + ↵+ RF ② ID + FP + PW + ↵+ RF ③ RF + ↵+ FP + PW + ↵

When you try one of the above modes, short ID and group ID authentications are also available (refer to "1.6 Authentication types" in Chapter 1).

⑤ Input Fingerprint

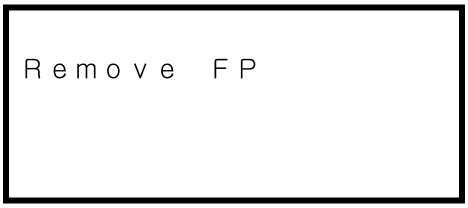
If you select fingerprint authentication mode or other one that includes fingerprint authentication, you must input your fingerprint. You should do it twice. After the first input, take your finger off, and then input the fingerprint again.

Place the fingerprint on the sensor.



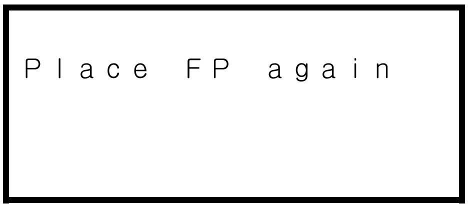
Place Your FP

If the following screen appears after the first fingerprint input, take your finger off from the sensor.



Remove FP

Place the same fingerprint again.

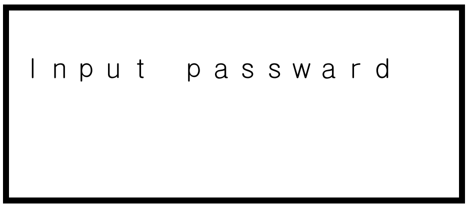


Place FP again

If the fingerprint input is successful, a success message will appear. If it fails, a failure message will appear and you will return to the initial registration screen.

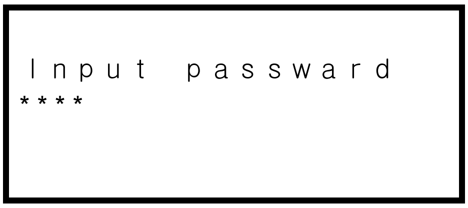
⑥ Input password

If you select password authentication mode or other one that includes password authentication, you must enter the password. Password can be 4 - 8 characters long.



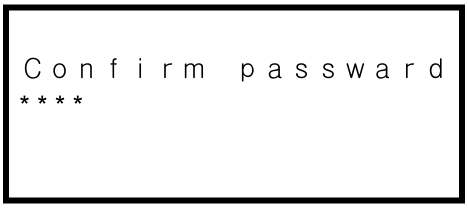
Input passward

For security, password is displayed as 『*』.



Input passward
****

Enter the password again for confirmation.



Confirm passward
****

If the password input is successful, a success message will appear. If it fails, a failure message will appear and you will return to the initial registration screen.

⑦ Input RF card.

If you chose to use RF card when you setup the system, use the RF card to register the user. Place the RF card near the fingerprint input sensor. If you did not choose the RF option when you setup the terminal environment, press the Enter key to go to the next step.

```
Contact RF Card
Press Enter to
skip
```

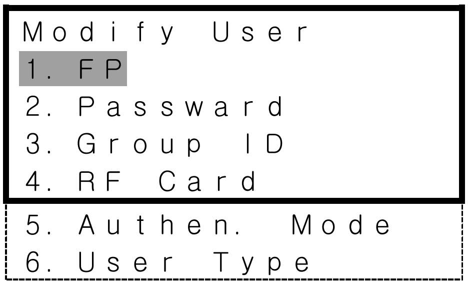
If the RF input is successful, a success message will appear. If it fails, a failure message will appear and you will return to the initial registration screen.

■ Modify User

Use this feature to change the information on a registered user. You can change fingerprint, password, group ID, RF card, authentication mode and user type. If you select『Modify User』, the following screen will appear so that you can enter the user ID whose information you want to modify.

```
Input ID
1234
```

Enter the ID and press the Enter key, and you'll see the following items in the displayed screen. Move to the submenu you want to choose with the direction keys and press the Enter key.

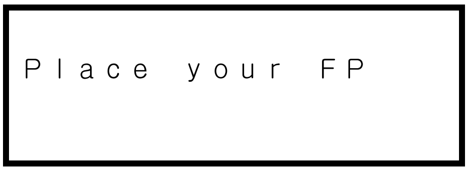


```
Modify User
1. FP
2. Passward
3. Group ID
4. RF Card
5. Authen. Mode
6. User Type
```

- **Fingerprint**

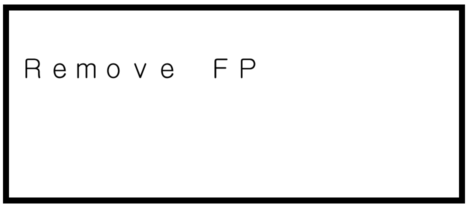
  Change the fingerprint of each registered user. As you did in the first fingerprint enrollment, input the fingerprint twice. After the first input, take your finger off, and then input the fingerprint again.

  Place the fingerprint on the sensor.



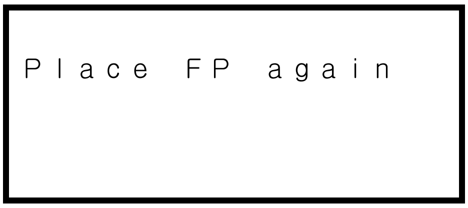
```
Place your FP
```

If the following screen appears after the first fingerprint input, take your finger off from the sensor.



```
Remove FP
```

Place the same fingerprint again.

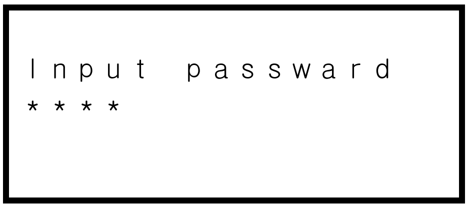


```
Place FP again
```

- **Password**

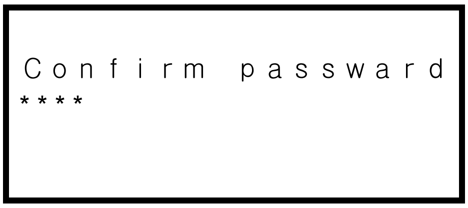
  Change the password of each registered user.

  Enter a new password.



```
Input passward
****
```

Enter the password again for confirmation.



```
Confirm passward
****
```

- **Group ID**

Change the group ID where the user belongs to.

Enter a new group ID. If you don't want to use a group ID, press the Enter key to skip this step.

```
Input Group ID
0
```

- **Contact RF Card**

Change the RF card of each registered user.

```
Contact RF Card
```

- **Authentication Mode**

Change the authentication mode of each registered user.

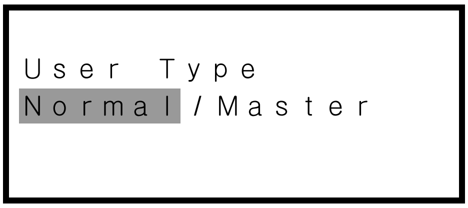
Select a new authentication mode you want to use.

```
Authen. Mode
 - FP
 - PW
 - RF
 - FP / PW
 - FP / RF
 - PW / RF
 - FP & PW
 - FP & RF
 - PW & RF
 - FP & PW & RF
```

- **User Type**

  Change a user type of each registered user.

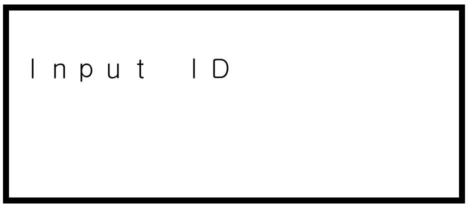
  Choose either Normal or Master.



User Type
Normal /Master

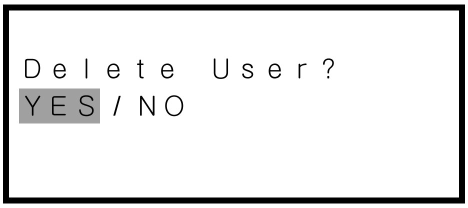
■ **Delete User**

Enter the user ID you want to delete.



Input ID

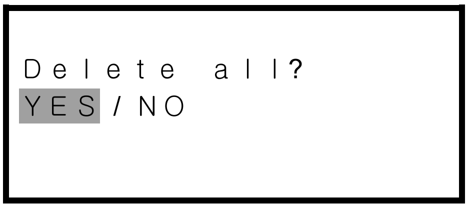
The below confirmation screen will appear. Choose either YES or NO, and press the Enter key.



Delete User?
YES / NO

■ Delete All

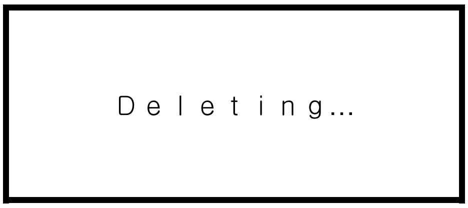
Delete all registered users in the terminal.
Choose either YES or NO, and press the Enter key.



```
Delete all?
YES / NO
```

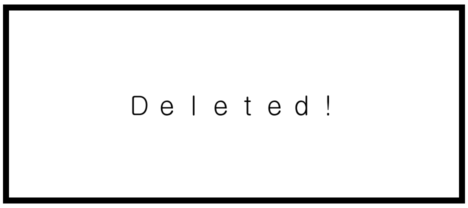
⚠ All registered users in the terminal will be deleted. Please use this feature very carefully.

If you choose 『**YES**』 to delete all users, the following message will appear, showing you that deletion is in progress.



```
Deleting...
```

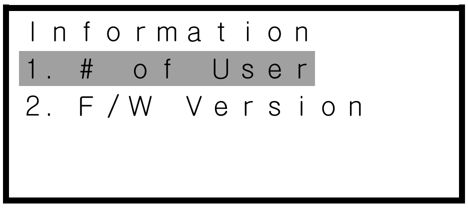
When deletion is complete, the following message will appear, and you will return to the previous screen.



```
Deleted!
```

3.2 Information

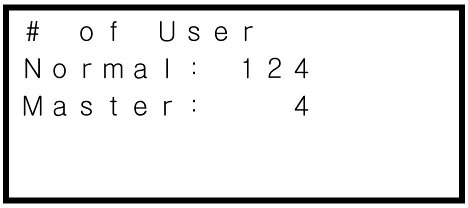
You can check the terminal information with this menu.



```
Information
1. # of User
2. F/W Version
```

■ Number of User

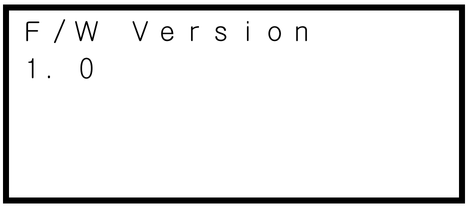
It shows you the total number of users registered in the terminal. The number of normal and master users are displayed separately on the screen.



```
# of User
Normal: 124
Master:   4
```

■ Firmware Version

It shows you the firmware version of the terminal.



```
F/W Version
1. 0
```