NAC2500 RC/MC
USER MANUAL

NITGEN
biometric solutions

To Contact Us

Tel. +82-80-060-1600
(Toll Free)
Fax. +82-2-513-2191
E-mail: customer@nitgen.com
URL: http://www.nitgen.com

Table of Contents

Chapter 1. Introduction

1.1 Product Introduction

■ Overview

The use of biometrics system continuously increases in various authentication systems and in areas that require a higher level of security because of its ease of use and economical benefits. Among a number of biometrics system, a fingerprint recognition system is not only easy to use but also enables economical product development. It takes up the most part of the market as it allows a wide variety of application. NITGEN, a leader in the fingerprint recognition area, has provided fingerprint recognition solutions for the management of PC security, knowledge, safe, access control, electronic payment and financial clearings. Continuous R&D activities and quality management ensure that NITGEN meets evolving needs and demands of the market and the customers.

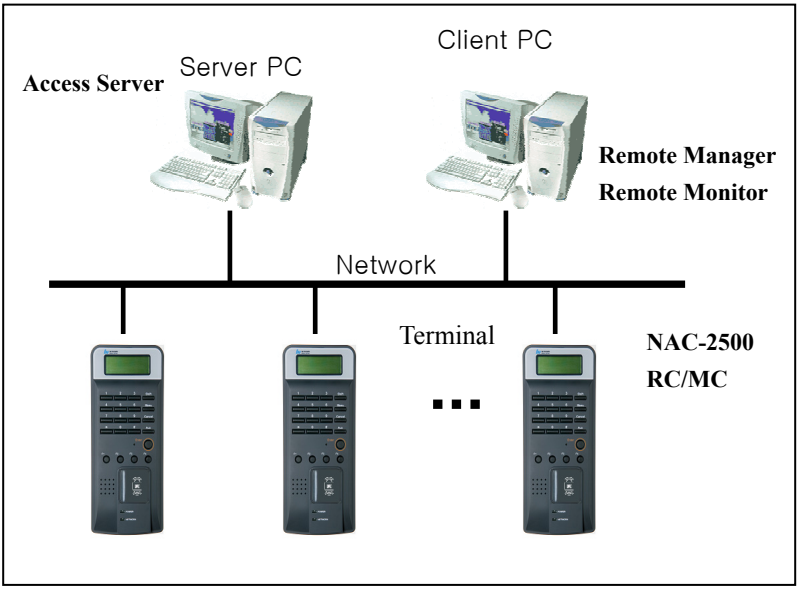
NITGEN access control system is a culmination of world-renowned technologies from NITGEN including fingerprint recognition algorithms, optical sensor, embedded design and software applications. Unlike legacy access control systems that use only password and ID card, it provides the ease of use and tight security with no risk of forgetting password, stolen cards or forgery. The system is designed to provide maximum operational efficiency over the network by enabling remote monitoring on terminals that have been independent so far.

NITGEN access control system allows various combinations of FR card, password and fingerprints. It also meets the common set of requirements and special needs in the corporate and

government sectors with such functions as shortened ID, 1:N matching and voice guidelines.

This manual describes how to use NITGEN access control terminal NAC-2500 RC/MC.

■ System Components



	Main Features
Server PC	1. Server S/W : Access Sever 2. Terminal communication, log data collection 3. user information & log DB 4. authentication
Client PC	1. Client S/W : Remote Manager/Monitor

	2. user registration and other management 3. Terminal status and event monitoring
Terminal (NAC-2500 RC/MC)	1. user check and authentication 2. access door control

NITGEN access control terminal(NAC-2500 RC/MC) can be used alone for full functionality or can be used in connection with the network together with admin programs (Access Server, Remote Manager, Remote Monitor) in order to reduce the number of terminals and to ensure an easier and a more effective management. Server S/Wand Client S/W can be placed within one PC.

1.2 Product Features and Specification

■ Product Features

NITGEN access control system **(NAC-2500 RC/MC)** has the following features.

① access control and management on small & medium number of users

② a combination of various authentication methods (password, RF card)

③ network-based access control on terminals for multiple users

④ easy remote management on the system (Server/Client PC can be separated)

⑤ view on user's access history and various additional

functions

⑥ real-time access monitoring

⑦ access control by period and time

⑧ SDK (S/W Developer's Kit) for the development of application programs such as attendance management program (separate)

⑨ high-speed 1:N authentication

■ System Specification (Connected to Server)

Specification	Details
Connection Terminal	Maximum 255 units
Remote Management	8 concurrent accesses to server
# of Users to be Registered	10,000 users
Network	TCP/IP, 10M bps
Authentication Type	RF card ,Password

Note) Enterprise version software

- Unlimited terminal access. (Proportional to system capacity)
- Unlimited number of registered users. (Proportional to system capacity)
- 1:1 server authentication only.

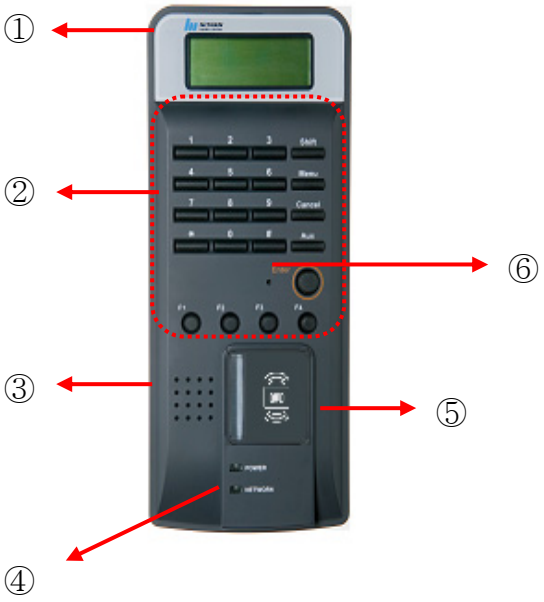
■ Detailed Specification: Terminal

Function		Spec.
Display	Type	128 * 32 Dots LCD
	Language	Default: Korean, English, Japanese, Chinese, Spanish, French, Thai, Indonesian Additional: Korean, English, Portugee, Polish, Swedish, Arabic, Farsi
Authentication	Algorithm	FRR: less than 0.1%, FAR: less than 0.001%
# of registered users	Terminal	10,000
Communication	TCP/IP	10 base-T Ethernet (optional)
	RS-485	Max. 115200bps (Custom requirement)
	Wiegand	1. Input: provided with the use of external card reader 2. Output 2.1 Access Controller mode: Facility Code and ID 2.2 Reader mode: Values read from Card reader ※4 characters only for ID
Size	Case	90 (W)* 200 (L)* 48 (H) mm
Door support	Dead Bolt / Strike / EM Lock / auto door	

Power	Adapter 1	In: AC 100V ~ 240V, 50/60 Hz Out: DC 12V, 3A (24V OK)
	Adapter 2	In: AC 100V ~ 240V, 50/60 Hz Out: DC 5V, 3A
Additional Function	Guidelines recorded in voice	
	Firmware Download	
	ID length (4 ~ 15 digits)	
	Authentication results to be displayed in LED	
Optional	Network Board	
	Door Control Board	
	RF Module (125KHz HID, 13.56MHz Mifare)	
Temperature	Storage	-25℃ ~ 65℃
	Operation	-20℃ ~ 60℃ (with no dew condensation)
Humidity	Storage	15% ~ 90% RH
	Operation	25% ~ 85% RH

Chapter 2. How to Use

2.1 Detailed Product Parts



① LCD: All activities are displayed with text message.
② Key pad: Used for ID input and environment setting. Details are as follows.

Key	Description
0 ~ 9	To type in numbers

*, #	To move a curser up and down for menu selection and to change direction. *(Backward), #(Forward)
Enter	To complete ID type-in or environment setting.
Delete	To erase typed-in numbers one by one or to move to higher level in menu.
Menu	To set or change an environment.
F1 ~ F4	User-customizable buttons that can be used for attendance management including arrival/leave/go-out/return. F1~F4 can be set freely depending on software requirements.
SHIFT	Reserved
AUX	Reserved

③ Speaker: Used for recorded voice guidelines and warnings.
④ LED lamp: Showing operations of the terminal. Each lamp represents the followings.

Function	Operation	Color
Authentication	To display the results of authentication. Green for success and red for failure.	Green/red
Power	To display power status wit LED on for power on.	Red
Network	To display network connection with LED on for network connected.	Green

⑤ RF Card input window : To contact or approach RF Card input window. Without operation of keypad, RF Card Number will be automatically input by approaching or contacting RF Card input window.

⑥ Reset switch: To reset the terminal if the terminal is not in normal operation unexpectedly.

2.2 LCD Screen Layout

■ Initial Screen of Terminal

The initial screen of terminal is as follows. The bottom line displays current date and time.

```
Contact    RF    Card
        13:46:17
```

2.3 Authentication

NITGEN Access Control System recognizes password, and RF CARD (optional) for authentication. Users can get authentication by freely choosing any method depending on their own environment.

2.3.1 RF Card Authentication

User identity is confirmed through a RF CARD that he or she has. By registering RF CARD numbers in the system, the use of lost or stolen card can be prevented. To initiate authentication by using a RF CARD, you can either contact RF card when the initial screen appears or contact RF card when the following message is displayed after typing in user ID.

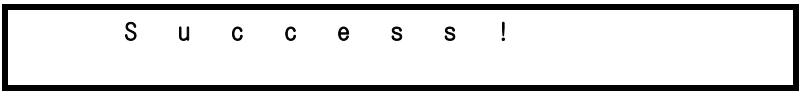
1) 1:1 Authentication

Input your ID in the initial screen of terminal.
(Please input full ID)

```
I N P U T     I D :
1 2 3 4
```

When the screen changes as follows, to contact or approach with RF Card .

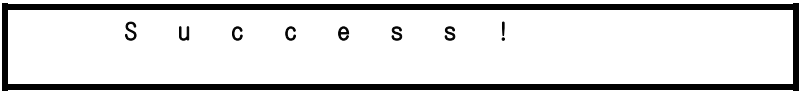
인증이 성공되면 다음과 같은 메시지가 출력됩니다.
The following message is displayed if authentication is successful.



2) 1:N Authentication

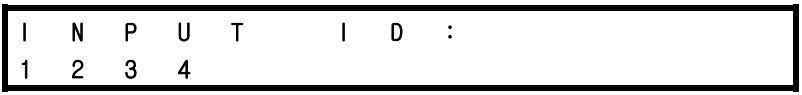
In the initial screen of terminal, contact or approach the RF Card Window with RF Card.

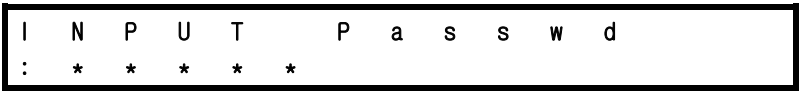
The following message displays if authentication is successful.



2.3.2 Password Authentication

It checks the right to access by using 4~8 digit password and it is used in special occasions including damaged fingerprint.





Password can be set up to 8 digits.

2.3.3 Others: Automatic Attendance Mode

The result of attendance can automatically remain in log history only with general 1:N authentication. When a specific attendance status is repeated many times, the user does not need to take trouble to press the same function key (F1~F4) each time.

In an automatic attendance mode, the initial screen changes as follows and when the 1:N match is tried, the authentication result is automatically attached with the relevant attendance status.

To set or delete the automatic attendance mode, please take the

following steps.

1) To set the mode: Please press an appropriate function key (F1~F4) for more than 5 seconds when the initial screen appears to set the automatic attendance mode for each key. When setting is completed, you will hear a setting tone.

2) To delete the mode: The automatic attendance mode is deleted if you press the DELETE key for more than 5 seconds. When deletion is completed, you will hear a deletion tone.

Chapter 3. Environment Setting

3.1 Menu Composition

The following table shows the entire menu composition of terminal. The menu is helpful in setting initial environment, user registration, fingerprint recognition device, and network. To use the menu, please press the menu button on the key pad of Terminal.

You can not set up below menus remarked with Grey color in NAC-2500 RC/MC Terminal.

Please refer to chapter 3 for user registration, information change, user deletion, number of registered users and version-related information.

Higher menu		Detailed Menu		Sub menu	
1	User Management	1	User registration		
		2	User info change		
		3	User deletion		
		4	Deletion of all users		
2	Fingerprint sensor setting	1	Sensor brightness	(1~100)	
		2	Security level	1	1:1 mode
				2	1:N mode (Please try menu 3 times after setting number 1)
		3	Capture mode		

		4	Time setting for fingerprint input		
		5	AUTO-ON setting		
		6	1:N time setting	1	Whether to use 1:N time setting or not
				2	Time setting (“time setting” possible only when it is on)
3	UI setting	1	Language		
		2	Voice guideline		
		3	Button tone		
4	System Setting	1	Log storing		
		2	RF card		
		3	WIEGAND	1	OFF
				2	26BIT
				3	34BIT
		4	Function key setting		
		5	Authentication mode		
		6	Time setting		
		7	Terminal mode		
		8	Time zone		
5	Network	1	Terminal ID		
		2	TCP/IP	1	DHCP yes or no?
				2	Terminal IP
				3	Sebnet Mask
				4	Gateway
				5	Server IP
		3	Time limit		
		4	Port setting		
6	Information	1	Number of users		

		2	Firmware version	
7	Factory default	1	DB Format	
		2	Factory format	
		3	Number of registered fingerprints	
		4	Number of characters in ID	
		5	Reset terminal	

3.2 Entering into Menu

■ Master Authentication

At the time of initial installation of terminals, environment can be set without master's authentication. However, master authentication is a must in order to change environment settings after master setting. To view menu, please press a master button which will display the following screen for master authentication. You can see the menu after inputting the ID of master and conduction authentication with selected authentication methods including password and RF.

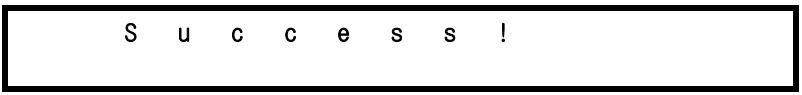
```
I N P U T   M A S T E R   I D
1 2 3 4
```

⚠ For an independently installed terminal that does not use any network, an initially registered user will be automatically registered as master. Please refer to chapter 3 "user registration" for detailed registration method. During the initial user registration, default values at "authority setting" will be set as master.

⚠ When using network, an initially registered user can choose between either a master or a normal user. It is the same as a registration process for normal users.

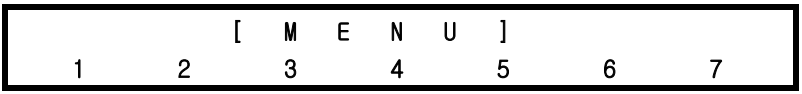
■ Result Display

The following message is displayed if master authentication is successful. After one second, you can enter into the menu. However, you will get a failure message when the authentication is not successful which is same as the failure message for general authentication failure.



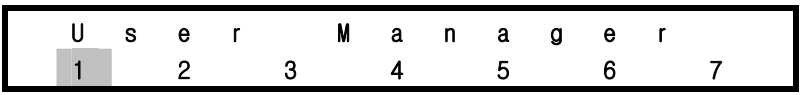
3.3 Basic Menu

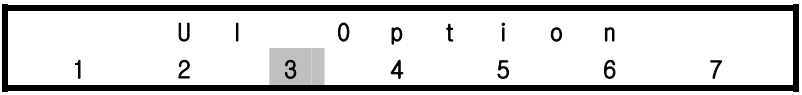
The following screen is enabled after pressing a menu button at the initial screen of terminal and if master authentication is successful. You can choose basic menu by pressing #, * keys or number keys.

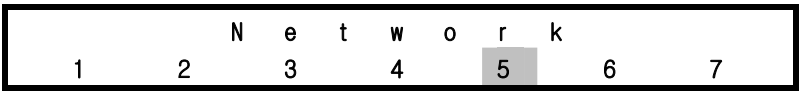


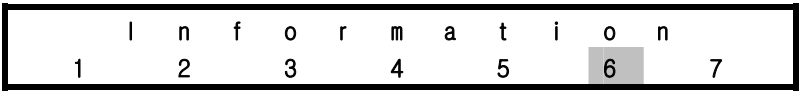
The following explains the basic menu. If you press ENTER in the basic menu, you can move to detailed menu which is a sub menu of each basic menu. Please press DELETE to go back to the basic menu from detailed menu or to go back to the initial screen from the basic menu.

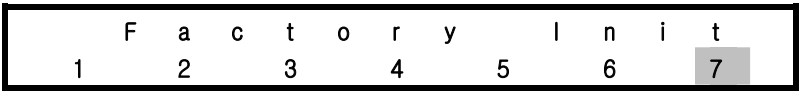
The higher menu has the following 7 categories.







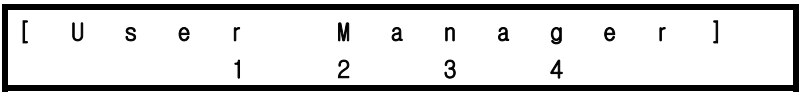




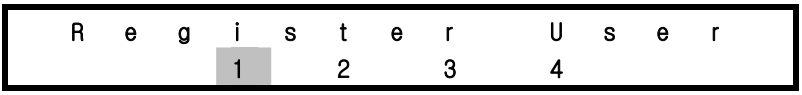
3.4 Detailed Menu

3.4.1 User Management

The user management menu manages database in which user information is stored. It is accessible only through master's authentication (see Master Authentication in chapter 2.) Four sub menus are provided including user registration, change and deletion. Use direction buttons and choose ENTER.



3.4.1.1 User Registration



It is designed to store the information of users into database who will use the access controller. Please register the user with the following procedures after master authentication.

⚠ User registration is conducted in terminal when the terminal mode is set at SO. It can be conducted either in server or in terminal if the mode is set at NL. Note that terminal registration is possible if network is in normal operation under the NL mode, but is not possible if network is disconnected.

⚠ To change SO mode into NL mode, user DB in the terminal should all be erased and re-registered.

1) To input user ID

When user registration menu is selected, you will see the following screen that waits for the input of user ID. After typing in an appropriate user ID, please press ENTER. If the same ID already exists, a failure message will be displayed and the system goes back to a previous menu.

```
I N P U T   I D :
1 2 3 4
```

⚠ To correct ID during typing, please use a delete button. It will erase characters one by one or will go back to a higher menu when no character is input.

2) Authority setting

The following explains how to set user authority between

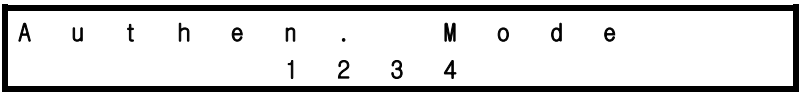
normal user and master. Please use a directional key and press ENTER to finish.

- Normal user: no right to terminal management with access authority only via identification.

- Master: terminal manager who has not only the right to access but also user DB management, environment setting and other menu.

3) Choice on Authentication

Please choose the authentication mode of users among password, RF CARD, and other combinations. Please use a directional key and press ENTER to finish.



⚠ If RF is not selected during system setting, authentication with RF will not be displayed in authentication mode screen.

- How to use by authentication mode

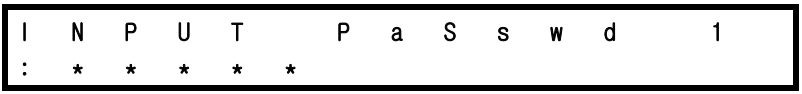
※Legend: PW(password), RF(RF CARD), Enter(↵)
"/" (OR combination), "&" (AND combination)

Mode	Description
password	Password only for authentication. ① ID + ↵+ PW + ↵
RF	RF CARD only for authentication. ① RF
password/RF	Password or RF CARD for authentication. ① RF ② ID + ↵+ PW + ↵(PW failure, RF)
password& RF	Both password and RF CARD authentication should be a success to complete authentication. ① RF + PW + ↵ ② ID + ↵+ PW + ↵+ RF

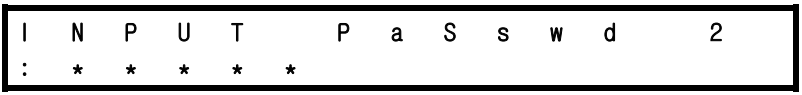
4) Password input

User password is input when password or password-included authentication is selected. Your password can be between 4~8 digits.

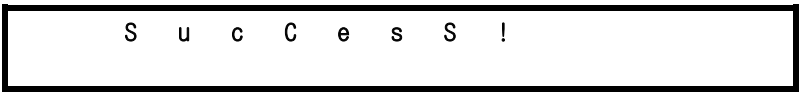
For security reason, the input password will be displayed as 『*』.



The input password is confirmed.



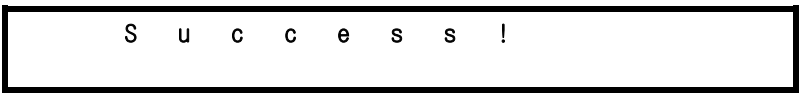
You will get a success message for successful password input and will get a failure message for failed password input. In case of failure, you will go back to the initial registration screen.



5) RF CARD input

When RF CARD is selected at System Setting, users can be registered by using RF CARD. Please approach user's RF CARD near fingerprint sensor. Make sure that RF option is selected during terminal environment setting.

You will get a success message for successful RF CARD input and will get a failure message for failed RF CARD input. In case of failure, you will go back to the initial registration screen.



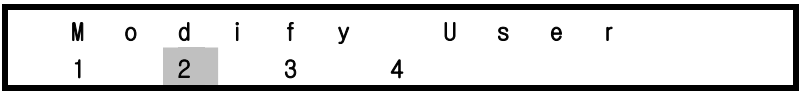
6) Other Registration Methods

The previous methods can be freely combined for registration. Please refer to the following.

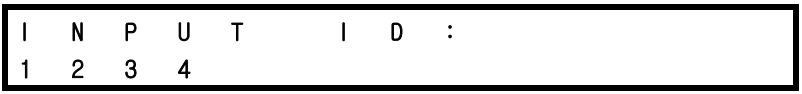
1. Password 2.RF
3. Password & RF 4. Password & RF

3.4.1.2 User Information Change

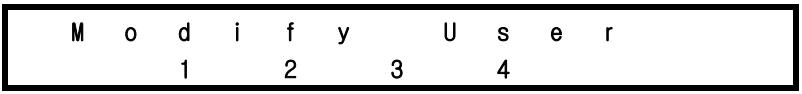
It is designed to change user information including changes in fingerprint, password, RF CARD, Authentication, and authority.



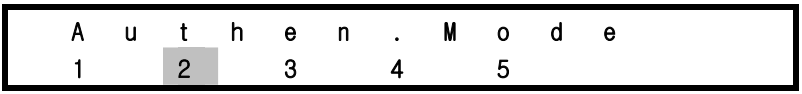
When choosing 「user information change」, the following screen will be displayed to input user ID.



After inputting ID and pressing ENTER, the following changeable items will be displayed. Please use a directional key and press ENTER to finish.



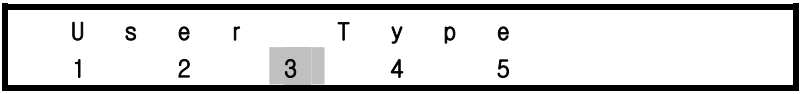
1) Authentication method change



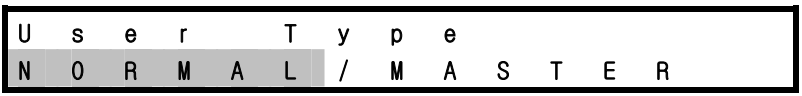
Please selected authentication method that will be changed.

1. password 2.RF
3. password / RF 4. password & RF

2) Authority change

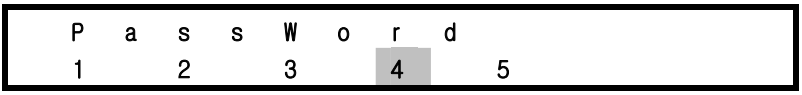


It changes the authority of individual registered users. User authority consists of normal and master user. Master users can enter into menu to do various terminal controls. Therefore, it is desirable to allocate master user authority only to a limited number of users.

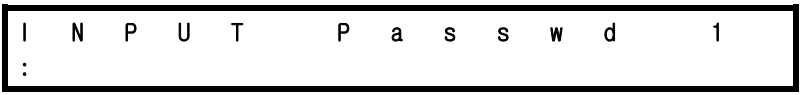


3) Password change

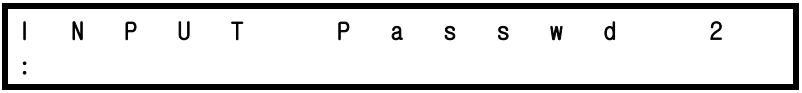
Registered password can be changed.



Please input new password.



Please input the password again.



You will get a success message for successful input and will get a failure message for failed input. In case of failure, you

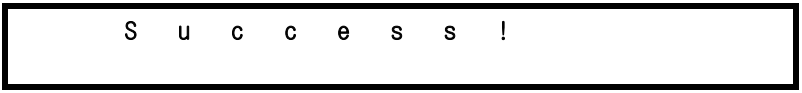
will go back to the initial registration screen.

4) RF CARD change

RF CARD of individual registered users can be changed.

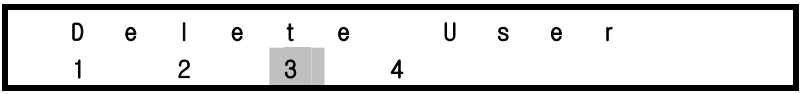
Please contact the RF CARD when the following message appears.

You will get a success message for successful input and will get a failure message for failed input. In case of failure, you will go back to the initial registration screen.

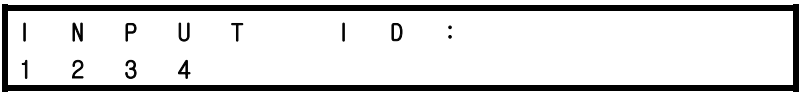


3.4.1.3 User Deletion

Registered users can be deleted and deleted.

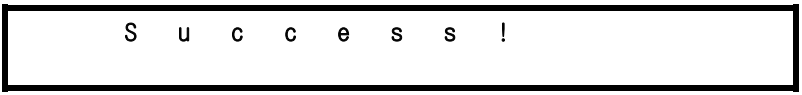


Please input user ID to be delete. When the ID does not exist, the process fails and goes back to the initial screen.



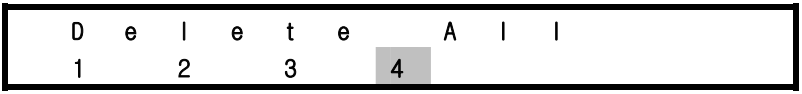
Please confirm the selection.

The following message appears for successful deletion.



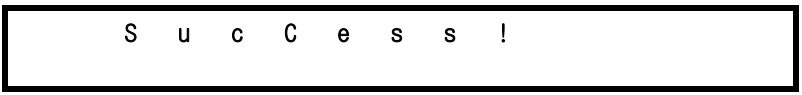
3.4.1.4 Deletion of All Users

All users can be deleted at once.



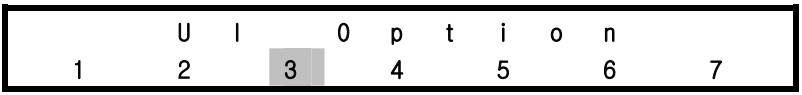
⚠ Please be careful as it will delete all registered users within a terminal.

When 「yes」 is selected, the deleting procedure begins.

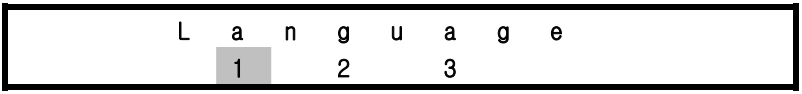


3.4.2 UI (User Interface) Setting

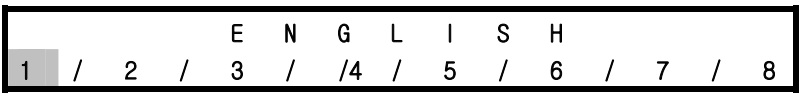
The third function under the main menu is UI setting.

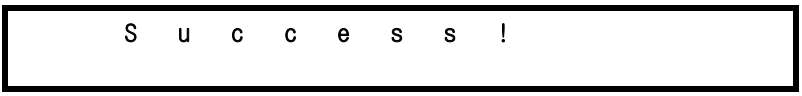


3.4.2.1 Language



You can choose From Korean to Indonesian.

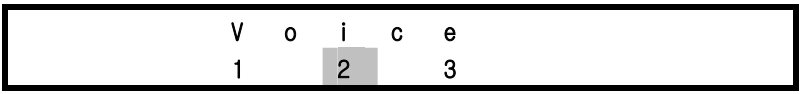


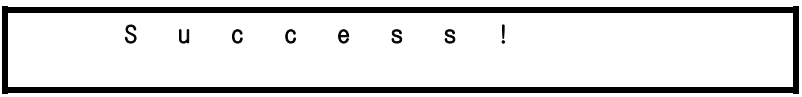


Default Supported Language :

1.Korean, 2.English, 3.Japanese, 4.Chinese,
5.Spanish, 6.French, 7.Thai, 8.Indonesian

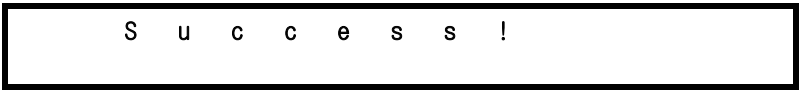
3.4.2.2 Voice Guidelines





3.4.2.3 Button tone

It decides whether you will hear a button tone or not when a specific button is pressed.



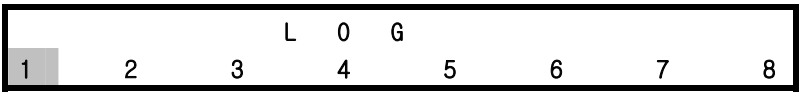
3.3.4 System Setting

The fourth main menu is system setting.

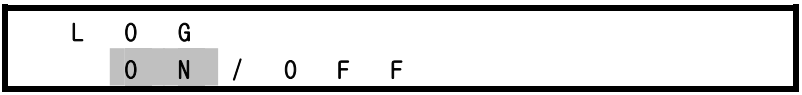
You can then enter into the sub menu of System Option.

3.4.3.1 Log Storage

The first menu decides whether to store log or not.

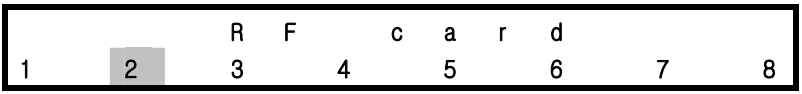


When log is on, relevant authentication log during user authentication is sent to a server.

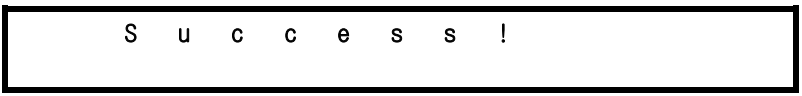


3.4.3.2 RF CARD

It is to select whether RF CARD is used for user authentication.
Please use a directional button and press ENTER to finish.

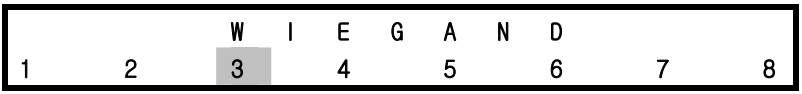


You have three options: OFF RF CARD is not used, 26bit for low frequency HID card, 34bit for high frequency Mifare card.



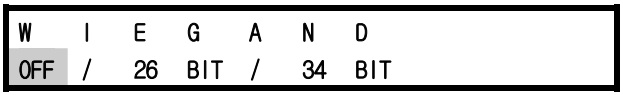
3.4.3.3 Wiegand

It decides whether to use Wiegand communication protocol to send authentication results and user ID to a server.



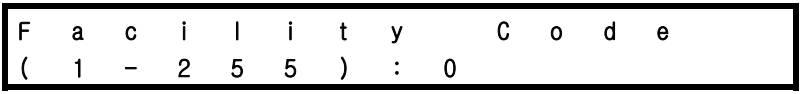
Please press ENTER to go into a sub menu.

Wiegand 통신 프로토콜은 3가지 중 하나를 선택합니다.

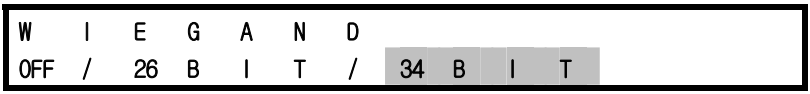


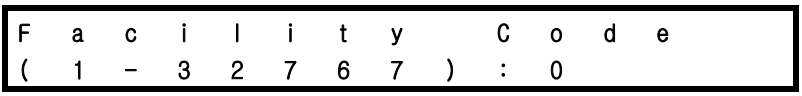
OFF는 Wiegand 출력을 사용하지 않습니다.
다음 단계로는 해당 비트 출력에 대한 Facility Code를 설정합니다.

Facility code for 26 bits has values between 1~255.



Please set the facility code for 34 bits.

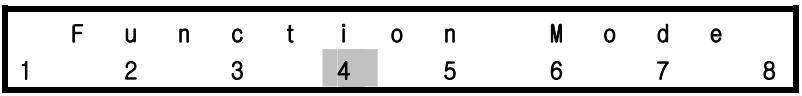




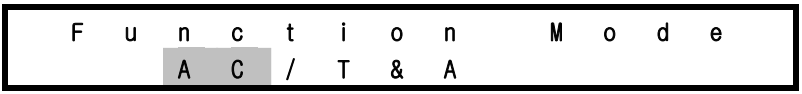
% please refer to the appendix for details about Wiegand output format.

3.4.3.4 Function Key

It decides whether to use Function keys (F1~F4) or not. When access control mode is set, function keys will not be used. Yet, attendance mode will use function keys.



AC refers to access control mode and T&A refers to attendance mode.

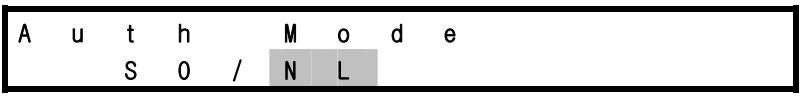


3.4.3.5 Authentication Mode

Please select authentication mode.

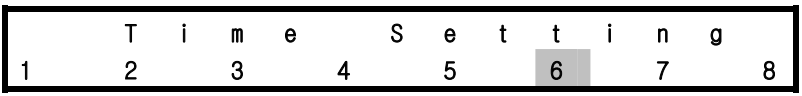
There are 2 modes available. In S0 mode, a terminal is not connected to network and operates standalone. In this case, database only within the terminal is searched for authentication. In NL mode, a terminal is connected to network and it requires a server authentication. Please refer to

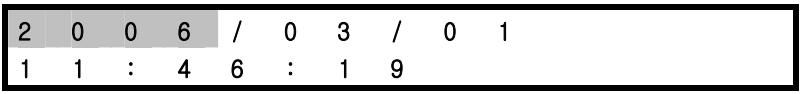
Access manager manual for details on server authentication.



3.4.3.6 Time Setting

You can set time for a terminal.





The setting is sustained for 9 hours during power shortage.

3.4.3.7 Terminal Mode

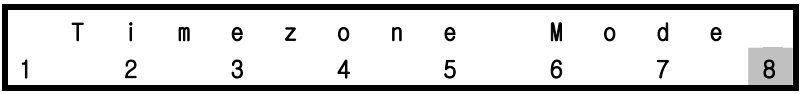
Terminal mode is an option to control Wiegand output. When a terminal is set at normal mode, wiegand output is Facility Code and user ID. If it is set at reader mode, wiegand output is ay values read from a card reader.

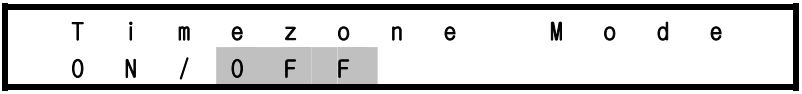
Terminal Mode							
1	2	3	4	5	6	7	8

Terminal Mode							
Reader/Terminal							

3.4.3.8 Time zone

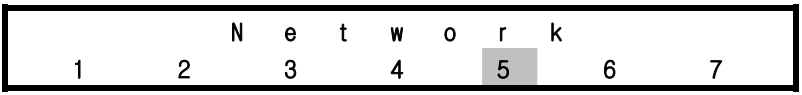
It is to decide whether to use Time zone or not. It Time zone is on, the function will be used. Please refer to Access manager manual for details on the use of time zone.



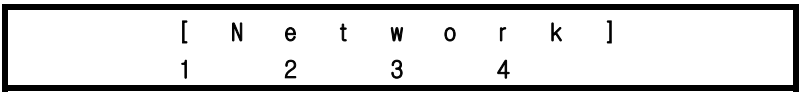


3.4.4 Network Setting

The fifth main menu is network setting.

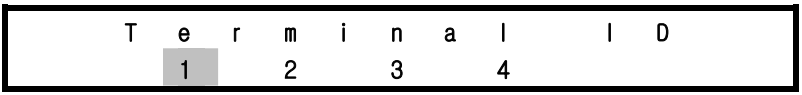


When selecting network setting, you will find the following 4 sub menu.

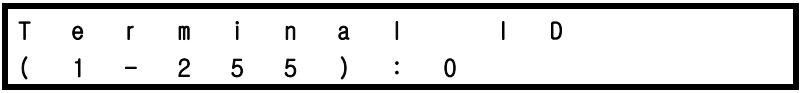


3.4.4.1 Terminal ID

The values for Terminal ID should not be overlapping within one server and a unique number for each terminal is used for network access.

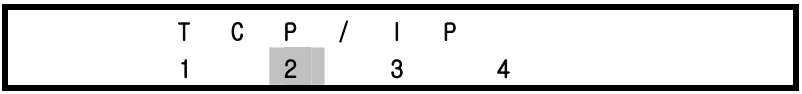


The values can vary between 1~255.



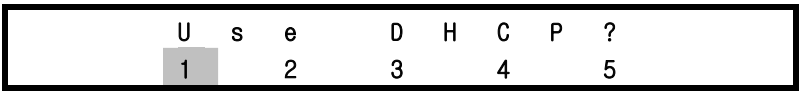
3.4.4.2 TCP/IP

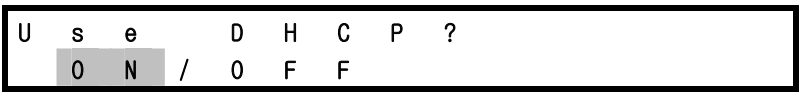
The following is about TCP/IP setting.



There are 5 sub-menus out of which 2 may not appear depending on DHCP setting.

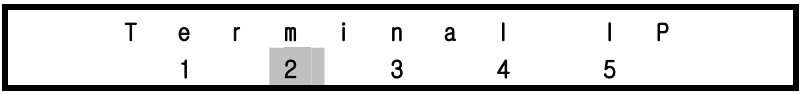
① DHCP





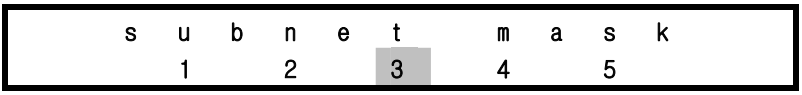
② Terminal IP

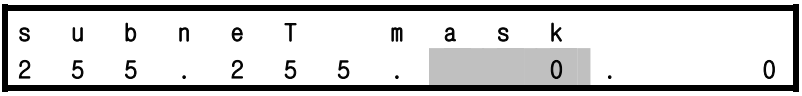
Terminal IP is manually set. It does not appear if DHCP is ON.



③ Subnet Mask

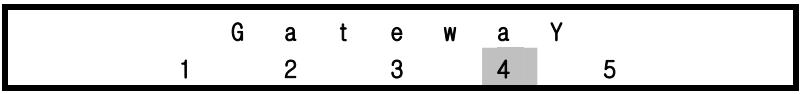
Subnet mask is manually set. It does not appear if DHCP is ON.

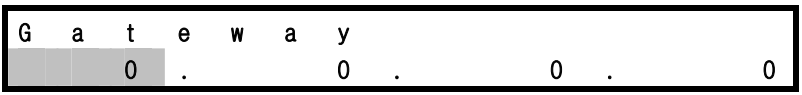




④ Gateway

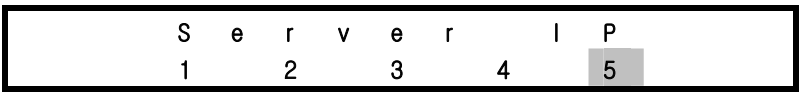
Gateway can be set when needed and it is used mostly when connected to external network. If the system is used only within Intranet, you do not need to input any value for it.





⑤ Server IP

Please input Server IP that has an Access Server installed and the value of the IP should be a fixed IP.

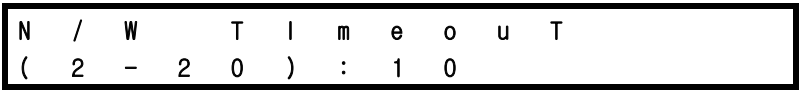


3.4.4.3 Limiting Communication Time

A terminal sends a signal on a regular basis in order to check connection status to a server, and the current menu selects the cycle. The value should be set with an extreme caution and both long and short time have strength and weakness.

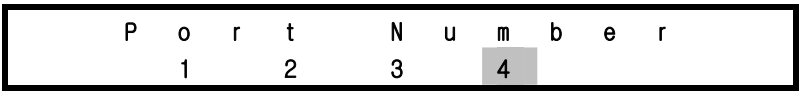
When the time is short, the terminal status is quickly reflected to a server. In turn, longer time makes a response slower. If the value is too small, network connection is on and off continuously if communication lines are not in a good condition.

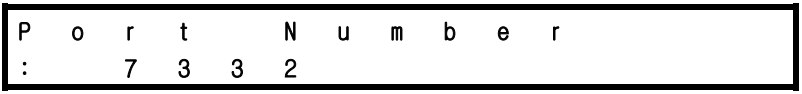
Therefore, this value should be changed depending on network environment and mostly, it is desirable to use factory setting values.



3.4.4.4 Port Setting

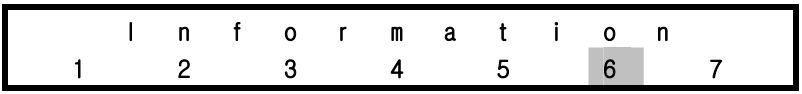
Please input connection port number to be used for a server.
In most cases, factor setting values do not change.





3.4.5 Cofirmation of Terminal Information

You can check terminal information from the sixth main menu.



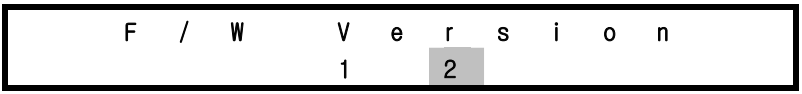
3.4.5.1 Number of Users

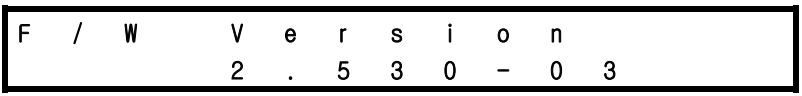
It gives information on the number of users currently registered in a terminal. There are normal users and master users.

Currently, the system has 123 normal users and 4 master users.

3.4.5.2 Version Check

You can find information on the version of firmware in a terminal.

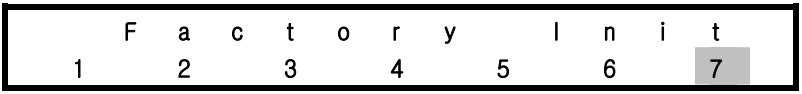




The current firmware version is 2.530-03.

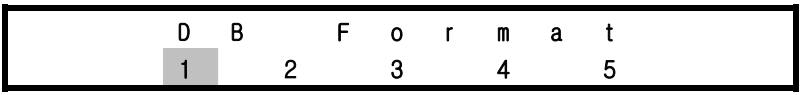
3.4.6 Factory Default Setting

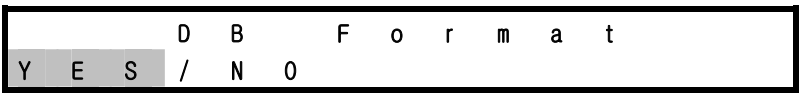
The menu is used only once during factory testing or site installation.

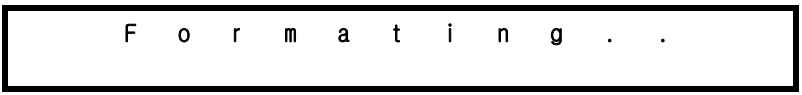


3.4.6.1 DB Format

All DB are formatted.



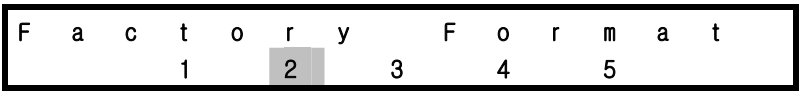


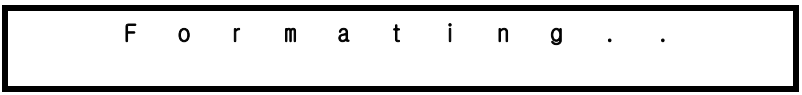


When format is completed, the system goes back to the initial screen.

3.4.6.2 Factory Format

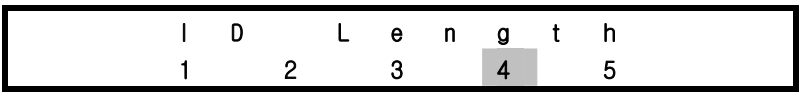
Factory Format is a command to restore all information stored within a terminal into initial values including user DB, option DB, log information and logo. Therefore, the function should be used with an extreme caution.

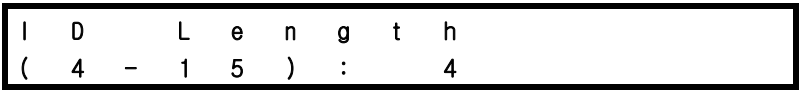




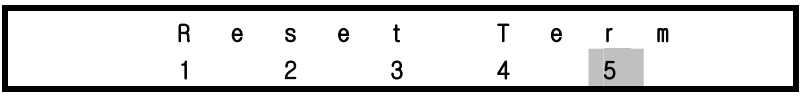
3.4.6.3 Number of Characters in ID

The length of ID for a site will be selected. As the length of ID is a fixed value for each site, the function should be used with an extreme caution. The value cannot be changed if there is DB in existence.





3.4.6.4 Reset Terminal



Terminals can be reset without disassembling. Please choose 『yes』 in a confirmation screen to reset a terminal.

Appendix 1: Network Connection Error and Solutions

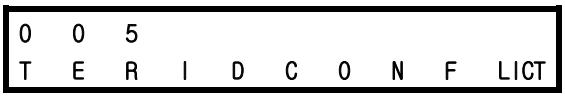
When a terminal is not registered in a server, it should be registered on the server.

When a terminal ID is not valid, please check the ID again and set it again with a valid ID (1~255.)

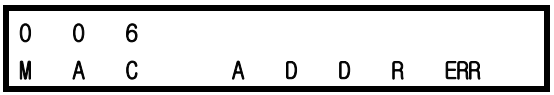
If the number of user ID characters in a server and a terminal is not the same, please set the same number of characters for both IDs.

If the number of registered user fingerprints in a server and a terminal is not the same, please set the same number of fingerprints for the server and the terminal.

When a terminal ID conflicts, please change the terminal ID into an unregistered one.



When MAC Address is not consistent, please contact the customer service center.



Appendix 2: Terminal Initialization Error and Solutions

The following is a list of terminal initialization errors and solutions.

Err. Code	Details	Solution
001	*Unidentified Error*	*Rebooting or A/S*
002	*FPGA Initialization Failure*	*Rebooting or A/S*
003	LCD Initialization Failure	To check LCD module connection or A/S
004	RTC Initialization Failure	A/S
005	Optic module Error	To check Optic module connection or A/S
010	System Software Error	A/S
011		A/S
012		A/S
013		A/S
014		A/S
015		Rebooting
016		A/S

※ Error code 001~003 refer to steps before LCD initialization and therefore do not appear on LCD screen.

Appendix 3: Law and Regulation

Device Type	User Guideline
B-level Device (home communication device)	The device is designed for home users and can be used for all locations including residential areas as it is registered as a qualified device against electromagnetic wave.

Appendix 4: Wiegand Protocol Format

1. Wiegand Input

- 26 Bit

P	8 Bit (site code)	16 Bit (card number)	P

LSB MSB

- 34 Bit

P	16 Bit (site code)	16 Bit (card number)	P

LSB MSB

2. Wiegand Output

- Output: MSB → LSB
- Even Parity: Odd number 1
- Odd Parity: Even number 1

2.1 Terminal mode <Access Controller>

- 26 Bit

P	8 Bit (facility code)	16 Bit (user ID)	P

Even Parity Odd Parity

LSB MSB

- 34 Bit

P	16 Bit (facility code)	16 Bit (user ID)	P

Even Parity Odd Parity

LSB MSB

2.2 Terminal mode <Reader>

Wiegand Input to be used without any change.

Appendix 5 : EMERGENCY Screen

1) EMERGENCY (Door Open)

When a door is forced open by an unauthorized user for access, doors with door sensors detect the attempt and display the following EMERGENCY message.

```
E M E R G E N C Y !
D o o r   O p e n !
```

In this case, the emergency will be cancelled when the door is checked by a system manager who enters into the menu in a terminal. Please check the following if the emergency message continuously appears.

Door sensor Y or N	Check
Yes	- operation of door sensor - connection status of door sensor
No	If warning time for “door open” is set at 0 (see 2.4 Door Setting)