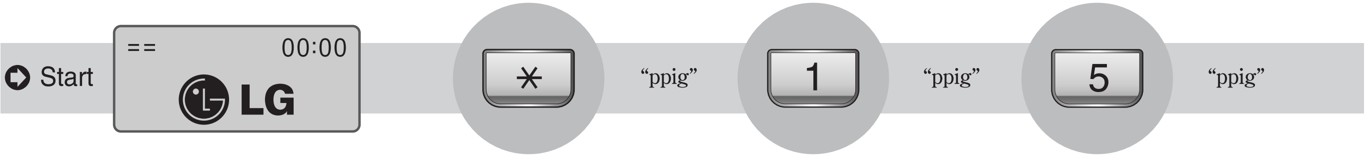
3. Configuration settings

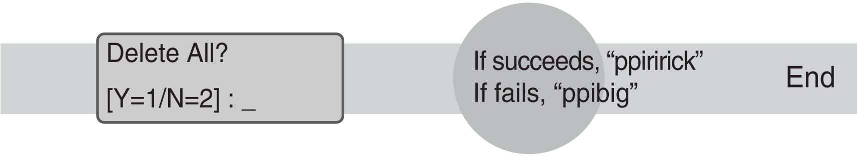
3.3.5. Delete All Users



Press [*] for over 2 sec. to enter main menu.

Press [1] to register a new user.

Press [5].



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

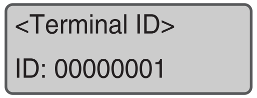
- If succeeds, it deletes all.
- If fails, it returns to the '5. Delete All' screen.

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

3.4. Network settings

□ In the main menu, press [2] to select ‘2.Network’ to see the following screen.
When this setting is done, press [ENTER] to move to the next setting.

3.4.1. Terminal ID

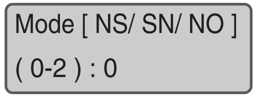

<Terminal ID>
ID: 00000001

- Press [ENTER] to move to the next setting.

Default screen ➔ [*] ➔ [2]

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

3.4.2. Connection mode


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

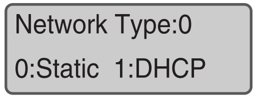
- Press [ENTER] to move to the next setting.

Default screen ➔ [*] ➔ [2] ➔ [ENTER]

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

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

3.4.3. Connection method



Network Type:0

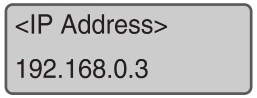
0:Static 1:DHCP

- Press [ENTER] to move to the next setting.

Default screen ➔ [*] ➔ [2] ➔ [ENTER] ➔ [ENTER]

- Press [0] for Static IP, the default is ‘0’.
- Press [1] for DHCP.
- For static IP settings, refer to ‘3.4.4. IP address’, ‘3.4.5. Subnet mask’ and ‘3.4.6. Gateway’. In case of dynamic IP, there is no need for additional settings.

3.4.4. IP address



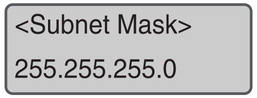
<IP Address>

192.168.0.3

- Press [ENTER] to move to the next setting.

- Press [#] to delete an old IP and enter the new IP.
- If the IP address is ‘210.98.100.50’, enter as below:
  [2] [1] [0] [9] [8] [*] [1] [0] [0] [5] [0]

3.4.5. Subnet mask



<Subnet Mask>

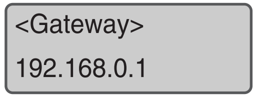
255.255.255.0

- Press [ENTER] to move to the next setting.

- Press [#] to delete an old value and enter the new value.
- If the subnet mask is ‘255.255.255.0’, enter as below:
  [2] [5] [5] [2] [5] [5] [2] [5] [5] [0]

3.4. Network settings

3.4.6. Gateway

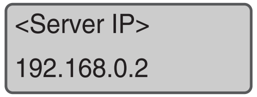


<Gateway>
192.168.0.1

- Press [ENTER] to move to the next setting.

- Press [#] to delete an old value and enter the new value.
- If the gateway IP address is '210.98.100.1', enter as below:
  [2] [1] [0] [9] [8] [*] [1] [0] [0] [1]

3.4.7. Server IP

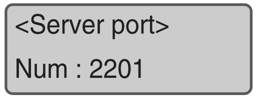


<Server IP>
192.168.0.2

- Press [ENTER] to move to the next setting.

- Press [#] to delete an old value and enter the new value.
- If the sever address is '210.98.100.121', enter as below:
  [2] [1] [0] [9] [8] [*] [1] [0] [0] [1] [2] [1]

3.4.8. Server port



<Server port>
Num : 2201

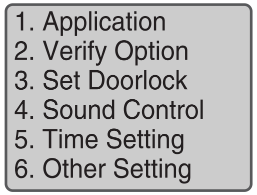
- After the network setting is completely done, press [ENTER] to return to the main menu.

- Press [#] to delete an old value and enter the new value.
- As the port number of the authentication server, the default is '2201'. Special care is required when changing this number because the corresponding number in the server should also be changed with the same number.
- If the server port is '2201', enter as below:
  [2] [2] [0] [1]

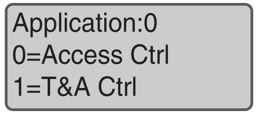
3. Configuration settings

3.5. Option settings

3.5.1. Application mode

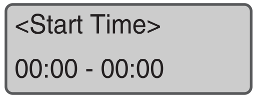


1. Application
2. Verify Option
3. Set Doorlock
4. Sound Control
5. Time Setting
6. Other Setting



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

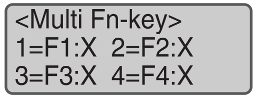
- Press [ENTER] to move to detailed settings for each operation mode.



<Start Time>

00:00 - 00:00

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

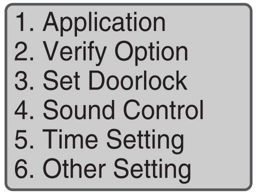


<Multi Fn-key>
1=F1:X 2=F2:X
3=F3:X 4=F4:X

Default screen ➔ [*] ➔ [3] ➔ [1]

- The default is '0=Access Ctrl'
- For access control application, set as '0'. For time & attendance, set as '1'.
- Access control
  - There are no detailed settings under access control application here. It moves to the upper menu.
- Time attendance control
  - By setting up those default times regarding Start/Leave/Out/Back, the terminal display mode after authentication can be automatically changed to programmed time & attendance mode. In addition, by using multi-Fn key, over 40 sub modes of time & attendance can be defined.
  - If time setting is not necessary, set as '00:00-00:00'
  - To change the start time from '00:00~00:00' to '06:00~09:59', press [#] to delete the existing setting time, and enter [0] [6] [0] [0] [0] [9] [5] [9] in sequence.
  - As long as no other function button is pressed during the setting time, it operates in start time mode. Even if the authentication for outside work (Out) happens by pressing [F3] function key, the terminal display mode after the authentication of outside work is automatically changes to start time mode, which is very convenient for users in time & attendance mode.
  - After setting <start time>, set <leave time> and <normal time> in the same manner. Note that each time must not overlap. Ex.)start time : '06:00~09:59', leave time : '17:00~22:00' and normal time : '10:00~16:59'.
- Multi Fn-key
  - Default setting: all 'X'
  - This menu is useful when more than 5 time & attendance modes are necessary.
  - When setting as 'X' : each function key represents a specific working mode such as F1=Start, F2=Leave, F3=Outside work (out) and F4=Back. When a function key is pressed, authentication mode is changed to the corresponding working mode.
  - When setting as 'O' : a mode is defined by the combination of a function key and a number key such as 'F3+1'. For example, if the setting is 1=F1: X 2=F2: X 3=F3: X 4=F4: O, 14 different working modes can be defined according to user input such as [ENTER]: normal, [F1]: start, [F2]: leave, [F3]: outside work(out), and [F4]+'0' ~ [F4]+'9'.
  - The O/X setting can be changed by pressing the corresponding number key. After setting is completed, press [ENTER] to move to the upper menu.

3.5.2. Option settings for authentication

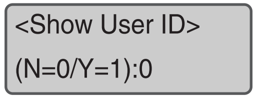


1. Application
2. Verify Option
3. Set Doorlock
4. Sound Control
5. Time Setting
6. Other Setting

Default screen ➔ [*] ➔ [3] ➔ [2]

- To set the basic option for authentication, press [2].

3.5.2.1. Settings for ID display when authentication is successful



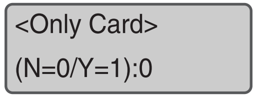
<Show User ID>

(N=0/Y=1):0

- Press [ENTER] to move to the next setting.

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

3.5.2.2. Settings for only card authentication



<Only Card>

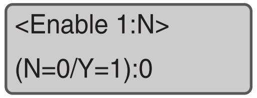
(N=0/Y=1):0

- Press [ENTER] to move to the next setting.

Default screen ➔ [*] ➔ [3] ➔ [2] ➔ [ENTER]

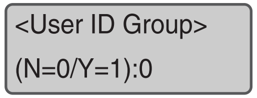
- Default setting : ‘0’
- Even if a user is registered to be authenticated with a card & password or a card & fingerprint, if it is set to ‘1’, a user can get access to an area through the relevant terminal only by using a card.
- This function is useful at building entrance door - among other places of a building with several installed terminals - where there is frequent entrance and exit and there is no need for severe access control.

3.5.2.3. 1:N authentication settings


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

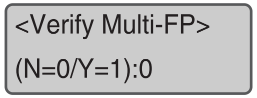
Default screen ➡ [*] ➡ [3] ➡ [2] ➡ [ENTER] ➡ [ENTER]

- Default setting : ‘1’.
- This enables fingerprint authentication without inputting a user ID or placing a card. For your information, even if a user is registered to be authenticated with 1:N authentication, only 1:1 authentication is allowed in the terminal if this is set to ‘0’.
- In cases that ID input or fingerprint authentication after placing a card - when card input replaces ID input - is unavoidably needed, it should be set to ‘0’.
- The followings are detailed settings about whether 1:N authentication is allowed or not.


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

■ When 1:N authentication is allowed as setting of ‘1’

- Default setting : ‘0’.
- If this setting is set to ‘1’, inputting fore part of ID digits stands for a specific group, which speeds up 1:N authentication by searching for same fingerprint only among the specific group. This faster matching speed is very useful in case that over 1,000 users are registered.
- If it is set to ‘1’, as mentioned above, fingerprint matching is executed only among the user group starting with the same fore part of ID digits. If it is set to ‘0’, inputted numbers is considered just as user’s ID and only 1:1 authentication is executed.
- For example, when a user ID is a 4-digit number and ‘12’ is inputted for authentication, if it is set to ‘1’, 1:N authentication is performed among user IDs ‘1200’~‘1299’. If it is set to ‘0’, 1:1 authentication only for user ID No. 12 is performed.


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

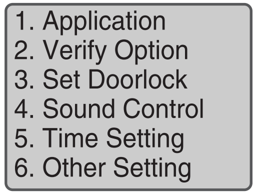
- After the setting is completely done, press [ENTER] to move to the upper menu.

■ When 1:N authentication is not allowed as setting of ‘0’

- Default setting : ‘0’.
- If it is set to ‘1’, for successful authentication, all registered fingerprints should be authenticated after ID (or card) input.
- This is used when a high security level is required for special areas. If a user of ‘ID 0001’ has 3 fingerprints registered to the unit, all 3 fingerprints should be authenticated after ID input.
- The authentication sequence for the 3 fingerprints does not matter in this case, but whole authentication fails if a single fingerprint is not successfully authenticated.

3. Configuration settings

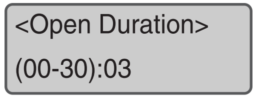
3.5.3. Doorlock


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

Default screen ➔ [*] ➔ [3] ➔ [3]

- Press [3] for door settings.

3.5.3.1. Door opening time


<Open Duration>

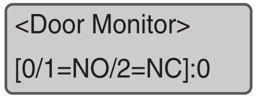
(00-30):03

- After this setting is completely done, press [ENTER] to move to the next setting.

Default screen ➔ [*] ➔ [3] ➔ [3]

- Default setting : ‘03’ (unit: sec.)
- This is used to set the door opening time after authentication is successfully done. This means the door opening time only for strike type but is not applicable to dead bolt type or auto door.
- If this is set to ‘00’, the door control in access control mode is out of control. Therefore, ‘00’ setting may be possible only for time & attendance mode, where there is no need for lock control.

3.5.3.2. Door status monitor


<Door Monitor>

[0/1=NO/2=NC]:0

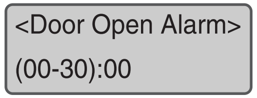
- Once the setting is completely done, Press [ENTER] to move to the next setting

Default screen ➔ [*] ➔ [3] ➔ [3] ➔ [ENTER]

- Default setting : ‘0’
- ‘0’ setting is for no monitoring, ‘1’ setting is for dead bolt type or auto door and ‘2’ setting is for strike type.
- When this is set to ‘1’ or ‘2’, the door status through connected terminal is periodically transmitted to the server.

[0]	NW - No monitoring
[1]	NO - Dead bolt type or auto door (In case that lock monitoring pin is low when the door is locked)
[2]	NC - Strike type (In case that lock monitoring pin is high when the door is locked)

3.5.3.3. Door open alarm

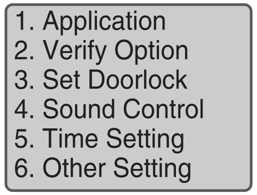

<Door Open Alarm>
(00-30):00

- Once the setting is completely done, press [ENTER] to move to the upper menu.

Default screen ➔ [*] ➔ [3] ➔ [3] ➔ [ENTER] ➔ [1] or [2] ➔ [ENTER]

- Default setting : ‘00’
- For smoothly operation of this setting, the relevant lock should be the lock type to be able to monitor whether the door is open or closed and its monitoring pin should properly be connected to the terminal. The previously mentioned setting for monitoring door status should be set to ‘1’ or ‘2’ for this operation.

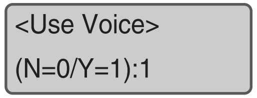
3.5.4. Volume


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

Default screen ➔ [*] ➔ [3]

- Press [4] for volume settings.

3.5.4.1. Voice

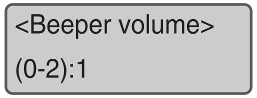

<Use Voice>
(N=0/Y=1):1

- Press [ENTER] to move to the next setting.

Default screen ➔ [*] ➔ [3] ➔ [4]

- Default setting : ‘1’
- To make voice information about terminal control available, set it to ‘1’. If not, set it to ‘0’.

3.5.4.2. Buzzer volume

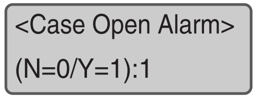

<Beeper volume>
(0-2):1

- Press [ENTER] to move to the next setting.

Default screen ➔ [*] ➔ [3] ➔ [4] ➔ [ENTER]

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

3.5.4.3. Case open alarm



<Case Open Alarm>

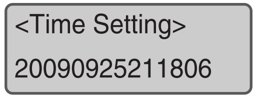
(N=0/Y=1):1

Default screen ➔ [*] ➔ [3] ➔ [4] ➔ [ENTER] ➔ [ENTER]

- Default setting : ‘1’
- An alarm sounds if the terminal case is damaged or opened. For this setting, VIRDI 4000 series have case open sensor installed.

- After this setting is completely done, press [ENTER] to move to the next setting.

3.5.5. Current time



<Time Setting>

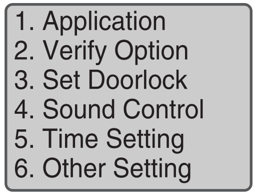
20090925211806

Default screen ➔ [*] ➔ [3] ➔ [5]

- This is to set the terminal current time. The above example represents the year 2009, month 9, date 25, hour 21, min. 18, and sec. 06. To change it, delete the old numbers with the [#] button before adding the new numbers.

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

3.5.6. Other

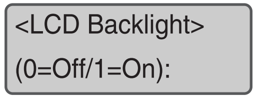


1. Application
2. Verify Option
3. Set Doorlock
4. Sound Control
5. Time Setting
6. Other Setting

Default screen ➔ [*] ➔ [3] ➔ [6]

- Press [6] for other settings.

3.5.6.1. LCD Backlight On/Off



<LCD Backlight>

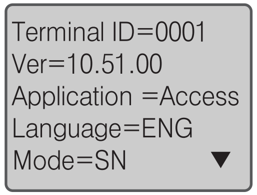
(0=Off/1=On):

Default screen ➔ [*] ➔ [3] ➔ [6]

- Default setting : ‘0’.
- This is to set LCD backlight. If it is set to ‘1’, LCD backlight is on all the times. On the other hand, if it is set to ‘0’, the LCD backlight is normally off and keypad operation or placing a card makes the backlight on. Since it has passed 10 seconds after relevant operation is done, backlight becomes off.

- After the setting is completely done, press [ENTER] to move to the upper menu.

3.6. Terminal information view



Terminal ID=0001
Ver=10.51.00
Application =Access
Language=ENG
Mode=SN ▼

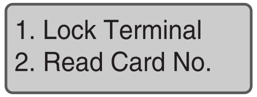
Default screen ➔ [*] ➔ [4]

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

Terminal ID	Terminal ID
Version	Terminal firmware version
Application	Terminal application mode (Access/T&A)
Language	Language for text and voice of the LCD screen
Mode	Connection mode between terminal and network server
Network type	Network connection type (static IP/DHCP)
Mac address	Terminal ethernet hardware address
IP address	Terminal IP address
Gateway	Terminal gateway address
Subnet mask	Terminal subnet mask address
Server IP	IP address of network server connected to the terminal
Svr-port	Port number of network server program
Card Reader	Card reader type
FP-Sensor	Fingerprint sensor type
1:1 Level	Identification level for 1:1 authentication
1:N Level	Identification level for 1:N authentication
Max User	Maximum user capacity to be able to be registered to a terminal
Max FP	Maximum fingerprint capacity to be able to be registered to a terminal. For example, if there are 100 registered users and two fingerprints per user are registered, it means a total of 200 fingerprints is registered.
All User	Number of current users registered to a terminal including administrators
All Admin	Number of administrators registered to a terminal
All FP	Number of fingerprints currently registered to a terminal
1:N User	Number of users for 1:N authentication
1:N FP	Number of fingerprints for 1:N authentication
All Log	Authentication records stored in a terminal

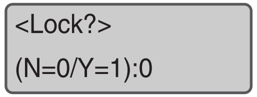
3.7. Extra functions

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



1. Lock Terminal
2. Read Card No.

3.7.1. Terminal lock



<Lock?>

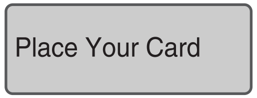
(N=0/Y=1):0

- After the setting is completely done, press [ENTER] to move to the upper menu.

Default screen ➲ [*] ➲ [5] ➲ [1]

- Default setting ‘0’ : Releasing terminal lock
  ‘1’ : Setting terminal lock
- An administrator in local terminal ? not by server program - can directly set up or release the terminal lock to the local terminal. If it is set to ‘1’, the terminal is locked and nobody is accessible to the specific area through locked terminal until the administrator unlocks the terminal.
- For this setting, ‘Allow admin to access’ in terminal configuration of server program should be permitted.

3.7.2. Read card number



Place Your Card

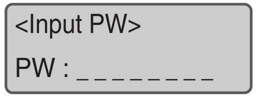
- To exit from this setting, press [#] to move to the upper menu.

Default screen ➲ [*] ➲ [5] ➲ [2]

- This is an extra function which is not related to terminal configuration settings. By using this function, an administrator can read the card number when she/he places a card to the terminal mounted with card reader, in order to register the placed card to server. If this LCD screen pops up and then an administrator places a card to the terminal, the card number shows in the LCD screen.

3.8. Device settings

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

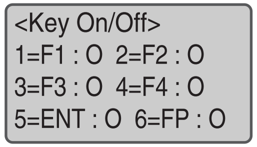


```
<Input PW>
PW : _ _ _ _ _ _ _ _
```

Default screen ➔ [*] ➔ [6]

- In the most of cases, There is no need for modifying the device settings after installation. Therefore, be careful not to modify the device settings without any obvious reasons.
- This previously set password from factory is to call administrator’s attention, which is fixed one and should not be changed.
- Input ‘084265’ as the previously set password and press [ENTER] to show the detailed setting items.

3.8.1. Function key



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

- After the setting is completely done, press [ENTER] to move to the upper menu.

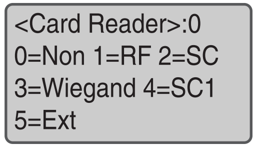
Default screen ➔ [*] ➔ [6] ➔ ‘084265’+[ENTER] ➔ [1]

- Default setting : all ‘O’
- This is to enable or disable the function keys. ‘O’ means enabling the function key and ‘X’ means disabling the function key. Whenever the number conformed to a function key in this setting is pressed, this setting is changed between ‘O’ and ‘X’.
- In this setting, 1 conforms to [F1], 2 conforms to [F2], 3 is for [F3] and 4 is for [F4]. For example, if an administrator presses [1] one time in this setting and [F1] key is disabled - [X], a user can not enter into start mode by pressing [F1] key button as [F1] key is disabled.
- Additionally, if only [F1] or [F2] is set to ‘O’, the terminal can be used in either always start or always leave mode.
- 6 (FP) is used for setting detection function of fake finger.

3. Configuration settings

3.8.2. Card reader

3.8.2.1. Card reader type setting



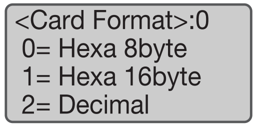
```
<Card Reader>:0
0=Non 1=RF 2=SC
3=Wiegand 4=SC1
5=Ext
```

- After the setting is completely done, press [Ent] to move to the next menu.

Default screen → [*] → [6] → ‘084265’+[Ent] → [2]

- Default setting : ‘0’
- This is to set the card reader mounted in a terminal. Refer to the followings for correct setting:
  - ‘0’ : No card reader
  - ‘1’ : Low-frequency RF Card reader mounted
  - ‘2’ : High-frequency smart card reader
  - ‘3’ : Wiegand card reader like HID card module
  - ‘4’ : Other smart RF reade
  - ‘5’ : External card reader
- If a card reader is mounted into a terminal and the above setting is correctly done, when [F1]~[F4] or [Ent] is pressed, the authentication mode is changed and 1:1 fingerprint authentication is ready for operation - in this case, 1:N fingerprint authentication is not performed except for auto sensing setting.

3.8.2.2. Card reader format setting



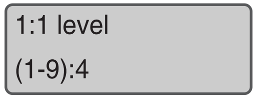
```
<Card Format>:0
 0= Hexa 8byte
 1= Hexa 16byte
 2= Decimal
```

- After the setting is completely done, press [Ent] to move to the upper menu.

- Default setting : ‘0’
- Set up format of data from card reader
  - 0: Hexa data value with 8byte
  - 1: Hexa data value with 16byte
  - 2: Decimal data value

3.8.3. Fingerprint sensor

3.8.3.1. 1:1 verification level



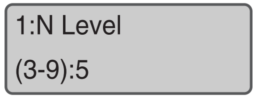
1:1 level
(1-9):4

- Press [ENTER] to move to the next setting.

Default screen ➔ [*] ➔ [6] ➔ ‘084265’+[ENTER] ➔ [3]

- Default setting : ‘4’.
- This is to set 1:1 matching security level for a terminal between the fingerprint captured from fingerprint input window and the relevant fingerprint stored in a terminal. The higher 1:1 matching level means the higher security. But possibility of authentication failure is getting higher as higher matching rate is required.
- For an example of 1:1 authentication with ID input, if inputted ID number is ‘1234’, there is authentication process between the fingerprint captured from fingerprint input window and the fingerprint associated with ID ‘1234’ in a terminal.

3.8.3.2. 1:N identification level



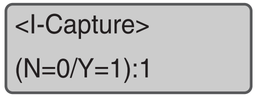
1:N Level
(3-9):5

- Press [ENTER] to move to the next setting.

Default screen ➔ [*] ➔ [6] ➔ ‘084265’+[ENTER] ➔ [3] ➔ [ENTER]

- Default setting : ‘5’
- This is to set 1:N authentication security level between the fingerprint captured from fingerprint input window and all the fingerprints in a terminal which are allowed for 1:N authentication.
- For your information, 1:N authentication level is not set for respective user but only for a terminal.

3.8.3.3. Intelligent-Capture

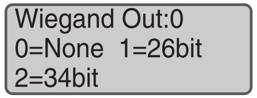

<I-Capture>
(N=0/Y=1):1

- After the setting is completely done, press [ENTER] to move to the upper menu.

Default screen → [*] → [6] → '084265'+[ENTER] → [3] → [ENTER] → [ENTER]

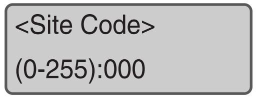
- Default setting : '1'
- This adjusts the sensor settings automatically to enhance good fingerprint detection capability by reducing bad influences from humid fingers and/or residual fingerprints which are left on a sensor window due to sweat and/or contaminants on fingertip.
- If it is set to '0', fingerprint capturing time gets shorter but its authentication rate for dry or wet finger becomes lower.
- If it is set to '1', fingerprint capturing time becomes longer than that of above '0' setting but its authentication rate gets higher. Therefore, '1' setting is recommended.

3.8.4. Wiegand output


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

Default screen → [*] → [6] → '084265'+[ENTER] → [4]

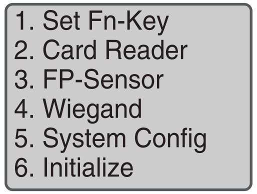
- Default setting : '0'
- If Wiegand output from the local terminal is needed for external access controller with Wiegand input, an administrator can set this setting as '1' or '2'.
  - In case of '1' setting, "site code [1 byte] and user ID [2 bytes]" are transmitted through Wiegand output port. User ID should be set as less than 4 digits.
  - In case of '2' setting, "site code [1 byte] and user ID [3 bytes]" are transmitted through Wiegand output port. User ID should be set as less than 7 digits.
- This setting is not related to external Wiegand reader.
- In cases of '1' or '2' settings, the below-mentioned site code should be set.
  - Default setting : '000'.
  - An administrator can assign the site code of from 0 to 255 which is transmitted together with a user ID.


<Site Code>
(0-255):000

- After the setting is completely done, press [ENTER] to move to the upper menu.

3. Configuration settings

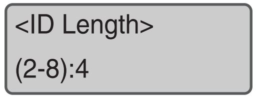
3.8.5. System configuration



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

Default screen ➔ [*] ➔ [6] ➔ ‘084265’+[ENTER] ➔ [5]

3.8.5.1. User ID length



<ID Length>

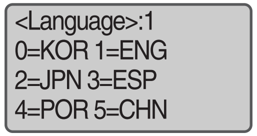
(2-8):4

- Press [ENTER] to move to the next setting.

Default screen ➔ [*] ➔ [6] ➔ ‘084265’+[ENTER] ➔ [5]

- Default setting : ‘4’
- This ID length can be 2~8 digits and should be the same as that of ID registered in the server program. If the ID registered in the server program is ‘000075’, input ‘6’.
- With modifying this ID length shorter than before during normal operation after installation, an administrator may not be able to be authenticated and enter into main menu if she/he has longer ID length, compared to the modified ID length. Therefore, be careful to give serious consideration before modifying the ID length.

3.8.5.2. Language



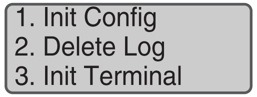
<Language>:1
0=KOR 1=ENG
2=JPN 3=ESP
4=POR 5=CHN

- After the setting is completely done, press [ENTER] to move to the upper menu.

Default screen ➔ [*] ➔ [6] ➔ ‘084265’+[ENTER] ➔ [5] ➔ [ENTER]

- Default setting : ‘1’ (English)
- Voice output languages are as follow, ‘0’: Korean, ‘1’: English, ‘2’: Japanese, ‘3’: Spanish, ‘4’: Portuguese and ‘5’: Chinese.
- LCD characters correspond to the assigned language.

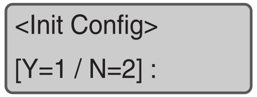
3.8.6. Terminal initialization


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

Default screen ➲ [*] ➲ [6] ➲ ‘084265’+[ENTER] ➲ [6]

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

3.8.6.1. Configuration settings initialization


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

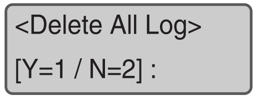
Default screen ➲ [*] ➲ [6] ➲ ‘084265’+[ENTER] ➲ [6] ➲ [1]

- To initialize configuration settings, press [1]. If not, press [2].
- All the configuration settings except for Mac (physical) address are initialized; user’s information and authentication records are not deleted.

※If this configuration settings initialization is done, the language for voice output and display characters is changed to English. If you need to set as other language, refer to ‘3.8.5.2. Language’.

- After this configuration setting initialization is successfully done, it moves to the upper menu together with a ‘ppiririck’ buzzer sound.

3.8.6.2. Authentication record initialization

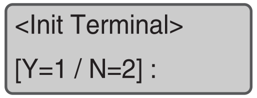

<Delete All Log>
[Y=1 / N=2] :

Default screen ➲ [*] ➲ [6] ➲ ‘084265’+[ENTER] ➲ [6] ➲ [2]

- To initialize the log data, press [1]. If not, press [2].
- All the log data related to authentication are deleted; configuration settings and user’s information are not deleted.

- After this configuration setting initialization is successfully done, it moves to the upper menu together with a ‘ppiririck’ buzzer sound.

3.8.6.3. Factory default initialization


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

Default screen ➲ [*] ➲ [6] ➲ ‘084265’+[ENTER] ➲ [6] ➲ [3]

- To initialize everything to factory default, press [1]. If not, press [2].
- Except for the Mac (physical) address stored in the terminal, all configuration settings, user’s information and authentication records (log data) are deleted, which becomes same as factory default.
- If this factory default initialization is done, the language for voice output and display characters is changed to English. If you need to set as other language, refer to ‘3.8.5.2. Language’.

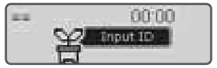
- After this configuration setting initialization is successfully done, it moves to the upper menu together with a ‘ppiririck’ buzzer sound.

4. How to use

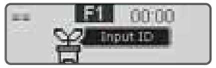
4.1. Access control application

□ Default screen ➔ [*] ➔ [3] Option ➔ [1] Application ➔ [0] for access control application

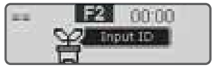
4.1.1. Authentication mode



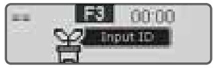
- Normal mode ; authentication with [ENTER]



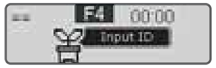
- F1 mode ; authentication with [F1]



- F2 mode ; authentication with [F2]



- F3 mode ; authentication with [F3]



- F4 mode ; authentication with [F4]

- Fingerprint authentication
  - Fingerprint authentication in the corresponding mode by pressing a relevant function key; [Enter], [F1], [F2], [F3] and [F4]. Fingerprint authentication through auto sensing without pressing any keys. This authentication is performed in the current mode displayed in the screen.
- Password authentication
  - After inputting the user ID and changing the authentication mode by pressing the corresponding function key, input the password for authentication.
- Card authentication after the following settings are done : menu ➔ '6.Device' settings ➔ '2.Card reader' ➔ <Card Reader> is set to [1] or over
  - Pressing the function key changes just authentication mode. For card authentication, press the corresponding function key and then place the card close to the terminal.