

AY-B9250BT

Professional Fingerprint Reader

User Manual



Copyright © 2019 by Rosslare. All rights reserved.

This manual and the information contained herein are proprietary to ROSSLARE ENTERPRISES LIMITED and/or its related companies and/or subsidiaries' (hereafter: "ROSSLARE"). Only ROSSLARE and its customers have the right to use the information.

No part of this manual may be re-produced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of ROSSLARE.

ROSSLARE owns patents and patent applications, trademarks, copyrights, or other intellectual property rights covering the subject matter in this manual.

TEXTS, IMAGES, AND ILLUSTRATIONS INCLUDING THEIR ARRANGEMENT IN THIS DOCUMENT ARE SUBJECT TO THE PROTECTION OF COPYRIGHT LAWS AND OTHER LEGAL RIGHTS WORLDWIDE. THEIR USE, REPRODUCTION, AND TRANSMITTAL TO THIRD PARTIES WITHOUT EXPRESS WRITTEN PERMISSION MAY RESULT IN LEGAL PROCEEDINGS.

The furnishing of this manual to any party does not give that party or any third party any license to these patents, trademarks, copyrights or other intellectual property rights, except as expressly provided in any written agreement of ROSSLARE.

ROSSLARE reserves the right to revise and change this document at any time, without being obliged to announce such revisions or changes beforehand or after the fact.

Table of Contents

- Table of Contents 3**
- 1. Before Getting Started 5**
 - 1.1. Safety Notes 5**
 - 1.2. Product Details 6**
 - 1.2.1. FRONT 6
 - 1.2.2. REAR 7
 - 1.2.3. Input / Output 8
 - 1.3. Screen information during operation 9**
 - 1.3.1. Initial Screen 9
 - 1.3.2. Icons 9
 - 1.3.3. Function KEY 10
 - 1.3.4. Main Screen 10
 - 1.4. LED information during operation 12**
 - 1.5. Voice information during operation 12**
 - 1.6. Buzzer guide announced during operation 12**
 - 1.7. How to register and enter the correct fingerprint 13**
- 2. Product Description 14**
 - 2.1. Product Features 14**
 - 2.2. Diagram 15**
 - 2.2.1. Single Type (Door Lock) 15
 - 2.2.2. Single Type (Lock Controller) 15
 - 2.2.3. Dummy Type 15
 - 2.2.4. Network Type (Door Lock) 16
 - 2.2.5. Network Type (Lock Controller) 16
 - 2.3. Product Specification 17**
- 3. Environment Setting 18**
 - 3.1. Checkpoints before Environment Setting 18**
 - 3.1.1. Menu 18
 - 3.1.2. Administration authentication 18
 - 3.1.3. How to access the menu without administrator authentication 19
 - 3.1.4. Save Settings 19
 - 3.1.5. Default Setting 20
 - 3.1.6. Setting guide for Network Configuration 21
 - 3.2. Access and Registration between Rosslare Bio9000 and terminal 22**
 - 3.2.1. Install Rosslare Bio9000 22
 - 3.2.2. Execute Rosslare Bio9000 22
 - 3.2.3. Set in terminal 23
 - 3.2.4. LAN connection in terminal 23
 - 3.2.5. Register the terminal in Rosslare Bio9000 24
 - 3.3. Menu Configuration 25**
 - 3.4. USER Menu 30**
 - 3.4.1. ADD 30
 - 3.4.2. AUTO ADD 32
 - 3.4.3. MODIFY 33
 - 3.4.4. DELETE 34
 - 3.4.5. DELETE ALL 34
 - 3.5. NETWORK Menu 34**
 - 3.5.1. AUTH Mode 35
 - 3.5.2. Terminal ID 36
 - 3.5.3. Terminal 36
 - 3.5.4. Server 37
 - 3.6. OPTION Menu 37**

| | | |
|--------------------|--|-----------|
| 3.6.1. | ATTEND | 38 |
| 3.6.2. | Screen..... | 39 |
| 3.6.3. | SAVE | 42 |
| 3.6.4. | TIMEOUT | 43 |
| 3.6.5. | LOCKING..... | 44 |
| 3.7. | INT DEVICE Menu..... | 45 |
| 3.7.1. | FP SENSOR | 45 |
| 3.7.2. | BEEP | 47 |
| 3.7.3. | VOICE | 47 |
| 3.7.4. | BLE | 47 |
| 3.7.5. | TAMPER | 47 |
| 3.8. | EXT DEVICE Menu | 48 |
| 3.8.1. | DOORLOCK | 48 |
| 3.8.2. | RS485 | 51 |
| 3.8.3. | WIEGAND | 51 |
| 3.9. | STATUS Menu | 53 |
| 3.9.1. | DB INFO | 54 |
| 3.9.2. | NETWORK..... | 54 |
| 3.9.3. | OPTION | 54 |
| 3.9.4. | INT DEVICE | 54 |
| 3.9.5. | EXT DEVICE..... | 55 |
| 3.9.6. | I/O PORT | 55 |
| 3.9.7. | VERSION..... | 55 |
| 3.10. | RECOVERY Menu..... | 55 |
| 3.10.1. | INITIALIZE..... | 56 |
| 3.10.2. | SELF TEST | 57 |
| 3.10.3. | BACKUP | 60 |
| 3.10.4. | REBOOT | 61 |
| Appendix 1. | Glossary | 62 |
| Appendix 2. | Declaration of Conformity | 63 |
| Appendix 3. | Radio Equipment Directive (RED) | 64 |
| Appendix 4. | RoHS Directive | 65 |

1. Before Getting Started

1.1. Safety Notes

● **Warning**

| | | | |
|--|--|--|--|
| <p>Do not operate the terminal with wet hands, and pay attention not to let any liquid such as water enter inside the terminal. - > Otherwise, malfunction or electric shock may be caused.</p> | | <p>Keep the terminal away from inflammables. - > Otherwise, it may cause a fire.</p> | |
| <p>Do not disassemble, repair or remodel the terminal at your disposal. - > Otherwise, it may cause malfunction, electric shock, or a fire.</p> | | <p>Do not allow children to touch the terminal carelessly. - > Otherwise, it may cause safety accidents of children or malfunction.</p> | |

- Non-compliance of safety notes may cause death or serious injury for users.

● **Cautions**

| | | | |
|--|--|---|--|
| <p>Do not install the terminal in a place exposed to direct sunlight. → Otherwise, it may cause malfunction, deformation and discoloration.</p> | | <p>Do not install the terminal in humid or dusty places. → Otherwise, it may cause malfunction.</p> | |
| <p>Do not clean this terminal by sprinkling water, nor wipe it with benzene, thinner, and alcohol. → Otherwise, it may cause electric shock or a fire.</p> | | <p>Keep the terminal away from magnets. → Otherwise, it may cause failure and malfunction.</p> | |
| <p>Keep the fingerprint input section clean. → Otherwise, the fingerprint cannot be recognized correctly.</p> | | <p>Do not spray insecticides or inflammables on the terminal. → Otherwise, it may cause deformation and discoloration.</p> | |
| <p>Keep the terminal away from shock or sharp objects. → Otherwise, it may damage the terminal and result in malfunction.</p> | | <p>Do not install the terminal in a place where there is a severe change in temperature. → Otherwise, it may cause malfunction.</p> | |

- Non-compliance of safety notes may cause personal injury or property damage for users.

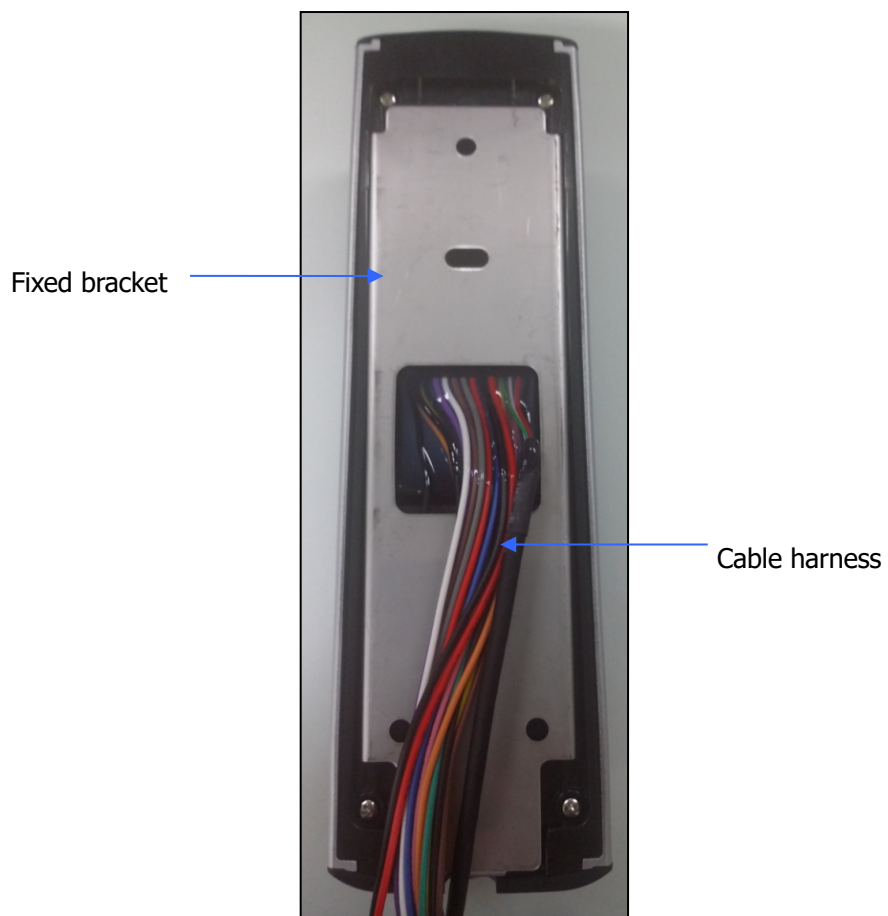
* We are not responsible for any accidents and damage that may arise from non-compliance of the information in this manual.

1.2. Product Details

1.2.1. FRONT

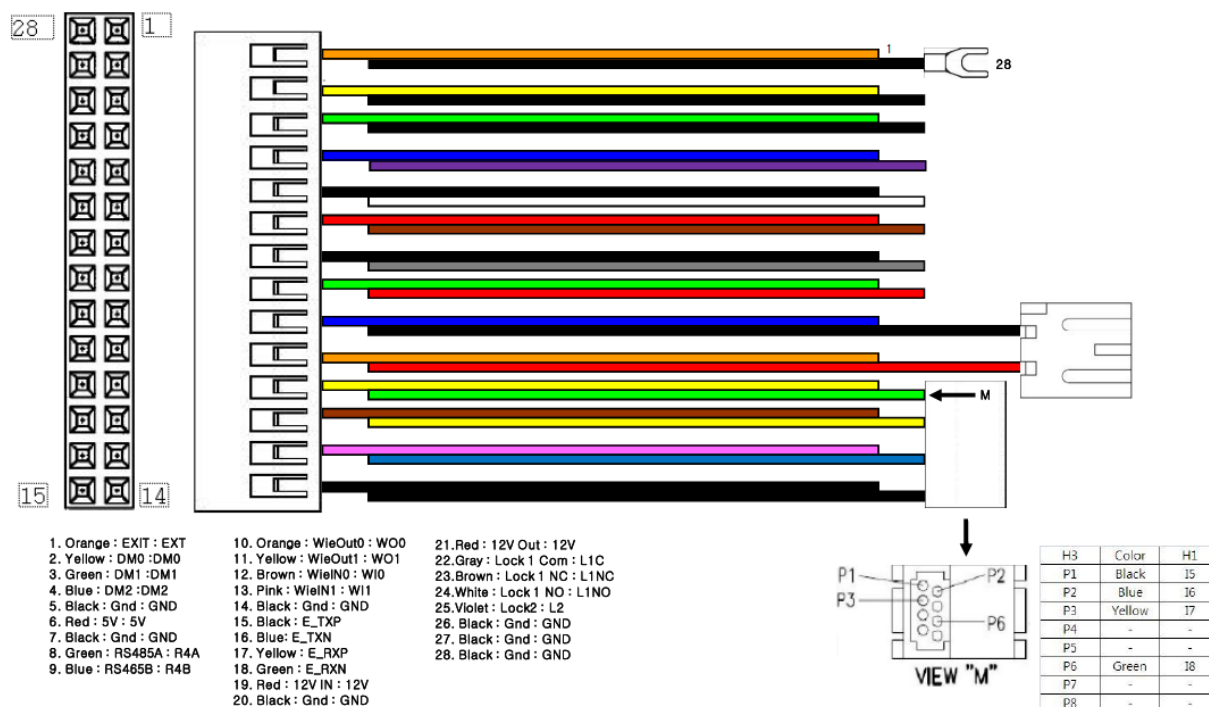


1.2.2. REAR



1.2.3. Input / Output

1.2.3.1. Cable & Connector



1.2.3.2. Pin Details

| Pin number | Line color | Label (Line name) | Explanation | IN/OUT | Note |
|------------|------------|-------------------|--------------|--------|--|
| 1 | ORANGE | EXT | Inside open | IN | Connect to Exit button |
| 2 | YELLOW | DM0 | DoorMonitor0 | IN | Sense door state(DM0) |
| 3 | GREEN | DM1 | DoorMonitor1 | IN | Sense door state(DM1) |
| 4 | BLUE | DM2 | DoorMonitor2 | IN | Sense door state(DM2) |
| 5 | BLACK | GND | GND | - | Ground connection(for door monitor) |
| 6 | RED | 5V | DC5V | OUT | DC 5V output |
| 7 | BLACK | PGND | Power GND | - | Power supply ground connection |
| 8 | GREEN | R4A | RS485A | BI | RS-485 interface |
| 9 | BLUE | R4B | RS485B | BI | RS-485 interface |
| 10 | ORANGE | WO0 | WIE_OUT0 | OUT | Output WIGAND (WO0) |
| 11 | YELLOW | WO1 | WIE_OUT1 | OUT | Output WIGAND (WO1) |
| 12 | BROWN | WI0 | WIE_IN0 | IN | Input WIGAND (WI0) |
| 13 | PURPLE | WI1 | WIE_IN1 | IN | Input WIGAND (WI1) |
| 14 | BLACK | GND | GND | - | Ground connection (WIGAND signal) |
| 15 | RED | - | N_TXN | OUT | LAN I/F (LAN cable) |
| 16 | BLACK | - | N_TXP | OUT | LAN I/F (LAN cable) |
| 17 | GREEN | - | N_RXN | IN | LAN I/F (LAN cable) |
| 18 | WHITE | - | N_RXP | IN | LAN I/F (LAN cable) |
| 19 | RED | 12V | DC12V | IN | DC 12V power supply input |
| 20 | BLACK | GND | Power GND | - | Power supply ground connection (Adapter) |
| 21 | RED | 12V | DC12V | OUT | DC 12V put out power |
| 22 | GRAY | L1C | LOCK1_COM | OUT | Lock1 COM terminal |

| | | | | | |
|----|--------|------|-----------|-----|---|
| 23 | BROWN | L1NC | LOCK1_NC | OUT | Lock1 NC terminal |
| 24 | WHITE | L1NO | LOCK1_NO | OUT | Lock1 NO terminal |
| 25 | PURPLE | L2 | LOCK2 | OUT | Lock2 terminal |
| 26 | BLACK | GND | GND | - | Ground connection (Lock connector) |
| 27 | BLACK | PGND | Power GND | - | Power supply ground connection (Lock power) |
| 28 | BLACK | PGND | Panel GND | - | Panel ground connection (Earth) |

1.2.3.3. Terminal <- > EM Type Door Lock wiring

| Category | T2 terminal (Line name) | EM Door Lock |
|--------------|-------------------------|------------------|
| Lock | L1NC (Green) | + |
| GND | GND (Black) | - |
| Door Monitor | DM0 (Black) | NC(Normal Close) |

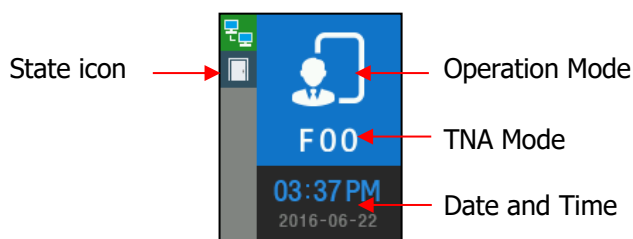
1.2.3.4. Terminal <- > WIEGAND Device wiring

| Category | T2 terminal (Line name) | WIEGAND Device |
|-----------------|-------------------------|-----------------|
| WIEGAND INPUT0 | WI0 | Wiegand output0 |
| WIEGAND INPUT1 | WI1 | Wiegand output1 |
| WIEGAND OUTPUT0 | WO0 | Wiegand input0 |
| WIEGAND OUTPUT1 | WO1 | Wiegand input1 |
| GND | GND | GND |

1.3. Screen information during operation







1.3.1. Initial Screen

When powering on at first, the screen is displayed as follow.








1.3.2. Icons

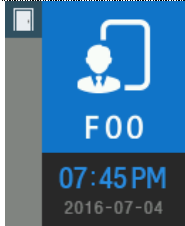
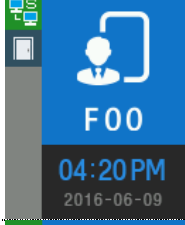
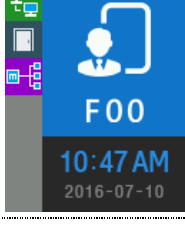
| | | |
|-------------------------|------|--|
| Server connection State | NONE | : No use network |
| | | : LAN line is disconnected. |
| | | : LAN line is connected (only link is connected) |
| Gate State | | : Connected with server |
| | | : Gate is closed. |
| | | : Gate is opened |

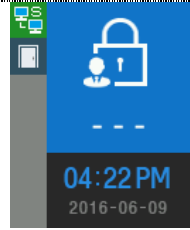

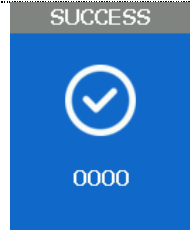
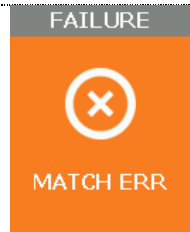
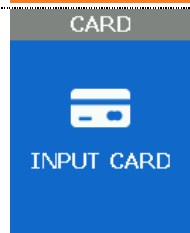
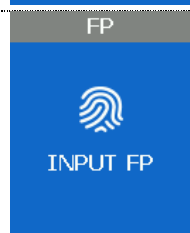
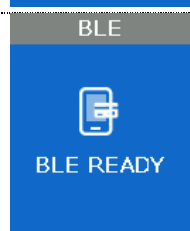
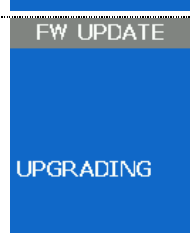
| | | |
|----------------------|---|---|
| |  | : Gate is opened forcedly (unusual door open state) |
| |  | : Gate communication problem |
| Warning signal State | NONE | : Normal |
| |  | : Terminal Disassembly State |
| Fire detection State | NONE | : Normal |
| |  | : Sensed by fire detector (valid on DM2 fire set) |
| BLE connection State | NONE | : Disconnected with Admin App |
| |  | : Connected with Admin App |
| UDL connection State | NONE | : UDL is not used (Normal state) |
| |  | : UDL is connected |

1.3.3. Function KEY

| Icon | Meaning | Function Key | Explanation |
|---|-------------------|---------------|-------------------------------------|
|  | UP | F1 | Move cursor up |
|  | DOWN | F3 | Move cursor down |
|  | LEFT | F2 | Move cursor to left |
| | ESC | F2 long | Move to upper menu |
|  | RIGHT | F4 | Move cursor to right |
| | ENTER | F4 long or F4 | Move to submenu |
|  | ENABLE DISABLE | F2 | Category choice (ENABLE or DISABLE) |

1.3.4. Main Screen

| | |
|---|---|
|  | Operating in Exclusive mode Initial Screen |
|  | Operating in Network mode Initial Screen |
|  | Operating in Dummy mode Initial Screen |

| | |
|---|---|
|  | <p>Operating in lock mode (Reject all users authentication)</p> |
|  | <p>Menu of Initial Screen</p> |
|  | <p>Authentication success</p> |
|  | <p>Authentication failure</p> |
|  | <p>Waiting for Card Input</p> |
|  | <p>Waiting for Fingerprint Input</p> |
|  | <p>Waiting for Admin App registration</p> |
|  | <p>Upgrading firmware</p> |

1.4. LED information during operation

| LED | Operating state | Remark |
|------------------|--------------------------|---|
| RED | Normal | OFF |
| | Alarm | ON or Flash |
| | Authentication Failure | ON (Maintain during authentication time) → OFF |
| GREEN | Normal | OFF |
| | LOCK OPEN | ON |
| | Authentication Success | ON (Maintain during authentication time) → OFF |
| BLUE | Terminal Normal(alive) | Flash at intervals of 5 seconds |
| Function Key LED | Enter menu | Always ON |
| | Touch in initial screen. | ON(Maintain for 10 seconds) → OFF |

1.5. Voice information during operation

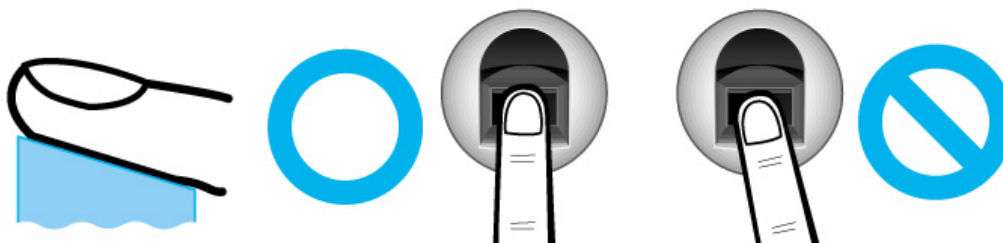
| Category | Voice information |
|------------------------|--------------------------------|
| Fingerprint Input | Please enter your fingerprint. |
| Authentication success | You are authorized. |
| Authentication failure | Please try again. |

1.6. Buzzer guide announced during operation

| Buzzer Sound | State | Explanation |
|--------------|--|--|
| Beep | Key touch Card tag Fingerprint touch | -Pressing key or reading card -When inputting fingerprint, input has been completed and hands can take off. |
| 2 Beeps | Failure | If authentication fails or the user's input is wrong |
| Long Beep | Waiting for input | It shows the state for waiting user's input such as fingerprint or password. |
| Short Beeps | Success | Authentication success or setting completion |

1.7. How to register and enter the correct fingerprint

- Correct fingerprint input method
Enter your fingerprint as if you take a thumbprint by using your forefinger if possible. The fingerprint cannot be correctly registered and entered only by your fingertips. The center of the fingerprint should be touched with the fingerprint input section.



- Enter the fingerprint of your forefinger if possible. When using your forefinger, you can enter your fingerprint correctly and safely.
- Make sure that the fingerprint is unclear or wounded. Too dry, wet, blurry or wounded fingerprints are difficult to recognize. In this case, the fingerprint of another finger should be registered.



- Precautions subject to your fingerprint state. The availability of the fingerprint may vary subject to your fingerprint state.
 - This product consists of a fingerprint recognition system and cannot recognize the damaged or unclear fingerprints. The fingerprint should be registered using the RF card.
 - **If your hands are dry, you can blow your breath on the system** to operate it more smoothly.
 - For children, too small or unclear fingerprints may be difficult or impossible to use. They need to register a new fingerprint every six months.
 - For seniors, the fingerprint with too many lines may not be registered.
 - It is recommended that you register more than two fingerprints if possible.
 - In order to increase the fingerprint authentication rate, it is recommended to use six of the ten fingers as illustrated below (both thumbs, forefingers, middle fingers).

2. Product Description

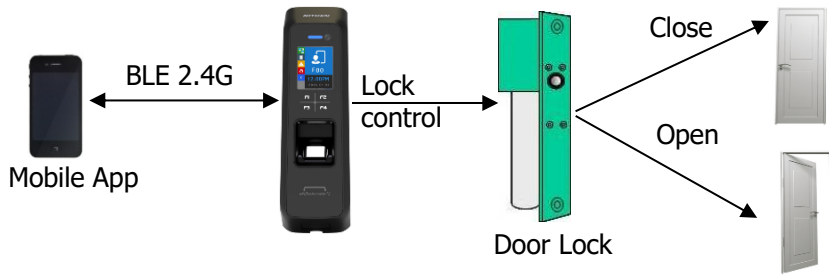
2.1. Product Features

- BLE is equipped. Door Control with smartphone is possible at close range.
- It is equipped with Color Camera, and it saves the visitor’s video when authentication succeeds or fails.
- Optional, Available to use as RF(125kHz), Smart Card(13.56MHz), HID Reader
- Easy to verify your ID via fingerprint
 - The use of the fingerprint recognition technology (Biometrics) can prevent forgetting your password, losing your card or key, or avoid the risk of their theft. The use of personal fingerprints enhances the security of authentication.
- Access control system using the local area network (LAN)
 - The fingerprint reader communicates with the authentication server using a TCP/IP protocol. Therefore, this terminal can be applied to the existing LAN and has easy expandability. It ensures a fast speed by **10/100 Mbps Auto Detect** and facilitates management and monitoring via the network.
- Provide various registration and authentication method

| | |
|----------------------|---|
| Fingerprint | Fingerprint registration Fingerprint authentication |
| Card | Card registration Card authentication |
| Card or Fingerprint | Card, Fingerprint registration Card or Fingerprint authentication |
| Card and Fingerprint | Card, Fingerprint registration Fingerprint authentication after Card authentication |
| Mobile card | Mobile Card registration (registration only via server and admin App) Mobile Card authentication |

2.2. Diagram

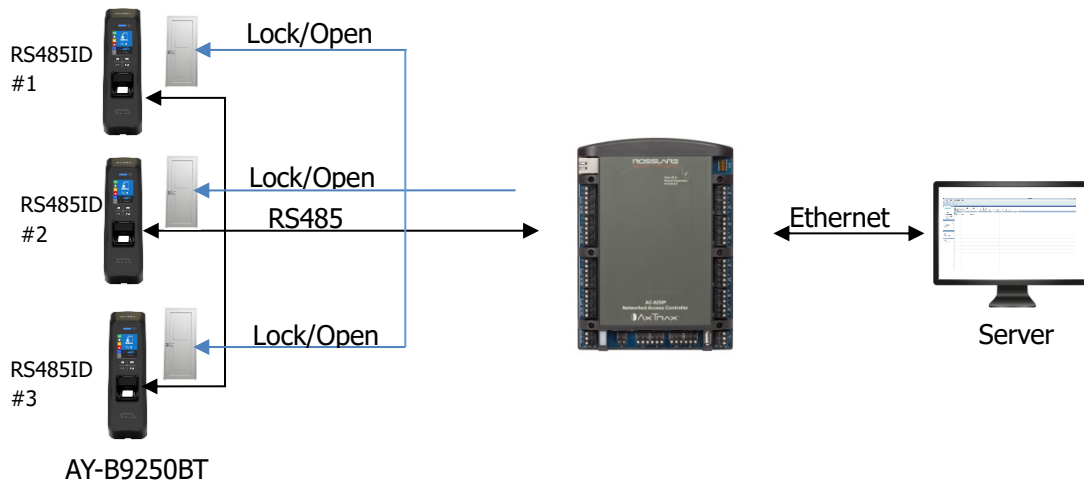
2.2.1. Single Type (Door Lock)



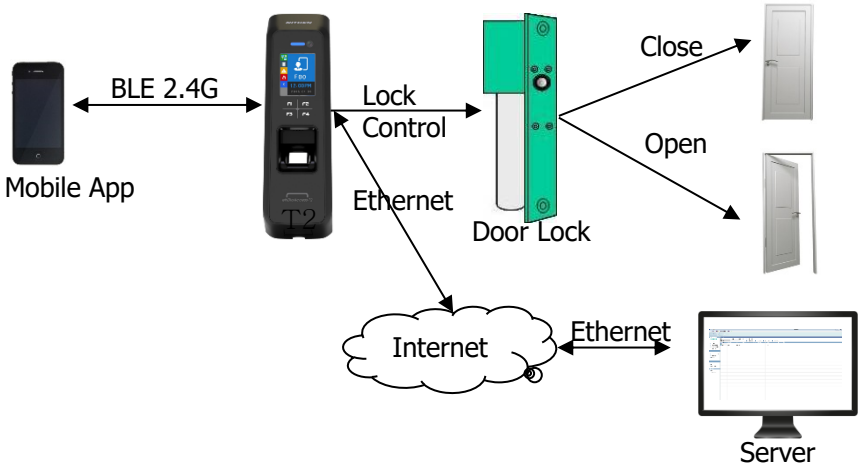
2.2.2. Single Type (Lock Controller)



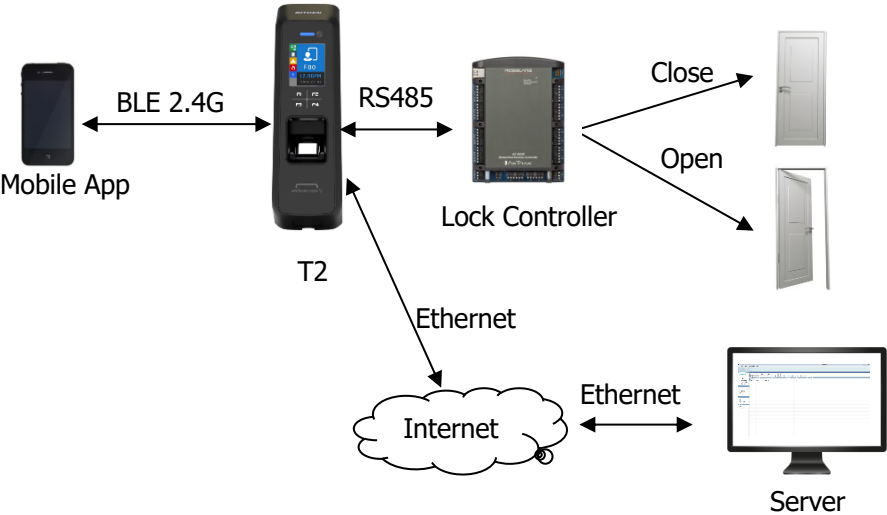
2.2.3. Dummy Type



2.2.4. Network Type (Door Lock)



2.2.5. Network Type (Lock Controller)



2.3. Product Specification

| Category | Spec |
|-------------------------|--|
| CPU | 32Bit RISC CPU(400MHz) |
| MEMORY | 64M DDR RAM, 32M NOR,128M NAND |
| Camera | VGA, F2.8, View angle 61 degree |
| LCD | 1.77" Color LCD |
| Fingerprint Sensor | Optical / 500 DPI |
| Authentication Method | Fingerprint, RF Card, Mobile Card |
| Authentication Speed | 1:N < within 1 sec. (based on 1,000 fingerprints) |
| Fingerprint capacity | 20,000 Fingerprints, 10,000 users (Two identical fingerprints registration per user) Note) Similar fingerprint inspection is possible when the number of fingerprints is less than 200. |
| Log capacity | 100,000 logs |
| Communication interface | TCP/IP, Wiegand In/Out (26/34bit),RS485 |
| Lock | Deadbolt, EM Lock, Door Strike, Automatic Door |
| Temperature / Humidity | -20~60 °C / < RH 90% |
| Certification | KC, CE, FCC |
| Size | 58mm(W) * 191mm(H) * 62mm(D) |

3. Environment Setting

3.1. Checkpoints before Environment Setting

3.1.1. Menu

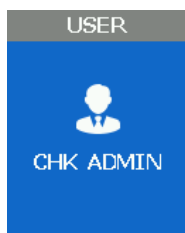
Press F4 long until the menu screen is displayed.



It is available to enter the menu without authentication because the manager doesn't register when shipping the product.

3.1.2. Administration authentication

When the administrator is registered, the admin authentication screen is displayed at first as follows.



► Administrator authentication

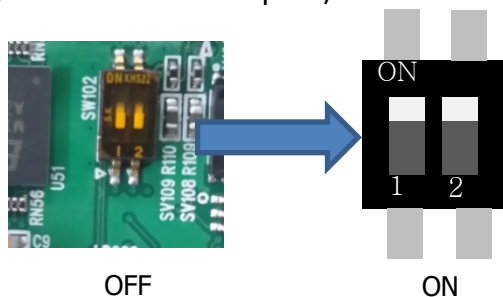
Administrator authentication is progressed with fingerprint and card. You can access each menu if the authentication succeeds.

Admin authentication is displayed only if there is a registered user. Admin authentication displays only if admin is enrolled already. The admin authentication is needed only in accessing menu mode. It enables to access every menu until you completely escape from main menu.

3.1.3. How to access the menu without administrator authentication

This is the method to enter the Menu in exceptional cases such as losing your administrator card that is registered in the terminal or inability to make a fingerprint authentication because of absence of administrator.

- ① Power terminal OFF.
- ② Disassemble device and make case open state.
- ③ While case opens, make DIP of rear side switch ON state as follows.

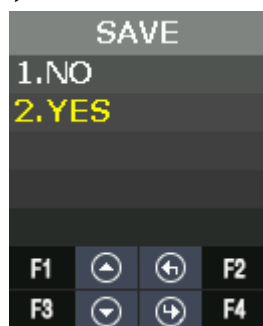


- ④ Power terminal ON.
- ⑤ After the terminal completely booted, Press F1 longer to enter the menu with buzzer sound "Ppiririk".

★ Caution: You should return DIP SWITCH OFF after modification.

3.1.4. Save Settings

▶ If there are some changes, the following screen appears.



- ▶ If you select "YES", then save them with buzzer sound "Ppibibig" and reboot.
- ▶ If there are no changes, it returns to the previous menu screen.
- ▶ While changing the settings in the menu, if there is no input for 30 seconds, it returns to the previous menu.

3.1.5. Default Setting

| Category | Default setting |
|--|--|
| MENU > NETWORK | USE |
| MENU > NETWORK > USE > AUTH MODE | TN |
| MENU > NETWORK > USE > TERMINAL ID | 1 |
| MENU > NETWORK > USE > TERMINAL > | STATIC |
| MENU > NETWORK > USE > TERMINAL > STATIC > | IP:192.168.0.3 SN:255.255.255.0 GW:192.168.0.1 |
| MENU > NETWORK > USE > SERVER | IP:192.168.0.2 PORT: 7332 |
| MENU > OPTION > ATTEND > TYPE | F1~F4 |
| MENU > OPTION > ATTEND > AUTO TNA | NO |
| MENU > OPTION > SCREEN > LANGUAGE | English |
| MENU > OPTION > SCREEN > SHOW ID | YES |
| MENU > OPTION > SCREEN > USER LOGO | NO |
| MENU > OPTION > SCREEN > USER ID LEN | 4 |
| MENU > OPTION > SCREEN > DATE > FORMAT | YYMMDD |
| MENU > OPTION > SAVE > LOG SAVE | Yes |
| MENU > OPTION > SAVE > IMAGE SAVE | No |
| MENU > OPTION > TIME OUT > RESULT | 1sec |
| MENU > OPTION > TIME OUT > NET ERROR | 30sec |
| MENU > OPTION > TIME OUT > PING | 60sec |
| MENU > OPTION > LOCKING | NO USE |
| MENU > INT DEVICE > FP SENSOR > 1:1 LEVEL | 5 |
| MENU > INT DEVICE > FP SENSOR > 1:N LEVEL | 8 |
| MENU > INT DEVICE > FP SENSOR > LFD LEVEL | NONE |
| MENU > INT DEVICE > FP SENSOR > AUTH TIME | 5sec |
| MENU > INT DEVICE > BEEP | 3 |
| MENU > INT DEVICE > VOICE | 3 |
| MENU > INT DEVICE > TAMPER | Alarm |
| MENU > EXT DEVICE > DOORLOCK > LOCK1 > TYPE | STRIKE/OK |
| MENU > EXT DEVICE > DOORLOCK > LOCK1 > OPEN TIME | 3sec |
| MENU > EXT DEVICE > DOORLOCK > LOCK2 > TYPE | None |
| MENU > EXT DEVICE > DOORLOCK > LOCK2 > OPEN TIME | 3sec |
| MENU > EXT DEVICE > DOORLOCK > OPEN ALARM | 5sec |
| MENU > EXT DEVICE > DOORLOCK > DM0 | NONE |
| MENU > EXT DEVICE > DOORLOCK > DM1 | NONE |
| MENU > EXT DEVICE > DOORLOCK > DM2 | NONE |
| MENU > EXT DEVICE > RS485 > TYPE | NONE |
| MENU > EXT DEVICE > RS485 > DEV ID | 0 |
| MENU > EXT DEVICE > WIEGAND > WIRE-INPUT | NONE |
| MENU > EXT DEVICE > WIEGAND > WIRE-OUTPUT | NONE |
| MENU > EXT DEVICE > WIEGAND > WIRE-OUTPUT> 26 BIT or 34 BIT > SITE CODE | 0 |
| MENU > EXT DEVICE > WIEGAND > WIRE-OUTPUT> 26 BIT or 34 BIT > SITE CODE > SEND INFO | UID |

3.1.6. Setting guide for Network Configuration

3.1.6.1. Single Type (Door Lock=STRIKE)

| Menu position | Possible setting |
|-------------------------------------|------------------|
| MENU>NETWORK> | NO USE |
| MENU>EXT DEVICE>DOORLOCK>LOCK1>TYPE | STRIKE/OK |
| MENU>EXT DEVICE>DOORLOCK>DM0 | N/O or N/C |
| MENU>EXT DEVICE>DOORLOCK>LOCK2>TYPE | NONE |
| MENU>EXT DEVICE>DOORLOCK>DM1 | NONE |
| MENU>EXT DEVICE>DOORLOCK>DM2 | NONE |
| MENU>EXT DEVICE>RS485>TYPE | NONE |

3.1.6.2. Single Type (Door Lock=MOTOR)

| Menu position | Possible setting |
|-------------------------------------|------------------|
| MENU>NETWORK> | NO USE |
| MENU>EXT DEVICE>DOORLOCK>LOCK1>TYPE | MOTOR1 |
| MENU>EXT DEVICE>DOORLOCK>DM0 | N/O or N/C |
| MENU>EXT DEVICE>DOORLOCK>LOCK2>TYPE | MOTOR2 |
| MENU>EXT DEVICE>DOORLOCK>DM1 | N/O or N/C |
| MENU>EXT DEVICE>DOORLOCK>DM2 | NONE |
| MENU>EXT DEVICE>RS485>TYPE | NONE |

3.1.6.3. Network Type (Door Lock=STRIKE)

| Menu Position | Possible setting |
|-------------------------------------|--|
| MENU>NETWORK> | USE |
| MENU>NETWORK>USE>AUTH MODE | TN |
| MENU>NETWORK>USE>TERMINAL ID | 0001 |
| MENU>NETWORK>USE>TERMINAL>STATIC | IP:192.168.0.3 SN:255.255.255.0 GW:192.168.0.1 |
| MENU>NETWORK>USE>SERVER | IP:192.168.0.2 PORT:7332 |
| MENU>EXT DEVICE>DOORLOCK>LOCK1>TYPE | STRIKE/OK |
| MENU>EXT DEVICE>DOORLOCK>DM0 | N/O or N/C |
| MENU>EXT DEVICE>DOORLOCK>LOCK2>TYPE | NONE |
| MENU>EXT DEVICE>DOORLOCK>DM1 | NONE |
| MENU>EXT DEVICE>DOORLOCK>DM2 | NONE |
| MENU>EXT DEVICE>RS485>TYPE | NONE |

3.1.6.4. Network Type (Door Lock=MOTOR)

| Menu Position | Possible setting |
|----------------------------------|--|
| MENU>NETWORK> | USE |
| MENU>NETWORK>USE>AUTH MODE | TN |
| MENU>NETWORK>USE>TERMINAL ID | 0001 |
| MENU>NETWORK>USE>TERMINAL>STATIC | IP:192.168.0.3 SN:255.255.255.0 GW:192.168.0.1 |

| | |
|-------------------------------------|-----------------------------|
| MENU>NETWORK>USE>SERVER | IP:192.168.0.2 PORT:7332 |
| MENU>EXT DEVICE>DOORLOCK>LOCK1>TYPE | MOTOR1 |
| MENU>EXT DEVICE>DOORLOCK>DM0 | N/O or N/C |
| MENU>EXT DEVICE>DOORLOCK>LOCK2>TYPE | MOTOR2 |
| MENU>EXT DEVICE>DOORLOCK>DM1 | N/O or N/C |
| MENU>EXT DEVICE>DOORLOCK>DM2 | NONE |
| MENU>EXT DEVICE>RS485>TYPE | NONE |

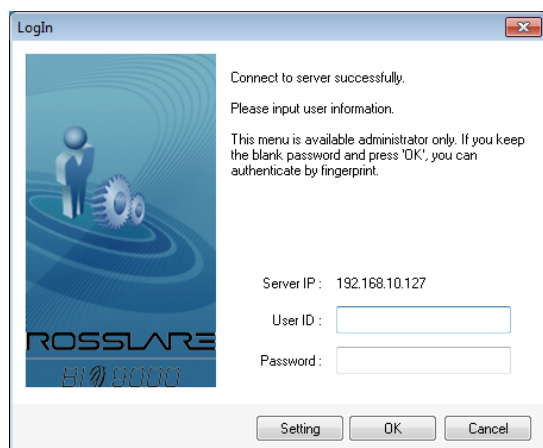
3.2. Access and Registration between Rosslare Bio9000 and terminal

3.2.1. Install Rosslare Bio9000

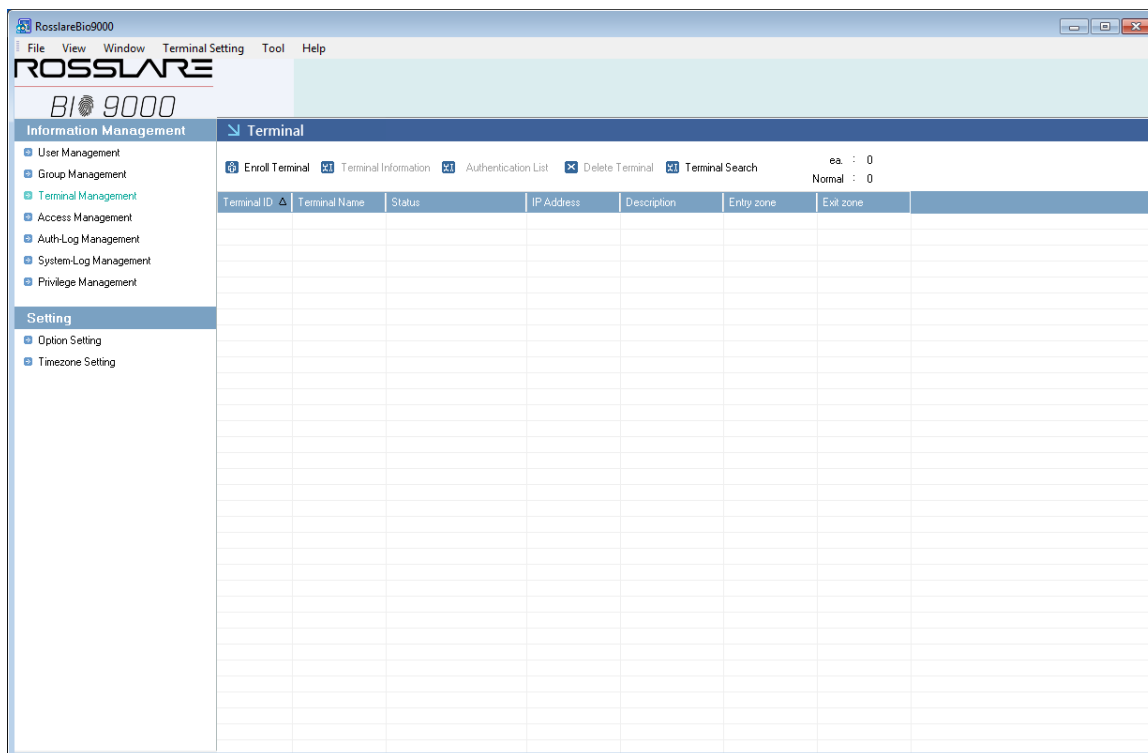
When shipping the product, it comes with a CD to install Rosslare Bio9000 on your PC. For installation guide, please refer to the relevant document.

3.2.2. Execute Rosslare Bio9000

If executing the program, login screen is displayed. Enter User ID that is previously registered and password and then press **OK**.



If login is successful, the screen is displayed as follows.



3.2.3. Set in terminal

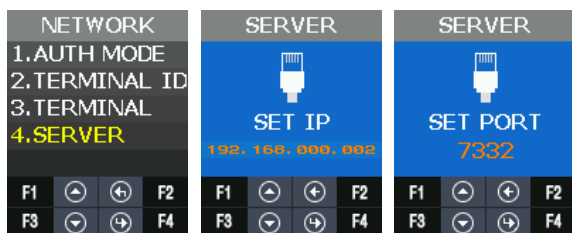
In order to connect the terminal to the server, set to the network mode and set the information.

Move to **MENU > NETWORK > USE > TERMINAL** and check whether lower information is correct or not. If you have not changed the device network information, it is displayed as follows.



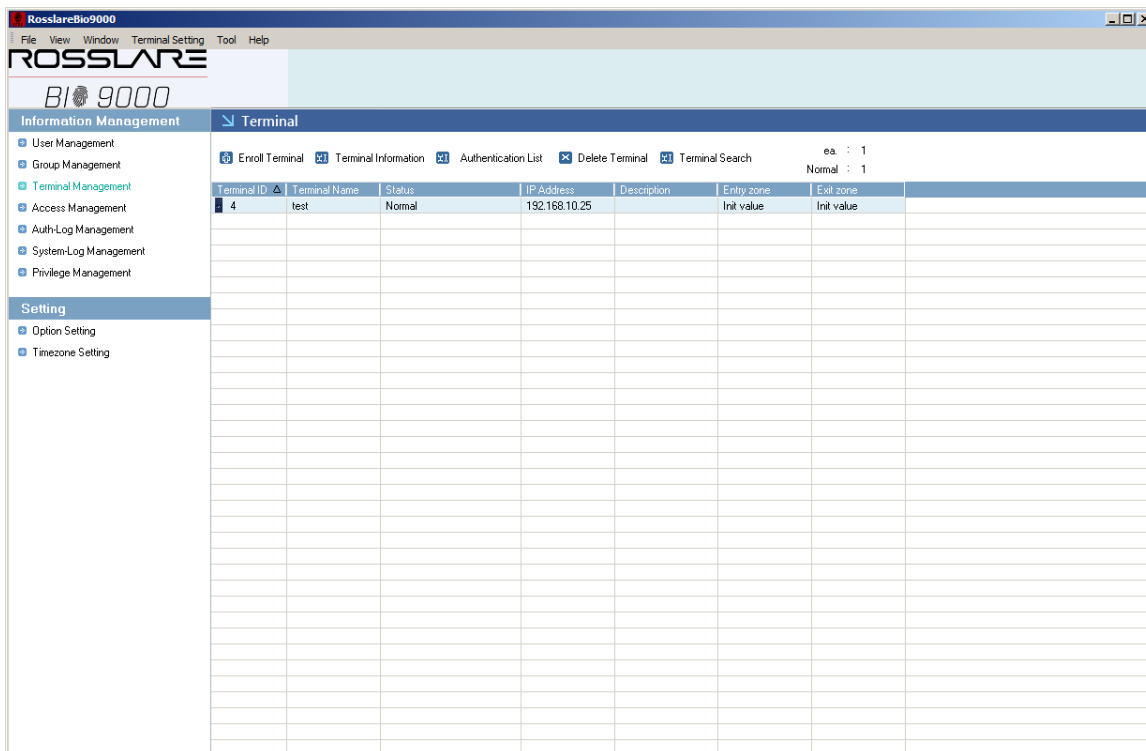
In order to access the server

Move to **MENU > NETWORK > USE > SERVER** and check the lower information correctly sets or not. If you do not change the server network information, it is displayed as follows.



3.2.4. LAN connection in terminal

At first, you can see the unregistered state because the terminal is not registered.



For more details about Rosslare Bio9000 operation, please refer to the guide document.

3.3. Menu Configuration

The whole menu is composed of seven, and main characteristics are as follows.



| Menu | Submenu1 | Submenu2 | Submenu3 |
|------|----------|---|---------------|
| USER | ADD | USER | USER ADMIN |
| | | INPUT ID | |
| | | *Authentication Type Card FP MCARD *Authentication Condition OR AND ※ MCARD is OR condition only. ※ MCARD is not admitted to set up, state check only. | |
| | | Password | |

| | | | | |
|------------|----------|---|--|-------------|
| | AUTO ADD | FP | UID > FP1 > FP2 > OK | |
| | | Card | UID > Card > OK | |
| | MODIFY | INPUT ID | | |
| | | *Authentication Type Card FP MCARD *Authentication Condition OR AND ※ MCARD is OR condition only. ※ MCARD is not admitted to set up, state check only. | | |
| | | FP registration (When checking authentication mode) | | |
| | | Card registration (When checking authentication mode) | | |
| | DELETE | Delete ID | | |
| DELETE ALL | | | | |
| NETWORK | NO USE | Operate in single mode | | |
| | USE | AUTH MODE | Server/Terminal Terminal/Server Server Terminal | |
| | | TERMINAL ID | TERMINAL ID | |
| | | STATIC DHCP | STATIC | IP |
| | | | | Subnet mask |
| | | | | Gateway |
| | | | DHCP | |
| SERVER | SERVER | Port No | | |
| OPTION | ATTEND | TYPE | NONE M1 F1~F2 M2 F1~F4 M3 F1~F49 | |
| | | AUTO TNA | NO YES | |
| | SCREEN | LANGUAGE ENGLISH(0) KOREAN(1) INDONESIAN(2) MULTILINGUAL(3) ARABIC(4) SPANISH(5) PORTUGUESE(6) FRENCH(7) RUSSIAN(8) FARSI(9) JAPANESE(10) CHINESE(11) | | |

| | | | |
|---------------|-----------|-------------------|--|
| | | SHOW ID | NO YES |
| | | USER LOGO | NO USE USE |
| | | USER ID LEN | 4~16 |
| | SAVE | LOG SAVE | NO YES |
| | | IMAGE SAVE | NO YES |
| | TIMEOUT | RESULT | |
| | | NET ERROR | |
| | | PING | |
| | Date | FORM | YYMMDD DDMMYY MMDDYY |
| | | SETTING | YYYYMMDD-hhmmss |
| INT DEVICE | FP SENSOR | 1:1 LEVEL (1~9) | |
| | | 1:N LEVEL (5~9) | |
| | | LFD LEVEL | NONE LOW MIDDLE HIGH |
| | | AUTH TIME | |
| | BEEP | 0~3 | |
| | VOICE | 0~5 | |
| | BLE | BLE READY | |
| | TAMPER | NO ALARM ALARM | |
| EXT DEVICE | DOOR LOCK | LOCK1 | *TYPE Not Use Strike/OK Indication Motor1 Schedule alarm *OPEN TIME 3[1~20sec] |
| | | LOCK2 | * TYPE NONE Fail Indication Motor2 Schedule alarm * OPEN TIME 3[1~20sec] |
| | | OPEN ALARM TIME | 5[0~20sec] 0: No Alarm 1~20: Alarm |
| | | DM0 | NONE Lock Normal Open Lock Normal Close |
| | | | |

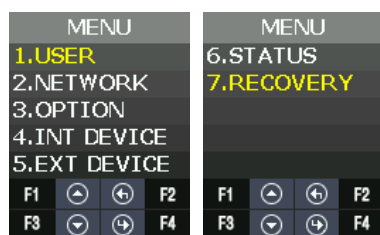
| | | | |
|-------|---------|---|---|
| | | DM1 | NONE Lock Normal Open Lock Normal Close |
| | | DM2 | Not use Normal Open Normal Close Fire Normal Open Fire Normal Close Panic Normal Open Panic Normal Close Urgent Norm Open Urgent Normal Close |
| | RS485 | TYPE | NONE |
| | | DEV ID: 0~255 | |
| | WIEGAND | WIRE-INPUT | *TYPE NONE WIE26BIT WIE34BIT CUSTOM |
| | | WIRE-OUTPUT | *TYPE NONE WIE26BIT WIE34BIT CUSTOM *SiteCode *More Information UID CARD |
| STATE | DB INFO | USER CNT: USER MAX: ADMIN: FP CNT: FP MAX: CARD CNT: CARD MAX: M.CD CNT: LOG CNT: LOG MAX: | |
| | NETWORK | TID: xxxx NET: YES, MODE:TN NET TYPE: STATIC ENCRYPT: DES CIP/SN/GW----- xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx MAC: xx: xx: xx: xx: xx: xx SIP/PORT----- | |

| | | | |
|--|------------|--|--|
| | | xxx.xxx.xxx.xxx xxxx | |
| | OPTION | ATTEND: M2(F1~F4) AUTO TNA: YES LANGUAGE: English SHOW ID: YES LOGO USE: NO UID LEN:4 DATE: YYMMDD LOG SAVE: YES IMG SAVE:NO SHOW TO: x PING TO: x NET TO: x: | |
| | INT DEVICE | CARD TYPE: RF/SC CARD FMT: STD FP1:1:x FP1: N:x LFD: xx AUTH TIME: BEEP VOL: VOICE VOL: BLE Name/MAC---- XXXXXXX (BLE Name) XXXXXXXXXXXXXXXXXXXX TAMPER:ALARM | |
| | EXT DEVICE | LOCK1----- TYPE: STRIKE/OK OUT: N/O OPEN: 3000ms LOCK2 ----- TYPE: NONE OUT: N/O OPEN: 3000ms DOOR WARN: 0sec FORCE OPEN:NO RS485 ID: xxx WIEGAND----- IN/OUT :34B/34B SITECODE: xxx SEND:USERID | |
| | I/O PORT | LOCK1: HIGH LOCK2: HIGH DM0: HIGH DM1: HIGH DM2: HIGH W0IN: HIGH W1IN: HIGH INSIDE: HIGH TAMPER SW:HIGH | |

| | | | |
|----------|------------|--|---|
| | VERSION | HW FW Card BLE SN(Serial Number) | |
| RECOVERY | INITIALIZE | CONFIG | |
| | | LOG DB | |
| | | FACTORY | |
| | SELF TEST | INT DEVICE | VOICE CARD FP SENSOR CAMERA LED |
| | | EXT DEVICE | DOORLOCK SENSOR IN |
| | BACKUP | LOG EXPORT | |
| | | USER EXPORT | |
| | | USER IMPORT | |
| | | FW UPDATE | |
| | REBOOT | | |

3.4. USER Menu

USER menu has the feature as follows.

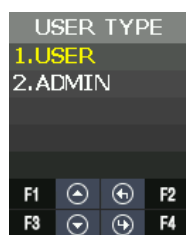



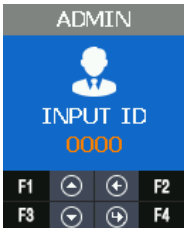
| Category | Explanation |
|-------------------|--|
| ADD | Use to add user and admin with various certification conditions. |
| AUTO ADD | Use to add Card or Fingerprint user automatically. |
| MODIFY | Use to add certification conditions, card or fingerprint of registered user. |
| DELETE | Use to delete a registered particular user. |
| DELETE ALL | Use to delete all registered users. |

3.4.1. ADD

3.4.1.1. USER TYPE

If you press **ADD** in the menu, the screen asking the user type is displayed as follow.



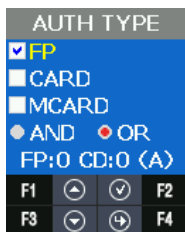
| USER TYPE | Explanation |
|-----------|--|
| USER | Only available for authentication No Authorization to access menu When selecting user, the screen is displayed as follow.  |
| ADMIN | Available to add and delete user. Available to access menu and modify it. When selecting the administrator, the screen is displayed as follows.  |

3.4.1.2. AUTH TYPE

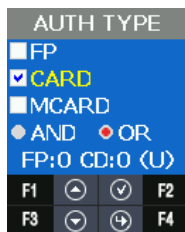
There are FP (Fingerprint), Card, and MCARD (Mobile card) in the menu. But MCARD can only provide the check state, and do not provide checking or unchecking. For checking or unchecking with MCARD, it is only available via **Server** and **Admin App**. There are **AND** and **OR** in authentication conditions. In **AND**, all authentication conditions should be satisfactory and then authentication succeeds. In **OR**, one of authentication conditions should be satisfactory and authentication succeeds.

FP:0 → FP is abbreviation of Finger Print.
 0 means the registered FP number. (1FP means 2 fingerprints)
 CD:0 → CD is abbreviation of CARD.
 0 means the registered CARD number.
 Maximum card number is 1.

(U) → Means your Registration Authority is general user (USER).
 (A) → Means your Registration Authority is administrator (ADMIN).



[FR Authentication]



[Card Authentication]



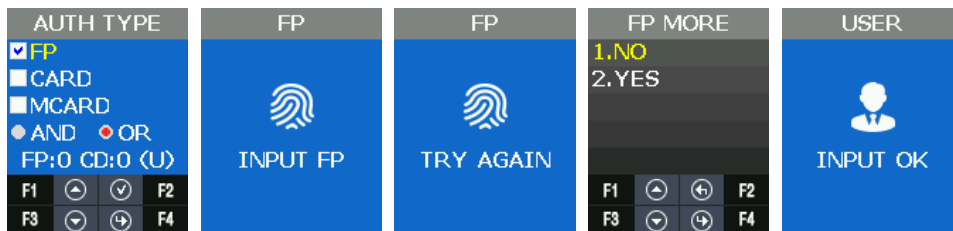
[FP or Card Authentication]



[FP and Card Authentication]

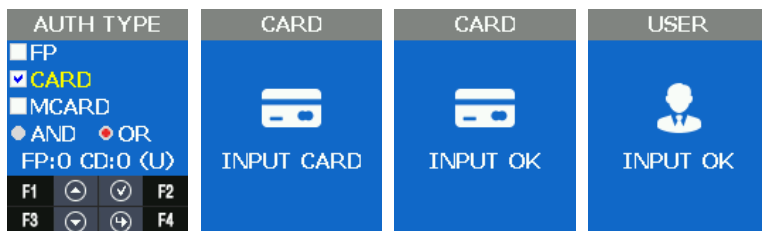
3.4.1.3. INPUT FP

Input the same fingerprint twice when you check the Fingerprint as authentication type. If you want to add only one fingerprint, select **1. NO**. If you input the fingerprint second times and they are normal, **INPUT OK** is displayed. If you want to add more fingerprints, select **2. YES**. One user can register 20 people for maximum.



3.4.1.4. INPUT CARD

When you check **Card** as **AUTH TYPE**, you need to follow steps as below. If you input CARD on Waiting state, registration completes and **INPUT OK** screen is displayed.



EM CARD ex) Card No.(5byte): 08h 01h 16h 1Dh D6h

| Card Format | Card No. | Display Method |
|-------------|------------------------|--|
| Standard | 02207638 (16001DD6) | (3+5)digits Decimal [022(16h)+07638(1DD6h)] |

SC CARD ex) Card No.(4byte): 52h 9Dh 06h E3h

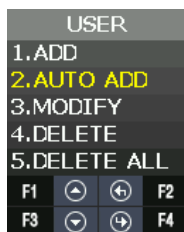
| Card Format | Card No. | Display Method |
|-------------|----------|----------------|
| Standard | 529D06E3 | 8digits Hex |

3.4.2. AUTO ADD

AUTO ADD is used when you want to register general users (not admin user) consecutively with card or fingerprint.

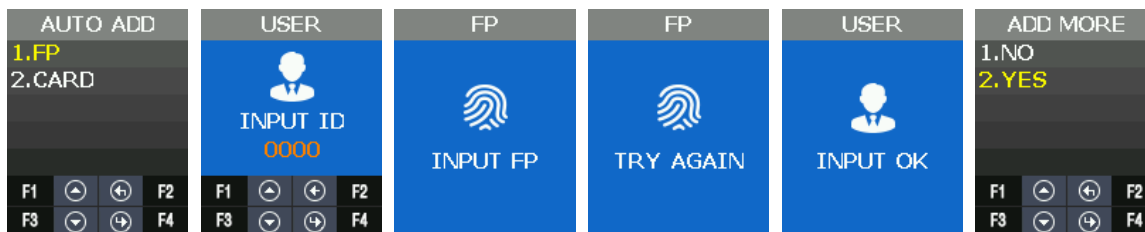
If you select **FP**, it adds users by increasing ID consecutively only with fingerprint.

If you select **CARD**, it adds users by increasing ID consecutively only with card.



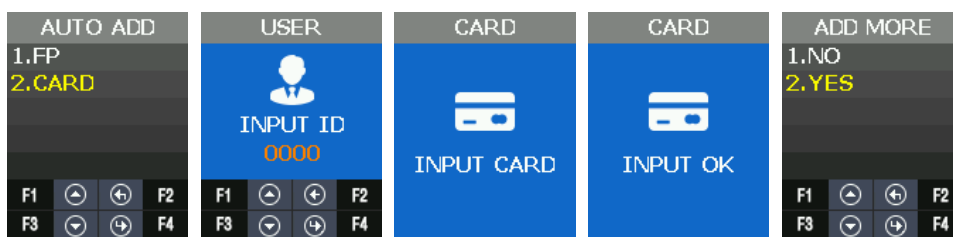
3.4.2.1. AUTO ADD – 1. FP

This is the menu when registering the users continuously only by fingerprint. Input fingerprint in twice and then the registration succeeded. If you want to add more users, select **2. YES**, and continue the registration. User ID increases automatically.



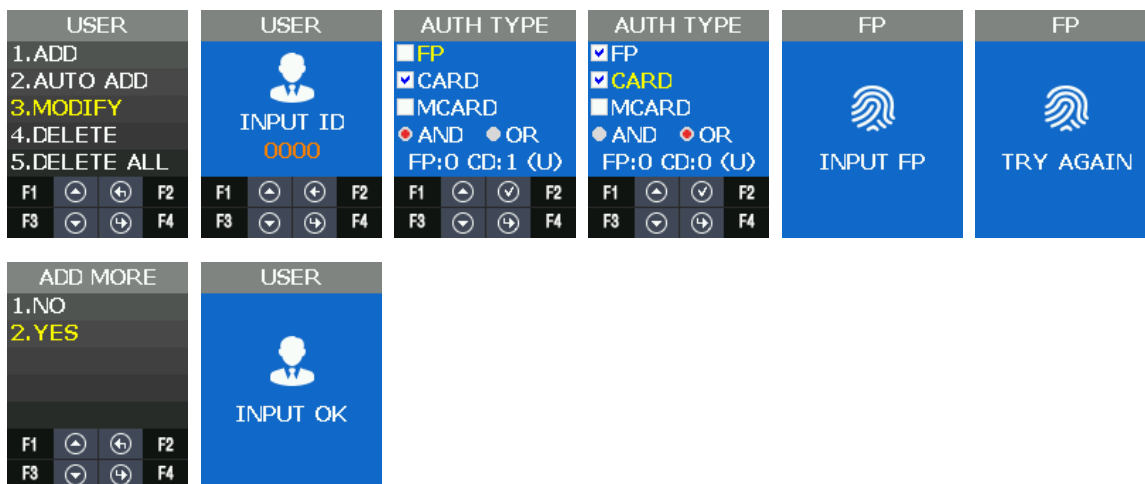
3.4.2.2. AUTO ADD

This is the menu when registering the users continuously only by card. After inputting the card, **INPUT OK** is displayed on the screen. If you want to add the other user, select **2. YES**, and register the user. User IDs increases automatically.



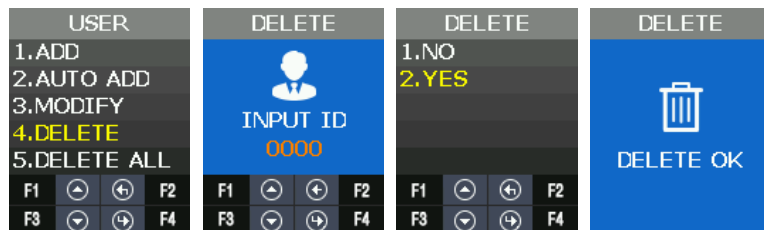
3.4.3. MODIFY

It is used when modifying the authentication type of the registered user. In authentication type, authentication type (fingerprint, card) and authentication condition (AND, OR) can be changed. If the modification type is modified, authentication information about the authentication type can be input.



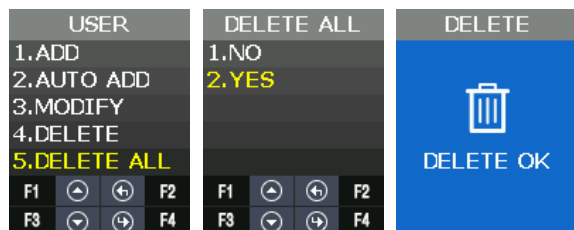
3.4.4. DELETE

It is used when deleting the registered users.



3.4.5. DELETE ALL

It is used when deleting all the registered users. It should be careful when trying to delete, because all the users (general user, administrator) are deleted.



3.5. NETWORK Menu

Network menu has the following features.



| Category | Explanation | Remarks |
|----------|--|--------------|
| NO USE | Network not used | Standalone |
| USE | AUTH MODE TERMINAL ID TERMINAL SERVER | Network mode |

| Operation Mode | Explanation |
|----------------|--|
| Standalone | This is the operation mode independently without server and communication. The administrator can control all the functions of the terminal. Authentication log is saved in the terminal but is not sent to server. After converting Standalone mode into Network mode and accessing in server, the authentication log saved internally is sent to sever. If you want to see the authentication log data in Standalone mode, |

| | |
|--------------|--|
| | move RECOVERY > BACKUP > LOG EXPORT from main menu, download it in USB through UDL module and check it by Rosslare Bio9000 program. |
| Network Mode | This is the operation mode by communicating with the server and it can control the functions of the terminal by the remote-control. Depending on the authentication mode, the order of authentication can be different. (Authentication order about whether trying to authenticate in the terminal or the server first) Authentication log is sent to the server if the network is connected regardless of authentication mode. |

3.5.1. AUTH Mode

Authentication mode means the authentication priority to determine whether authentication processing is done in the terminal or the server when user-authentication. It is a valid setting only when using the network. All authentication log is sent to server through the network.



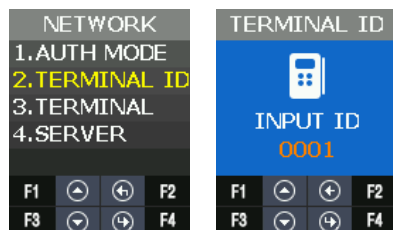
| AUTH MODE | Explanation |
|-----------------|--|
| Server/Terminal | Server → Terminal After trying to do server authentication at first, terminal authentication is processed. |
| Terminal/Server | Terminal → Server After trying to do terminal authentication at first, server authentication is processed. |
| Server | Server only Authentication is processed only in server. |
| Terminal | Terminal only Authentication is processed only in terminal. Even if it is "Terminal Only", authentication log is sent to server. |

★ In Server Only" mode, if the network is disconnected, all the authentication is processed in fail. If the mode is not "Server Only" (Server/Terminal, Terminal/Server, Terminal) and the network is disconnected, authentication is processed in the base of DB in the terminal.

3.5.2. Terminal ID

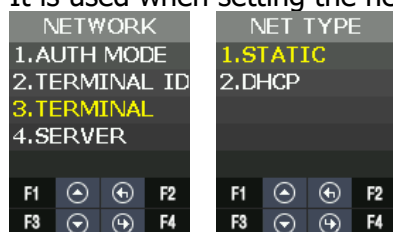
Terminal ID is a valid information only when using the network, and it can be set in the range of 1~200.

If a user registered in the terminal exists, you can't change the Terminal ID.



3.5.3. Terminal

It is used when setting the network information in the terminal.



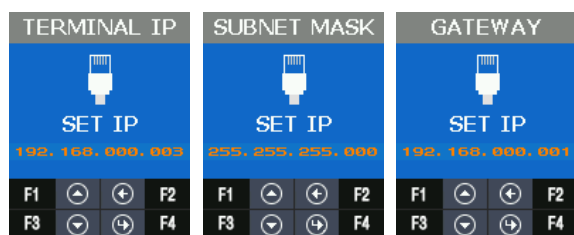
Network setting in the terminal can be set in Static IP and DHCP.

STATIC: Set the value as a user wants.

DHCP: Allocated flexibly. (It can be operated normally when using the router supporting DHCP.)

If **STATIC** is used, it is used when setting IP, Subnet mark and Gateway address of the terminal.

The following is the default setting value.



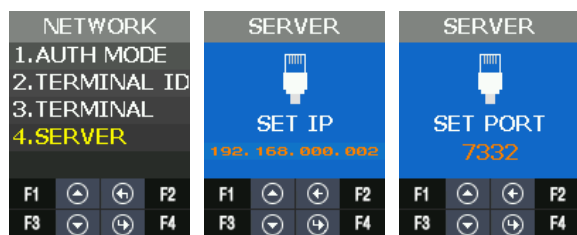
| Category | Default Setting Value |
|-------------|-----------------------|
| Terminal IP | 192.168.0.3 |
| SUBNET MASK | 255.255.255.0 |
| GATEWAY | 192.168.0.1 |

It can set the address value as follows.

| Function Key | Function Explanation |
|--------------|----------------------------|
| F1 | Increase the setting value |
| F3 | Decrease the setting value |
| F2 | Move to left |
| F4 | Move to right |
| F4 Long | Save the setting value |

3.5.4. Server

When the terminal accesses in server through the network, set the information.

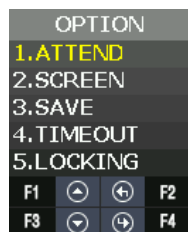


Default setting value is as follows.

| Category | Default Setting Value |
|-------------|-----------------------|
| Server IP | 192.168.0.2 |
| Port number | 7332 |

3.6. OPTION Menu

User menu has the same function as follows.

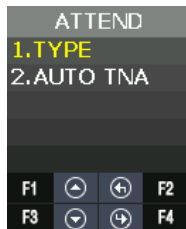


| Category | Explanation |
|----------|---|
| ATTEND | TYPE AUTO TNA |
| SCREEN | LANGUAGE SHOW ID USER LOGO USER ID LEN DATE |
| SAVE | LOGO SAVE IMAGE SAVE |
| TIMEOUT | RESULT NET ERROR PING |

| | |
|---------|--------------|
| LOCKING | NO USE / USE |
|---------|--------------|

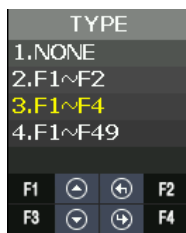
3.6.1. ATTEND

TNA related menu is configured.



| Category | Explanation |
|----------|---|
| TYPE | When Function Key is used in time and attendance option, it is used. |
| AUTO TNA | Use to determine whether to remain Function Key or not shown in the default screen. |

3.6.1.1. TYPE



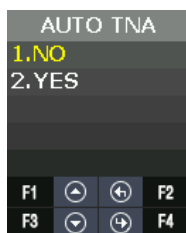
It is used when setting ATTEND mode. If setting ATTEND mode, ATTEND mode is displayed in the screen when pressing Function Key shortly (F1~F4) in the default screen.

| Mode | Explanation |
|--------|---|
| NONE | F00 is only displayed in default screen. |
| F1~F2 | F1~F2 Function Key is recognized and F01, F02 are displayed in default screen. |
| F1~F4 | F1~F4 Function Key is recognized and, F01, F02, F03, F04 are displayed in default screen. |
| F1~F49 | F1~F4 Function Key is recognized and F01, F02, F03, F04, F11~F49 are displayed. |

| Function Key | Meaning |
|--------------|----------------|
| F00 | ACCESS MODE |
| F01 | CLOCK-IN MODE |
| F02 | CLOCK-OUT MODE |
| F03 | CHECK-OUT MODE |
| F04 | CHECK-IN MODE |
| F11~F49 | EXPANDED MODE |

TNA mode (F00~F49) is converted into F00 after 10 seconds if you don't use AUTO TNA.

3.6.1.2. AUTO TNA

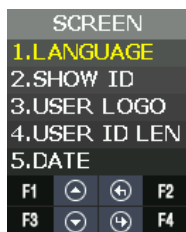


AUTO TNA is the menu to determine whether to remain continually the setting TNA mode or not.

| Category | Explanation |
|----------|---|
| NO | The TNA mode is automatically returned into F00 after 10 seconds. |
| YES | The TNA mode is continuously displayed. |

3.6.2. Screen

The screen display related menu is configured.



| Category | Explanation |
|-------------|--|
| LANGUAGE | Change the language which is displayed in the screen and is spoken. |
| SHOW ID | When authentication succeeds, you can set whether showing ID or not. |
| USER LOGO | You can set whether the logo image for customers is used or not in the default screen. |
| USER ID LEN | It is used when modifying the length of user's ID. |
| DATE | It is used when modifying Year/ Month/ Day and time displayed in the default screen. |

3.6.2.1. Language

It is used to change the voice language and menu text displayed on the screen.

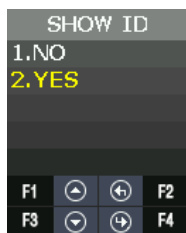
Voice guidance is available in English, Korean, Indonesian, Thai, Arabic, Spanish, Portuguese, French, Russian, Farsi, Japanese, and Chinese.

Language support for all menu text is in English, Korean, Indonesian, Spanish, Portuguese, French, Japanese and Chinese.

Language support for some text is in Farsi, Arabic, Thai and Russian.



3.6.2.2. SHOW ID

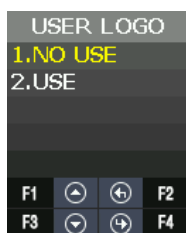




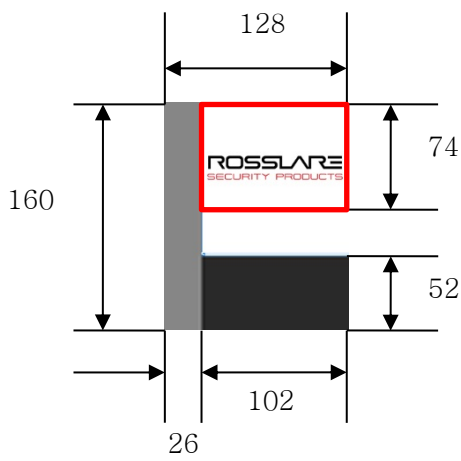
It is used to determine whether to show your ID at the time of authentication success window.

| Category | Explanation |
|----------|--|
| NO USE | Do not show your ID at the time of authentication success Screen Yes "*****" When authentication successes, it doesn't show user's ID on the screen. For example, "*****". |
| USE | When authentication successes, it shows user's ID on the screen. For example, "*****". |

3.6.2.3. USER LOGO

It is used to determine whether the displayed image shows the customer's logo or not in the default screen.



| Category | Explanation |
|---|---|
| <p>NO USE</p>  | <p>Use basically the provided default image</p> |
| <p>USE</p>  | <p>Use the customer's logo image</p> <p>To use the customer's logo image, you should update the customer's image through the server first and then the customer's image is displayed in the default screen.</p> <p>When editing the customer's image, it should be edited in the red box as the left picture. The full image size is 128 (W) x160 (H) pixel, and the red box image size is 102 (W) x74 (H) pixel.</p>  |

3.6.2.4. USER ID LEN

It is used to change the length of user's ID. If changing the user's ID, it should change in the absence of a DB because it affects user's DB that is internally registered. The setting range can be set from 4 to 16.

If a user registered in the terminal exists, you can't change the length of User ID.



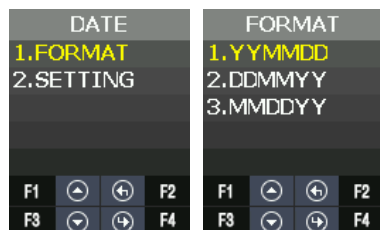
3.6.2.5. DATE

It is used to select the order of Year, Month and Day displayed in the default screen.

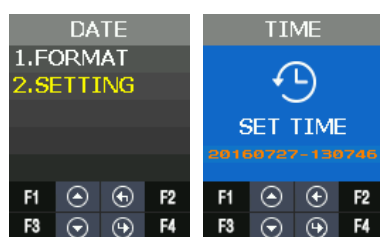
YY: Year

MM: Month

DD: Day

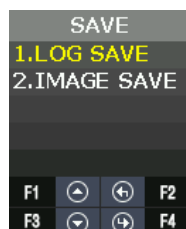


Through SETTING, you can set current Year, Month, Day and Time.



3.6.3. SAVE

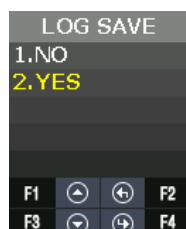
It is the menu including the function related to SAVE.



3.6.3.1. LOG SAVE

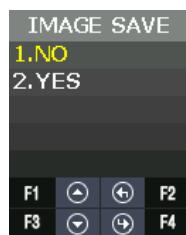
It is used to set whether to save the authentication log in memory or not.

The default setting is YES.



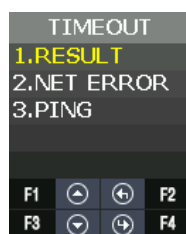
3.6.3.2. IMAGE SAVE

It is used to set whether to save the captured photo from camera when authentication successes or fails. The default setting is Fail.



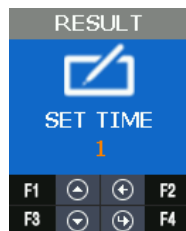
3.6.4. TIMEOUT

It is the menu that has the setting related with timeout.



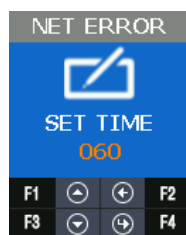
3.6.4.1. RESULT

It is used to set the authentication result display how long it keeps for a seconds. The setting range can be set from 0 to 5 seconds. If it set to 0, then don't display the authentication result.



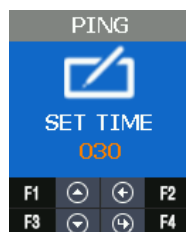
3.6.4.2. NET ERROR

If it does not communicate with the server over a period of time, it is used to set whether there is a network communication error. If PING doesn't come for a setting time in the server, it retries to connect the terminal. The setting range is available for 60~600 seconds.



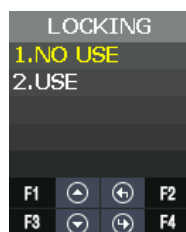
3.6.4.3. PING

It sets the cycle that terminal sets PING command to the server.
The setting range is available for 30~255 seconds.



3.6.5. LOCKING

Locking mode is the function that it rejects the authentication of all users until the administrator enters the menu and releases the locking mode.
The default setting is **NO USE**.



The default screen is displayed as follows when setting to use locking mode.



3.7. INT DEVICE Menu



INT DEVICE menu has the features as follows.

| Category | Explanation |
|-----------|---|
| FP SENSOR | 1:1 LEVEL 1: N LEVEL LFD LEVEL AUTH TIME |
| BEEP | Set Beep Sound. |
| VOICE | Set Voice Sound |
| BLE | BLE registration mode |
| TAMPER | Set the alarm when opening terminal case. |

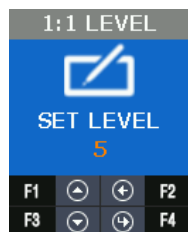
3.7.1. FP SENSOR

For the fingerprint recognition, it sets for the user registration and authentication about the module installed inside.



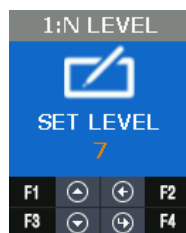
3.7.1.1. 1:1 LEVEL

It is the authentication level used when it tries 1:1 fingerprint authentication.



3.7.1.2. 1: N LEVEL

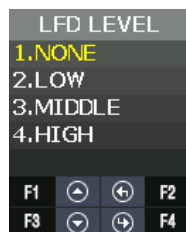
It is the authentication level used when it tries 1: N fingerprint authentication.



3.7.1.3. LFD LEVEL

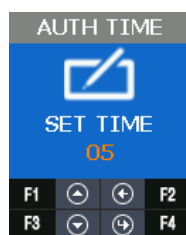
It sets LFD LEVEL to prevent the duress fingerprint.

If setting LFD LEVEL higher and higher, the ability to prevent the input of duress fingerprint produced by rubber, paper, film, and silicon etc. reinforces but too dry fingerprint cannot be input well. Also the authentication speed can be slow.



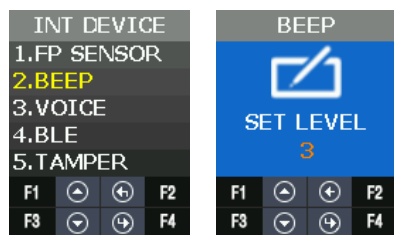
3.7.1.4. AUTH TIME

It means the maximum time to process 1: N authentication. If the authentication time exceeds, authentication timeout occurs. The authentication time is 2 to 10 seconds, the default is 5 seconds.



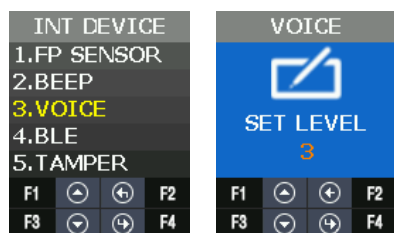
3.7.2. BEEP

It informs key touch, authentication success, and failure as beep and sets the beep level. The beep level is available from 0 to 3.



3.7.3. VOICE

It supports the notice such as authentication success/failure and authentication retrieval. It sets the authentication level. The voice level is available from 0 to 5.

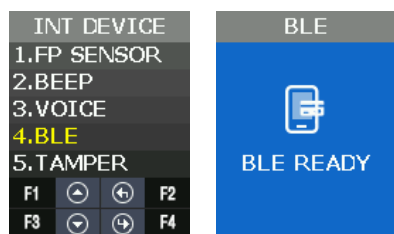


3.7.4. BLE

When registering the terminal in Administrator’s App, this menu is required.

By using this menu, it can make the terminal BLE READY. Only if the terminal is BLE READY, it can perform the registration procedure of the terminal after the administrator app accesses the terminal.

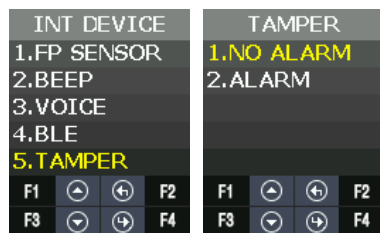
When pressing F3 long in the default screen of the terminal, it performs same operation with this menu.




Regarding the method to register the terminal in the administrator APP, please refer **3.2 How to register the terminal** in the administrator App.

3.7.5. TAMPER

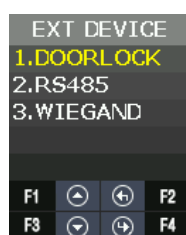
When disassembling the terminal randomly, it sets whether to sound the alarm.



If selecting **1. NO ALARM**, even if disassembling the terminal, the alarm doesn't sound but  icon is displayed.

If selecting **2. ALARM**,  icon displays and the beep sounds in at regular intervals.

3.8. EXT DEVICE Menu

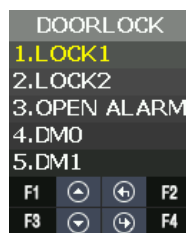


EXT DEVICE has the features as follows.

| Category | Explanation |
|----------|--|
| DOORLOCK | It sets the control device to lock through the internal relay. |
| RS485 | It sets the devices using RS485. |
| WIEGAND | It sets the device using WIEGAND. |

3.8.1. DOORLOCK

It is the menu to set lock device (Strike, Motor type door lock) by using LOCK1 and LOCK2 port.



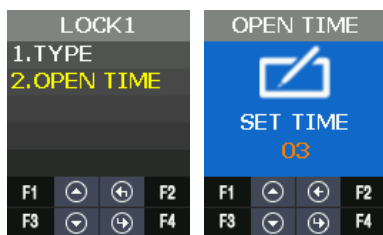
3.8.1.1. LOCK1 type

| Category | Explanation |
|-----------|--|
| NONE | No Use |
| Strike/OK | When connecting the light to mark authentication success/failure or 2. STRIKE/OK. |
| MOTOR1 | When connecting Motor lock |



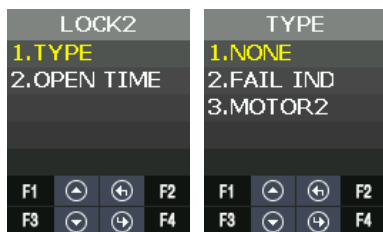
3.8.1.2. LOCK1 OPEN TIME

It sets the time to give the signal when LOCK 1 sets **2. STRIKE/OK**. Strike type means the time from opening to locking the door after authenticating. The default value is 3 seconds and the input range is 1 to 20 seconds.



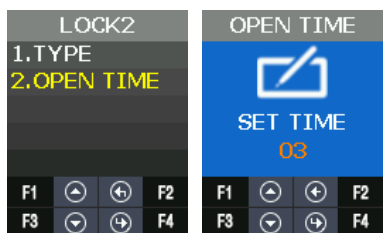
3.8.1.3. LOCK2 type

| | |
|----------|--|
| NONE | When not using |
| FAIL IND | When connecting the light to mark authentication failure in Lock 2 |
| MOTOR2 | When connecting motor lock |



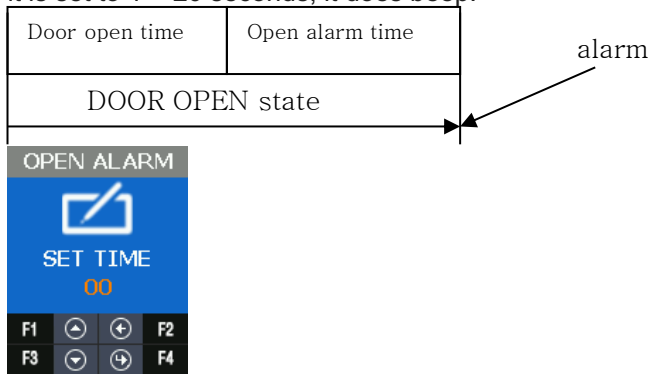
3.8.1.4. LOCK2 OPEN TIME

If Lock 2 sets FAIL IND, it sets the time to give the signal. The default value is 3 seconds and the input range is 1 to 20 seconds.



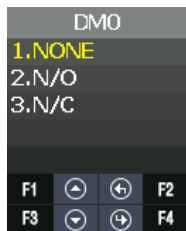
3.8.1.5. OPEN ALARM

When the door open time expires and the door open alarm time is exceeded, the alarm sounds. The default value is 5 seconds and the input range is 0 ~ 20 seconds. If it is set to 0, it does not beep. If it is set to 1 ~ 20 seconds, it does beep.



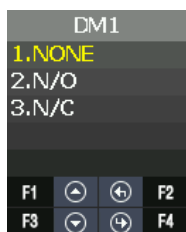
3.8.1.6. DM0

DM0(Door Monitor 0) is the input port and it is used to detect the signal state of door open.



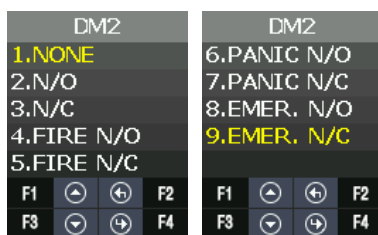
3.8.1.7. DM1

DM1(Door Monitor 1) is the input port and it is used to detect the signal state of lock.

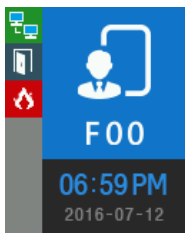


3.8.1.8. DM2

DM2(Door Monitor 2) is the input port and it is used to detect a various of sensor and alarm.

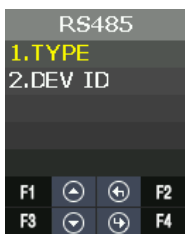


For example, if connecting with fire sensor, it should set 4. FIRE N/O or 5. FIRE N/C and it may cause fire alarm and icon in case of fire. In case of fire, the door automatically opens for safety.



3.8.2. RS485

It is the setting for the device with RS485 communication to interface with external.



3.8.2.1. TYPE

| TYPE | Explanation |
|------|-----------------------|
| NONE | It doesn't use RS485. |

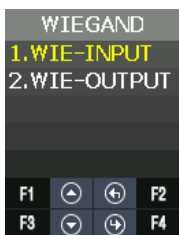
3.8.2.2. DEV ID

DEV ID is the ID that distinguishes devices and it can be set up 0-7 during RS484 communication.



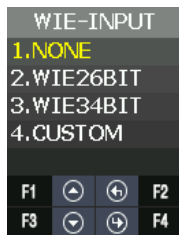
3.8.3. WIEGAND

WIEGAND supports each one of Input port and Output port.



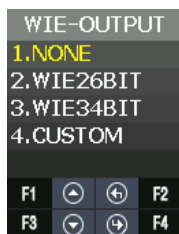
3.8.3.1. WIRE-INPUT

It is used to set the input type when working with the device connected into WIEGAND input port.



| Category | Explanation |
|----------|--|
| NONE | WIEGAND input port is not used. |
| WIE26BIT | EM, HID26 Card Module |
| WIE34BIT | MIFARE Card Modules |
| CUSTOM | Use Access Manager program and set Wiegand format. |

3.8.3.2. WIRE-OUTPUT



| Category | Explanation |
|----------|--|
| NONE | WIEGAND output port is not used. |
| WIE26BIT | EM, HID26 Card Module |
| WIE34BIT | MIFARE Card Modules |
| CUSTOM | Use Access Manager program and set Wiegand format. |

3.8.3.3. CUSTOM BIT LENGTH

It can set BIT length as 1~128.



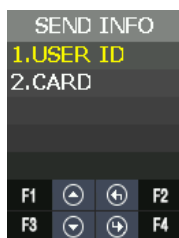
3.8.3.4. SITE CODE

It is used to set the value of Site Code that is sent to WIEGAND output port.



3.8.3.5. SEND INFO

It is used to select the transmitting data by the output port.



| SEND INFO | Type | None |
|-----------|--------|--|
| USER ID | 26 Bit | E.Parity(1)+ Site Code(8bit) + ID(16bit) + O.Parity(1) |
| | 34 Bit | E.Parity(1)+ Site Code(8bit) + ID(24bit) + O.Parity(1) If the length of the User ID greater than 8, and sent in the following format without site code: E.Parity(1)+ ID(32bit) + O.Parity(1) |
| Card | 26 Bit | E.Parity(1) + 24bit Card Number+ O.Parity(1) |
| | 34 Bit | E.Parity(1) + 32bit Card Number + O.Parity(1) |

3.9. STATUS Menu



STATE menu has the following features.

| STATE information | Explanation |
|-------------------|---|
| DB INFO | User DB, Authentication log data |
| NETWORK | The setting information related to network |
| OPTION | TNA, Screen setting, Saving, Time out, Lock mode |
| INT DEVICE | Display the setting state related to the internal device. |
| EXT DEVICE | Display the setting state related to the external device. |
| I/O PORT | Display the current signal of Input / Output port that interfaces with outside. |
| VERSION | Display the version of the equipped device in the terminal. |

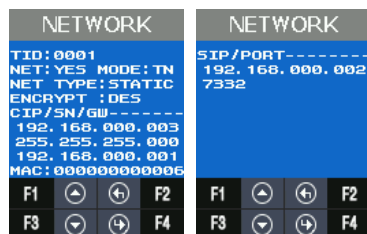
3.9.1. DB INFO

It displays User's DB information and the authentication log information.



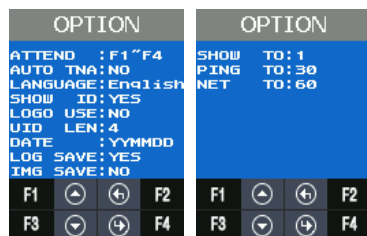
3.9.2. NETWORK

It displays the network setting value.



3.9.3. OPTION

It displays the option setting value.



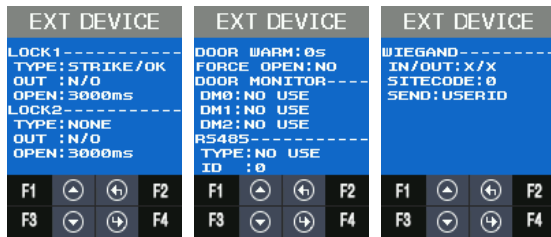
3.9.4. INT DEVICE

It displays the setting value related to the internal device.



3.9.5. EXT DEVICE

It displays the setting information related to the external device.



3.9.6. I/O PORT

It reflects the current I/O Port state and displays it on the screen.

Output Port: LOCK1, LOCK2

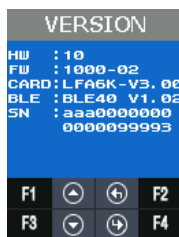
Input Port: DM0~DM2, W0IN, W1IN, INSIDE Open, Tamper

When the input port shorts GND, the signal modifies from **HIGH** to **LOW**.



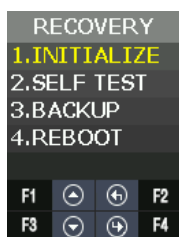
3.9.7. VERSION

It displays the equipped module in the terminal and other version information.



3.10. RECOVERY Menu

RECOVERY has the features as follows.



| Category | Explanation |
|----------|-------------|
|----------|-------------|

| | |
|------------|---|
| INITIALIZE | CONFIG LOG DB FACTORY |
| SELF TEST | INT DEVICE EXT DEVICE |
| BACKUP | LOG EXPORT USER EXPORT USER IMPORT FW UPDATE |
| REBOOT | REBOOT |

3.10.1. INITIALIZE

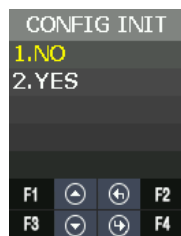
It is used to initialize CONFIG, LOG DB, and FACTORY in the terminal.



3.10.1.1. CONFIG

It is used to initialize the modified setting value in the menu as the default value when shipping from factory.

If a user registered in the terminal exists, you can't initialize the configuration information.



3.10.1.2. LOG DB INIT

It is used to delete the user authentication log saved in the terminal.



3.10.1.3. FACTORY INIT

If trying FACTORY INIT, setting data, authentication log data, and user registration information are initialized as setting state when shipping from factory.

★ It should be careful because the current data can be lost when you setting wrong.



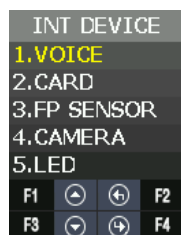
3.10.2. SELF TEST

It is used when the terminal tests the operation state about internal & external device by itself.



3.10.2.1. INT DEVICE

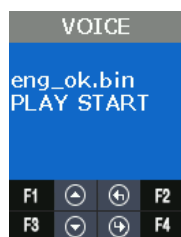
It could test VOICE, CARD, FP SENSOR, CAMERA and LED equipped internally by itself.



| Category | Explanation |
|-----------|------------------------------|
| VOICE | Voice output test |
| CARD | Card recognition test |
| FP SENSOR | Fingerprint recognition test |
| CAMERA | Camera equipment test |
| LED | LED output test |

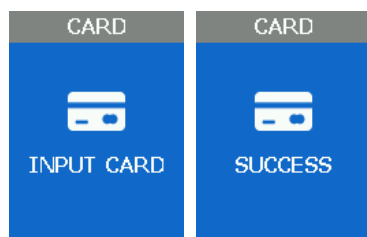
Voice Test

When authentication successes, it repeats and play voice guidance.



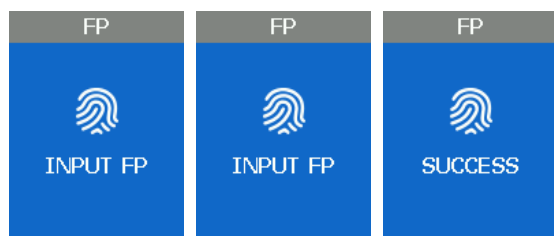
Card Test

As you see below, the screen displays "INPUT CARD" state at first. When recognizing the card, "Success" screen displays and it returns "INPUT CARD" state again. If you want to stop testing, press **F2**.



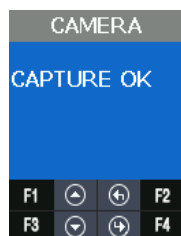
FP Sensor Test

FP Sensor Test is used to test the operation state of FP sensor from terminal. Input your fingerprint twice, if they are same, it shows "Success" screen. Otherwise, if not, it shows "Failure" screen.



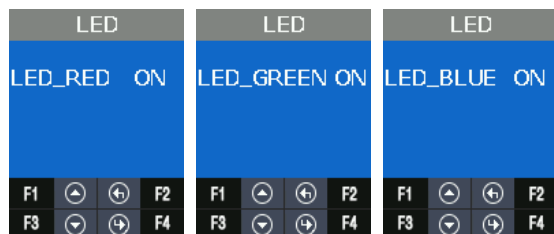
Camera Test

It is used to check whether the camera state is normal in the terminal to capture photos.



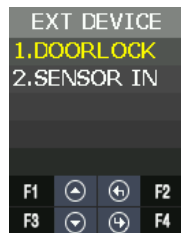
LED Test

It is used to check whether the state is normal about RED, GREEN and BLUE LED used to inform the operation state. At intervals of 2 seconds, RED, GREEN and BLUE LED changes from ON to OFF.



3.10.2.2. EXT DEVICE

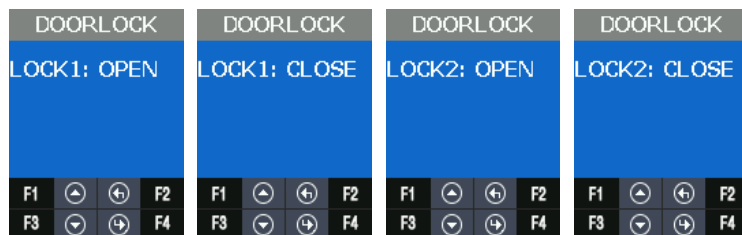
It can test the features related to the external device by itself.



| Category | Explanation |
|-----------|--|
| DOORLOCK | Lock1, Lock2 |
| SENSOR IN | DM0 DM1 DM2 INSIDE OPEN TAMPER |

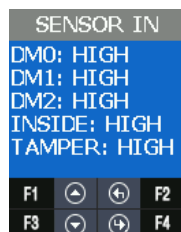
DOORLOCK Test

It is used to check the state of LOCK1, LOCK2 OPEN /CLOSE from the terminal.
The procedure is as follows.



SENSOR IN



It is used to check the signal state about the input port.
When the port shorts GND, if signal changes LOW, it is normal.

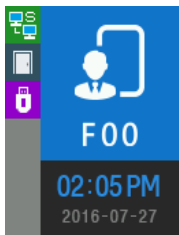


3.10.3. BACKUP

When the saved data from the terminal sends to USB by using UDL device or brings the data from USB memory and then applies it, it is used. It is available only when the UDL module is. UDL is the option module, so it is not basically provided. If you want to get more information about UDL module, please contact customer service. USB memory recommends using SanDisk.(NOTICE: UDL Device is not supported for all USB memory. UDL module may not work depending on the USB memory size, manufacturer, and method.)



If Terminal detect UDL Device and USB memory,  icon is displayed in the default screen. If  icon isn't displayed, all backup function doesn't operate.



3.10.3.1. LOG EXPORT

The saved log data from terminal saves in USB memory through UDL (User Data Downloader module).

Only the log data in the selected period sends to USB and saves it through UDL.

The file name saved in USB memory is divided by period as follows.

1. **1Day:** L1Day.NLG,
2. **1~30Day:** L30Day.NLG
3. **1~90Day:** L90Day.NLG
4. **1~180Day:** L180Day.NLG
5. **ALL:** ALL.NLG



3.10.3.2. USER EXPORT

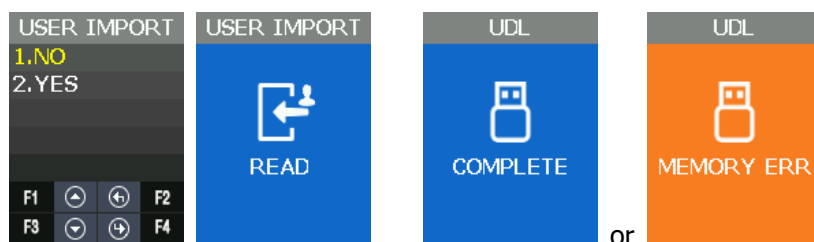
The saved User DB from the terminal saves in USB memory through UDL. It saves as USER.NDB file.



3.10.3.3. USER INPUT

It reads the user DB from USB memory through UDL and adds it in terminal user DB. If inputting user DB in the terminal, all existing user DB are deleted. If you need the existing user DB saved in the terminal, back up first and try to input the user. It opens USER.NDB file in USB memory and brings into the terminal through UDL. The user registration data that you brought is reflected in the internal DB and added.

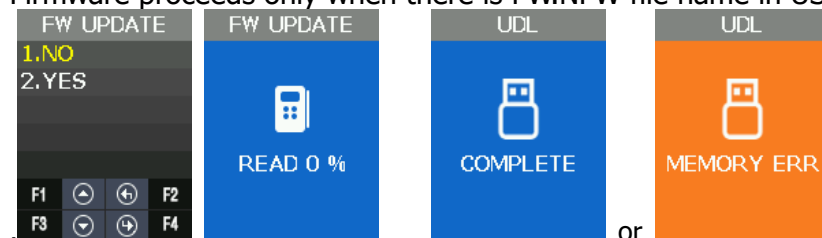
※ CAUTION: If you press F2 Key to stop in READ state, user loading fails.



3.10.3.4. FW UPDATE

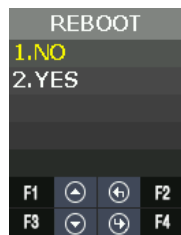
It is used when reading the firmware from USB memory through UDL and updating the terminal firmware.

Firmware proceeds only when there is FW.NFW file name in USB memory.



3.10.4. REBOOT

It is used when rebooting the terminal.



Appendix 1. Glossary

<Glossary >

- Administrator (Admin)
 - The administrator can access the terminal menu mode. He/she has the authority to add/modify/delete terminal users and to change the operating environment by changing settings.
 - If there is no registered administrator in the terminal, anybody can access to the terminal menu and change settings. **It is recommended that more than one administrator be registered in the terminal.**
 - The administrator has the authority to change critical environmental settings of the fingerprint reader. So, special attention is required to its registration and operation.
- 1:1 Authentication
 - The user fingerprint is verified after entering User ID or Card.
 - Only User ID or the user fingerprint registered to the card is compared. This is called One-to-One Authentication.
- 1: N Identification
 - The user is searched only by the fingerprint.
 - The same fingerprint as the input fingerprint is identified among the registered fingerprints without User ID or Card entered. This is called One-to-N Identification.
- Authentication Level
 - As a level used for fingerprint authentication, it is displayed in Step 1 to 9. Authentication cannot be allowed before the degree of match between two fingerprints is higher than the set authorization level.
 - The higher authentication level may ensure the higher security. But it requires the relatively high concordance rate. When authenticating User ID, it high likely to deny authentication.
 - 1:1 Level: Authentication level applied when 1:1 authentication
 - 1: N Level: Authentication level applied when 1: n authentication
- Authentication Method
 - It refers FP (Fingerprint) Authentication, RF (Card) Authentication and a various types of authentication methods made by each of a combination.
- LFD (Live Finger Detection): Fake fingerprint prevention function
 - The LFD allows only actual fingerprints to be entered, except for any fake fingerprints made of rubber, paper, film, and silicon and the like.

Appendix 2. Declaration of Conformity

- This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:
 - This device may not cause harmful interference.
 - This device must accept any interference received, including interference that may cause undesired operation.
- Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

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 communications. 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 different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

CAUTION: Exposure to radio frequency radiation

This equipment should be installed and operated with a minimum distance of 20 cm between the radiator and your body.

Appendix 3. Radio Equipment Directive (RED)

Rosslare hereby declares that the AY-H6355BT is in compliance with essential requirements and other relevant provisions of Directive 2014/53/EU.

Appendix 4. RoHS Directive

Under our sole responsibility that the following labeled AY-U9xxBT is tested to conform to the Restriction of Hazardous Substances (RoHS) directive – 2011/65/EU – in electrical and electronic equipment.



Asia Pacific, Middle East, Africa

Rosslare Enterprises Ltd.
Kowloon Bay, Hong Kong
Tel: +852 2795-5630
Fax: +852 2795-1508
support.apac@rosslaresecurity.com

United States and Canada

Rosslare Security Products, Inc.
Southlake, TX, USA
Toll Free: +1-866-632-1101
Local: +1-817-305-0006
Fax: +1-817-305-0069
support.na@rosslaresecurity.com

Europe

Rosslare Israel Ltd.
22 Ha'Melacha St., P.O.B. 11407
Rosh HaAyin, Israel
Tel: +972 3 938-6838
Fax: +972 3 938-6830
support.eu@rosslaresecurity.com

Latin America

Rosslare Latin America
Buenos Aires, Argentina
support.la@rosslaresecurity.com

China

Rosslare Electronics (Shenzhen) Ltd.
Shenzhen, China
Tel: +86 755 8610 6842
Fax: +86 755 8610 6101
support.cn@rosslaresecurity.com

India

Rosslare Electronics India Pvt Ltd.
Tel/Fax: +91 20 40147830
Mobile: +91 9975768824
sales.in@rosslaresecurity.com

ROSSLARE
SECURITY PRODUCTS



• EN ISO 13485

