AY-B91x0BT

Professional Fingerprint Readers

User Manual

Models:
AY-B9120BT
AY-B9150BT

ROSSLARE
SECURITY PRODUCTS

Table of Contents

1. Before Getting Started

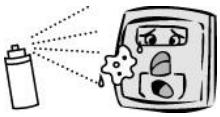
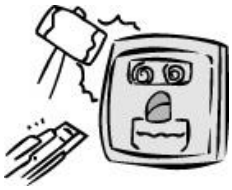
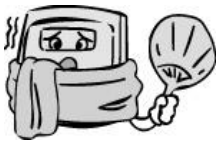
1.1. Safety Notes

- Warning

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

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

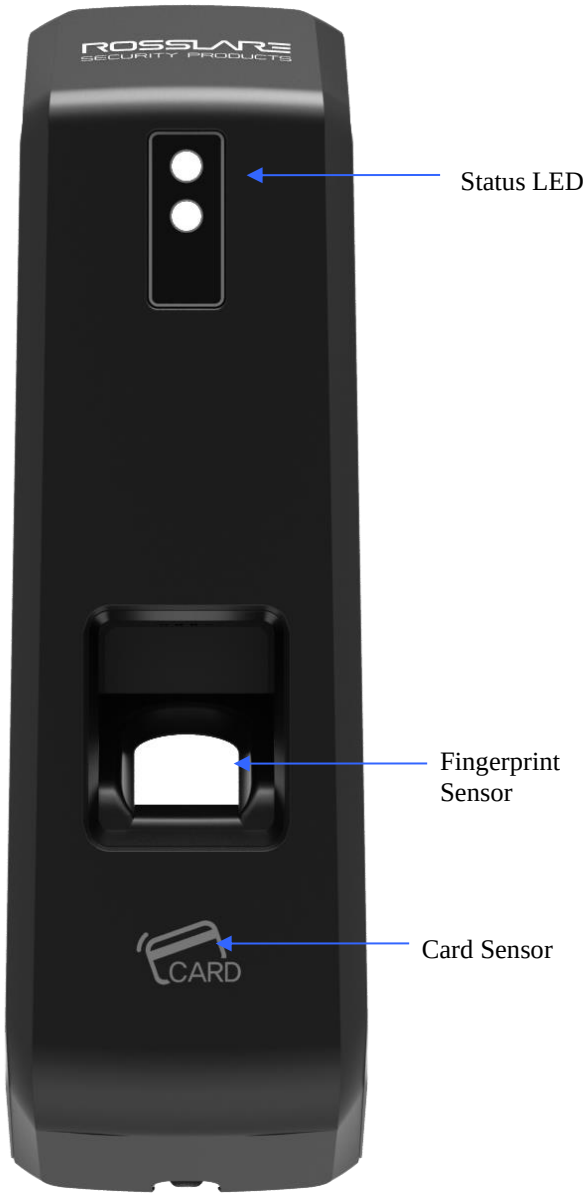
- Cautions

Do not install the terminal in a place exposed to direct sunlight. → Otherwise, it may cause malfunction, deformation and discoloration. 	Do not install the terminal in humid or dusty places. → Otherwise, it may cause malfunction. 
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. 	Keep the terminal away from magnets. → Otherwise, it may cause failure and malfunction. 
Keep the fingerprint input section clean. → Otherwise, the fingerprint cannot be recognized correctly. 	Do not spray insecticides or inflammables on the terminal. → Otherwise, it may cause deformation and discoloration. 
Keep the terminal away from shock or sharp objects. → Otherwise, it may damage the terminal and result in malfunction. 	Do not install the terminal in a place where there is a severe change in temperature. → Otherwise, it may cause malfunction. 

- 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



1.3. LED signals displayed during operation

●	Lighting	: Normal status
	Flickering	: When the input of fingerprint and card user is on standby
●	Lighting	: Light up for 1 second upon successful authentication.
	Flickering	: Flicker at one second interval when FW is downloaded and when an administrator application is entered.
●	Lights out	: Normal status
	Lighting	: Light up for one second when authentication fails.
	Flickering	: Flicker for one second upon the warning status (forced opening, non-connection of server, etc.).

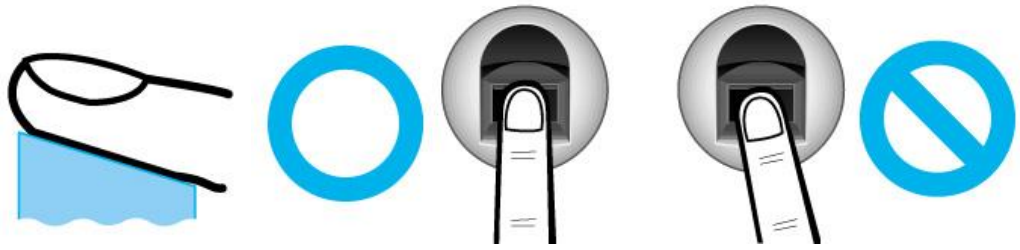
1.4. Buzzer guide announced during operation

Beep	When fingerprint or card is read	When the card is read, When the FP is entered in the FP window
2 beeps	When failure	If authentication fails or the user's input is wrong, If the control and setting of the terminal fail
Long beeping	When input standby	When it is notified that the input of fingerprint and card user is on standby
Short beeping	When success	If authentication is successful, If the terminal is successfully booted, If the control and setting of the terminal and successfully completed

1.5. How to register and enter 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.

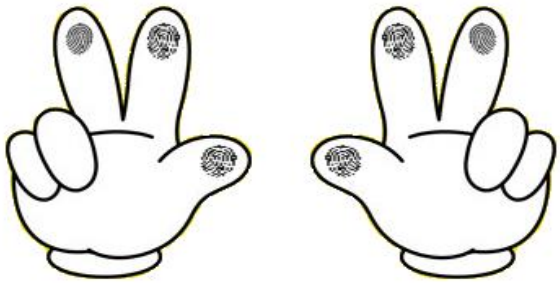


- Make sure that the fingerprint is clear and not wounded.
  Too dry, wet, blurry or wounded fingerprints are difficult to recognize. In this case, the fingerprint of another finger should be registered.

- Precautions subject to your fingerprint status

  The availability of the fingerprint may vary subject to your fingerprint status.

  - This product consists of a fingerprint recognition system and cannot recognize 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, a 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

The AY-B91x0BT series of professional-grade fingerprint readers include a high-speed optical sensor with a capacity of 20,000 templates featuring powerful algorithms with liveness check and encrypted data storage.

The readers include BLE connectivity that integrates to Rosslare My BLE-ID™ and BLE-Admin™ applications, and have RS-485, TCP/IP and Wiegand 26-Bit and 34-Bit connectivity.

The AY-B91x0BT series consists of the following products:

- AY-B9120BT – Professional Fingerprint reader with EM + BT
- AY-B9150BT – Professional Fingerprint reader with MIFARE + BT

Note: The standalone management software is RosslareBio9000. Please refer to the *Rosslare Bio9000 Software Manual*. For AxTraxNG™ integration, please refer to the *AxTraxNG™ Software Installation and User Manual*.

2.1. Product Features

- 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.

- Waterproof and dustproof functions
  - Acquired the IP65 level of waterproof and dustproof certification.

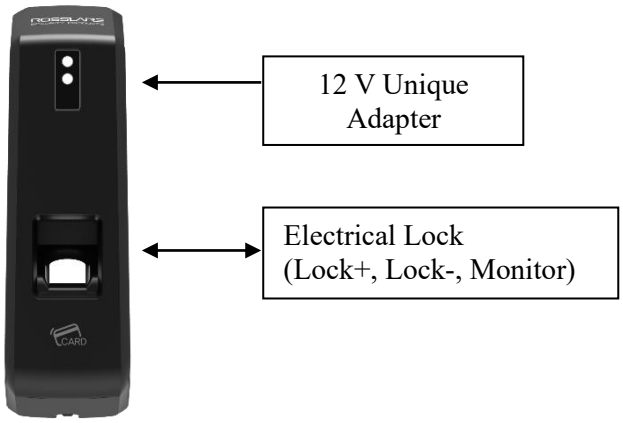
- Various card options
  - 125 kHz-based EM cards, and 13.56 MHz-based MIFARE cards are supported optionally.

- 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.

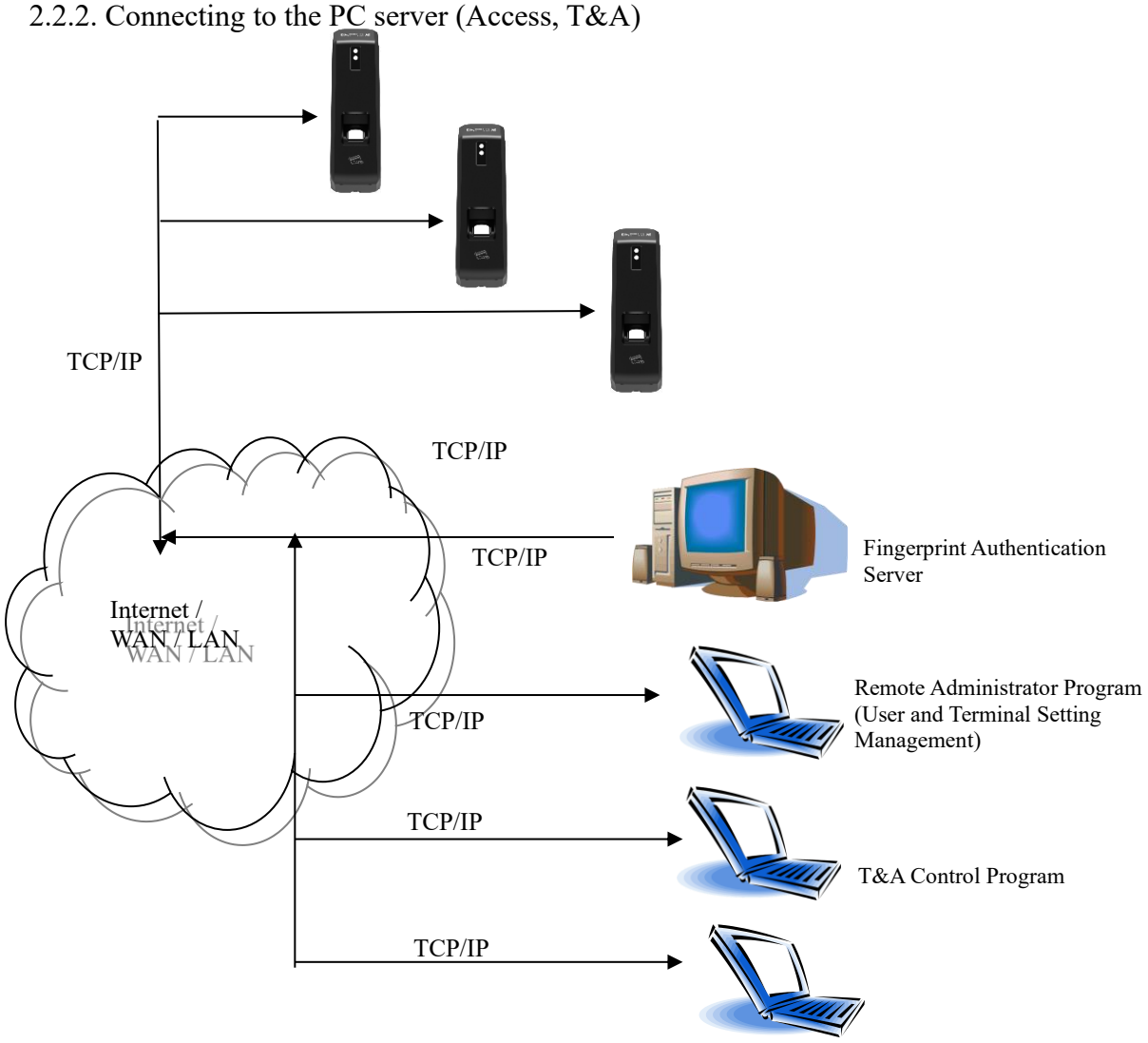
- **Mobile interlocking function**
  - By using Smartphone Bluetooth, the terminal can be set to Admin App.

2.2. Configuration Diagram

2.2.1. Standalone Use (Access)



2.2.2. Connecting to the PC server (Access, T&A)



3. Environment Setting

3.1. Terminal Setting

3.1.1. Setting via Rosslare Bio9000

- Card Format
  The type of card to be used can be set.

Settings	Display Method
No Use	Do not use the card authentication
EM	Use a low-frequency (125 kHz) EM card
MIFARE	Use a high-frequency (13.56 MHz) MIFARE card

- Wiegand Output
  This mode is available if the terminal is equipped with a separate controller operated by Wiegand input.

Settings	Display Method
No Use	Do not use the Wiegand communication
26Bit	Perform the Wiegand communication by a format of 26-Bit
34Bit	Perform the Wiegand communication by a format of 34-Bit

- Device Mode
  If reader mode is selected, Wiegand output is Card Number when authentication is Success.
  If access control is selected, Wiegand output is User's ID when authentication is Success.

- Sitecode
  Set the value of Sitecode to transfer upon Wiegand output.
  If Wiegand output is 26bit, a value of 0 to 255 can be set. If Wiegand output is 34-Bit, a value of 0 to 32767 can be set.

- Ext 485
  Can select external RS-485 device.

- 485 ID
  Can assign ID of External RS-485 device to 0-7.

- 1:N Level
  When 1:N authentication, set the verification level to 5-9.

- 1:1 Level
  When 1:1 authentication, set the verification level to 1-9.

- Max ID Length
  This indicates the length of ID which can be entered to the maximum.

- Network Mode
  Set whether the terminal is used to either a standalone mode or a network mode.

- Node ID
  Set the terminal ID to add to ACM Pro in the range of 1 to 2000.

- Use DHCP
  Set whether to use a static IP.

- Terminal IP

Set the terminal IP.

- Server IP
  When the terminal is used in conjunction with Rosslare Bio9000, set the server IP.

- Subnet Mask
  Set the subnet mask value of the terminal.

- Gateway
  Set the gateway value of the terminal.

- Port No.
  Set the Rosslare Bio9000 Server port to 2000-65535. (Default: 7332)

- Network Timeout
  Set the communication cycle time between the Rosslare Bio9000 server and the terminal to the range of 2-20.

- Time Synchronization
  Set time of device to time of smart phone.

- Firmware Version
  The terminal firmware version and the BLE firmware version are displayed.

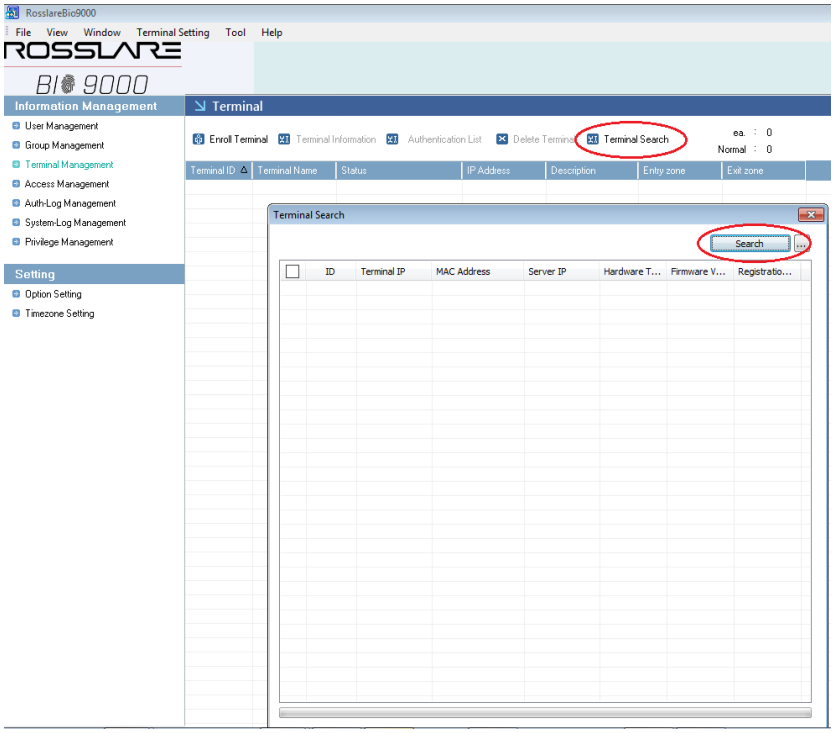
- Initialize
  All data except logs and user information are initialized.

- Factory Initialization
  Initialize the settings of the terminal as set at a factory.

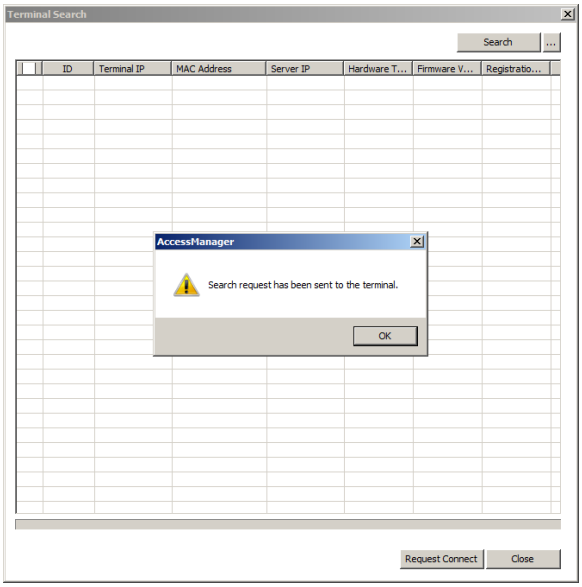
※ **The terminal is rebooted after saving the settings. Therefore, it is recommended to access the terminal after 30 to 60 seconds.**

3.1.2. To set the terminal IP via Rosslare Bio9000

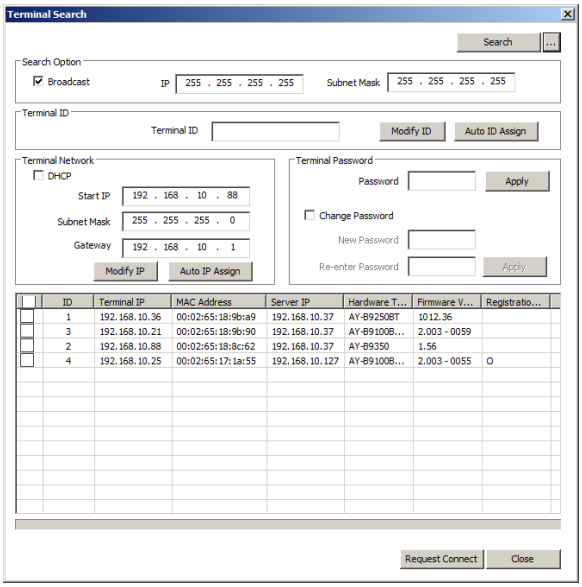
By running terminal search items in the terminal management menu of Rosslare Bio9000, perform the setting of terminal IP.



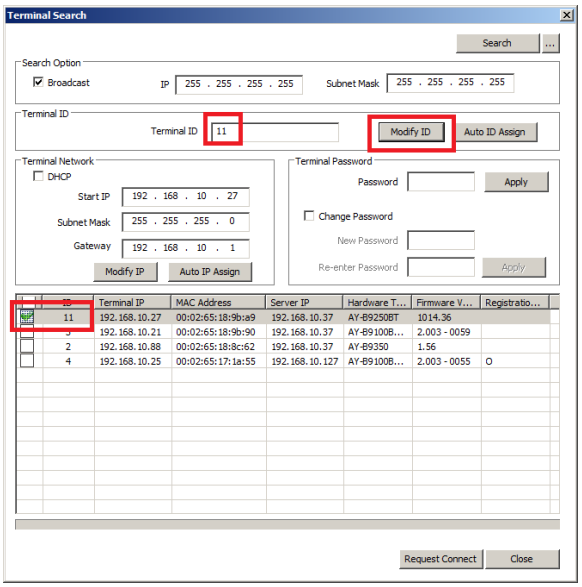
When clicking the Search button on the above screen, the unregistered terminals appear as shown below.



When clicking the "..." button, the detailed setting screen appears as shown below.



To change the terminal ID and network settings, select the terminal to set, enter the change value, and click the "Modify IP" button. Then, you can check that the terminal value has been changed.



Set Terminal ID and Terminal Network and then click the "Request Connect" button at the bottom, and the terminal appears as the unregistered status on the screen.

*** For more details, please refer to the Rosslare Bio9000 Manual.**

3.2 Configuration with the BLE-Admin Application

1. Download the Rosslare BLE-Admin application from Google Play or App Store using the following QR code.

2. Open the application, select the required reader from the list displayed.
3. Enter the password.

NOTES:

Use the default password (9999) when you log in to the BLE-Admin application for the first time.

- It is highly recommended that you change the password (see step 4).

4. On the main screen, configure the following:

Option	Remarks
Door Name	Assign name to selected door reader
Password	Change password

5. Tap **Set Configuration** and configure the following:

Parameter	Remarks
Terminal IP	Enter the Terminal IP
Port	Slide to select the Port Number
Subnet Mask	Enter the Subnet Mask
Default Gateway	Enter the Default Gateway
Server IP	Enter the Server IP
Wiegand Format	Select the Wiegand Format: • Wiegand 26-bit (default) • Weigand 34-bit
Weigand Mode	Select the Wiegand Mode: • Card Number (default) • User ID
LFD Mode	Select to turn the LFD Mode On or Off
DHCP	Select to turn DHCP On or Off

NOTE: The My BLE-ID application allows a mobile device to be used as a credential. Download the application from Google Play or App Store using the following:

4. How to Use Terminal

4.1. Authentication

4.1.1. Fingerprint Authentication

Place your finger on the fingerprint sensor. The fingerprint sensor lights on and receives fingerprint input. Keep your finger on the fingerprint sensor until the light turns off completely.

4.1.2. Card Authentication

Place the card on the card sensor of the terminal.

4.1.3. Multiple Authentication

For users who have to be authenticated by the combination of authentication methods such as “Card and Fingerprint”, if the first input authentication method is successful, the remaining authentication method is performed.

5. Troubleshooting

5.1. When the fingerprint authentication time is too long or fails:

- When the terminal operates by the 1:N (Server) authentication in the network mode, if the server is used for personal or business use, a server load may reduce the fingerprint recognition rate and require the long fingerprint authentication time. It is recommended to build a dedicated server.
- Check that there are no scratches or foreign matter on your finger or FP sensor. If there is foreign matter, wipe it with a dry cloth. If there is a large scratch, re-register another fingerprint through the administrator.
- If the fingerprint status is bad, lower the individual security level in the user information and attempt 1:1 Authentication.
- If the RF card registered by the user's ID has been authenticated, when the fingerprint authentication fails, whether the user exists or not is verified. Check that the user is a registered user.

5.2. When the fingerprint is not entered well:

Very dry or wet fingerprints may not be normally entered.
If the fingerprint is wet, wipe it with a dry towel. If the fingerprint is dry, blow your breath or apply oil on your hands. Then, try to enter the fingerprint again.

5.3. When the RF card authentication fails:

Check that the card possessed by users conforms to the card type set in the "RF Card Type" in the "Option Setting" of the Rosslare Bio9000 program.

5.4. When the network is not connected:

- Check that the terminal is registered in the terminal management item in the information management menu of Rosslare Bio9000.
- If the terminal is not registered, check that it is set in the terminal search of Rosslare Bio9000.
  - Server IP on which Rosslare Bio9000 is installed
  - Check that the terminal ID is set up correctly.
  - If DHCP is not used, check the relevant information.

5.5. When the authentication is successful but the door does not open:

Check that the access is controlled by the time zone.

5.6. When the user is not registered:

This product is set by default to operate as a network mode.
If the connection is abnormal in the network mode, the user cannot be registered.
Check the network connection status.

5.7. When the product is unstable or does not work:

- Select the terminal in the terminal management menu of Rosslare Bio9000, click the right mouse button, and select the [terminal Restart] item. The terminal restarts.
- If the server management program is being used, try to run the server again.
- If the terminal does not normally work after checking all of the above, please contact our Customer Support Team.

Appendix 1. 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 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
  - 1:1 Level: Authentication level applied when 1:1 authentication
  - 1:N Level: Authentication level applied when 1:n authentication

- LFD (Live Finger Detection): Fake fingerprint prevention function
  - The LFD allows only actual fingerprints to be entered, preventing 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-B91x0BT 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-B91x0BT 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