

suprema

# BioLite Net

IP based Outdoor Fingerprint Terminal

User Guide



This manual is provided for information purpose only. All information included herein is subject to change without notice. Suprema is not responsible for any changes, direct or indirect, arising from or related to us of this manual.

© Copyright 2008 Supremainc. All rights reserved.

# Contents

<b>Safety Instructions .....</b>	<b>5</b>
<b>1. Before Use .....</b>	<b>6</b>
1.1 Components .....	6
1.2 Body.....	7
1.3 Methods for fingerprint input.....	8
1.4 System setup procedure.....	10
1.4.1 Registering the initial administrator .....	11
1.4.2 Network configuration.....	12
1.4.3 Stand-alone configuration.....	15
1.4.4 Configuring Secure I/O.....	17
1.4.5 Configuring environment settings.....	18
1.5 Authorization methods .....	19
1.5.1 Finger Only.....	19
1.5.2 Finger or PIN.....	20
1.5.3 Finger and PIN .....	23
1.5.4 PIN Only.....	24
1.5.5 Card Only .....	25
<b>2. User Management.....</b>	<b>26</b>
2.1 Enrolling a user.....	26
2.1.1 Registration on the terminal .....	26
2.1.2 Registration on the card .....	29
2.2 Editing a user data .....	31
2.3 Deleting a user data.....	35
<b>3. Configuration for Screen and Sound.....</b>	<b>36</b>
3.1 Date, Time .....	36
3.2 Backlight .....	37
3.3 Sound .....	39
<b>4. Device Configuration .....</b>	<b>40</b>
4.1 Authorization.....	40
4.2 In/Out .....	45
4.3 System.....	52
<b>5. Attendance Management .....</b>	<b>56</b>
5.1 Operating environment.....	56
5.2 Setup for attendance management .....	57
5.3 Operation modes .....	58
5.3.1 Key Input .....	58
5.3.2 Manual.....	58
5.3.2 Auto.....	59
5.3.3 Fixed.....	60

<b>6. FAQ.....</b>	<b>61</b>
6.1 Error messages.....	61
6.2 Troubleshooting .....	62
6.3 Usage summary .....	63
6.4 System Installation .....	64
6.4.1 Cable specifications.....	64
6.4.2 Installing the bracket.....	65
6.4.3 Connecting Power & RS-485.....	66
6.4.4 Connecting the switch.....	66
6.4.5 Connecting the relay.....	67
6.4.6 Connecting Network.....	68
6.4.7 Connecting Wiegand.....	68
6.4.8 Electrical specifications.....	69
6.5 Specifications .....	70
6.6 FCC Notice.....	72

# Safety Instructions

## Installation



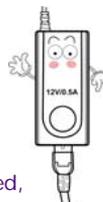
Do not arbitrarily install or repair the product.

The warranty does not apply to any product damage caused by an arbitrary installation or repair.



Use the power adapter provided or one for 12V 0.5A or above.

When sharing the power with other devices such as electric door lock, check the power capacity considering power requirements for each device. If appropriate power is not used, it may not operate normally.



## In Use



Ensure that password does not exposed to unauthorized individuals. Frequent change of password is recommended.

Any illegal access your product may happen.



Be cautioned for the fingerprint contact area not to be contaminated or damaged by dirty hands or foreign materials.

It may affect fingerprint recognition performance or cause a failure.



Do not forcibly press the buttons of the product and avoid any contact with sharp object to the device.

It may cause a failure.

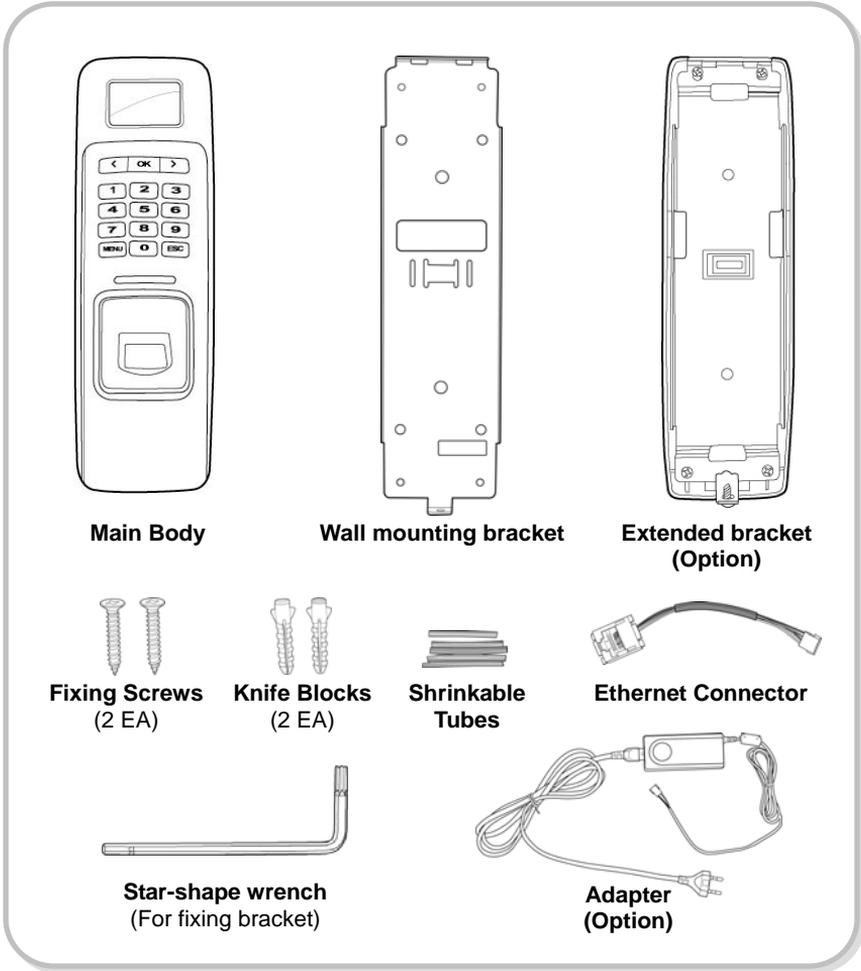


Do not clean the device with any form of liquid. Use soft and dry cloth only.



# 1. Before Use

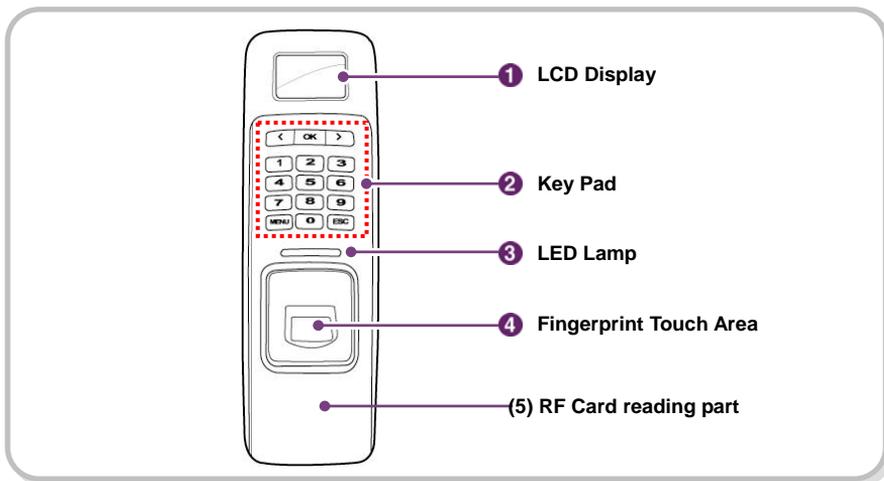
## 1.1 Components



Note

The components shown above may differ depending on the installation environment.

## 1.2 Body



No.	Name	Description
1	LCD Display	The operation status is displayed.
2	Key Pad	<p>0–9 Buttons: Used to enter the ID and password.                      &lt; &gt; Arrow Buttons: Used to move the selected item.   Button: Used to select the desired function.   Button: Used to enter or exit the menu.   Button: Used to exit from the menu or cancel the desired action.</p>
3	LED Lamp	<p>The operation status is displayed with an alert sound.</p> <ul style="list-style-type: none"> <li>– Green (Sound: beep beep beep beep!): Authorization success</li> <li>– Red (Sound: beep beep beep!) : Authorization failure</li> <li>– Pink (Sound: beep!) : Processing</li> <li>– Blue and Yellow blink in turn at an interval of 2 seconds (No sound): No IP address is given because DHCP is set in TCP/IP Setup</li> <li>– Blue and Sky Blue blink in turn at an interval of 2 seconds (No sound): Normal operation</li> <li>– Red and Pink blink in turn at an interval of 2 seconds (No sound): Device locked or no administrator</li> <li>– Blue and Red blink in turn at an interval of 2 seconds (No sound): The time is reset due to battery discharge.</li> <li>– At first use, Red blinks at an interval of 2 seconds (No sound): Initialization error, Consult with the manufacturer.</li> <li>– In normal use, Red blinks at an interval of 2 seconds (No sound): On the watch.</li> <li>– Yellow blinks shortly (No sound): Entry standby or in communication for getting an IP when DHCP is set in TCP/IP Setup</li> </ul>
4	Fingerprint Touch Area	Used to input a fingerprint for authentication.

## 1.3 Methods for fingerprint input

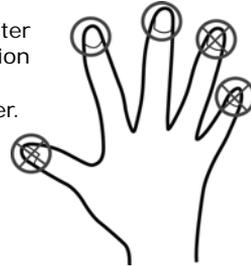
BioLite Net can easily recognize fingerprints even though the angle and location of the pattern change. However, it is recommended to properly input fingerprints for more precise recognition.

### Selecting a finger on fingerprint enrollment

Up to two fingerprints can be enrolled for each user in preparation of any abnormal situation like having a wounded finger or carrying an object with a hand.

In the case of a low recognition, the user can register the same fingerprint twice to increase the recognition rate.

It is recommended to use the index or middle finger. In case of other fingers, the recognition rate decreases because it tends to be more difficult to place the finger in the center of the sensor area.



### How to properly place a fingerprint

Place your finger firmly on the sensor area.

Adjust the finger so that its middle position can be located in the center of the sensor.

When the finger is vertically placed or its angle goes astray, the recognition may be a failure.



When enrolling your fingerprint, the first finger input window prompts. Then register the desired finger on the terminal as shown in the figure below.

When the re-entry window appears with a “tick” sound, re-enter the previously enrolled finger. The fingerprint input is made twice.

(Gently push your finger on the sensor to have a full fingerprint.)





Note

### In case fingerprint is not recognized normally

BioLite Net is designed to normally operate regardless of weather change or the angle and location of the fingerprint to place.

However, the recognition rate may vary depending on the external environment or fingerprint condition.

In abnormal cases, follow the directions below:

1. Retry after drying the wetness of your finger.
2. When your finger is too dry, retry after blowing on your fingertip.
3. When you have a cut on your registered finger, register another fingerprint.

BioLite Net



Before Use



Caution

### Cautions while registering your fingerprint

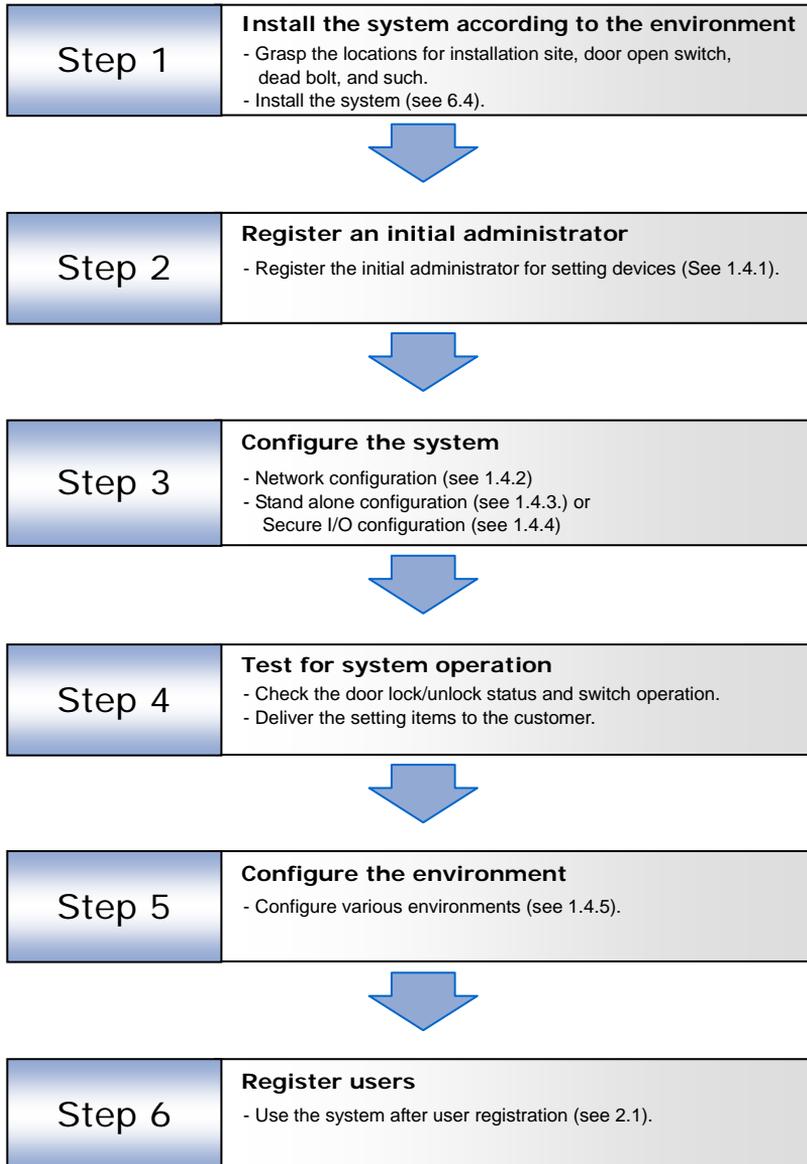
The initial fingerprint registration is important.

Because the recognition process compares the scanned fingerprint with the registered one, an abnormally registered fingerprint can cause a failure.

To increase the recognition rate, follow the directions below:

1. Put the center of your fingerprint on the middle of the sensor.
2. If you have a cut in your finger or your fingerprint is not clear enough, retry with another finger.
3. When fingerprint recognition is in progress, do not move your fingerprint .

## 1.4 System setup procedure



## 1.4.1 Registering the initial administrator

There is no administrator set for the product in the initial status. So register an administrator for configuring the environments for relay, door open switch, door open detection sensor, and such.

BioLite Net



Before Use

1. When the product is connected, a window appears as shown in the right figure. Enter an ID and press **OK**.

Enter ID  
1  
Enroll Admin

2. When the authorization mode window appears, use ◀/▶ buttons to move to **PIN Only**, and press **OK**.

Operation Mode  
◀ PIN Only ▶  
Enroll

3. When the password entry window appears, enter the desired password and press **OK**.

Enter PIN  
\*\*\*\*  
Enroll

4. When the password re-entry window appears, enter the previously input password again and press **OK**.

Confirm PIN  
\*\*\*\*  
Enroll

5. The completion message window appears.

Completed



Note

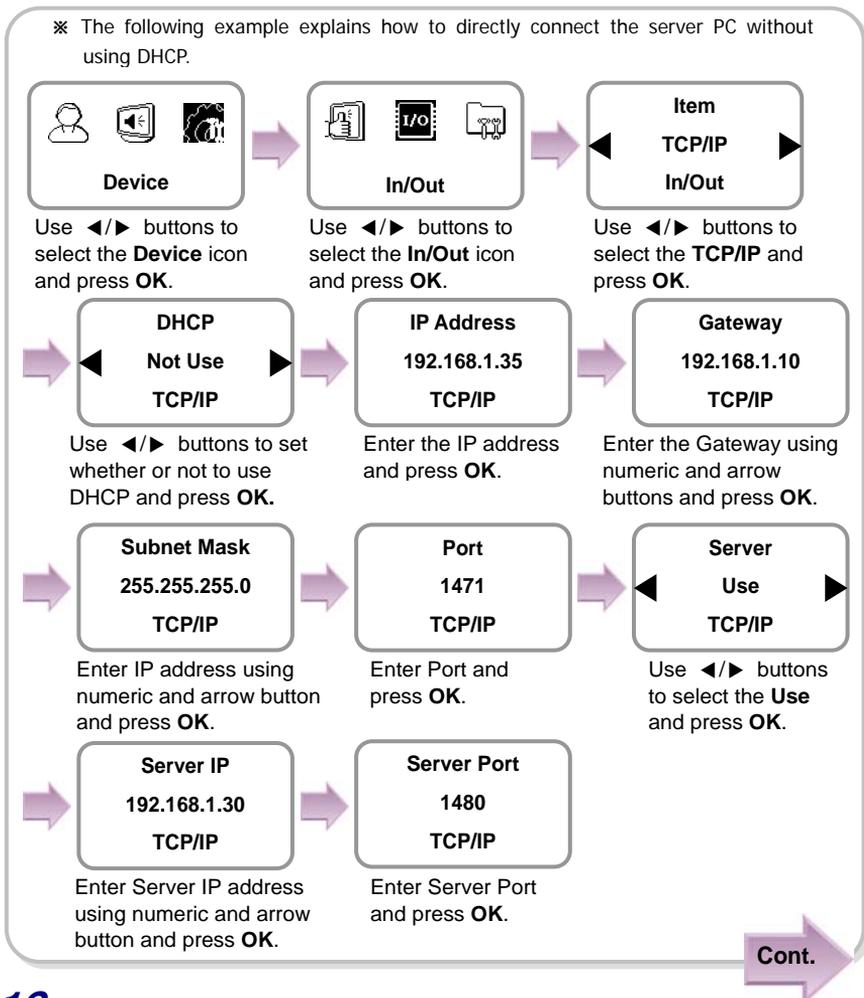
This procedure is necessary to temporarily configure the installation-related settings. Modify the administrator information after the installation is complete.

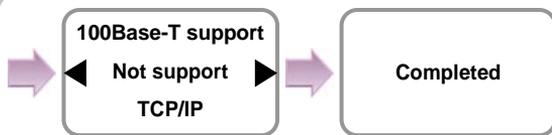
## 1.4.2 Network configuration

The network configuration is required to connect the dedicated PC software or other devices via network. Configure the settings according to the communication environment in your place.

### [In case of configuring the network via Ethernet]

1. Connect the terminal to the computer that has the dedicated PC software according to the network environment after seeing “6.4.6 Connecting network.”
2. Configure the settings for TCP/IP port and server according to the installation environment.





Use ◀/▶ buttons to set whether or not to support 100Base-T and press **OK**.

The completion message window appears.



Note

When you exit from the menu before completing the TCP/IP setting, the data is not stored so please finish the remaining steps until the setting completion message appears.

※**IP Address/Gateway/Subnet Mask Setup:** If DHCP is used, the values for IP address, gateway, and subnet mask are automatically assigned. Otherwise, set DHCP to **Not Use** and enter the corresponding values.

(When the right arrow is pressed, "." is entered while the left arrow deletes characters one by one.)

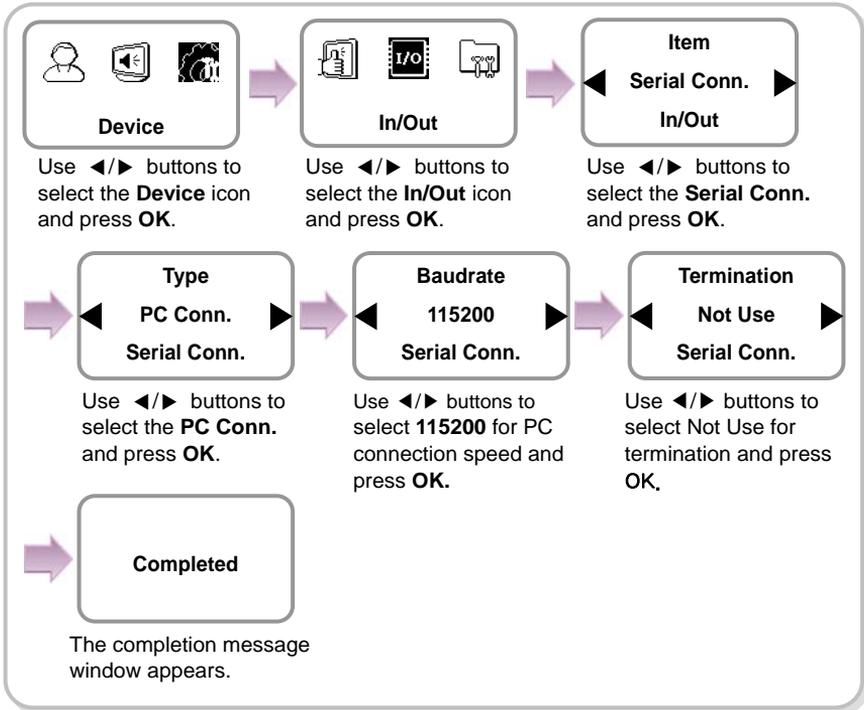
※**Server:** To directly connect the server of the dedicated PC software that enables monitoring and setting the terminal, use Server for its setup and enter the values for IP address and port number. (Refer to the dedicated PC software manual.)

※**TCP/IP Port, Server Port:** Should be the same values defined in the dedicated PC software. It is recommended to set the TCP/IP port to "1471" and Server to "1480." (When the port number is modified as you want, TCP/IP communication may not be active.)



## [In case of configuring the network via RS-485]

1. Connect the terminal to the computer that has the dedicated PC software or to another device according to the network environment after seeing "6.4.3 Connecting Power & RS-485."
2. Configure the settings for RS-485 according to the installation environment.

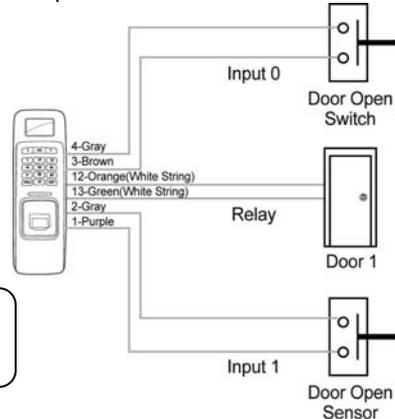


### 1.4.3 Stand-alone configuration

This configuration is required to use the device for stand alone purpose, which requires no communication with PC or other devices.



1. As shown in the figure, connect BioLite Net to respective switches.



Note

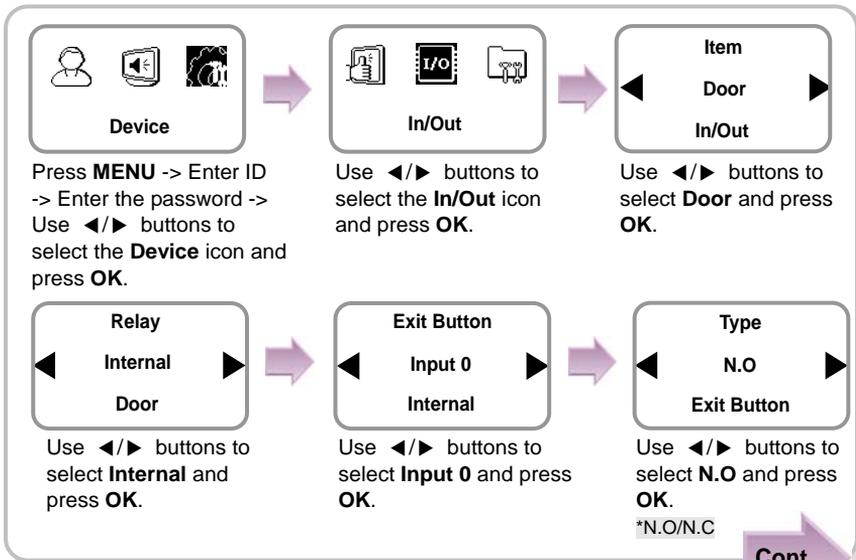
For actual wiring method, see "6.4 System Installation."

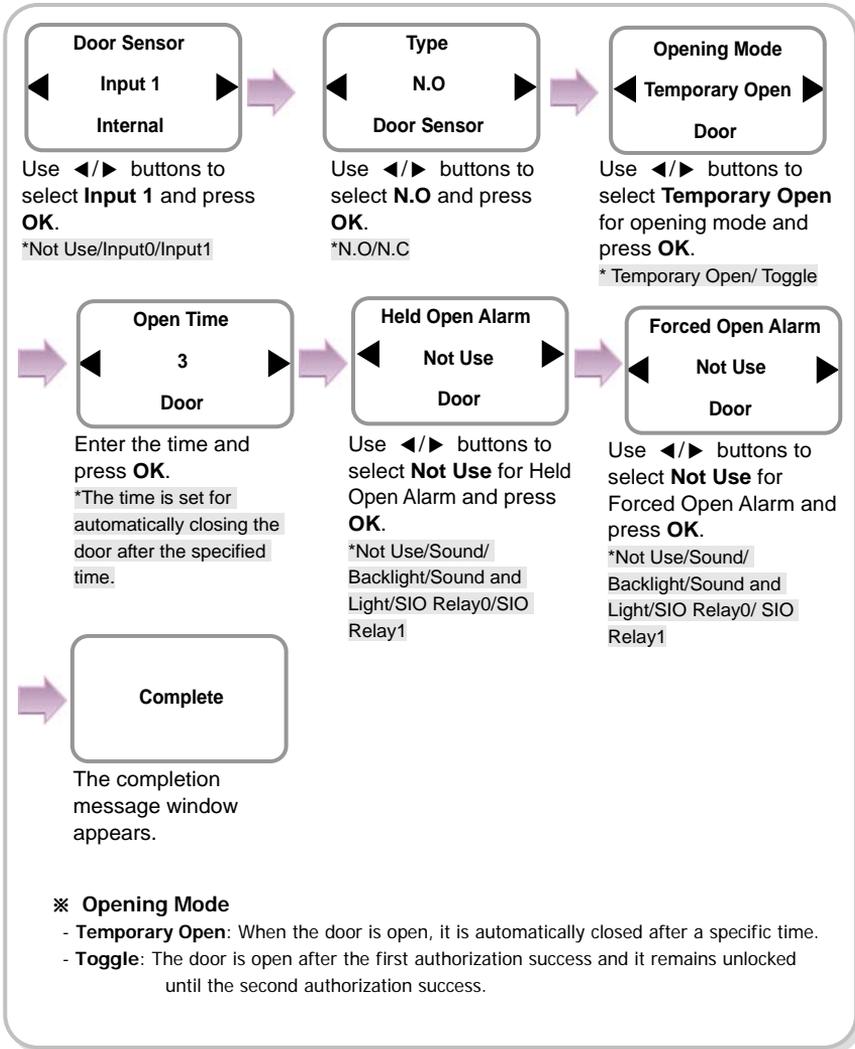
2. Configure the internal relay settings as shown below. (It is explained based on the figure above.)



Note

Follow the instructions below only when the dedicated PC software is not used. When using the software, refer to the software manual.





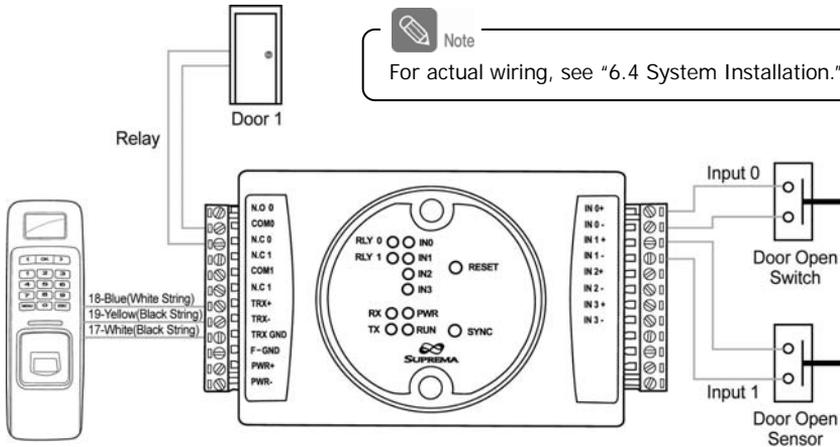
Note

When you exit from the menu before completing the relay setup, the configuration is not stored so please finish configuration until the message "Complete" appears.

## 1.4.4 Configuring Secure I/O

This connects BioLite Net to Secure I/O.

1. Connect wires between BioLite Net, Secure I/O, and respective switches as shown below.

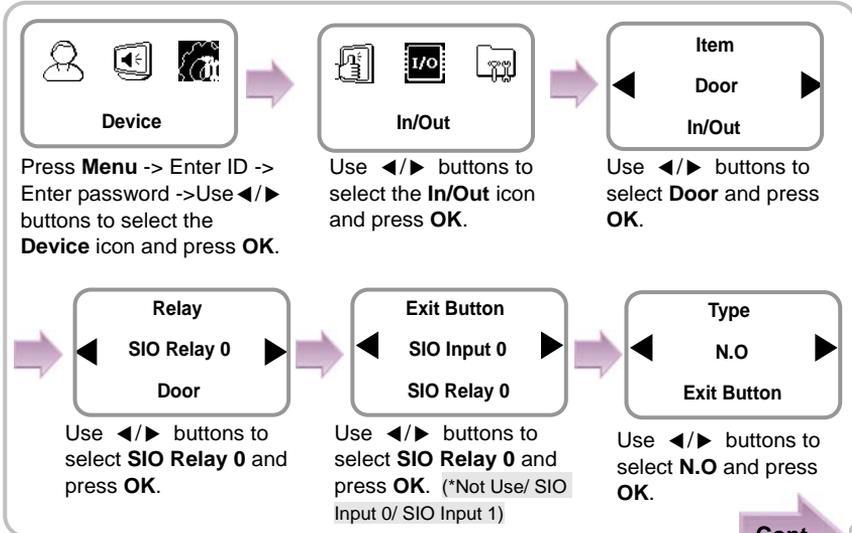


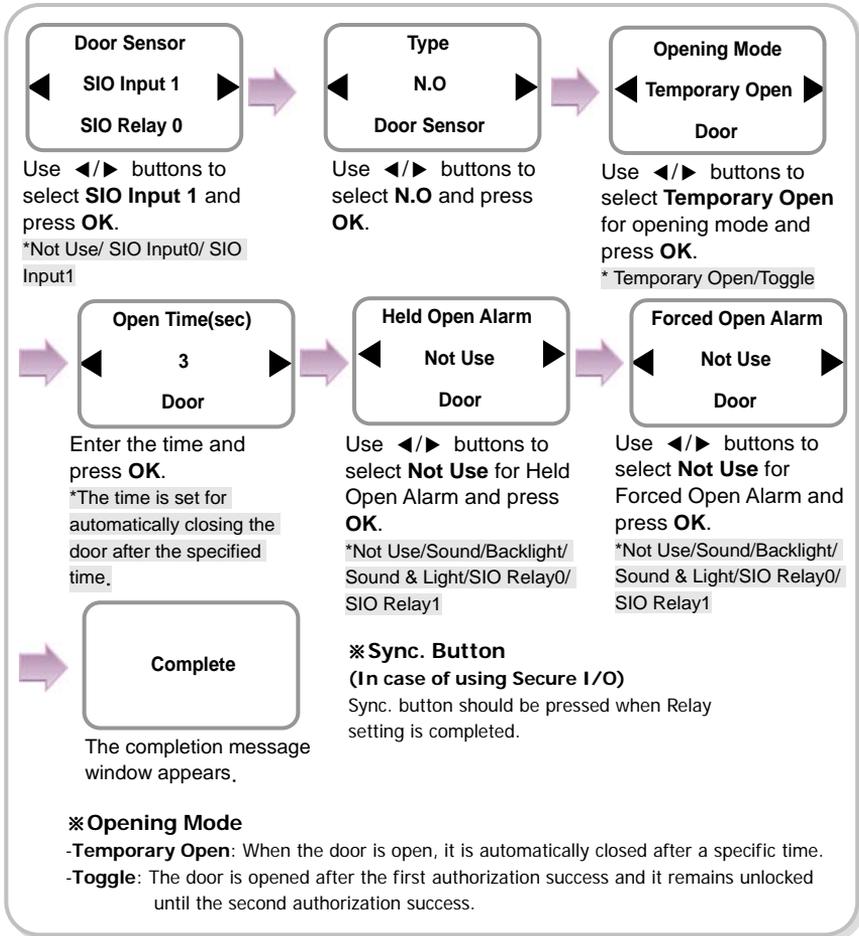
2. Configure the relay settings as shown below. (Based on the figure above)



**Note**

Follow the instructions below only when the dedicated PC software is not used. When using the software, refer to the software manual.





Note

When you exit from the menu before completing the relay setup, the configuration is not stored so please finish configuration until the message "Complete" appears.

### 1.4.5 Configuring environment settings

- ◆ Settings for date and time: Set the values as "3.1 Date, Time."
- ◆ Fingerprint authorization related settings: Set the values after reading the case of fingerprint selection in "4.1 Authorization."
- ◆ Operation mode setting: Finish the setting after seeing the operation mode selection case in "4.1 Authorization."

# 1.5 Authorization methods

For changing the terminal authorization method, see the operation mode selection case in “4.1 Authorization.”

To separately set the authorization method for each user, see “2.2 Editing a user data.”

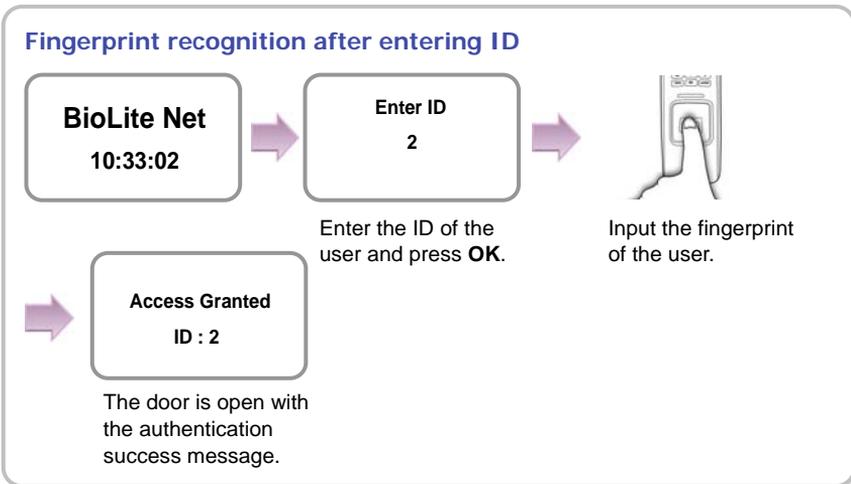
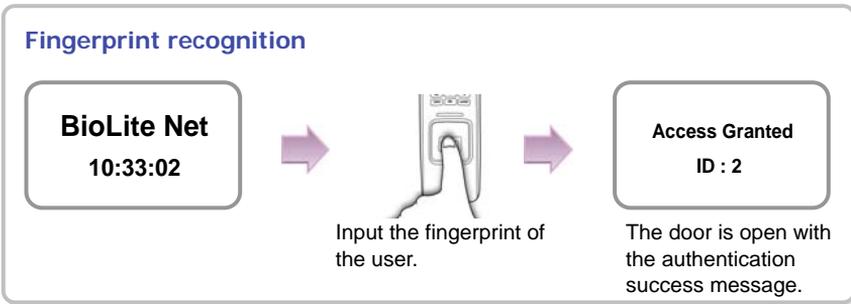


Before Use

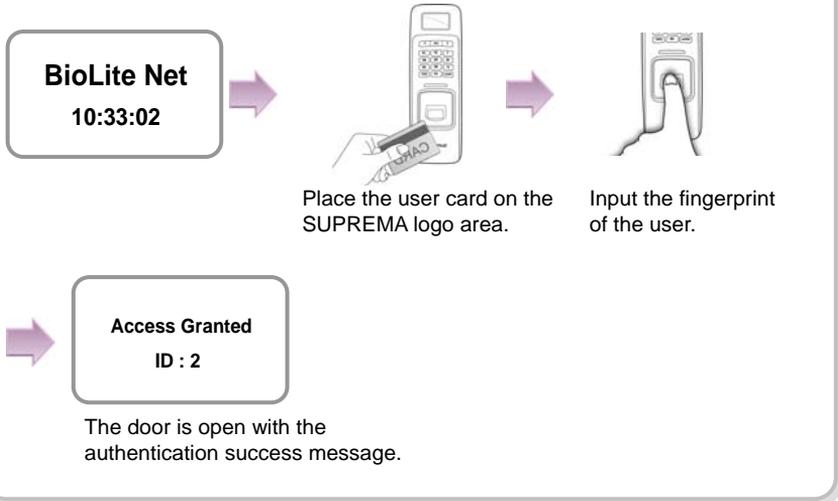
## 1.5.1 Finger Only

When the user authorization method is set to “Finger Only,” you can open the door by using the three different methods:

1. Fingerprint recognition
2. Fingerprint recognition after entering ID
3. Fingerprint recognition after identifying user card



### Fingerprint recognition after identifying user card

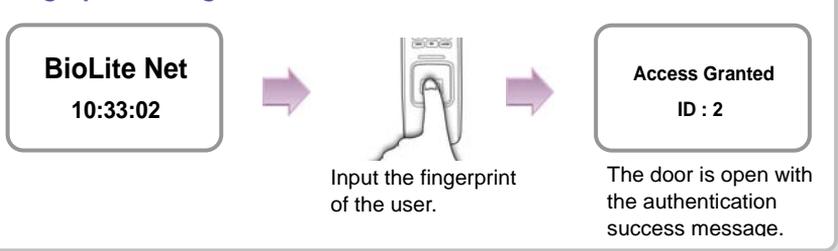


### 1.5.2 Finger or PIN

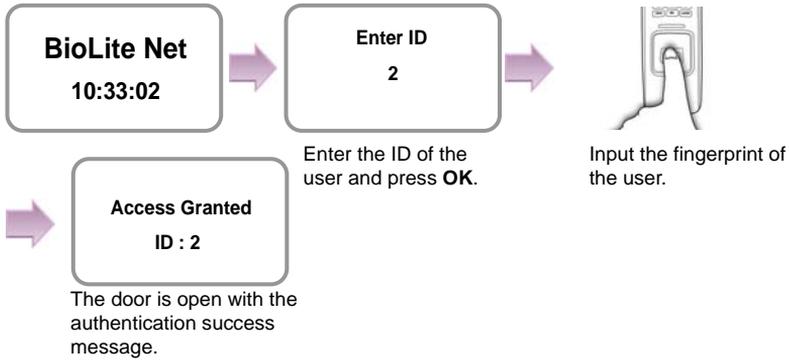
When the user authorization method is set to “Finger or PIN,” you can open the door by using the five different methods:

1. Fingerprint recognition
2. Fingerprint recognition after entering ID
3. Password entry after entering ID
4. Fingerprint recognition after identifying the user card
5. PIN entry after identifying the user card

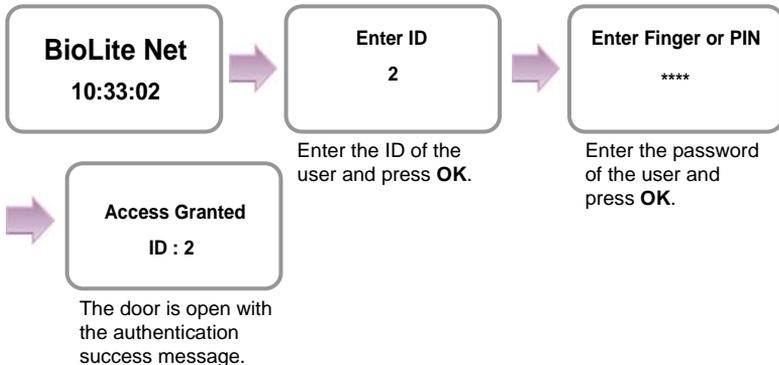
### Fingerprint recognition



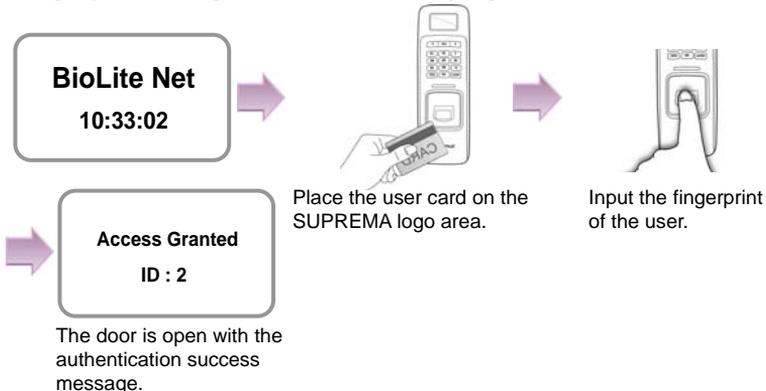
### Fingerprint recognition after entering ID



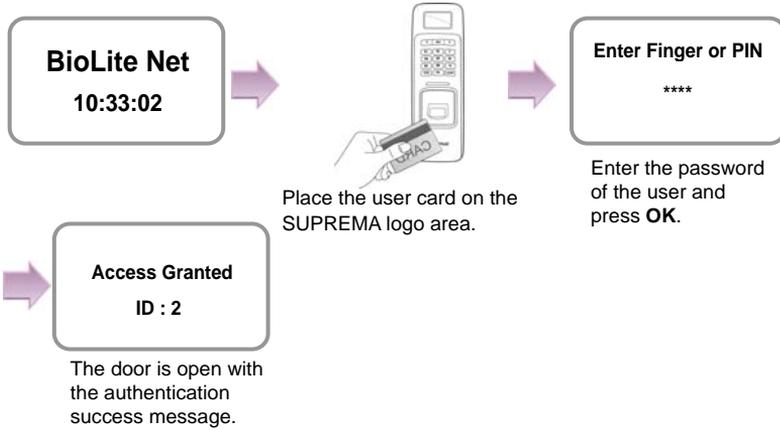
### PIN entry after entering ID



### Fingerprint recognition after identifying user card



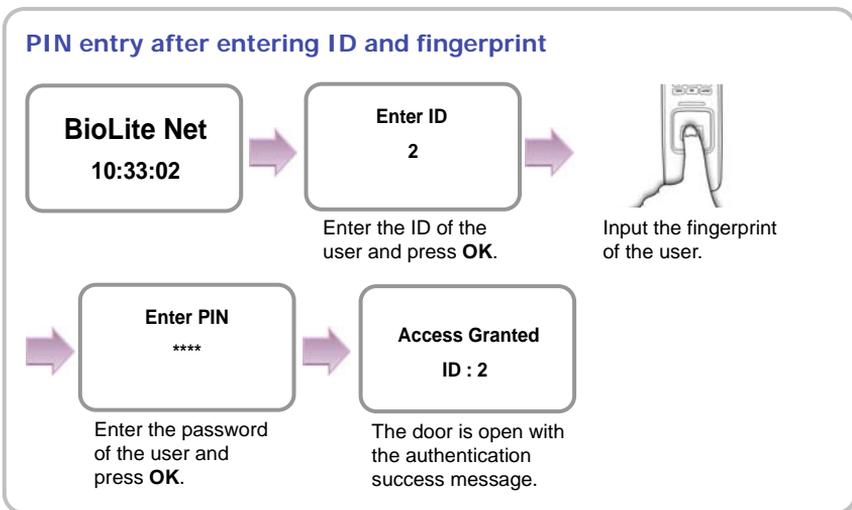
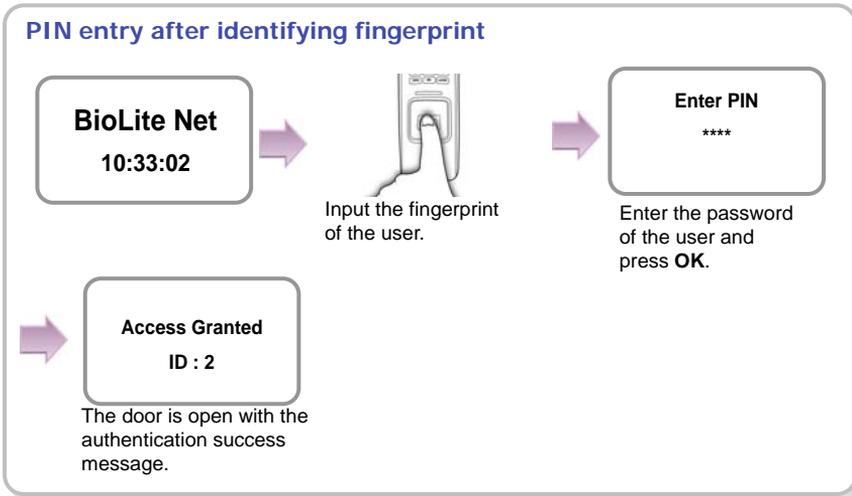
## PIN entry after identifying the user card

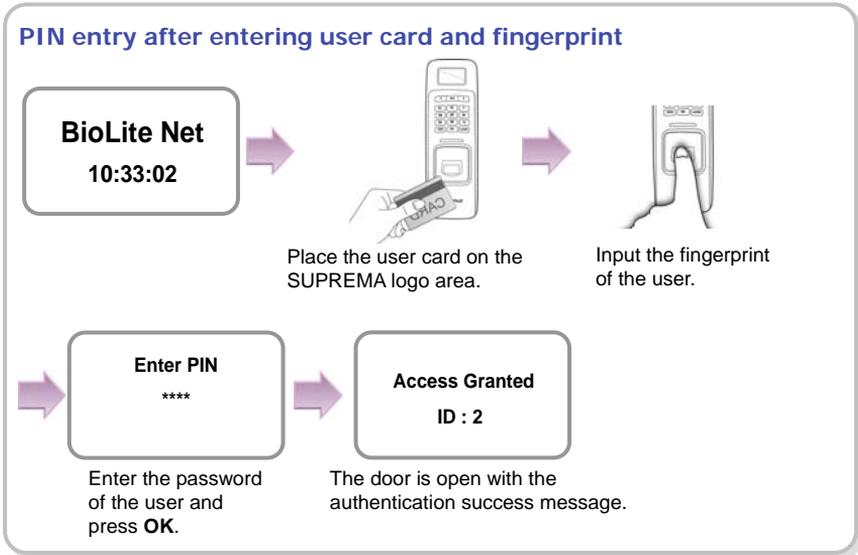


### 1.5.3 Finger and PIN

When the user authorization method is set to “Finger and PIN,” you can open the door by using the three different methods:

1. PIN entry after identifying fingerprint
2. PIN entry after entering ID and fingerprint
3. PIN entry after entering user card and fingerprint

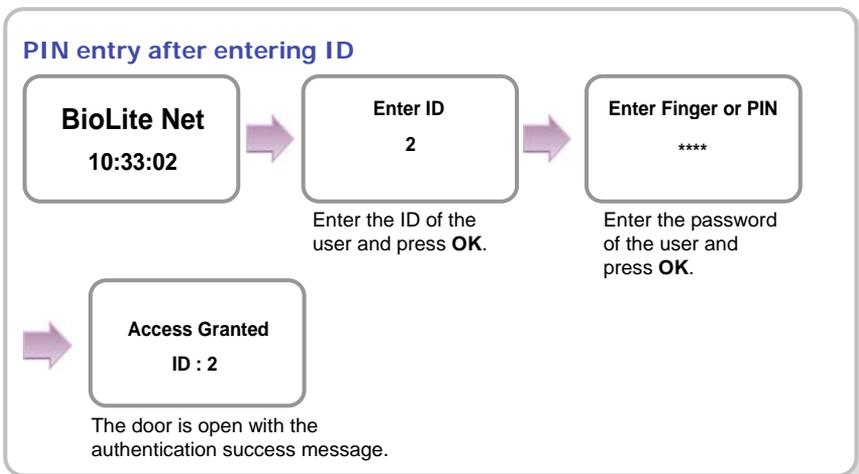


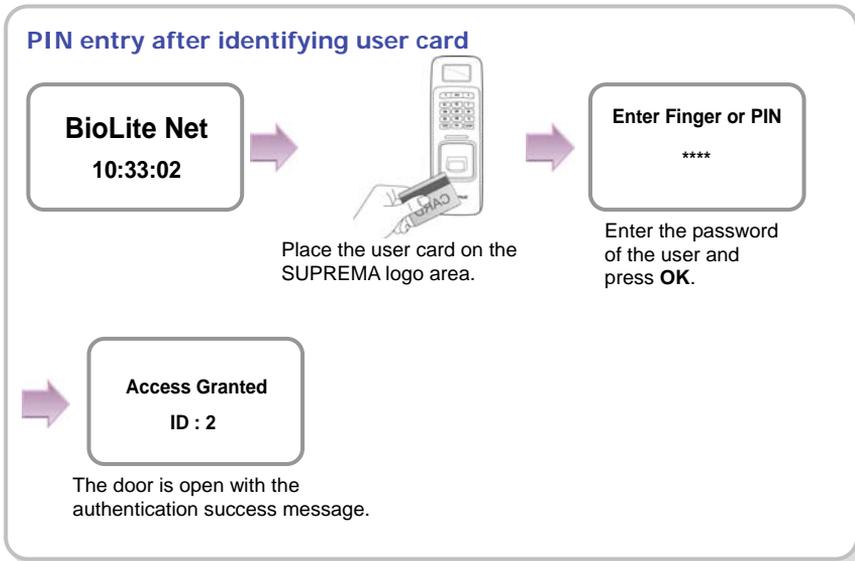


#### 1.5.4 PIN Only

When the user authorization method is set to “PIN Only,” you can open the door by using the two different methods:

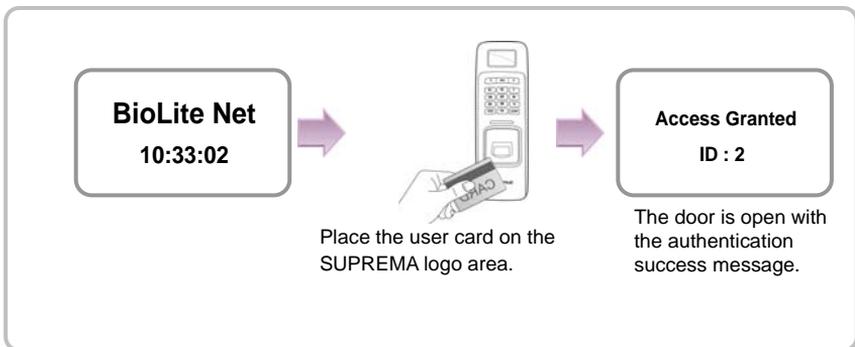
1. PIN entry after entering ID
2. PIN entry after identifying user card





### 1.5.5 Card Only

When the user authorization method is set to “Card Only,” you can open the door by following the instructions below:



Note

For “Card Only,” register the card user on the dedicated PC software first.

## 2. User Management

The user management and other environment settings can be updated after authorizing the registered administrator (see 1.4.1 “Registering the initial administrator”).

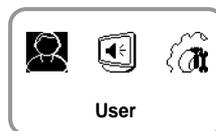
### 2.1 Enrolling a user

#### 2.1.1 Registration on the terminal

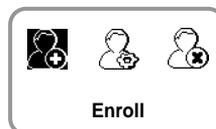
---

The information of a new user can be saved on the terminal.

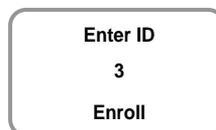
1. Use ◀/▶ buttons to select the **User**  icon and press **OK**.



2. Use ◀/▶ buttons to select **Enroll**  icon and press **OK**.

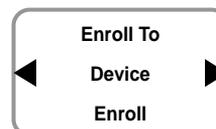


3. The ID that can be used appears. Use it or enter another ID and press **OK**.  
(1–8 digit number)



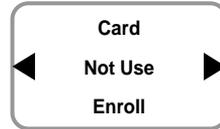
ID is used to edit or delete the user data so please keep it carefully.

4. Use ◀/▶ buttons to select **Device** on the **Enroll To** and press **OK**.  
※ **You can save the user information (including finger print) on your terminal or card.**



5. Use ◀/▶ buttons to select a card ID entry type and press **OK**.

※**Not Use/Read Card/Manual Input/User ID**



※**Card ID: Not Use/Read Card/Manual Input/User ID**

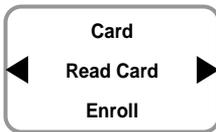
- **Not Use:** Only the finger print data is saved.
- **Read Card:** The card ID must be identified by touching the card on the terminal.
- **Manual Input:** The card ID (maximum 10 digits) must be directly entered.
- **User ID:** The selected User ID is used as Card ID (Card ID=User ID)

BioLite Net



User Mgmt

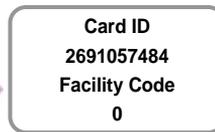
### In case of Read Card



Use ◀/▶ buttons to select **Read Card** and press **OK**.

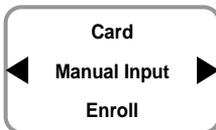


Place the user card on the SUPREMA logo area.

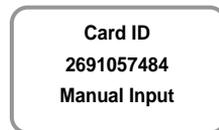


When identified, enter the **Facility Code**.

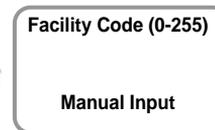
### In case of Manual Input



Use ◀/▶ buttons to select **Manual Input** and press **OK**.



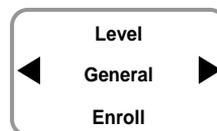
Directly enter the card ID through the keypad.



Enter the **Facility Code**

6. Use ◀/▶ buttons to select Level and press **OK**.  
(Level: General /Administrator)

※The user enrollment and environment configuration are enabled only in Administrator level.



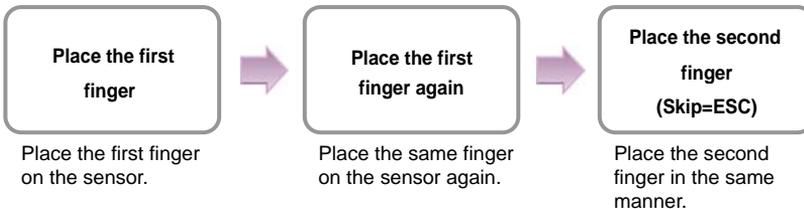
7. Enter the finger or PIN depending on the **operation mode**.  
(Password: 4–8 digit number, Fingerprint: 1<sup>st</sup> finger or 1<sup>st</sup> + 2<sup>nd</sup> fingers)



Note

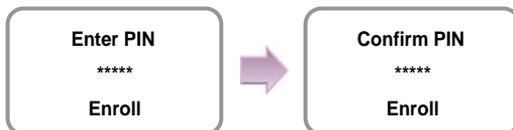
Enter the required information after selecting **Device > Authorization > Operation Mode > Auth Mode**.

### Finger Only/Finger or PIN/Finger and PIN



- ※ In order to skip the second fingerprint enrollment after enrolling the first fingerprint, press **ESC**.
- ※ The user can enroll one or two fingerprints for passing the door.

### PIN Only/ Finger and PIN



- ※ For password, it is recommended to enter 4 to 8 digit number not to be easily exposed.

8. When the user enrollment is successfully done, the completion message window appears.

- ※ User can be enrolled up to maximum 5000.

**Completed**

## 2.1.2 Registration on the card

The information of a new user can be saved on a card.

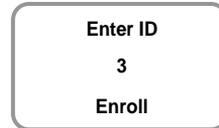
1. Use ◀/▶ buttons to select the **User**  icon and press **OK**.



2. Use ◀/▶ buttons to select **Enroll**  icon and press **OK**.

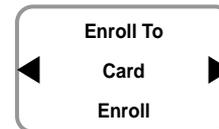


3. The ID that can be used appears. Use it or enter another ID and press **OK**.  
(1–8 digit number)



ID is used to edit or delete the user data so please keep it carefully.

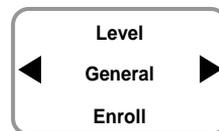
4. Use ◀/▶ buttons to select **Card** on the **Enroll To** and press **OK**.  
※ **You can save the user information (including finger print) on your terminal or card.**



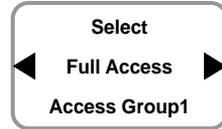
Only a rewritable card such as Mifare card can save the user information.

5. Use ◀/▶ buttons to select Level and press **OK**.  
(Level: General /Administrator)

※ The user enrollment and environment configuration are enabled only in Administrator level.

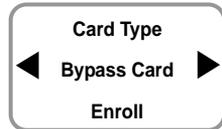


6. Use ◀/▶ buttons to select Access Group and press **OK**.



7. Use ◀/▶ button to select **Card Type** and press **OK**.

※**Bypass Card/Use Template**

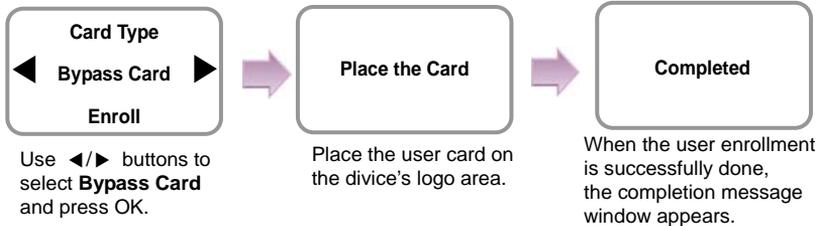


Note

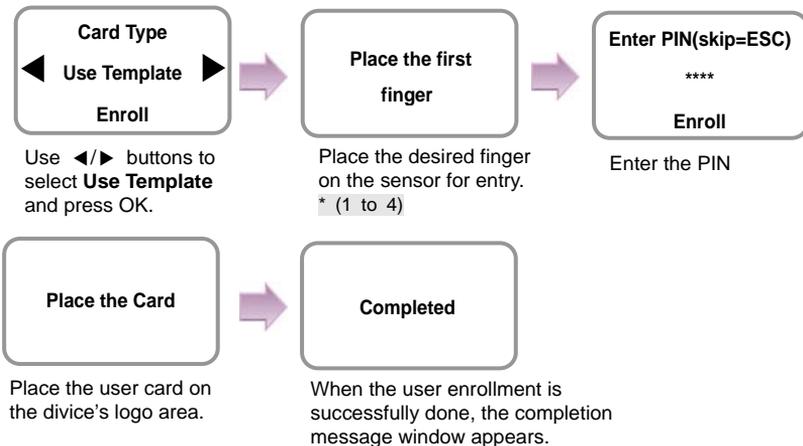
※**Card: Bypass Card/Use Template**

- **Bypass Card**: User can be authorized using a card only. The user information is saved by touching the card.
- **Use Template**: User can be authorized by touching the card and then fingerprint.

### In case of Bypass Card



### In case of Use Template



※ In case of Mifare card, the 1K card can save up to 2 fingerprint data but the 4K card up to 4. The card layout information can be set using the PC software.

## 2.2 Editing a user data

You can modify the data of the previously enrolled user.

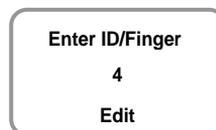
1. Use ◀/▶ buttons to select the **User** (👤) icon and press **OK**.



2. Use ◀/▶ buttons to select the **Edit** (👤✎) icon and press **OK**.



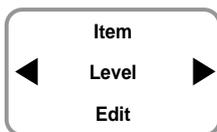
3. Enter the ID or fingerprint of the desired user and press **OK**.



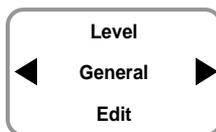
4. Use ◀/▶ buttons to select the desired item and press **OK**.

※ select any of Level/Operation Mode/Security Level/Finger/PIN/Access Group(1~4)

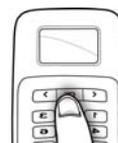
### Changing the user level



Use ◀/▶ buttons to select **Level** and press **OK**.



Use ◀/▶ buttons to select **General** or **Administrator**.

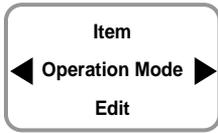


Press **OK**.

※ The settings for user, screen/sound, device, and such can be configured only by the administrator level.



## Changing the authorization method



Use ◀/▶ buttons to select **Operation Mode** and press **OK**.



Use ◀/▶ buttons to select an desired operation mode and press **OK**.



Press **OK**.



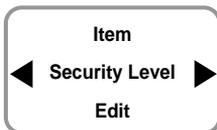
Note

This authorization method setting for each user has higher priority than the terminal setting that has been defined in **Device > Authorization > Operation Mode > Auth Mode**. Note that this function is applied to the case when the user enters ID or card and when **Use** is set in **Device > Authorization > Operation Mode > Private Auth**

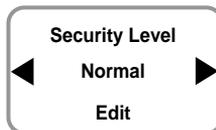
※ **Authorization methods:** \*Finger Only/PIN Only/Finger or PIN  
/ Finger and PIN/Card Only/Per Device

- **Finger Only:** Only fingerprint is used.
- **PIN Only:** Only PIN is used.
- **Finger or PIN:** Fingerprint or PIN is used.
- **Finger and PIN:** Both fingerprint and PIN are used.
- **Card Only:** Only user card is used.
- **Per Device:** The mode set in "Device > Authorization > Operation Mode > Auth Mode" is used.

## Changing the security level of the user



Use ◀/▶ buttons to select **Security Level** and press **OK**.



Use ◀/▶ buttons to select a security level.

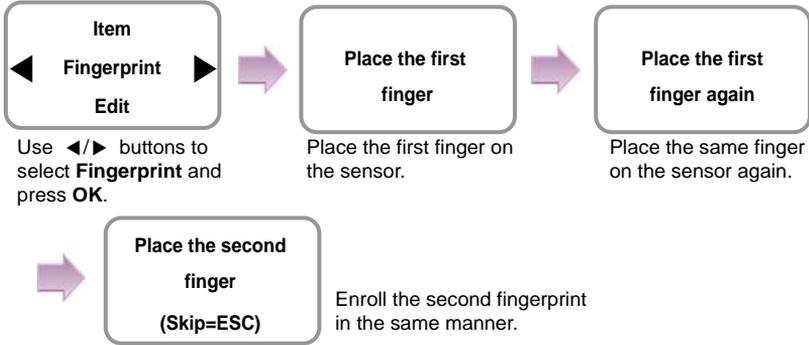


Press **OK**.

※ **Security Level:** \*Per Device/Lower/Low/Normal/High/Higher

- **Per Device:** The security level in "Device>Authorization>Fingerprint>" on page 39 is applied.
- The higher the security level, the more sensitive the fingerprint recognition. But the authorization failure rate can increase.

### Changing the fingerprint of the user



### Changing the PIN of the user



### Changing the access group



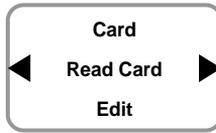
Note

Setting the access groups other than Full Access or No Access is enabled through the dedicated PC software only. Using the terminal, you cannot add or edit them but only selecting them is enabled for each user.

## Changing the card



Use ◀/▶ buttons to select **Card** and press **OK**.



Use ◀/▶ buttons to select card input type  
\* Not use/ Read Card/  
Manual Input / User ID



Press **OK**.

※ **Card**: \*Not use/Read Card/Manual Input/User ID

- **Not use**: Card is not used
- **Read Card**: User information is changed after touching a card on the terminal.
- **Manual Input**: User information is changed after entering the card ID.
- **User ID**: The corresponding user ID is changed using a card ID.

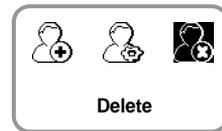
## 2.3 Deleting a user data

You can delete unnecessary user data.

1. Use ◀/▶ buttons to select the User (👤) icon and press **OK**.



2. Use ◀/▶ buttons to select the Delete (👤✖) icon and press **OK**.



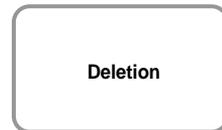
3. After entering the ID or finger to delete and press **OK**.



4. When the action is successfully made, the message Deletion appears.

※The deleted user cannot be recovered.

If necessary, enroll it again.



Note

- If all the users including the administrator are deleted, you must register the initial administrator again (see 1.4.1).
- When an administrator is deleted by mistake except normal users, the initial administrator registration step does not require registering normal users.



# 3. Configuration for Screen and Sound

## 3.1 Date, Time

You need to set the current system date and time.

After setting the date and time, the log data can store correct information.

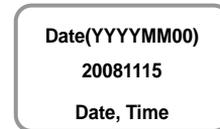
1. Use ◀/▶ buttons to select the **Screen, Sound**  icon and press **OK**.



2. Use ◀/▶ buttons to select the **Date, Time**  icon and press **OK**.



3. Enter the current date by following the suggested format and press **OK**.  
**For example**, in case of November 15 in 2008, enter "20081115" and press **OK**.



4. Enter the current time by following the suggested format and press **OK**.  
**For example**, in case of 10:20 55 AM, enter "102055" and press **OK**.



## 3.2 Backlight

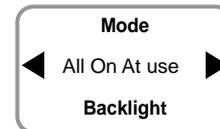
1. Use ◀/▶ buttons to select the **Screen, Sound** (👤📺🔊) icon and press **OK**.



2. Use ◀/▶ buttons to select **Backlight** (💡) icon and press **OK**.



3. Use ◀/▶ buttons to select a backlight operation status and press **OK**.



BioLite Net

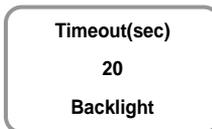


Screen & Sound

### All On At Use (FW V1.21 or later)



Use ◀/▶ buttons to select the **Always On At Use** and press **OK**.



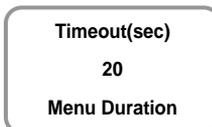
Enter the backlight-on time (second) on the menu window.

※ When no input is made on the menu window, it sets the time to automatically turn off the LCD/Keypad backlight.

### Always On



Use ◀/▶ buttons to select the **Always On** and press **OK**.



When no operation is made, it sets the time (second) to switch the screen.

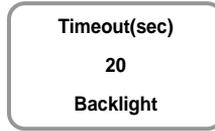
※ When no input is made, it sets the time to exit from the menu.

## On at Use

※When no input is made on the menu window, it sets the time to automatically turn off the LCD backlight.



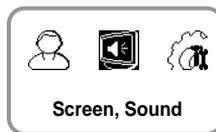
Use ◀/▶ buttons to select the **On at Use** and press **OK**.



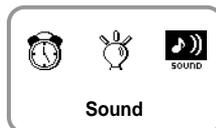
Enter the backlight-on time (second) on the menu window.

### 3.3 Sound

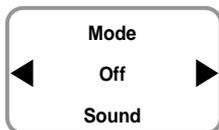
1. Use ◀/▶ buttons to select the **Screen, Sound**  icon and press **OK**.



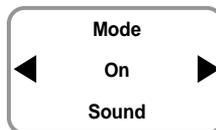
2. Use ◀/▶ buttons to select **Sound**  icon and press **OK**.



3. Use ◀/▶ buttons to select the sound operation status and press **OK**.



Or



BioLite Net



Screen & Sound

# 4. Device Configuration

## 4.1 Authorization

1. Use ◀/▶ buttons to select the **Device** (👤) icon and press **OK**.



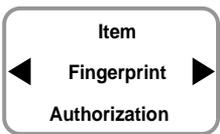
2. Use ◀/▶ buttons to select the **Authorization** (🔑) icon and press **OK**.



3. Use ◀/▶ buttons to select any of Fingerprint, and Operation Mode and press **OK**.



### In case of Fingerprint



Use ◀/▶ buttons to select **Fingerprint** and press **OK**.



Use ◀/▶ buttons to select **Security Level** and press **OK**.



Use ◀/▶ buttons to select **Security Level** and press **OK**.  
\* Normal /Secure/More Secure

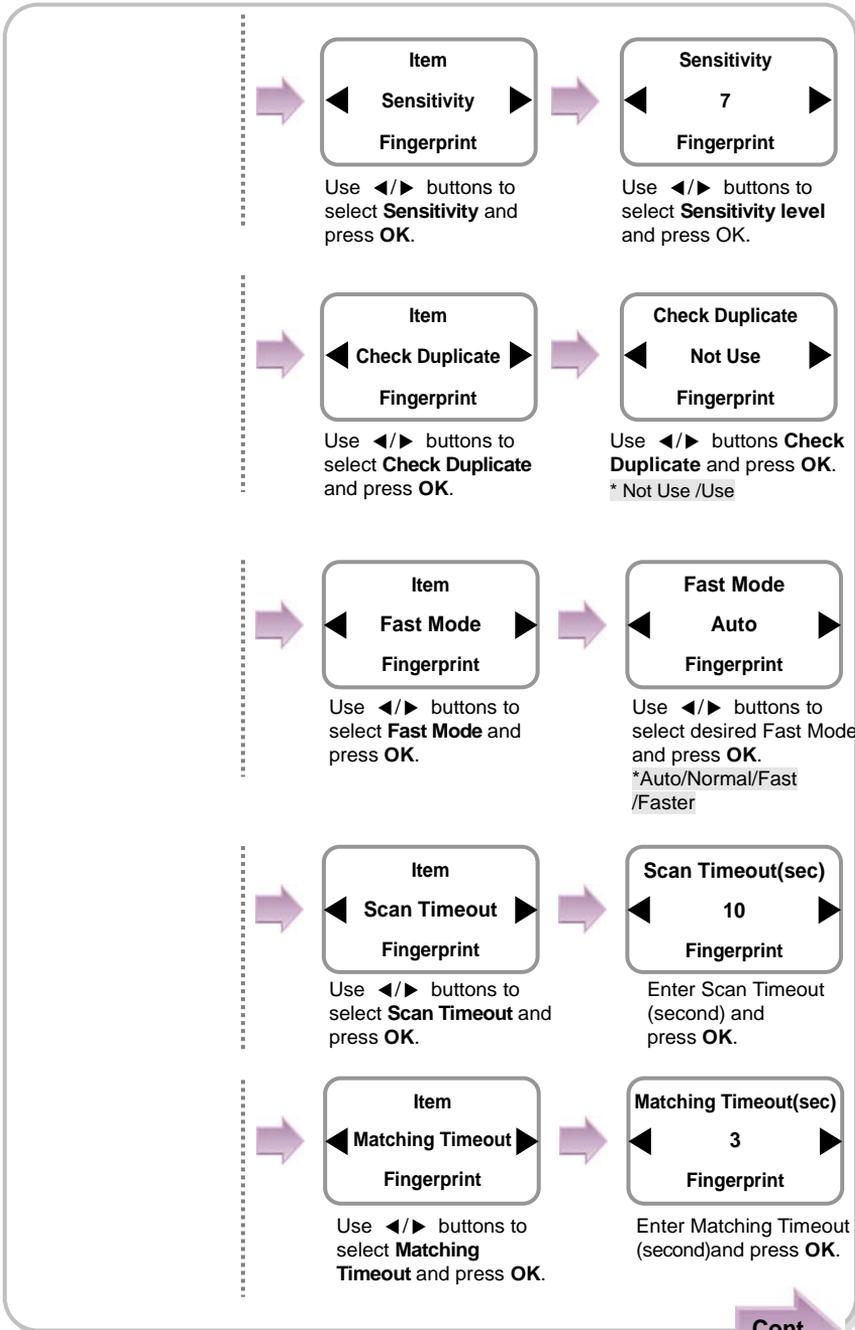


Use ◀/▶ buttons to select **Image Quality** and press **OK**.



Use ◀/▶ buttons to select **Image Quality** and press **OK**.  
\*Normal/High/Low

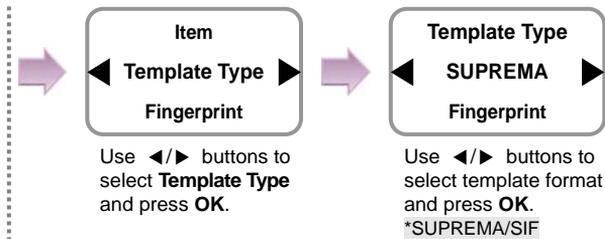




Cont.

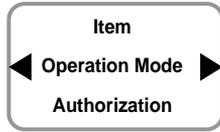


Device

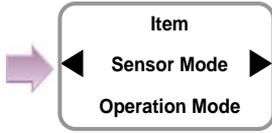


- ※ **Security Level:** The higher the security level, the more sensitive the fingerprint recognition. But the authorization failure rate can increase.
- ※ **Image Quality:** It is the image quality level used when entering the fingerprint data. In case of Low, the fingerprint can be easily input but the correct authorization is not guaranteed.
- ※ **Sensitivity:** The higher the value, the more sensitive the sensor.
- ※ **Check Duplicate:** When enrolling a user, it determines whether or not to check the fingerprint data is already enrolled.
- ※ **Fast Mode:** You can set the fingerprint recognition speed. If it is set to Fast, the recognition accuracy may decrease.
- ※ **Scan Timeout:** You can set the terminal standby time for entering fingerprint. If entry is not made within the specified time, the message, "Entry time is over" appears.
- ※ **Matching Timeout:** You can set the maximum authorization time after entering fingerprint. If this time limit expires, matching stops and the authorization fails.
- ※ **Template Type:** Format used in the terminal when identifying fingerprints (SUPREMA/SIF)  
- SUPREMA: SUPREMA's own template format, SIF: ISO/IEC compatible template format  
(To change the template format, there must be no fingerprint data stored on the terminal.)

## In case of Operation Mode



Use ◀/▶ buttons to select **Operation Mode** and press **OK**.



Use ◀/▶ buttons to select **Sensor Mode** and press **OK**.

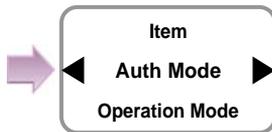


Use ◀/▶ buttons to select a sensor mode.  
\*Always On/ID Entered/OK Pressed

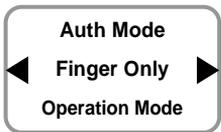


Use ◀/▶ buttons to select the applicable time zone and press **OK**.

- ※ **Sensor Mode:** \*Always On/ID Entered/OK Pressed
- **Always On:** The sensor always waits for a fingerprint input.
- **ID Entered/OK Pressed:** If you enter ID or press **OK**, you can enter the time zone for using the sensor.
- ※ **Applied time:** Use the dedicated PC software for setting the time zone except All Time and Not Use. With the terminal, you cannot add and edit it but only selection is not possible.



Use ◀/▶ buttons to select **Auth Mode** and press **OK**.



Use ◀/▶ buttons to select the authorization method press **OK**.



Use ◀/▶ buttons to select the applicable time zone and press **OK**.



Use ◀/▶ buttons to set whether or not to use the double mode and press **OK**.

※**Auth Mode:** \*Finger Only/PIN Only/Finger or PIN / Finger and PIN /Card Only  
If no authorization setting exists for each user, the user authorization method that has been set on the terminal is applied.

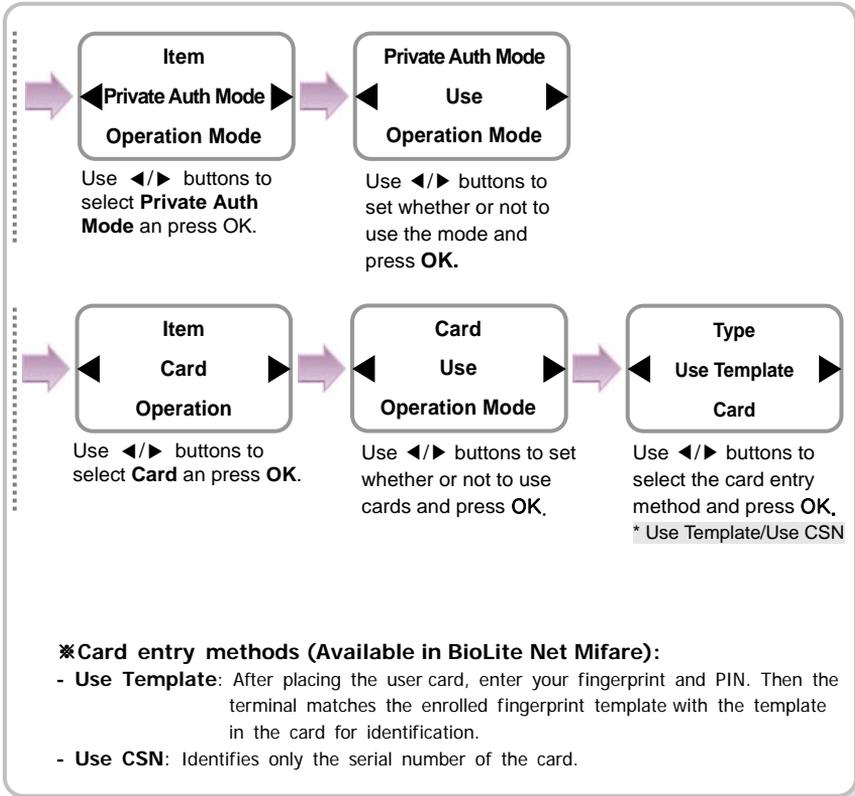
※**Double Mode:** When consequent two users are authorized successfully, entrance and exit are allowed.

Cont.

BioLite Net

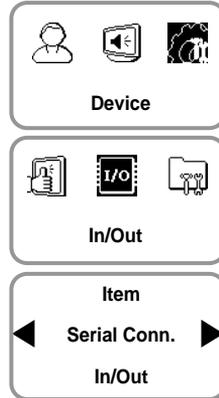


Device

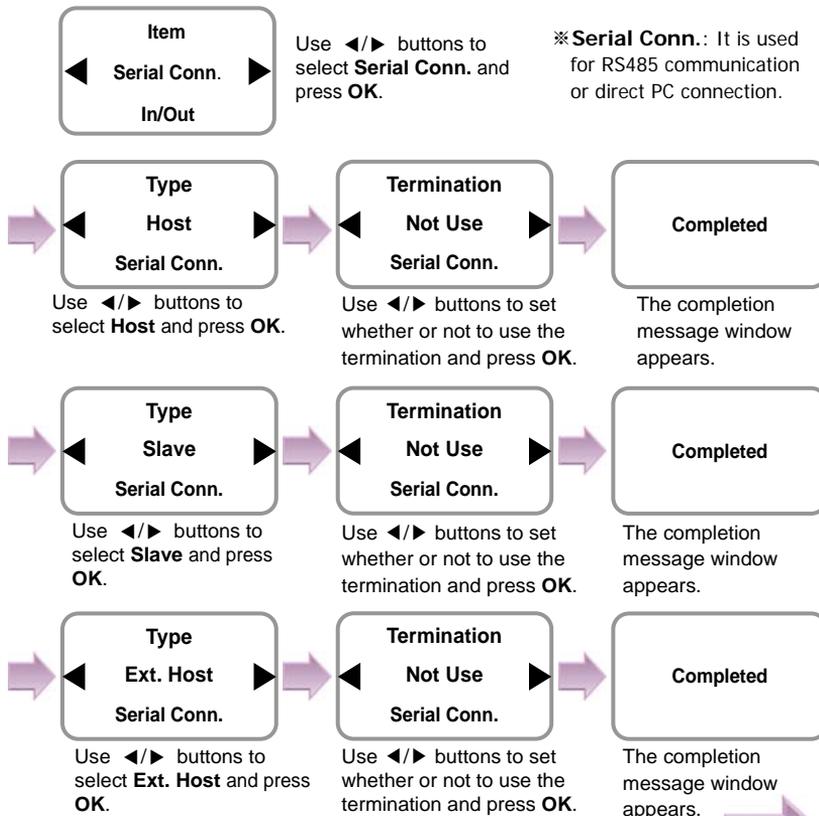


## 4.2 In/Out

1. Use ◀/▶ buttons to select the **Device**  icon and press **OK**.
2. Use ◀/▶ buttons to select **In/Out**  icon and press **OK**.
3. Use ◀/▶ buttons to select any of Serial Conn., Tamper On, Door Wiegand, and TCP/IP and press **OK**.

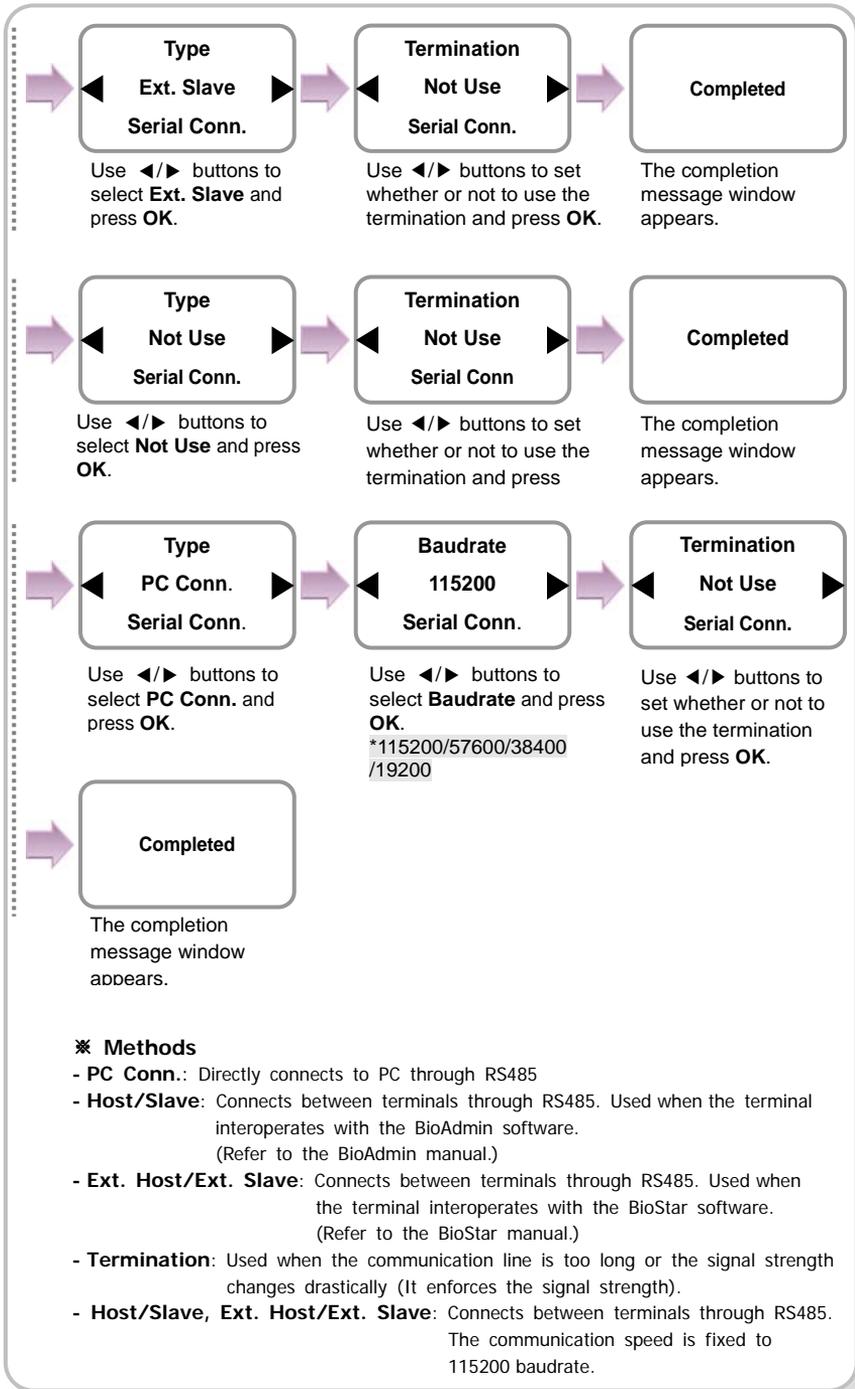


### In case of Serial Conn. (selection of connection method)



Cont. →





## In case of Tamper On



Use ◀/▶ buttons to select **Tamper On** and press **OK**.



Use ◀/▶ buttons to select a tamper method.



Press **OK**.

※ **Tamper**: \*Ignore/Locked

- **Locked**: When the device is forcibly removed, the Device is locked.  
(To release the lock, the administrator must perform authorization.)

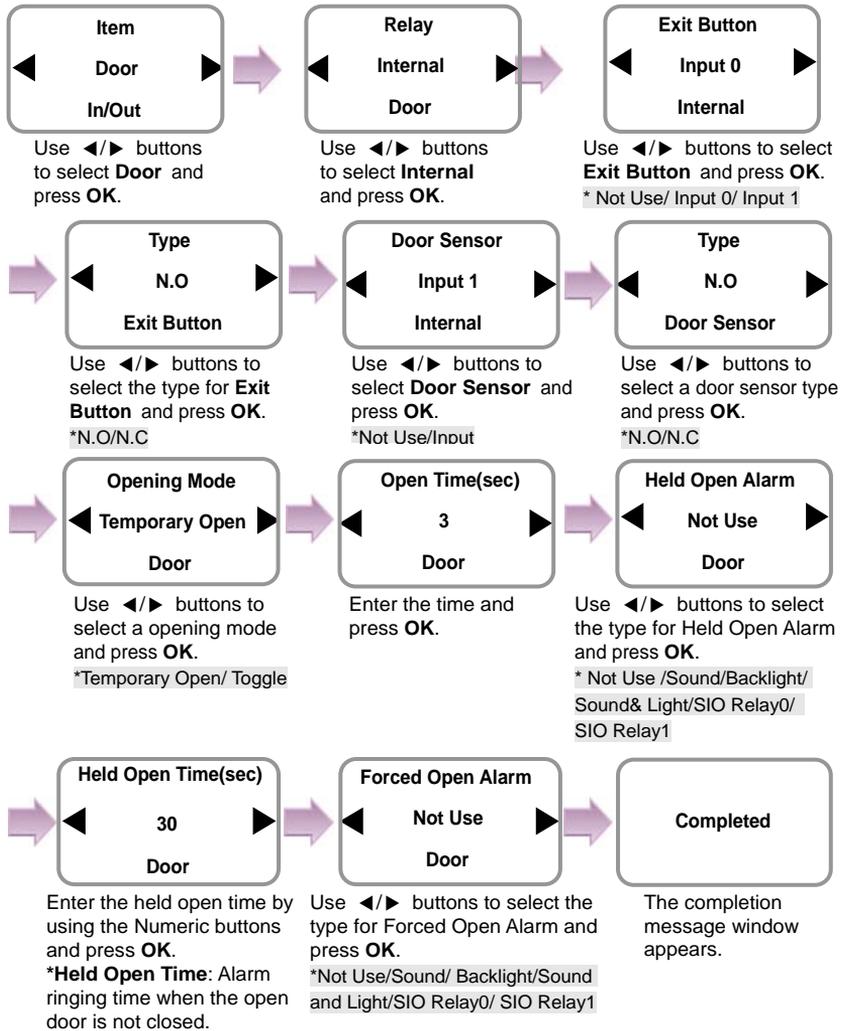
BioLite Net



Device

## In case of Door (When using the internal relay)

※ It is used only when the stand-alone BioLite Net is installed without interoperating with the dedicated PC software.



Note

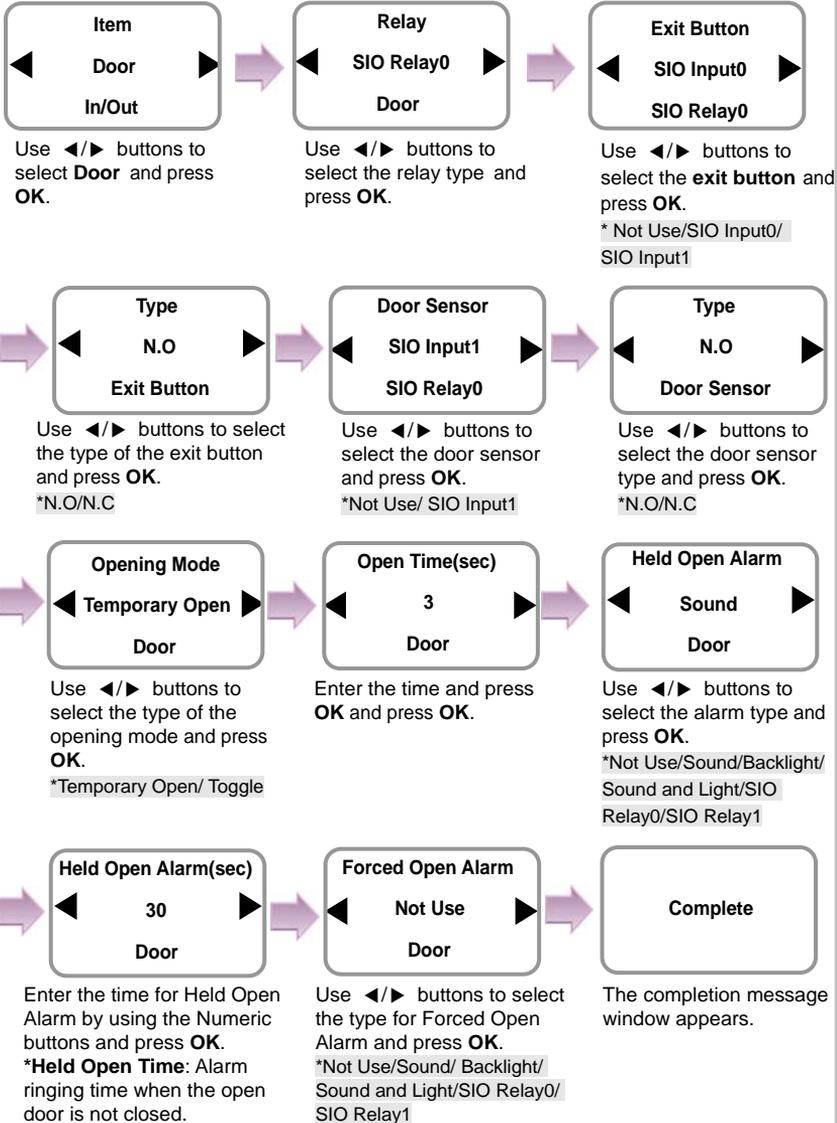
When you exit from the menu before completing the relay setup, the configuration is not stored so please finish configuration until the message "Complete" appears.

### ※ Opening Mode

- **Temporary Open**: When the door is open, it is automatically closed after a specific time.
- **Toggle**: The door is opened after the first authorization success and it remains unlocked until the second authorization success.

## In case of Door (When using the SIO relay)

※ It is used only when the stand-alone BioLite Net is installed without interoperating with the dedicated PC software.



## In case of Wiegand

※Standard 26Bit Format is used for Wiegand In/Out format. The setting can be changed using the dedicated PC software.



Use ◀/▶ buttons to select **Wiegand** and press **OK**.



Use ◀/▶ buttons to select **Wiegand** and press **OK**.

\*Card ID In/ Card ID Out/User ID In/ User ID Out/Not Use

※**Wiegand types:** \*Card ID In/Card ID Out/User ID In/User ID Out

- **Card ID In:** The card ID is entered.
- **Card ID Out:** The card ID is output.
- **User ID In:** The user ID is entered.
- **User ID Out:** The user ID is output.



Note

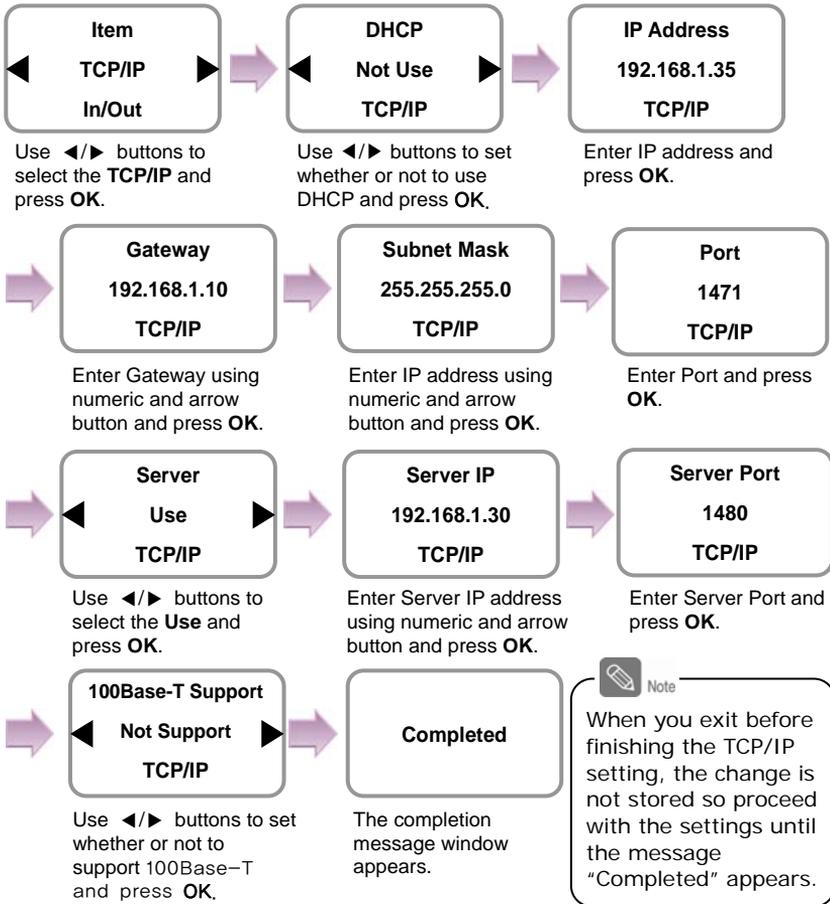
**When the user whose user ID is 2 registers the card ID (1234567),**

- **Card ID In:** When "1234567" is entered through the Wiegand port, the user is successfully authorized.
- **Card ID Out:** When the user card is read through the terminal, the card ID "1234567" is output through the Wiegand port.
- **User ID In:** When "2" is entered through the Wiegand port, the user is successfully authorized.
- **User ID Out:** When the user is successfully authorized, the user ID "2" is output through the Weigand port.

※For Wiegand connection, see "6.4.7 Connection Wiegand."

## In case of TCP/IP

※It directly connects to the server for the dedicated PC software without using DHCP.



- ※ **IP Address/Gateway/Subnet Mask Setup:** If DHCP is used, the values for IP address, gateway, and subnet mask are automatically assigned. Otherwise, set DHCP to **Not Use** and enter the corresponding values.  
(When the right arrow is pressed, "." is entered while the left arrow deletes characters one by one.)
- ※ **Server:** To directly connect the server of the dedicated PC software that enables monitoring and setting the terminal, use Server for its setup and enter the values for IP address and port number. **(Refer to the dedicated PC software manual.)**
- ※ **TCP/IP Port, Server Port:** Should be the same values defined in the dedicated PC software. It is recommended to set the TCP/IP port to "1471" and Server to "1480."  
(When the port number is modified as you want, TCP/IP communication may not be active.)

BioLite Net



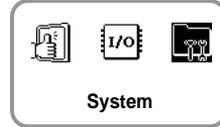
Device

## 4.3 System

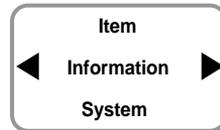
1. Use ◀/▶ buttons to select the **Device** (👤) icon and press **OK**.



2. Use ◀/▶ buttons to select the **System** (🔧) icon and press **OK**.



3. Use ◀/▶ buttons to select any of Information, Factory Default, Delete All Log, Delete User DB, and Language and press **OK**.



### In case of Information



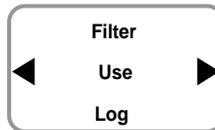
Use ◀/▶ buttons to select **Log** and press **OK**.



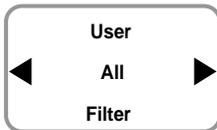
Use ◀/▶ buttons to select **Not Use** and press **OK**.



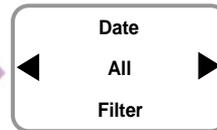
The entire logs appear.  
(Use ◀/▶ buttons to see the previous/next logs.)



Use ◀/▶ buttons to select **Use** and press **OK**.



Use ◀/▶ buttons to select any of All and Select ID and press **OK**.

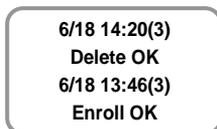


Use ◀/▶ buttons to select any of All and Specify Date and press **OK**.



Use ◀/▶ buttons to select the event type and press **OK**.

\*All/Success/Failure/In/Out/  
System



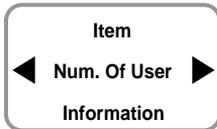
The log filtering result appears on the screen.  
(Use ◀/▶ buttons to see the previous/next logs.)

#### ※ Filter

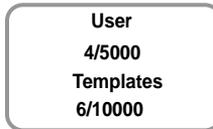
- Not Use: Displays all.
- Use: Only the specified log is displayed.  
(ID/Date/Event Type)

※ When the date is specified, the logs occurred earlier than the specified date appear.

## In case of Information – Continued



Use ◀/▶ buttons to select **Num. Of User** and press **OK**.



The number of current users and the number of fingerprints enrolled appear.



Use ◀/▶ buttons to select **Firmware Ver.** and press **OK**.



The version of the firmware appears.

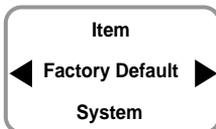


Use ◀/▶ buttons to select **Hardware Ver.** and press **OK**.

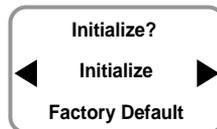


The version of the hardware appears.

## In case of Factory Default



Use ◀/▶ buttons to select **Factory Default** and press **OK**.



Use ◀/▶ buttons to determine whether or not to initialize it.  
\*Cancel/ Initialize

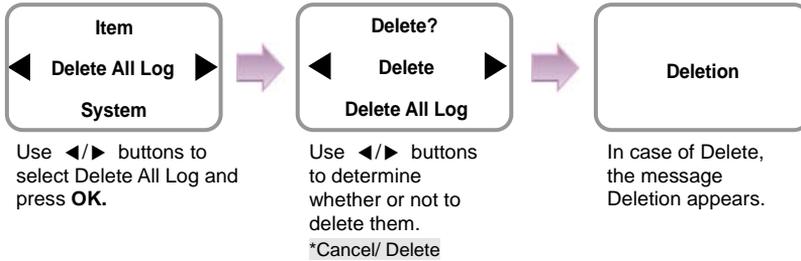


In case of Initialize, the message Initialized appears.

※ In case of Initialize, the settings are deleted but the log data and user DB are not deleted.

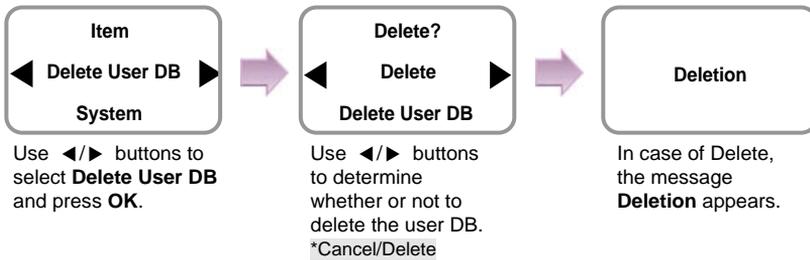


### In case of Delete All Log



※ In this case, all users' in/out data are deleted and they cannot be recovered.

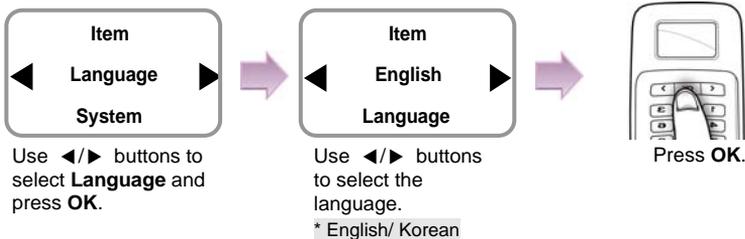
### In case of Delete User DB



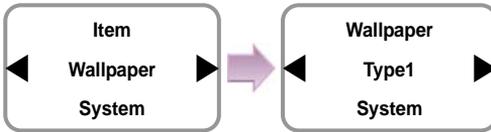
※ In this case, the users' DB is completely deleted so you must immediately register the initial administrator (see 1.4.1).

※ When the user DB is deleted, it cannot be recovered.

### In case of Language



### In case of Wallpaper



Use ◀/▶ buttons to select **Wallpaper** and press **OK**.

Use ◀/▶ buttons to select the type and press **OK**.

\*Type1/Type2

#### ※Types

- **Type1**: Only the time appears on the wallpaper screen.
- **Type2**: The number of users and TCP/IP connection status appears on the wallpaper screen.

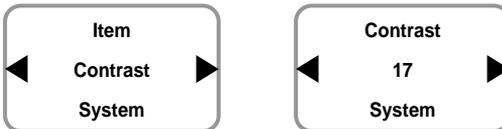
**In case of (8/5000) U** - Eight people are registered among 5000 (number of people that can be registered) and it is unlinked.



#### Characters on the Type2 wallpaper

- **U**: Unlinked (LAN is not connected.)
- **D**: Disconnected (LAN is connected but TCP/IP communication is not active.)
- **C**: Connected (LAN is connected and TCP/IP communication is active.)

### In case of Contrast



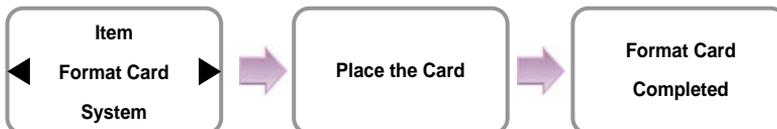
Use ◀/▶ buttons to select **Contrast** and press **OK**.

Use ◀/▶ buttons to select contrast level.

#### ※Contrast

Contrast value on the screen (Range: 10 to 30)

### In case of Format Card



Use ◀/▶ buttons to select **Format Card** and press **OK**.

Place the user card on the SUPREMA logo area.

After formatting a card, The format completion message window appears.

- ※ After formatting a card, the data on a rewritable card such as Mifare card is removed. (The card format can be set using the PC software.)



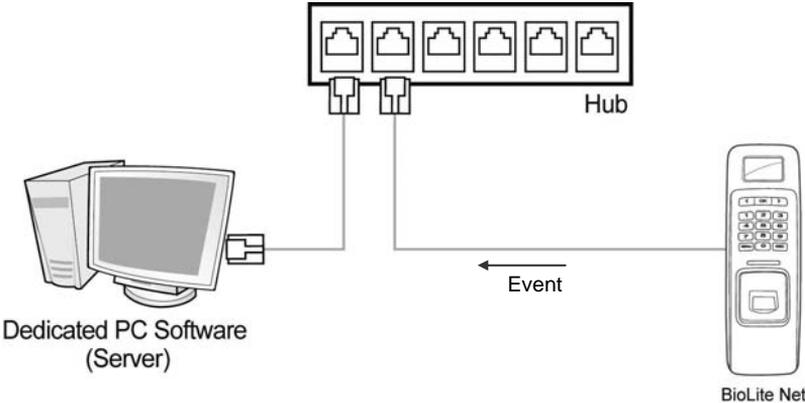
# 5. Attendance Management

## 5.1 Operating environment

When an event (attendance, leaving, return, and outside duty) is received from the terminal, it is reported to the server of the dedicated PC software. You can create a report from the events stored in the server.

With the dedicated PC software, you can also define new event other than the above-mentioned basic events and apply it to the report.

In case of basic events provided, each event causes the door to open. You can configure the settings according to the environment through the dedicated PC software.



## 5.2 Setup for attendance management

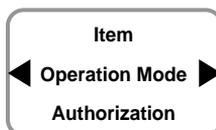
1. Use ◀/▶ buttons to select the **Device**  icon and press **OK**.



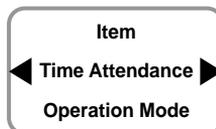
2. Use ◀/▶ buttons to select the **Authorization**  icon and press **OK**.



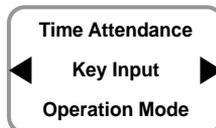
3. Use ◀/▶ buttons to select the **Operation Mode** and press **OK**.



4. Use ◀/▶ buttons to select the **Time Attendance** and press **OK**.



5. Use ◀/▶ buttons to select the Operation Mode of Time Attendance and press **OK**.



※**Operation modes:** \*Key Input/Fixed/Manual/Auto/Not Use

- **Key Input:** In usual time, the function is inactive. When ◀/▶ buttons are pressed, you can select the attendance status. When a user authorization is successful, the selected attendance log is recorded.
- **Fixed:** A specific attendance status continues. When a user authorization is successful, the corresponding log is recorded.
- **Manual:** The active attendance status appears on the screen and it can be changed using ◀/▶ buttons. Once it is changed, the status continues until another selection is made. Every authorization success makes the log recorded.
- **Auto:** The active attendance status appears on the screen. Fore each time zone, the active attendance statuses are fixed.
- **Not Use:** The function is not available.

BioLite Net

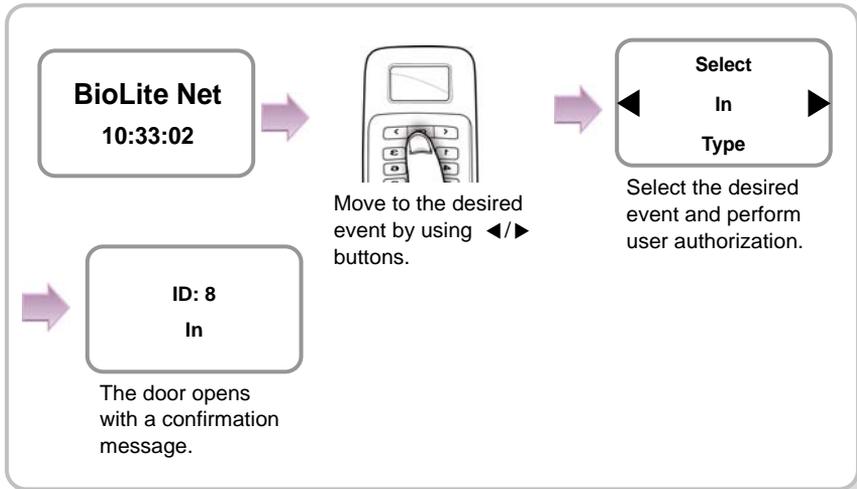


Device

## 5.3 Operation modes

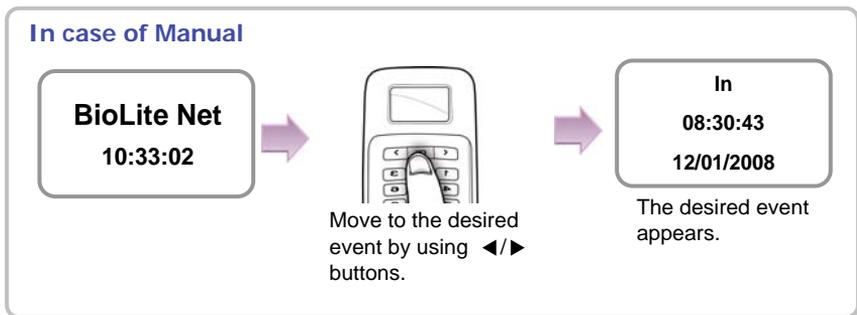
### 5.3.1 Key Input

When the operation mode is set to “Key Input,” this mode is used.



### 5.3.2 Manual

When the operation mode is set to “Manual”, this mode is used.



### In case of Manual



※ **Manual:** It is convenient to those who need to change an event type manually everytime they enter or leave..

### 5.3.2 Auto

When the operation mode is set to “Auto,” this mode is used.

This mode can set the corresponding time zone for each attendance event through the dedicated PC software. Then the fixed event is set for the corresponding time zone.

### In case of Auto



※ **Auto:** While the event type and time zone are set through the dedicated PC software, you can totally use this mode for all the users who are entering or leaving.



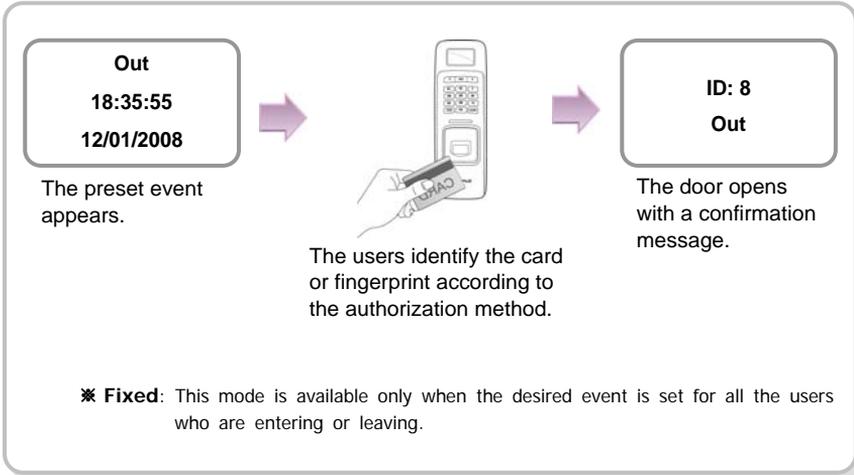
### 5.3.3 Fixed

---

When the operation mode is set to “Fixed,” this mode is used.

This mode is used after fixing the event through the dedicated PC software if required.

In this case, the setting can be changed only through the dedicated PC software and you cannot change the attendance event through the terminal.



# 6. FAQ

## 6.1 Error messages

Error Message	Description
<b>!Access Restricted</b>	The authentication trial happens except for the allowed time zone.
<b>!Cannot Change</b>	A template already exists when you want to change the template format.
<b>!Cannot Format</b>	The card is not formatted due to improper card touch.
<b>!Cannot Write</b>	The user information is not saved due to improper card touch.
<b>!Device Locked</b>	The device is locked because the case has been open.
<b>!Duplicate Card</b>	The card has been already registered.
<b>!Duplicate Finger</b>	When enrolling a user fingerprint, the fingerprint that has been input already exists in the device (when checking the duplicated case).
<b>!Duplicated Time</b>	The time zone is duplicated.
<b>!Failed</b>	The number of users exceeds 5000, so you cannot enroll more users.
<b>!Failed</b>	The user ID to delete does not exist.
<b>!ID In Use</b>	The user ID to enroll already exists.
<b>!Invalid Value</b>	An invalid value is entered.
<b>!Mode Error</b>	The authorization mode is different from the setting.
<b>!No Card</b>	You tried authorization with a unregistered card.
<b>!No Log</b>	There is no log data.
<b>!Not Administrator</b>	A normal user tries to enter the menu.
<b>!Not Authorized</b>	The fingerprint authentication for the administrator fails when entering the menu.
<b>!Not Matched</b>	The entered fingerprint or password is not matched to the enrolled one. - In case of fingerprint entry, the entered two fingerprints of the same finger are different.
<b>!Not Recognizable</b>	The fingerprint data cannot be extracted due to wrong finger input.
<b>!Time Out</b>	The fingerprint data is not entered while the sensor is active.
<b>!Unknown Finger</b>	The entered fingerprint for entering the menu or editing/deleting a user data does not exist.
<b>!Unknown ID</b>	The user ID that does not exist in the device is entered.
<b>!Wrong PIN</b>	The entered password for authentication is not matched the enrolled one.



## 6.2 Troubleshooting

Category	Trouble	Solution
Power	The power is supplied but the device does not operate.	<ul style="list-style-type: none"> <li>- When the device is disconnected from the bracket, it may not work when using the tamper switch.</li> <li>- Check the adapter or power cable.</li> </ul>
Password	The password is lost.	<ul style="list-style-type: none"> <li>- Enter the queried password after contacting the administrator in case of a normal user.</li> <li>- When the administrator password is lost, contact with the installation agency.</li> </ul>
	The locked door is not open after entering the password and pressing <b>OK</b> .	<ul style="list-style-type: none"> <li>- Check whether the correct password is input.</li> <li>- Check whether you have changed the password recently.</li> <li>- If you cannot find the password, contact the administrator.</li> </ul>
Fingerprint	The fingerprint has been enrolled but its recognition encounters an error.	<ul style="list-style-type: none"> <li>- BioLite Net has the technology of Suprema that won the first award in FVC2004 and FVC2006 because it has world number one quality in recognition.</li> <li>- For better performance in fingerprint recognition, correct registration is a must.</li> <li>- Enroll the fingerprint again after seeing "1.4 Methods for fingerprint input"</li> <li>- The recognition rate may vary due to the characteristic of each finger so enroll the fingerprint of another finger.</li> </ul>
	It was good at recognizing fingerprints but suddenly it fails in recognition.	<ul style="list-style-type: none"> <li>- Check whether the finger or the sensor is covered with sweat, moisture, or dust.</li> <li>- In case the fingerprint has any damage, the device may consider it as the one of wrong person.</li> <li>- Wipe the finger or sensor with a dry cloth and retry.</li> <li>- When the fingerprint is so dry, blow your steam of breath into it and retry.</li> </ul>
Door lock	Even if you close the door, the door is not locked.	<ul style="list-style-type: none"> <li>- The electric lock failure is most likely to happen. Check it after contacting the installation agency.</li> </ul>
Time	The time is not correct.	<ul style="list-style-type: none"> <li>- BioLite Net has an embedded battery but it can be discharged by a long time use. Accordingly the time may not be correct. Correct the time after seeing "3.1 Date, Time."</li> </ul>
TCP/IP	The terminal data is not found by the dedicated PC software.	<ul style="list-style-type: none"> <li>- Check the connection status after setting on the terminal like <b>Terminal &gt; System &gt; Wallpaper &gt; Type2</b>.</li> <li>- When U is displayed: Check the LAN connection status.</li> <li>- When D is displayed: Check the IP address. If you set like <b>Terminal &gt; In/Out -&gt; TCP/IP -&gt; DHCP Not Use</b>, the current IP address appears. If you use DHCP, the actual address received from the DHCP server appears. If the IP address is set correctly, check the port number.</li> </ul>
Administrator connection	The administrator mode cannot be entered because of losing the administrator password or resignation.	<ul style="list-style-type: none"> <li>- BioLite Net allows the administrator to give access rights so only the administrator can enter the menu.</li> <li>- When you have no choice but to enter the administrator menu, you can be granted an administrator password after following the predefined procedure. (Contact with the installation agency.)</li> </ul>

## 6.3 Usage summary

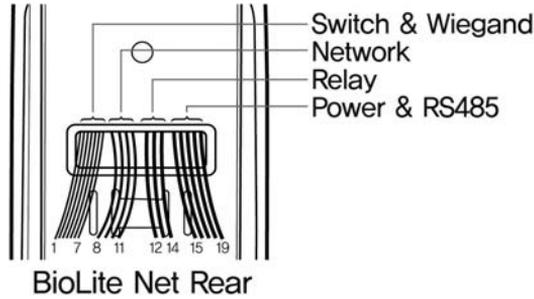
- ※ It provides the mainly used functions.
- ※  button: Used to select the desired function.

Function	Method for setting (Sequentially perform the following items.)
Initial administrator registration	Enter ID → Enter password → Enter password again
Date & time setting	Select <b>Screen, Sound</b>  icon → Select <b>Date, Time</b>  icon → Enter date → Enter time
User registration	Select <b>User</b>  icon → Select <b>Enroll</b>  icon → Enter ID → Select <b>General</b> or <b>Administrator</b> in Level → Enter fingerprint or PIN
User password modification	Select <b>User</b>  icon → Select <b>Edit</b>  icon → Enter ID or fingerprint → Select <b>PIN</b> → Enter the desired password → Enter it again
User fingerprint modification	Select <b>User</b>  icon → Select <b>Edit</b>  icon → Enter ID or fingerprint → Select <b>Fingerprint</b> → Enter the fingerprint of the user → Enter it again
User authorization method modification	Select <b>User</b>  icon → Select <b>Enroll</b>  icon → Enter ID or fingerprint → Select <b>Operation Mode</b> → Select an authorization method
User deletion	Select <b>User</b>  icon → Select <b>Delete</b>  icon → Enter ID or fingerprint to delete
All user deletion	Select <b>Device</b>  icon → Select <b>System</b>  icon → Select <b>Delete User DB</b> → Select <b>Delete</b>
Initialization (Environment settings deletion)	Select <b>Device</b>  icon → Select <b>System</b>  icon → Select <b>Factory Default</b> → Select <b>Initialize</b>



## 6.4 System Installation

### 6.4.1 Cable specifications



Type	No.	Name	Color
<b>Switch &amp; Wiegand</b>	1	SWIN0	Purple
	2	GND	Gray
	3	SWIN1	Brown
	4	GND	Gray
	5	W-DATA0	Green
	6	W-DATA1	White
	7	W-GND	Black
<b>Network</b>	8	ERX -	Yellow
	9	ERX +	Blue
	10	ETX -	Orange
	11	ETX +	Pink
<b>Relay</b>	12	Relay Normal Close	Orange (White String)
	13	Relay Common	Green (White String)
	14	Relay Normal Open	Gray (White String)
<b>Power &amp; RS485</b>	15	Power 12V	Red
	16	Power Ground	Black
	17	RS485 Ground	White (Black String)
	18	RS485 +	Blue (White String)
	19	RS485 -	Yellow (Black String)

## 6.4.2 Installing the bracket

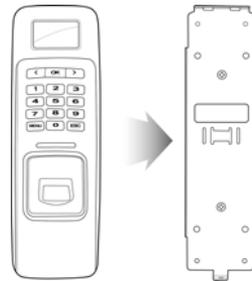
1. Fix the bracket to the place where BioLite Net is to be installed using the fixing screws.



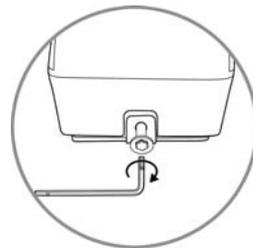
Note

If the installation place is on concrete, drill holes, insert knife blocks into the holes, and fix them by using fixing screws.

2. Install BioLite Net on the bracket.



3. Fix BioLite Net and the wall mount bracket by rotating the star-shaped screw by the hexagonal wrench.



Note

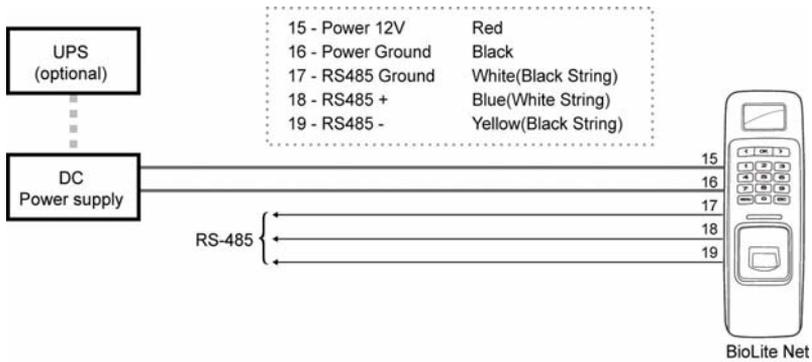
The extension bracket (Option) is provided for wiring aid according to the installation environment. Remove the basic bracket on the body for use of this bracket

BioLite Net



F  
A  
Q

### 6.4.3 Connecting Power & RS-485

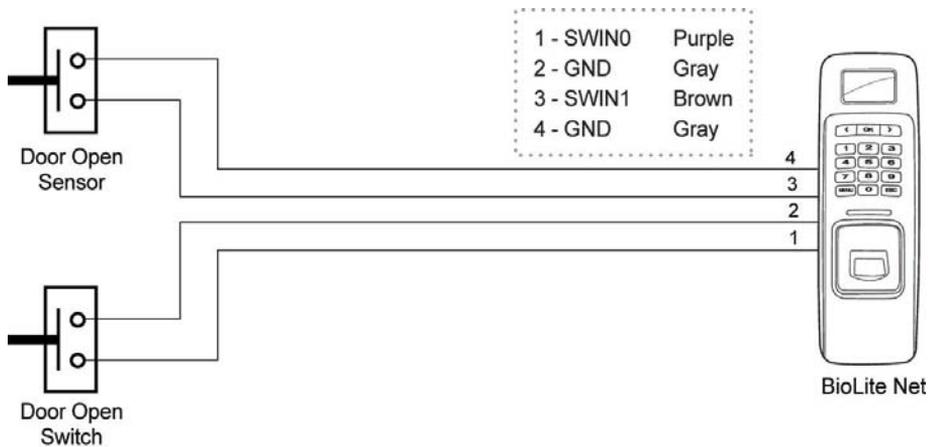


※RS-485 is used for connecting to another device  
(e.g. PC, BioStation, BioEntry Plus, BioLite Net, Secure I/O, etc.).



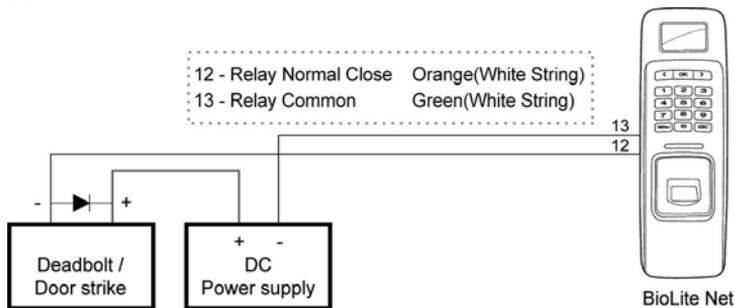
Note  
For power supply, use a product of DC 12V ( $\pm 10\%$ ) and minimum 500mA.  
To share the power adapter with another device, the required current sum of terminal (500mA) and another device must not exceed the current capacity.

### 6.4.4 Connecting the switch

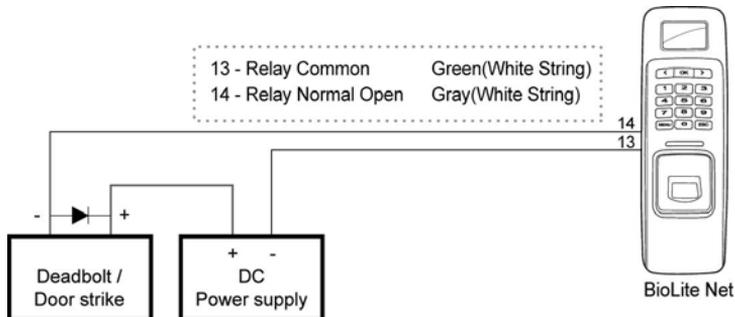


## 6.4.5 Connecting the relay

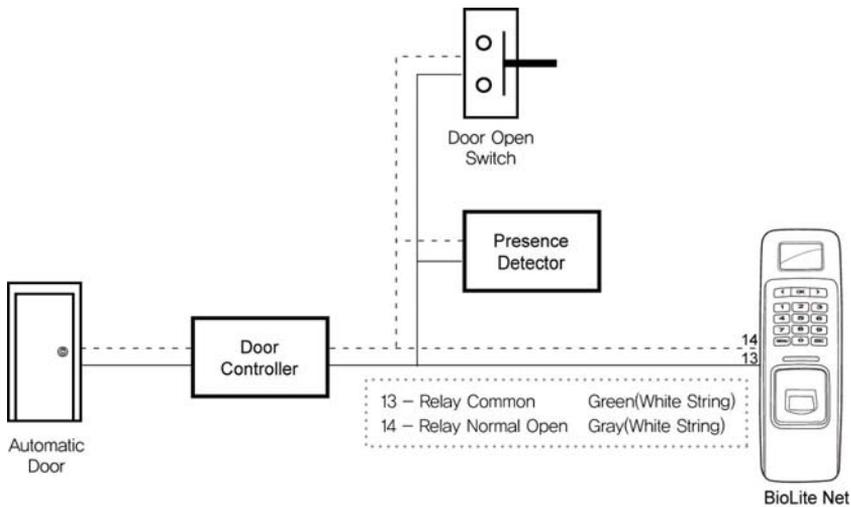
### 1. Fail safe lock



### 2. Fail secure lock



### 3. Automatic door

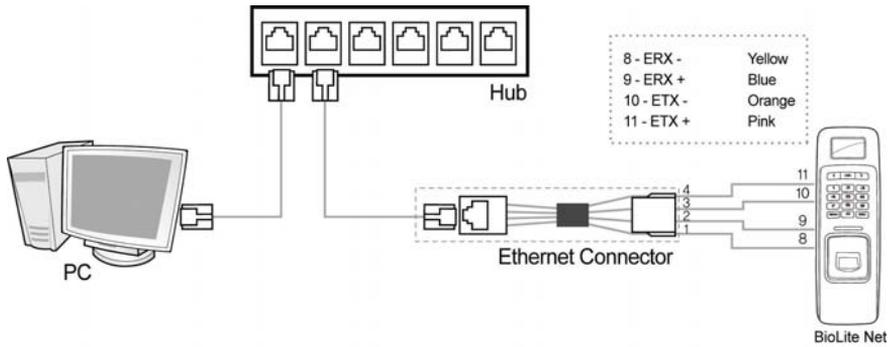


BioLite Net

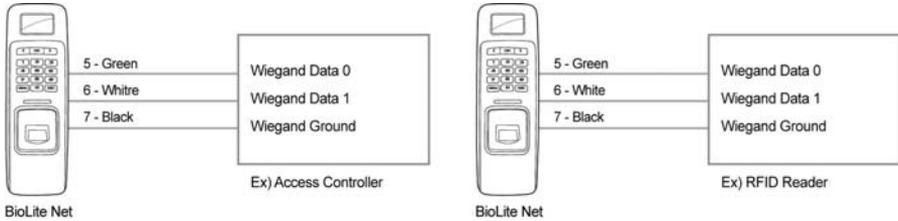


F  
A  
Q

## 6.4.6 Connecting Network



## 6.4.7 Connecting Wiegand



**When BioLite Net is used for Wiegand output device**

**When BioLite Net is used for Wiegand input device**

## 6.4.8 Electrical specifications

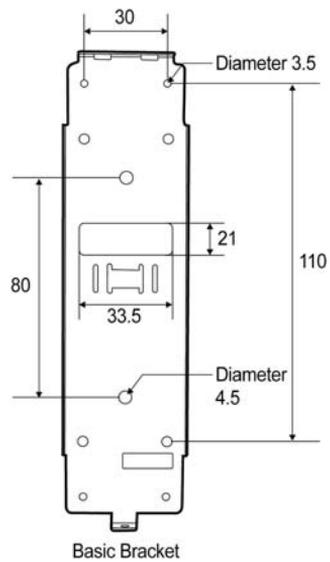
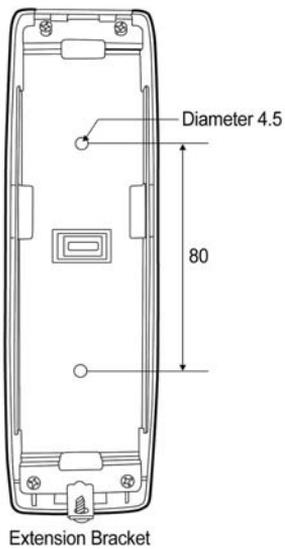
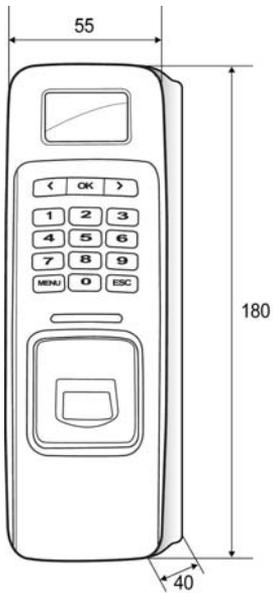
Type	Name	Min.	Typ.	Max.	Notes
Power	Voltage (V)	10.8	12	13.2	Use regulated DC power adaptor only
	Current (mA)	-		250	
Switch Input	VIH (V)	-	TBD	-	
	VIL (V)	-	TBD		
	Pull-up resistance ( $\Omega$ )	-	4.7k	-	The input ports are pulled up with 4.7k resistors
Relay	Switching capacity (A)	-	-	1 0.3	30V DC 125V AC
	Switching power (resistive)	-	-	30W 37.5VA	DC AC
	Switching voltage (V)	-	-	110 125	DC AC



## 6.5 Specifications

Item	Specification
<b>CPU</b>	400MHz DSP
<b>Fingerprint sensor</b>	500dpi optical sensor
<b>User capacity</b>	5000 users (2 fingerprints per user)
<b>Log capacity</b>	50,000 events
<b>Matching speed</b>	Less than 1 second
<b>Operation mode</b>	Fingerprint, Password, Fingerprint + Password, Card
<b>Internal relay</b>	Deadbolt, EM lock, door strike, automatic door
<b>TTL I/O</b>	2 inputs for exit switch and door sensor
<b>Wiegand In/Out</b>	1 Port (Wiegand Input or Wiegand Output is used according to the configuration.)
<b>LCD</b>	128 x 64 Graphic LCD (Monochrome)
<b>Keypad</b>	3x4 keypad, 3 navigation keys
<b>IP rate</b>	IP65 Class
<b>Operation Temperature</b>	-20℃ ~ 50℃
<b>Rated Voltage</b>	DC 12V (Min. 500mA and above) (When sharing the power with a device such as electric door lock, enough power is required considering the power requirement for the connected device.)
<b>Supportable Cards</b>	125kHz EM4100 Card (BioLite Net EM) 13.56MHz Mifare Card (BioLite Net)
<b>Size</b>	60 x 185 x 40 mm (Width x Height x Depth)
<b>Certified</b>	KCC, CE, FCC

## Mechanical Specifications



BioLite Net



F  
A  
Q

## 6.6 FCC Notice

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.

Modifications not expressly approved by the manufacturer could void the user's authority to operate the equipment under FCC rules.



## **Suprema Inc.**

16F Parkview Office Tower, Jeongja-dong, Bundang-gu Seongnam,  
Gyeonggi, Korea 463-863

TEL : 82-31-783-4502

FAX : 82-31-783-4503

Online Customer Support : [support@supremainc.com](mailto:support@supremainc.com)

Company website : [www.supremainc.com](http://www.supremainc.com)