suprema

BioLite Net

IP based Outdoor Fingerprint Terminal

User Guide

suprema

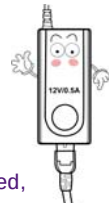
Contents

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

Endure 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 fingerprin recognition performanc or cause a failure.

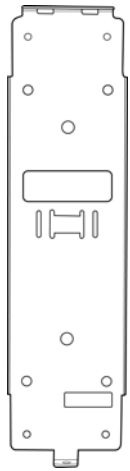
Do not forcibly press the buttons of the product and avoid any contact with sharp object to the device.
It may cause a failure.

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

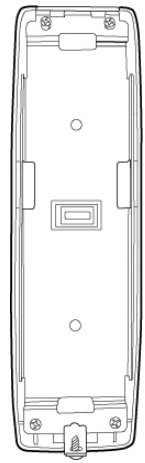
1. Before Use

1.1 Components

Main Body



Wall mounting bracket



Extended bracket (Option)

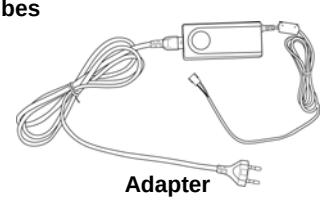
Fixing Screws
(2 EA)

Knife Blocks
(2 EA)

Shrinkable Tubes

Ethernet Connector

Star-shape wrench
(For fixing bracket)

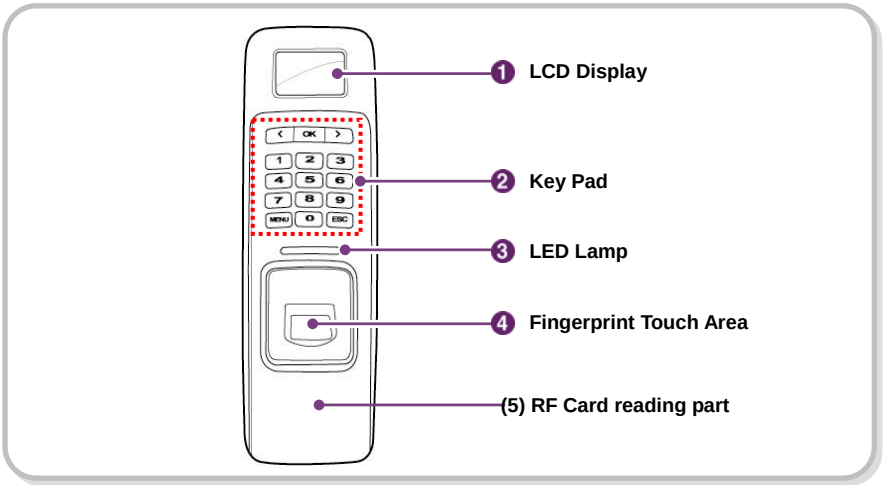


Adapter (Option)

Note

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

1.2 Body



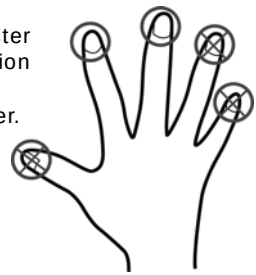
No.	Name	Description
1	**LCD Display**	The operation status is displayed.
2	**Key Pad**	0–9 Buttons: Used to enter the ID and password. < > Arrow Buttons: Used to move the selected item. OK Button: Used to select the desired function. MENU Button: Used to enter or exit the menu. ESC Button: Used to exit from the menu or cancel the desired action.
3	**LED Lamp**	The operation status is displayed with an alert sound. – Green (Sound: beep beep beep beep!): Authorization success – Red (Sound: beep beep beep!) : Authorization failure – Pink (Sound: beep!) : Processing – 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 – Blue and Sky Blue blink in turn at an interval of 2 seconds (No sound): Normal operation – Red and Pink blink in turn at an interval of 2 seconds (No sound): Device locked or no administrator – Blue and Red blink in turn at an interval of 2 seconds (No sound): The time is reset due to battery discharge. – At first use, Red blinks at an interval of 2 seconds (No sound): Initialization error, Consult with the manufacturer. – In normal use, Red blinks at an interval of 2 seconds (No sound): On the watch. – Yellow blinks shortly (No sound): Entry standby or in communication for getting an IP when DHCP is set in TCP/IP Setup
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.

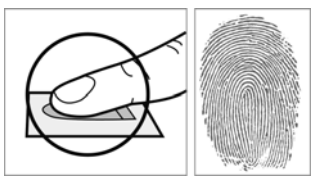
Selecting a finger on fingerprint enrollment

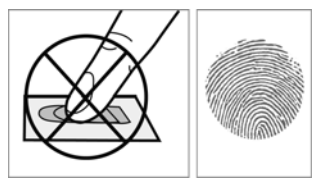
Up to two fingerprints can be enrolled for each user in preparation of any abnormal situation like having a wounded finger or carrying an object with a hand.
In the case of a low recognition, the user can register the same fingerprint twice to increase the recognition rate.
It is recommended to use the 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.



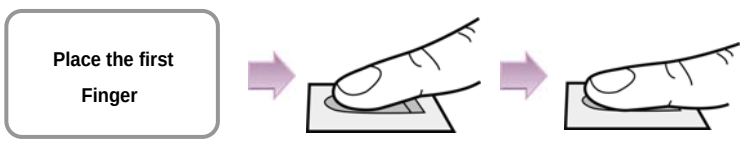
How to proerply place a fingerprint

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.

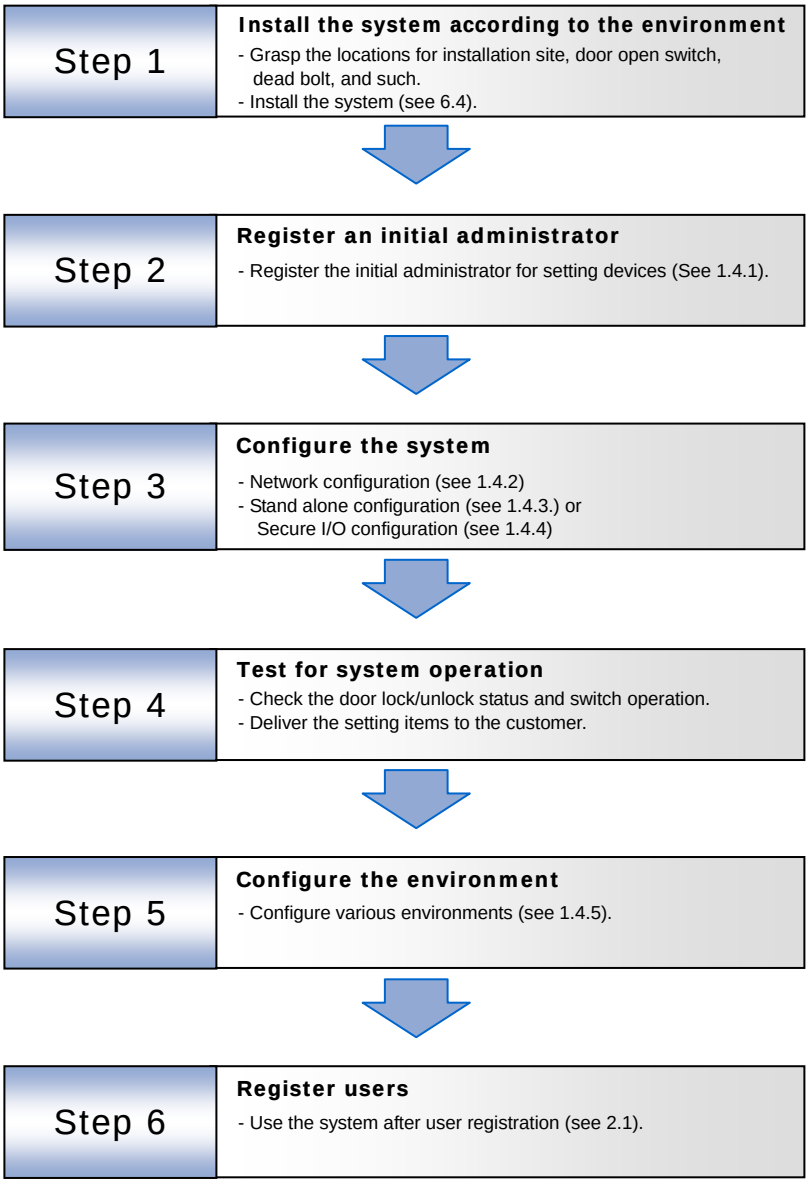
Caution

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 .

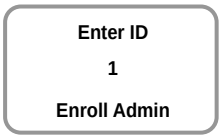
1.4 System setup procedure



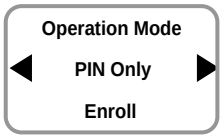
1.4.1 Registering the initial administrator

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.

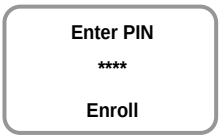
1. When the product is connected, a window appears as shown in the right figure. Enter an ID and press **OK**.



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



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



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

5. The completion message window appears.

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

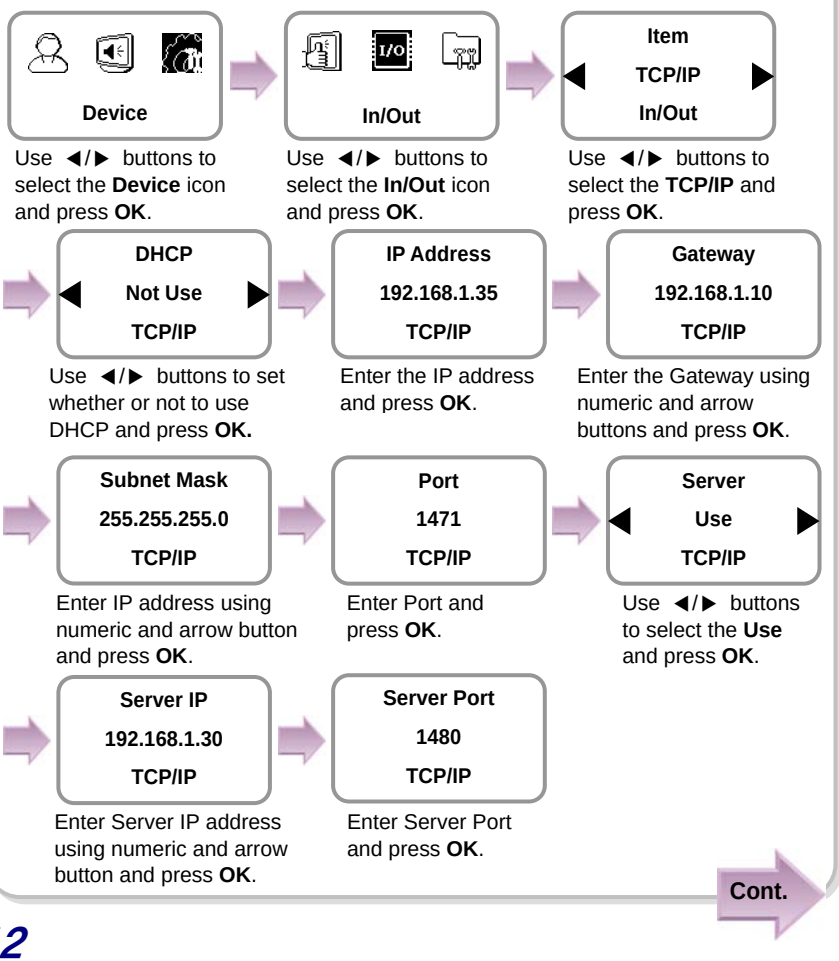
The network configuration is required to connect the dedicated PC software or other devices via network. Configure the settings according to the communication environment in your place.

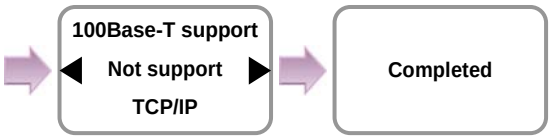
[In case of configuring the network via Ethernet]

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.

※ The following example explains how to directly connect the server PC without using DHCP.





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.)

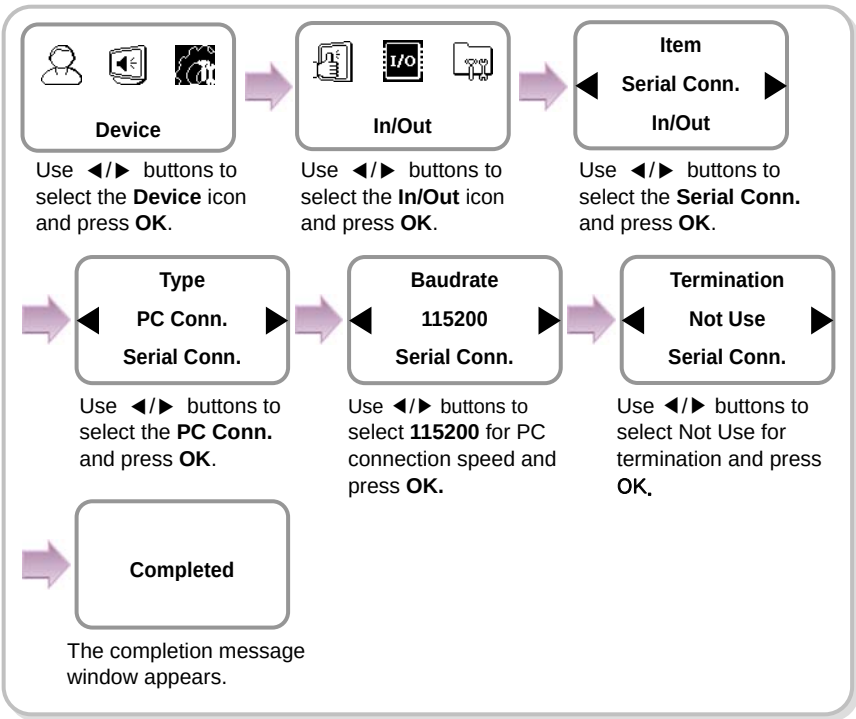
※**Server**: To directly connect the server of the dedicated PC software that enables monitoring and setting the terminal, use Server for its setup and enter the values for IP address and port number. (Refer to the dedicated PC software manual.)

※**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.”

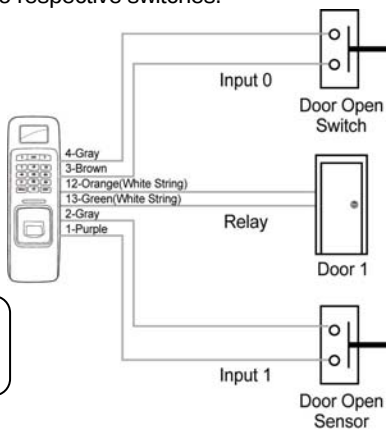
2. Configure the settings for RS-485 according to the installation environment.



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.



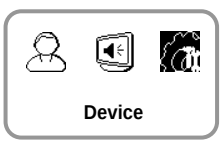
Note

For actual wring method, see “6.4 System Installation.”.

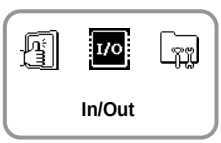
2. Configure the internal relay settings as shown below. (It is explained based on the figure above.)

Note

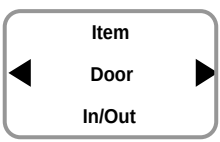
Follow the instructions below only when the dedicated PC software is not used. When using the software, refer to the software manual.



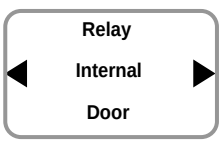
Press **MENU** -> Enter ID -> Enter the password -> Use ◀/▶ buttons to select the **Device** icon and press **OK**.



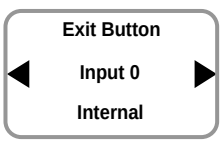
Use ◀/▶ buttons to select the **In/Out** icon and press **OK**.



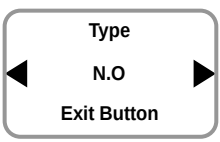
Use ◀/▶ buttons to select **Door** and press **OK**.



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

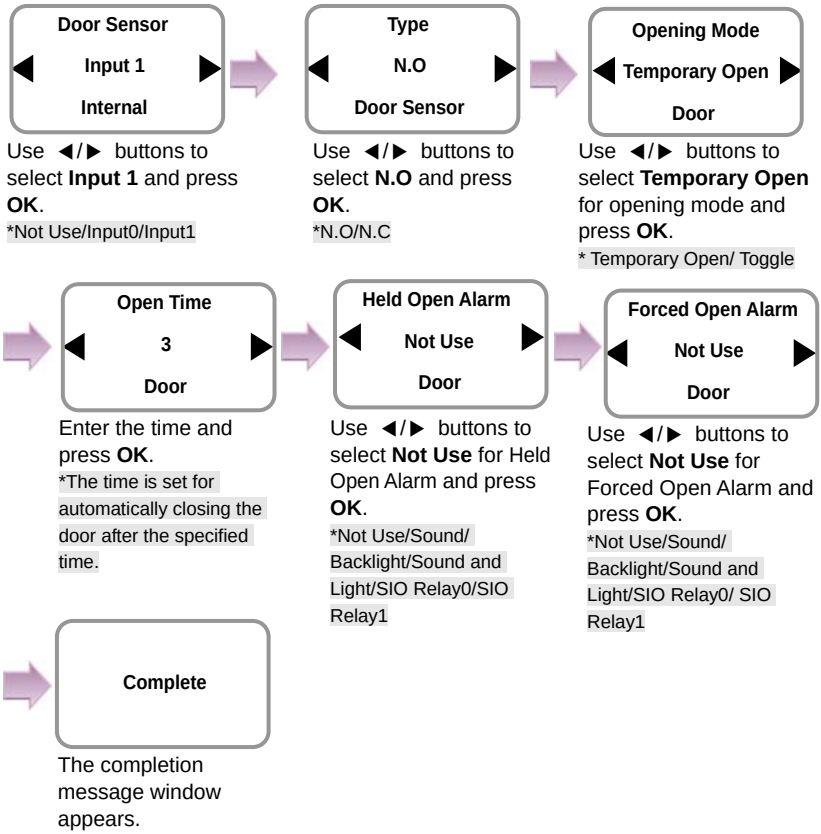


Use ◀/▶ buttons to select **Input 0** and press **OK**.



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

Cont.



※ Opening Mode

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

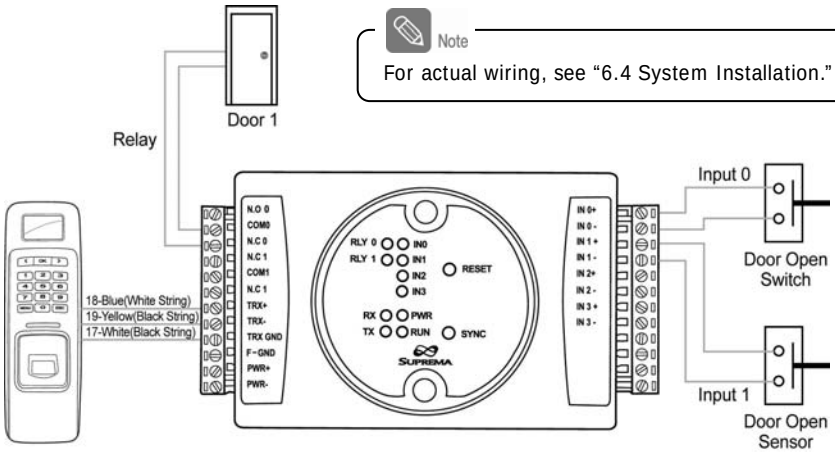
Note

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.

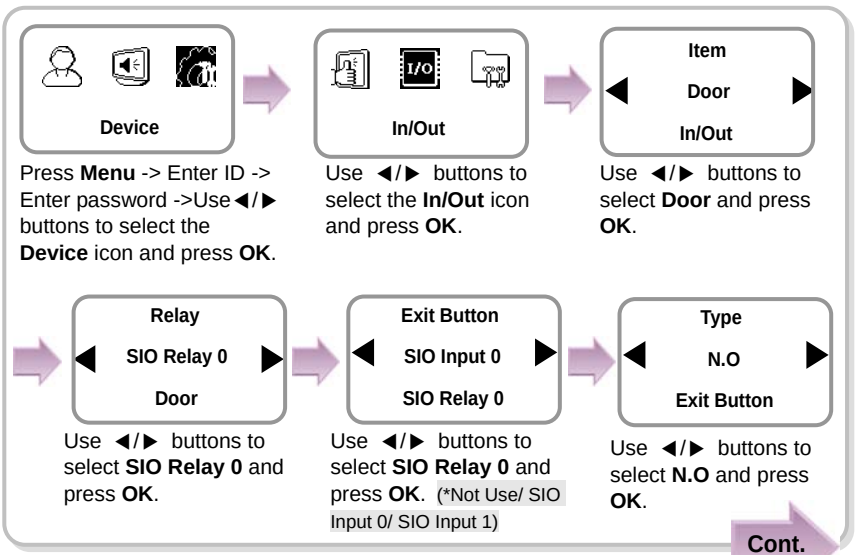
1. Connect wires between BioLite Net, Secure I/O, and respective switches as shown below.



> Note
> For actual wiring, see "6.4 System Installation."

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.



Press **Menu** -> Enter ID -> Enter password ->Use◀/▶ buttons to select the **Device** icon and press **OK**.

Use ◀/▶ buttons to select the **In/Out** icon and press **OK**.

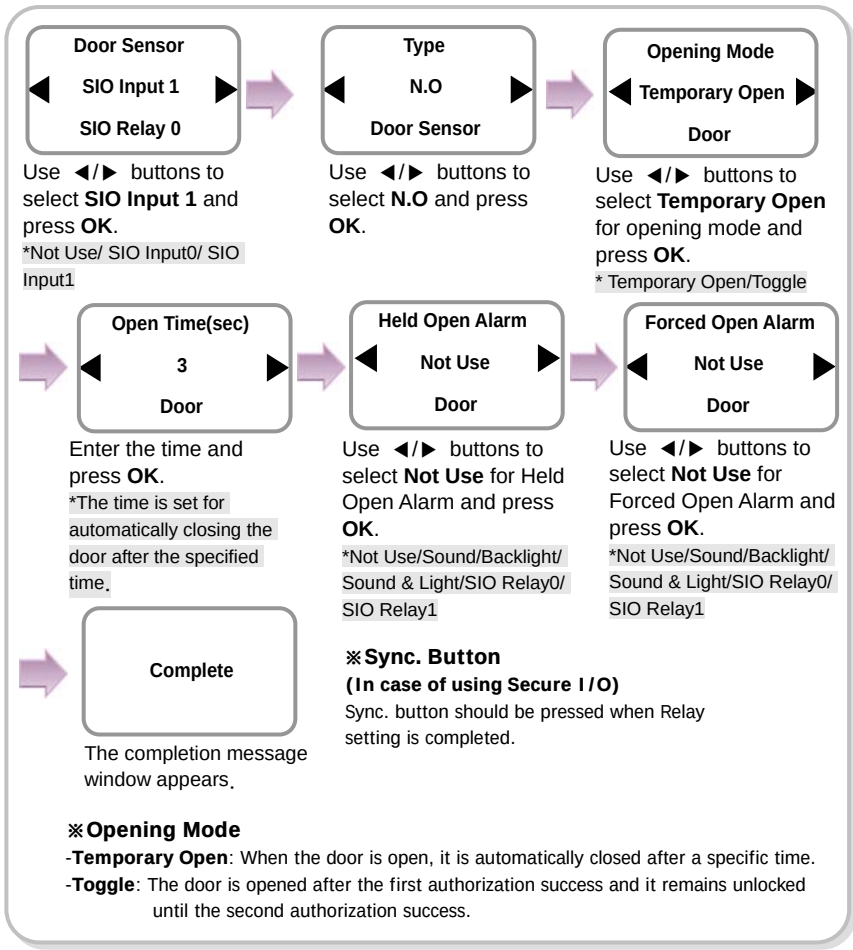
Use ◀/▶ buttons to select **Door** and press **OK**.

Use ◀/▶ buttons to select **SIO Relay 0** and press **OK**.

Use ◀/▶ buttons to select **SIO Relay 0** and press **OK**. (*Not Use/ SIO Input 0/ SIO Input 1)

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

Cont.



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

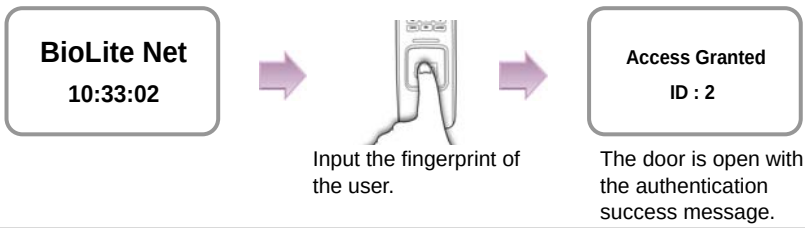
For changing the terminal authorization method, see the operation mode selection case in “4.1 Authorization.”
To separately set the authorization method for each user, see “2.2 Editing a user data.”

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

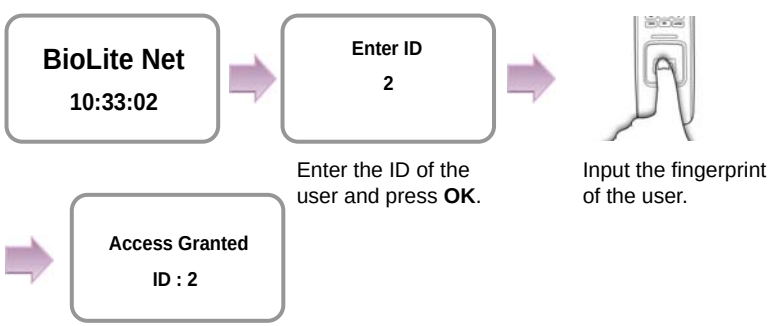
Fingerprint recognition



Input the fingerprint of the user.

The door is open with the authentication success message.

Fingerprint recognition after entering ID

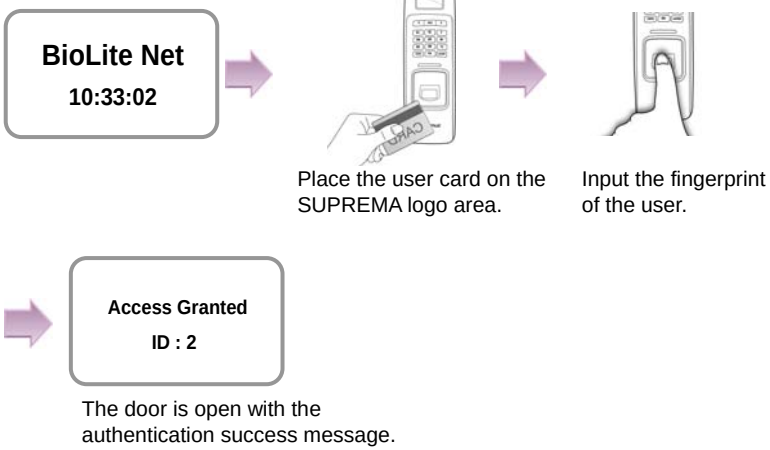


Enter the ID of the user and press **OK**.

Input the fingerprint of the user.

The door is open with the authentication success message.

Fingerprint recognition after identifying user card

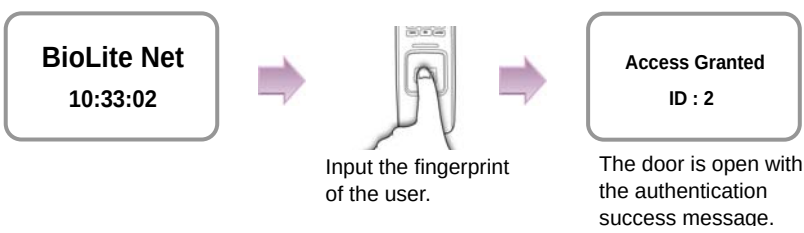


1.5.2 Finger or PIN

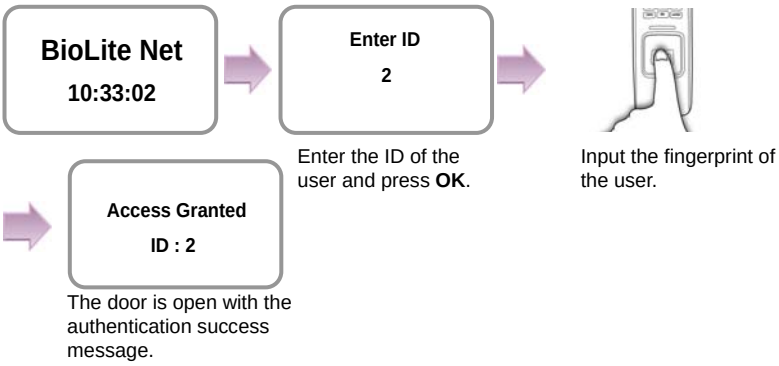
When the user authorization method is set to “Finger or PIN,” you can open the door by using the five different methods:

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

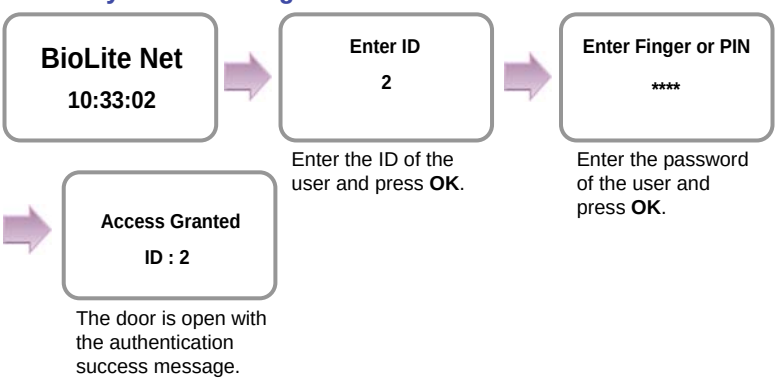
Fingerprint recognition



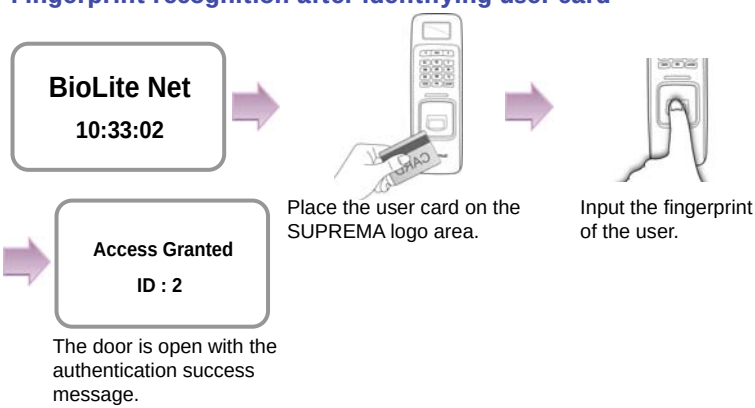
Fingerprint recognition after entering ID



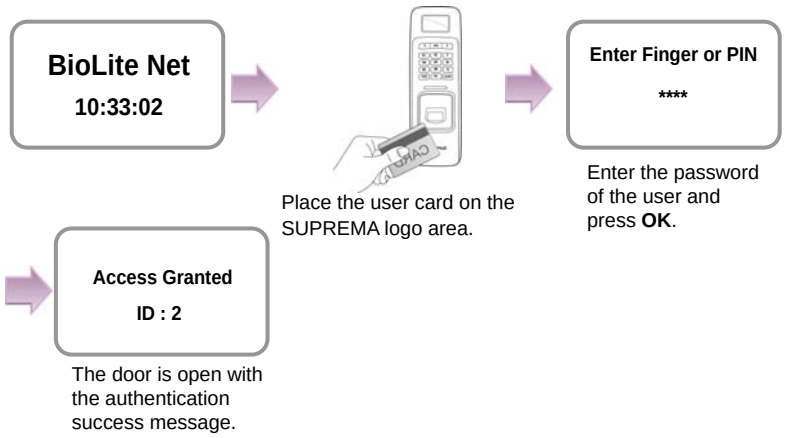
PIN entry after entering ID



Fingerprint recognition after identifying user card



PIN entry after identifying the user card

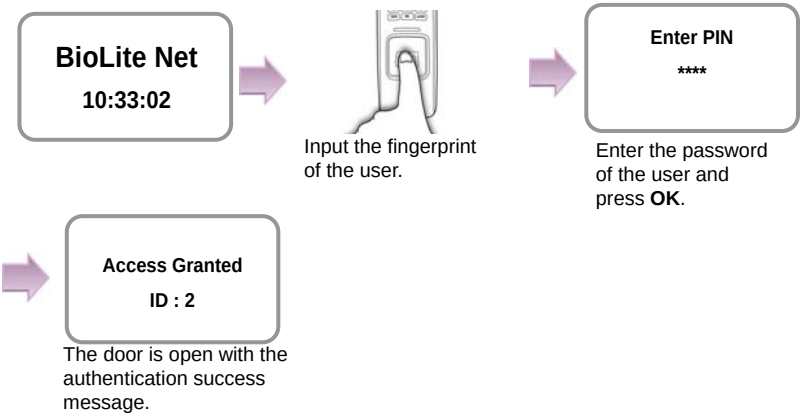


1.5.3 Finger and PIN

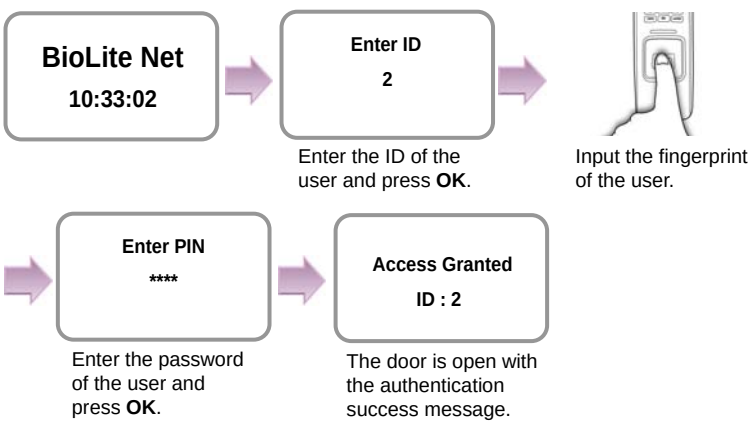
When the user authorization method is set to “Finger and PIN,” you can open the door by using the three different methods:

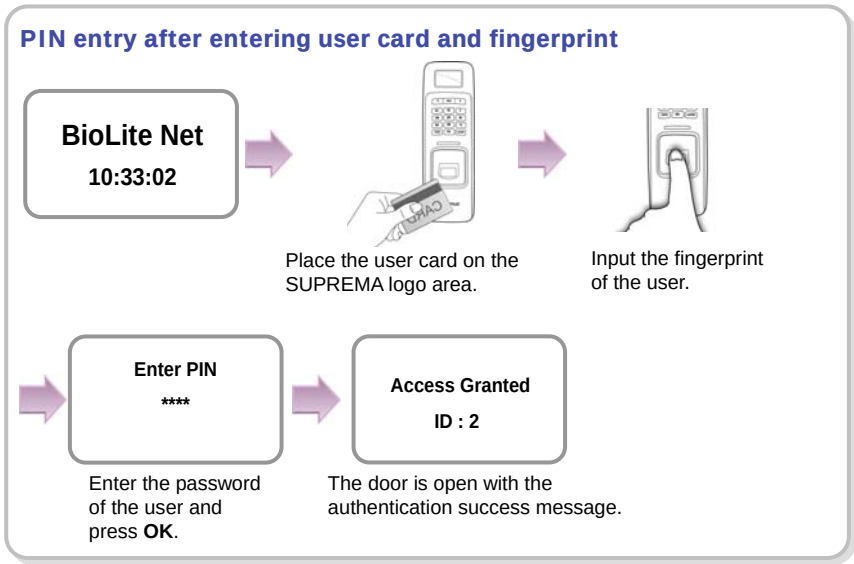
1. PIN entry after identifying fingerprint
2. PIN entry after entering ID and fingerprint
3. PIN entry after entering user card and fingerprint

PIN entry after identifying fingerprint



PIN entry after entering ID and fingerprint

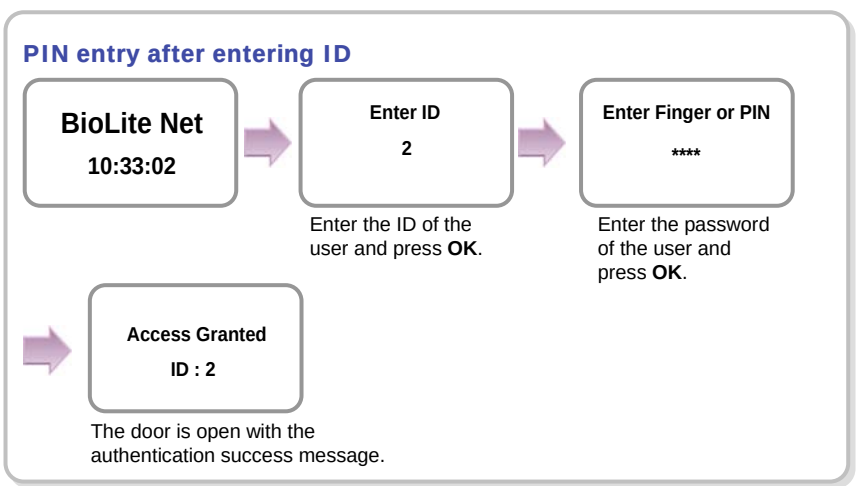




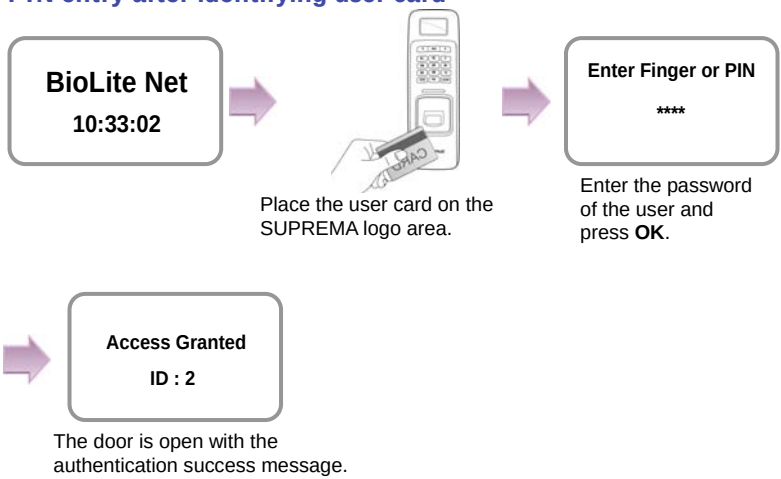
1.5.4 PIN Only

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

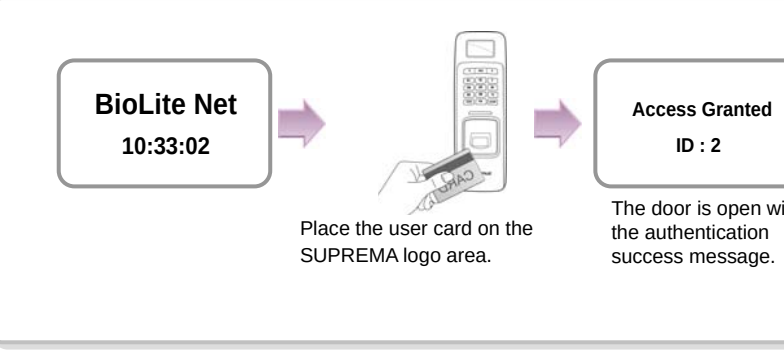


PIN entry after identifying user card



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

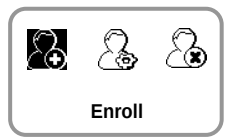
The user management and other environment settings can be updated after authorizing the registered administrator (see 1.4.1 “Registering the initial administrator”).

2.1 Enrolling a user

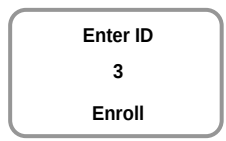
You can enroll a new user as shown below:

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)

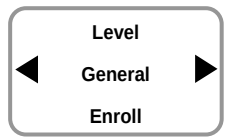


Note

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

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

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

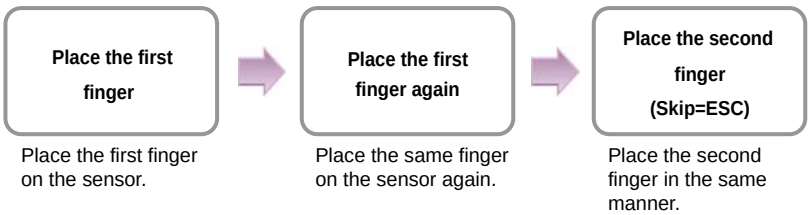


5. Enter the finger or PIN depending on the **operation mode**.
(Password: 4–8 digit number, Fingerprint: 1st finger or 1st + 2nd fingers)

Note

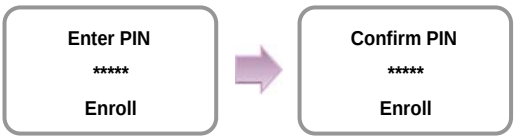
Enter the required information after selecting **Device > Authorization > Operation Mode > Auth Mode**.

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.

6. When the user enrollment is successfully done, the completion message window appears.
※ User can be enrolled up to maximum 5000.

2.2 Editing a user data

You can modify the data of the previously enrolled user.

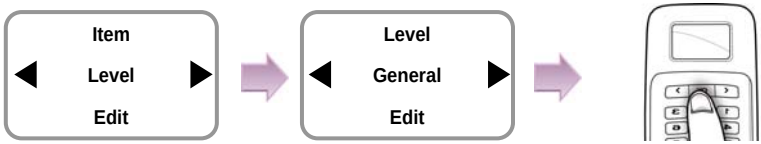
1. Use ◀/▶ buttons to select the **User** ( ) icon and press **OK**.

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 37 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

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

Place the first finger on the sensor.

Place the same finger on the sensor again.

Enroll the second fingerprint in the same manner.

Changing the PIN of the user

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

Enter the desired password and press **OK**.

After re-entering the password of the user, press **OK**.

Changing the access group

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

Use ◀/▶ buttons to select access privilege for selected Access Group
*Full Access/No Access/Not Use/Or user designated Access Group

Press **OK**.

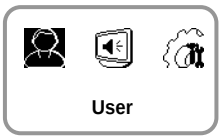
Note

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.

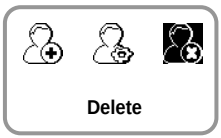
2.3 Deleting a user data

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

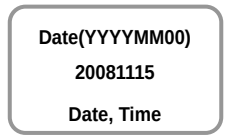
3.1 Date, Time

You need to set the current system date and time.
After setting the date and time, the log data can store correct information.

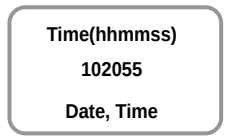
1. Use ◀/▶ buttons to select the **Screen, Sound** ( ) icon and press **OK**.

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

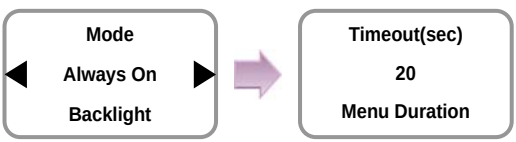
1. Use ◀/▶ buttons to select the **Screen, Sound** ( ) icon and press **OK**.

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

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

Always On

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

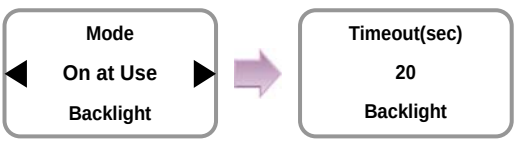


Use ◀/▶ buttons to select the **Always On** and press **OK**.

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

On at Use

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



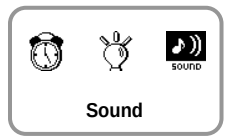
Use ◀/▶ buttons to select the **On at Use** and press **OK**.

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

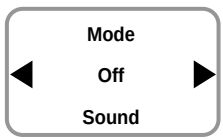
3.3 Sound

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

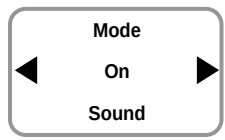
2. Use ◀/▶ buttons to select **Sound** ( ) icon and press **OK**.



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



Or



4. Device Configuration

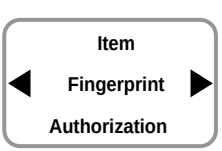
4.1 Authorization

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**.

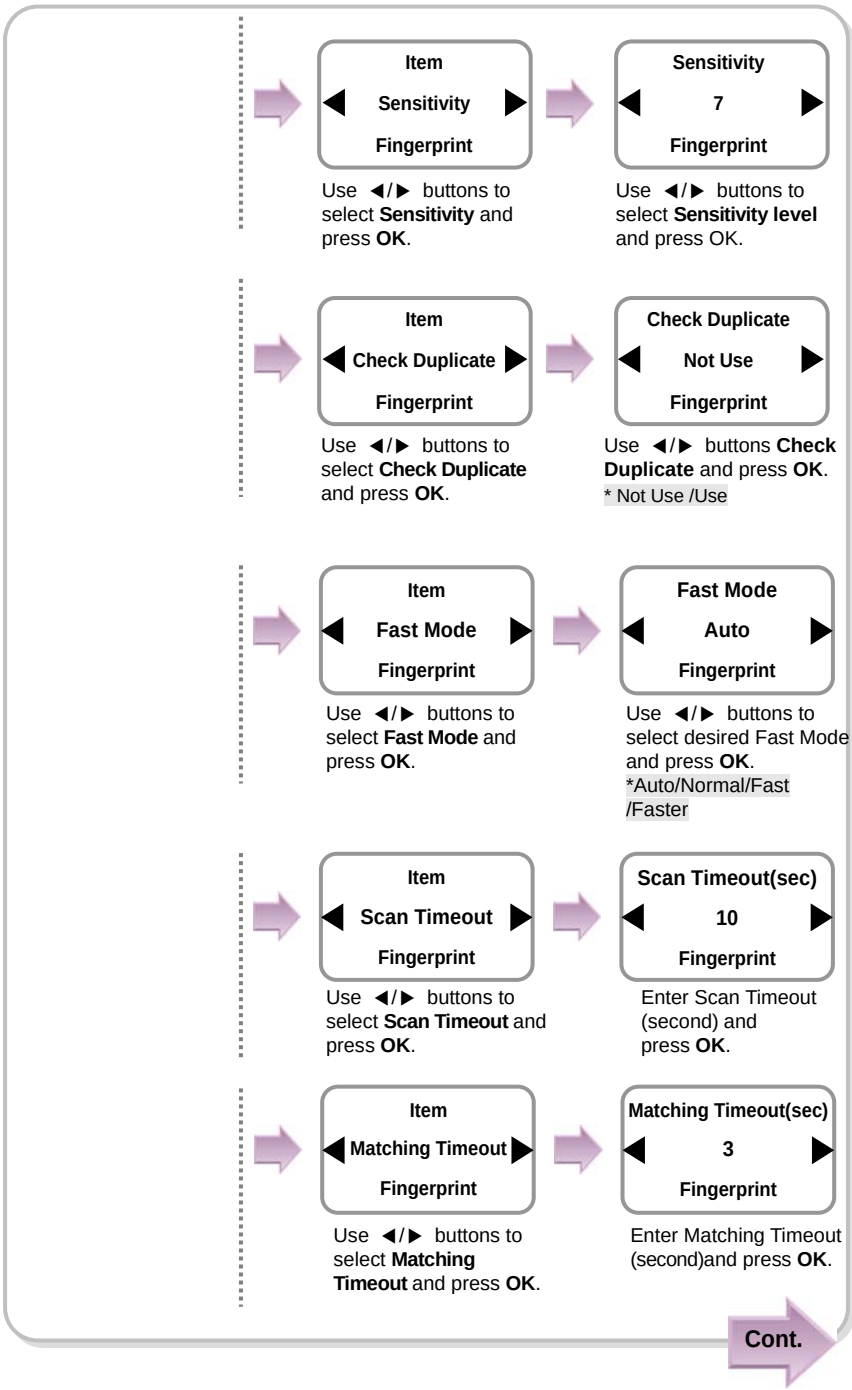
Use ◀/▶ buttons to select **Security Level** and press **OK**.

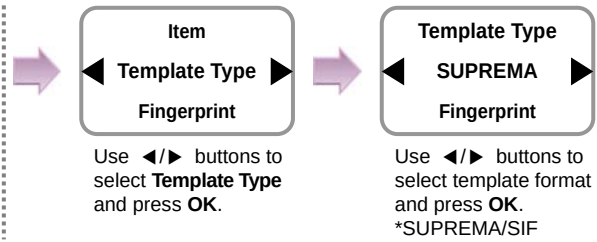
Use ◀/▶ buttons to select **Security Level** and press **OK**.
* Normal /Secure/More Secure

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

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

Cont.


Item
Sensitivity
Fingerprint
Sensitivity
7
Fingerprint
Use ◄/► buttons to select **Sensitivity** and press **OK**.
Use ◄/► buttons to select **Sensitivity level** and press OK.
Item
Check Duplicate
Fingerprint
Check Duplicate
Not Use
Fingerprint
Use ◄/► buttons to select **Check Duplicate** and press **OK**.
Use ◄/► buttons **Check Duplicate** and press **OK**.
* Not Use /Use
Item
Fast Mode
Fingerprint
Fast Mode
Auto
Fingerprint
Use ◄/► buttons to select **Fast Mode** and press **OK**.
Use ◄/► buttons to select desired Fast Mode and press **OK**.
*Auto/Normal/Fast /Faster
Item
Scan Timeout
Fingerprint
Scan Timeout(sec)
10
Fingerprint
Use ◄/► buttons to select **Scan Timeout** and press **OK**.
Enter Scan Timeout (second) and press **OK**.
Item
Matching Timeout
Fingerprint
Matching Timeout(sec)
3
Fingerprint
Use ◄/► buttons to select **Matching Timeout** and press **OK**.
Enter Matching Timeout (second)and press **OK**.
Cont.



※ **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.

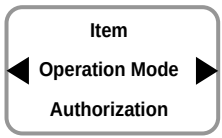
※ **Matching Timeout**: You can set the maximum authorization time after entering fingerprint. If this time limit expires, matching stops and the authorization fails.

※ **Template Type**: Format used in the terminal when identifying fingerprints (SUPREMA/SIF)

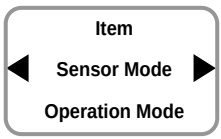
- SUPREMA: SUPREMA's own template format, SIF: ISO/IEC compatible template format

(To change the template format, there must be no fingerprint data stored on the terminal.)

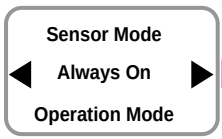
In case of Operation Mode



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



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

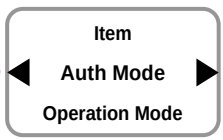


Use ◀/▶ buttons to select a sensor mode. *Always On/ID Entered/OK Pressed

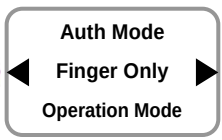
Use ◀/▶ buttons to select the applicable time zone and press **OK.**

※ **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.

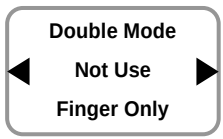


Use ◀/▶ buttons to select **Auth Mode** and press **OK**.



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

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

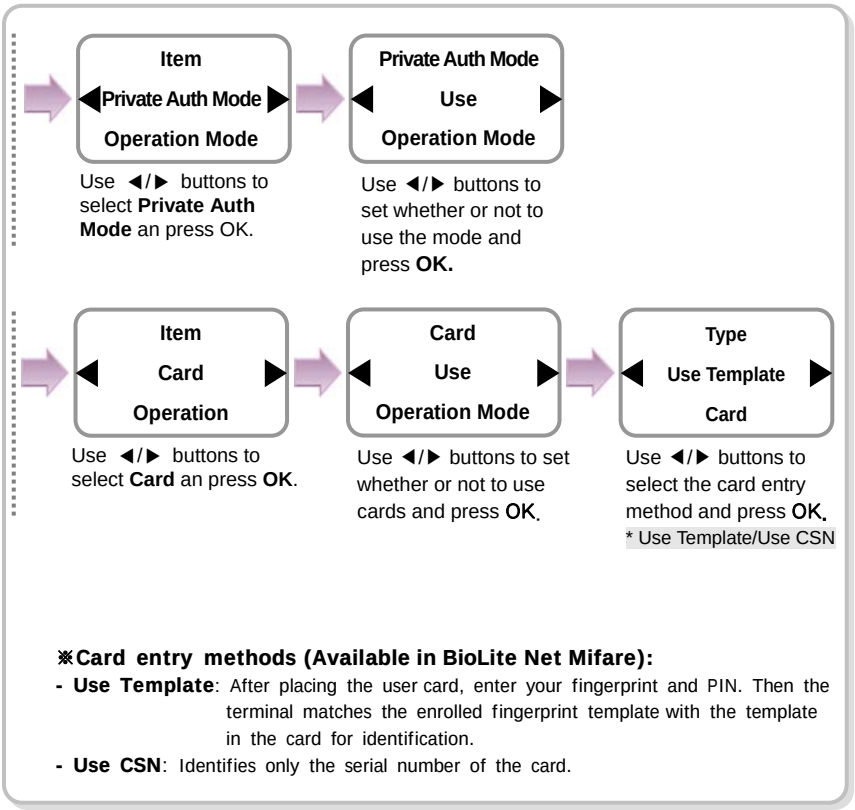


Use ◀/▶ buttons to set whether or not to use the double mode and press **OK**.

※**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.

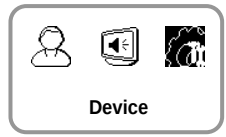


※Card entry methods (Available in BioLite Net Mifare):

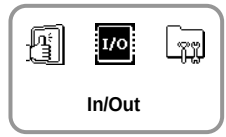
- **Use Template**: After placing the user card, enter your fingerprint and PIN. Then the terminal matches the enrolled fingerprint template with the template in the card for identification.
- **Use CSN**: Identifies only the serial number of the card.

4.2 In/Out

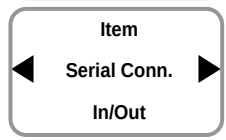
1. Use ◀/▶ buttons to select the **Device** ( ) icon and press **OK**.



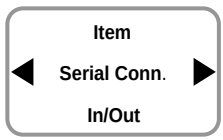
2. Use ◀/▶ buttons to select **In/Out** ( ) icon and press **OK**.



3. Use ◀/▶ buttons to select any of Serial Conn., Tamper On, Door Wiegand, and TCP/IP and press **OK**.



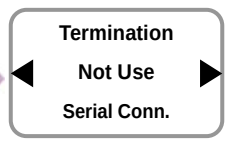
In case of Serial Conn. (selection of connection method)



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

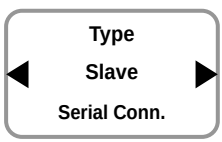
※**Serial Conn.**: It is used for RS485 communication or direct PC connection.

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

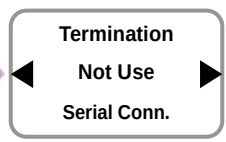


Use ◀/▶ buttons to set whether or not to use the termination and press **OK**.

The completion message window appears.

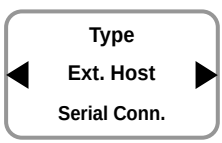


Use ◀/▶ buttons to select **Slave** and press **OK**.

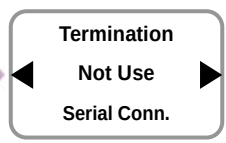


Use ◀/▶ buttons to set whether or not to use the termination and press **OK**.

The completion message window appears.



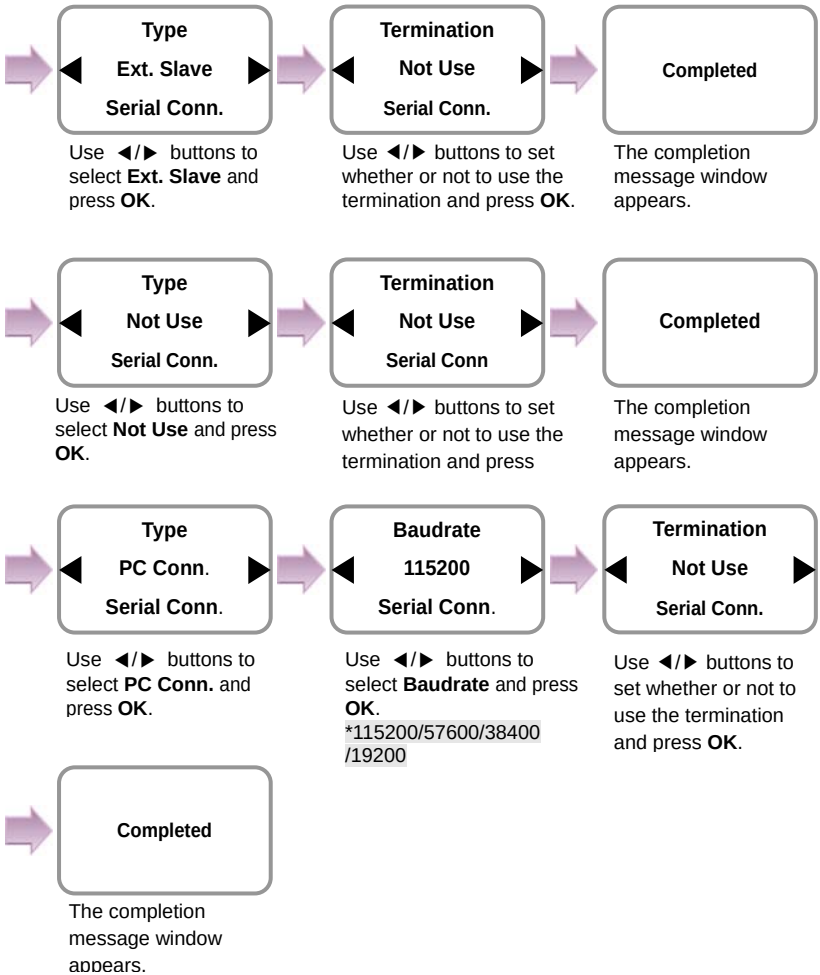
Use ◀/▶ buttons to select **Ext. Host** and press **OK**.



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

The completion message window appears.

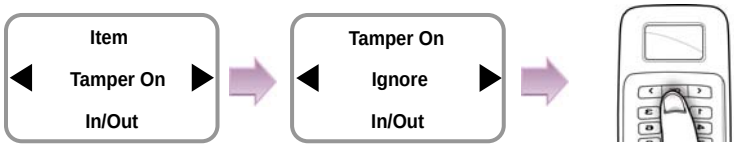
Cont.



※ Methods

- **PC Conn.**: Directly connects to PC through RS485
- **Host/Slave**: Connects between terminals through RS485. Used when the terminal interoperates with the BioAdmin software. (Refer to the BioAdmin manual.)
- **Ext. Host/Ext. Slave**: Connects between terminals through RS485. Used when the terminal interoperates with the BioStar software. (Refer to the BioStar manual.)
- **Termination**: Used when the communication line is too long or the signal strength changes drastically (It enforces the signal strength).
- **Host/Slave, Ext. Host/Ext. Slave**: Connects between terminals through RS485. The communication speed is fixed to 115200 baudrate.

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.)

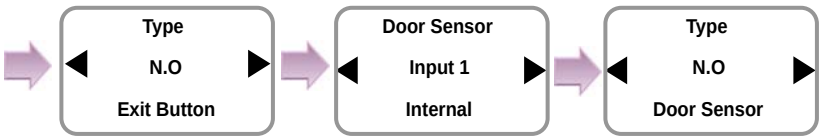
In case of Door (When using the internal relay)

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

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

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

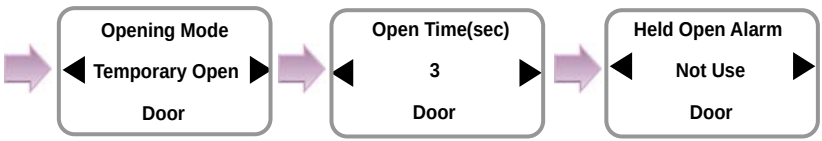
Use ◀/▶ buttons to select **Exit Button** and press **OK**.
* Not Use/ Input 0/ Input 1



Use ◀/▶ buttons to select the type for **Exit Button** and press **OK**.
*N.O/N.C

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

Use ◀/▶ buttons to select a door sensor type and press **OK**.
*N.O/N.C



Use ◀/▶ buttons to select a opening mode and press **OK**.
*Temporary Open/ Toggle

Enter the time and press **OK**.

Use ◀/▶ buttons to select the type for Held Open Alarm and press **OK**.
* Not Use /Sound/Backlight/ Sound& Light/SIO Relay0/ SIO Relay1

Enter the held open time by using the Numeric buttons and press **OK**.
***Held Open Time**: Alarm ringing time when the open door is not closed.

Use ◀/▶ buttons to select the type for Forced Open Alarm and press **OK**.
*Not Use/Sound/ Backlight/Sound and Light/SIO Relay0/ SIO Relay1

The completion message window appears.

Note

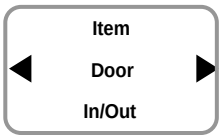
When you exit from the menu before completing the relay setup, the configuration is not stored so please finish configuration until the message “Complete” appears.

※ 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)

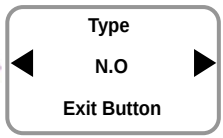
※ It is used only when the stand-alone BioLite Net is installed without interoperating with the dedicated PC software.



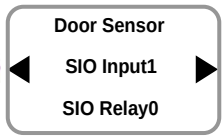
Use ◀/▶ buttons to select **Door** and press **OK**.

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

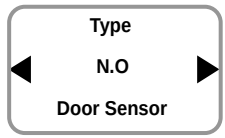
Use ◀/▶ buttons to select the **exit button** and press **OK**.
* Not Use/SIO Input0/ SIO Input1



Use ◀/▶ buttons to select the type of the exit button and press **OK**.
*N.O/N.C



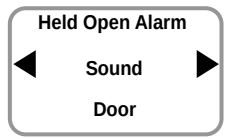
Use ◀/▶ buttons to select the door sensor and press **OK**.
*Not Use/ SIO Input1



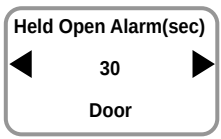
Use ◀/▶ buttons to select the door sensor type and press **OK**.
*N.O/N.C

Use ◀/▶ buttons to select the type of the opening mode and press **OK**.
*Temporary Open/ Toggle

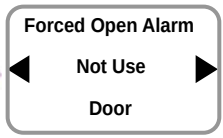
Enter the time and press **OK** and press **OK**.



Use ◀/▶ buttons to select the alarm type and press **OK**.
*Not Use/Sound/Backlight/ Sound and Light/SIO Relay0/SIO Relay1



Enter the time for Held Open Alarm by using the Numeric buttons and press **OK**.
***Held Open Time**: Alarm ringing time when the open door is not closed.

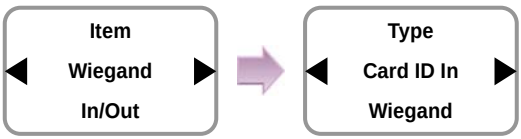


Use ◀/▶ buttons to select the type for Forced Open Alarm and press **OK**.
*Not Use/Sound/ Backlight/Sound and Light/SIO Relay0/ SIO Relay1

The completion message window appears.

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.

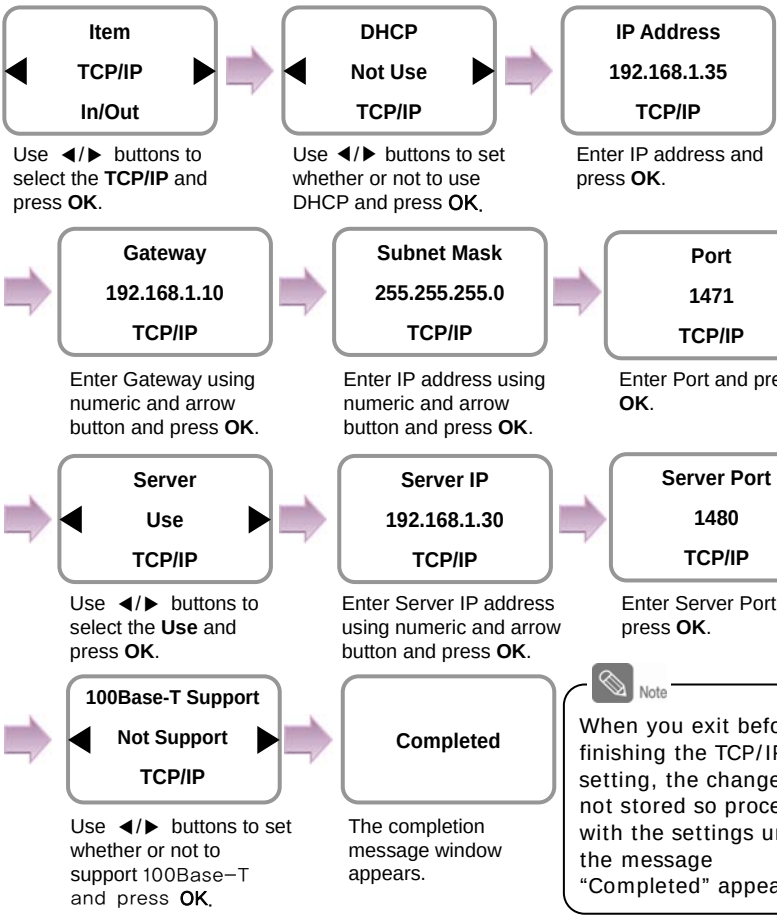
Note

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.)

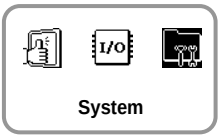
※**Server**: To directly connect the server of the dedicated PC software that enables monitoring and setting the terminal, use Server for its setup and enter the values for IP address and port number. **(Refer to the dedicated PC software manual.)**

※**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.)

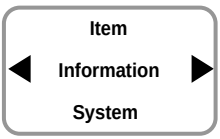
4.3 System

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

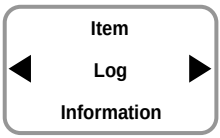
2. Use ◀/▶ buttons to select the **System** ( ) icon and press **OK**.



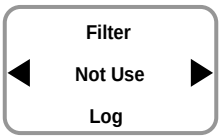
3. Use ◀/▶ buttons to select any of Information, Factory Default, Delete All Log, Delete User DB, and Language and press **OK**.



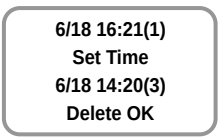
In case of Information



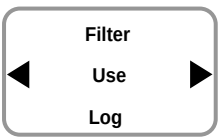
Use ◀/▶ buttons to select **Log** and press **OK**.



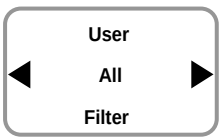
Use ◀/▶ buttons to select **Not Use** and press **OK**.



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



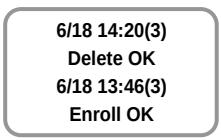
Use ◀/▶ buttons to select **Use** and press **OK**.



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

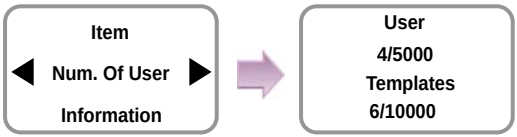


The log filtering result appears on the screen. (Use ◀/▶ buttons to see the previous/next logs.)

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

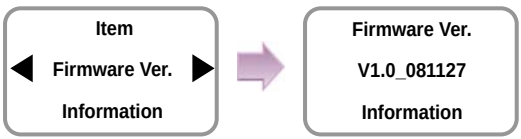
※When the date is specified, the logs occurred earlier than the specified date appear.

In case of Information — Continued



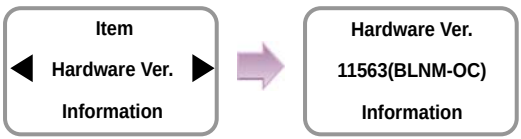
Use ◀/▶ buttons to select **Num. Of User** and press **OK**.

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

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

Use ◀/▶ buttons to determine whether or not to delete them.
*Cancel/ Delete

In case of Delete, the message Deletion appears.

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

In case of Delete User DB

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

Use ◀/▶ buttons to determine whether or not to delete the user DB.
*Cancel/Delete

In case of Delete, the message **Deletion** appears.

※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

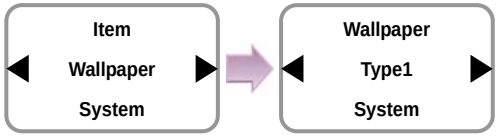
Use ◀/▶ buttons to select **Language** and press **OK**.

Use ◀/▶ buttons to select the language.
* English/ Korean/Custom

Press **OK**.

※ To use custom language, desired language resource file needs to be downloaded to t he device using **BioStar S/W** on PC. Please refer to BioStar user guide for details

In case of Wallpaper



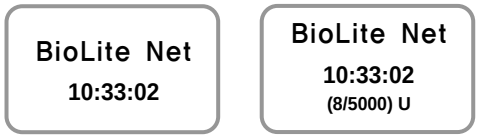
Use ◀/▶ buttons to select **Wallpaper** and press **OK**.

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.

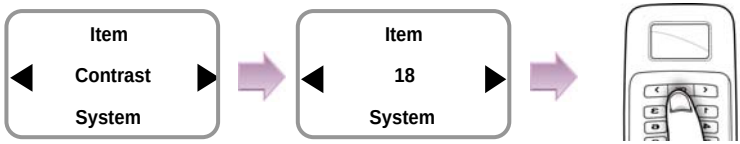


Type1 **Type2**

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 adjust contrast parameter.
* Default value is 18

Press **OK**.

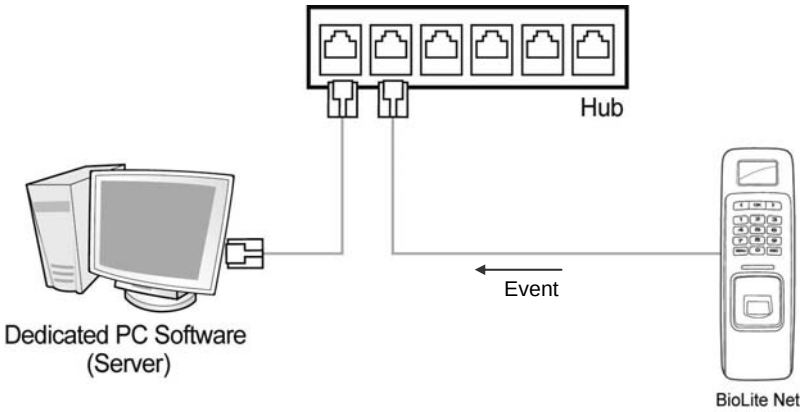
※ Contrast value is not affected by Factory default.

5. Attendance Management

5.1 Operating environment

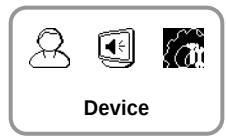
When an event (attendance, leaving, return, and outside duty) is received from the terminal, it is reported to the server of the dedicated PC software. You can create a report from the events stored in the server.
With the dedicated PC software, you can also define new event other than the above-mentioned 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.



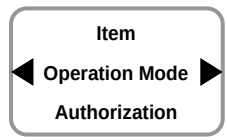
5.2 Setup for attendance management

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

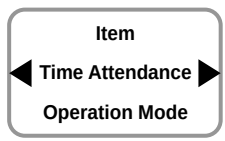


2. Use ◀/▶ buttons to select the **Authorization** ( ) icon and press **OK**.

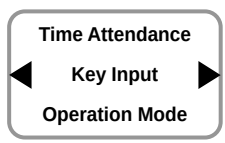
3. Use ◀/▶ buttons to select the **Operation Mode** and press **OK**.



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**.



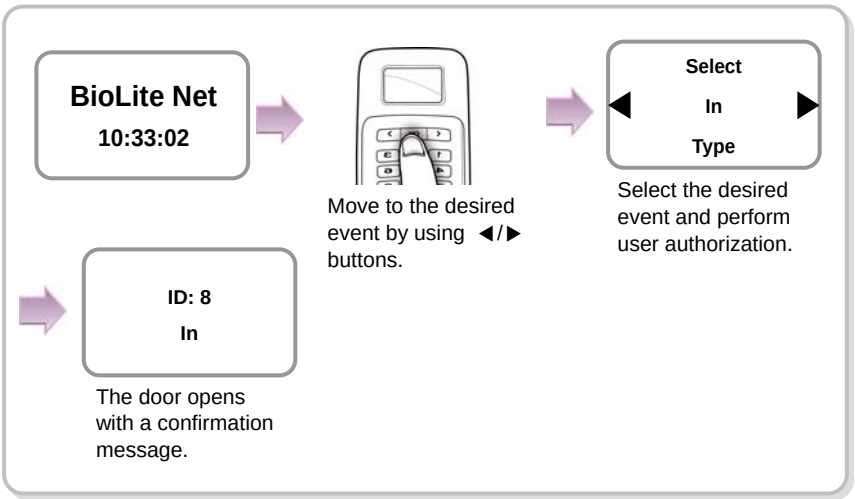
※**Operation modes**: *Key Input/Fixed/Manual/Auto/Not Use

- **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.

5.3 Operation modes

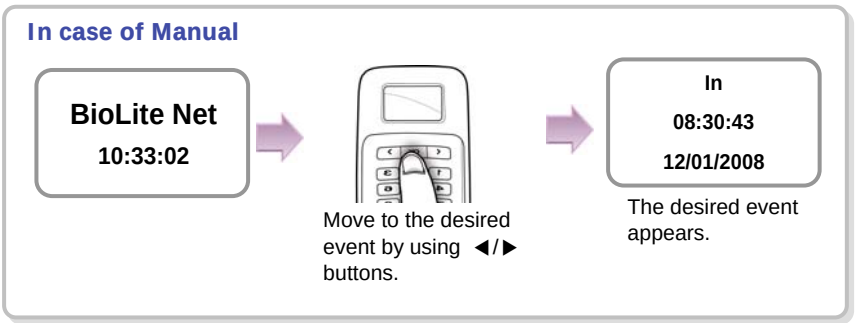
5.3.1 Key Input

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

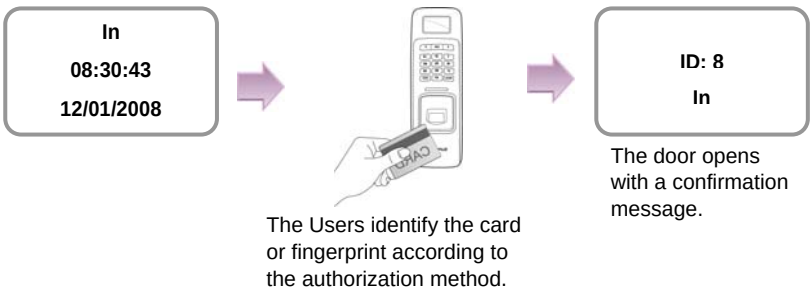


5.3.2 Manual

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

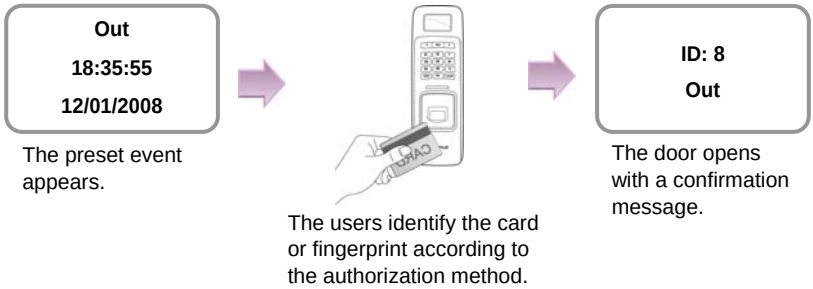
When the operation mode is set to “Auto,” this mode is used.
This mode can set the corresponding time zone for each attendance event through the dedicated PC software. Then the fixed event is set for the corresponding time zone.

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.



※ **Fixed**: This mode is available only when the desired event is set for all the users who are entering or leaving.

6. FAQ

6.1 Error messages

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

6.2 Troubleshooting

Category	Trouble	Solution
Power	The power is supplied but the device does not operate.	- When the device is disconnected from the bracket, it may not work when using the tamper switch. - Check the adapter or power cable.
Password	The password is lost.	- Enter the queried password after contacting the administrator in case of a normal user. - When the administrator password is lost, contact with the installation agency.
	The locked door is not open after entering the password and pressing **OK**.	- Check whether the correct password is input. - Check whether you have changed the password recently. - If you cannot find the password, contact the administrator.
Fingerprint	The fingerprint has been enrolled but its recognition encounters an error.	- 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. - For better performance in fingerprint recognition, correct registration is a must. - Enroll the fingerprint again after seeing "1.4 Methods for fingerprint input" - The recognition rate may vary due to the characteristic of each finger so enroll the fingerprint of another finger.
	It was good at recognizing fingerprints but suddenly it fails in recognition.	- Check whether the finger or the sensor is covered with sweat, moisture, or dust. - In case the fingerprint has any damage, the device may consider it as the one of wrong person. - Wipe the finger or sensor with a dry cloth and retry. - When the fingerprint is so dry, blow your steam of breath into it and retry.
Door lock	Even if you close the door, the door is not locked.	- The electric lock failure is most likely to happen. Check it after contacting the installation agency.
Time	The time is not correct.	- 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."
TCP/IP	The terminal data is not found by the dedicated PC software.	- Check the connection status after setting on the terminal like **Terminal > System > Wallpaper > Type2**. - When U is displayed: Check the LAN connection status. - When D is displayed: Check the IP address. If you set like **Terminal > In/Out -> TCP/IP -> DHCP Not Use**, 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.
Administrator connection	The administrator mode cannot be entered because of losing the administrator password or resignation.	- BioLite Net allows the administrator to give access rights so only the administrator can enter the menu. - 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.)

6.3 Usage summary

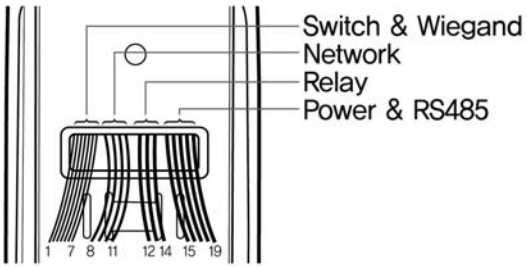
※ It provides the mainly used functions.

※ [OK] 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 **Screen, Sound** (🔊) icon → Select **Date, Time** (🕐) icon → Enter date → Enter time
User registration	Select **User** (👤) icon → Select **Enroll** (👤+) icon → Enter ID → Select **General** or **Administrator** in Level → Enter fingerprint or PIN
User password modification	Select **User** (👤) icon → Select **Edit** (👤✎) icon → Enter ID or fingerprint → Select **PIN** → Enter the desired password → Enter it again
User fingerprint modification	Select **User** (👤) icon → Select **Edit** (👤✎) icon → Enter ID or fingerprint → Select **Fingerprint** → Enter the fingerprint of the user → Enter it again
User authorization method modification	Select **User** (👤) icon → Select **Enroll** (👤+) icon → Enter ID or fingerprint → Select **Operation Mode** → Select an authorization method
User deletion	Select **User** (👤) icon → Select **Delete** (👤−) icon → Enter ID or fingerprint to delete
All user deletion	Select **Device** (📡) icon → Select **System** (🖥) icon → Select **Delete User DB** → Select **Delete**
Initialization (Environment settings deletion)	Select **Device** (📡) icon → Select **System** (🖥) icon → Select **Factory Default** → Select **Initialize**

6.4 System Installation

6.4.1 Cable specifications



BioLite Net Rear

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

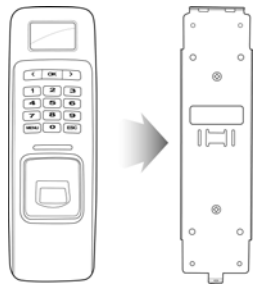
6.4.2 Installing the bracket

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

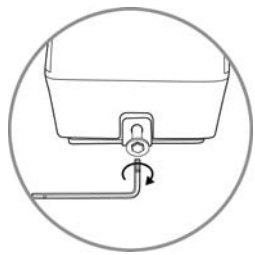
Note

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.



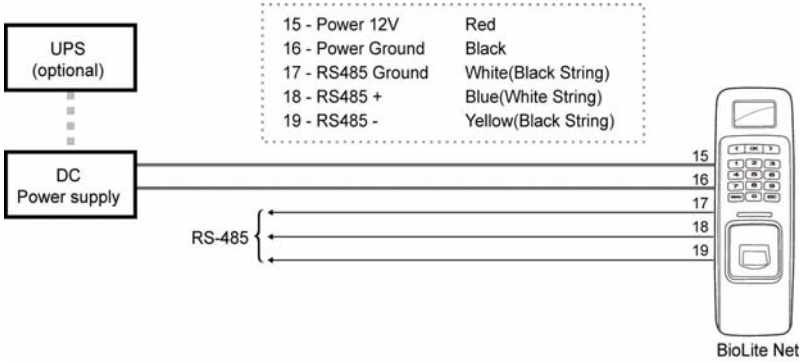
3. Fix BioLite Net and the wall mount bracket by rotating the star-shape screw by the hexagonal wrench.



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

6.4.3 Connecting Power & RS-485

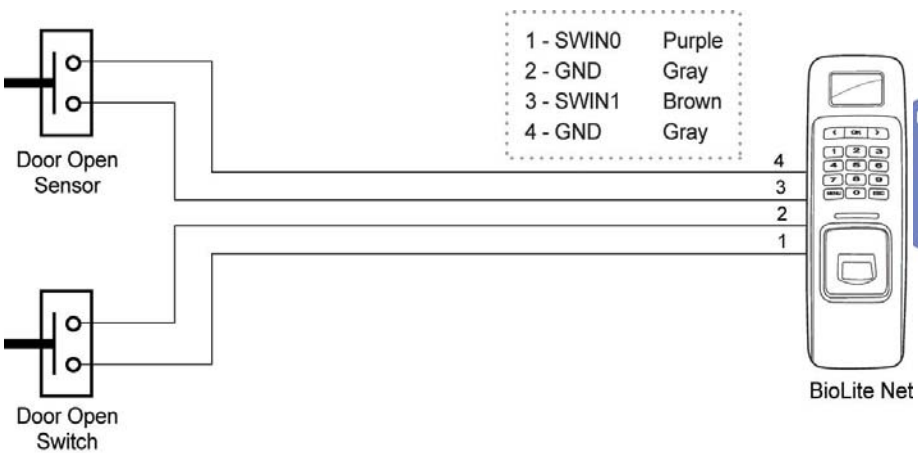


※RS-485 is used for connecting to another device
(e.g. PC, BioStation, BioEntry Plus, BioLite Net, Secure I/O, etc.).

Note

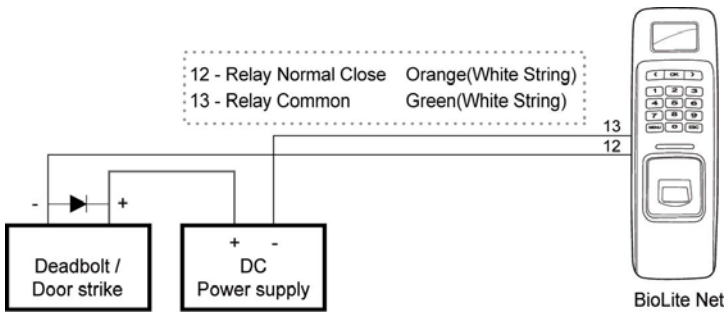
For power supply, use a product of DC 12V (± 10%) and minimum 500mA.
To share the power adapter with another device, the required current sum of terminal (500mA) and another device must not exceed the current capacity.

6.4.4 Connecting the switch

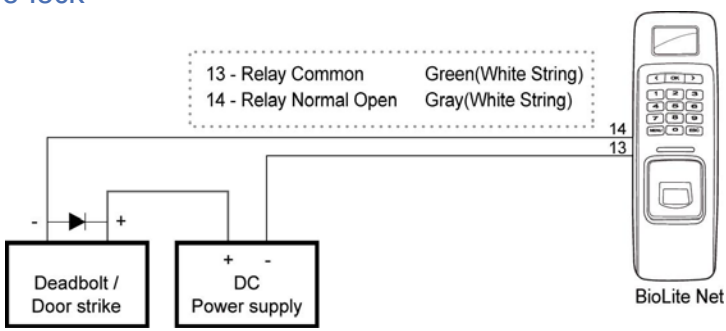


6.4.5 Connecting the relay

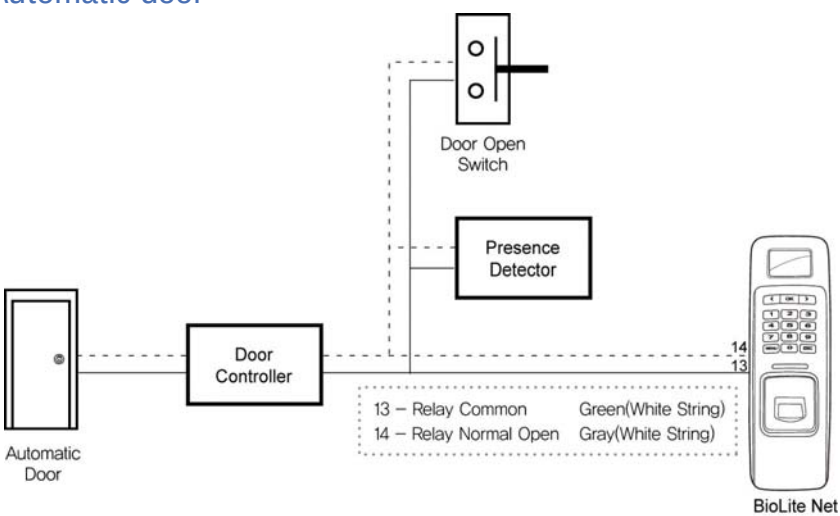
1. Fail safe lock



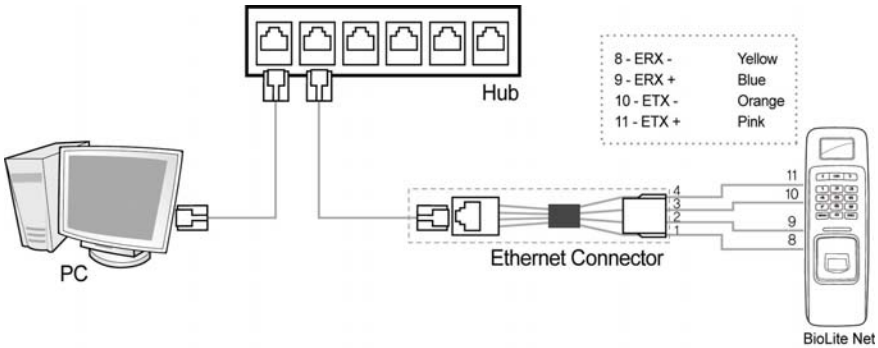
2. Fail secure lock



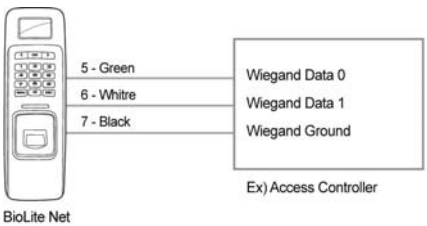
3. Automatic door



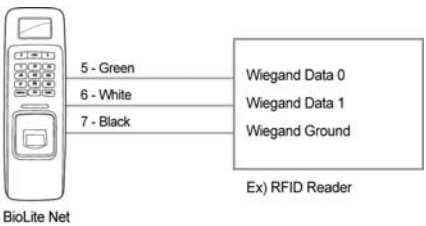
6.4.6 Connecting Network



6.4.7 Connecting Wiegand



When BioLite Net is used for Wiegand output device



When BioLite Net is used for Wiegand input device

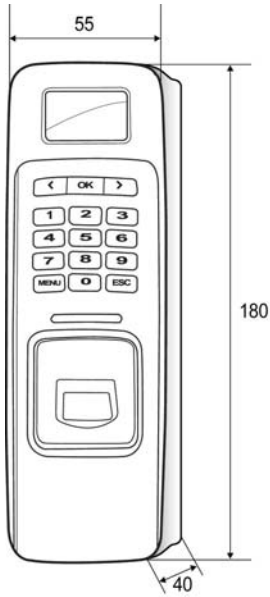
6.4.8 Electrical specifications

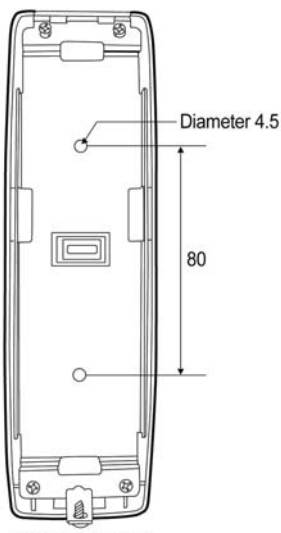
Type	Name	Min.	Typ.	Max.	Notes
Power	Voltage (V)	10.8	12	13.2	Use regulated DC power adaptor only
	Current (mA)	-		250	
Switch Input	VIH (V)	-	TBD	-	
	VIL (V)	-	TBD		
	Pull-up resistance (Ω)	-	4.7k	-	The input ports are pulled up with 4.7k resistors
Relay	Switching capacity (A)	-	-	1 0.3	30V DC 125V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

6.5 Specifications

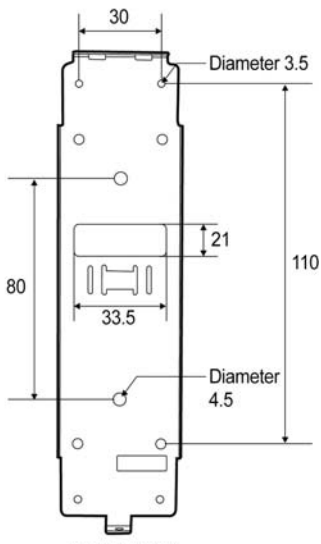
Item	Specification
CPU	400MHz DSP
Fingerprint sensor	500dpi optical sensor
User capacity	5000 users (2 fingerprints per user)
Log capacity	50,000 events
Matching speed	Less than 1 second
Operation mode	Fingerprint, Password, Fingerprint + Password, Card
Internal relay	Deadbolt, EM lock, door strike,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

Mechanical Specifications





Extension Bracket



Basic Bracket

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 operated 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
Company website : www.supremainc.com