



# USER GUIDE

## BioLite Net

---

English

**Version 2.20**

# Contents

---

<b>Safety Instructions .....</b>	<b>4</b>
<b>Getting Started .....</b>	<b>6</b>
Components .....	6
Part names and features .....	7
How to Scan a Fingerprint.....	8
Choosing a finger for registration .....	8
How to register a fingerprint .....	8
<b>User Management .....</b>	<b>9</b>
Registering User Information .....	9
Changing User Information .....	10
Changing or Adding a fingerprint .....	10
Changing PIN.....	10
Changing or Adding a card .....	10
Changing authority .....	11
Deleting a User .....	11
Checking User Capacity Status .....	11
<b>Authentication Configuration .....</b>	<b>12</b>
Fingerprint Authentication configuration .....	12
Card Authentication configuration .....	12
ID Authentication configuration .....	12
Matching Timeout configuration .....	13
Scan Timeout configuration .....	13
<b>Display/Sound Configuration.....</b>	<b>14</b>
Backlight Timeout configuration .....	14
Menu Timeout configuration.....	14
Message Timeout configuration.....	14
Language selection .....	14
Sound configuration .....	14
<b>Device Configuration .....</b>	<b>15</b>
Checking Device Information .....	15
Date/Time configuration.....	15
Fingerprint configuration .....	15
Template Type configuration.....	15
Security Level configuration.....	15
Authentication Speed (Fast Mode) configuration .....	16
Sensitivity configuration .....	16
How to configure a Relay .....	16
<b>Communication Configuration.....</b>	<b>17</b>
TCP/IP configuration .....	17
Server IP configuration .....	17
Device IP configuration.....	17
RS-485 configuration .....	17
RS-485 Mode configuration .....	17
Baud Rate configuration .....	18
Termination configuration.....	18
<b>Device Reset .....</b>	<b>18</b>

Full Reset .....	18
Reset Without Net .....	18
Reboot .....	18
<b>Troubleshooting .....</b>	<b>19</b>
Checklist before Requesting Service.....	19
<b>Product Specifications .....</b>	<b>20</b>
Dimensions.....	21
<b>FCC Compliance Information.....</b>	<b>22</b>
<b>Appendix .....</b>	<b>23</b>
Disclaimers .....	23
Copyright Notice .....	23

# Safety Instructions

Please read the following instructions carefully before using the product. This information is important for ensuring the safety of the user and for preventing damage to the user's property.

## Warning

Violation of the instructions may cause serious injury or death.

### Installation Instructions

**Do not install the product in direct sunlight or in a location that is damp or dusty.**

- This can cause a fire or electric shock.

**Do not install the product near any heat source such as electric heaters.**

- This can cause a fire from overheat or electric shock.

**Install the product in a dry place.**

- Moisture can cause product damage or electric shock.

**Install the product in a place where there is no electromagnetic interference.**

- This can cause product damage or electric shock.

**Have qualified service professionals install or repair the product.**

- Otherwise, it can cause a fire, electric shock, or injury.
- If the product is damaged due to a user's unauthorized installation or dismantling of the product, a service fee will be charged for repair.

### Operating Instructions

**Be careful not to spill any liquid such as water, drinks, or chemicals inside the product.**

- This can cause fire, electric shock, or product damage.

## Caution

Ignoring these instructions may result in minor injuries or damage to the product.

### Installation Instructions

**Protect the power cord from being walked on or pinched.**

- This can cause product damage or injury.

**Keep the product away from strong magnetic objects such as magnets, TVs, monitors (especially CRT monitors), or speakers.**

- This can cause a failure.

**Only use the power adapter included with the product or a DC power adapter providing a current more than 500mA.**

- This device does not work if the proper power source is not used.

**If installing the product outside where the product is completely exposed, it is recommended to install the product together with the enclosure.**

**Use a separate power supply for Secure I/O 2, electric lock and BioLite Net respectively.**

- If connecting and using the power supply to these devices together, the devices may malfunction.

## Operating Instructions

**Do not drop the product or subject it to shock or impact during use.**

- This can cause a failure.

**Keep the password secret from others and change it periodically.**

- Failure to do so may lead to an illegal intrusion.

**Do not press the buttons on the product with excessive force or with a sharp tool.**

- This can cause a failure.

**Be careful not to contaminate or damage the fingerprint reader with a dirty hand or materials.**

- This can decrease performance or cause failure to read a fingerprint.

**Clean the product with a soft, dry cloth. Do not use alcohol, benzene, or water.**

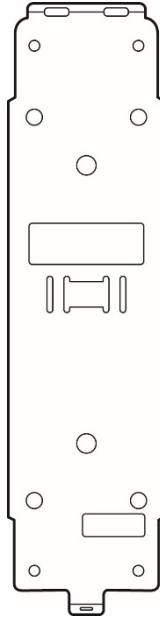
- This can cause a product failure.

# Getting Started

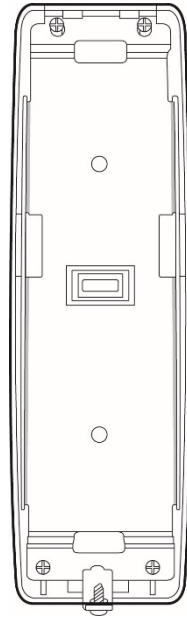
## Components



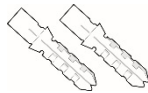
BioLite Net



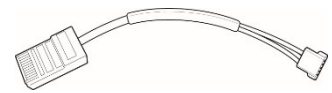
Main bracket



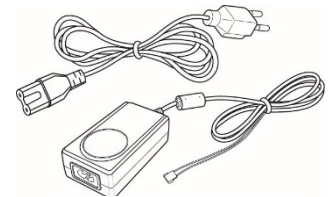
Extension bracket

Mounting screws  
(2 pcs)Screw anchors  
(2 pcs)

Heat shrink tubes



Ethernet connector

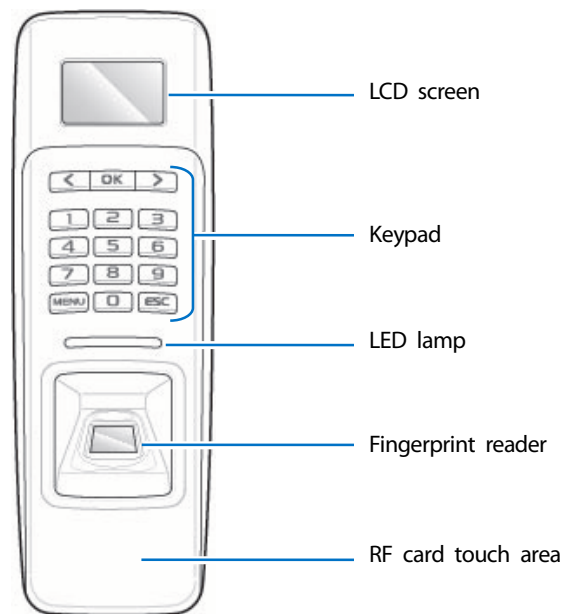
Hex wrench  
(for mounting bracket)Diode  
(1 pc)

Adapter

### Note

- The components may differ depending on where the product is installed.
- For more information about installation, visit [www.supremainc.com](http://www.supremainc.com).

## Part names and features



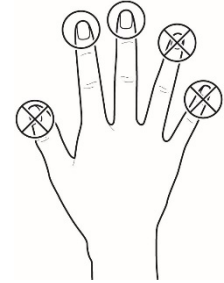
Name	Feature
<b>LCD screen</b>	Displays various information or settings.
<b>Keypad</b>	<ul style="list-style-type: none"> <li>• 0–9 buttons: For entering an ID or password.</li> <li>• &lt; &gt; direction button: Navigates to an item. When entering numbers or an IP address, the &lt; button can be used to delete the value entered.</li> <li>• <b>OK</b> button: Chooses a function.</li> <li>• <b>MENU</b> button: Enters or exits a menu.</li> <li>• <b>ESC</b> button: Moves back to the previous screen or cancels an input.</li> </ul>
<b>LED lamp</b>	<p>Shows the status of the product with different colors and beeps.</p> <ul style="list-style-type: none"> <li>• Green: Authentication success.</li> <li>• Red: Authentication failure.</li> <li>• Pink: Processing.</li> <li>• Blue and yellow alternate flashing every 2 seconds: The IP address has not been received via <b>DHCP</b> in <b>Device IP</b> configuration.</li> <li>• Blue and sky-blue alternate flashing every 2 seconds: Normal operation.</li> <li>• Red and pink alternative flashing every 2 seconds: The device is locked or no administrator.</li> <li>• Blue and red alternate flashing every 2 seconds: The clock has been reset due to an empty internal battery. (The clock needs to be reconfigured.)</li> <li>• Red flashes every 2 seconds on first use: Failure to reset. Contact the manufacturer.</li> <li>• Yellow flashes briefly: Waiting for an input.</li> </ul>
<b>Fingerprint reader</b>	Reads fingerprints placed on it for entering and exiting.
<b>RF card touch area</b>	Reads RF cards for entering and exiting.

## How to Scan a Fingerprint

Register a fingerprint correctly to improve the recognition rate of the fingerprint. BioLite Net can read a fingerprint even when the angle or position of the finger has changed. If you register a fingerprint with the following instructions, the recognition rate can be improved.

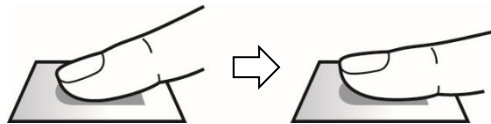
### Choosing a finger for registration

- Each person can register up to 10 fingerprints. If some fingers were injured or used to carry something, they should not be used.
- If a fingerprint is not well scanned, the fingerprint can be registered twice, which improves the recognition rate.
- If a finger is injured or the fingerprint is not clear, please use another finger for registering.
- The index finger or middle finger is preferred for registering a fingerprint. The other fingers may show a lower recognition rate because those fingers tend to have difficulty being placed at the center of the fingerprint reader.



### How to register a fingerprint

- 1 When “Scan 1st finger” message appears on the LCD screen for the fingerprint registration, place a finger on the fingerprint recognition area and then press softly in order to improve the recognition.



- 2 After a beep sounds and a screen appears to scan again, scan the finger again. (The finger should be scanned twice for registering.)

#### Note

##### Precautions for registering a fingerprint

Registering a finger is the most important procedure because this device uses the registered fingerprint to compare it with a fingerprint that the device tries to read. Please ensure the following when registering a fingerprint:

- Place a finger firmly on the fingerprint reader for it to be read completely.
- The center of the fingerprint should be placed at the center of the fingerprint reader.
- If a finger is injured or the fingerprint is not clear, please use another finger for registering.
- Follow the instructions on the screen and place the finger correctly without movement when a finger is read.
- If the finger is lifted up, not placed at the center, or only part of the finger is placed on the fingerprint reader, the fingerprint may not register.



##### Precautions for reading a fingerprint

BioLite Net can read fingerprints regardless of the change in seasons or condition of the fingers. However, the external environment or the finger's placement can affect the recognition rate.

If a fingerprint is not well read, the following actions are recommended.

- If there is water or sweat on the finger, please wipe it off before placing the finger.
- If the finger is too dry, please blow softly on the fingertip before placing the finger.
- If the finger is injured, please register another finger.
- The fingerprint that is registered on the first attempt tends to be placed incorrectly. So, register a fingerprint multiple times according to 'Precautions for registering a fingerprint'.






# User Management

## Registering User Information

User information including fingerprints can be registered.

### Note

- User information cannot be registered if  **RS-485 Mode** is set to **Slave**. Refer to **RS-485 Mode configuration** in order to change the communication mode.

- 1** Press the **MENU** button, and then authenticate with the administrator authentication method.
- 2** Select  **User** >  **Add User**, and then press **OK** button.
- 3** Enter the ID of the user to be registered, and then Press **OK** button.
  - The ID can be a number of 1–4294967294.
- 4** Select the number of fingerprints of the user to be registered, and then press **OK** button. After scanning the fingerprint of the registered finger, the same finger should be scanned one more time.
  - If the number of fingerprints is set to 0, the user cannot use a fingerprint for authentication.
- 5** Select the number of cards to be registered, and then press **OK** button. Scan the card that will be assigned to the user.
  - If the number of cards is set to 0, the user cannot use a card for authentication.
- 6** Select User Level, and then press **OK** button.
  - **Normal**: indicates the level of normal users who cannot use the configuration menu.
  - **User Mgmt**: can register or change the user information.
  - **Configuration**: can change the configurations such as screen/sound, device, or communication.
  - **Administrator**: can use every configuration menu.
- 7** Enter a PIN, and then press **OK** button. Enter the PIN again for confirmation, and then press **OK** button.


### Note

- To prevent the unauthorized user from the menu, you must register the **Administrator**.
- Keep the ID in a separate place after writing down because it will be used for changing or deleting user information.
- More than two fingerprints per user ID can be registered in order to improve the fingerprint recognition rate.
- Enter a number of 4–16 digits to prevent leaking of the PIN.




## Changing User Information

User administrator or Super administrator can change the information of a registered user. They can add the fingerprints or card of the user, and also change PIN or authority.




### Note

- User information cannot be changed if  **RS-485 Mode** is set to **Slave**. Refer to **RS-485 Mode configuration** in order to change the communication mode.

### Changing or Adding a fingerprint

- 1 Press the **MENU** button, and then authenticate with the administrator authentication method.
- 2 Select  **User** >  **Edit User**, and then press **OK** button.
- 3 Enter the ID of the user to be changed, and then press **OK** button.
- 4 Select  **Fingerprint**, and then press **OK** button.
- 5 Select the fingerprint number to be changed or **New**, and then press **OK** button.
- 6 After scanning a fingerprint, the same finger should be scanned one more time.




### Changing PIN

- 1 Press the **MENU** button, and then authenticate with the administrator authentication method.
- 2 Select  **User** >  **Edit User**, and then press **OK** button.
- 3 Enter the ID of the user to be changed, and then press **OK** button.
- 4 Select  **PIN**, and then press **OK** button.
- 5 Enter a new PIN, and then press **OK** button.
- 6 Enter the PIN again for confirmation, and then press **OK** button.




### Note

- Enter a number of 4–16 digits to prevent leaking of the PIN.

### Changing or Adding a card

- 1 Press the **MENU** button, and then authenticate with the administrator authentication method.
- 2 Select  **User** >  **Edit User**, and then press **OK** button.
- 3 Enter the ID of the user to be changed, and then press **OK** button.
- 4 Select  **Card**, and then press **OK** button.
- 5 Select the card number to be changed or added, and then press **OK** button.
- 6 Scan a card.


## Changing authority



- 1 Press the **MENU** button, and then authenticate with the administrator authentication method.
- 2 Select  **User** >  **Edit User**, and then press **OK** button.
- 3 Enter the ID of the user to be changed, and then press **OK** button.
- 4 Select  **User Level**, and then press **OK** button.
- 5 Select a new authority, and then press **OK** button.
  - **Normal**: cannot use every menu.
  - **User Mgmt**: can use only **User** menu.
  - **Configuration**: can use every menu except User menu.
  - **Administrator**: can use every menu.

## Deleting a User



A registered user can be deleted.

### Note

- User information cannot be deleted if  **RS-485 Mode** is set to **Slave**. Refer to **RS-485 Mode configuration** in order to change the communication mode.

- 1 Press the **MENU** button, and then authenticate with the administrator authentication method.
- 2 Select  **User** >  **Delete User**, and then press **OK** button.
- 3 Enter the ID of the user to be deleted, and the press **OK** button.
- 4 Press **OK** button to confirm the deletion.


### Note



- The deleted user cannot be restored. If necessary, the user should be registered as a new user.
- Use  **User** >  **Delete all users** menu in order to delete all users.

## Checking User Capacity Status

The information including the number of registered users, fingerprints, or cards can be looked up.

### Note

- User registration status cannot be looked up if  **RS-485 Mode** is set to **Slave**. Refer to **RS-485 Mode configuration** in order to change the communication mode.

- 1 Press the **MENU** button, and then authenticate with the administrator authentication method.
- 2 Select  **User** >  **User Capacity**, and then press **OK** button.
- 3 The capacity status will appear.

# Authentication Configuration

## Fingerprint Authentication configuration

A schedule can be configured for each authentication method using fingerprints.

### Note

- Fingerprint authentication mode cannot be configured if **MODE RS-485 Mode** is set to **Slave**. Refer to **RS-485 Mode configuration** in order to change the communication mode.

- Press the **MENU** button, and then authenticate with the administrator authentication method.
- Select **Authentication** > **Finger**, and then press **OK** button.
- Select the authentication mode that you want, press **OK** button.
  - Fingerprint**: This mode uses only a fingerprint.
  - Finger+PIN**: After recognizing a fingerprint, a PIN should be entered.
- Select a schedule to be used, and then press **OK** button.

### Note

- A new schedule can be registered in BioStar. Refer to BioStar administrator manual for details.

## Card Authentication configuration

A schedule can be configured for each authentication method using cards.

### Note

- Card authentication mode cannot be configured if **MODE RS-485 Mode** is set to **Slave**. Refer to **RS-485 Mode configuration** in order to change the communication mode.

- Press the **MENU** button, and then authenticate with the administrator authentication method.
- Select **Authentication** > **Card**, and then press **OK** button.
- Select the authentication mode that you want, press **OK** button.
  - Card**: This mode uses only a card.
  - Card+Finger**: After authenticating a card, a fingerprint should be recognized.
  - Card+PIN**: After authenticating a card, a PIN should be entered.
  - Card+Finger/PIN**: After authenticating a card, either a fingerprint should be recognized or a PIN should be entered.
  - Card+Finger+PIN**: After authenticating a card, both the fingerprint recognition and the PIN entering are needed.
- Select a schedule to be used, and then press **OK** button.

### Note

- A new schedule can be registered in BioStar. Refer to BioStar administrator manual for details.





## ID Authentication configuration

A schedule can be configured for each authentication method using IDs.

### Note

- ID authentication mode cannot be configured if **MODE RS-485 Mode** is set to **Slave**. Refer to **RS-485 Mode configuration** in order to change the communication mode.

- Press the **MENU** button, and then authenticate with the administrator authentication method.
- Select **Authentication** > **ID**, and then press **OK** button.
- Select the authentication mode that you want, press **OK** button.

-  **ID+Finger**: After entering an ID, a fingerprint should be recognized.
-  **ID+PIN**: After entering an ID, a PIN should be entered.
-  **ID+Finger/PIN**: After entering an ID, either a fingerprint should be recognized or a PIN should be entered.
-  **ID+Finger+PIN**: After entering an ID, both the fingerprint recognition and the PIN entering are needed.

**4** Select a schedule to be used, and then press **OK** button.


#### Note

- A new schedule can be registered in BioStar. Refer to BioStar administrator manual for details.

## Matching Timeout configuration

For the server matching, a timeout can be configured. If the server matching is not completed within the configured time, the authentication fails.

#### Note

- The time for Server matching cannot be configured if  **RS-485 Mode** is set to **Slave**. Refer to **RS-485 Mode configuration** in order to change the communication mode.

**1** Press the **MENU** button, and then authenticate with the administrator authentication method.


**2** Select  **Authentication** >  **Matching Timeout**, and then press **OK** button.

**3** Select the time that you want, and then press **OK** button.

## Scan Timeout configuration

For the user authentication, a timeout can be configured. If the user authentication is not completed within the configured time, the authentication fails.

#### Note

- Authentication time cannot be configured if  **RS-485 Mode** is set to **Slave**. Refer to **RS-485 Mode configuration** in order to change the communication mode.

**1** Press the **MENU** button, and then authenticate with the administrator authentication method.



**2** Select  **Authentication** >  **Scan Timeout**, and then press **OK** button.

**3** Select the time that you want, and then press **OK** button.

# Display/Sound Configuration



## Backlight Timeout configuration

The time to turn off the light of LCD screen can be configured.

- 1 Press the **MENU** button, and then authenticate with the administrator authentication method.
- 2 Select  **Display/Sound** >  **Backlight Timeout**, and then press **OK** button.
- 3 Select the time that you want, and then press **OK** button.



## Menu Timeout configuration

The time to make the menu screen disappear can be configured. If there is no button input within the configured time, the display is changed to the Home screen.


- 1 Press the **MENU** button, and then authenticate with the administrator authentication method.
- 2 Select  **Display/Sound** >  **Menu Timeout**, and then press **OK** button.
- 3 Select the time that you want, and then press **OK** button.

## Message Timeout configuration

The time for the configuration completion message or notification message to disappear automatically can be configured.



- 1 Press the **MENU** button, and then authenticate with the administrator authentication method.
- 2 Select  **Display/Sound** >  **Msg Timeout**, and then press **OK** button.
- 3 Select the time that you want, and then press **OK** button.

### Note

- If  **RS-485 Mode** is set to **Slave**, slave device operates according to timeout setting of master device. Refer to **RS-485 Mode configuration** in order to change the communication mode.



## Language selection

The system language can be configured.

- 1 Press the **MENU** button, and then authenticate with the administrator authentication method.
- 2 Select  **Display/Sound** >  **Language**, and then press **OK** button.
- 3 Select the language that you want, and then press **OK** button.

## Sound configuration



The sound can be turned on or off by configuration.

- 1 Press the **MENU** button, and then authenticate with the administrator authentication method.
- 2 Select  **Display/Sound** >  **Sound**, and then press **OK** button.
- 3 Choose whether the sound is on or off, and then **OK** button.

# Device Configuration



## Checking Device Information

Device ID, F/W version, or MAC address can be displayed.

- 1 Press the **MENU** button, and then authenticate with the administrator authentication method.
- 2 Select  **Device** >  **Device Info**, and then press **OK** button.
- 3 Direction buttons can be used to navigate the screen to find out the device information.
- 4 Press **ESC** button to get back the previous screen.


## Date/Time configuration

Current date and time can be configured. Date and time should be configured to get the correct log data.

- 1 Press the **MENU** button, and then authenticate with the administrator authentication method.
- 2 Select  **Device** >  **Date/Time**, and then press **OK** button.
- 3 Enter the current date in the requested format, and then press **OK** button.
  - For example, the date of November 15th, 2014 is entered by pressing '20141115' at the keypad.
- 4 Enter the current time in the requested format, and then press **OK** button.
  - For example, the time of 5:20PM is entered by pressing '172055' at the keypad.

## Fingerprint configuration




### Template Type configuration

- 1 Press the **MENU** button, and then authenticate with the administrator authentication method.
- 2 Select  **Device** >  **Fingerprint** >  **Template Type**, and then press **OK** button.
- 3 Select the fingerprint template type that you want, and then press **OK** button.
  - **SUPREMA / ISO 19794-2 / ANSI-378**

#### Note

- After deleting all the user fingerprint information, change the template type. If there is any user fingerprint information, the template type cannot be changed.




### Security Level configuration

- 1 Press the **MENU** button, and then authenticate with the administrator authentication method.
- 2 Select  **Device** >  **Fingerprint** >  **Security Level**, and then press **OK** button.
- 3 Select the security level that you want, and then press **OK** button.
  - **Normal / Secure / Most Secure**




#### Note

- As the security level becomes higher, the recognition fail rate may increase.

### Authentication Speed (Fast Mode) configuration






- 1 Press the **MENU** button, and then authenticate with the administrator authentication method.
- 2 Select  **Device** >  **Fingerprint** >  **FastMode**, and then press **OK** button.
- 3 Select the authentication speed that you want, and then press **OK** button.
  - **Auto / Normal / Fast / Fastest**

### Sensitivity configuration

- 1 Press the **MENU** button, and then authenticate with the administrator authentication method.
- 2 Select  **Device** >  **Fingerprint** >  **Sensitivity**, and then press **OK** button.
- 3 Select the sensitivity that you want, and then press **OK** button.
  - The sensitivity can be set in the range of 1–7, and as the value becomes larger, the fingerprint sensor operates more sensitively.

### How to configure a Relay

Follow the steps below to configure the relay settings. This should be done only when the device does not have any door settings transferred from BioStar since configuring both the relay settings and the door settings could cause an unexpected operation of the relay.

- 1 Press the **MENU** button, and then authenticate with the administrator authentication method.
- 2 Select  **Device** >  **Door** >  **Relay**, and then press the **OK** button.
- 3 Press the **OK** button after entering the time that the relay is on.
- 4 Press the **OK** button after entering the time that you want.
- 5 Select  **Door Sensor**, and then press the **OK** button.
- 6 Press the **OK** button after selecting the port that will be used to control the door sensor.
- 7 Select  **Exit Button**, and then press the **OK** button.
- 8 Press the **OK** button after selecting the port that will be used to control the exit button.

#### Note




- The **INIT** switch of Secure I/O 2 should be pressed after completing the relay setup when Secure I/O 2 is used together.
- Refer to BioStar administrator guide when setting up the door with BioStar.



# Communication Configuration

## TCP/IP configuration




### Server IP configuration

- 1 Press the **MENU** button, and then authenticate with the administrator authentication method.
- 2 Select  **Communication** >  **IP Address** >  **Server IP**, and then press **OK** button.
- 3 Select whether to use server.
- 4 If set **Server Discovery** to **Enabled**, entering IP address and port, and then press **OK** button.

#### Note

- When entering IP, a period (.) can be entered by pressing the > button on the keypad.

### Device IP configuration




- 1 Press the **MENU** button, and then authenticate with the administrator authentication method.
- 2 Select  **Communication** >  **IP Address** >  **Device IP**, and then press **OK** button.
- 3 In order to use a dynamic IP, set **DHCP** to **Enabled**, and then press **OK** button.
- 4 In order to set the IP value directly, set **DHCP** to **Disabled**. After entering **Device IP**, **Gateway**, **Subnet mask**, and **Device Port**, press **OK** button.

#### Note




- When entering IP, a period (.) can be entered by pressing the > button on the keypad.

## RS-485 configuration




### RS-485 Mode configuration

- 1 Press the **MENU** button, and then authenticate with the administrator authentication method.
- 2 Select  **Communication** >  **RS485** >  **RS-485 Mode**, and then press **OK** button.
- 3 Select the communication mode that you want, and then press **OK** button.

### Baud Rate configuration

- 1 Press the **MENU** button, and then authenticate with the administrator authentication method.
- 2 Select  **Communication** >  **RS485** >  **Baud Rate**, and then press **OK** button.
- 3 Select the baud rate that you want, and then press **OK** button.




### Termination configuration

- 1 Press **MENU** button, and then get authenticated with the administrator authority authentication method.
- 2 Select  **Communication** >  **RS485** >  **Termination**, and then press **OK** button.
- 3 Select whether the termination is used or not, and then press **OK** button.
  - If a connection wire is too long when connecting by RS-485, this can be used to enhance the signal strength.

## Device Reset


### Full Reset

All user information and configuration information are initialized.

- 1 Press the **MENU** button, and then authenticate with the administrator authentication method.
- 2 Select  **Device** >  **Device Reset** >  **Full Reset**, and then press **OK** button.
- 3 In order to conduct the initialization, press **OK** button.




### Reset Without Net

The communication configurations such as Server IP or RS-485 configuration are not initialized.

- 1 Press the **MENU** button, and then authenticate with the administrator authentication method.
- 2 Select  **Device** >  **Device Reset** >  **Config+IP Reset**, and then press **OK** button.
- 3 In order to conduct the initialization, press **OK** button.

### Reboot

The device can reboot.

- 1 Press the **MENU** button, and then authenticate with the administrator authentication method.
- 2 Select  **Device** >  **Device Reset** >  **Reboot**, and then press **OK** button.

# Troubleshooting

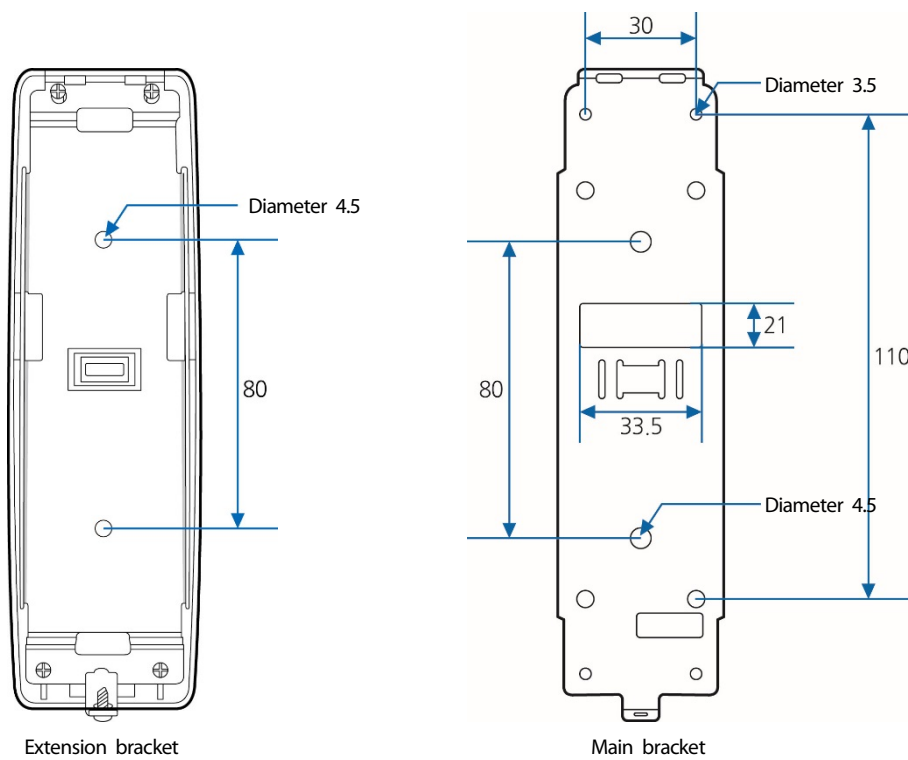
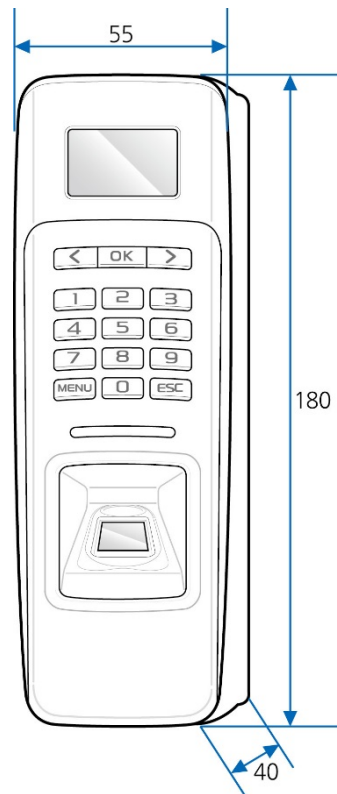
## Checklist before Requesting Service

Category	Problem	Solution
<b>Power</b>	Power is supplied to the device, but the device does not work.	<ul style="list-style-type: none"> <li>• If the terminal is apart from the bracket, it may not work due to the tamper switch.</li> <li>• Check the adapter or power connection cable.</li> </ul>
<b>PIN</b>	I've lost my PIN.	<ul style="list-style-type: none"> <li>• For a normal user's PIN, contact your administrator and then enter PIN again.</li> <li>• If an administration's PIN is lost, contact your installer.</li> </ul>
	I cannot open a locked door when I enter a PIN and then press the <b>OK</b> button.	<ul style="list-style-type: none"> <li>• Check whether the registered PIN is entered correctly.</li> <li>• Check whether PIN has recently been changed.</li> <li>• If you cannot find the PIN, ask an administrator to enter PIN again.</li> </ul>
<b>Fingerprint sensor</b>	A fingerprint is registered successfully, but it is not well recognized and suffers a lot of errors.	<ul style="list-style-type: none"> <li>• Refer to '<b>How to Register a fingerprint</b>', and then register the fingerprint again.</li> <li>• Since there would be a variation of recognition rate due to the different characteristics of each fingerprint, please try to register another fingerprint.</li> </ul>
	The fingerprint recognition does not work.	<ul style="list-style-type: none"> <li>• Check whether the finger or the fingerprint sensor has sweat, water, or dust on it, and then wipe it clear.</li> <li>• If a finger is injured, the finger may be recognized as another person's finger.</li> <li>• Try again after clearing the finger and the fingerprint sensor with a dry cloth.</li> <li>• If the finger is too dry, try again after blowing gently on the finger.</li> </ul>
<b>Door lock</b>	The locking device does not work when the door is closed.	<ul style="list-style-type: none"> <li>• The electrical locking device may have a problem. Ask your installer to get it examined.</li> </ul>
<b>Time</b>	The time displayed is not correct.	<ul style="list-style-type: none"> <li>• Even though BioLite Net includes an internal battery, the time could become incorrect due to the discharge of the internal battery if power has not been applied to the system for a long time. Refer to <b>Date/Time configuration</b> in order to adjust the time.</li> </ul>
<b>Administrator Connection</b>	The administrator mode cannot be accessed due to the loss of administrator PIN or the resignation of the administrator.	<ul style="list-style-type: none"> <li>• Since in BioLite Net administrators are in charge of permitting the right of entrance, only the administrators can access the menu.</li> <li>• If it is inevitable to access the administrator menu, it is possible to get a PIN issued in accordance with the predefined procedure. Ask your installer about the procedure to issue a password.</li> </ul>

## Product Specifications

Category	Feature	Specification
Main	Biometric	Fingerprint
	IP Rating	IP 65
	RF Card	125KHz EM, 13.56MHz Mifare/DESFire
	Multi-Controller	Yes
Capacity	Max. User (1:1)	5,000
	Max. User (1:N)	5,000
	Max. Template (1:1)	10,000
	Max. Template (1:N)	10,000
	Max. Text Log	50,000
Interface	TCP/IP	Yes
	RS-485	1ch Host or Slave (Selectable)
	Wiegand	1ch In or Out (Selectable)
	TTL Input	2 Inputs
	Relay	1 Relay
Relay	Voltage	Max. 24VDC
	Current	Typ. 0.5A, Max. 1.0A
Hardware	CPU	533MHz DSP
	Memory	16MB RAM + 8MB Flash
	LCD	128 x 64 Graphic LCD (Mono)
	LED	Multi-Color
	Sound	Multi-tone Buzzer
	Operating Temp.	-20°C ~ 50°C
	Tamper	Yes
	Power	12VDC
	Dimensions (W x H x D mm)	60 x 185 x 40
	Certification	CE, FCC, MSIP(KCC), RoHS

## Dimensions



## FCC Compliance Information

THIS DEVICE COMPLIES WITH PART 15 OF THE FCC RULES.

Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference, and
- (2) This device must accept any interference received, including interference that may cause undesired operation.

Note: 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.

# Appendix

## Disclaimers

- This document provides the information pertaining to Suprema's products.
- The right of use is granted only to the products that are covered by the sales agreement and conditions guaranteed by Suprema. Any license of intellectual property that is not dealt within this document is not granted.
- Suprema does not provide any warranty or liability of fitness or merchantability for a particular purpose and of infringement of patents, copyrights, or other intellectual properties, regarding the sales or use of Suprema's products.
- Do not use Suprema's products in either circumstances where people could be hurt or die as a consequence of malfunctions of the products or circumstances related to medical treatments, the rescue of lives, or life supports. If a user suffers an accident in one of the circumstances mentioned above, employees, subsidiaries, branches, partners, and distributors of Suprema are exempt from liability even when it is claimed that there is a significant fault in the design or production process, and also they are not liable for any direct or indirect cost or expenditure including legal costs.
- Suprema can change the standard and specification of its products anytime without notice in order to improve the stability, functions, or design of the products. Designers should keep in mind that the functions or explanations denoted as "to be implemented" or "not defined" can be changed anytime. Suprema will implement or define such items in the shortest possible time, and will not accept any liability for problems incurred including compatibility issues.
- Contact Suprema, sales representatives of Suprema, or local distributors in order to get the latest specifications before ordering products.

## Copyright Notice

Suprema has the copyright of this document. The rights of other product names, brands, and trademarks belong to individuals or organizations who own them.



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

---

Suprema Inc. 16F Parkview Office Tower, Jeongja-dong, Bundang-gu Seongnam, Gyeonggi, 463-863 Korea  
Tel) +82-31-783-4502 Fax) +82-31-783-4503

**Sales information** [sales@supremainc.com](mailto:sales@supremainc.com) **Technical support** [support@supremainc.com](mailto:support@supremainc.com)