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

Contents

Safety Instructions

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.

Do not clean the device with any form of liquid. Use soft and dry cloth only.
It may cause a failure.
Do not forcibly press the buttons of the product and avoid any contact with sharp object to the device. Be cautioned for the fingerprint contact area not to be contaminated or damaged by dirty hands or foreign materials.
It may affect fingerprint recognition performance or cause a failure.
Endure that password does not exposed to unauthorized individuals. Frequent change of password is recommended.
Any illegal access to your product may happen.

1. Before Use

1.1 Components

Main Body **Wall mounting bracket** **Extended bracket (Option)**
Shrinkable Tubes
Fixing Screws **Ethernet Connector** (2 EA)
Knife Blocks (2 EA)

Star-shape wrench
(For fixing bracket)
Adapter
(Option)
The components shown above may differ depending on the installation environment.

1.2 Body

(5) RF Card reading part
Key Pad
Fingerprint Touch Area
LED Lamp
LCD Display

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.
Button: Used to select the desired function.
Button: Used to enter or exit the menu.
Button: Used to exit from the menu or cancel the desired action.
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.)

Finger
Place the first

In case fingerprint is not recognized normally

3. When you have a cut on your registered finger, register another fingerprint.
1. Retry after drying the wetness of your finger.
2. When your finger is too dry, retry after blowing on your fingertip.
In abnormal cases, follow the directions below:
However, the recognition rate may vary depending on the external environment or fingerprint condition.
BioLite Net is designed to normally operate regardless of weather change or the angle and location of the fingerprint to place.

Cautions while registering your fingerprint

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. Put the center of your fingerprint on the middle of the sensor.
To increase the recognition rate, follow the directions below:
Because the recognition process compares the scanned fingerprint with the registered one, an abnormally registered fingerprint can cause a failure.
The initial fingerprint registration is important.

1.4 System setup procedure

Step 1 - Grasp the locations for installation site, door open switch, dead bolt, and such.
- Install the system (see 6.4).

Install the system according to the environment

Step 2 - Register the initial administrator for setting devices (See 1.4.1).

Register an initial administrator

Configure the system

Step 3 - Network configuration (see 1.4.2)
- Stand alone configuration (see 1.4.3.) or
Secure I/O configuration (see 1.4.4)

Configure the environment

Step 5 - Configure various environments (see 1.4.5).

Step 4 - Check the door lock/unlock status and switch operation.

- Deliver the setting items to the customer.

Test for system operation

Step 6 - Use the system after user registration (see 2.1).

Register users

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.

Enter ID
1
Enroll Admin

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**.

Enroll
PIN Only
Operation Mode

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

Enter PIN
****
Enroll

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

Confirm PIN
****
Enroll

5. The completion message window appears.

Completed

This procedure is necessary to temporarily configure the installationrelated 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.

Item
TCP/IP
Device In/Out In/Out
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 the **TCP/IP** and press **OK**.
TCP/IP
DHCP
Not Use 192.168.1.35
TCP/IP
IP Address
TCP/IP
Gateway
192.168.1.10
Enter the IP address and press **OK**.
Enter the Gateway using numeric and arrow buttons and press **OK**.
Use □/□ buttons to set whether or not to use DHCP and press **OK.**
TCP/IP
Subnet Mask
255.255.255.0
TCP/IP
Port
1471
TCP/IP
Use
Server
Use □/□ buttons to select the **Use** and press **OK**.
Enter IP address using numeric and arrow button and press **OK**.
Server IP
192.168.1.30
TCP/IP
Enter Server Port and press **OK**.
Enter Server IP address using numeric and arrow button and press **OK**.
TCP/IP
1480
Server Port

Enter Port and
press **OK**.
Cont.

□□

□

□□□

□**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.)
The completion
message window
appears.□□
Use □/□ buttons to
set whether or not to
support 100Base-T
and press **OK**.
100 ort
N t
Base-T supp
ot suppor
□
Completed
TCP/IP □
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.
□

[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.

Device In/Out
Use □/□ buttons to
select the **In/Out** icon
and press **OK**.
Use □/□ buttons to
select the **Serial Conn.**
and press **OK**.
Completed
Use □/□ buttons to
select **115200** for PC
connection speed and
press **OK.**
Use □/□ buttons to
select Not Use for
termination and press
□□□□

Baudrate
115200
Serial Conn.
Type
PC Conn.
Serial Conn.
Termination
Use □/□ buttons to select the **Device** icon and press **OK**.
Use □/□ buttons to select the **PC Conn.** and press **OK**.
Serial Conn.
Not Use
Item
Serial Conn.
In/Out
The completion message window appears.

□

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.

2. Configure the internal relay settings as shown below. (It is explained based on the figure above.)
For actual wring method, see "6.4 System Installation."□□
Follow the instructions below only when the dedicated PC software is not used. When using the software, refer to the software manual.□
In/Out
Door
Item
Device In/Out
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
Relay
Internal
Door
Exit Button
Use □/□ buttons to select the **In/Out** icon and press **OK**.
Press **MENU** -> Enter ID -> Enter the password ->

Use □/□ buttons to select the **Device** icon and press **OK**.
Use □/□ buttons to select **Door** and press **OK**.
Type
N.O
Exit Button
Input 0
Internal
Cont.
□
Door Sensor
Input 1
Internal
Use □/□ buttons to select **Input 1** and press **OK**.
*Not Use/Input0/Input1□
Use □/□ buttons to select **N.O** and press **OK**.
Type
N.O
Door Sensor
*N.O/N.C□
Use □/□ buttons to select **Temporary Open** for opening mode and press **OK**.
Door
Temporary Open
Opening Mode
* Temporary Open/ Toggle□
Enter the time and press **OK**.
*The time is set for automatically closing the door after the specified time.
Use □/□ buttons to select **Not Use** for Held Open Alarm and press **OK**.
*Not Use/Sound/ Backlight/Sound and Light/SIO Relay0/SIO Relay1
Held Open Alarm
Not Use
Door
Open Time
3
Door
Use □/□ buttons to select **Not Use** for Forced Open Alarm and press **OK**.
*Not Use/Sound/ Backlight/Sound and Light/SIO Relay0/ SIO

Relay1□
Complete
Forced Open Alarm
Not Use
Door
The completion message window appears.
□
□ **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.
□
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.

Cont.

For actual wiring, see "6.4 System Installation."

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

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

Device In/Out
Use □/□ buttons to select the **In/Out** icon and press **OK**.
Press **Menu** -> Enter ID -> Enter password ->Use□/□ buttons to select the **Device** icon and press **OK**.
In/Out
Item
Door
Use □/□ buttons to select **Door** and press **OK**.
Type
N.O
Exit Button
Relay
SIO Relay 0
Door
Exit Button
SIO Input 0
SIO Relay 0
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**.
□

□□

□**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.

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.”

□**Sync. Button**
(In case of using Secure I/O)
Sync. button should be pressed when Relay setting is completed.□
Enter the time and press **OK**.
*The time is set for automatically closing the door after the specified time□□
Use □/□ buttons to select **Not Use** for Held Open Alarm and press **OK**.
*Not Use/Sound/Backlight/ Sound & Light/SIO Relay0/ SIO Relay1□
Door Sensor
SIO Input 1
SIO Relay 0
Held Open Alarm
Not Use
Door
Use □/□ buttons to select **N.O** and press **OK**.
Use □/□ buttons to select **SIO Input 1** and press **OK**.
*Not Use/ SIO Input0/ SIO Input1□
Type Opening Mode
Temporary Open
Door
Use □/□ buttons to select **Temporary Open** for opening mode and press **OK**.
* Temporary Open/Toggle□
N.O
Door Sensor

Open Time(sec)
3
Door
Forced Open Alarm
Use □/□ buttons to
select **Not Use** for
Forced Open Alarm and
press **OK**.
*Not Use/Sound/Backlight/
Sound & Light/SIO Relay0/
SIO Relay1□
The completion message
window appears□□
Not Use
Door
Complete
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.□

□

1.5 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

□□□

Fingerprint recognition after entering ID

Input the fingerprint of
the user.
The door is open with
the authentication
success message.
BioLite Net Access Granted
10:33:02 ID : 2
BioLite Net Enter ID
2
10:33:02
Enter the ID of the
user and press **OK**.
Input the fingerprint
of the user.
Access Granted
ID : 2
The door is open with
the authentication
success message.

□

Fingerprint recognition after identifying user card

BioLite Net

10:33:02
Place the user card on the
SUPREMA logo area.
Input the fingerprint
of the user.
Access Granted
ID : 2
The door is open with the
authentication success message.

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

BioLite Net **Access Granted**
10:33:02 **ID : 2**
The door is open with
the authentication
success message.
Input the fingerprint
of the user.

Fingerprint recognition after entering ID
PIN entry after entering ID
Fingerprint recognition after identifying user card
Enter Finger or PIN
****

BioLite Net **Enter ID**
2
10:33:02
Enter the ID of the
user and press **OK**.
Input the fingerprint of
the user.
The door is open with the
authentication success
message.
Access Granted
ID : 2

BioLite Net **Enter ID**
2
10:33:02
Enter the ID of the
user and press **OK**.
Enter the password
of the user and
press **OK**.
Access Granted
ID : 2

The door is open with
the authentication
success message.

BioLite Net

10:33:02

Input the fingerprint
of the user.
The door is open with the
authentication success
message.
Place the user card on the
SUPREMA logo area.
Access Granted
ID : 2

PIN entry after identifying the user card

BioLite Net **Enter Finger or PIN**

10:33:02 ****

Enter the password
of the user and
press **OK**.
Place the user card on the
SUPREMA logo area.
Access Granted
ID : 2
The door is open with
the authentication
success message.

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

The door is open with the
authentication success
message.
Access Granted
ID : 2
Enter PIN

**** **BioLite Net**

10:33:02

Input the fingerprint
of the user.
Enter the password
of the user and
press **OK**.

BioLite Net **Enter ID**

2

10:33:02

Enter the ID of the

user and press **OK**.
Input the fingerprint
of the user.
The door is open with
the authentication
success message.
Enter PIN
Access Granted
****
ID : 2
Enter the password
of the user and
press **OK**.

PIN entry after entering user card and fingerprint

BioLite Net
10:33:02
Input the fingerprint
of the user.
Place the user card on the
SUPREMA logo area.

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 entering ID

The door is open with the
authentication success message.
Access Granted
ID : 2
Enter PIN
****
Enter the password
of the user and
press **OK**.
Access Granted
ID : 2
The door is open with the
authentication success message.
Enter the password
of the user and
press **OK**.
Enter the ID of the
user and press **OK**.
Enter Finger or PIN
****
BioLite Net **Enter ID**
2
10:33:02

PIN entry after identifying user card

BioLite Net **Enter Finger or PIN**
10:33:02 ********
Enter the password

of the user and
press **OK**.
Place the user card on the
SUPREMA logo area.
Access Granted
ID : 2
The door is open with the
authentication success message.

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:
Access Granted
ID : 2
BioLite Net
10:33:02
The door is open with
the authentication
success message.
Place the user card on the
SUPREMA logo area.
For “Card Only,” register the card user on the dedicated PC software first.

2. User Management

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

2.1 Enrolling a user

2.1.1 Registration on the terminal

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

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

2. Use □/□ buttons to select **Enroll** ( ) icon and press **OK**.

Enroll

3. The ID that can be used appears. Use it or enter another ID and press **OK**.
(1–8 digit number)
Enter ID
3
Enroll
ID is used to edit or delete the user data so please keep it carefully.□

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

□□□

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

Card□
Not Use□
□**Not Use/Read Card/Manual Input/User ID Enroll**
□
□**Card ID: Not Use/Read Card/Manual Input/User ID**

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

In case of Read Card

In case of Manual Input

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

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

Level
General
Enroll
Card ID
Card□ □ **2691057484**
Read Card□ **Place the Card Facility Code**
Enroll 0
Use □/□ buttons to select **Read Card** and press OK.
When identified, enter the **Facility Code**.□
Place the user card on the SUPREMA logo area.
Card□
Manual Input□
Enroll
Card ID Facility Code (0-255)
2691057484 □
Manual Input Manual Input
Directly enter the card ID through the keypad.□
Use □/□ buttons to select **Manual Input** and press OK.
Enter the Facility Code
□
□

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

□□

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

Finger Only/Finger or PIN/Finger and PIN

Place the second
Place the first Place the first

finger
finger finger again
(Skip=ESC)
Place the first finger
on the sensor.
Place the same finger
on the sensor again.
Place the second
finger in the same
manner.
In order to skip the second fingerprint enrollment after enrolling the first fingerprint, press **ESC**.
The user can enroll one or two fingerprints for passing the door.

PIN Only/ Finger and PIN

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

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

Completed
Enter PIN Confirm PIN
******* *******
Enroll Enroll

2.1.2 Registration on the card

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

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

User

2. Use / buttons to select **Enroll** ( ) icon and press **OK**.

Enroll

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

Enter ID
3
Enroll
ID is used to edit or delete the user data so please keep it carefully.

4. Use / buttons to select **Card** on the **Enroll To** and press **OK**. **Enroll To**

You can save the user information (including finger print) on your terminal or card.

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

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

Level

General
□The user enrollment and environment configuration are enabled only in Administrator level. **Enroll**
□

6. Use □/□ buttons to select Access Group and press **OK**.
Select
Full Access
Access Group1

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

□Bypass Card/Use Template
Card Type
Bypass Card
Enroll

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

In case of Bypass Card

In case of Use Template

Place the user card on the divice's logo area.
Card Type
Use □/□ buttons to select **Use Template** and press OK.
Place the desired finger on the sensor for entry.
* (1 to 4)
Enter the PIN□
Place the user card on the divice's logo area.
When the user enrollment is successfully done, the completion message window appears.
When the user enrollment is successfully done, the completion message window appears.
□In case of Mifare card, the 1K card can save up to 2 fingerprint data but the 4K card up to 4. The card layout information can be set using the PC software.□
Bypass Card
Enroll
□
Place the Card Completed□
Use □/□ buttons to select **Bypass Card** and press OK.
Completed□
□
Place the Card
Card Type
Use Template
Enroll
Enter PIN(skip=ESC)
****

Enroll
Place the first
finger

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**.

User

2. Use □/□ buttons to select the **Edit** ( ) icon and press **OK**.

Edit

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

Enter ID/Finger
4
Edit

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

Item

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

Level□
Edit
Use □/□ buttons to select **Level** and press **OK**.
Use □/□ buttons to select **General** or **Administrator**.
Press **OK**.
Level
General
Edit

Changing the authorization method

□**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

□**Security Level:** *Per Device/Lower/Low/Normal/High/Higher
- Per Device: The security level in "Device>Authorization>Fingerprint>" on page 39 is applied.
- The higher the security level, the more sensitive the fingerprint recognition. But the authorization failure rate can increase.

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**

Item
Operation Mode
Edit
Use □/□ buttons to select **Operation Mode** and press **OK**.
Use □/□ buttons to select an desired operation mode and press **OK**.
Press **OK**.
Operation Mode
Finger Only
Edit
Use □/□ buttons to select **Security Level** and press **OK**.
Use □/□ buttons to select a security level.
Item
Security Level
Edit
Security Level
Normal
Edit
Press **OK**.

□

Changing the fingerprint of the user

□ □ □

Changing the PIN of the user

Changing the access group

Item
Access Group1
Edit
Select
Full Access
Access Group1

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.

Place the first finger again
Item
Fingerprint Place the first
Edit finger
Use □/□ buttons to select **Fingerprint** and press **OK**.

Place the first finger on the sensor.
Place the same finger on the sensor again.
Place the second finger
(Skip=ESC)
Enroll the second fingerprint in the same manner.
Item
PIN
Edit
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**.
Enter PIN
****
Edit
Confirm PIN
****
Edit
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 Acce ss Group
Press **OK**.

Changing the card

Item Card
Card Read Card
Edit Edit
Use /□ buttons to select **Card** and press **OK**.
Press **OK**.
Use /□buttons to select card input type
* Not use/ Read Card/ Manual Input / User ID
Card: *Not use/Read Card/Manual Input/User ID
- **Not use**: Card is not used
- **Read Card**: User information is changed after touching a card on the terminal.
- **Manual Input**: User information is changed after entering the card ID.
- **User ID**: The corresponding user ID is changed using a card ID.

2.3 Deleting a user data

You can delete unnecessary user data.

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

2. Use □/□ buttons to select the Delete ( ) icon and press **OK**.
Delete

3. After entering the ID or finger to delete and press **OK**. **Enter ID/Finger**
4
Delete

4. When the action is successfully made, the message Deletion appears. **Deletion**
□The deleted user cannot be recovered.
If necessary, enroll it again.
- 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**.
Screen, Sound
Date, Time
Date(YYYYMM00)
20081115
Date, Time
Time(hhmmss)
102055

Date, Time

□

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

On at Use

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

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

Mode□

Always On□

Backlight

Timeout(sec)□

20

Menu Duration

Mode□

On at Use

Backlight

Timeout(sec)

20

Backlight

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

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

Screen, Sound

Backlight

Mode

Always On

Backlight

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

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

□

□□

3.3 Sound

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

Screen, Sound

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

Sound

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

Or

Mode
On
Sound
Mode
Off
Sound

□

4. Device Configuration

4.1 Authorization

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

Device

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

□

Authorization
Item
Fingerprint
Authorization
Item Item
Fingerprint
Authorization
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□
Security Level
Fingerprint
Security Level
Normal
Fingerprint
Item
Image Quality□
Fingerprint
Image Quality
Normal
Fingerprint

Cont.

Cont.

Item
Fast Mode
Fingerprint
Fast Mode
Auto
Fingerprint
Item
Scan Timeout
Fingerprint
Scan Timeout(sec)
10
Fingerprint
Item
Matching Timeout
Fingerprint
Matching Timeout(sec)
3
Fingerprint
Use / buttons to select **Sensitivity** and press **OK**.
Use / buttons to select **Sensitivity level** and press OK.

Use / buttons to select **Check Duplicate** and press **OK**.
Item
Sensitivity
Fingerprint
Sensitivity
7
Fingerprint
Item
Check Duplicate
Fingerprint
Check Duplicate
Not Use
Fingerprint
Use / buttons **Check Duplicate** and press **OK**.
* Not Use /Use
Use / buttons to select **Fast Mode** and press **OK**.
Use / buttons to select **Scan Timeout** and press **OK**.
Use / buttons to select **Matching Timeout** and press **OK**.
Enter Scan Timeout (second) and press **OK**.
Enter Matching Timeout (second)and press **OK**.

Use □/□ buttons to
select desired Fast Mode
and press **OK**.
*Auto/Normal/Fast
/Faster
□

□ □ □

Item□ Template Type
Template Type
□ **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.)
Fingerprint
SUPREMA□
Fingerprint
Use □/□ buttons to
select **Template Type**
and press **OK**.
Use □/□ buttons to
select template format
and press **OK**.
*SUPREMA/SIF
□

In case of Operation Mode

Item□ Use □/□ buttons to
select **Operation**
Mode an press OK.
Operation Mode□
Authorization

□ □

Cont.

□ **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.
□**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.
Use □/□ buttons to
select the applicable
time zone and press
OK.
Schedule
All Time□
Always On
Use □/□ buttons to
select **Sensor Mode**
an press OK.
Use □/□ buttons to
select a sensor mode.
*Always On/ID Entered/
OK Pressed
Item Sensor Mode
Sensor Mode Always On
Operation Mode Operation Mode
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**.
Finger Only
Not Use□
Double Mode□
Item□
Auth Mode
Operation Mode
Auth Mode□
Finger Only□
Operation Mode Finger Only
Schedule□
All Time□
Use □/□ buttons to
select **Auth Mode** and
press **OK**.
□

□**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.
Use □/□ buttons to
set whether or not to
use the mode and
press **OK.**□
Use □/□ buttons to set
whether or not to use
cards and press □□□□
Use □/□ buttons to
select the card entry
method and press □□□□

* Use Template/Use CSN□
Item Private Auth Mode□
Private Auth Mode Use□
Operation Mode Operation Mode
Use □/□ buttons to
select **Private Auth**
Mode an press OK.
Item□ **Card**□ **Type**□
Card□ **Use**□ **Use Template**□
Operation Operation Mode Card
Use □/□ buttons to
select **Card** an press **OK**.
□

4.2 In/Out

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

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

□ □
In/Out

3. Use □/□ buttons to select any of Serial Conn., Tamper On, Door Wiegand, and TCP/IP and press **OK**.
Item
Serial Conn.
In/Out

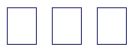
In case of Serial Conn. (selection of connection method)

Item □**Serial Conn.**: It is used for RS485 communication or direct PC connection.
Use □/□ buttons to
select **Serial Conn.** and
press **OK**.
Serial Conn.
In/Out
Use □/□ buttons to set whether or not to use the termination and press **OK**.
The completion
message window
appears.
Type Termination □
Host Not Use Completed
Serial Conn. Serial Conn.
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.□
Type Termination □
Slave Not Use
Serial Conn. Serial Conn.
Completed□

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.□
Type Termination □
Ext. Host Not Use
Serial Conn. Serial Conn.
Completed□
Use □/□ buttons to select **Ext. Host** and press **OK**.

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.
The completion message window appears.
Completed
Use □/□ buttons to set whether or not to use the termination and press **OK**.
The completion message window appears.□
Type Termination□ □
Ext. Slave□ Not Use□
Serial Conn. Serial Conn.
Completed□
Use □/□ buttons to select **Ext. Slave** and press **OK**.
Use □/□ buttons to set whether or not to use the termination and press
The completion message window appears.□
Type□ Termination□ □
Not Use□ Not Use□
Serial Conn. Serial Conn
Completed□
Use □/□ buttons to select **Not Use** and press

OK.
Use □/□ buttons to
set whether or not to
use the termination
and press **OK**.
Baudrate
115200
Serial Conn.
Type□ Termination□
PC Conn.
Serial Conn.
Not Use□
Serial Conn.
Use □/□ buttons to
select **PC Conn.** and
press **OK**.
Use □/□ buttons to
select **Baudrate** and press
OK.
*115200/57600/38400
/19200
□

In case of Tamper On

□□

Item Tamper On
□ **Tamper:** *Ignore/Locked
- Locked: When the device is forcibly removed, the Device is locked.
(To release the lock, the administrator must perform authorization.)
Tamper On
In/Out
Use □/□ buttons to Press **OK**.
select **Tamper On□**and
press **OK**.
Use □/□ buttons
to select a tamper
method.
Ignore
In/Out
□

□□□

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.

□□

□□ **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.

Item
Door
In/Out
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□
Relay
Internal
Door
Exit Button
Input 0
Internal
Use □/□ buttons to
select the type for **Exit**
Button□and press **OK**.
*N.O/N.C□
Type
N.O
Exit Button
Door Sensor
Input 1
Internal
Type
Use □/□ buttons to
select a door sensor type□
and press **OK**.
*N.O/N.C□
Use □/□ buttons to
select **Door Sensor**□and
press **OK**.
*Not Use/Input
Opening Mode
Temporary Open
Door
Held Open Alarm
Not Use
Door
Open Time(sec)
3
Door
N.O
Door Sensor
Use □/□ buttons to
select a opening mode□
and press **OK**.
Enter the time and
press **OK**.
Use □/□ buttons to select
the type for Held Open Alarm□
and press **OK**.
*Temporary Open/ Toggle□ * 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.
Forced Open Alarm
Not Use
Door
Completed
Held Open Time(sec)
30
Door
Use □/□ buttons to select the
type for Forced Open Alarm and

press **OK**.
The completion
message window
appears.
*Not Use/Sound/ Backlight/Sound
and Light/SIO Relay0/ SIO Relay1□
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.□
□

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 the relay type□and
press **OK**.
Use □/□ buttons to
select the **exit button** and
press **OK**.□
* Not Use/SIO Input0/
SIO Input1□
Relay
SIO Relay0
Door
Exit Button
SIO Input0
SIO Relay0
Item
Door
In/Out
Use □/□ buttons to
select **Door**□and press
OK.
Use □/□ buttons to select
the type of the exit button
and press **OK**.
*N.O/N.C□
Type
N.O
Exit Button
Door Sensor
SIO Input1
SIO Relay0
Type
Use □/□ buttons to
select the door sensor
type and press **OK**.
*N.O/N.C□
Use □/□ buttons to
select the door sensor
and press **OK**.
*Not Use/ SIO Input1□
N.O
Door Sensor
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□
Held Open Alarm
Sound
Door
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.
Held Open Alarm(sec)
30
Door
Opening Mode Open Time(sec)
Temporary Open
Door
Use □/□ buttons to select the type of the opening mode and press **OK**.
*Temporary Open/ Toggle□
3
Door
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.
Forced Open Alarm
Not Use
Door
Complete
□

In case of Wiegand

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

□□□

□**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.
Use □/□ buttons to select Wiegand and press **OK.**
Item Type
Wiegand Card ID In
In/Out Wiegand
*Card ID In/ Card ID Out/User ID In/ User ID Out/Not Use□
Use □/□ buttons to select **Wiegand**□and press **OK**.

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."

□

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

In case of TCP/IP

Item DHCP□ IP Address□
TCP/IP□ Not Use□ 192.168.1.35□
In/Out TCP/IP TCP/IP□

. Use □/□ buttons to select the **TCP/IP** and press **OK**.
Use □/□ buttons to set whether or not to use DHCP and press □□□□
Enter IP address and press **OK**.

□□

□**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.)

□

When you exit before finishing the TCP/IP setting, the change is not stored so proceed with the settings until the message "Completed" appears.

Gateway□
192.168.1.10□
TCP/IP
Subnet Mask□
255.255.255.0□
TCP/IP
Port□
1471□
TCP/IP□
Enter Gateway using numeric and arrow button and press **OK**.
Enter IP address using numeric and arrow button and press **OK**.
Enter Port and press **OK**.

Server□ Server IP□ Server Port□

Use□ 192.168.1.30□ 1480□
TCP/IP TCP/IP TCP/IP
Use □/□ buttons to
select the **Use** and
press **OK**.
Enter Server IP address
using numeric and arrow
button and press **OK**.
Enter Server Port and
press **OK**.
The completion
message window
appears.□
□
Completed□
□
100Base-T Support
Not Support□
TCP/IP
Use □/□ buttons to set
whether or not to
support □□□□□□□□□□
_____□□□□□□□□□□□□□□□□
□

4.3 System

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

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

System

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

In case of Information

Item
Use □/□ buttons to
Log select **Log** and press **OK**.
Information
Filter
Use □/□ buttons to
select **Not Use** and
press **OK**.
Not Use
Log
The entire logs appear.
(Use □/□ buttons to see
the previous/next logs.)
6/18 16:21(1)
Set Time□
6/18 14:20(3)
Delete OK
Use □/□ buttons to

select **Use** and press
OK.
Filter
Use
Log
User
All
Filter
Date
All
Filter
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**.
The log filtering result
appears on the screen.
(Use □/□ buttons to see
the previous/next logs.)
6/18 14:20(3)
Delete OK
6/18 13:46(3)
Enroll OK
Use □/□ buttons to select
the event type and press **OK**.
*All/Success/Failure/In/Out/
System□
Event
All
Filter
□ **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

User

In case of Factory Default

□In case of Initialize, the settings are deleted but the log data and user DB are not deleted.
Use □/□ buttons to
select **Num. Of User**
and press **OK**.
The version of the
firmware appears.
Item
Num. Of User
Information
Templates
4/5000
6/10000
Item
Firmware Ver.
Information

Firmware Ver.
V1.0_081127
Information
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
hardware appears.
Item
Hardware Ver.
Information
Hardware Ver.
11563(BLNM-OC)
Information
Use □/□ buttons to
select **Hardware Ver.**
and press **OK**.
Item Initialize?
Factory Default
System
Use □/□ buttons to
select **Factory Default**
and press **OK**.
Use □/□ buttons to
determine whether or
not to initialize it.
*Cancel/ Initialize□
Initialize
Factory Default
Initialized
In case of Initialize,
the message
Initialized appears.
□

In case of Delete All Log

Item

Use □/□ buttons to
select Delete All Log and
press **OK.**
□In this case, all users' in/out data are deleted and they cannot be recovered.

In case of Delete User DB

□

□

□In this case, the users' DB is completely deleted so you must immediately register the initial administrator (see 1.4.1).
□When the user DB is deleted, it cannot be recovered.

In case of Language

In case of Delete,
the message
Deletion appears.
Use □/□ buttons
to determine
whether or not to
delete them.
*Cancel/ Delete□
Delete All Log

System
Delete?
Delete
Delete All Log
Deletion
Item
Delete User DB
System
In case of Delete,
the message
Deletion appears.
Use □/□ buttons to
select **Delete User DB**
and press **OK**.
Use □/□ buttons
to determine
whether or not to
delete the user DB.
*Cancel/Delete
Delete?
Delete
Delete User DB
Deletion
Use □/□ buttons to
select **Language** and
press **OK**.
Use □/□ buttons
to select the
language.
* English/ Korean□
Press **OK**.
Item Item
English
Language
Language
System
□

In case of Wallpaper

Use □/□ buttons to
select **Wallpaper** and
press **OK**.
Item□ Wallpaper□
Wallpaper□
□Types
- Type1: Only the time appears on the wallpaper screen.
- Type2: The number of users and TCP/IP connection status appears
on the wallpaper screen.
In case of (8/5000) U - Eight people are registered among 5000
(number of people that can be registered) and it is unlinked.
Characters on the Type2 wallpaper
- U: Unlinked (LAN is not connected.)
- D: Disconnected (LAN is connected but TCP/IP communication is not active.)
- C: Connected (LAN is connected and TCP/IP communication is active.)

In case of Contrast

In case of Format Card

□ After formatting a card, the data on a rewritable card such as Mifare card
is removed. (The card format can be set using the PC software.)
Use □/□ buttons to
select the type and
press **OK**.□

*Type1/Type2
System
Type1□
System
□□□□□□□□□□
□□□□□□□□□□
10:33:02
10:33:02 (8/5000) U
Type1 Type2
After formatting a card, The format completion message window appears.
Place the user card on the SUPREMA logo area.
Format Card□
Completed□
Item□
Format Card□
System
□
Place the Card
□**Contrast**
Contrast value on the screen (Range: 10 to 30)
Item□ **Contrast**□
Contrast□ **17**□
System System
Use □/□ buttons to select **Contrast** and press OK.
Use □/□ buttonsto select contrast level.□
Use □/□ buttons to select **Format Card** and press OK.
□

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 abovementioned
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.
Event
□□□
□

5.2 Setup for attendance management

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

□□

Device

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

Authorization

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

Item□
Operation Mode
Authorization

4. Use □/□ buttons to select the **Time Attendance** and press **OK**. **Item□**

Time Attendance□
Operation Mode

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

Key Input□
Operation Mode

□**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.

Select□

BioLite Net In
10:33:02 Type
Select the desired event and perform user authorization.□
Move to the desired event by using □/□ buttons.
ID: 8
In
The door opens with a confirmation message.□

5.3.2 Manual

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

In case of Manual

In
BioLite Net 08:30:43

10:33:02 12/01/2008
The desired event
Move to the desired appears.
event by using □/□
buttons.

□

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.
The Users identify the card
or fingerprint according to
the authorization method.
In
08:30:43
12/01/2008
The door opens
with a confirmation
message.
ID: 8
In
The users identify the card
or fingerprint according to
the authorization method.
Out
18:35:55 ID: 8
Out
12/01/2008
The door opens
with a confirmation
message.
The event for the
corresponding time
zone appears.
□

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.
Out
18:35:55 ID: 8
Out
12/01/2008
The door opens

with a confirmation
message.
The preset event
appears.
The users identify the card
or fingerprint according to
the authorization method.
 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

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

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.

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.

Password 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.

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.

Fingerprint 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.

 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

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

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.).

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

□□

□

□□□

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.