www.supremainc.com

USER GUIDE

BioStation L2

English

Version 1.21

EN 102.00.BSL2 V1.21A

Contents

Safety Instructions 4

Introduction 6
- Components 6
- Name and function of each part 7
  - Cables and connectors 8
- How to enroll a fingerprint correctly 10
  - Selecting a finger for fingerprint input 10
  - Fingerprint enroll method 10

Admin Menu 11
- All Menus 11

User 12
- Registering user information 12
- Modifying user information 13
- Delete All Users 13
- View User Usage 13

Authentication 14
- Mode 14
  - Fingerprint Mode 14
  - Card Mode 14
  - ID Mode 15
- T&A Mode 15
- Fingerprint 16
- Server Matching 17

Display & Sound 18

Device 19
- Date & Time 19
- Relay 19
- Device Info 19
- Memory Info 20
- Restart Device 20
- Restore to default 20
- Factory Default 20
- Delete the Root Certificate 20

Network 21
- Network Settings 21
  - Ethernet 21
  - Server 21
- Serial Settings 22
  - RS-485 22

Event Log 23
- Search Log 23
- Delete All Logs 23
- View Log Usage 23

Troubleshooting 24

Checklist before reporting a failure 24

Product Specifications 25
Dimensions 26

FCC compliance information 27

Appendices 28
Escape clause 28
Copyright notice 28

Safety Instructions

Observe the following instructions to use the product safely and prevent any risk of injury or property damage.

⚠Warning

Noncompliance of instructions could lead to serious injury or death.

Installation

Do not install the product in a place with direct sunlight, moisture, dust, or soot.

- A fire or electric shock may occur.

Do not install the product in a place with heat from an electric heater.

- A fire or electric shock may occur due to overheating.

Install the product in a dry place.

- Otherwise, a product damage or electric shock may occur due to moisture.

Install the product in a place with no electromagnetic interference.

- Otherwise, a product damage or electric shock may occur.

The user should not install or repair the product independently.

- A fire, electric shock, or personal injury may occur.
- If the product has been damaged due to independent installation or repair of the product by the user, free A/S service will not be provided.

Usage

Do not allow liquids such as water, beverages, or chemicals get into the product.

- A fire, electric shock, or product damage may occur.

⚠Caution

Noncompliance of instructions could lead to minor injury or product damage.

Installation

Do not install the power supply cable in a place where people pass by.

- Product damage or physical injury may occur.

Do not install the product near a highly magnetic object such as a magnet, TV, (especially CRT) monitor, or speaker.

- A product failure may occur.

Use only a power supply adaptor of D.C 12 V and 500 mA or higher.

- If the proper power is not used, the product may not operate normally.

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 the Secure I/O 2, electric lock and BioStation L2 respectively.

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

When installing a number of devices, allow a space between the devices for installation.

- Otherwise, one device may affect the RF performance of other devices, resulting in malfunction.

Operation

Do not drop the product or apply an impact to the product.

- A product failure may occur.

Manage the password with care not to disclose it to others and change the password periodically.

- Otherwise, illegal intrusion may occur.

Do not press the buttons on the product forcibly or using a sharp tool.

- A product failure may occur.

Be careful not to contaminate or damage the fingerprint contact unit with a dirty hand or foreign substances.

- Deterioration in fingerprint authentication performance and a product failure may occur.

When cleaning the product, wipe the product with a soft and dry cloth and no water, benzene or alcohol.

- Otherwise, a product failure may occur.

BioStation L2 uses a capacitive screen and buttons. If the environment is moist from wet weather or the product surface is smeared with a lot of water, wipe off the product with a dry towel before using it.

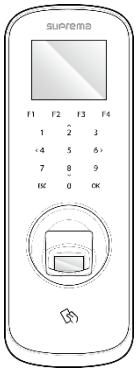
RTC battery

Replacing the battery with an incorrect type of battery may cause explosion.

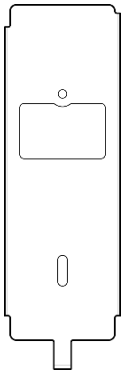
Discard the battery according to the appropriate regional or international waste regulations.

Introduction

Components

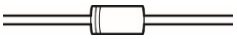


BioStation L2

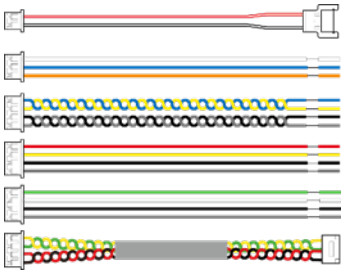


Wall bracket

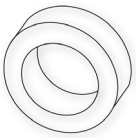
PVC anchor
(2 EA)



Diode
(1 EA)



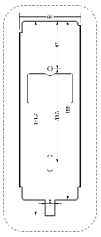
Connection cable
(2 pins 1 EA, 3 pins 1 EA, 4 pins 4 EA)



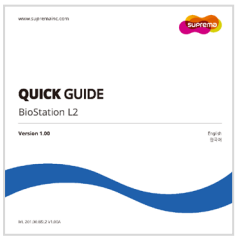
Ferrite core
(1 EA)

Fixing screw
(2 EA)

120 Ω resistor
(1 EA)



Drilling template

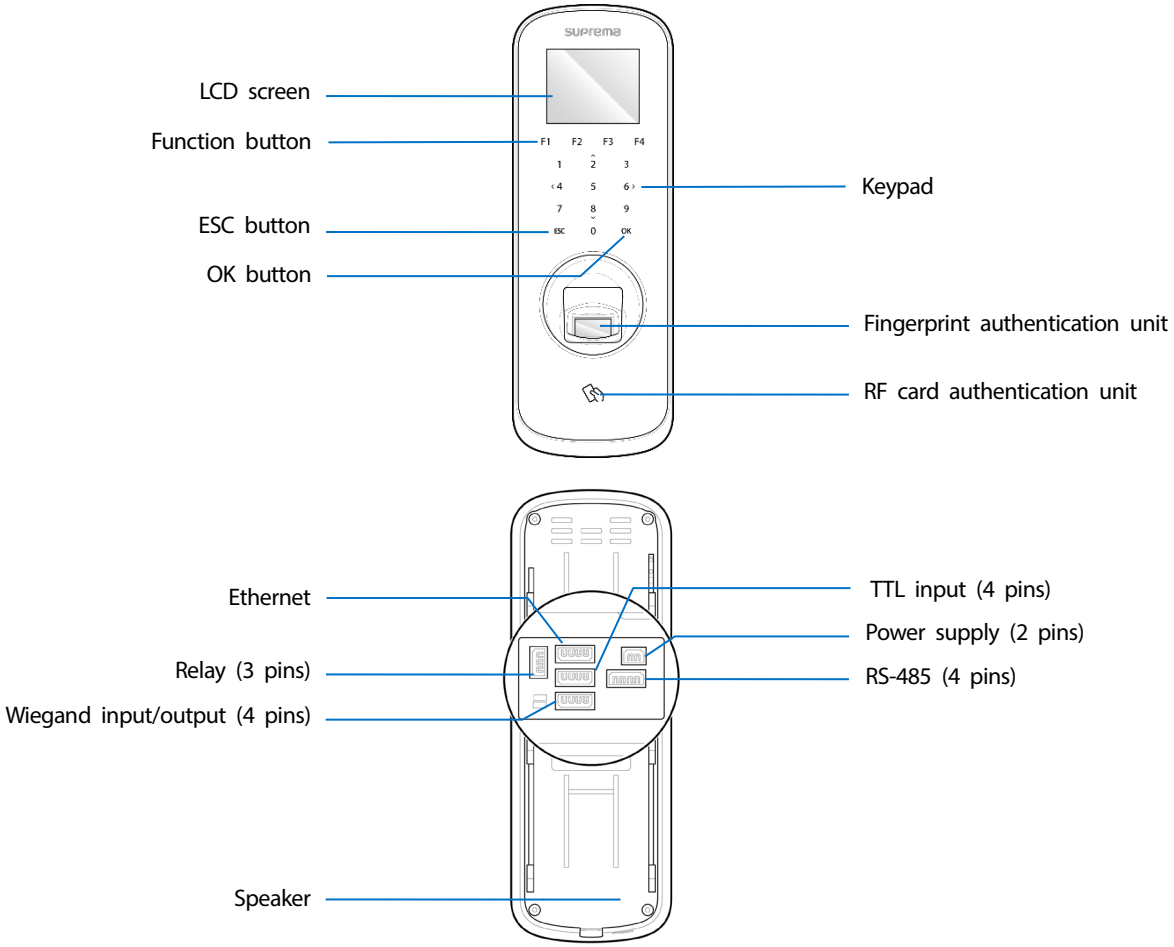


Quick guide

Note

- Components may vary according to the installation environment.
- For additional content regarding product installation, access the Suprema website (www.suprema.co.kr) and view the installation guide.

Name and function of each part



Name	Description
LCD screen	Provides UI for operation.
Function button	Used for the T&A Key, changing a letter, or entering a space.
Keypad	• **0** ~ **9**: Used for entering a number or letter. • 2, ‹ 4, 6 ›, 8: Used for moving to the desired item.
OK button	Used for selecting and setting T&A Mode. If a job code is set, you can change the job code of the user by pressing this button long.
ESC button	Used for opening the menu, moving to the previous screen or canceling input.
Speaker	Delivers sound.
Fingerprint authentication unit	Part to scan the fingerprint for entrance.
RF card authentication unit	Part to scan the card for entrance.
TTL input (4 pins)	Connects the TTL input cable.
RS-485 (4 pins)	Connects the RS-485 cable.
Relay (3 pins)	Connects the relay cable.
Power supply (2 pins)	Connects the power supply cable.
Ethernet (4 pins)	Connects the Ethernet cable.
Wiegand input and output (4pins)	Connects the Wiegand input and output cable.

Cables and connectors

Power

Pin	Name	Color
1	PWR +VDC	Red (white stripe)
2	PWR GND	Black (white stripe)

Relay

Pin	Name	Color
1	RLY NO	White
2	RLY COM	Blue
3	RLY NC	Orange

RS-485

Pin	Name	Color
1	485 TRXP	Blue
2	485 TRXN	Yellow
3	485 GND	Black
4	SH GND	Gray

TTL input

Pin	Name	Color
1	TTL IN0	Red
2	TTL IN1	Yellow
3	TTL GND	Black
4	SH GND	Gray

Wiegand input and output

Pin	Name	Color
1	WG D0	Green
2	WG D1	White
3	WG GND	Black
4	SH GND	Gray

Ethernet

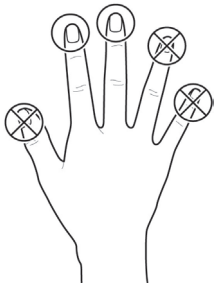
Pin	Name	Color
1	ENET RXN	Yellow
2	ENET RXP	Green
3	ENET TXN	Red
4	ENET TXP	Black

How to enroll a fingerprint correctly

In order to improve the fingerprint authentication rate, enroll the fingerprint correctly. BioStation L2 can recognize a fingerprint even if the angle and position of a user's fingerprint input change. If you enroll a fingerprint with attention to the following matters, the authentication rate can be improved.

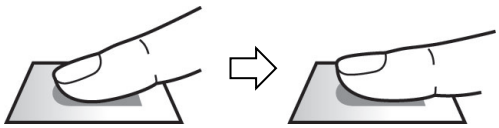
Selecting a finger for fingerprint input

- In preparation for a situation in which the fingerprint of a specific finger cannot be used, for example if the user is lifting a load with one hand or a finger gets hurt, up to 10 fingerprints for each user can be enrolled.
- In the case of a user whose fingerprint cannot be recognized well, the authentication rate can be improved by enrolling the same finger twice repeatedly.
- If a finger has a cut or the fingerprint is blurry, select another finger for the fingerprint.
- It is recommended to use the index finger or the middle finger when scanning the fingerprint. The authentication rate can be reduced if it is difficult to place another finger at the center of fingerprint sensor accurately.



Fingerprint enroll method

1 When a message saying "Place your finger on the sensor." is displayed on the LCD screen for enrolling the fingerprint, place the finger with the fingerprint you wish to enroll on the fingerprint authentication unit and press the finger gently for better authentication.



2 When the re-input screen is displayed after a beep sound, scan the fingerprint of the enrolled finger again (scan the fingerprint of a finger to be enrolled twice).

Note

Cautions for enrolling a fingerprint

When a fingerprint is recognized, it is compared with the initially registered fingerprint, so the initial fingerprint enroll is the most important. Pay attention to the following matters when enrolling the fingerprint.

- Place the finger deep enough to contact with the sensor completely.
- Place the center of the fingerprint in the center of the sensor.
- If a finger has a cut or the fingerprint is blurry, select another finger for the fingerprint.
- Scan the fingerprint correctly without moving according to the instruction on the screen.
- If you make the finger upright so that the contact area with the sensor is decreased or the angle of finger is warped, fingerprint authentication may not be performed.

When the fingerprint recognition fails

BioStation L2 can recognize a fingerprint regardless of a change in season or finger condition. However, the authentication rate may vary according to the external environment or fingerprint input method.

If the fingerprint authentication cannot be done smoothly, it is recommended to take the following measures.

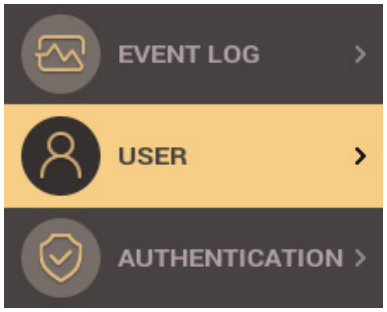
- If the finger is smeared with water or sweat, dry off the finger and then scan the finger.
- If the finger is too dry, blow your breath on the fingertips and then scan the finger.
- If the finger has a cut, register the fingerprint of another finger.
- The initially enrolled fingerprint often may have not been scanned correctly, so enroll the fingerprint again according to '**Cautions for enrolling a fingerprint**'.

Admin Menu

All Menus

1 Press **ESC** and authenticate with the Admin level credential.

2 Select the desired menu.



Note

- If the administrator has not been designated, the menu screen will be displayed when you press **ESC**.

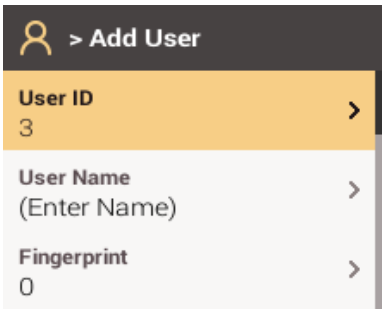
User

Registering user information

The user information including fingerprints can be registered.

1 Press **ESC** and authenticate with the Admin level credential.

2 Select **USER** > **Add User**, then press 6 ›.



3 Select the desired item, then press and set ‹ 4 or 6 ›. When you press **OK**, the user information will be registered.

- **User ID**: Enter the user ID you wish to register. Enter the desired ID using the number keypad, then press **OK**. A number between 1 and 4294967295 can be entered for ID.
- **User Name**: Enter the user name using the number keypad and the function button.
- **Fingerprint**: Enroll a fingerprint for user authentication. Scan the fingerprint of a finger you wish to enroll, and then scan the fingerprint of the same finger again. You can delete the fingerprint by selecting a fingerprint to delete and pressing ‹ 4. You can also scan the fingerprint again by pressing 6 ›. To add a fingerprint, select **+ Add Finger**, then press 6 ›.
- **Card**: Register a card for user authentication. Scan the card that will be assigned to the user.
- **PIN**: Enter the PIN you wish to use. Enter the PIN you wish to use, and then enter the same PIN again for confirmation. Enter a number between 4 and 16 digits to prevent leaking.
- **Operator Level**: Select the level you wish to assign to a user.
- **Start Date**: Set a start date to use the user account.
- **Expiry Date**: Set the expiry date of the user account.
- **1:1 Security Level**: Set the security level for 1:1 authentication.
- **Duress**: Select a fingerprint to be used as a duress fingerprint. This can be used only when 2 or more fingerprints have been enrolled.
- **Private Auth Mode**: Change the authentication method according to the user.

4 To save settings, press **OK**.

Note

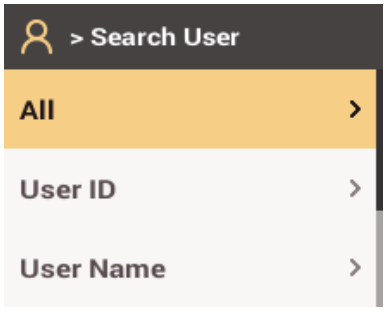
Available menus vary according to the set operator level.

- **Normal User**: This is the normal user level. Menus cannot be accessed.
- **Administrator**: All menus can be accessed.
- **Configuration**: **AUTHENTICATION**, **DISPLAY & SOUND**, **DEVICE**, **NETWORK** menus can be accessed.
- **User Management**: **USER** menu can be accessed.

Modifying user information

User Management or Administrator can modify the registered user information. A fingerprint or card can be added, and PIN and level can be modified.

1. Press **ESC** and authenticate with the Admin level credential.
2. Select **USER** > **Search User**, then press 6 ›.
3. Select your search terms. You can search for a user by **All**, **User ID**, **User Name**, **Fingerprint**, or **Card**.



4. Select the user you wish to modify and press 6 ›. Modify the information by referring to **Registering user information**.
   - To delete a user, press ‹ 4, then press **OK**.

Note

- **Access Groups** can be registered in **BioStar 2**. For detailed contents regarding registering an access group, refer to BioStar 2 Administrator's manual.

Delete All Users

You can delete all registered users at once.

1. Press **ESC** and authenticate with the Admin level credential.
2. Select **USER** > **Delete All Users**, then press 6 ›.
3. When you press **OK**, all registered users will be deleted.

View User Usage

You can see the number of registered users, fingerprints and cards at a glance.

1. Press **ESC** and authenticate with the Admin level credential.
2. Select **USER** > **User Usage**, then press 6 ›.

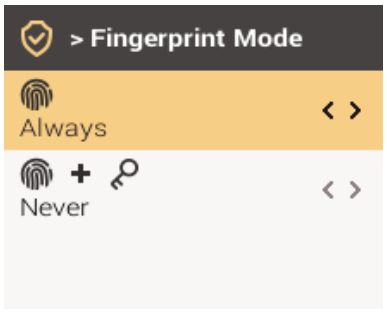
Authentication

Mode

Fingerprint Mode

You can set the schedule to be used for each authentication method using a fingerprint.

1. Press **ESC** and authenticate with the Admin level credential.
2. Select **AUTHENTICATION** > **Auth Mode** > **Fingerprint Mode**, then press 6 ›.
3. Select the desired item and set the schedule by pressing ‹ 4 or 6 ›.



- : Mode to use a fingerprint only.
- + : Mode to authenticate with a fingerprint and then enter a PIN.

4. To save settings, press **OK**.

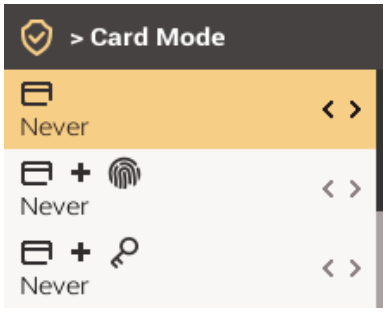
Note

- A schedule can be set in BioStar 2. If there is no set schedule, only **Not Used** and **Always** can be selected.
- For detailed contents regarding setting a schedule, refer to BioStar 2 Administrator's manual.

Card Mode

You can set the schedule to be used for each authentication method using a card.

1. Press **ESC** and authenticate with the Admin level credential.
2. Select **AUTHENTICATION** > **Auth Mode** > **Card Mode**, then press 6 ›.
3. Select the desired item and set the schedule by pressing ‹ 4 or 6 ›.



- : Mode to use a card only.
- + : Mode to authenticate with a card and then authenticate with a fingerprint.
- + : Mode to authenticate with a card and then enter a PIN.
- + / : Mode to authenticate with a card and then authenticate with a fingerprint or enter a PIN.
- + + : Mode to authenticate with a card and then use both fingerprint authentication and PIN input.

4. To save settings, press **OK**.

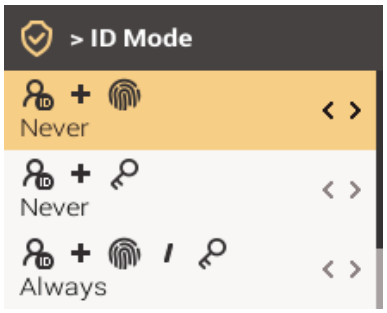
Note

- A schedule can be set in BioStar 2. If there is no set schedule, only **Not Used** and **Always** can be selected.
- For detailed contents regarding setting a schedule, refer to BioStar 2 Administrator's manual.

ID Mode

You can set the schedule to be used for each authentication method using ID.

1. Press **ESC** and authenticate with the Admin level credential.
2. Select **AUTHENTICATION** > **Auth Mode** > **ID Mode**, then press 6 ›.
3. Select the desired item and set the schedule by pressing ‹ 4 or 6 ›.



- + : Mode to enter ID and then authenticate with a fingerprint.
- + : Mode to enter ID and then enter a PIN.
- + / : Mode to enter ID and then authenticate with a fingerprint or enter a PIN.
- + + : Mode to enter ID and then use both fingerprint authentication and PIN input.

4. To save settings, press **OK**.

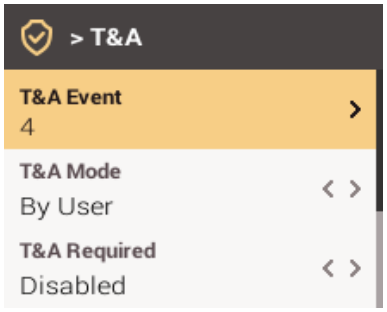
Note

- A schedule can be set in BioStar 2. If there is no set schedule, only **Not Used** and **Always** can be selected.
- For detailed contents regarding setting a schedule, refer to BioStar 2 Administrator's manual.

T&A Mode

You can set how to register T&A Mode.

1. Press **ESC** and authenticate with the Admin level credential.
2. Select **AUTHENTICATION** > **T&A Mode**, then press 6 ›.
3. Select the desired item and then change the settings by pressing ‹ 4 or 6 ›.



- **T&A Event**: View the set T&A event.
- **T&A Mode:** Set the method to use T&A mode.
- **T&A Required**: Set to require a user to select a T&A event when authenticating. If **Use** is set, you can set to require a user to select a T&A event when authenticating.
- **T&A Fixed**: Set to use only a T&A event selected by the administrator. This option can be used when **Fixed** is set for **T&A Mode**.
- **Job Code**: Select whether or not to use Job Code.

4 To save settings, press **OK**.

Note

- When **Use** is set for **Job Code**, you can change the user job code. You can select the desired job code by pressing OK long and authenticating.

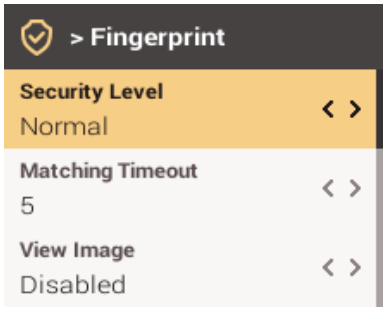
Fingerprint

You can change settings regarding the fingerprint authentication.

1 Press **ESC** and authenticate with the Admin level credential.

2 Select **AUTHENTICATION** > **Fingerprint**, then press 6 ›.

3 Select the desired item and then change the settings by pressing ‹ 4 or 6 ›.



- **Security Level**: Set the security level for 1:N authentication.
- **Matching Timeout**: Set the fingerprint matching timeout. If the authentication is not completed during a set time, the authentication will fail.
- **View Image**: Set to view the original image when scanning the fingerprint.
- **Sensor Sensitivity**: Set the sensitivity of the fingerprint authentication sensor. To obtain more precise fingerprint information by increasing the sensor sensitivity, set the sensor sensitivity higher.
- **Fake finger detected**: Set the fake fingerprint inspection level. If the fake fingerprint inspection level is higher, the rejection rate on actual human fingerprints will increase.
- **1:N Fast Mode**: Set the fingerprint authentication speed. If you select **Auto**, the authentication speed will be set according to all fingerprint templates enrolled on the device.
- **Template Format**: Set the fingerprint template format. SUPREMA is set as the default, and if you change the template format, all fingerprints saved previously cannot be used. Use caution when changing the Template Format.
- **Sensor Mode**: When **Auto On** is set, the fingerprint sensor recognizes a user's fingerprint and turns on. When **Always On** is set, the sensor is always on.
- **Advanced Enrollment**: Inspect the quality of a scanned fingerprint in order to save high quality fingerprint information When Use is set and the quality of the fingerprint is low, it notifies such information to the user and helps the user scan the fingerprint correctly.

4 To save settings, press **OK**.

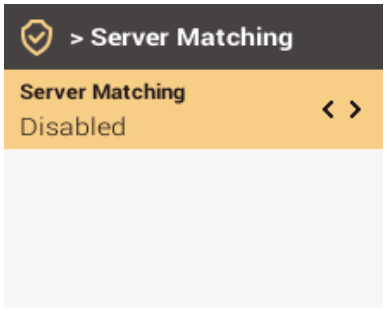
Note

- Change the template format after deleting the fingerprint information of all users. If the fingerprint information of a user has been enrolled, the template format cannot be changed.

Server Matching

When you set Server Matching, the user authentication is not carried out in the device, but rather in BioStar. Server Matching can be useful when there is a large amount of user information in the device or you do not wish to publicly expose the device where user credential information is saved.

1. Press **ESC** and authenticate with the Admin level credential.
2. Select **AUTHENTICATION** > **Server Matching**, then press 6 ›.

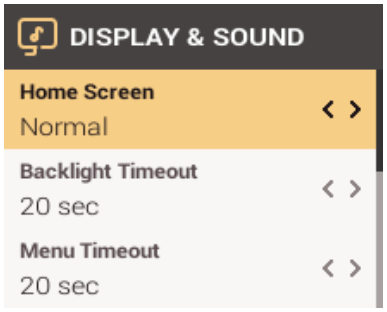


3. Change the settings by pressing ‹ 4 or 6 ›.
4. To save settings, press **OK**. .

Display & Sound

You can change the display and sound settings of the device.

1. Press **ESC** and authenticate with the Admin level credential.
2. Select **DISPLAY & SOUND**, then press 6 ›.
3. Select the desired item and then change the settings by pressing ‹ 4 or 6 ›.



- **Home Screen**: Change the style of the home screen.
- **Backlight Timeout**: Set the time (second) to turn off the lighting of LCD screen.
- **Menu Timeout**: Set the time (sec) for the menu screen to disappear automatically. If there is no button input during a set time, the screen will return to the home screen.
- **Message Timeout**: Set the time (sec) for a setting complete message or information message to disappear automatically.
- **Language**: Set the language you wish to use.
- **Voice Instruction**: Set to use the voice instruction instead of alarm sounds.
- **Volume**: Set the volume.

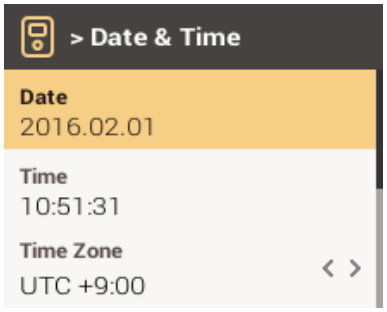
4. To save settings, press **OK**. .

Device

Date & Time

You can set date and time. Set the date and time accurately in order to collect accurate log data.

1. Press **ESC** and authenticate with the Admin level credential.
2. Select **DEVICE** > **Date & Time**, then press 6 ›.
3. Select the desired item and then change the settings by pressing ‹ 4 or 6 ›.



- **Date**: Check the current date. To modify it directly, set **Disabled** for **Time Sync**.
- **Time**: Check the current time. To modify it directly, set **Disabled** for **Time Sync**.
- **Time Zone**: Set the time reference of the current location.
- **Time Sync**: Synchronize the server and the time. If you wish to synchronize the server and the time, enable **Time Sync**.
- **Date Format**: Set the date format. You can select among **YYYY/MM/DD**, **MM/DD/YYYY** and **DD/MM/YYYY**.
- **Time Format**: Set the time format. You can select either **24-Hour** or **AM/PM**.

4. To save settings, press **OK**. .

Relay

You can set the open time and the input port of the exit button in the device. option is useful when the device is used as a standalone.

1. Press **ESC** and authenticate with the Admin level credential.
2. Select **DEVICE** > **Relay**, then press 6 ›.
   - **Open Time**: Set the duration for the door to remain open when standard user authentication has been carried out.
   - **Exit Button**: Select the input port where the exit button is connected.
   - **Switch**: Select the relay type (N/O or N/C).
3. To save settings, press **OK**. .

Device Info

You can view the model name, firmware version of Device ID and MAC address.

1. Press **ESC** and authenticate with the Admin level credential.
2. Select **DEVICE** > **Device Info**, then press 6 ›.
3. You can view the information including **Model Name, Device ID, HW, FW, Kernel** and **MAC**.
4. To return to the previous screen, press **ESC**.

Memory Info

You can view the status of memory usage.

1. Press **ESC** and authenticate with the Admin level credential.
2. Select **DEVICE** > **Device Info**, then press 6 ›.
3. View the memory usage status of the device.
4. To return to the previous screen, press **ESC**.

Restart Device

You can restart the device.

1. Press **ESC** and authenticate with the Admin level credential.
2. Select **DEVICE** > **Restart Device,** then press 6 ›.
3. To restart the device, press **OK**. To cancel, press **ESC**.

Restore to default

Device settings, network setting, and operator levels will be reset.

1. Press **ESC** and authenticate with the Admin level credential.
2. Select **DEVICE** > **Restore to default**, then press 6 ›.
3. To reset all device settings, press **OK**. To cancel, press **ESC**.

Note

- When you reset, the operator level will be reset as well. After resetting, make sure to set the operator level again.
- Language setting will not change after resetting.

Factory Default

This will delete all data and root certificate on the device and reset the settings.

1. Press the **ESC** button then authenticate as an administrator.
2. Select **DEVICE** > **Factory Default**, then press 6 ›.
3. To restore the factory defaults, press **OK**. To cancel, press **ESC**.

Note

- You can only use **Factory Default** when the root certificate is stored on the device..

Delete the Root Certificate

This will delete the root certificate on the device.

1. Press the **ESC** button then authenticate as an administrator.
2. Select **DEVICE** > **Delete the Root Certificate**, then press 6 ›.
3. To delete the root certificate, press **OK**. To cancel, press **ESC**.

Note

- You can only use **Delete the Root Certificate** when the root certificate is stored on the device and device administrator is set.

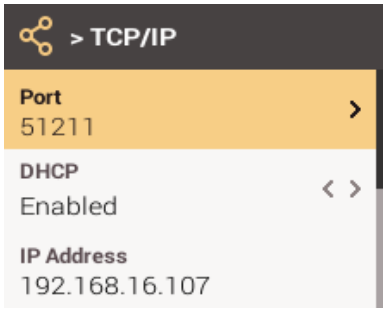
Network

Network Settings

You can change the network settings of the device.

Ethernet

1. Press **ESC** and authenticate with the Admin level credential.
2. Select **NETWORK** > **TCP/IP**, then press 6 ›.
3. Select the desired item and then change the settings by pressing ‹ 4 or 6 ›.

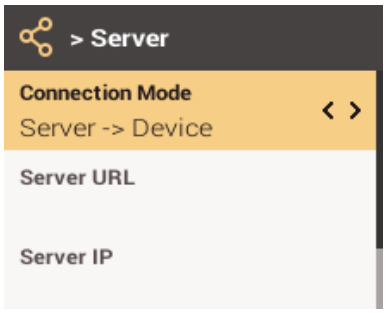


- **Port**: Set the device port.
- **DHCP**: Set whether or not to use DHCP. If **Disabled** is set, the user can modify **Port**, **IP Address**, **Gateway**, or **Subnet Mask**.
- **IP Address**: View the IP address of the device. To modify, set **DHCP** to **Disabled**.
- **Gateway**: View the gateway of the device. To modify, set **DHCP** to **Disabled**.
- **Subnet Mask**: View the subnet mask of the device. To modify, set **DHCP** to **Disabled**.
- **DNS**: Set the DNS server address.

4. To save settings, press **OK**. .

Server

1. Press **ESC** and authenticate with the Admin level credential.
2. Select **NETWORK** > **Server**, then press 6 ›.
3. Select the desired item and then change the settings by pressing ‹ 4 or 6 ›.



- **Connection Mode:** When you select **Device -> Server**, you can send a connection signal from the device to a server with the input information directly. When you select **Server -> Device**, **Server IP** and **Server Port** cannot be entered.
- **Server URL**: Enter server URL instead of **Server IP**. Input is accepted only when **Device -> Server** is set for **Connection Mode**.
- **Server IP**: Enter the IP of the PC where BioStar 2 is installed. Input is accepted only when **Device -> Server** is set for **Connection Mode**.
- **Server Port**: Enter the port of the PC where BioStar 2 is installed. Input is accepted only when **Device -> Server** is set for **Connection Mode**.

4. To save settings, press **OK**. .

Serial Settings

RS-485

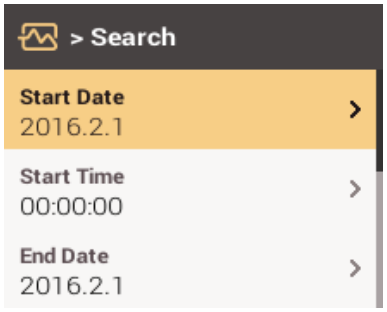
1. Press **ESC** and authenticate with the Admin level credential.
2. Select **NETWORK** > **RS-485**, then press 6 ›.
   - **Mode**: Select the **RS-485** mode.
   - **Baud Rate**: Select the desired baud rate.
3. To save settings, press **OK**. .

Event Log

Search Log

You can set a condition and search a log.

1. Press **ESC** and authenticate with the Admin level credential.
2. Select **EVENT LOG**.> **Search**, then press 6 ›.
3. Select the desired item and then change the settings by pressing ‹ 4 or 6 ›.



4. When you press **OK**, a log that matches the set condition will be displayed on the screen.
5. To return to the previous screen, press **ESC**.

Delete All Logs

You can delete all saved logs.

1. Press **ESC** and authenticate with the Admin level credential.
2. Select **EVENT LOG** > **Delete All**, then press 6 ›.
3. To delete all logs, press **OK**. To cancel, press **ESC**.

View Log Usage

You can check the status of log usage.

1. Press **ESC** and authenticate with the Admin level credential.
2. Select **EVENT LOG** > **Log Usage**, then press 6 ›.
3. Check the log usage of the device.
4. To return to the previous screen, press **ESC**.

Troubleshooting

Checklist before reporting a failure

Category	Problem	Solution
Power	The power is being supplied but the device does not operate.	• If the terminal and the bracket are far away from each other, the device may not operate due to the temper switch. • Check the adaptor or the power cable.
PIN	I lost my PIN.	• For a normal user PIN, request it from the administrator and enter it again. • If you have lost the Admin PIN, contact the installation company.
	I entered my PIN and pressed the **OK** button, but I still cannot open the door.	• Check if you have entered the registered PIN correctly. • Check if you have changed the PIN recently. • If you cannot remember the PIN, request it from the administrator and enter it again.
Fingerprint	The fingerprint has been enrolled but fingerprint authentication cannot be done smoothly and errors occur frequently.	• Check '**How to enroll a fingerprint correctly**' and enroll the fingerprint again. • If your fingerprint has a cut, the device may recognize your fingerprint as someone else's fingerprint. • If there are a large number of enrolled fingerprints, change **Matching Timeout** and try again. • The authentication rate may vary for each fingerprint due to different characteristics. Enroll the fingerprint of another finger.
	Suddenly fingerprint authentication cannot be done.	• Check if the finger or the fingerprint sensor is smeared with sweat, water or dust, and wipe the finger or the fingerprint sensor clean. • Wipe your finger and the fingerprint sensor with a dry towel and then try again. • If the fingerprint of your finger is too dry, blow on the fingerprint and then try again.
Door Lock	The door cannot be locked when I close the door.	• The electric lock may be malfunctioning. Have an inspection through the installation company.
Time	Suddenly the time has become incorrect.	• BioStation L2 is equipped with a built-in battery, but if power is not supplied for an extended period of time, the built-in battery may die, causing the time to become incorrect. For information on correcting the time, referring to **Date & Time**.
Admin Access	I lost my Admin PIN, so I cannot access the Admin mode.	• Because the administrator grants an access permission in BioStation L2, only the administrator can access the Admin menu. • If you need to access the Admin menu, you can issue a PIN through a required procedure. Ask the installation company for the procedure to issue the password.

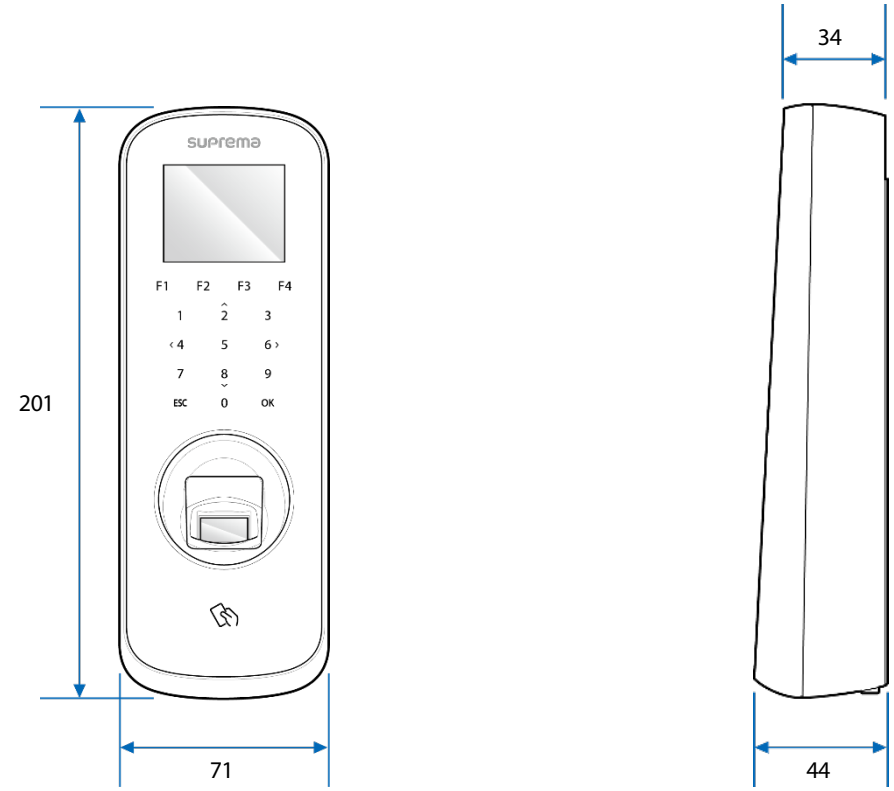
Product Specifications

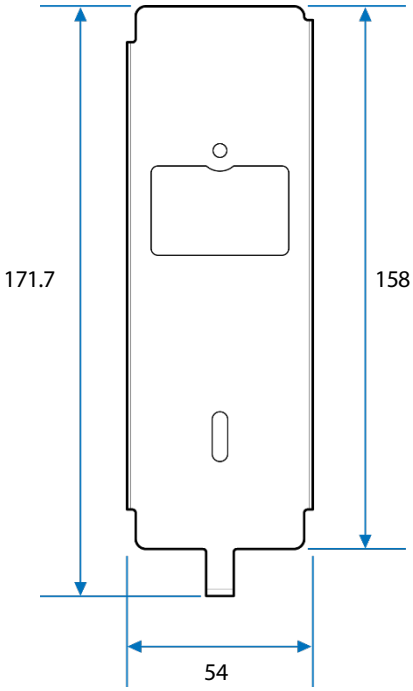
Category	Feature	Specification
Credential	Biometric	Fingerprint
	RF Option	• BSL2-OE: 125kHz EM • BSL2-OM: 13.56Mhz MIFARE, MIFARE Plus, DESFire/EV1, FeliCa, NFC, ISO14443A, ISO15693
	RF read range*	MIFARE: 50 mm, DESFire: 50 mm, Felica: 30 mm, ISO15693: 50 mm
General	CPU	1.2 GHz Quad Core
	Memory	2GB Flash + 256 MB RAM
	LCD type	2" color TFT LCD
	LCD resolution	220 x 176 pixels
	Sound	16-bit Hi-Fi
	Operating temperature	-20 °C ~ 50 °C
	Storage temperature	-40 °C ~ 70 °C
	Operating humidity	0 % ~ 80 %, non-condensed
	Storage humidity	0 % ~ 90 %, non-condensed
	Dimension (W x H x D)	71 mm x 201 mm x 44 mm (Bottom) / 34 mm (Top)
	Weight	Device: 280 g Bracket: 61 g (including washers and bolts)
	Certificates	CE, FCC, KC, RoHS, REACH, WEEE
Fingerprint	Image dimension	272 x 320 pixels
	Image bit depth	8 bits, 256 grayscale
	Resolution	500 dpi
	Template	SUPREMA / ISO 19794-2 / ANSI 378
	Extractor / Matcher	MINEX certified and compliant
	LFD	Supported
Capacity	Max. User (1:1)	500,000
	Max. User (1:N)	100,000
	Max. Template (1:1)	1,000,000
	Max. Template (1:N)	200,000
	Max. Text Log	1,000,000
Interface	Ethernet	Supported (10/100 Mbps, auto MDI/MDI-X)
	RS-485	1ch Master / Slave (Selectable)
	Wiegand	1 ch Input / Output (selectable)
	TTL input	2 ch Input
	Relay	1 Relay
	Tamper	Supported
Electrical	Power	Voltage: 12VDC Current: Max. 600 mA
	Switch input VIH	Min. 4 V Max. 5 V
	Switch input VIL	Max. 1 V
	Switch pull-up resistor	4.7 kΩ (The input ports are pulled up with 4.7 kΩ.)
	Wiegand output VOH	Min. 4 V Max. 5 V
	Wiegand output VOL	Max. 1 V
	Wiegand output pull-up resistor	Internal pull-up with 1 kΩ
	Relay	Voltage: Max. 30 VDC Current: 1A, Max. 2A

* RF read range will vary depending on the installation environment.

Dimensions

(Unit: mm)





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 may void the user's authority to operate the equipment under FCC rules.

This appliance and its antenna must not be located together or operated in conjunction with any other antenna or transmitter.
A minimum separation distance of 20 cm must be maintained between the antenna and individuals for this appliance to satisfy the RF exposure requirements.

Appendices

Escape clause

- The information in this manual is provided with regard to the Suprema's products.
- The right to use is acknowledged only for products included in the terms and conditions of the sales agreement guaranteed by Suprema. The right of license to other intellectual property rights not discussed in this manual is not acknowledged.
- Suprema does not guarantee or hold responsibility for the suitability and commerciality of the product for a specific purpose, or the infringement of patent, copyright, or other intellectual property rights with regard to sales or usage of Suprema's products.
- Do not use a Suprema product in situations related to medical, rescue of human lives, or maintenance of life, as a person may get injured or lose his/her life due to product malfunction. If an accident occurs while a consumer is using the product under the situations described as examples above, employees, subsidiaries, branches, affiliated companies and distributors of Suprema do not accept responsibility nor will they reimburse for all related direct and indirect expenses or expenditure including attorney fees even if the consumer has discovered any shortcomings in the product design or manufacturing process and claims this as a significant fault.
- Suprema may modify the product size and specifications at any time without proper notice in order to improve the safety, function and design of the product. Designers must keep in mind that functions or descriptions indicated as "to be implemented" or "undefined" may change at any time. Suprema will implement or define such functions or descriptions in the near future and Suprema accepts no responsibility for compatibility issues and any other problems arising from such compatibility issues.
- If you wish to obtain the newest specifications before ordering the product, contact Suprema through a Sales Representative or local distributor of Suprema.

Copyright notice

The copyright of this document is vested in Suprema. The rights of other product names, trademarks and registered trademarks are vested in each individual or organization that owns such rights.

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 **Technical support** support@supremainc.com