www.supremainc.com

USER GUIDE

BioStation A2

English

Version 1.2

Contents

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 Secure I/O 2, electric lock and BioStation A2 respectively.

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

Keep at least 10cm distances between the devices when install multiple devices.

- Otherwise, RF performance is affect to the other device, the devices may not operate normally.

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 A2 uses capacitive buttons and screen. 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.

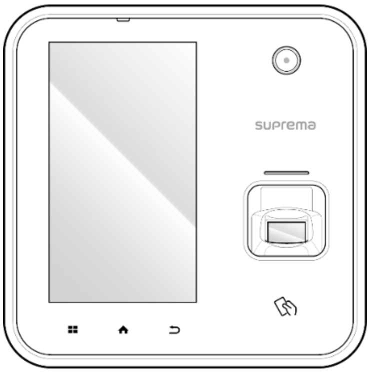
RTC battery

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

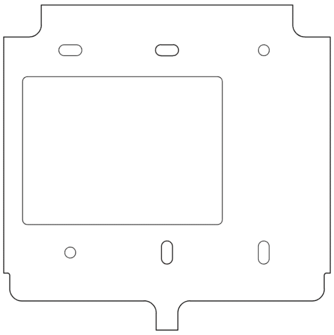
Discard the battery according to the appropriate regional or international waste regulations.

Introduction

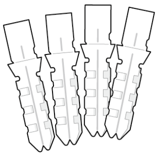
Components



BioStation A2

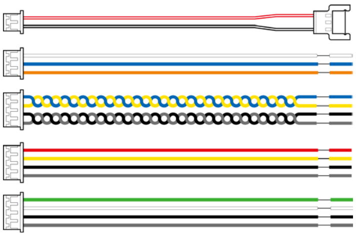


Wall bracket

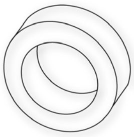


PVC anchor
(4 EA)

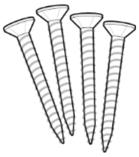
Diode
(1 EA)



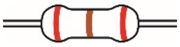
Connection cable
(2 pins 1 EA, 3 pins 2 EA, 4 pins 4 EA)



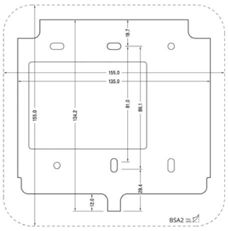
Ferrite core
(1 EA)



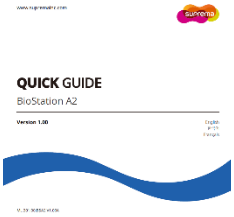
Fixing screw
(4 EA)



120 Ω resistor
(1 EA)



Drilling template

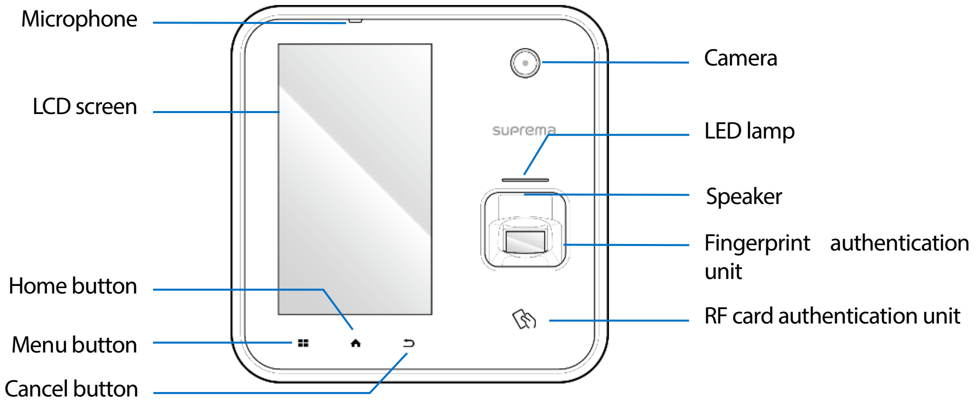


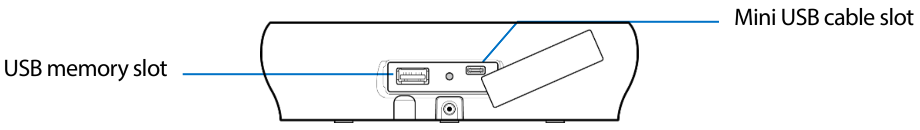
Quick guide

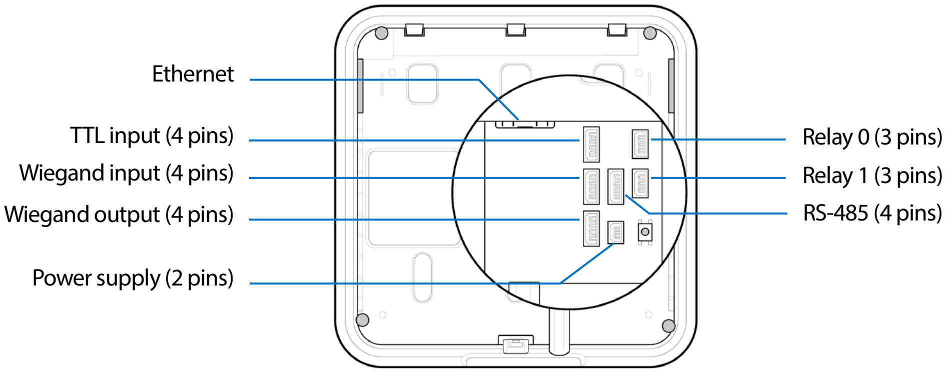
Note

- 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





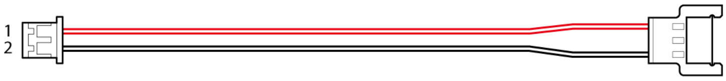


Name	Description
Microphone	Delivers the voice of the user when the interphone is connected.
LCD screen	Provides UI for operation.
Menu button (■■)	Displays the list of menus.
Home button (⌂)	Navigates to the home screen.
Cancel button (↩)	Navigates back to the previous screen.
Speaker	Delivers sound.
LED lamp	Indicates the operational status of the product with the color of the LED lamp.
Fingerprint authentication unit	Part to scan the fingerprint for entrance.
RF card authentication unit	Part to scan the card for entrance.
USB memory slot	Connects USB memory.
Mini USB cable slot	Will be supported in the future.
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	Connects the Ethernet cable.
Wiegand input (4 pins)	Connects the Wiegand input and output cable.
Wiegand output (4 pins)	Connects the Wiegand input and output cable.

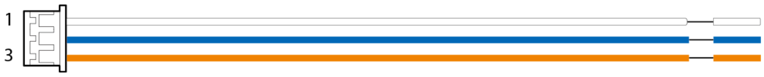
Cables and connectors

Power



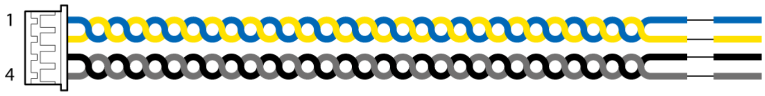
Pin	Name	Color
1	PWR +VDC	Red (white stripe)
2	PWR GND	Black (white stripe)

Relay



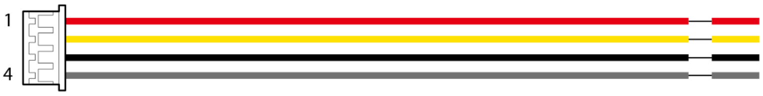
Pin	Name	Color
1	RLY NO	White
2	RLY COM	Blue
3	RLY NC	Orange

RS-485



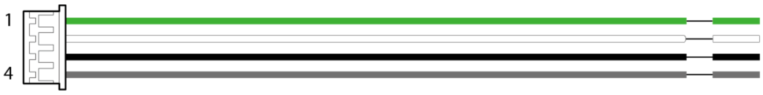
Pin	Name	Color
1	485 TRXP	Blue
2	485 TRXN	Yellow
3	485 GND	Black
4	SH GND	Gray

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



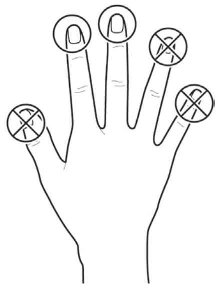
Pin	Name	Color
1	WG D0	Green
2	WG D1	White
3	WG GND	Black
4	SH GND	Gray

How to enroll a fingerprint correctly

In order to improve the fingerprint authentication rate, enroll the fingerprint correctly. BioStation A2 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.

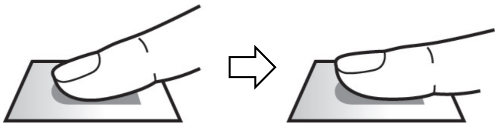
Selecting a finger for fingerprint input

- 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 “Scan the fingerprint.” 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.



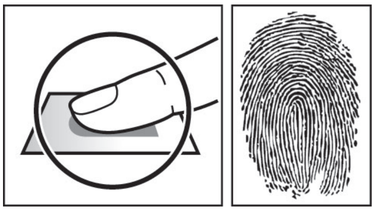
2 When the re-input screen is displayed after a beep sound, scan the fingerprint of the enrolled finger again (scan the fingerprint of a finger to be enrolled twice).

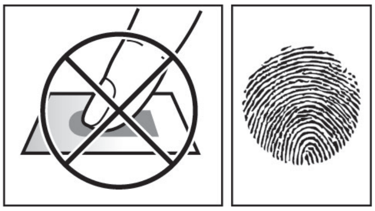
Note

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 A2 can recognize a fingerprint regardless of a change of 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.

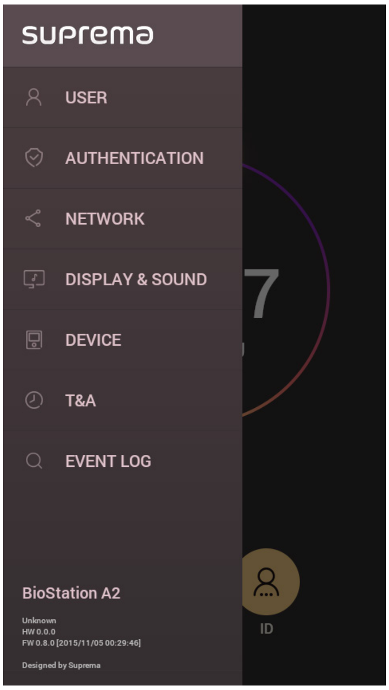
- If the finger is smeared with water or sweat, dry off the finger and then scan the finger.
- If the finger is too dry, blow your breath on the fingertips and then scan the finger.
- If the finger has a cut, register the fingerprint of another finger.
- The initially enrolled fingerprint often may have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

Admin Menu

All Menus

1 Press ⊞ and authenticate with the Admin level credential.

2 Select the desired menu.



BioStation A2

Unknown
HW 0.0.0
FW 0.8.0 [2015/11/05 00:29:46]

Designed by Suprema

Note

- In case the administrator has not been designated, the menu screen will be displayed when you press ⊞.

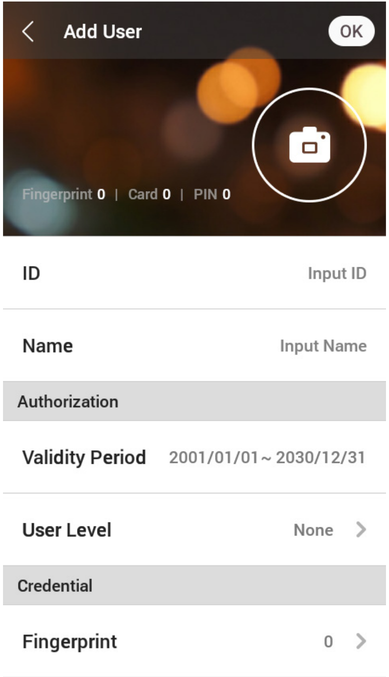
User

Registering user information

The user information including fingerprints can be registered.

1 Press ⊞ and authenticate with the Admin level credential.

2 Press **User** > +.



Add User OK

Fingerprint 0 | Card 0 | PIN 0

ID Input ID

Name Input Name

Authorization

Validity Period 2001/01/01 ~ 2030/12/31

User Level None >

Credential

Fingerprint 0 >

3 Select and set the desired item. When you press **OK**, the user information will be registered.

- 📷: Take a picture of a user with the built-in camera.
- **ID**: Enter the user ID you wish to register. A number between 1 and 4294967295 can be entered for ID.
- **Name**: Enter the user name.
- **Validity Period**: Set a **Start Date** and **End Date** to use the user account. When you press the first date, you can set **Start Date**, and when you press the second date, you can set **End Date**.
- **Access Group**: Select an access group for the user. Access groups can be registered only in BioStar 2.
- **User Level**: Select the level you wish to assign to a user.
- **Fingerprint**: Enroll a fingerprint for user authentication. Press + and enroll the fingerprint. Scan the fingerprint of a finger you wish to enroll, and then scan the fingerprint of the same finger again. To enroll an additional fingerprint, press + again.
- **Card**: Register a card for user authentication. Press + and scan the card which will be assigned to the user. To register an additional card, press + again.
- **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.
- **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.

Note

Available menus vary according to the set user level.

- None: This is the general user level and menus cannot be accessed.
- **Administrator**: All menus can be accessed.
- **Configuration**: **AUTHENTICATION**, **DISPLAY & SOUND**, **DEVICE**, **NETWORK** menus can be accessed.
- **User Mgmt**: **USER** menu can be accessed.

Modifying user information

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

1 Press ▦ and authenticate with the Admin level credential.

2 Press **User** > 🔍.

3 Select your search terms. You can search for a user by **ID**, **name**, **fingerprint** or **card**.

4 Select the user you wish to modify and press ✎. Modify the information by referring to **Registering user information**.

- To delete a user, press 🗑 and 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 ▦ and authenticate with the Admin level credential.

2 Press **User** > 🗑 and select **Delete All** or a user you wish to delete.

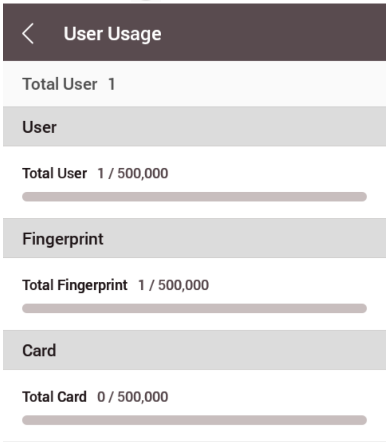
3 When you press **OK**, all registered users will be deleted.

View User Usage

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

1 Press ▦ and authenticate with the Admin level credential.

2 Press **User** > ⓘ.



User Usage

Total User 1

User

Total User 1 / 500,000

Fingerprint

Total Fingerprint 1 / 500,000

Card

Total Card 0 / 500,000

Authentication

Auth Mode

Modifying Auth Mode

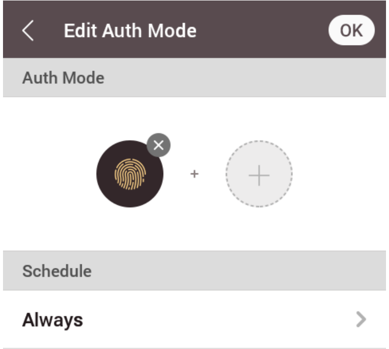
You can set the authentication method and schedule according to each credential. You can set up to 3 auth modes.

1 Press ▦ and authenticate with the Admin level credential.

2 Press **Authentication** > **Auth Mode**.

3 Select the auth mode you wish to change.

4 When you press ⊗, the selected credential will be deleted, and when you press ⊕, available credentials to be added will be displayed on the screen.



Edit Auth Mode OK

Auth Mode

Schedule

Always

5 Set the desired auth mode and select a schedule.

Category	Description
Fingerprint	• ◎: Mode to use a fingerprint only • ◎ + 🔑: Mode to authenticate with a fingerprint and then enter PIN
Card	• ▤: 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 PIN • ▤ + ◎ / 🔑: Mode to authenticate with a card and then authenticate with a fingerprint or enter PIN • ▤ + ◎ + 🔑: Mode to authenticate with a card and then use both fingerprint authentication and PIN input.
ID	• 👤 + ◎: Mode to enter ID and then authenticate with a fingerprint • 👤 + 🔑: Mode to enter ID and then enter PIN • 👤 + ◎ / 🔑: Mode to enter ID and then authenticate with a fingerprint or enter PIN • 👤 + ◎ + 🔑: Mode to enter ID and then use both fingerprint authentication and PIN input

6 When you press **OK**, settings will be saved.

Note

- A schedule can be set in BioStar 2. If there is no set schedule, only **Always Use** can be selected.
- For detailed contents regarding setting a schedule, refer to BioStar 2 Administrator's manual.

Delete Auth Mode

1. Press ⊞ and authenticate with the Admin level credential.
2. Press **Authentication** > **Auth Mode**.
3. Press 🗑 and select an item to delete.
4. When you press **OK**, the selected item will be deleted.

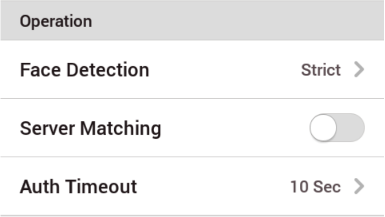
Add Auth Mode

You can register up to 3 auth modes.

1. Press ⊞ and authenticate with the Admin level credential.
2. Press **Authentication** > **Auth Mode**.
3. Press ＋.
4. Set the desired auth mode by pressing ⊕, and then select a schedule.
5. When you press **OK**, the auth mode will be added.

Operation

1. Press ⊞ and authenticate with the Admin level credential.
2. Press **AUTHENTICATION** and then modify items below **Operation**.



Operation

Face Detection Strict >

Server Matching ○

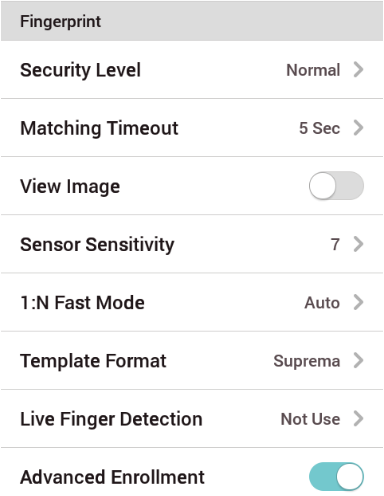
Auth Timeout 10 Sec >

- **Face Detection**: When you set Face Detection, BioStation A2 can detect real face, and authentication can be done only when a face is detected after authenticating with a fingerprint, card, or PIN.
- **Server Matching**: When you set Server Matching, the user authentication is not carried out in the device, but instead is carried out 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.
- **Auth Timeout**: If the authentication is not completed during a set time, the authentication will fail. You can set a time between 3 seconds and 20 seconds.

Fingerprint

You can change settings regarding the fingerprint authentication.

1. Press ⊞ and authenticate with the Admin level credential.
2. Press **AUTHENTICATION** and then modify items below **Fingerprint**.



Fingerprint	
Security Level	Normal >
Matching Timeout	5 Sec >
View Image	○
Sensor Sensitivity	7 >
1:N Fast Mode	Auto >
Template Format	Suprema >
Live Finger Detection	Not Use >
Advanced Enrollment	●

- 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.
- **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.
- **Live Finger Detection**: Set the fake fingerprint inspection level. If the fake fingerprint inspection level is higher, the rejection rate on actual human fingerprints will increase.
- **Advanced Enrollment**: You can check the quality of a scanned fingerprint to save high quality fingerprint data. If enabled is selected, the user will be notified when the fingerprint quality is low. This helps users to scan the fingerprints correctly.

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.

NETWORK

Network Settings

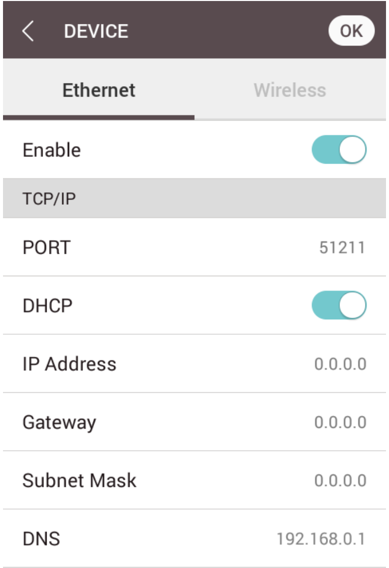
You can change the network settings of the device.

Ethernet

1 Press ⊞ and authenticate with the Admin level credential.

2 Press **Network** > **Device** > **Ethernet.**

3 Enable Ethernet setting.



< DEVICE OK

Ethernet Wireless

Enable	●
TCP/IP	
PORT	51211
DHCP	●
IP Address	0.0.0.0
Gateway	0.0.0.0
Subnet Mask	0.0.0.0
DNS	192.168.0.1

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

4 To modify network information manually, disable DHCP setting. When you press ✎, you can modify **PORT**, **IP Address**, **Gateway**, **Subnet Mask** and **DNS**.

Note

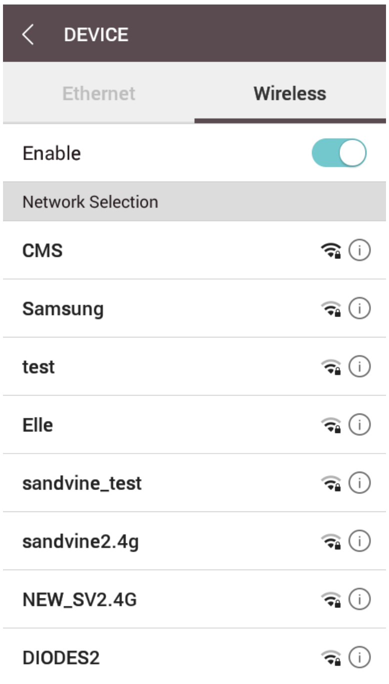
- **Ethernet** cannot be used with **Wireless** at the same time.

Wireless

1 Press ⊞ and authenticate with the Admin level credential.

2 Press **Network** > **Device** > **Wireless**.

3 When you activate Wireless setting, the list of networks available to connect will be displayed.



DEVICE

Ethernet | Wireless

Enable

Network Selection

CMS

Samsung

test

Elle

sandvine_test

sandvine2.4g

NEW_SV2.4G

DIODES2

4 Select the network you wish to connect to and enter the password. When you press **OK**, the connection to the wireless network will be made.

5 To set the network information of wireless LAN manually, press ⓘ of the network name you wish to use and disable DHCP setting. Pressing ✎ allows you to modify IP Address, Gateway and Subnet Mask.

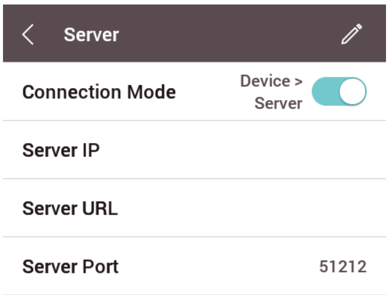
Note

- **Wireless** cannot be used with **Ethernet** at the same time.
- To connect to **Wireless**, a wireless router is required. For content regarding the installation and configuration of wireless router, refer to the user's manual of the wireless router.

Server

1 Press ▦ and authenticate with the Admin level credential.

2 Press **Network** > **Server**.



Server

Connection Mode: Device > Server

Server IP

Server URL

Server Port: 51212

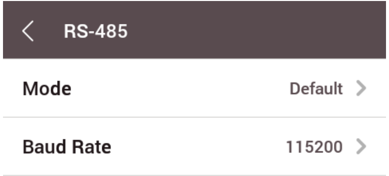
- **Connection Mode**: When you select **Device** > **Server**, you can send a connection signal from the device to a server with the input information directly. When you select **Server** > **Device**, **Server IP** and **Server Port** cannot be entered.
- **Server IP**: Enter the IP of the PC where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

Serial Settings

RS-485

1 Press ▦ and authenticate with the Admin level credential.

2 Press **Network > RS-485** and change the desired item.



RS-485

Mode Default

Baud Rate 115200

- **Mode**: Select the **RS-485** mode.
- **Baud Rate**: Select a desired baud rate.

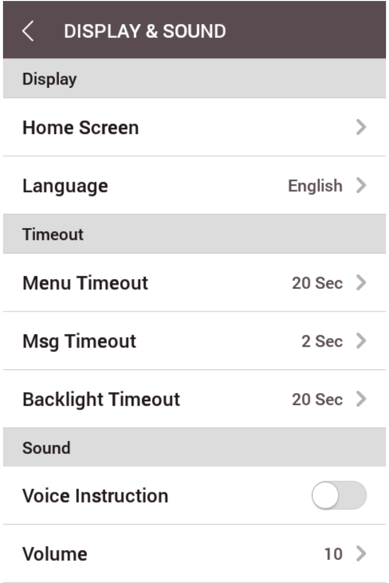
DISPLAY & SOUND

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

1 Press ⊞ and authenticate with the Admin level credential.

2 Press **DISPLAY & SOUND**.

3 Change the desired item.



DISPLAY & SOUND

Display

Home Screen

Language English

Timeout

Menu Timeout 20 Sec

Msg Timeout 2 Sec

Backlight Timeout 20 Sec

Sound

Voice Instruction

Volume 10

- **Home Screen**: Select items to be displayed in the background of the home screen.
- **Language**: Set the language you wish to use.
- **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.
- **Msg Timeout**: Set the time (sec) for a setting complete message or information message to disappear automatically.
- **Backlight Timeout**: Set the time (second) to turn off the lighting of LCD screen.
- **Voice Instruction**: Set to use the voice instruction instead of alarm sounds.
- **Volume**: Set the volume.

Device

Camera

Set by checking the frequency to prevent an image from blinking. BioStation A2 supports both 50 Hz and 60 Hz.

1 Press ⊞ and authenticate with the Admin level credential.

2 Press **Device** > **Camera** > **Power Line Frequency**.

3 Select and set the desired item and press **OK**.

Relay

You can set the open time and the input port of the exit button in the device.

1 Press ⊞ and authenticate with the Admin level credential.

2 Press **Device** > **Relay**.

- **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).

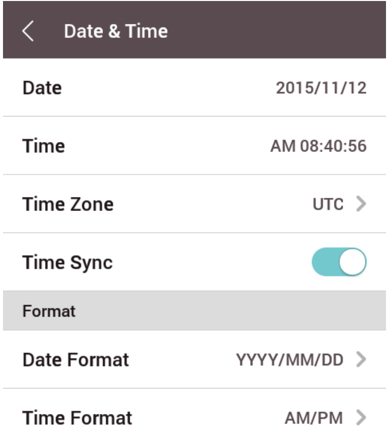
Date & Time

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

1 Press ⊞ and authenticate with the Admin level credential.

2 Press **Device** > **Date & Time**.

3 Change the desired item.



< Date & Time

Date 2015/11/12

Time AM 08:40:56

Time Zone UTC >

Time Sync ●

Format

Date Format YYYY/MM/DD >

Time Format AM/PM >

- **Date**: Check the current date. To modify it directly, disable **Time Sync.**
- **Time**: Check the current time. To modify it directly, disable **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**.

Device Info

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

1 Press ⊞ and authenticate with the Admin level credential.

2 Press **Device** > **Device Info**.

3 You can view the information including **Model Name, Device ID, HW, FW, Kernel, MAC** and **WiFi MAC**.

Memory Info

You can view the status of memory usage.

1 Press ⊞ and authenticate with the Admin level credential.

2 Press **Device** > Memory Info.

USB Memory

You can connect USB memory, import the user information from the device or export the user information or logs to the device. Also, you can upgrade the firmware.

1 Press ⊞ and authenticate with the Admin level credential.

2 Press **Device** > **USB Memory**.

3 Select the desired item and change the setting.

- **Export**: Select information which you want to export to the connected USB memory. Select the desired item and press **OK**.
- **Import**: Select User to import the user information from the connected USB memory. Select the desired item and press **OK**.
- **FW Upgrade**: If firmware files are saved in the connected USB memory, press **OK** to upgrade the firmware.

Note

The type of supported USB memory is as follows. If you use a different type of USB memory, the function may not operate normally.

- Samsung Electronics: SUM-LSB 8GB, SUM-PSB 8GB, SUM-PSB 16GB, SUM-BSG 32GB
- LG Electronics: XTICK J3 WINDY 8GB, SMART USB MU1 White 8GB, MU 1 USB 32GB, MU28GBC 32GB, XTICK MOBY J1 16GB
- SanDisk: Cruzer 16GB, Cruzer Blade CZ50 4GB, Cruzer Blade CZ50 32GB, CZ48 Ultra USB 3.0 64GB, CZ80 USB3.0 64GB, CZ52 64GB, Cruzer Glide Z60 128GB, Cruzer Force CZ71 32GB
- Sony: Micro Vault Click 8GB, MicroVault CLICK 16GB, USM-SA1 32GB
- Transcend: JetFlash 760 8GB, JetFlash 760 32GB, JetFlash 500 8GB
- memorette: MINI500 8GB
- A-DATA: S102 PRO 8GB
- TG Sambo: Pastel 8GB

Restart Device

You can restart the device.

1 Press ⊞ and authenticate with the Admin level credential.

2 Press **Device** > **Restart Device**.

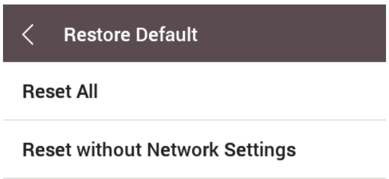
3 To restart the device, press **OK**. To cancel, press **Cancel**.

Restore Default

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

1 Press ▦ and authenticate with the Admin level credential.

2 Press **Device** > **Restore Default**.



3 To reset all device settings, select **Reset All** and press **OK**. To reset all settings except for network settings, select **Reset without Network Settings** and press **OK**.

Note

- When you reset, the user level will be reset as well. After resetting, make sure to set the user 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 ▦ and authenticate with the Admin level credential.

2 Press **DEVICE** > **Factory Default**.

3 To restore the factory defaults, press **OK**.

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 ▦ and authenticate with the Admin level credential.

2 Press **DEVICE** > **Delete the Root Certificate**.

3 To delete the root certificate, press **OK**.

Note

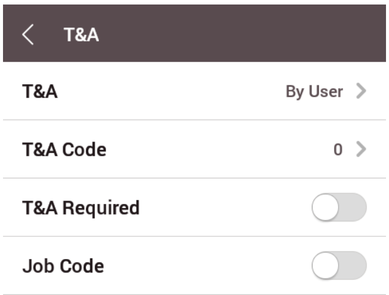
- You can only use **Delete the Root Certificate** when the root certificate is stored on the device and device administrator is set.

T&A Mode

You can set how to register T&A Mode.

1 Press ⊞ and authenticate with the Admin level credential.

2 Press **T&A Mode**.



T&A

T&A By User

T&A Code 0

T&A Required ○

Job Code ○

3 Select and set the desired item.

- **T&A Mode**: Set the method to use T&A mode.
- **T&A Code**: Register a new T&A code.
- **T&A Event**: View T&A event.
- **T&A Required**: Set to require a user to select a T&A event when authenticating.
- **Job Code**: Select whether or not to use **Job Code**.

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

EVENT LOG

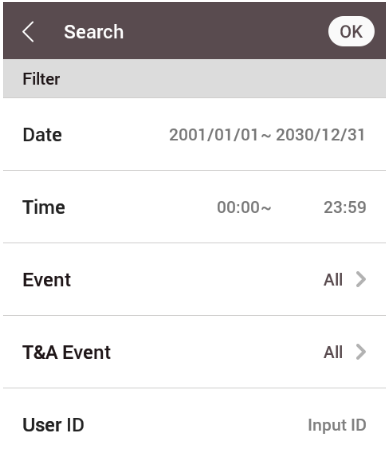
Search Log

You can set a condition and search a log.

1 Press ▦ and authenticate with the Admin level credential.

2 Press **EVENT LOG**.

3 Press ▽ and change the condition. When you press **OK**, a log that matches the condition will be displayed on the screen.



Search

OK

Filter

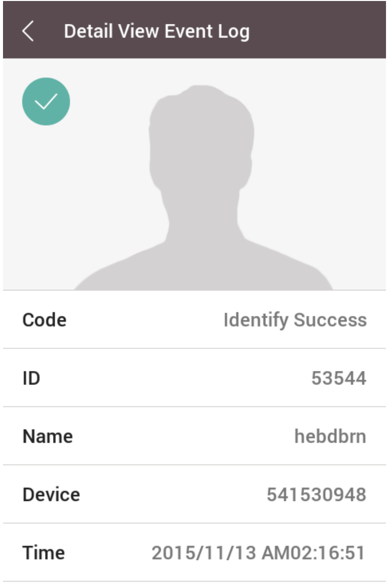
Date	2001/01/01 ~ 2030/12/31
Time	00:00~ 23:59
Event	All >
T&A Event	All >
User ID	Input ID

Detail View Log

1 Press ▦ and authenticate with the Admin level credential.

2 Press **EVENT LOG**.

3 Select a log to view detailed contents.



Detail View Event Log

Code	Identify Success
ID	53544
Name	hebdbrn
Device	541530948
Time	2015/11/13 AM02:16:51

Delete All Logs

You can delete all saved logs.

1 Press ⊞ and authenticate with the Admin level credential.

2 Press **EVENT LOG**.

3 To delete all logs, press 🗑 and then press **OK**. To cancel, press **Cancel**.

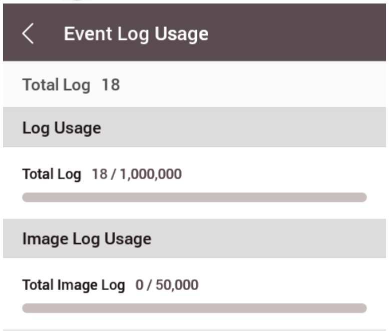
View Log Usage

You can check the status of log usage.

1 Press ⊞ and authenticate with the Admin level credential.

2 Press **EVENT LOG**.

3 Press ⓘ.



Event Log Usage

Total Log 18

Log Usage

Total Log 18 / 1,000,000

Image Log Usage

Total Image Log 0 / 50,000

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 A2 is equipped with a built-in battery but if power is not supplied for a long time, the built-in battery may die, causing the time to become incorrect. You can correct the time by referring to **Date & Time**.
Admin Access	I lost my Admin PIN, so I cannot access the Admin mode.	• The administrator grants an access permission in BioStation A2, so 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.

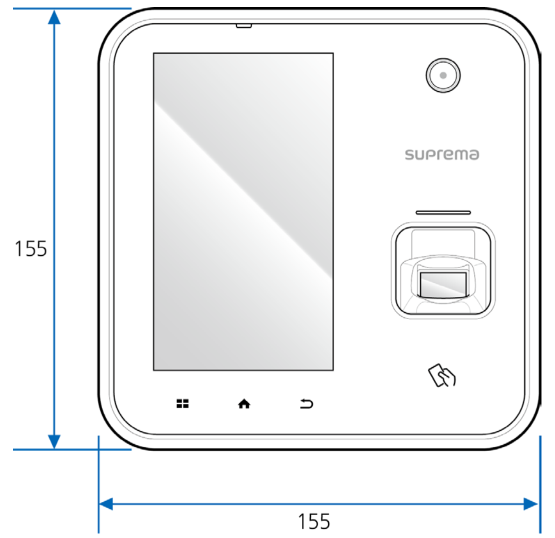
Product Specifications

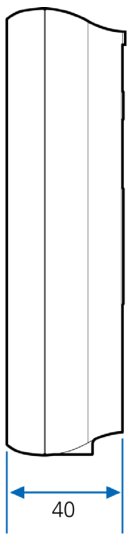
Category	Feature	Specification
Credential	Biometric	Fingerprint
	RF Option	● BSA2-OEPW: 125kHz EM ● BSA2-OHPW: 125kHz HID Prox ● BSA2-OIPW: 13.56MHz MIFARE, MIFARE Plus, DESFire/EV1, FeliCa, iCLASS SE/SR, NFC, ISO14443A, ISO15693 ● BSA2-OMPW: 13.56Mhz MIFARE, MIFARE Plus, DESFire/EV1, FeliCa, NFC, ISO14443A, ISO15693
	RF read range*	EM/HID Prox: 50 mm, MIFARE: 50 mm, DESFire: 50 mm, Felica: 30 mm, ISO15693: 50 mm
	LFD	Supported
General	CPU	1.0 GHz Quad Core
	Memory	8GB Flash + 1GB RAM
	LCD type	5" color TFT touch
	LCD resolution	480 x 854
	LED	Multiple colors
	Sound	24 bit/Voice DSP (echo cancel)
	Operating temperature	-20 °C - 50 °C
	Storage temperature	-40 °C - 70 °C
	Operating humidity	0% - 80%, non-condensing
	Storage humidity	0% - 90%, non-condensing
	Camera type	CMOS 2M pixels
	Camera resolution	1600 x 1200
	Camera angle	Diagonal 122°, Horizontal 64.7°, Vertical 103.3°
	Dimension (W x H x D)	155 mm x 155 mm x 40 mm
	Weight	Device: 440 g Bracket: 89 g (Including washer and bolt)
	Certificates	CE, FCC, KC, RoHS, REACH, WEEE
Fingerprint	Image dimension	272 x 320 pixels
	Image bit depth	8bit, 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	5,000,000
	Max. Image Log	50,000
Interface	Wi-Fi	Supported
	Ethernet	Supported (10/100 Mbps, auto MDI/MDI-X)
	RS-485	1ch Host or Slave (Selectable)
	Wiegand	1ch Input, 1ch Output
	TTL input	1ch Input
	Relay	2 Relay
	USB	USB 2.0 (Host)
	SD Card	microSD card (Supports up to 32GB)
	PoE	Supported (IEEE 802.3af compliant)
	Tamper	Supported
Electrical	Power	Voltage: 12 VDC Current: Max. 850 mA
	Switch input VIH	Min.: 3 V Max.: 5 V
	Switch input VIL	Max.: 1 V
	Switch Pull-up resistance	4.7 kΩ (The input pots are pulled up with 4.7 kΩ.)
	Wiegand output VOH	More than 4.8 V
	Wiegand output VOL	Less than 0.2 V
	Wiegand output Pull-up resistance	Internally pulled up with 1 kΩ
	Relay	Voltage: Max. 30 VDC Current: Max. 1 A

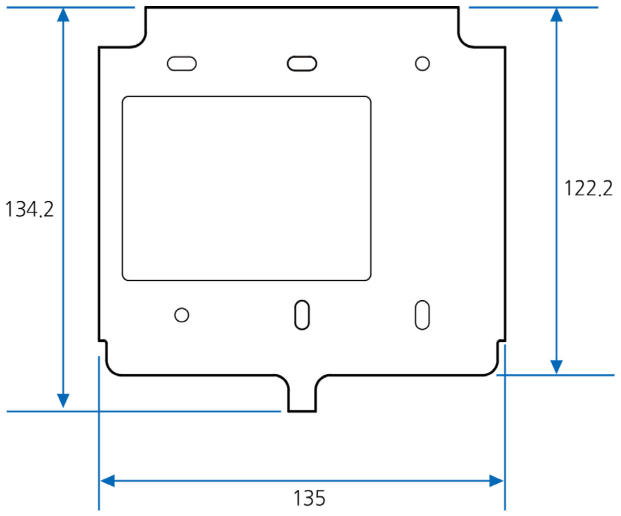
* RF read range will vary depending on installation environment.

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.

EU Declaration of Conformity (CE)

This product is CE marked according to the provisions of the R&TTE Directive (1999/5/EC).
Suprema Inc. hereby declares that this product is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC. This device is Class 1 radio equipment under the European Radio and Telecommunications Terminal Equipment (R&TTE) Directive (1999/5/EC).

For more information, contact us using the following contact information.
Suprema Inc.
Website: https://www.supremainc.com
Address: Parkview Tower F16, 248, Jeongjail-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, Korea (Jeongja-dong 6)
Tel: .31-783-4510 / Fax: 031-783-4517

Appendix

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

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