BioStation 3

USER GUIDE

Version 1.13

English
EN 102.00.BS3

suprema
SECURITY & BIOMETRICS

CONTENTS

Safety Instructions 4

Compliance Information 4

Getting Started 8

Components 8

Name and function of each part 9

Cables and connectors 11

Correct face enrollment and authentication method 18

Note for QR code usage and device license 19

Installation 20

Fixing the bracket and the product 20

Power supply connection 30

Network Connection 31

Input connection 32

Relay Connection 33

Connecting as a Standalone 35

Connecting to Secure I/O 2 37

Wiegand Connection 38

How to Use 39

Admin Menu 39

User 41

Authentication 45

Settings 53

Event Logs 71

Troubleshooting 73

Check items before reporting a malfunction 73

Product Specifications 75

Credentials 75

General 75

Capacity 76

Interface 77

Electrical 78

Dimensions and Weight 79

Regulatory Information 81

Regulatory & Licenses 81

FCC Compliance Information 82

IC information 83

EU Declaration of Conformity (CE) 83

Appendices 84

Disclaimers 84

Copyright Notice 85

Open Source License 85

Safety Instructions

Please read this safety instructions before you use the product to prevent injury to yourself and others and to prevent property damage.

The term ‘product’ in this manual refers to the product and any items provided with the product.

Compliance Information

Warning

Used to indicate warning information that could lead to serious injury or death if violated while using the product.

Caution

Used to indicate caution information that may result in minor injury or product damage if violated while using the product.

Info

Used to provide notes or additional information while using the product.

Note

Used to provide notes or additional information while using the product.

⚠ Warning

Install

Be especially careful of miswiring when using high-capacity power supplies.

- Serious fires, electric shocks, or product damage may occur due to miswiring.

Do not allow users to install or repair the product arbitrarily.

- Causes fire, electric shock, or injury.
- No free repair service will be provided if the product is damaged due to arbitrary installation or repair by the user.

Do not install the product in places exposed to direct sunlight, moisture, dust, or soot, or where gas may leak.

- May cause fire or electric shock.

When installing the product outdoors, make sure to install it in a shaded and well-ventilated area.

Do not use a completely sealed enclosure when installing the product outdoors.

- The internal temperature of the enclosure may rise due to direct sunlight, causing fire, electric shock, or product damage.

Do not install the product in places where heat is generated, such as near heaters.

- May cause fire or electric shock due to overheating.

Do not install in damp places.

- May cause electric shock or product damage due to moisture.

Do not install in places with electromagnetic interference.

- May cause electric shock or product damage.

Usage

Do not allow liquids such as water, beverages, or chemicals to enter the product.

- May cause fire, electric shock, or product damage.

Do not use damaged power adapters or plugs, or loose outlets.

- If connections are unstable, may cause fire or electric shock.

Do not bend or break the power cord excessively.

- May cause fire or electric shock.

⚠ Caution

Install

Read this manual carefully before installing the product to ensure safe and correct installation.

When wiring power cables and connectors, make sure to turn off the power to all devices you are connecting before wiring and connecting.

- Devices may malfunction.

Before connecting the power to the product, check the manual again to ensure that wiring is correct, then connect the power.

Do not install the product in places directly exposed to sunlight or ultraviolet light.

- May cause product damage, malfunction, discoloration, or deformation.

Do not leave power cables in passageways.

- May cause bodily injury or product damage.

Do not install near strong magnetic objects such as magnets, TVs, CRT monitors, or speakers.

- The device may malfunction.

When installing multiple devices, ensure the minimum spacing distance is observed.

- May affect the RF and BLE performance of other devices, causing them to malfunction.

Use a power adapter that has IEC/EN 62368-1 approval and is rated above the power consumption of the terminal device. It is recommended to use the power adapters sold by Suprema.

- Using an unsuitable power supply may cause devices to malfunction.
- Refer to the Power in the product specifications for maximum current consumption specifications.

Ensure that the product and Secure I/O 2, electric lock (electronic locking device) use separate power supplies.

- Devices may malfunction.

Do not connect the power supply and PoE+ power together.

- Devices may malfunction.

To meet IP65 standards, make sure to use a cable cover after connecting the product and cable. It is recommended to use an enclosure when installed outdoors with full exposure.

- Decreased waterproof and dustproof performance may cause malfunction.

When connecting PoE+ power, make sure to connect it according to PoE+ or PoE++ standards.

- Using standard PoE may cause devices to operate unstably or be permanently damaged.

Usage

Do not drop or subject the product to shock.

- The device may malfunction.

Ensure the power supply is not interrupted during firmware upgrades of the product.

- The device may malfunction.

Manage the password so others do not know it, and change it regularly.

- This may lead to unauthorized access.

Do not press the product's buttons (touchpad) forcefully or use sharp tools to press them.

- The device may malfunction.

Use the product within -20 °C to 50 °C and store it at appropriate temperatures, not too low or too high.

- The device may malfunction.

Be careful when cleaning the product.

- Gently wipe the product surface with a clean, dry cloth.
- If disinfecting the product, dampen a clean cloth with a suitable amount of disinfectant alcohol and gently wipe the product surface. Use disinfectant alcohol that contains 70-75% isopropyl alcohol and a clean, lint-free soft cloth.
- Do not spray disinfectant directly onto the product.

Do not use the product for purposes other than its intended use.

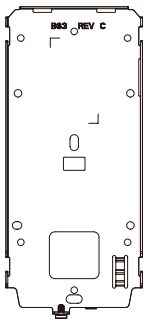
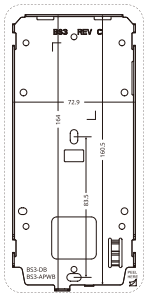
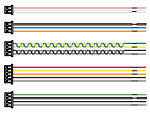
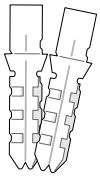
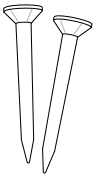
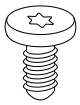
- The device may malfunction.

> **RTC Battery**
>
> Replacing with unauthorized or incorrect types of batteries may pose a risk of explosion. Dispose of batteries according to local or international waste regulations.

Getting Started

Provides initial procedures for getting started with the device.

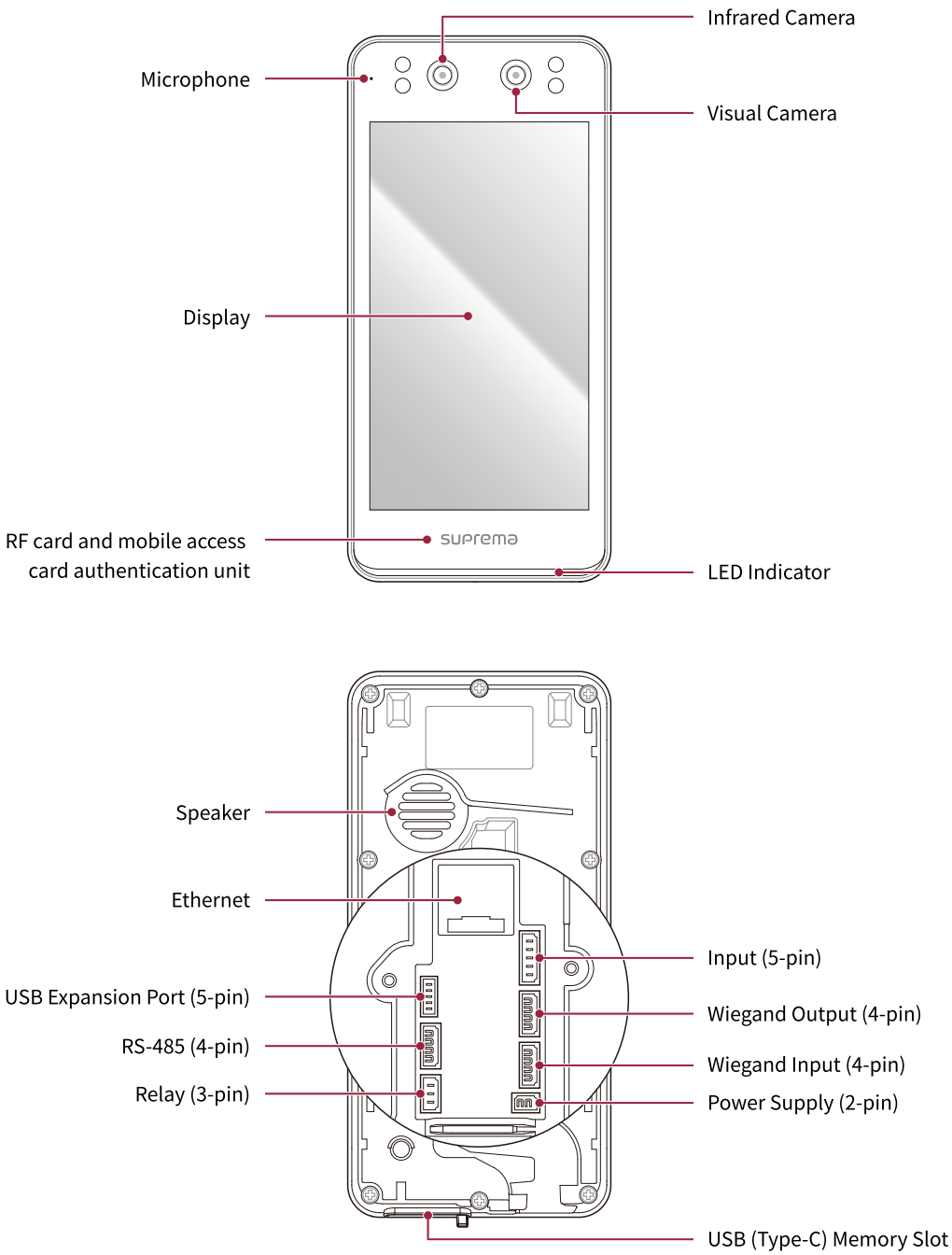
Components

				
BioStation 3	Wall Bracket	Drilling Template	Quick Guide	Connection Cables
				
Diode	120 Ω Resistor	PVC Anchors x2	Fixing Screws x2	Bracket Fixing Screw (Star Shaped)

Info

- Components may vary according to the installation environment.
- When assembling the product with the bracket, you can use the included bracket fixing screw (Star Shaped) instead of the product fixing screw for enhanced security.

Name and function of each part



- **Microphone**: Transmits the voice of the user when the interphone is connected.
  - Covering or blocking the microphone may interfere with voice transmission.
- **Infrared Camera**: Capture the infrared face image.
- **Visual Camera**: Capture an actual face image.
- **Display**: Provides a UI for operation.
- **RF card and mobile access card authentication unit**: Part to scan a RFID card or mobile access card for entrance.
- **LED Indicator**: Indicates the operational status of the device with the color of the LED.

  - Green: Authentication success.
  - Red: Authentication failure.
  - Blue: Normal operation.
  - Blue/Green blinking:
    - When setting **DHCP** to use, unable to retrieve IP address.
    - When in **Slave** mode, the connection to the master device is disconnected.
  - Red/Purple blinking: Device is locked.
  - Yellow blinking: Waiting for input.
- **Speaker**: Delivers sound.
- **Ethernet**: Connect the Ethernet cable.
- **Input (5-pin)**: Connect the input cable.
- **USB Expansion Port (5-pin)**: Connect other accessory products.
- **Wiegand Output (4-pin)**: Connect the Wiegand Output cable.
- **Wiegand Input (4-pin)**: Connect the Wiegand Input cable.
- **RS-485 (4-pin)**: Connect the RS-485 cable.
- **Relay (3-pin)**: Connect the Relay cable.
- **Power Supply (2-pin)**: Connects the power supply cable.
- **USB (Type-C) Memory Slot**: Connects the USB memory.

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

Input



Pin	Name	Color
1	INPUT0	Red
2	INPUT1	Yellow
3	INPUT2	Orange
4	INPUT GND	Black
5	SH GND	Gray

Wiegand input



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

Wiegand output



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

Set Up Master Administrator CE-oriented products

The **Master Admin** feature enhances the overall admin privileges of the device to improve device security and prevent unauthorized access and configuration changes. This feature applies only to **CE-oriented products** for the EU region, and **Master Administrator enrollment is required** on **CE products**. Only the enrolled master administrator can access the administrator menu and change device settings.

Info

- This feature is a required policy introduced to enhance security for **CE-oriented products** in the EU region, and it is not supported on **Global (Non-CE) products**.
- The master admin cannot delete directly and will be deleted only during **Factory Default**.

Master administrator support policy CE products vs Global (Non-CE) products

The **Master Admin** feature is activated only on **CE products with a label that has the CE mark**.

Use the sticker on the back label to identify **CE products** and **Global (Non-CE) products**. The feature works differently as follows.

- **CE products**: CE mark present
- **Global (Non-CE) products**: CE mark absent

Category	CE-oriented products	Global (Non-CE) products
Master Admin	Enabled (cannot disable)	Not supported
Admin 2-step Authentication	Required	Not supported
Minimum PIN length	At least 8 digits	At least 4 digits

When connected to BioStar X (or BioStar 2), the Master Admin setting changes based on device support, and the enablement of the Admin 2-step Authentication menu syncs automatically.

Behavior Logic During Firmware Upgrade

When you upgrade the firmware of an existing device, support for **Master Admin** and **Admin 2-step Authentication** can vary based on the combination of the **version before upgrade** and the **target version**.

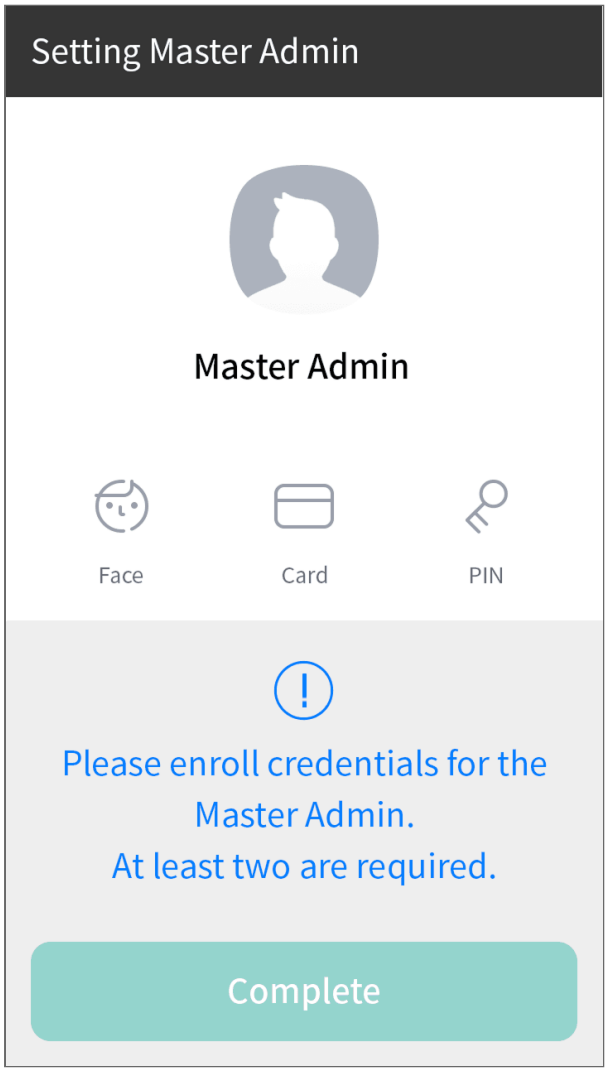
Contact Suprema Global Technical Support Team for detailed version support availability.

Register master admin on a new device

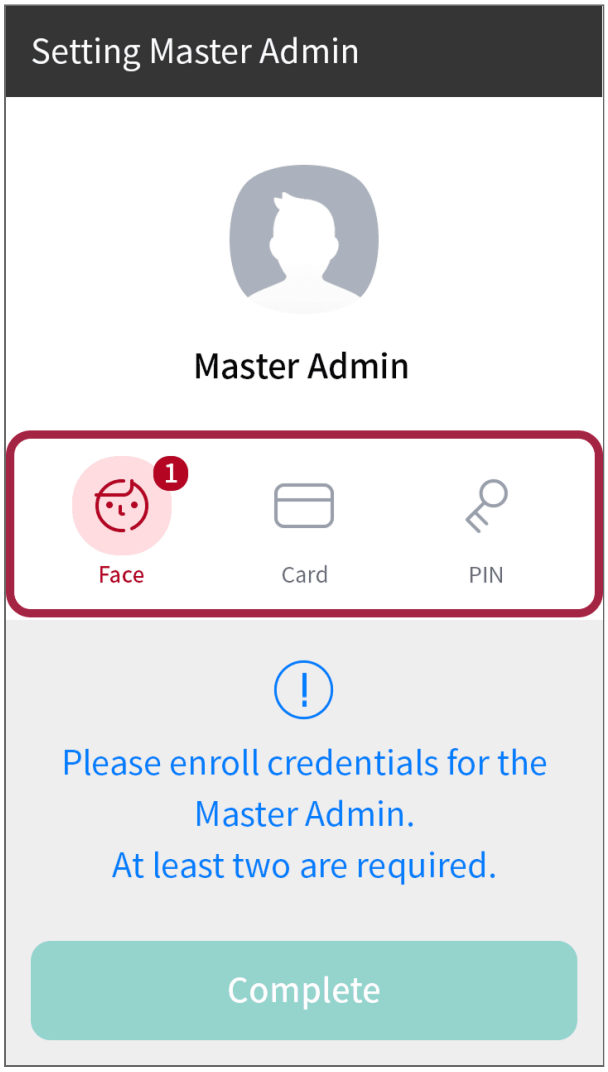
On a new device for CE products, you must enroll **Master Admin** from the start. If you do not enroll it, device use is restricted.

> **Info**
>
> - At first boot, the **Master Admin** enrollment screen appears. If you do not complete enrollment, you cannot move to the next screen.
> - Even if you connect to BioStar X (or BioStar 2) and assign a device-wide administrator, you must enroll **Master Admin** directly on the device to use all features.
> - New devices cannot perform firmware downgrades.

1. When the new device is booted for the first time, the **Master Admin** registration screen will appear.



2. According to EU security policy, **Master Admin** must enroll credentials of at least two types. Select and enroll two desired credentials.



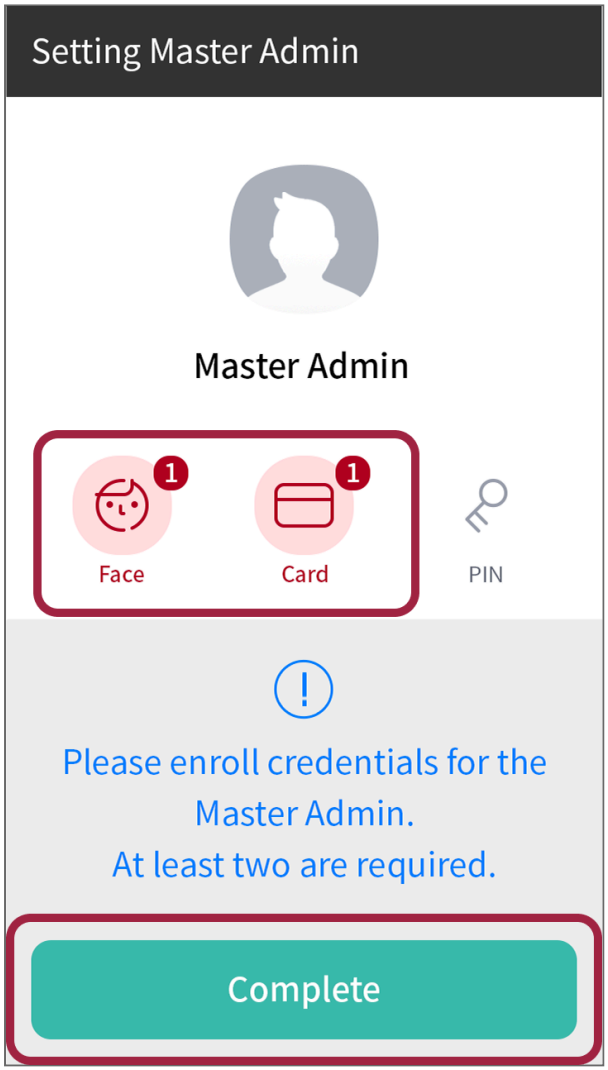
The credentials that can be enrolled for **Master Admin** are as follows.

Credential type	Number of enrollments	Conditions
Card	Up to 4	Supports only CSN and Wiegand types Duplicate enrollment within the same type is not allowed
Face	Up to 2	Enroll only on devices with the same algorithm
Fingerprint	Up to 2	-
PIN	1	At least 8 digits long (CE regulation applies)

Enrollment conditions

- You must enroll at least two types of credentials.
- All credentials supported by the device can be used as authentication means.

3. After enrolling two or more types of credentials, press the **Complete** button to complete the registration of **Master Admin**.



Additional Information

- **When enrolling PIN through BioStar software**

  Global (Non-CE) products that do not support the master administrator can enroll a PIN of at least 4 digits directly on the device. However, when enrolling users through BioStar X (or BioStar 2), the following versions require a PIN with at least 8 digits.

  – BioStar 2 v2.9.11 or later

  – BioStar X v1.0.0 to v1.0.2

  Users enrolled with a 4-digit PIN in the versions above cannot be assigned as device administrators.

- **Manual Device Hash Key Change**

  When manually changing the device hash key, a warning message will indicate that Master Admin PINs will be deleted. Please confirm the message before proceeding.

- **RS-485 Biometric Image Transmission Restriction**

  Biometric credential images are not transmitted over RS-485 communication, so substitute images appear when viewing the registered Master Admin face on slave devices.

Correct face enrollment and authentication method

Cautions for enrolling a faces

- Keep the distance between the device and your face at 60-100 cm when enrolling your face.
- Do not change your face expression.
- Do not wear masks, hats, or eye patches.
- Do not enroll a face wearing a mask. It may increase the False Acceptance Rate (FAR) if both faces with and without a mask are enrolled.
- Do not raise head up or lower head.
- Do not wear thick makeup.
- Do not close your eyes.
- Make sure that both of your shoulders correctly appear on the screen.
- Stand still and enroll your face by staring at the screen.
- Be careful not to display two faces on the screen. Enroll one person at a time.
- If you do not follow the instructions on the screen, the face enrollment may take longer or may fail.

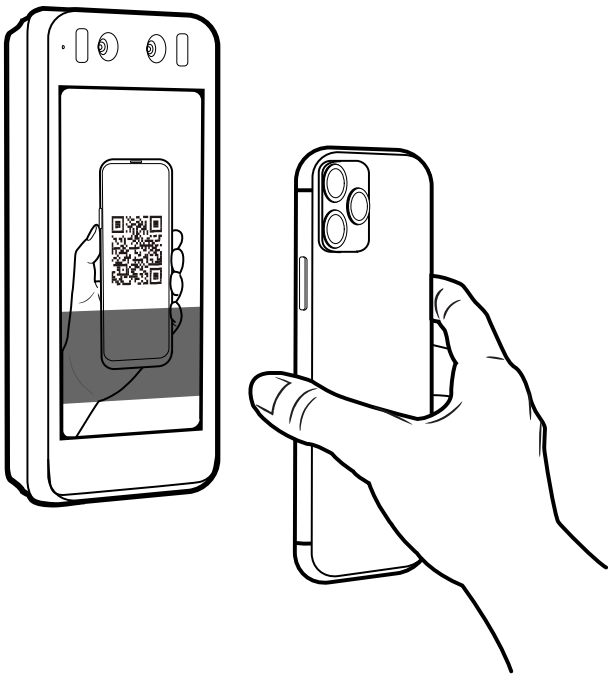
Cautions for authenticating a face

- Ensure that the face appears in the center of the device’s screen. When the guideline is displayed, follow the instructions shown on the screen to authenticate the face.
- If a part of the face is covered with a hat, a mask, an eye patch, or sunglasses authentication may fail. Do not cover the face; allow the device to recognize both the eyebrows and the face.
- Authenticate at a location 60~100 cm away from the device.
- Make sure that both of your shoulders correctly appear on the screen. Authentication may fail if your shoulders are not at the same height. Stand still, and then authenticate your face.

Note for QR code usage and device license

How to scan a QR code

You can issue a QR code to a user and use it as an authentication method. Scan the QR code properly by following the instructions on the screen to increase the recognition rate.



- Keep the distance between the device's camera and the QR code at 30~40 cm.
- Position the QR code in the center of the scan screen of the device.
- When authenticating with the QR code downloaded to your smartphone, adjust the brightness of your smartphone so that the device can read the QR code clearly.

Notes for device license

- Using the QR Code authentication requires a separate device license. Contact the place of purchase to issue a device license.
- The device license file is an encrypted file and cannot be modified arbitrarily.
- Device licenses are issued based on device ID. If the device ID is changed in an unusual way, the warranty service for the license is not provided.

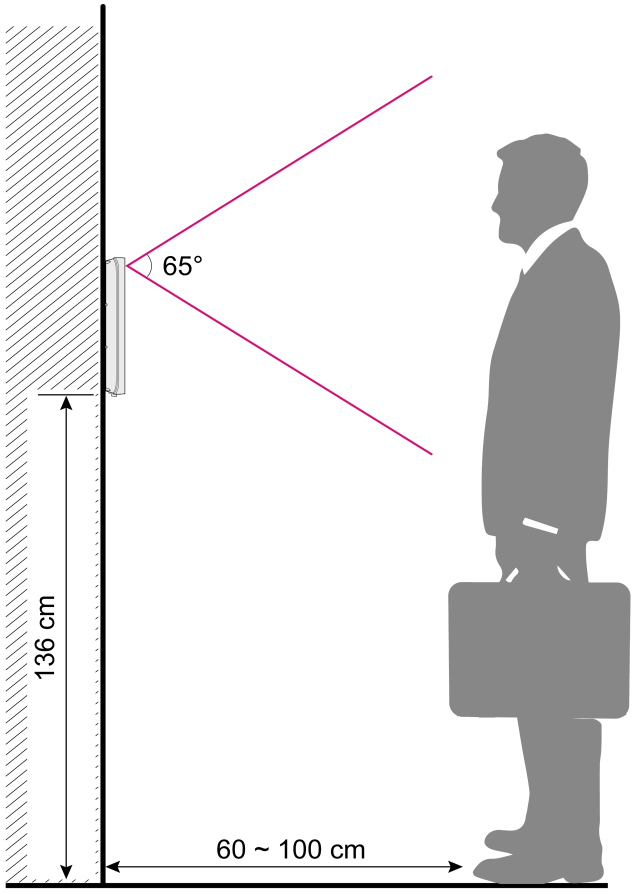
Installation

Provides the complete installation procedures and connection examples required for the device.

Fixing the bracket and the product

General bracket

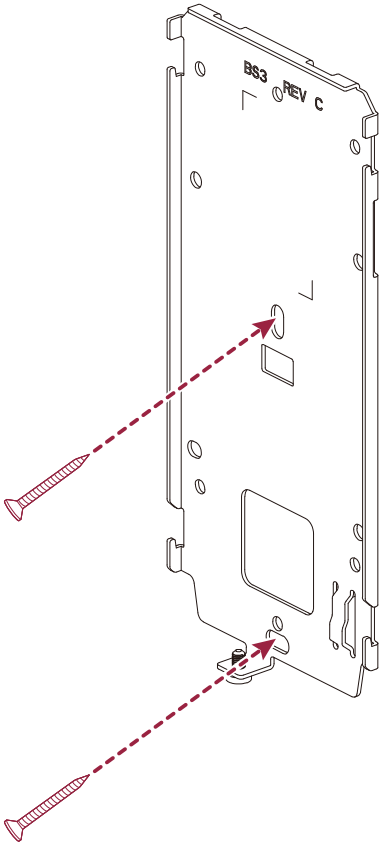
1. Determine the correct position to install the bracket using the provided drilling template.



Info

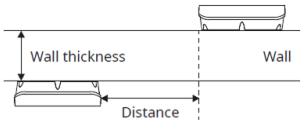
- The optimal height for installing device is 136 cm.
- Install the device where it does not reach the direct sunlight or UV light.
- Adjust the installation position so that the face is not exposed to direct sunlight when a user tries to authenticate.

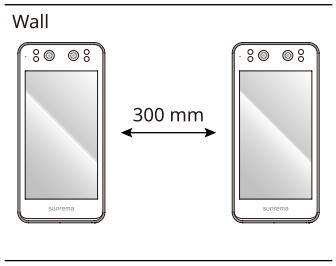
2. Secure the bracket tightly using the fixing screws at the location where the product will be mounted.



Info

- If installing the product on a concrete wall, drill a hole, insert a PVC anchor, and secure it with a fixing screw.
- To avoid RF interference, a minimum separation distance must be maintained.

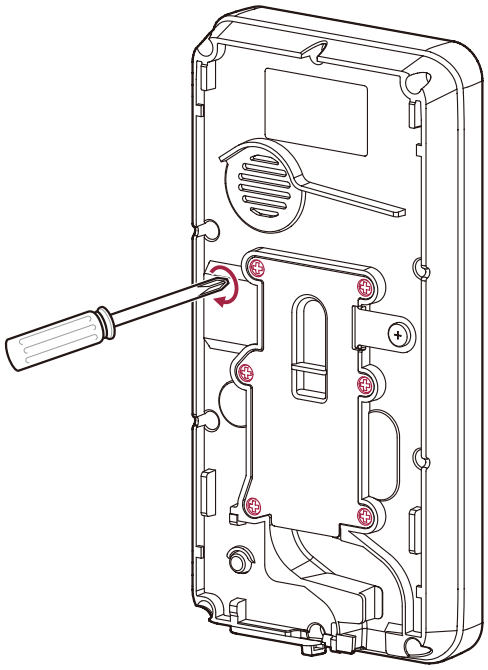




Wall thickness	Distance
100 mm	200 mm
120 mm	180 mm
150 mm	150 mm

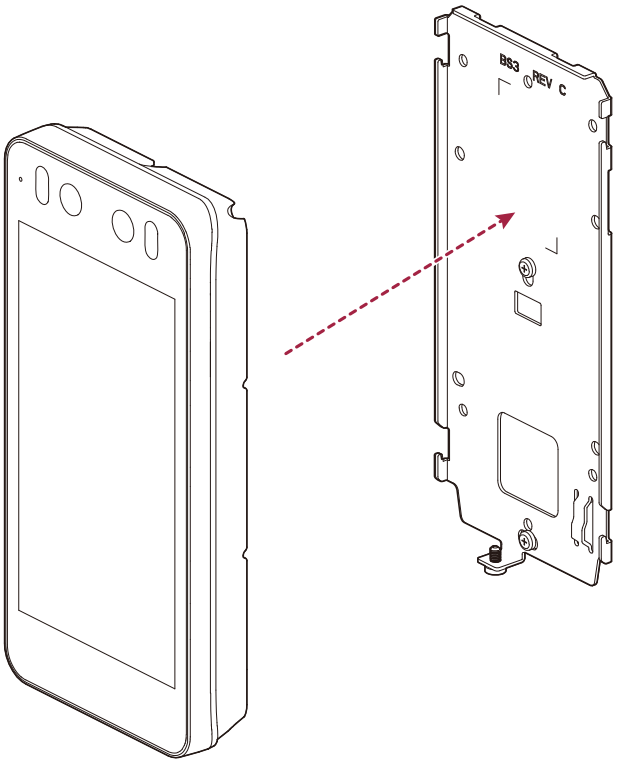
- When using a mobile access card, install devices maintaining a minimum distance of 1 m between devices to avoid BLE interference.

3. After attaching the cable cover, tighten the six screws on the cover to secure it firmly.

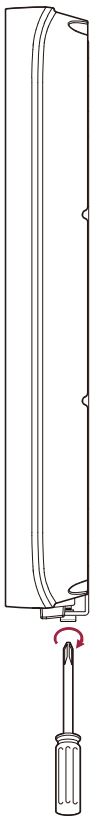


> **Info**
> Make sure that the cable cover is completely closed after connecting it to the product to maintain the water-resistant and dust-resistant features (IP65 rating).

4. Mount the product on the fixed bracket.



5. Rotate the fixing screws to assemble the product with the bracket.



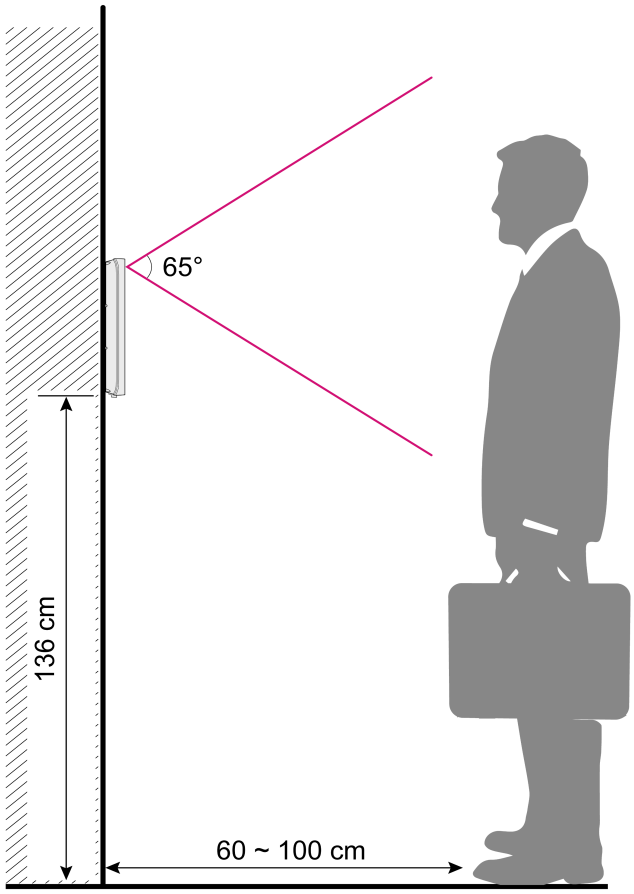
Info

When assembling the product with the bracket, you can use the included bracket fixing screw (Star Shaped) instead of the product fixing screw for enhanced security.

Tilting Bracket

Use the dedicated tilting bracket to adjust the authentication angle to suit the installation environment. The tilting bracket is sold separately.

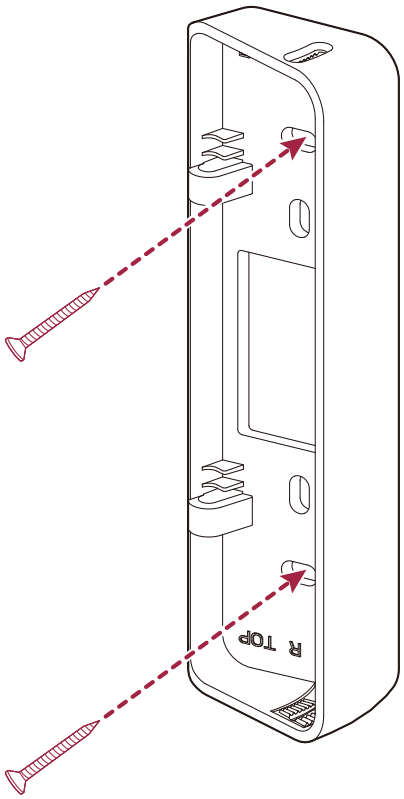
1. Determine the correct position to install the bracket using the provided drilling template.



Info

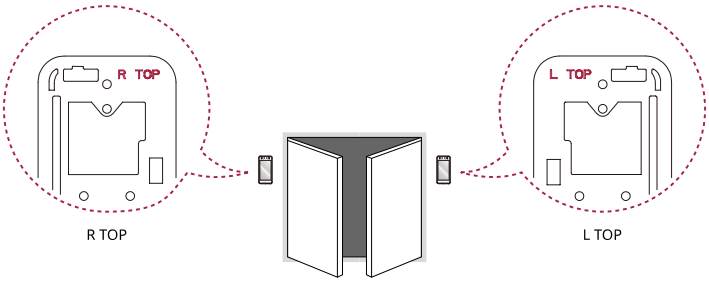
- The optimal height for installing device is 136 cm.
- Install the device where it does not reach the direct sunlight or UV light.
- Adjust the installation position so that the face is not exposed to direct sunlight when a user tries to authenticate.

2. Use the tilting bracket mounting screws to secure the back of the tilting bracket firmly to the installation location (wall).



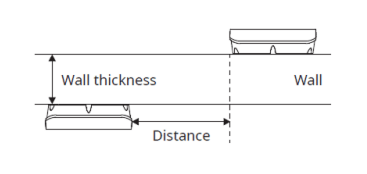
Depending on the installation location, install the tilting bracket with the top and bottom orientation as follows.

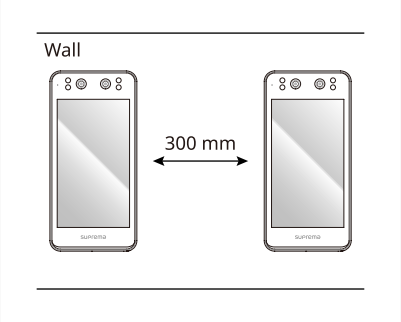
- When installing on the left side of the entrance: Install so the "R TOP" marking faces upward
- When installing on the right side of the entrance: Install so the "L TOP" marking faces upward



Info

- If installing the product on a concrete wall, drill a hole, insert a PVC anchor, and secure it with a fixing screw.
- To avoid RF interference, a minimum separation distance must be maintained.

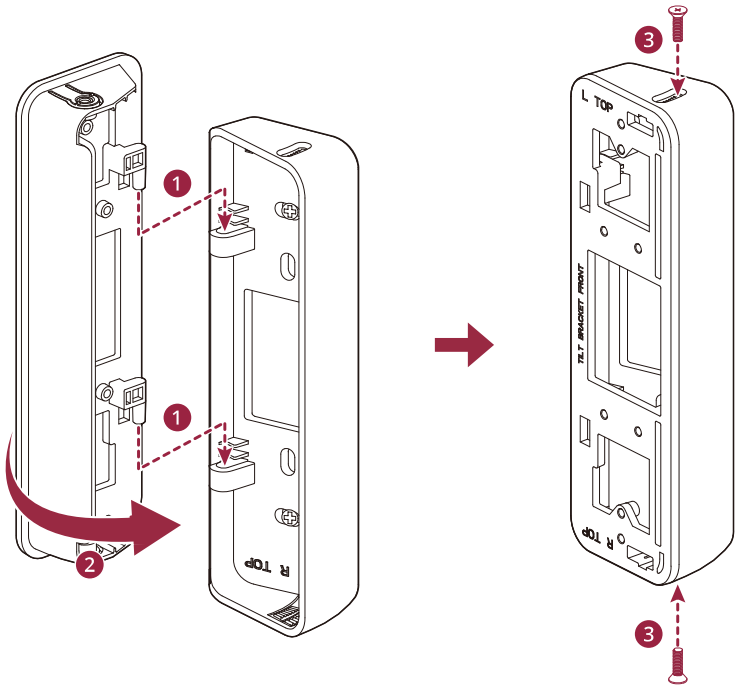




Wall thickness	Distance
100 mm	200 mm
120 mm	180 mm
150 mm	150 mm

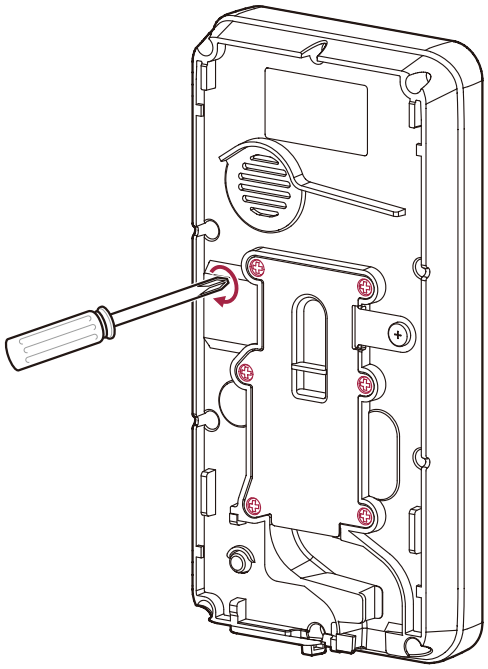
- When using a mobile access card, install devices maintaining a minimum distance of 1 m between devices to avoid BLE interference.

3. Join the front of the tilting bracket to the groove in the back, close it, and secure it with two screws in the upper and lower screw holes.



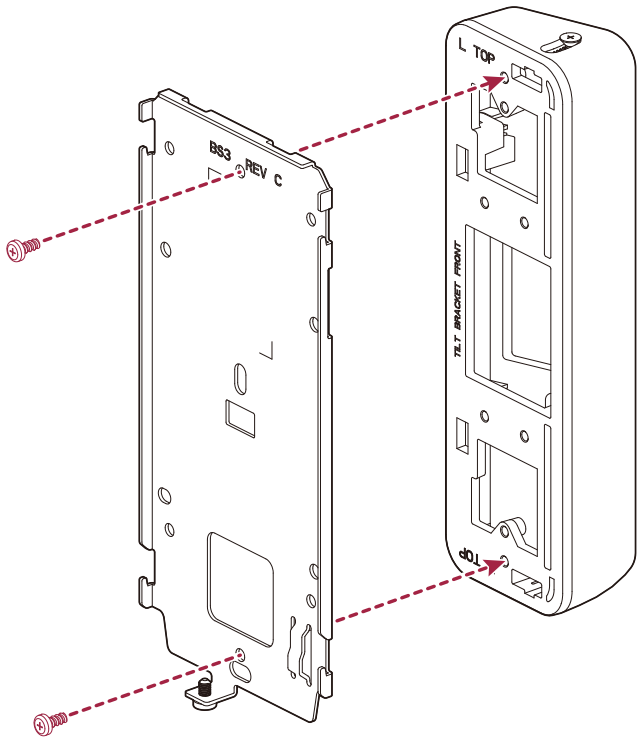
> **Info**
> If you tighten the screws too much, the angle cannot be adjusted. Tighten the screws to the proper level.

4. After attaching the cable cover, tighten the six screws on the cover to secure it firmly.

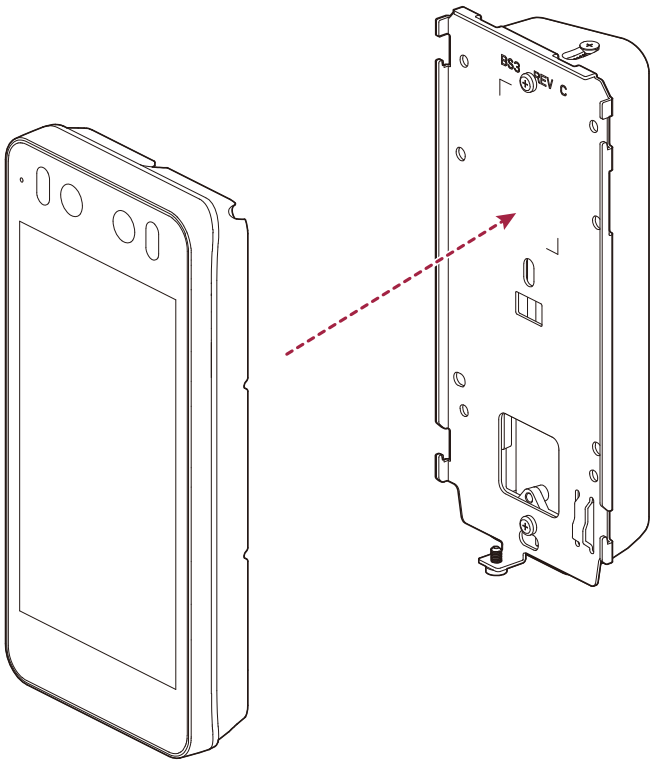


> **Info**
> Make sure that the cable cover is completely closed after connecting it to the product to maintain the water-resistant and dust-resistant features (IP65 rating).

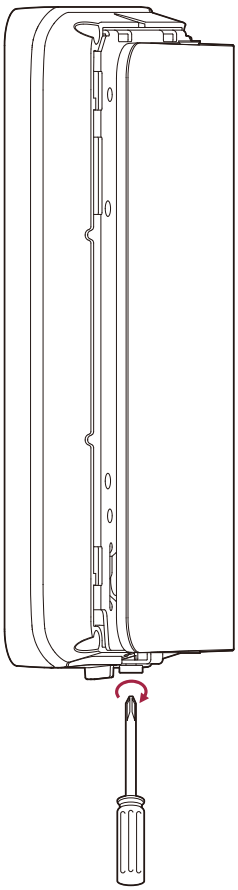
5. Secure the wall-mount bracket firmly on top of the tilting bracket.



6. Mount the product on the secured wall-mount bracket.



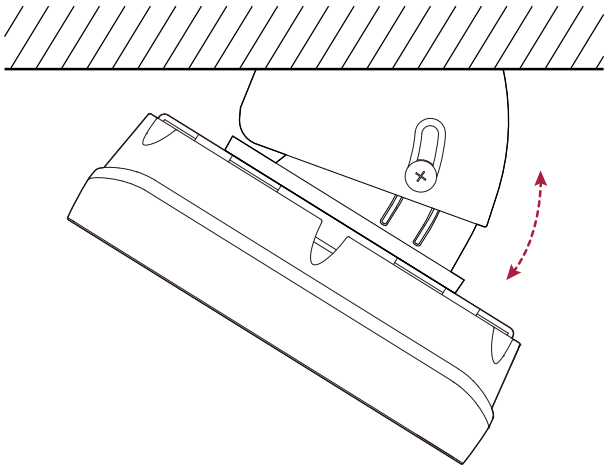
7. Tighten the product fixing screws to assemble the product and the wall-mount bracket.



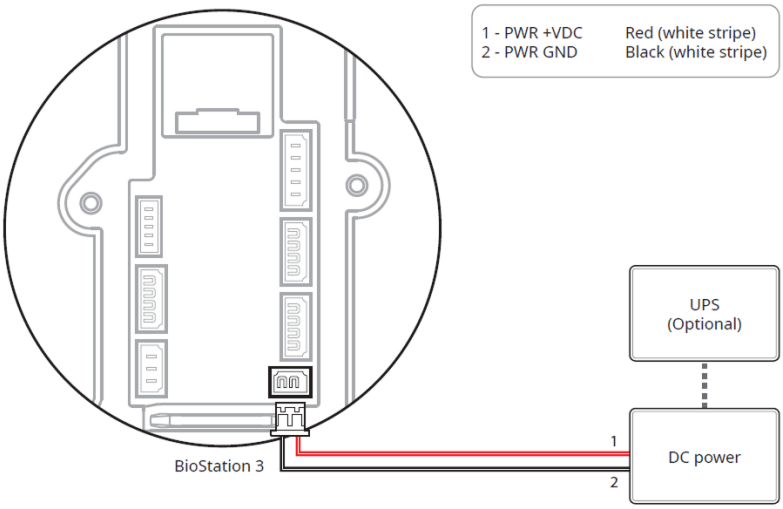
Info

When assembling the product with the bracket, you can use the included bracket fixing screw (Star Shaped) instead of the product fixing screw for enhanced security.

8. Adjust the tilting bracket to the desired angle.



Power supply connection



Caution

- DO NOT connect the device to the DC power supply (or adapter) and PoE power supply at the same time.
- Use the IEC/EN 62368-1 approved power adapter that supports higher power consumption than the product. If you wish to connect and use another device to the power supply adapter, you should use an adapter with a current capacity which is the same or larger than the total power consumption required for the terminal and another device.
  - Refer to the Power in the product specifications for maximum current consumption specifications.
- Use a separate power supply for Secure I/O 2, the electric lock, and the product respectively. If connecting and using the power supply to these devices together, the devices may malfunction.
- When connecting the power supply, be aware of the distance between the device and the power supply. The device should be connected as close as possible to the power supply so that the length of the connecting cable is kept to a minimum. If cable connections are made improperly it may cause the device to malfunction. It is recommended to use a 16 AWG or 18 AWG cable if the product is far from the power supply. The connection distance may differ depending on the standard of the cable used and the installation environment. This product supports both DC 24 V and DC 12 V power, so check the maximum length according to the cable specification to ensure that the unit is properly powered.

Cable standard	Max. extended length	
	DC 12V	DC 24V
16 AWG	50 m	150 m
18 AWG	30 m	136 m
20 AWG	20 m	90 m

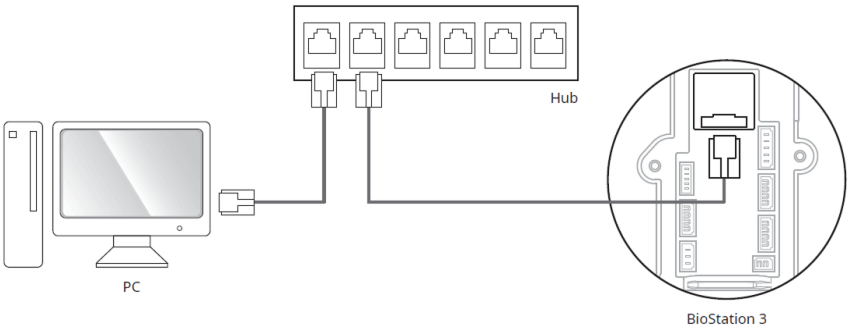
- DO NOT extend the length of power cable when using the power adapter.
- DO NOT use the CAT5 UTP 2-Wire for power supply purpose.

Network Connection

TCP/IP

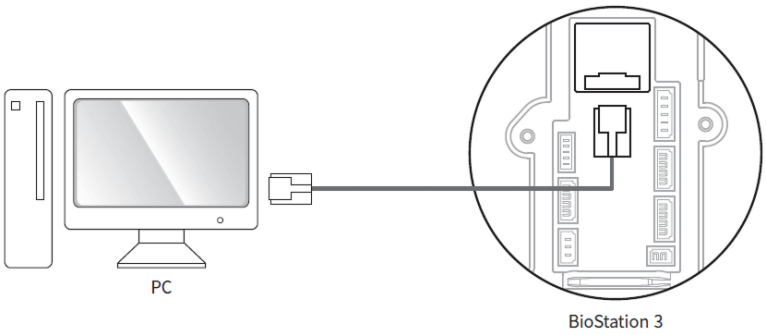
LAN connection (connecting to a hub)

You can connect to a hub using a standard CAT-5 or higher cable.



LAN connection (connecting to a PC directly)

This product supports automatic MDI/MDIX, so it can connect directly to a PC using either a crossover cable or a standard straight CAT-5 or higher cable.



Info

For a gigabit Ethernet switch, check the following information.

- Use a CAT-5e UTP (unshielded twisted pair) cable.
- Use all 4 pairs (8 wires) for the network connection.
- Do not use any pairs or wires in the network cable for other purposes.

Network ports and services

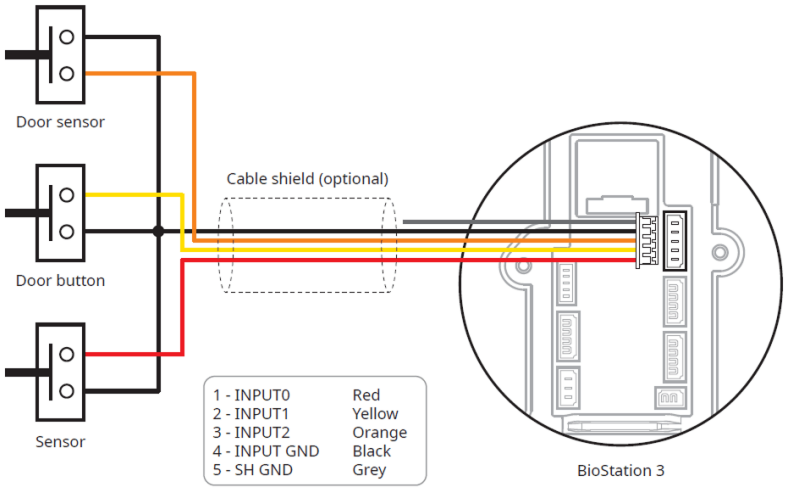
This device uses the following ports for network communication and stable service operation.

Protocol	Service
TCP	Used for communication services between the server and the device, and for the device operation status switching service.
UDP	Used for the device discovery service to search for devices on the network.

Info

These ports provide the product's normal network features. When configuring firewall rules or network security settings, allow these ports.

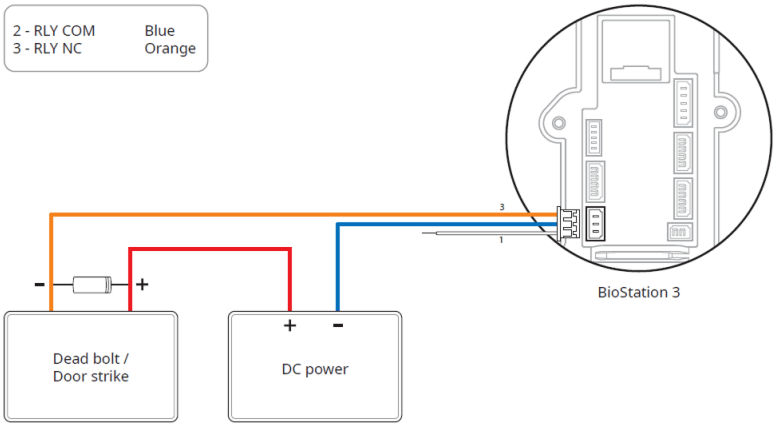
Input connection



Relay Connection

Fail Safe Lock

In order to use the Fail Safe Lock, connect N/C relay as shown in the figure below. There is normally a current flowing through the relay for the Fail Safe Lock. When the relay is activated, blocking the current flow, the door will open. If the power supply to the product is cut off due to a power failure or an external factor, the door will open.



Caution

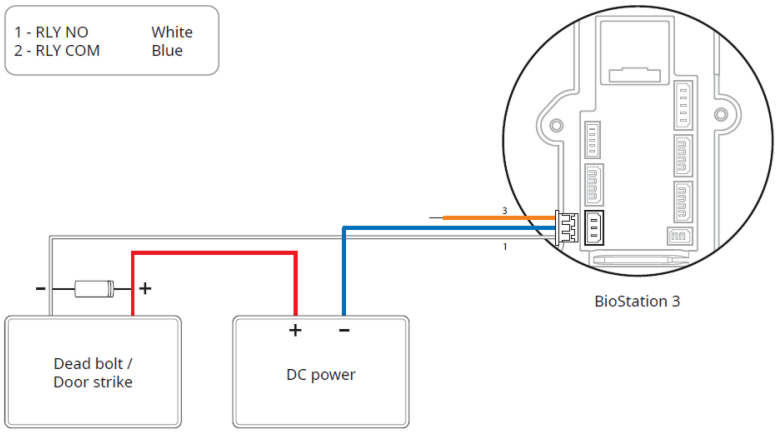
- Install a diode at both sides of the door lock wire as shown in the figure to protect the relay from the reverse current, which occurs when the door lock operates.
- Use a separate power supply for the product and the door lock.
- Suprema's standalone intelligent readers contain internal relays that can directly lock/unlock doors without external controllers for added convenience. For access control applications in need of security, however, it is NOT recommended to use the internal relay of a reader to prevent any tampering attacks which can potentially trigger the door unlock. For such applications, it is highly recommended to use a separate relay unit for a lock control such as Suprema's Secure I/O 2, DM-20 or CoreStation installed at a secure side of a door.

Info

Take caution of the installation direction of the diode. Install the diode close to the door lock.

Fail Secure Lock

In order to use the Fail Secure Lock, connect N/O relay as shown in the figure below. There is normally no current flowing through the relay for the Fail Secure Lock. When the current flow is activated by the relay, the door will open. If the power supply to the product is cut off due to a power failure or an external factor, the door will lock.



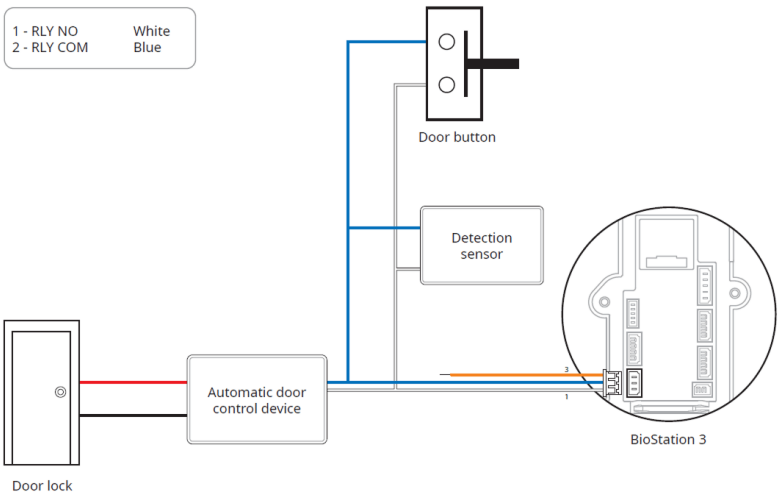
Caution

- Install a diode at both sides of the door lock wire as shown in the figure to protect the relay from the reverse current, which occurs when the door lock operates.
- Use a separate power supply for the product and the door lock.
- Suprema's standalone intelligent readers contain internal relays that can directly lock/unlock doors without external controllers for added convenience. For access control applications in need of security, however, it is NOT recommended to use the internal relay of a reader to prevent any tampering attacks which can potentially trigger the door unlock. For such applications, it is highly recommended to use a separate relay unit for a lock control such as Suprema's Secure I/O 2, DM-20 or CoreStation installed at a secure side of a door.

Info

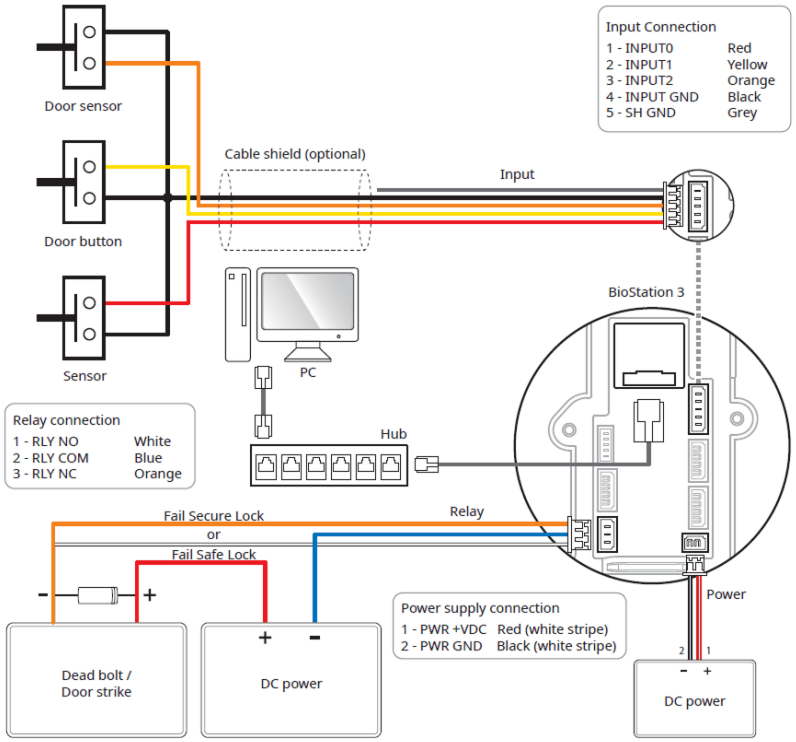
Take caution of the installation direction of the diode. Install the diode close to the door lock.

Automatic door connection



Connecting as a Standalone

The product can be connected to the door lock, door button, and door sensor directly without connecting a separate I/O device.



Caution

Suprema's standalone intelligent readers contain internal relays that can directly lock/unlock doors without external controllers for added convenience. For access control applications in need of security, however, it is NOT recommended to use the internal relay of a reader to prevent any tampering attacks which can potentially trigger the door unlock. For such applications, it is highly recommended to use a separate relay unit for a lock control such as Suprema's Secure I/O 2, DM-20 or CoreStation installed at a secure side of a door.

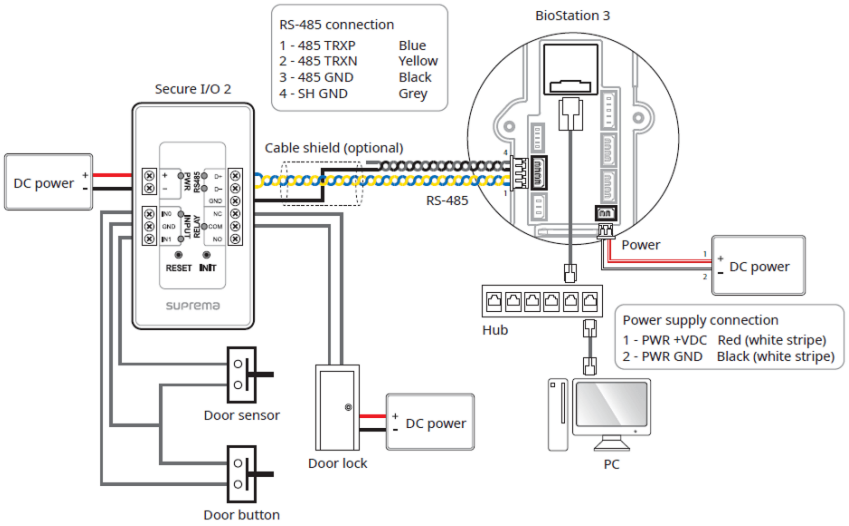
Info

- The device can be used as a multi-door controller with the slave devices with the RS-485 cable. The slave devices are used as dummy readers and authentication is performed in the master device.
- BioStation 3 cannot be used as a slave device when FaceStation 2, FaceLite is the master device, and vice versa.
- The maximum number of slave devices available to connect varies according to the authentication method, number of users, and number of devices. Also note that the number of slave devices affects the authentication performance.
- Connect up to 31 slave devices to a master device. The bandwidth of RS-485 allows for up to 7 fingerprint authentication devices to be connected.
- For more information, contact the Suprema Technical Support Team.

Connecting to Secure I/O 2

Secure I/O 2 is an I/O device, can be connected to the product with the RS-485 cable. Security can be maintained even if the connection between the product and Secure I/O 2 has been lost or the power supply to the product has been shut off due to external factors.

- Use an AWG24 twisted pair with a maximum length of 1.2 km for the RS-485 cable.
- It is recommended to use RS-485 cables with a characteristic impedance of 120 Ω.
- If connecting with a RS-485 daisy chain, connect the termination resistor (120 Ω) to both ends of the daisy chain connection. If connected to the middle line, the signal level becomes smaller and the communication performance will deteriorate. Make sure to connect it to both ends of the daisy chain connection.

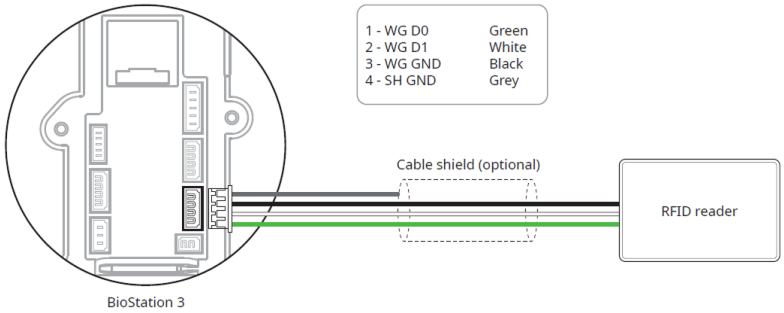


Info

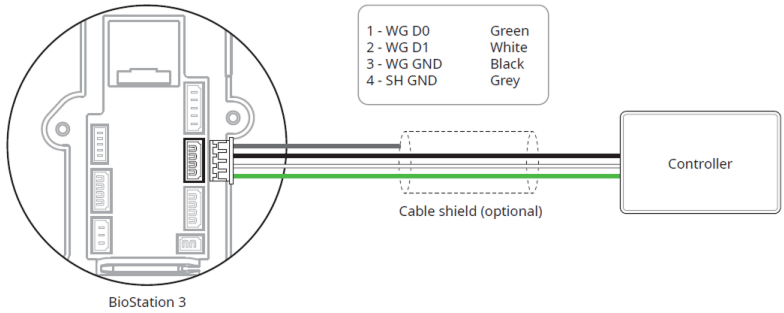
- The device can be used as a multi-door controller with the slave devices with the RS-485 cable. The slave devices are used as dummy readers and authentication is performed in the master device.
- BioStation 3 cannot be used as a slave device when FaceStation 2, FaceLite is the master device, and vice versa.
- The maximum number of slave devices available to connect varies according to the authentication method, number of users, and number of devices. Also note that the number of slave devices affects the authentication performance.
- Connect up to 31 slave devices to a master device. The bandwidth of RS-485 allows for up to 7 fingerprint authentication devices to be connected.
- For more information, contact the Suprema Technical Support Team.

Wiegand Connection

Used as a Wiegand input device.



Used as a Wiegand output device.



How to Use

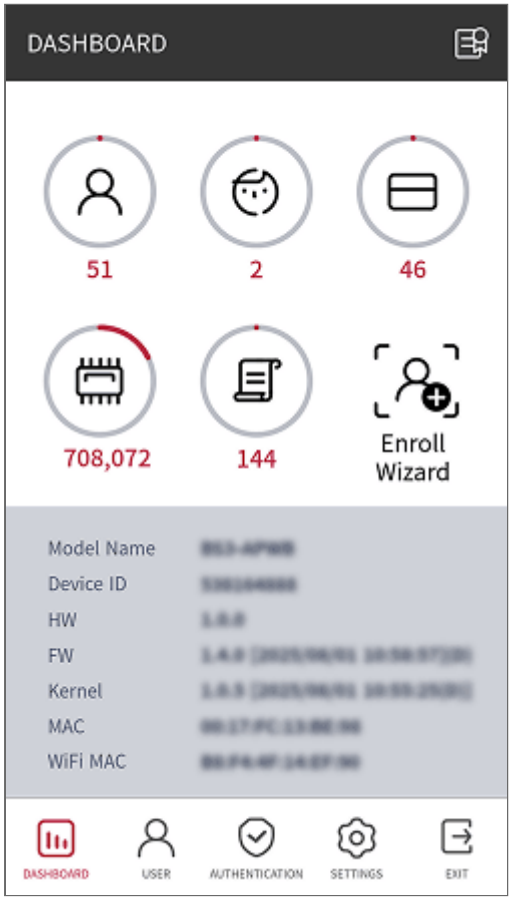
Provides guidance on how to use the main features of the device effectively.

Admin Menu

Provides guidance on the main menus and features accessible with administrator privileges.

DASHBOARD

1. Press and authenticate with the Admin level credential.
   You can check the status and information of the device at **DASHBOARD**. Alternatively, you can press **Enroll Wizard** to directly enroll a user.
2. To register a user or set up a device, select the desired menu from the bottom of the dashboard.



Info

- If an administrator is not designated, pressing will display the **DASHBOARD** screen.
- **WiFi MAC** can only be confirmed on the BS3-APWB model.

Door Control

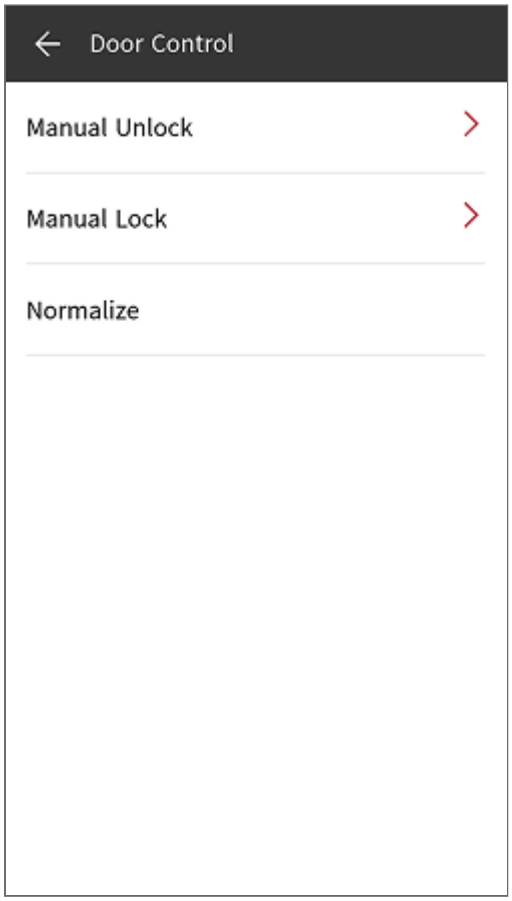
You can manually open, lock, or unlock the connected door.

> **Info**
>
> - You can control the door only when the device is configured as the master device.
> - Use **Administrator** or **Configuration** to control the door.

1. Select **Door** on the main screen.



2. Authenticate using administrator privilege method.
3. Choose the desired door control method.



- **Manual Unlock**: Set the time for immediate door opening or to keep the door open.
- **Manual Lock**: Set the time for immediate locking or to keep the door locked.
- **Normalize**: Cancel manual opening or manual lock hold.

> **Info**
> Set the manual open and manual lock-hold times from 1 to 86,400 seconds.

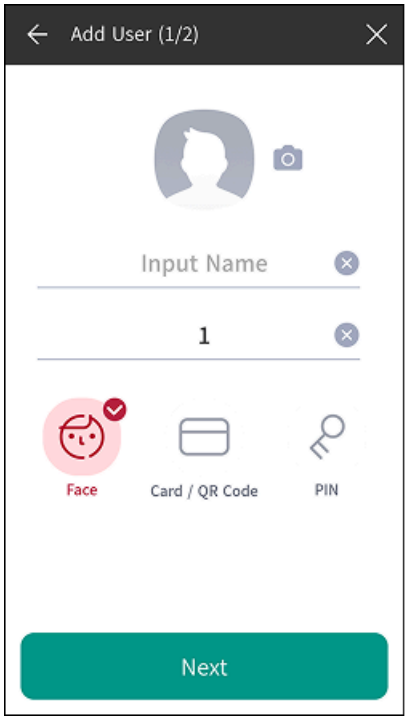
User

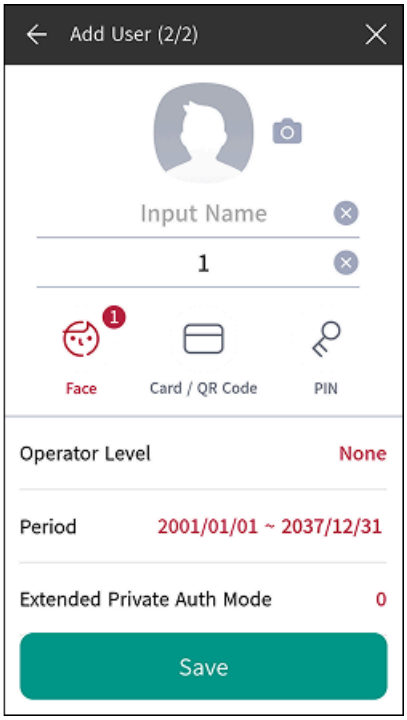
Describes how to register, edit, delete, and manage users.

Registering user information

You can register user information that includes biometric authentication data.

1. Press and authenticate with the Admin level credential.
2. Select **USER** → and set the desired items. User usage information appears.





- : Register a user photo.
- **Name**: Enter a user name. Enter up to 48 characters, including special symbols (`~` `!` `@` `#` `$` `%` `^` `&` `(` `)` `-` `_` `=` `+` `[` `]` `{` `}` `;` `.` `'`). However, names starting with `&` `@` `~` are not allowed.
- **ID**: Enter a number between 1 and 4294967295 to register a user ID. If **User ID Type** is set to **Alphanumeric**, enter up to 32 characters using alphanumerics and certain symbols (`_` `-` `.`). IDs cannot include spaces. Periods (`.`) are allowed, but the ID cannot be a single period (`.`) or two periods (`..`).
- **Face**: You can enroll a face for user authentication. Press **Face** → **Next** and follow the instructions on the screen to enroll your face. To add more faces, press . Please refer to Enrolling user faces to learn more about face enrollment.
- **Card / QR Code**: You can enroll a card for user authentication. Press **Card / QR Code** → **Next**, then scan the card to assign it to the user at the RF card authentication unit. To enroll more cards, press **Card / QR Code** → .
- **PIN**: You can enter the PIN you want to use. Press **PIN** → **Next** and enter the PIN you want to use. For confirmation, enter the PIN once more and then press **OK**. Enter a 4- to 16-digit PIN to prevent it from being exposed.

> **Info**
> When using **Master Admin** feature, enter at least an 8-digit number.

- **Operator Level**: You can select permissions to assign to the user.

> **Info**
>
> Available menus vary according to the set user level.
>
> – **None**: This is a general user level, and the menu is not available.
>
> – **Administrator**: You can use all menus.
>
> – **Configuration**: You can use the menus **AUTHENTICATION**, **DISPLAY & SOUND**, **DEVICE**, **NETWORK**, **EVENT LOG**.
>
> – **User Management**: You can use the menus **USER**, **EVENT LOG**.

- **Period**: You can set the duration for using the user account.
- **Extended Private Auth Mode**: You can set the extended personal authentication mode. This mode allows you to combine user authentication methods, including both faces. Otherwise, you can use the device's basic authentication mode.

3. Press **Save** to complete the registration of user information.

Enrolling user faces

1. Press and authenticate with the Admin level credential.
2. Select **USER** → .
3. Press **Face** → **Next**.
4. Adjust a distance between the face and screen and look straight at the camera of the device.
5. After the shooting is complete, press **OK** → **Save**. To retake your face picture, press **Re-Shot**.

Info

- The visual face data of this product are not compatible with face templates of FaceStation 2 or FaceLite.
- Enroll a user's face not only on the device, but also in bulk on BioStar X by uploading a photo or importing a CSV file. Send a face enrollment link to a user to let them enroll their face on their personal mobile device. For detailed information on each enrollment method, please refer to the BioStar X Administrator Guide.
- To use a Visual Face feature correctly, take a picture by following instructions below.
  - Keep the distance between the device and your face at 60-100 cm when enrolling your face.
  - Do not change your face expression.
  - Do not wear masks, hats, or eye patches.
  - Do not enroll a face wearing a mask. It may increase the False Acceptance Rate (FAR) if both faces with and without a mask are enrolled.
  - Do not raise head up or lower head.
  - Do not wear thick makeup.
  - Do not close your eyes.
  - Make sure that both of your shoulders correctly appear on the screen.
  - Stand still and enroll your face by staring at the screen.
  - Be careful not to display two faces on the screen. Enroll one person at a time.
  - If you do not follow the instructions on the screen, the face enrollment may take longer or may fail.

Modifying User Information

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

1. Press and authenticate with the Admin level credential.
2. Click **USER** → .
3. Select your search terms. You can search for users using **All**, **User ID**, **Name**, **Face**, **Card**.
4. Select the user to modify.
5. Modify the information by referring to Registering user information and press **OK**.

- To delete a user, select and then press **OK**.

Info

Access Group can be registered in BioStar X. For detailed information on registering an Access Group, please refer to the BioStar X Administrator Guide.

Delete All Users

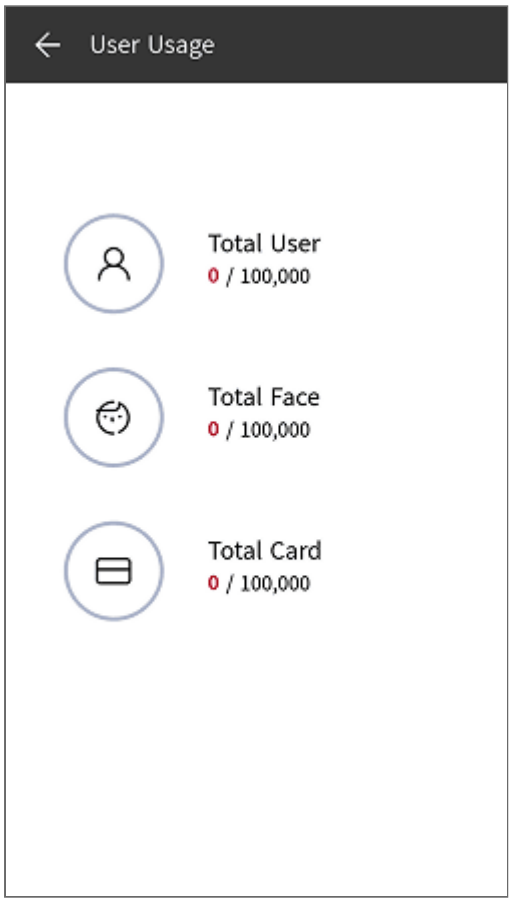
You can delete all registered users at once.

1. Press and authenticate with the Admin level credential.
2. Select **USER** → .
3. Select **Delete All** to check, then press **OK**.
4. To delete all users, press **OK**.

View User Usage

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

1. Press and authenticate with the Admin level credential.
2. Press **USER** → . User usage information appears.



Authentication

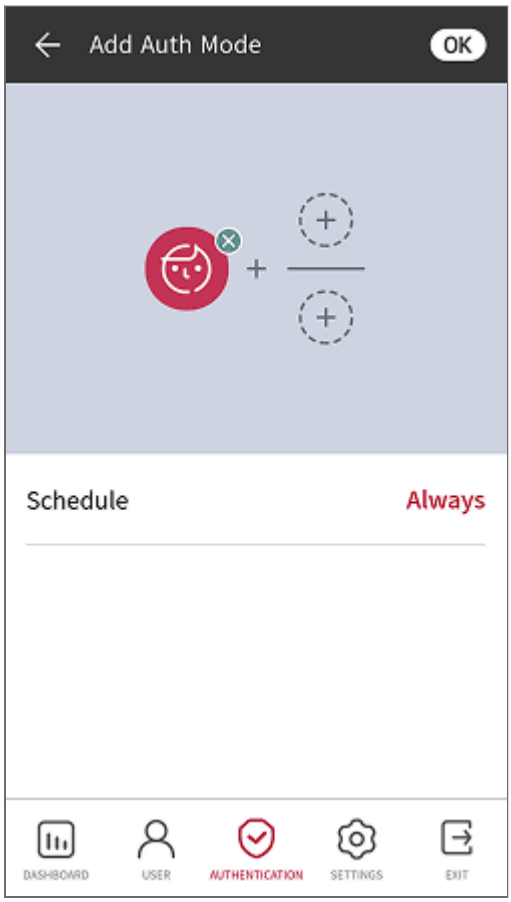
Describes the supported authentication methods and authentication procedures.

Authentication mode

Set the authentication mode. You can combine **Face**, **PIN**, **Card / QR Code**, and **ID** for authentication mode, and you can also set schedules for each authentication mode.

Registering auth mode

1. Press and authenticate with the Admin level credential.
2. Press **AUTHENTICATION** → **Auth Mode**.
3. Select .
4. Pressing will display the credential that can be added on the screen. Select the credentials to add. Press the while the credential is added, and the added credential will be deleted.



5. After setting the desired authentication mode, set **Schedule**.

Category	Description
Face	- : This mode uses only facial authentication. - + : This mode requires facial authentication followed by PIN entry.

Category	Description
Card / QR Code	- : This mode uses only card / QR code authentication. - + : This mode requires card / QR code authentication followed by facial authentication. - + : This mode requires card / QR code authentication followed by PIN entry. - + / : This mode requires card / QR code authentication followed by either facial authentication or PIN entry. - + + : This mode uses both facial authentication and PIN entry after card / QR code authentication.
ID	- ID + : This mode requires ID entry followed by facial authentication. - ID + : This mode requires ID entry followed by PIN entry. - ID + / : This mode requires ID entry followed by either facial authentication or PIN entry. - ID + + : This mode uses both facial authentication and PIN entry after ID entry.

Info

- **Schedule** can be configured in BioStar X. If no schedule is set, only **Always** can be selected.
- For more information about the **Schedule** settings, please refer to the BioStar X Administrator Guide.
- To use **QR Code** authentication, **AUTHENTICATION** must be clicked and **Operation** must have **QR Authentication** activated, and a separate device license is required. For more information, refer to License.

6. To save the settings, press **OK**.

Modifying auth mode

1. Press and authenticate with the Admin level credential.
2. Press **AUTHENTICATION** → **Auth Mode**.
3. Select the authentication mode to modify.
4. Modify the authentication mode by referring to Registering auth mode and press **OK**.

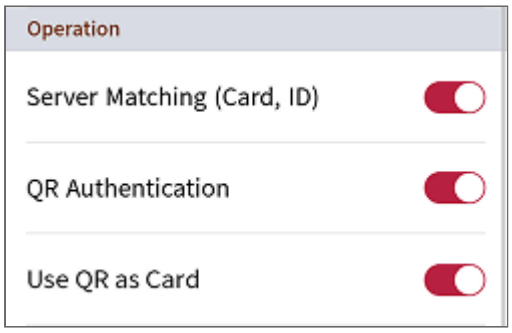
Delete auth mode

1. Press and authenticate with the Admin level credential.
2. Press **AUTHENTICATION** → **Auth Mode**.
3. Press and select the authentication mode to delete. You can select multiple options.
4. To delete the selected item, press **OK**.

Operation

You can set authentication-related options, such as **Server Matching** and **QR Authentication**.

1. Press and authenticate with the Admin level credential.
2. Press **AUTHENTICATION**, then enable the desired options in **Operation**.



- **Server Matching (Card, ID)**: Using server matching means BioStar X authenticates users, not the device. This is useful when the device stores large amounts of user information. It also helps avoid exposing a device that stores credential information outside.

  > **Info**
  >
  > – **Server Matching** can only use cards and IDs.
  >
  > – If you use **Server Matching**, you must enable server matching on both the device and BioStar X. For more information on BioStar X server matching settings, please refer to the BioStar X Administrator Guide.

- **QR Authentication**: Set whether to use QR code authentication through the device's camera.

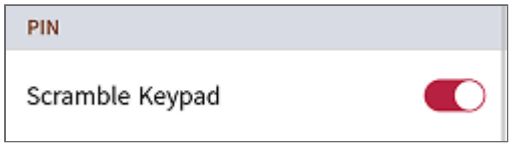
  > **Info**
  >
  > A separate device license is required to use **QR Authentication**. For more information, refer to License.

- **Use QR as Card**: You can set up authentication with a QR code that has the same data as the CSN card or Wiegand card issued to the user. This can only be set when **QR Authentication** is activated.

PIN

Set whether to use the scramble keypad when entering passwords.

1. Press and authenticate with the Admin level credential.
2. After pressing **AUTHENTICATION**, set whether to use **PIN** in **Scramble Keypad**.



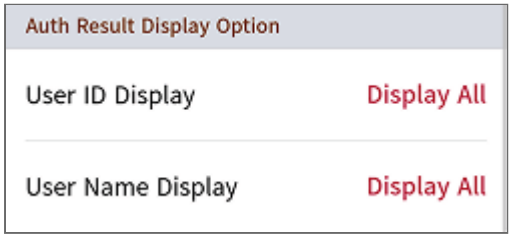
- **Scramble Keypad**: The positions of numeric keys can be scrambled randomly when entering a password to

prevent password leaks.

Auth result display option

You can set the auth result display option.

1. Press and authenticate with the Admin level credential.
2. After pressing **AUTHENTICATION**, change the desired items in **Auth Result Display Option**.

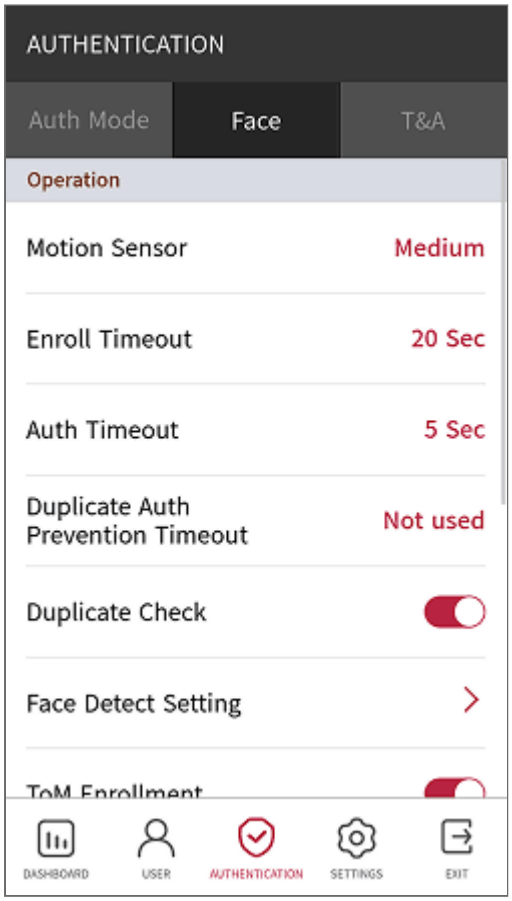


- **User ID Display**: You can select how the user ID is displayed on the authentication result screen of the device.
  - **Display All**: Displays the entire user ID.
  - **Mask All but First Letter**: Displays only the first letter of the user ID.
  - **Hide All**: Do not display the user ID.
- **User Name Display**: You can select how the user name is displayed on the authentication result screen of the device.
  - **Display All**: Displays the entire user name.
  - **Mask All but First Letter**: Displays only the first letter of the user name.
  - **Hide All**: Do not display the user name.

Face

You can change the configuration for facial authentication.

1. Press and authenticate with the Admin level credential.
2. Select **AUTHENTICATION** → **Face**.
3. Change the desired item.



- **Motion Sensor**: Set the sensitivity to detect motion around the device. When **Motion Sensor** is set to **Off**, touch the screen to authenticate your face.
- **Enroll Timeout**: If the face is not enrolled within the set time, the face registration will be canceled.
- **Auth Timeout**: If authentication is not completed within the set time, authentication fails.
- **Duplicate Auth Prevention Timeout**: Prevents duplicate authentication for the specified time when the same face is detected again. Set to **Not used** or 3~60 seconds.

> **Info**
> The **Duplicate Auth Prevention Timeout** setting is only available on the master device.

- **Duplicate Check**: You can check for duplicate faces during face registration.
- **Face Detect Setting**: Set the position and size of the area where the device detects faces during face authentication.

> **Info**
> For optimal performance, it is recommended to use default settings for the sub-options of **Face Detect Setting**. The default values of each option are as follows:
>
> – Maximum Head Pose Angle: 15
> – Detection Distance: Min 30 cm, Max 100 cm
> – Wide Search: Deactivated

- **ToM Enrollment**: By activating **ToM Enrollment**, you can enroll the **Template on Mobile** issued by BioStar X. **Template on Mobile** allows biometric authentication without storing user data on the BioStar X server, Airfob Portal, or device by storing the user's biometric template on a mobile access card.

  > **Info**
  >
  > For more information about **Template on Mobile**, please refer to the BioStar X Administrator Guide.

- **Store Visual Face Image**: You can set to store both the actual images and templates in Visual Face, or to store only the templates without saving the actual images. If disabled, all stored images of visual faces will be deleted, and newly enrolled visual faces will store templates excluding images.

  > **Info**
  >
  > After disabling this setting, connect to BioStar 2 v2.9.7 or later or BioStar X.

- **Security Level**: You can set the security level for 1:N authentication.
- **Operation Mode**: You can set the operating mode of the device for face authentication.
  - **Fusion Matching**: Both visual and infrared matching work to increase the accuracy of face authentication.
  - **Fast Matching**: Users can perform rapid authentication while walking within the device's authentication range.
- **Fake Detection**: You can prevent user authentication with spoofed faces such as photos. Activated when **Operation Mode** is set to **Fusion Matching**.

  > **Info**
  >
  > - Face anti-spoofing performance has been improved to pass the iBeta Level 1 ISO 30107-3 Presentation Attack Detection Test.
  > - In strong sunlight, it is recommended to use the **Fake Detection** function as **Normal**.

- **Advanced Settings**: You can change advanced settings for facial authentication, such as mask detection.
  - **Mask Detection**: You can set whether to use mask detection.
  - **Detection Mode**: You can set the method to check if a mask is worn. This is activated when the **Mask Detection** is set to **Enabled**.

    > **Info**
    >
    > - **Require Mask (Hard)**: Users not wearing a mask will be denied authentication and a mask non-compliance event logs.
    > - **Require Mask (Soft)**: Users not wearing a mask can be authenticated, but a mask non-compliance event logs.
    > - **Require No Mask**: Only users not wearing a mask can be authenticated, and when this mode is used, the mask check mode is fixed to **Check Before Authentication**.

  - **Mask Detection Level**: Set the sensitivity for detecting mask usage. This is activated when the **Mask**

Detection is set to **Enabled**.

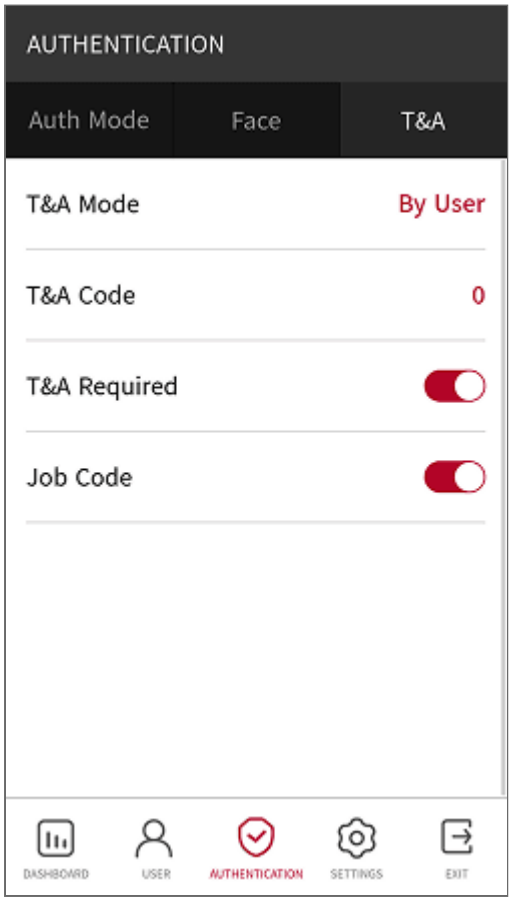
- **Check Mode**: Set the confirmation mode according to the purpose of the device.

> **Info**
>
> - **Check After Authentication**: After authentication, check whether the user is wearing a mask.
> - **Check Before Authentication**: Authenticate after checking whether the user is wearing a mask.
> - **Check Only**: The device can only be used to check if a mask is worn. When this mode is activated, any user wearing a mask can access it regardless of authentication.

T&A (Time and Attendance)

You can set how to register T&A mode.

1. Press and authenticate with the Admin level credential.
2. Select **AUTHENTICATION** → **T&A**.
3. Change the desired item.



- **T&A Mode**: Set how to use attendance mode.
- **T&A Code**: Register T&A events. To register attendance events, select **T&A Code** → and then set the icon to display on the screen, **T&A Event Name**, and **Schedule**.
- **T&A Required**: Set to require a user to select a T&A event when authenticating. Available when **T&A Mode** is set to

By User.

- **Fixed T&A Key**: Set to use only a T&A event selected by the administrator. Available when **T&A Mode** is set to **Fixed**.
- **Job Code**: Set whether to use the job code.

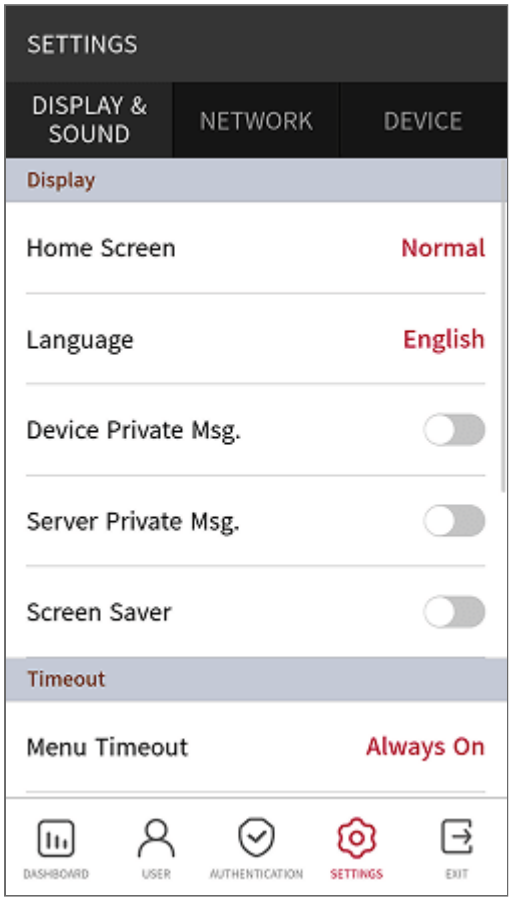
Settings

Provides instructions on how to set system and device configurations.

Display & Sound

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

1. Press and authenticate with the Admin level credential.
2. Press **SETTINGS** → **DISPLAY & SOUND**.
3. Change the desired item.



- **Home Screen**: You can choose items to display in the background of the home screen.
- **Language**: You can select the language that will be displayed on the screen.
- **Device Private Msg.**: Set whether to use a Private Message, which will be displayed on the screen when the user authenticates. The **Device Private Msg.** can be set using the BioStar Device SDK. If not set, does not display a message when authentication is successful even if **Device Private Msg.** is enabled on the device.

- **Server Private Msg.**: Set whether to use a Private Message, which will be displayed on the screen when the user authenticates. **Server Private Msg.** can be set using the BioStar X API. If not set, does not display a message when authentication is successful even if **Server Private Msg.** is enabled on the device.
- **Screen Saver**: Set whether the screen saver is enabled or not. Reduce power consumption by lowering screen brightness when the device is not in 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.
- **Message Timeout**: Set the time (sec) for a setting complete message or notification message to disappear automatically.
- **Backlight Timeout**: Set the time (sec) to turn off the lighting of the screen.
- **Voice Instruction**: You can use voice guidance instead of notification tones.
- **Volume**: Set the volume.
- **Intercom Speaker Volume**: Adjust the speaker volume when using the IP intercom.
- **Intercom Microphone Volume**: Adjust the microphone volume when using the IP intercom.

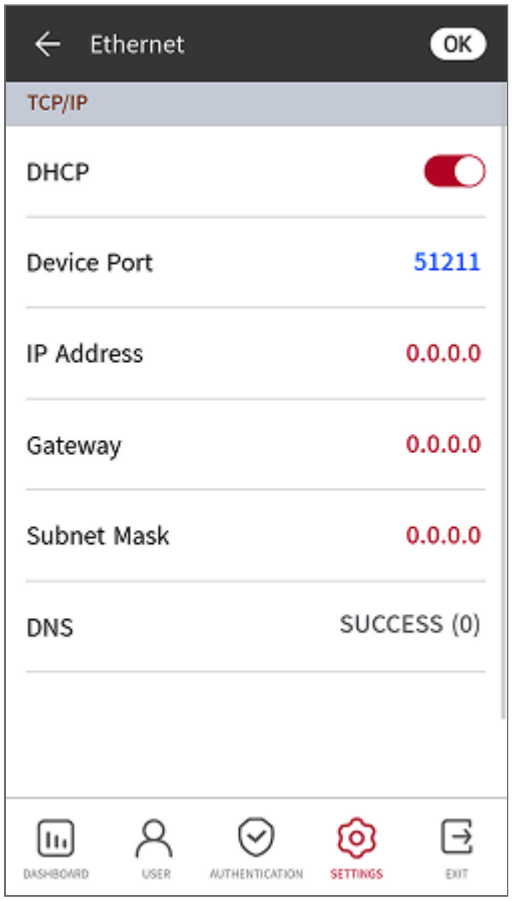
> **Info**
> For more information on the BioStar Device SDK, refer to the BioStar Device SDK page on the Suprema Knowledge Base.

Network

You can change the network settings of the device, such as Ethernet, server, OSDP, etc.

Ethernet

1. Press and authenticate with the Admin level credential.
2. Select **SETTINGS** → **NETWORK** → **Ethernet**.
3. Change the desired item.



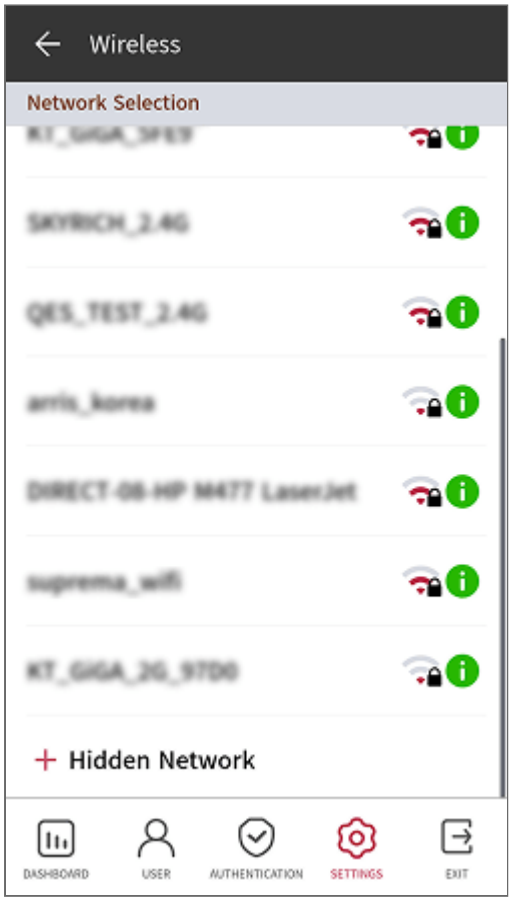
- **DHCP**: Set whether to use DHCP. If DHCP setting is disabled, the user can modify **IP Address**, **Gateway**, and **Subnet Mask**.
- **Device Port**: Set the device's port.
- **IP Address**: You can check the device's IP address. To modify, disable DHCP setting.
- **Gateway**: You can check the device's gateway. To modify, disable DHCP setting.
- **Subnet Mask**: You can check the device's subnet mask. To modify, disable DHCP setting.
- **DNS**: Set the DNS server address.

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

> **Info**
> **Ethernet** cannot be used with **Wireless**.

Wireless LAN

1. Press and authenticate with the Admin level credential.
2. Select **SETTINGS** → **NETWORK** → **Wireless**.
3. The list of networks available to connect will be displayed.



- **Hidden Network**: Add and connect to a wireless network by entering network information manually.
  - **SSID**: Enter the SSID. The SSID may be up to 32 characters long and include alphanumeric (case-sensitive), and special characters.
  - **Password**: Enter the password. The password can include alphanumeric and special characters only.

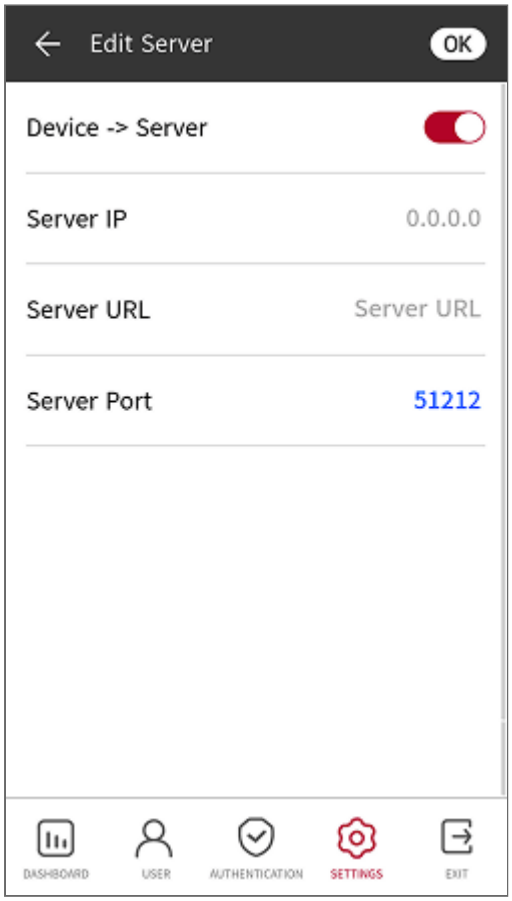
4. Select the network you wish to connect to and enter the password. When you press **OK**, the connection to the wireless network will be made.

5. Press the wireless network you wish to use and then disable DHCP settings to allow users to modify **IP Address**, **Gateway**, and **Subnet Mask**.

> **Info**
>
> - **Wireless** is only available for BS3-APWB model.
> - **Wireless** cannot be used with **Ethernet**.
> - 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. Select **SETTINGS** → **NETWORK** → **Server**.
3. Change the desired item.

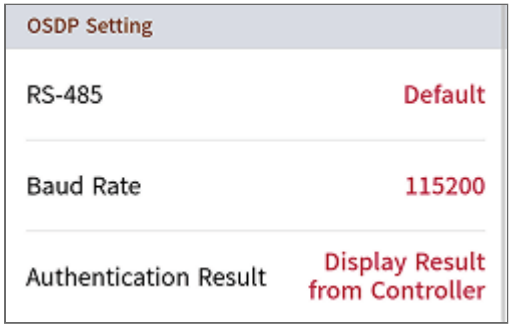


- **Device → Server**: You can send a connection signal from the device to a server with the input information directly. When **Device → Server** is enabled, the user can input **Server IP**, **Server URL**, and **Server Port**.
- **Server IP**: Enter the IP address of the PC on which BioStar X is installed.
- **Server URL**: You can enter **Server URL** instead of **Server IP**.
- **Server Port**: Enter the port of the PC on which BioStar X is installed.

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

OSDP settings

1. Press and authenticate with the Admin level credential.
2. Select **SETTINGS → NETWORK**.
3. Set the desired item in **OSDP Setting**.



- **RS-485**: Select the RS-485 mode.

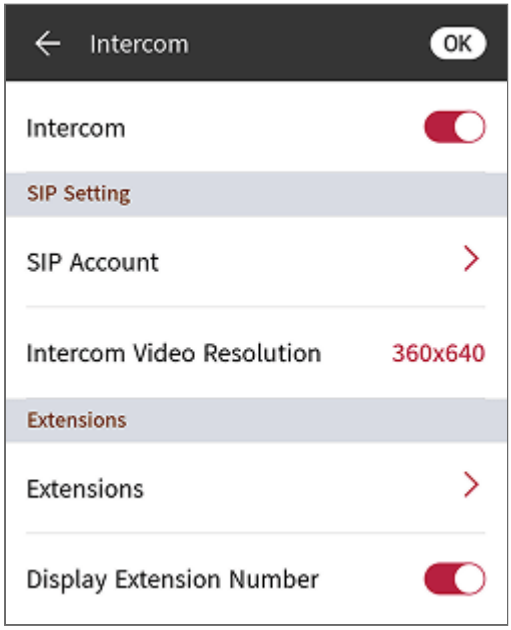
- **Baud Rate**: Select the desired baud rate.
- **Authentication Result**: When using **Intelligent Slave**, select to display the authentication results of 3rd party controllers or devices on the screen. This option can be used when **RS-485** mode is set to **Default** or **Slave**.

Device

IP Intercom

Set the account and extensions of intercom.

1. Press and authenticate with the Admin level credential.
2. Select **SETTINGS** → **DEVICE** → **Intercom**.



- **Intercom**: Set whether the intercom is enabled or not. Enabling intercom settings allows you to configure **SIP Account** and **Extensions**.
- **SIP Account**: Enter each item so that the device can be registered on the SIP server.
- **Intercom Video Resolution**: Select the resolution of the intercom video output from the device.
- **Extensions**: Add, delete, or edit extension numbers.
- **Display Extension Number**: Set whether to display extension numbers.

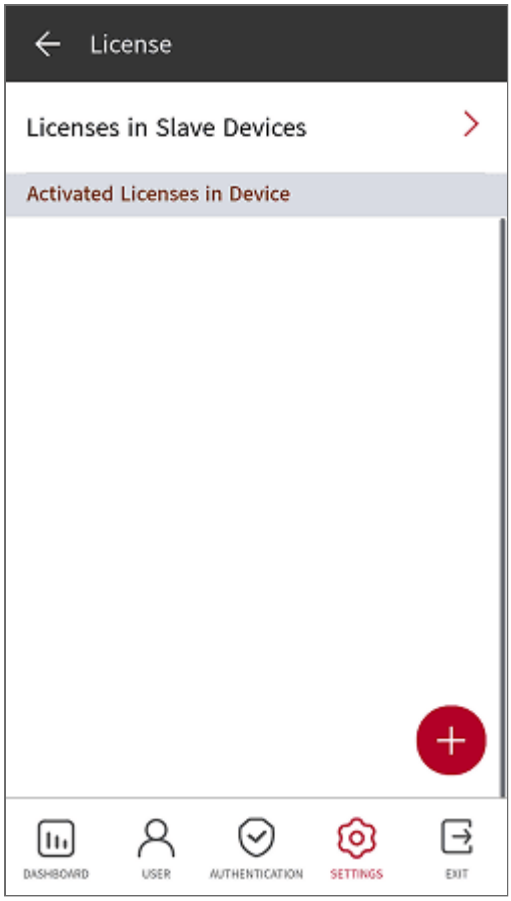
> **Info**
>
> - If **Display Name** is not set, it will not be possible to distinguish receivers.
> - Extension numbers can only enter alphanumeric (case sensitive), and special characters `+` `-` `@` `.`.

3. To save the settings, press **OK**.

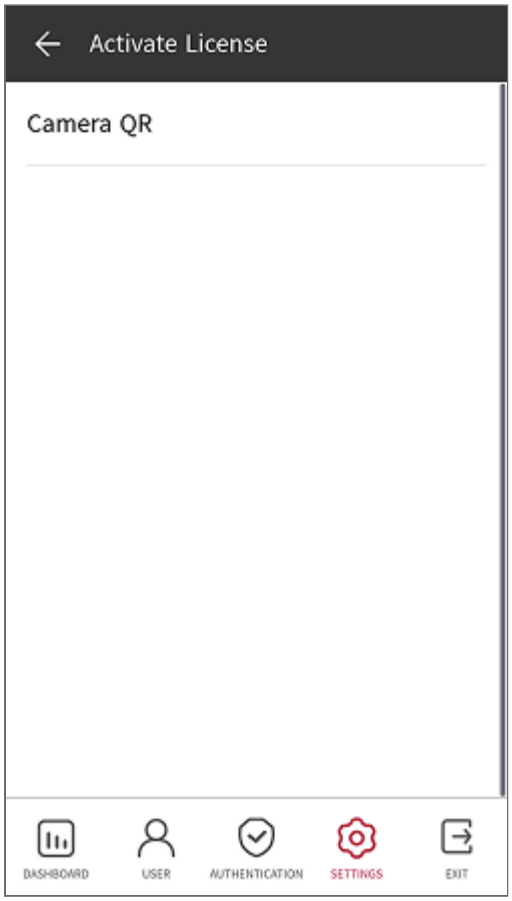
License

You can activate the device license or check **Licenses in Slave Devices** and **Activated Licenses in Device**.

1. Press and authenticate with the Admin level credential.
2. Select **SETTINGS** → **DEVICE** → **License**.
3. To activate the device license, connect the USB with the license to the device and select .



4. Licenses that can be activated appear on the screen. Activate the desired license.



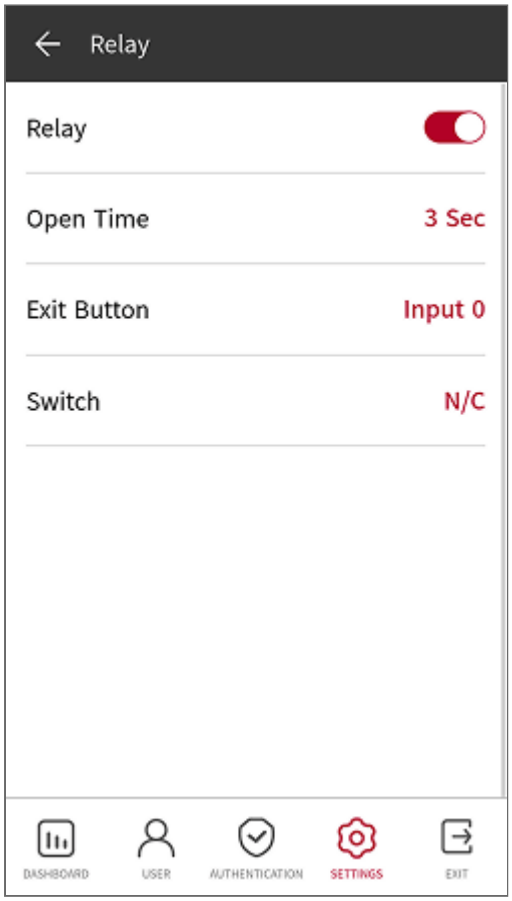
Info

- Contact the place of purchase to issue a device license.
- One feature is available per device license.
- You can include multiple device licenses in one device license file. (Supports up to 100)
- The device license file is an encrypted file and cannot be modified arbitrarily.
- Device licenses are issued based on device ID. If the device ID is changed in an unusual way, the warranty service for the license is not provided.

Relay

You can set the input ports of **Open Time** and **Exit Button** in the device.

1. Press and authenticate with the Admin level credential.
2. Select **SETTINGS** → **DEVICE** → **Relay**.

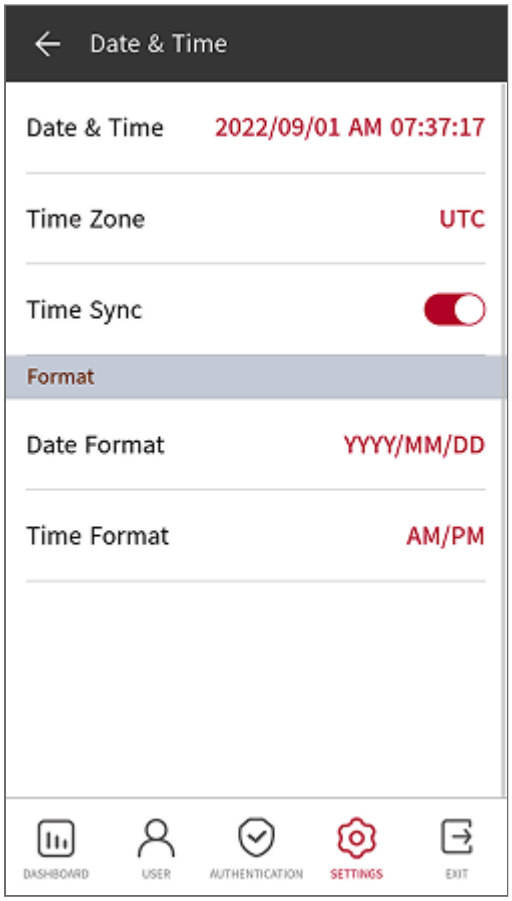


- **Relay**: You can set whether relay is enabled or not. To set **Open Time** and **Exit Button**, activate this option.
- **Open Time**: Set the duration for the door to remain open when standard user authentication has been carried out.
- **Exit Button**: Select the input port where the exit button is connected.
- **Switch**: Select the type of switch (**N/O** or **N/C**) for the Exit Button's input port.

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. Select **SETTINGS** → **DEVICE** → **Date & Time**.
3. Change the desired item.

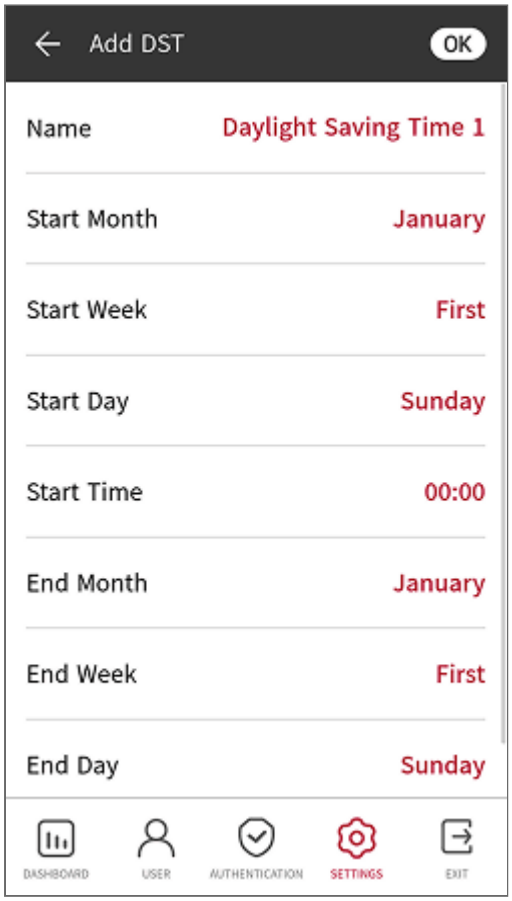


- **Date & Time**: Check the current date and time. To modify it manually, disable **Time Sync**.
- **Time Zone**: Set the time reference of the current location.
- **Time Sync**: Synchronize the server and the time. If you wish to synchronize the server and the time, enable **Time Sync**.
- **Date Format**: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

Daylight saving time

You can use the device by applying daylight saving time. Set the start and end time correctly.

1. Press and authenticate with the Admin level credential.
2. Select **SETTINGS** → **DEVICE** → **Daylight Saving Time** and then press to add additional daylight-saving time.
3. Change the desired item.



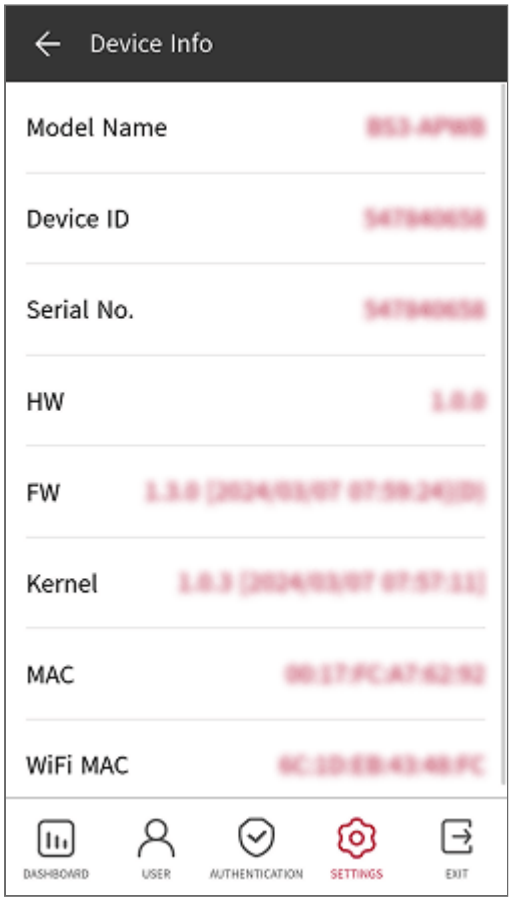
- **Name**: Set the name of daylight-saving time.
- **Start Month** / **Start Week** / **Start Day** / **Start Time**: Set details of when daylight-saving time begins.
- **End Month** / **End Week** / **End Day** / **End Time**: Set details of when daylight-saving time ends.

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

Device Information

You can view the model name, device ID, serial number, device and firmware version, kernel, and MAC address.

1. Press and authenticate with the Admin level credential.
2. Select **SETTINGS** → **DEVICE** → **Device Info**. You can view the information for **Model Name**, **Device ID**, **Serial No.**, **HW**, **FW**, **Kernel**, **MAC**, and **WiFi MAC**.



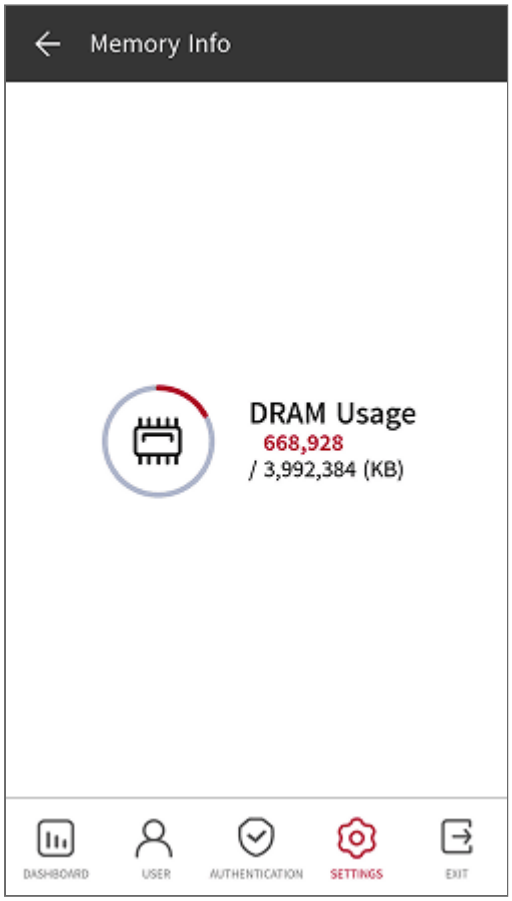
Info

- Long-press **MAC** to display **FAS_IR_SP** information showing the version of the face anti-spoofing algorithm. If you press **FAS_IR_SP**, you can check the entire hash value in a pop-up message.
- **WiFi MAC** can only be confirmed on the BS3-APWB model.

Memory information

View the status of memory usage.

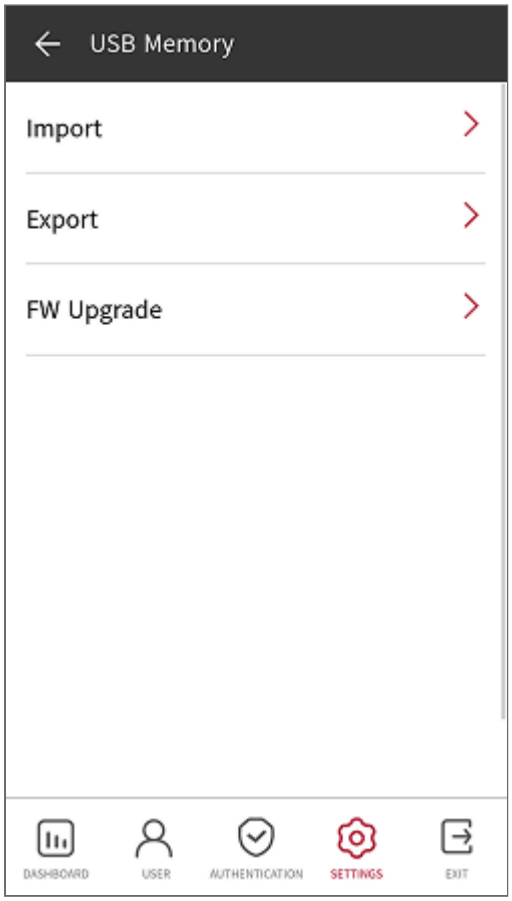
1. Press and authenticate with the Admin level credential.
2. Select **SETTINGS** → **DEVICE** → **Memory Info**. You can view the memory usage status of the device.



USB memory

Connect USB Memory and import user information to the device or export log and user information from the device. You can also upgrade the firmware.

1. Press and authenticate with the Admin level credential.
2. Select **SETTINGS** → **DEVICE** → **USB Memory**.
3. Select the desired item and change the setting.



- **Import**: Import user information from the connected USB memory.
- **Export**: Select information you wish to export to the connected USB memory.
- **FW Upgrade**: Upgrade the firmware if the firmware files are saved in the connected USB memory.

Caution

Do not disconnect the power supply while upgrading the firmware of the device. The device may malfunction.

Info

- It is recommended to use a USB flash drive formatted in exFAT. USB flash drives in FAT32 format may malfunction when more than 50,000 face credentials are stored.
- Check the amount of free space on your USB flash drive. To save 100,000 face credentials, a minimum of 15 GB of free space is required.

Secure Tamper

You can set whether to use security tamper. When the tamper is turned on, you can set to delete the entire user, the entire log, and the security key.

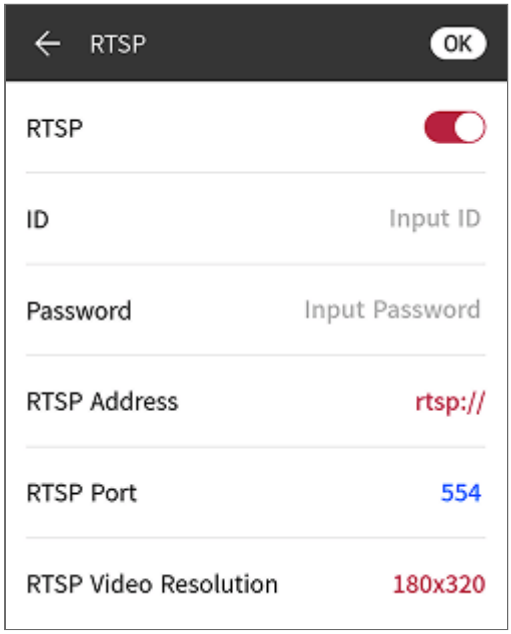
1. Press and authenticate with the Admin level credential.
2. Select **SETTINGS** → **DEVICE**.

3. Activate **Secure Tamper** to delete data of all registered users, all logs, and secure keys when a temper event occurs.

RTSP

Connect a third-party video management system (VMS) to monitor videos filmed with the product's visual camera.

1. Press and authenticate with the Admin level credential.
2. Select **SETTINGS** → **DEVICE** → **RTSP**.
3. Select the desired item and change the setting.



- **RTSP**: You can set whether RTSP is enabled or not. When RTSP setting is enabled, the user can configure **ID**, **Password**, **RTSP Address**, **RTSP Port**, and **RTSP Video Resolution**.
- **ID**: Enter the ID. The ID may have up to 32 characters, in a combination of alphanumeric (case-sensitive) characters and certain symbols `-` `_`.
- **Password**: Enter the password. The password may have 8-32 characters in a combination of alphabetic (capital and lowercase letters) and numeric characters.
- **RTSP Address**: Enter the RTSP address.
- **RTSP Port**: Enter the RTSP port number.
- **RTSP Video Resolution**: Select the resolution of the RTSP video output from the device.

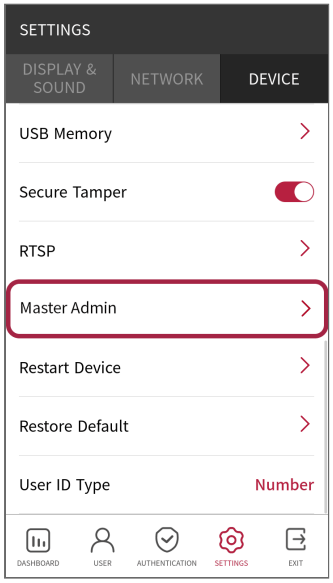
> **Info**
> When the device is configured as a slave device, the RTSP function may not be available.

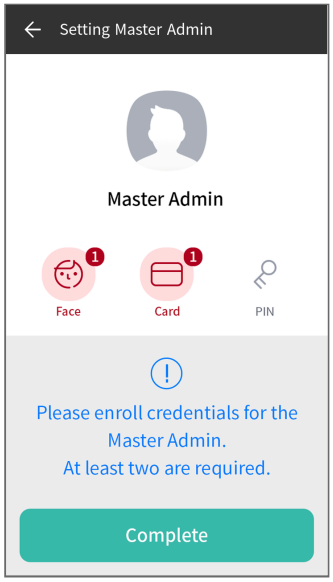
Master administrator CE-oriented products

You can change the authentication method of the Master Admin.

1. Press and authenticate with the Admin level credential.

2. Select **SETTINGS** → **DEVICE** → **Master Admin**.
3. Configure the desired authentication methods.





Info

- You must enroll at least two types of credentials.
- This feature is only available on devices with firmware version 1.4.0 or higher.

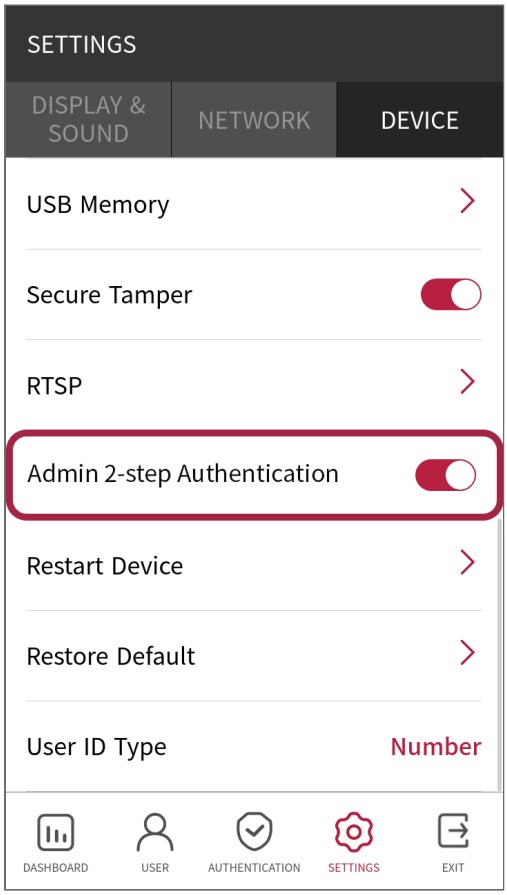
Administrator two-factor authentication CE-oriented products

A CE product that has been upgraded from firmware does not provide **Master Admin** settings, but you can use the **Admin 2-step Authentication** option to enhance overall administrator privileges and improve device security.

Info

- **Admin 2-step Authentication** can be activated only if all enrolled administrators have at least two types of credentials.
  - PIN cannot be used as a standalone credential, so the ID + PIN combination is not supported.
- The firmware upgrade device cannot be downgraded to a lower version after upgrading the firmware.

1. Press and authenticate with the Admin level credential.
2. Enable **SETTINGS** → **DEVICE** → **Admin 2-step Authentication**.

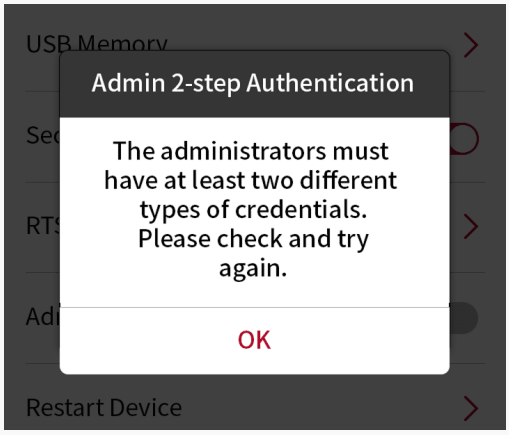


Info

If there are not two types of credentials enrolled for all administrators, activation fails and an error message is displayed.

Enroll two types of credentials for all administrators and try again.

- PIN cannot be used as a standalone credential, so the ID + PIN combination is not supported.



Caution

If you enable **Admin 2-step Authentication** and delete all administrators' credentials to fewer than two types, you cannot access the administrator menu when BioStar X or BioStar 2 is unavailable. Therefore, you need to be particularly careful when deleting administrator credentials.

Restart device

The user can restart the device.

1. Press and authenticate with the Admin level credential.
2. Select **SETTINGS** → **DEVICE** → **Restart Device**.
3. Press **OK** to restart the device. Press **Cancel** to return to the previous screen.

Restore default

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

1. Press and authenticate with the Admin level credential.
2. Select **SETTINGS** → **DEVICE** → **Restore Default**.
   - **All settings**: Initializes all settings stored on the device. Press **OK** to initialize all device settings. Press **Cancel** to return to the previous screen.
   - **Keep Network Settings**: Initializes all settings except for network settings. Press **OK** to initialize all settings except for network settings. Press **Cancel** to return to the previous screen.
   - **Factory Default**: Deletes all information saved in the device and the root certificate, restoring settings to default.
   - **Delete the Root Certificate**: Deletes the root certificate saved in the device.
3. If you proceed with **Restore Default**, the device will restart.

> **Info**
>
> - 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.
> - The **Factory Default** menu can be used when the root certificate is saved in the device.
> - The **Delete the Root Certificate** menu can be used only when the root certificate is saved in the device and an administrator has been designated.

User ID type

Select the type of user ID to register to the device.

1. Press and authenticate with the Admin level credential.
2. Select **SETTINGS** → **DEVICE** → **User ID Type**.
   - **Number**: You can enter a user ID with numbers only.
   - **Alphanumeric**: Enter a user ID using alphanumeric characters and certain symbols (`_` , `-` , and `.`).
3. Select to the desired item.

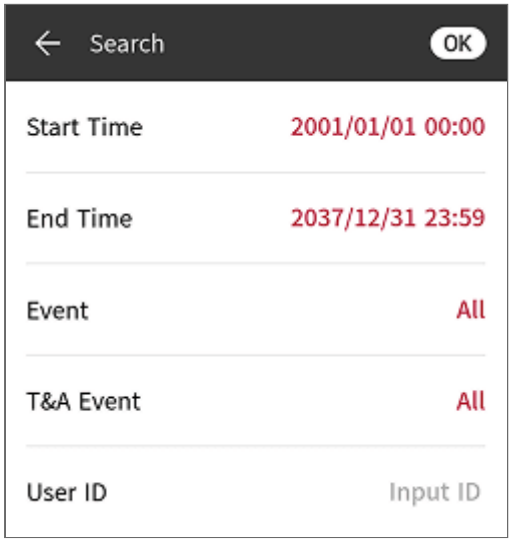
Event Logs

Describes how to view event logs generated by the device.

Search event logs

Set conditions to search logs.

1. Press and authenticate with the Admin level credential.
2. Select in **DASHBOARD**. All event logs appear.
3. Press to search a specific log and change the condition.



4. Set the search criteria and click **OK** to display logs that match the criteria.

Delete all logs

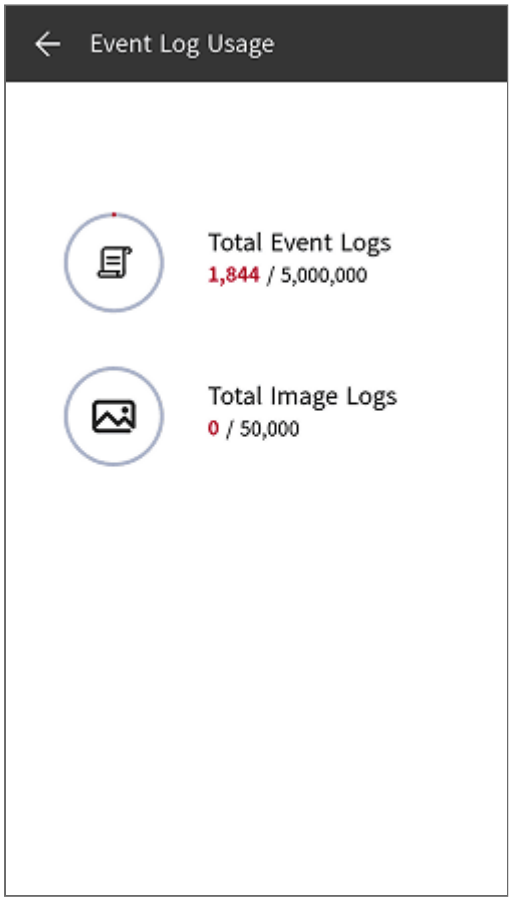
You can delete all saved logs.

1. Press and authenticate with the Admin level credential.
2. Select in **DASHBOARD**. All event logs appear.
3. To delete all logs, select and click **OK**. Press **Cancel** to return to the previous screen.

View log usage

You can check the status of log usage.

1. Press and authenticate with the Admin level credential.
2. Press → in **DASHBOARD**. Check the device's event log and image log usage.


Event Log Usage
Total Event Logs
1,844 / 5,000,000
Total Image Logs
0 / 50,000

Troubleshooting

This document provides information to solve unexpected issues that you may encounter when using the device.

Check items before reporting a malfunction

This document provides information to solve unexpected issues that you may encounter when using the device.

Power

Q. 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

Q. 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.

Q. 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.

Face

Q. The face has been registered but face authentication cannot be done smoothly, and errors occur frequently.

- Check Cautions for enrolling a faces and enroll the face again.
- If there are many enrolled faces, change **Matching Timeout** and try again.

Q. Face authentication has suddenly stopped working.

- Check Cautions for authenticating a face and try again.

Q. Mask Detection is set to Enabled, but face authentication cannot be done smoothly when wearing a mask.

- Authenticate your face twice with the mask pull down on the tip of your nose. Then, authenticate your face again wearing a mask that covers your nose completely. If the problem persists, contact the installation company.

Door lock

Q. The door cannot be locked when I close the door.

- The electric lock may be malfunctioning. Have an inspection through the installation company.

Time

Q. Suddenly the time has become incorrect.

- The device 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

Q. I lost my Admin PIN, so I cannot access the Admin mode.

- The administrator grants an access permission in the device, so only the administrator can access the Admin menu.
- If you have lost the Admin PIN, contact the installation company.

Master Administrator (CE-oriented products)

Q. Is Master Administrator setup supported after a firmware upgrade from an existing device?

- **Master Administrator** is **supported only on CE-oriented products with a CE-marked label**. Use the label sticker on the back of the product to identify **CE-oriented / global (Non-CE)** products. For details, see Master Administrator support policy.

Product Specifications

Provides key specifications of the product, including size, features, and performance.

Credentials

Biometric	**Face** • **Authentication Distance[1]:0.3 ~ 1.0 m** • **Authentication Height:1.4 ~ 1.9 m** • **Matching Speed:Within 0.2 seconds** • **Live Face Detection:Supported**	
RF Card	**BS3-DB**	**125kHz EM & 13.56MHz MIFARE, MIFARE Plus, DESFire, DESFire EV1/EV2/EV3, FeliCa**
	BS3-APWB	**125kHz EM, HID Prox & 13.56MHz MIFARE, MIFARE Plus, DESFire, DESFire EV1/EV2/EV3, FeliCa, iCLASS SE/SR/Seos**
RF Read Range[2]	**EM/HID Prox/MIFARE/DESFire/HID iCLASS: 30 mm, FeliCa: 15 mm**	
Mobile	**NFC, BLE**	
Scramble Keypad (PIN)	**Supported**	
QR/Barcode[3]	**Supported[4]**	
QR/Barcode Read Range[5]	**30 ~ 40 cm**	

General

Model Name	**BS3-DB, BS3-APWB**
CPU	**1.5 GHz Quad Core**
Memory	**32 GB Flash + 4 GB RAM**

Crypto Chip	**Supported**	
Display	**5.5" IPS color LCD**	
Display Resolution	**720 x 1280 pixels**	
Sound	**16 bit**	
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	• **IR: 2M pixels** • **Visual: 2M pixels**	
Dimensions (W x H x D)	**Device**	**82.5 x 171 x 23.4 (mm)**
	Bracket	**72.9 x 164 (mm)**
Weight	**Device**	• **BS3-DB: 370 g** • **BS3-APWB: 380 g**
	Bracket	**90 g (including washers and bolts)**
IP Rating	**IP65**	
IK Rating	**IK06**	
Certifications	**CE, UKCA, KC, FCC, IC, RCM, BIS, SIG, RoHS, REACH, WEEE, MIC, TELEC**	

Capacity

Max. User	**100,000**[6)]

Max. Credentials (1:N)	**Face: 50,000**
Max. Credentials (1:1)	• **Face: 100,000** • **Card: 100,000** • **PIN: 100,000**
Max. Text logs	**5,000,000**
Max. Image logs	**50,000**

Interface

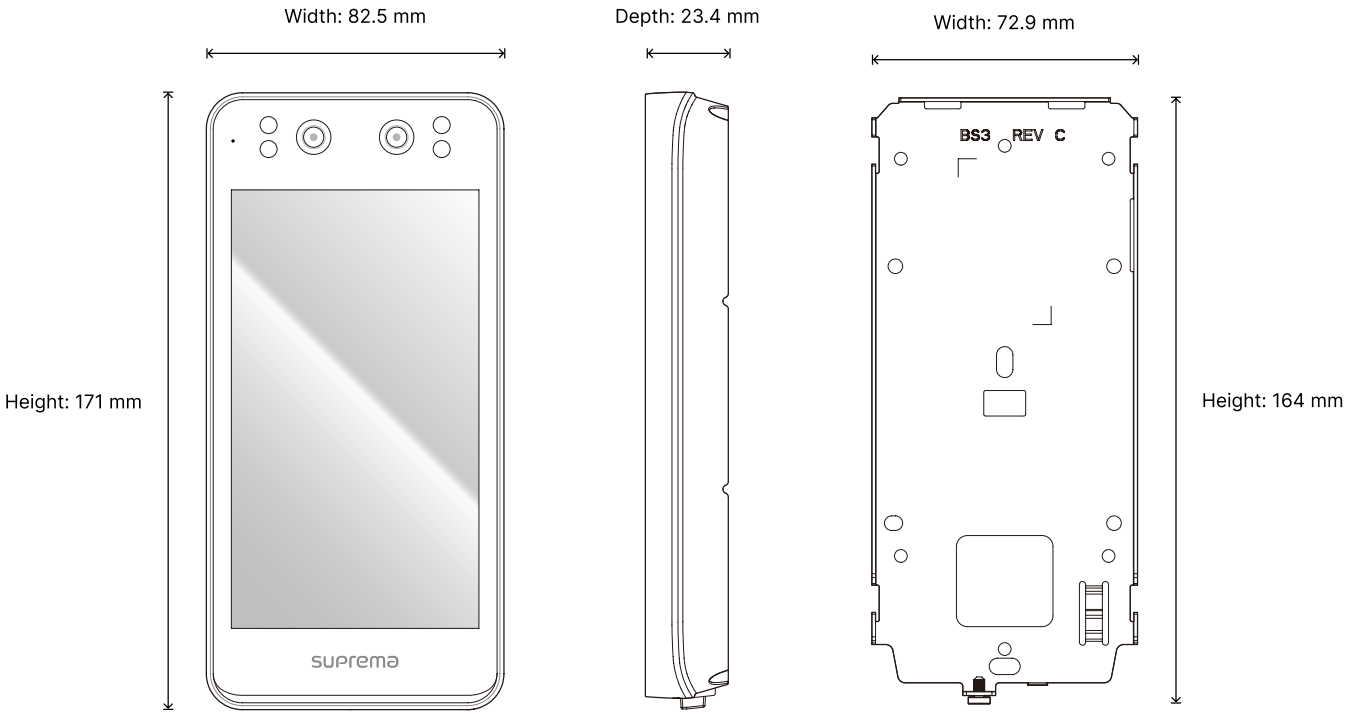
Ethernet	**Supported (10/100/1000 Mbps, auto MDI/MDI-X)**	
Wi-Fi	**BS3-DB**	**Not supported**
	BS3-APWB	**Supported (802.11 b/ g/ n 2.4 GHz)**
Network Protocol	**TCP, UDP**	
RS-485	**1 ch Master / Slave (Selectable)**	
RS-485 Communication Protocol	**OSDP V2 compliant**	
Wiegand	**1 ch Input, 1 ch Output**	
Input	**3 ch Inputs**	
Relay	**1 relay**	
PoE+[7)]	**BS3-DB**	**Not supported**
	BS3-APWB	**Supported (IEEE 802.3at compliant)**
Intercom	**Supported**	
RTSP	**Supported**	

USB	**USB 2.0 (Host)**
USB Expansion Port	**Supported**
Tamper	**Supported**

Electrical

Power	**12 Vdc**	**Current: Max. 1 A**
	24 Vdc	**Current: Max. 0.7 A**
Switch Input VIH	• **Min.: 3 V** • **Max.: 5 V**	
Switch Input VIL	**Max.: 1 V**	
Switch Pull-up Resistance	**4.7 kΩ (The input ports 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	• **2 A @ 30 VDC Resistive load** • **1 A @ 30 VDC Inductive load**	

Dimensions and Weight



Weight
- BS3-DB: 370 g
- BS3-APWB: 380 g

Weight: 90 g
(Including washer and bolt)

---

1) The minimum facial authentication distance indicated is the default setting for the product, and the recommended facial authentication distance is 0.6-1.0 m.

2) The RF detection range may vary depending on the installation environment.

3) Supports QR/Barcodes composed of up to 32 ASCII code strings.

4) Requires a separate license.

5) The indicated QR/Barcode recognition distance is a recommended distance, and the actual recognizable distance may vary depending on the QR/Barcode size and installation environment.

6) The number of users registered without having any credential data.

7) Requires PoE+ (IEEE 802.3at, 30 W) or PoE++ (IEEE 802.3bt, 60–100 W) power. Standard PoE (IEEE 802.3af, 15.4 W) is not supported. Using standard PoE may cause devices to operate unstably or be permanently damaged. Before connecting the device, make sure your network switch or PoE injector supports PoE+ or PoE++.

Info

- Product specifications are subject to change without notice for performance improvement.
- When this product is a master device, connecting a device with a fingerprint sensor as a slave allows authentication of fingerprints using the slave device.
  - Max. Fingerprint Credentials (1:N): 100,000
  - Max. Fingerprint Credentials (1:1): 100,000

Regulatory Information

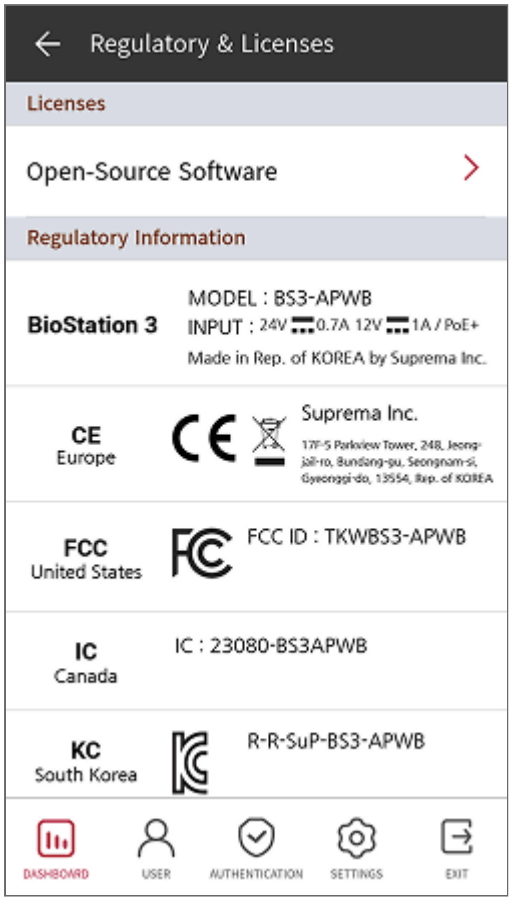
Provides information on regulations and certifications complied with by the product.

Regulatory & Licenses

You can check the license, regulatory certification, and compliance marks on the product.

- CE / FCC / IC / KC / UKCA / RCM / MIC / TELEC

1. Press and authenticate with the Admin level credential.
2. Touch **DASHBOARD** in the upper right corner and touch to check **Regulatory & Licenses**.



Info

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

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.

Info

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator and your body. Do not install or operate this device and its antenna in conjunction with any other antenna or RF transmission device.

IC information

This device complies with Industry Canada's licence-exempt RSSs.

Operation is subject to the following two conditions:

1. This device may not cause interference; and
2. This device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence.

L'exploitation est autorisée aux deux conditions suivantes :

1. l'appareil ne doit pas produire de brouillage ;
2. l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

EU Declaration of Conformity (CE)

This product is CE marked according to the provisions of the Radio Equipment Directive (RED) 2014/53/EU.

Hereby, Suprema Inc. declares that this product is in compliance with the essential requirements and other relevant provisions of Radio Equipment Directive (RED) 2014/53/EU and is marked with the CE mark. This device is a Class 1 radio device according to the instructions.

- Bluetooth transmit power: -0.1 dBm
- Bluetooth frequency: 2402~2480 MHz
- NFC frequency: 13.56 MHz
- RFID frequency: 13.56 MHz + 125 kHz

For more information, please contact us via the contact details below.

Suprema Inc.

Address: 17F Parkview Tower, 248, Jeongjail-ro, Bundang- gu, Seongnam-si, Gyeonggi-do, 13554, Rep. of KOREA

Tel: +82-31-783-4502 / Fax: +82-31-783-4503

Appendices

Includes legal notices contained in the product.

Disclaimers

- Information in this web site is provided in connection with Suprema products.
- The right to use is acknowledged only for Suprema products included in the terms and conditions of use or sale for such products guaranteed by Suprema. No license, express or implied, by estoppel or otherwise, to any intellectual property is granted by this web site.
- Except as expressly stated in an agreement between you and Suprema, Suprema assumes no liability whatsoever, and Suprema disclaims all warranties, express or implied including, without limitation, relating to fitness for a particular purpose, merchantability, or noninfringement.
- All warranties are VOID if Suprema products have been: 1) improperly installed or where the serial numbers, warranty date or quality assurance decals on the hardware are altered or removed; 2) used in a manner other than as authorized by Suprema; 3) modified, altered or repaired by a party other than Suprema or a party authorized by Suprema; or 4) operated or maintained in unsuitable environmental conditions.
- Suprema products are not intended for use in medical, lifesaving, life-sustaining applications, or other applications in which the failure of the Suprema product could create a situation where personal injury or death may occur. Should you purchase or use Suprema products for any such unintended or unauthorized application, you shall indemnify and hold Suprema and its officers, employees, subsidiaries, affiliates, and distributors harmless against all claims, costs, damages, and expenses, and reasonable attorney fees arising out of, directly or indirectly, any claim of personal injury or death associated with such unintended or unauthorized use, even if such claim alleges that Suprema was negligent regarding the design or manufacture of the part.
- Suprema reserves the right to make changes to specifications and product descriptions at any time without notice to improve reliability, function, or design.
- Personal information, in the form of authentication messages and other relative information, may be stored within Suprema products during usage. Suprema does not take responsibility for any information, including personal information, stored within Suprema’s products that are not within Suprema’s direct control or as stated by the relevant terms and conditions. When any stored information, including personal information, is used, it is the responsibility of the product users to comply with national legislation (such as GDPR) and to ensure proper handling and processing.
- You must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Suprema reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them.
- Except as expressly set forth herein, to the maximum extent permitted by law, the Suprema products are sold "as is".
- Contact your local Suprema sales office or your distributor to obtain the latest specifications and before placing your product order.

Copyright Notice

The copyright for this website is owned by Suprema. Rights to other product names, trademarks, and registered trademarks belong to the respective individuals or organizations that own them.

Open Source License

- The software for this product is created by modifying version 4.x of the Linux kernel, and the license for the Linux kernel follows the GPL. For more information about the GPL license, see the GNU General Public License.
- The glibc library included in this product follows the LGPL. For more information about the LGPL license, see the GNU Lesser General Public License.
- This product uses the “OpenSSL”, which is licensed under the OpenSSL and Original SSLeay licenses. For more information about the OpenSSL and Original SSLeay licenses, please see the OpenSSL License and Original SSLeay License.
- The source modified based on Linux kernel 4.x and glibc library included in this product can be downloaded by contacting the Suprema Technical Support Team.

Suprema Inc.

17F Parkview Tower, 248, Jeongjail-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, 13554, Rep. of KOREA

Tel: +82 31 783 4502 | Fax: +82 31 783 4503 | Inquiry: sales_sys@supremainc.com

For more information about Suprema's global branch offices,
visit the webpage below by scanning the QR code.
https://supremainc.com/en/about/global-office.asp

© 2026 Suprema Inc. Suprema and identifying product names and numbers herein are registered trade marks of Suprema, Inc.
All non-Suprema brands and product names are trademarks or registered trademarks of their respective companies.
Product appearance, build status and/or specifications are subject to change without notice.