BioStation 3

INSTALLATION GUIDE

Version 1.04

English
EN 101.00.BS3 V1.04

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 14

Note for QR code usage and device license 15

Installation 16

Fixing the bracket and the product 16

Power supply connection 27

Network Connection 28

Input connection 29

Relay Connection 30

Connecting as a Standalone 32

Connecting to Secure I/O 2 34

Wiegand Connection 36

Product Specifications 37

Credentials 37

General 37

Capacity 38

Interface 39

Electrical 40

Dimensions and Weight 41

Regulatory Information 43

Regulatory & Licenses 43

FCC Compliance Information 44

EU Declaration of Conformity (CE) 45

Appendices 46

Disclaimers 46

Copyright Notice 47

Open Source License 47

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.

The product is powered by Class 2 Power supply with 12 VDC or 24 VDC; or by UL 62368-1 listed PoE Power Source Equipment (PSE).

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.

For PoE / PoE+, the maximum distance from PSE is 100 meters or 328 feet.

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.

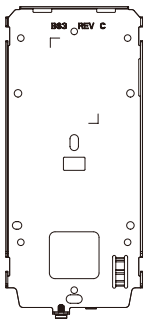
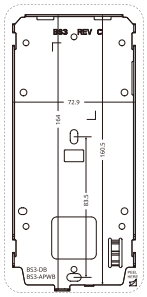
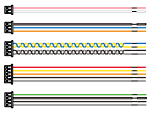
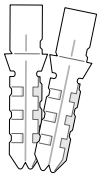
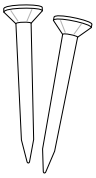
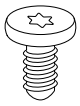
- The device may malfunction.

> **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.

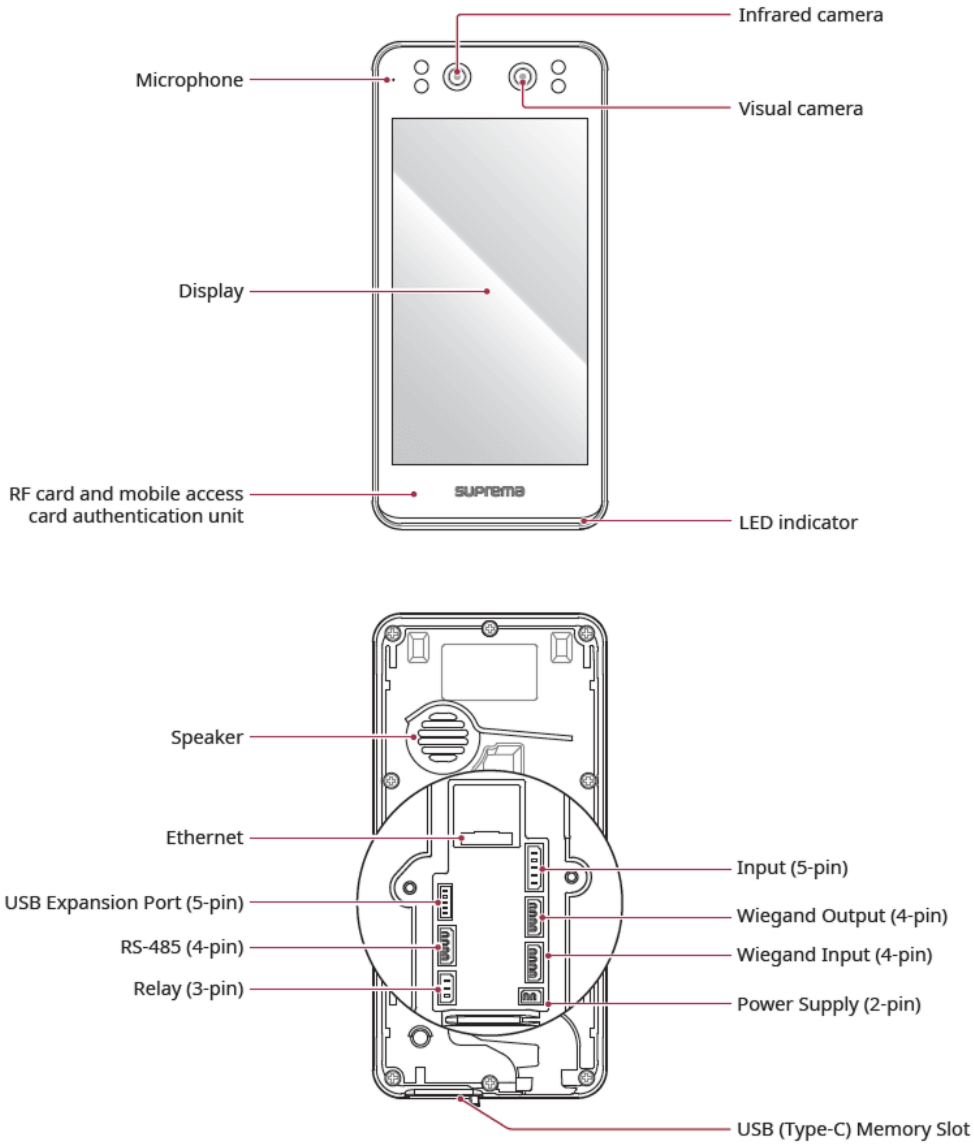
Components

				
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

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.

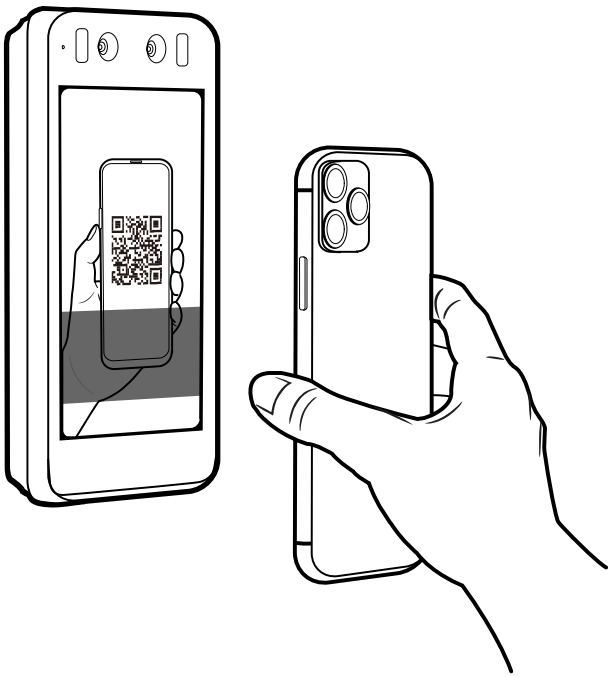
Cautions for authenticating a face

- 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.

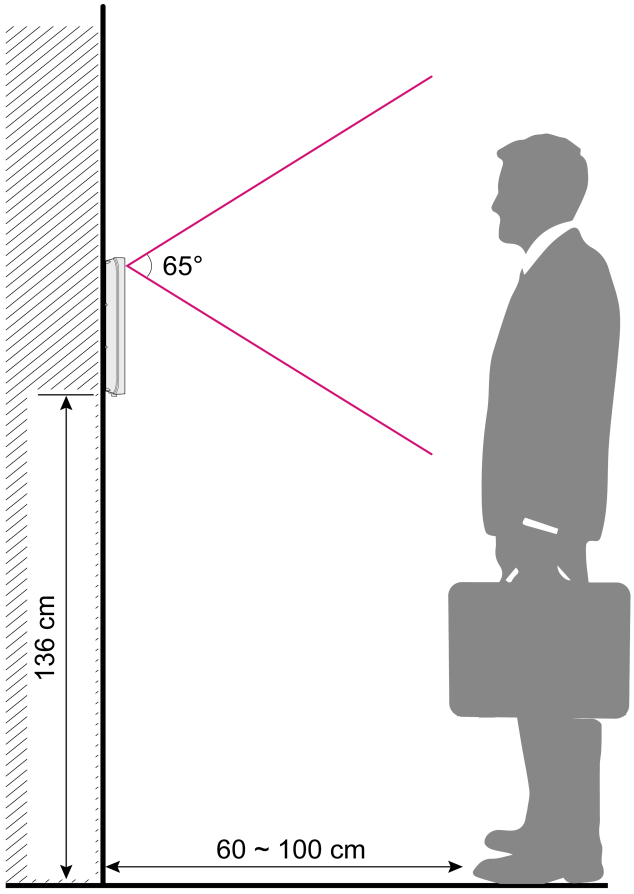
Installation

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

Fixing the bracket and the product

General bracket

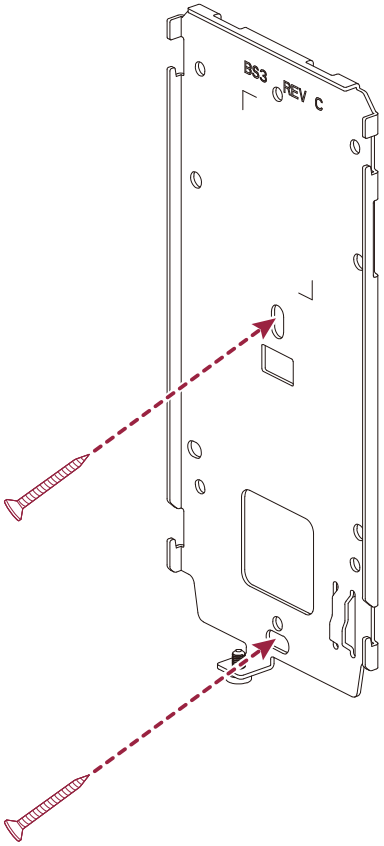
1. Determine the correct position to install the bracket using the provided drilling template.



Info

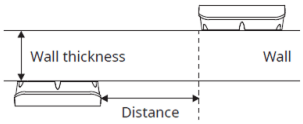
- The optimal height for installing device is 136 cm.
- Install the device where it does not reach the direct sunlight or UV light.
- Adjust the installation position so that the face is not exposed to direct sunlight when a user tries to authenticate.

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

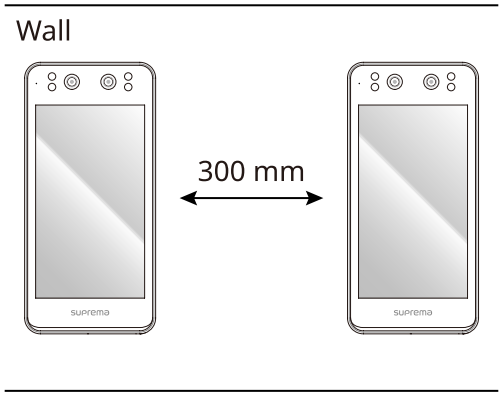


Info

- 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.

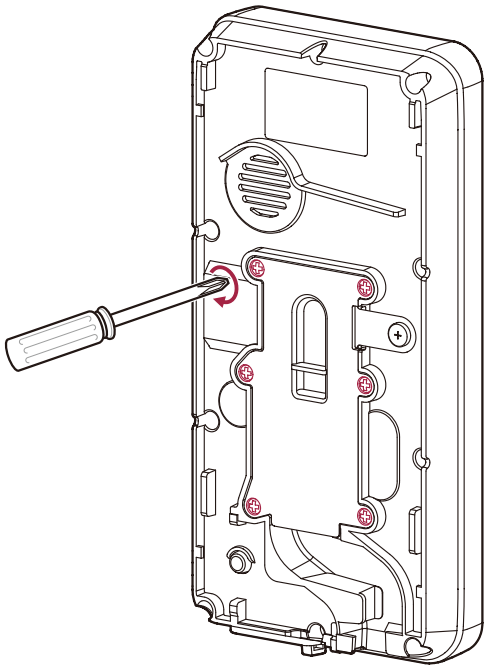


Wall thickness	Distance
100 mm	200 mm
120 mm	180 mm
150 mm	150 mm



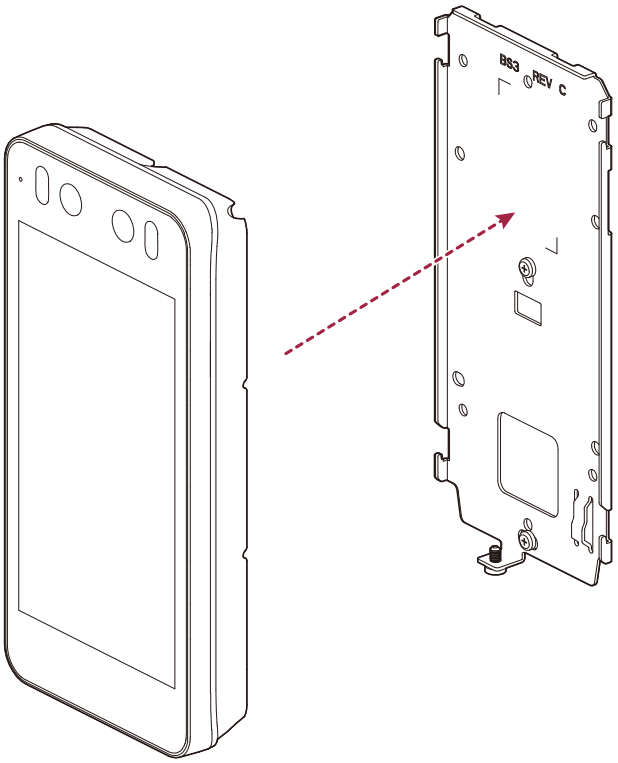
- When using a mobile access card, install devices maintaining a minimum distance of 1 m between devices to avoid BLE interference.

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

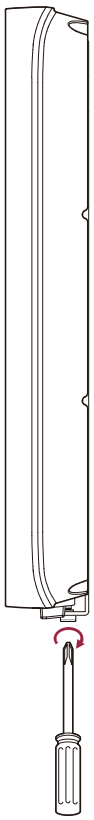


> **Info**
> Make sure that the cable cover is completely closed after connecting it to the product to maintain the water-resistant and dust-resistant features (IP65 rating).

4. Mount the product on the fixed bracket.



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



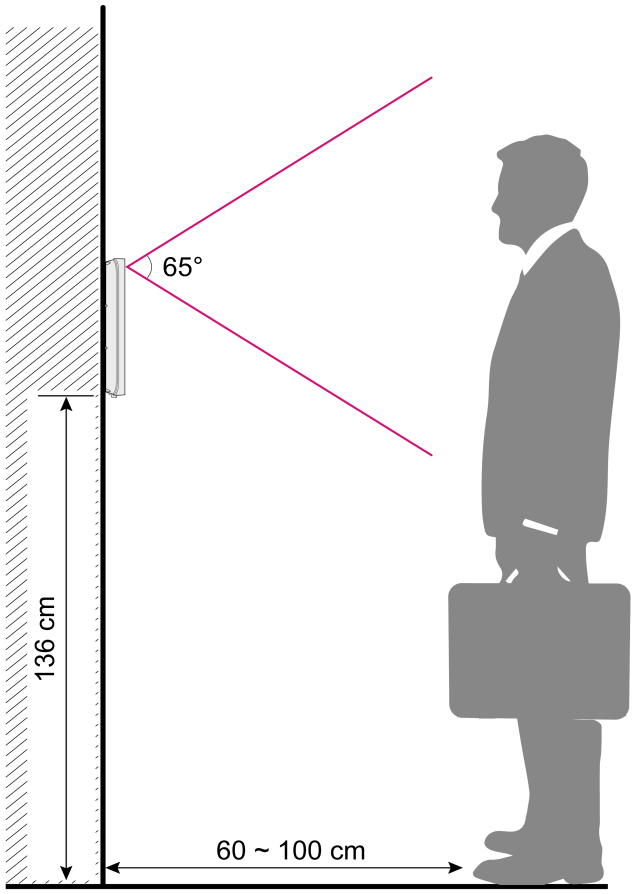
Info

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.

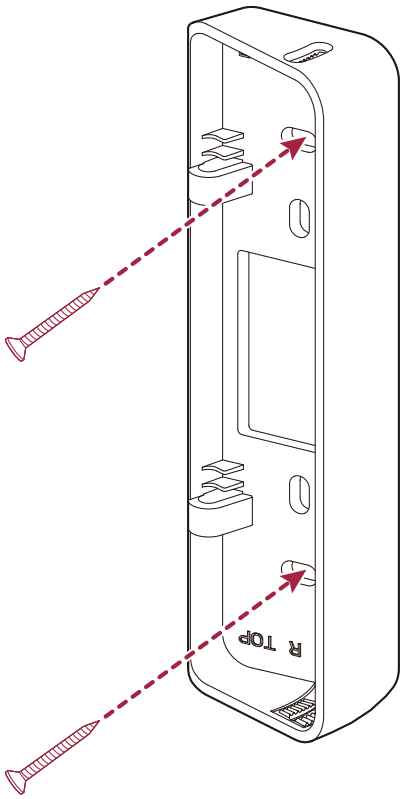
1. Determine the correct position to install the bracket using the provided drilling template.



Info

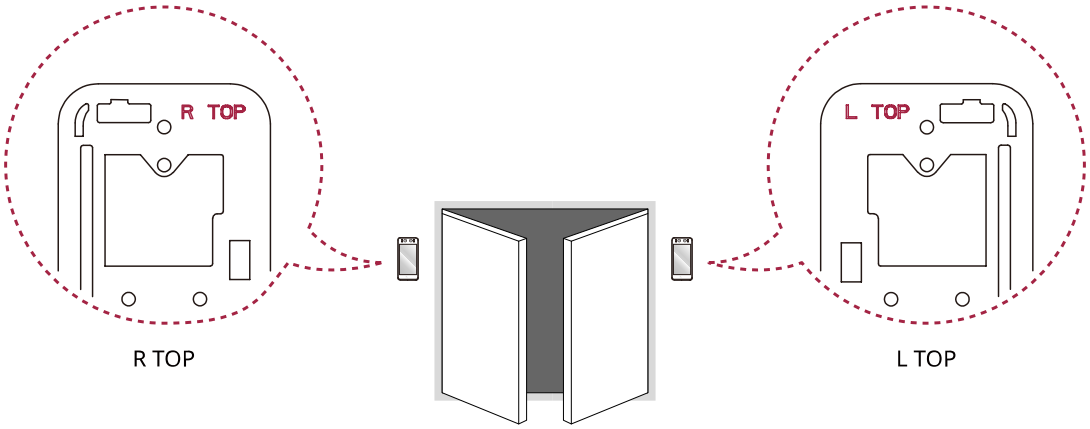
- The optimal height for installing device is 136 cm.
- Install the device where it does not reach the direct sunlight or UV light.
- Adjust the installation position so that the face is not exposed to direct sunlight when a user tries to authenticate.

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



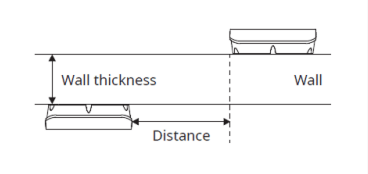
Depending on the installation location, install the tilting bracket with the top and bottom orientation as follows.

- 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

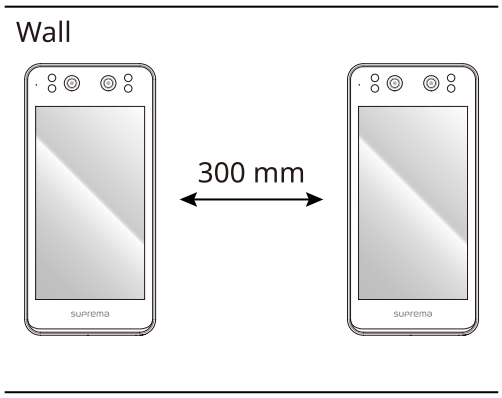


Info

- 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.

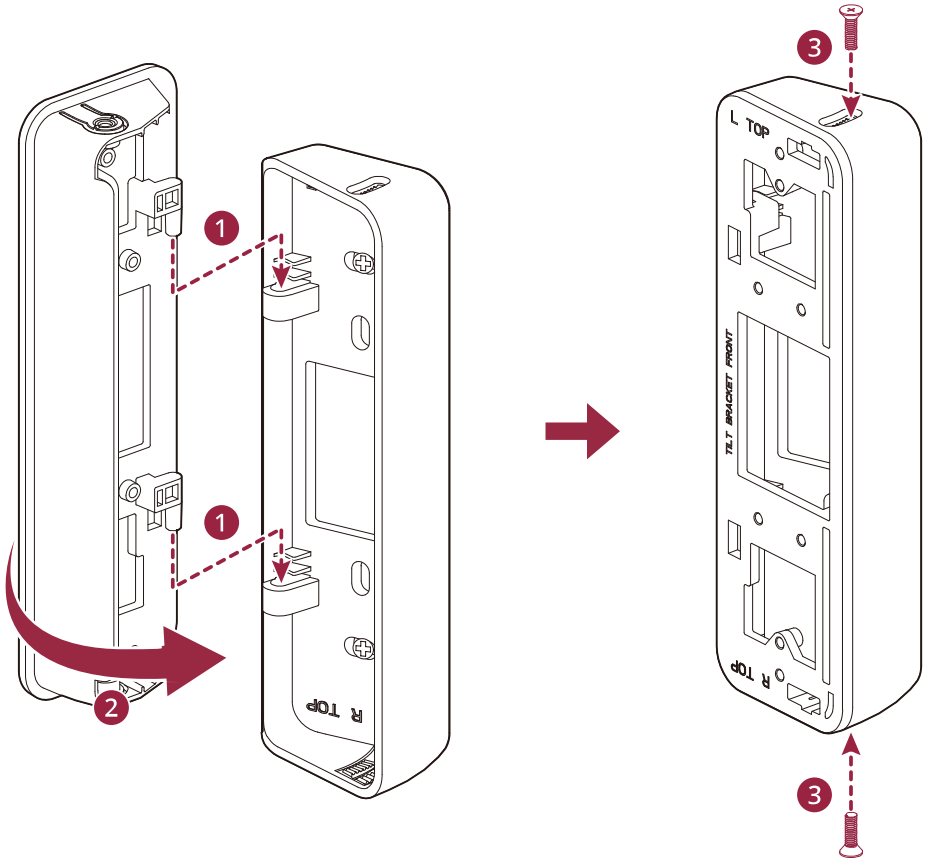


Wall thickness	Distance
100 mm	200 mm
120 mm	180 mm
150 mm	150 mm



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

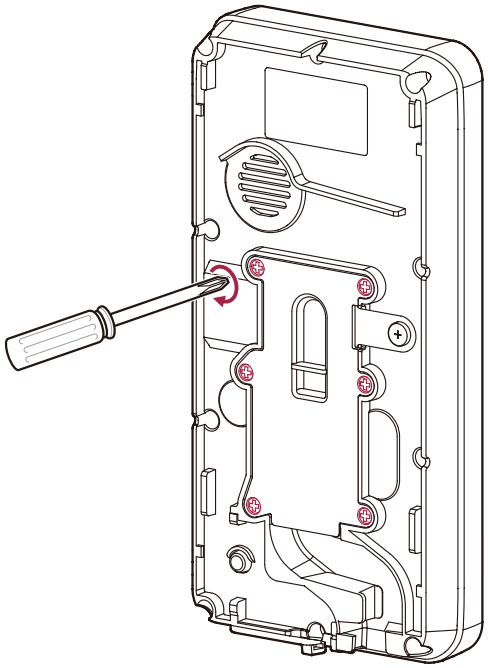
3. Join the front of the tilting bracket to the groove in the back, close it, and secure it with two screws in the upper and lower screw holes.



Info

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

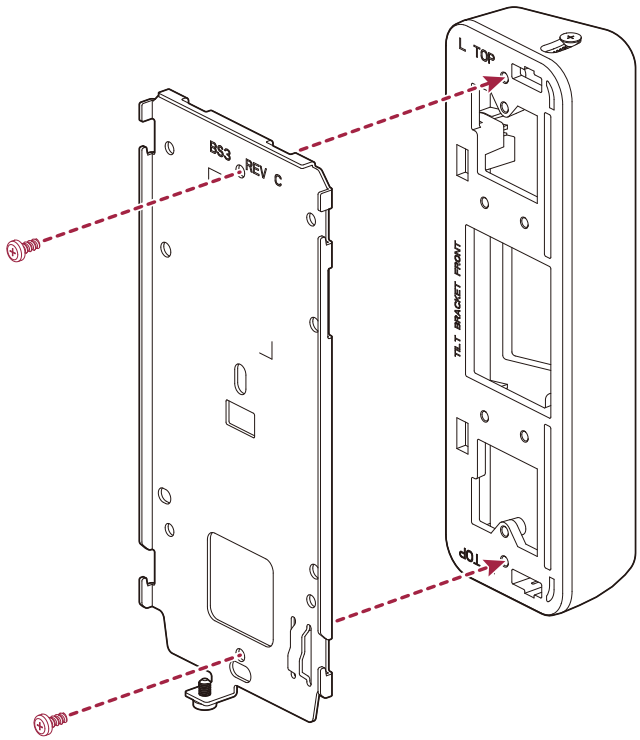
4. After attaching the cable cover, tighten the six screws on the cover to secure it firmly.



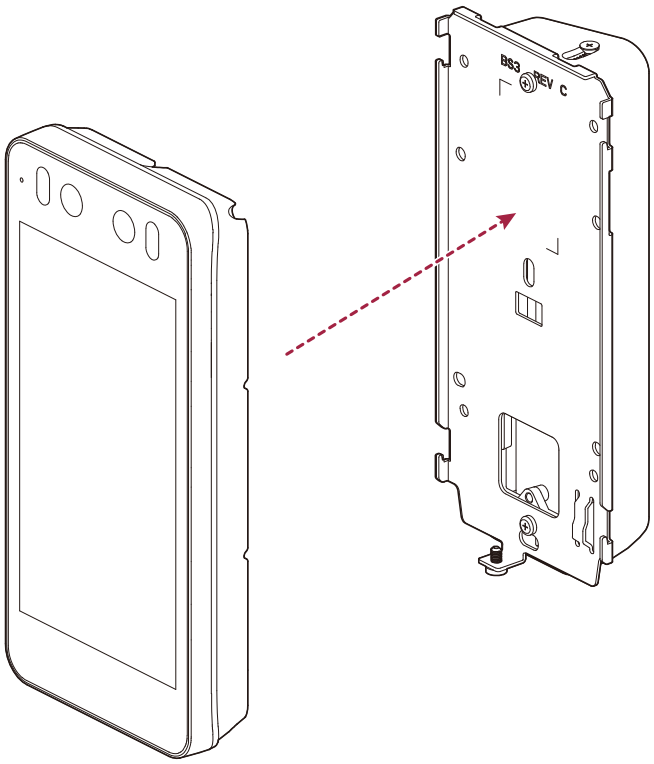
Info

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).

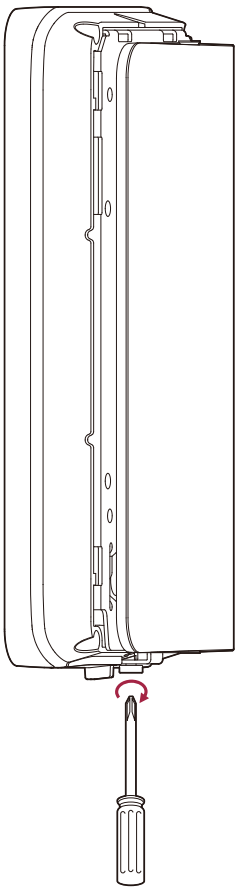
5. Secure the wall-mount bracket firmly on top of the tilting bracket.



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



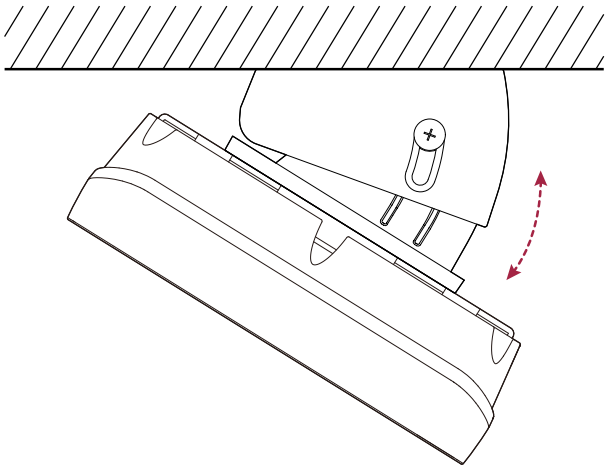
7. Tighten the product fixing screws to assemble the product and the wall-mount bracket.



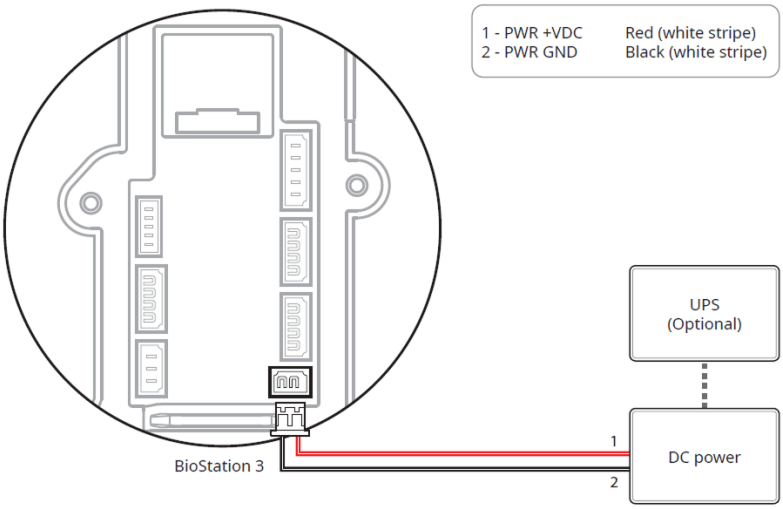
Info

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

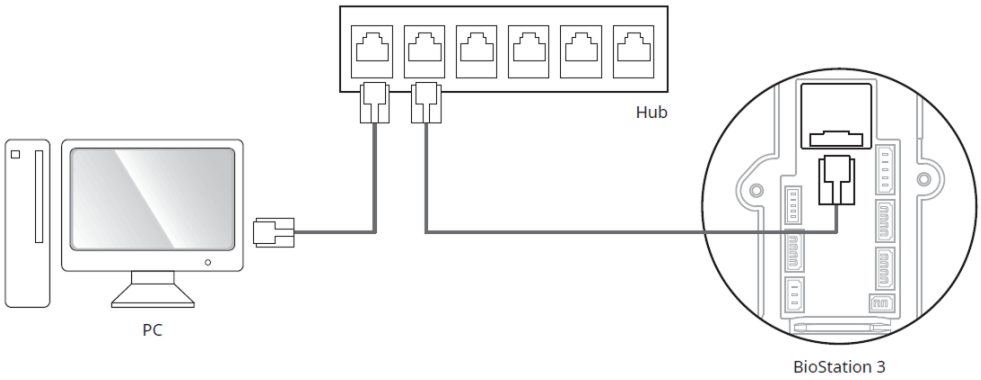
- DO NOT extend the length of power cable when using the power adapter.
- DO NOT use the CAT5 UTP 2-Wire for power supply purpose.

Network Connection

TCP/IP

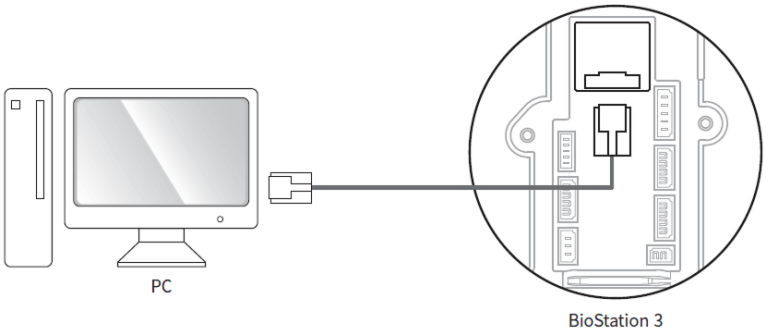
LAN connection (connecting to a hub)

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

When you use a gigabit network switch, see below information.

- Use a CAT-5e UTP(Unshielded Twisted Pair) cable.
- Use all 4 pairs (8 lines) of cable for network connection.
- DO NOT use the pair of cable for other purpose.

Network ports and services

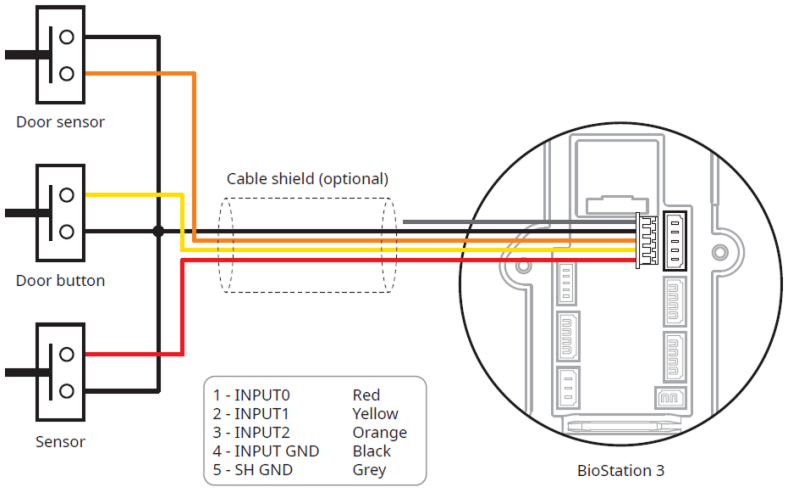
This device uses the following ports for network communication and stable service operation.

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 are used to provide normal network features of the product. When configuring firewall rules or network security settings, allow the use of these ports.

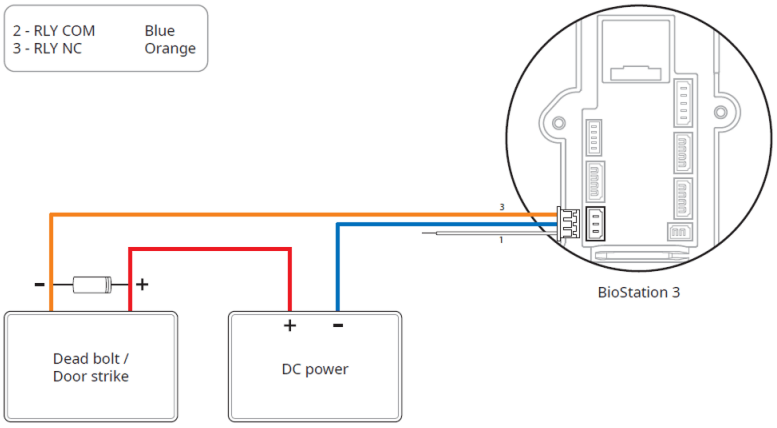
Input connection



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

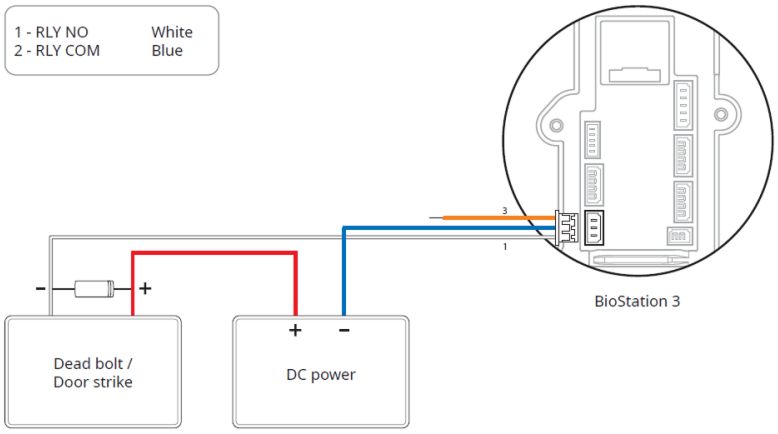
- Install a diode at both sides of the door lock wire as shown in the figure to protect the relay from the reverse current, which occurs when the door lock operates.
- Use a separate power supply for the product and the door lock.
- Suprema's standalone intelligent readers contain internal relays that 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.



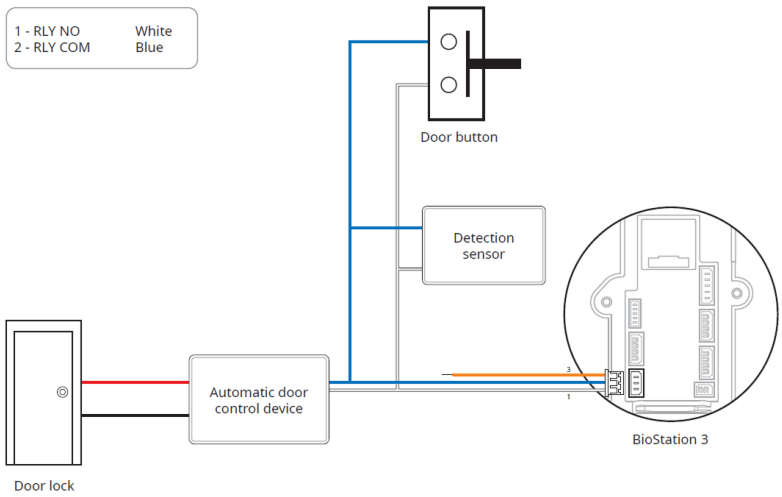
Caution

- 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

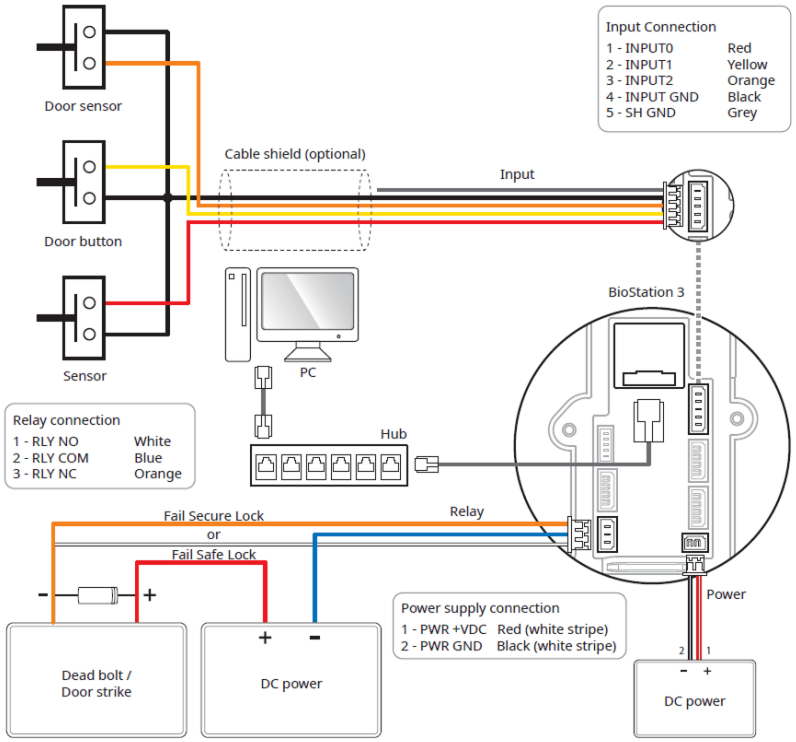
Take caution of the installation direction of the diode. Install the diode close to the door lock.

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.

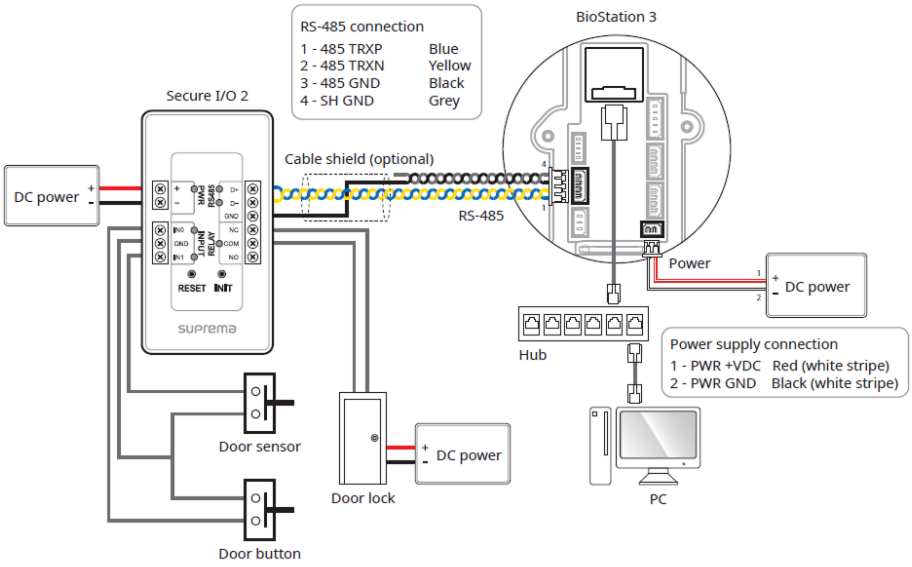
Info

- 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.
- If a fingerprint authentication device is configured as a slave device in BioStation 3, you cannot add another BioStation 3 as a slave device.
- If the fingerprint authentication device is the master device, BioStation 3 cannot be added as a slave device.
- When you connect BioStation 3 as a slave device while BioStation 3 is the master device, only one BioStation 3 can be added as a slave device.
- When BioStation 3 is the master device and another BioStation 3 is connected to it as a slave device, you can connect one additional Secure I/O 2 and DM-20 each.
- When BioStation 3 is the master device and another BioStation 3 is connected to it as a slave device, you cannot connect additional OM-120.
- BioStation 3 cannot be used as a slave device when FaceStation F2 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.

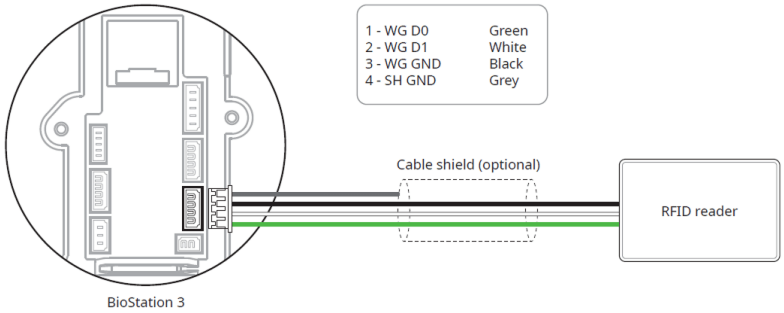


Info

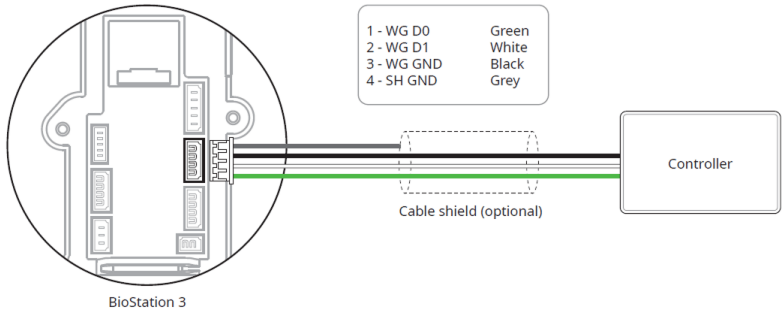
- The device can be used as a multi-door controller with the slave devices with the RS-485 cable. The slave devices are used as dummy readers and authentication is performed in the master device.
- If a fingerprint authentication device is configured as a slave device in BioStation 3, you cannot add another BioStation 3 as a slave device.
- If the fingerprint authentication device is the master device, BioStation 3 cannot be added as a slave device.
- When you connect BioStation 3 as a slave device while BioStation 3 is the master device, only one BioStation 3 can be added as a slave device.
- When BioStation 3 is the master device and another BioStation 3 is connected to it as a slave device, you can connect one additional Secure I/O 2 and DM-20 each.
- When BioStation 3 is the master device and another BioStation 3 is connected to it as a slave device, you cannot connect additional OM-120.
- BioStation 3 cannot be used as a slave device when FaceStation F2 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.



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**
IP Rating	**IP65**
IK Rating	**IK06**
Authentication	**CE, UKCA, KC, FCC, IC, RCM, BIS, SIG, RoHS, REACH, WEEE, MIC, TELEC, ETL Listed to UL 294**

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**

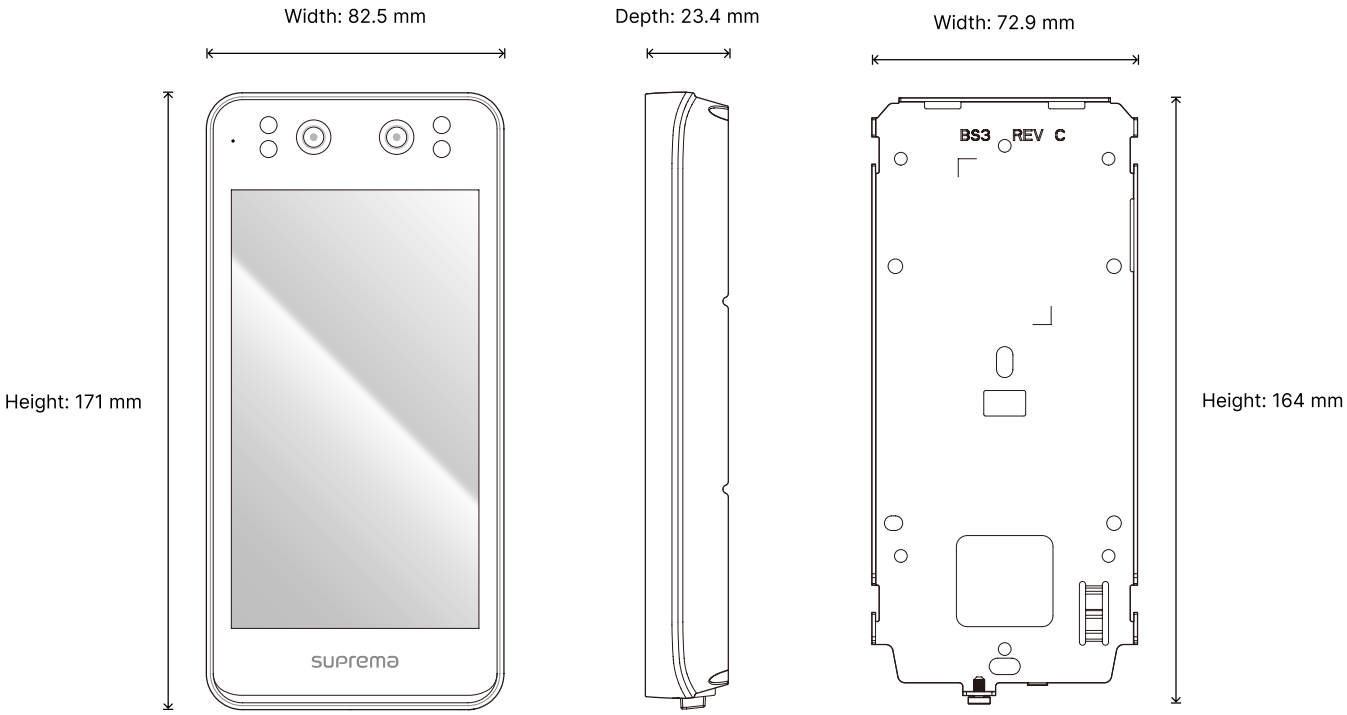
Interface

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**	
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**
	PoE+[7]	• **IEEE 802.3at compliant, 44-57 VDC Max. 600 mA** • **BS3-DB: Not supported** • **BS3-APWB: Supported**
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) RF read range will vary depending on 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

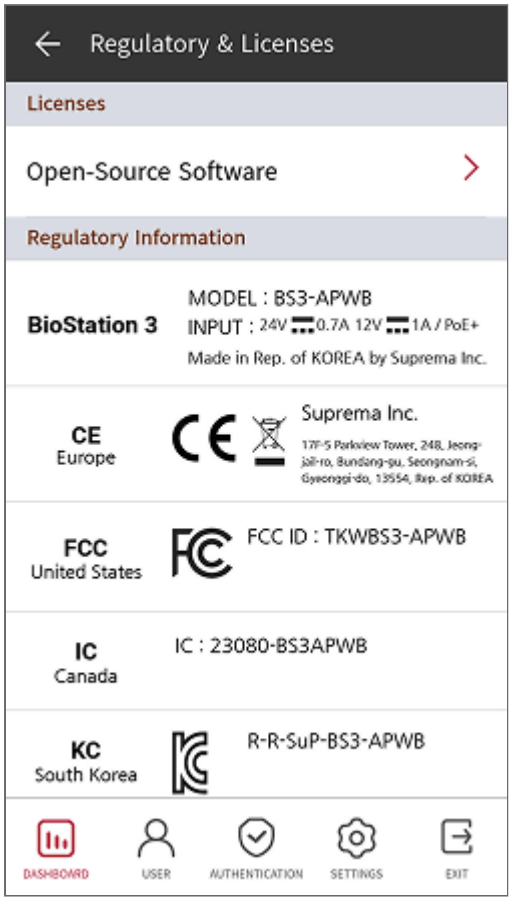
Provides information on regulations and certifications complied with by the product.

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.

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

© 2023 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.