FaceStation 2

USER GUIDE

Version 1.29

English
EN 102.00.FS2

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 10

Correct face enrollment and authentication method 12

Installation 14

Fixing the bracket and the product 14

Power supply connection 21

Network Connection 22

Input connection 23

Relay Connection 24

Connecting as a Standalone 26

Connecting to Secure I/O 2 27

Wiegand Connection 29

How to Use 30

Admin Menu 30

User 30

Authentication 34

Settings 38

Event Logs 47

Troubleshooting 50

Check items before reporting a malfunction 50

Product Specifications 52

Credentials 52

General 52

Capacity 53

Interface 53

Electrical 54

Dimensions and Weight 55

Regulatory Information 56

FCC Compliance Information 56

IC information 56

EU Declaration of Conformity (CE) 57

Appendices 58

Disclaimers 58

Copyright Notice 59

Open Source License 59

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.

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.

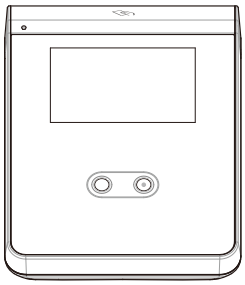
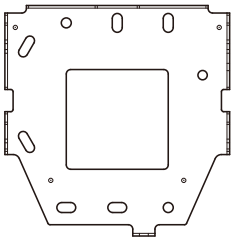
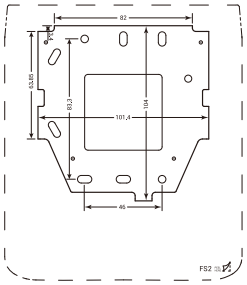
- The device may malfunction.

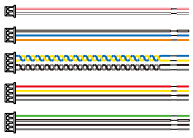
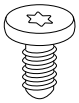
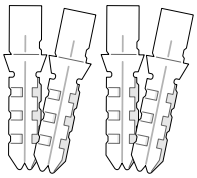
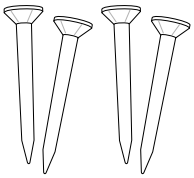
> **RTC Battery**
>
> Replacing with unauthorized or incorrect types of batteries may pose a risk of explosion. Dispose of batteries according to local or international waste regulations.

Getting Started

Provides initial procedures for getting started with the device.

Components

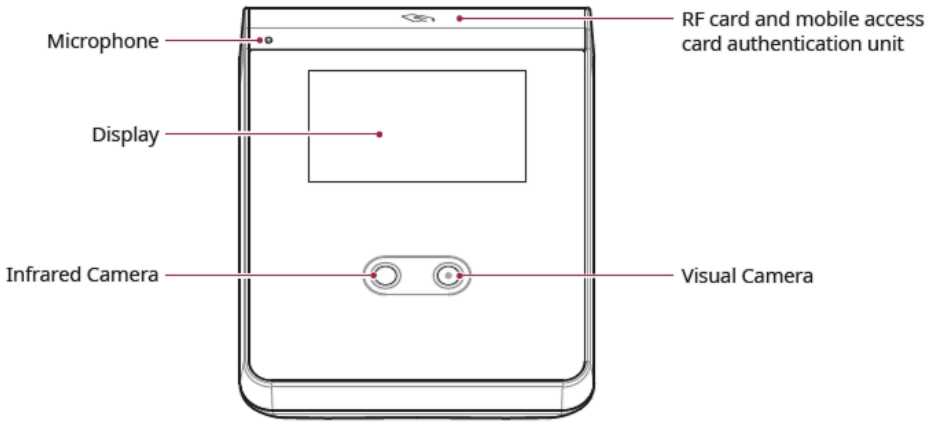
		
FaceStation 2	Wall Bracket	Drilling Template

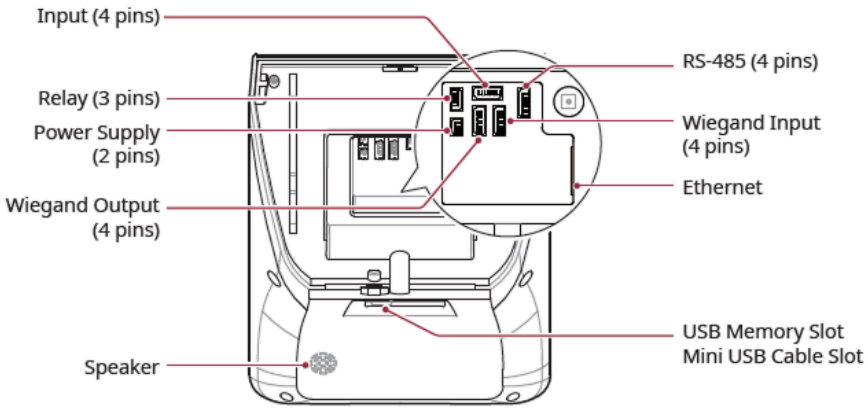
			
Connection Cables	Diode	120 Ω Resistor	Bracket Fixing Screw (Star Shaped)
			
PVC Anchor x4	Fixing Screw x4	Quick Guide	Open Source Software Guide

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.
- **Display**: Provides a UI for operation.
- **Infrared Camera**: Capture the infrared face image.
- **Visual Camera**: Capture an actual face image.
- **RF card and mobile access card authentication unit**: Part to scan a RFID card or mobile access card for entrance.
- **Speaker**: Delivers sound.
- **USB Memory Slot**: Connect the USB memory.

  - The Suprema thermal camera (TCM10-FS2) cannot be used simultaneously with the USB memory.

- **Mini USB Cable Slot**: Support coming soon.
- **Input (4-pin)**: Connect the 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.
- **Ethernet**: Connect the Ethernet cable.
- **Wiegand Input (4-pin)**: Connect the Wiegand Input cable.
- **Wiegand Output (4-pin)**: Connect the Wiegand Output cable.

Cables and connectors

Power



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

Relay



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

RS-485



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

Input



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

Wiegand Input and Output



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

Correct face enrollment and authentication method

Cautions for enrolling a faces

- Keep the distance between the device and your face at 40-80 cm when enrolling a 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 40~80 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.

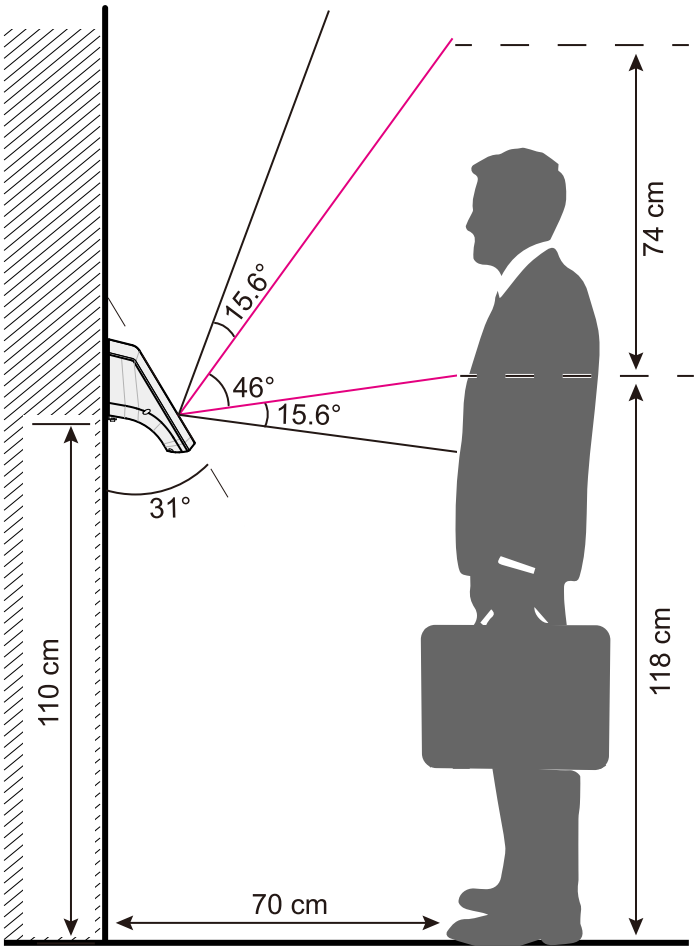
Installation

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

Fixing the bracket and the product

General bracket

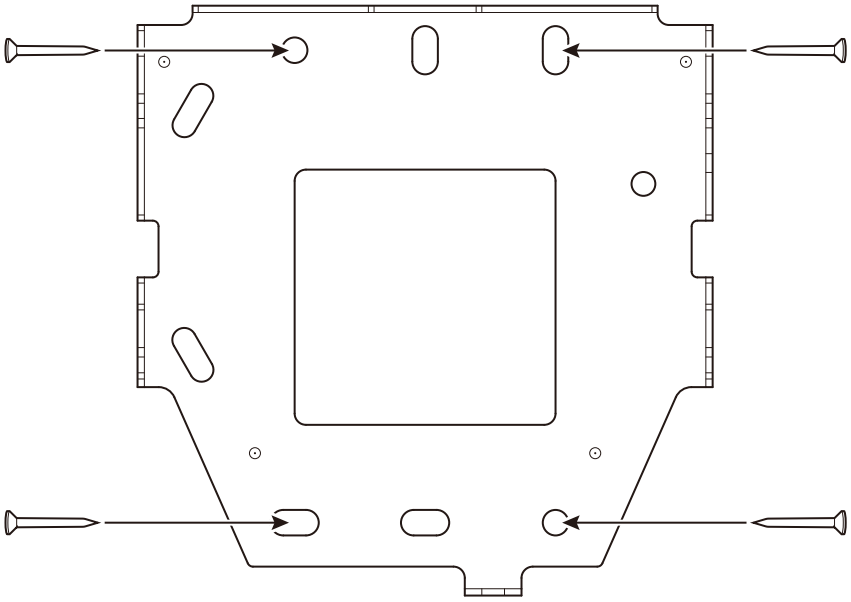
1. Determine the correct position to install the bracket using the provided drilling template.



Info

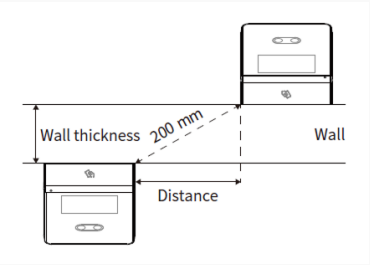
- The optimal height for installing device is 110 cm.
- Install the device where it does not reach the direct sunlight or UV light.
- Adjust the installation position so that the face is not exposed to direct sunlight when a user tries to authenticate.

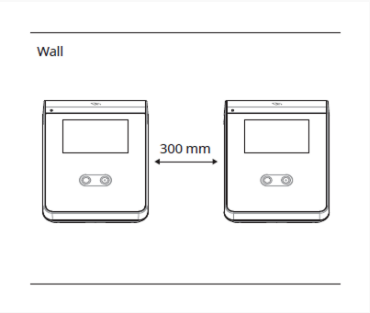
2. Secure the bracket tightly using the fixing screws at the location where the product will be mounted.



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.

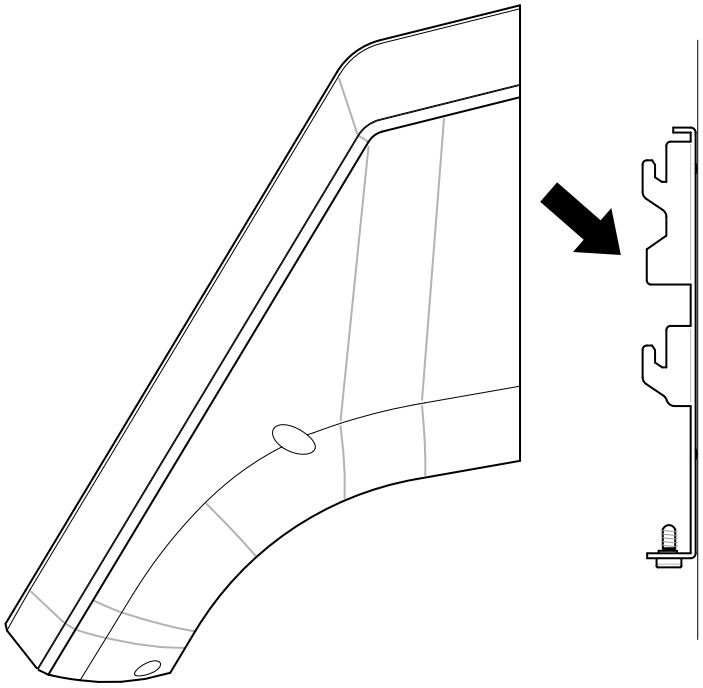




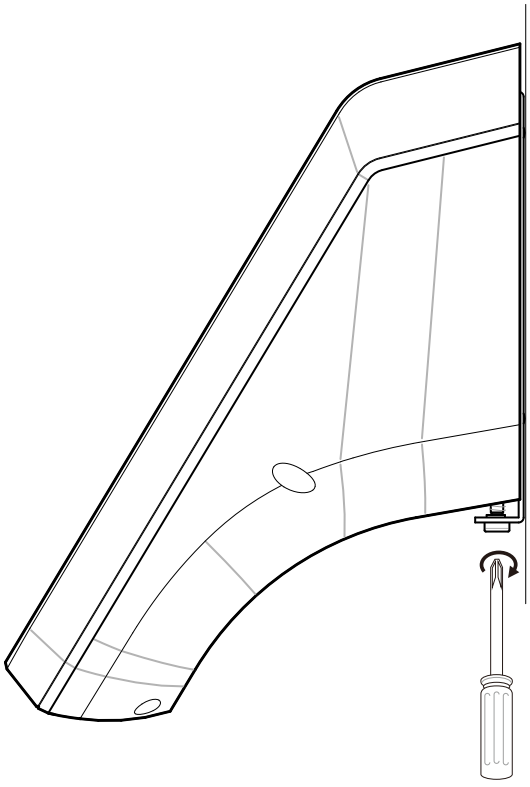
Wall thickness	Distance
100 mm	283 mm
120 mm	275 mm
150 mm	260 mm

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

3. Mount the product on the fixed bracket.



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



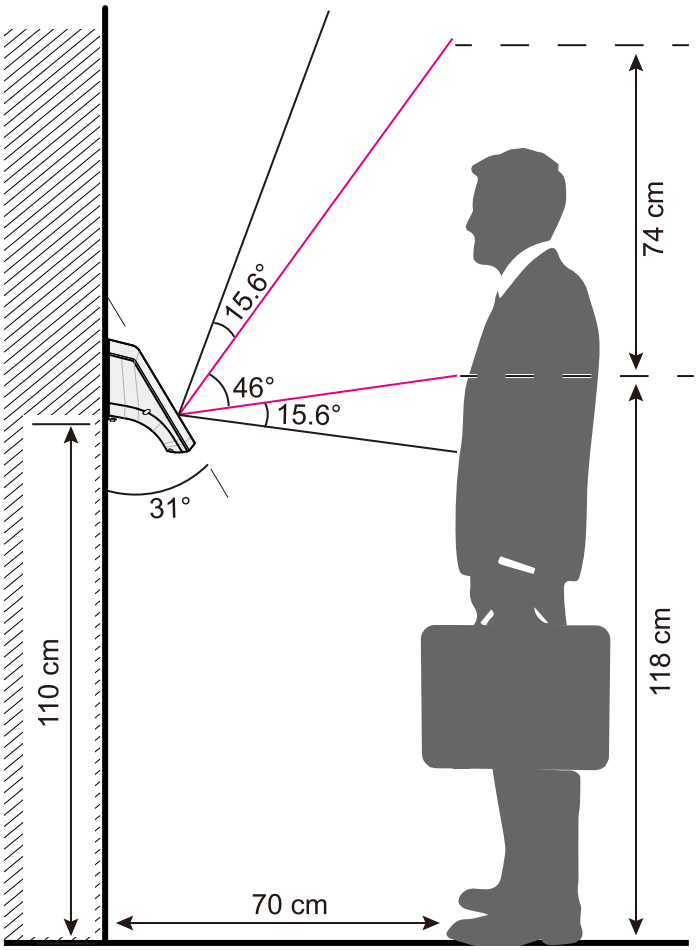
Info

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.

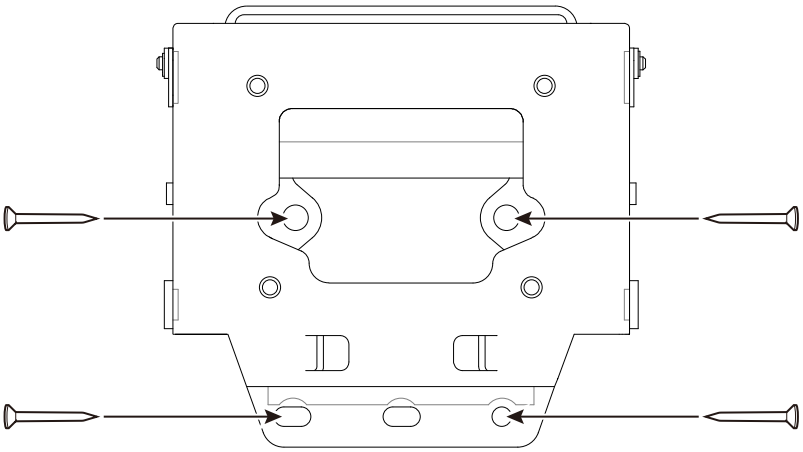
1. Determine the correct position to install the bracket using the provided drilling template.



Info

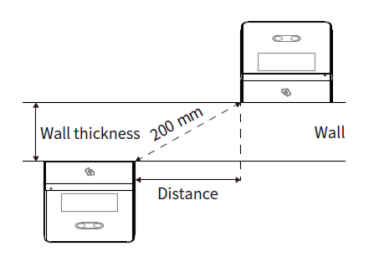
- The optimal height for installing device is 110 cm.
- Install the device where it does not reach the direct sunlight or UV light.
- Adjust the installation position so that the face is not exposed to direct sunlight when a user tries to authenticate.

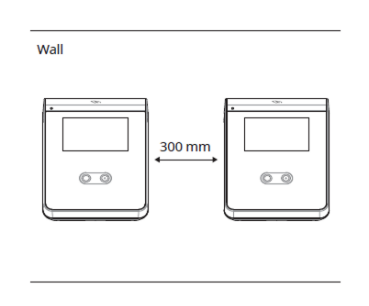
2. Secure the tilt bracket firmly to the installation location (wall) using the fixing screws for the tilt bracket.



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.

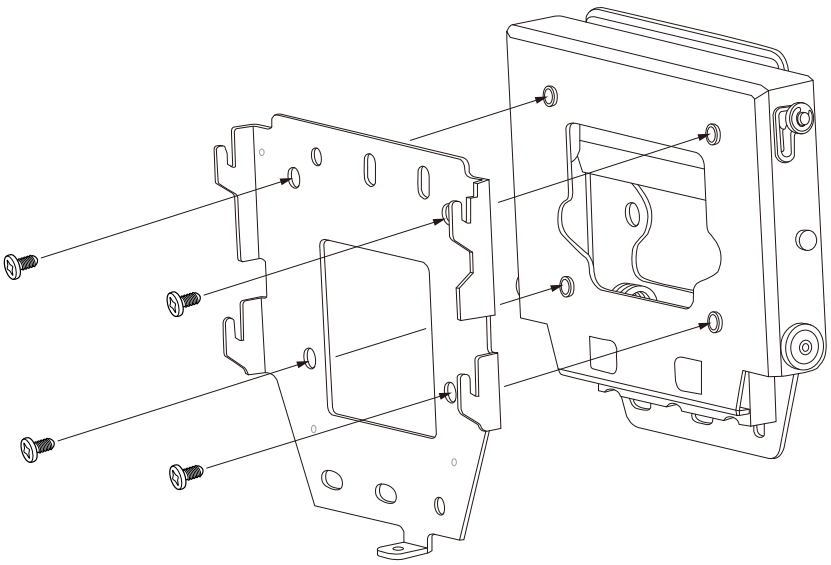




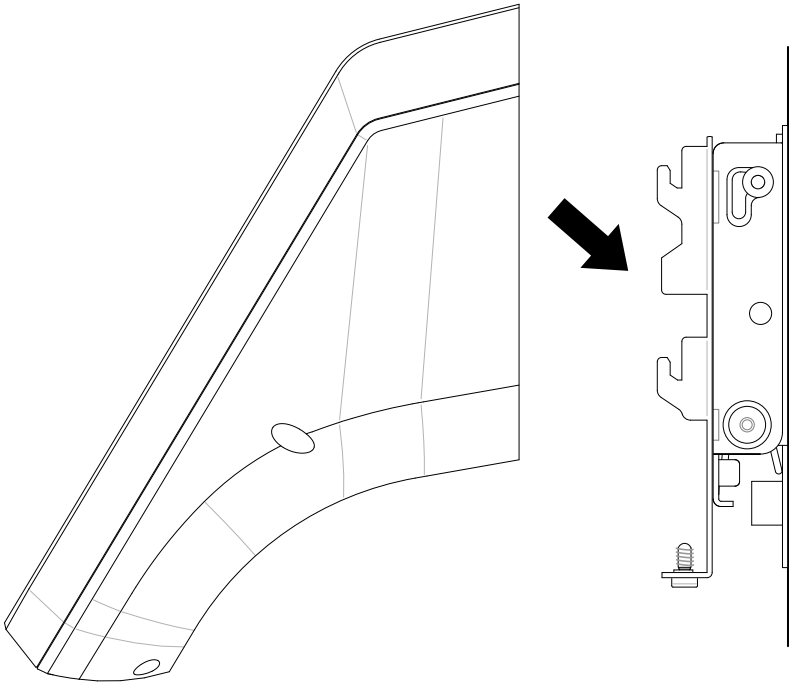
Wall thickness	Distance
100 mm	283 mm
120 mm	275 mm
150 mm	260 mm

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

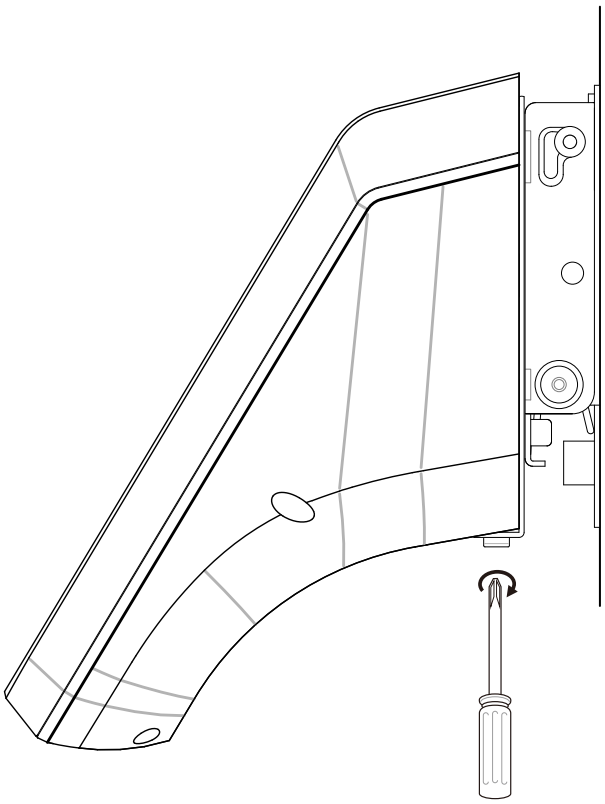
3. Secure the wall-mount bracket firmly on top of the tilting bracket.



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



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

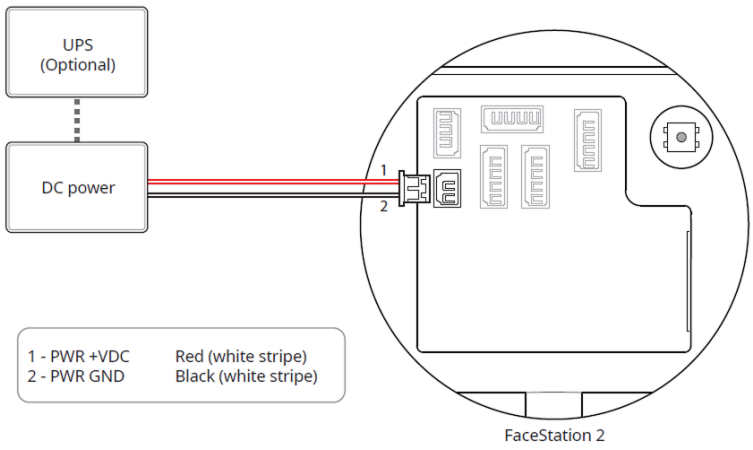


Info

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.

6. Adjust the tilting bracket to the desired angle.

Power supply connection



Caution

- 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.

Cable standard	Max. extended length
16 AWG	150 m
18 AWG	136 m
20 AWG	90 m

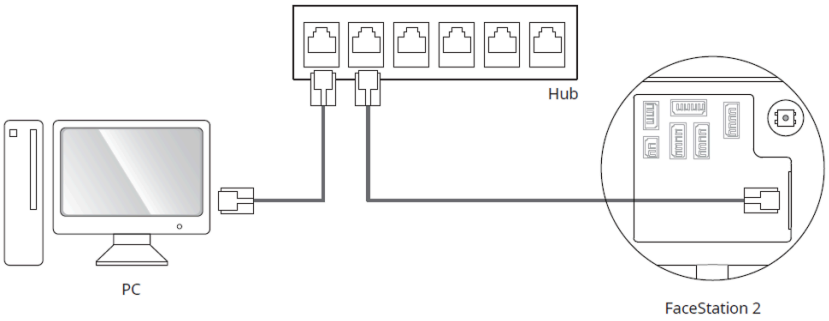
- DO NOT extend the length of power cable when using the power adapter.
- DO NOT use the CAT5 UTP 2-Wire for power supply purpose.

Network Connection

TCP/IP

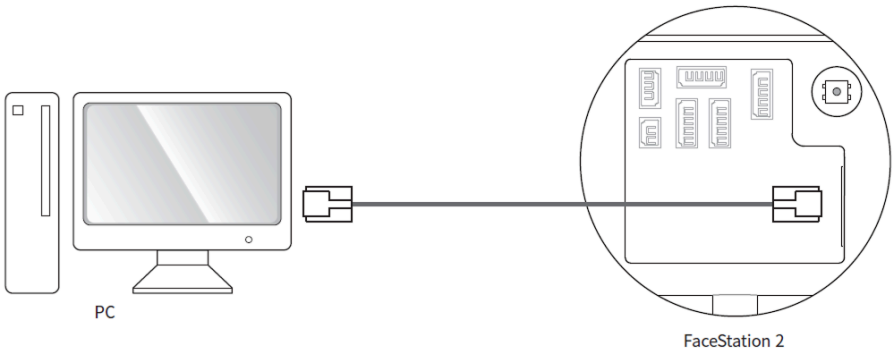
LAN connection (connecting to a hub)

You can connect the product to a hub using a general type CAT-5 cable.



LAN connection (connecting to a PC directly)

This device has an automatic MDI/MDIX function so that it can be connected to a PC directly using a normal straight type CAT-5 cable or a cross 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

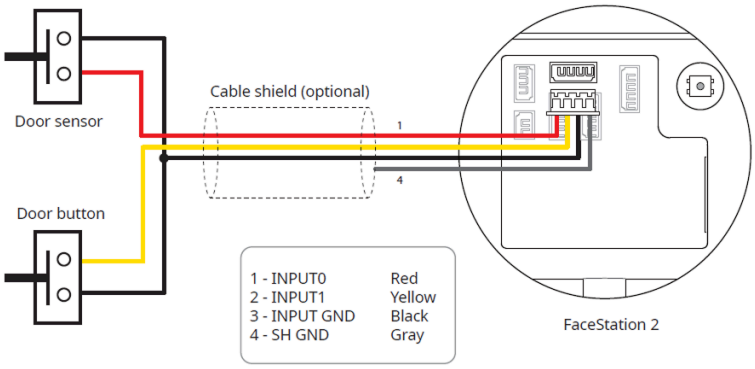
This device uses the following ports for network communication and stable service operation.

Protocol	Service Description
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.

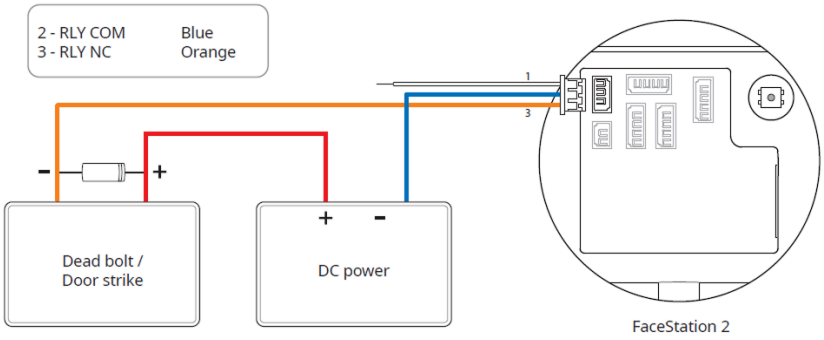
Input connection



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

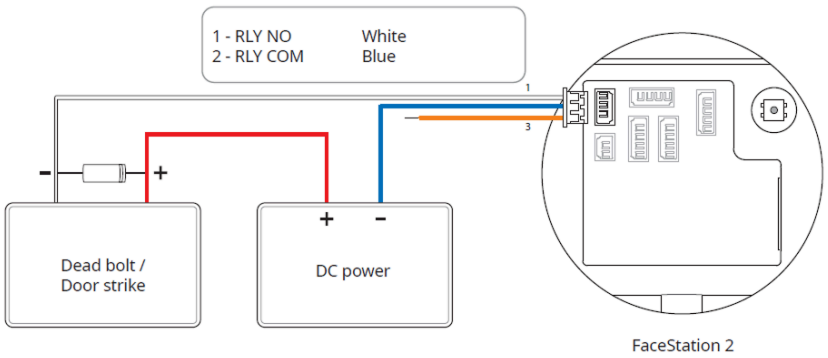
- Install a diode at both sides of the door lock wire as shown in the figure to protect the relay from the reverse current, which occurs when the door lock operates.
- Use a separate power supply for the product and the door lock.
- Suprema's standalone intelligent readers contain internal relays that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



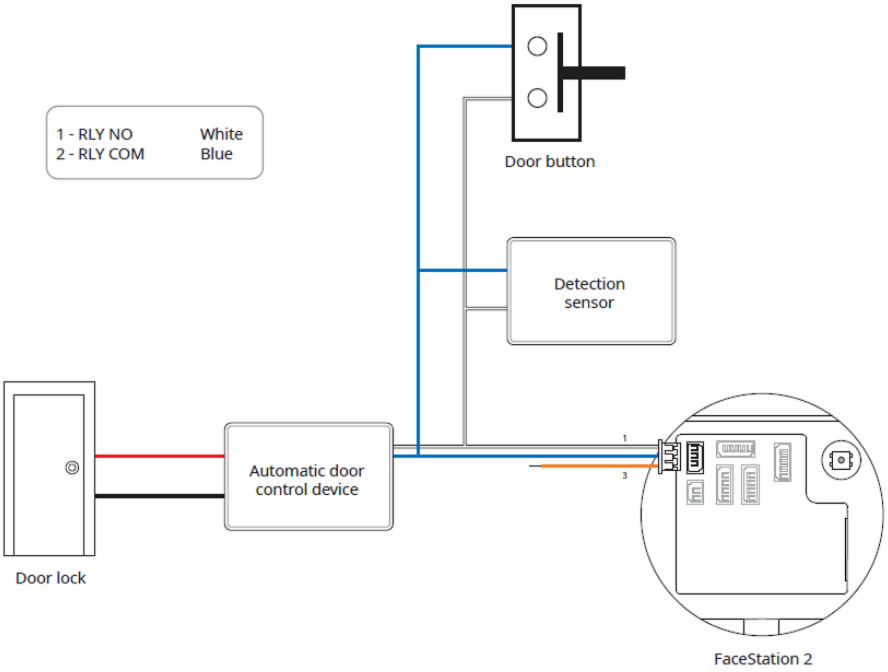
Caution

- 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

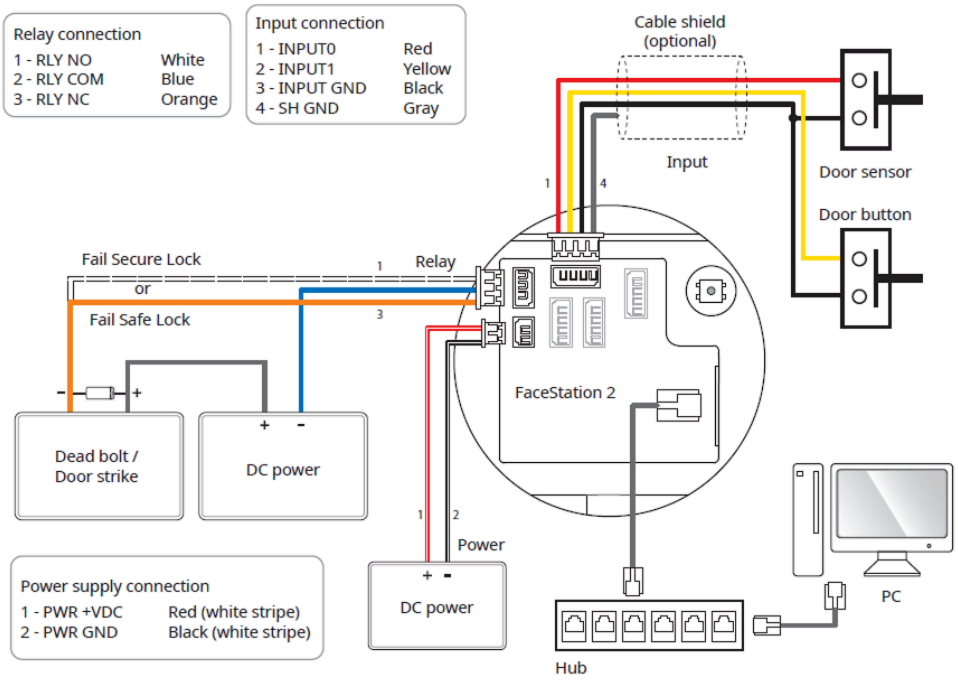
Take caution of the installation direction of the diode. Install the diode close to the door lock.

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.

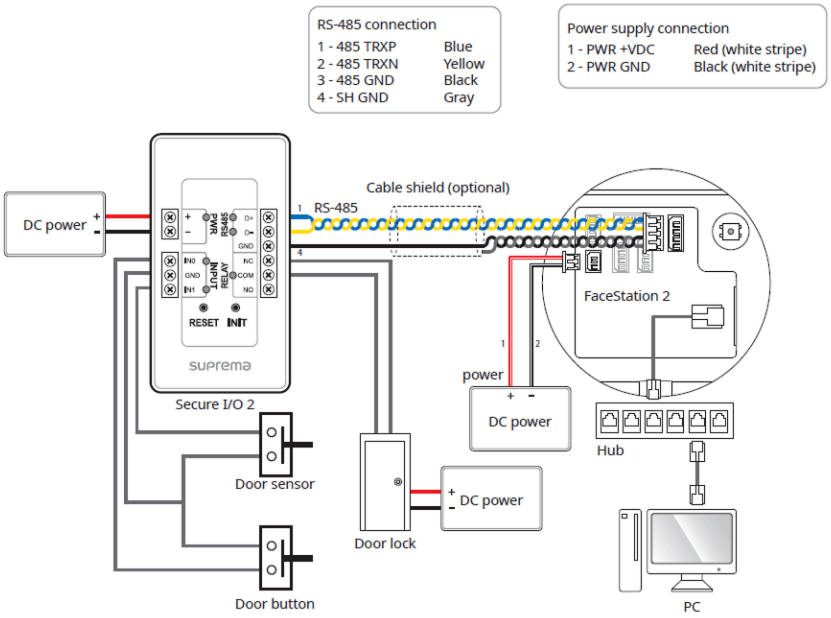
Info

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

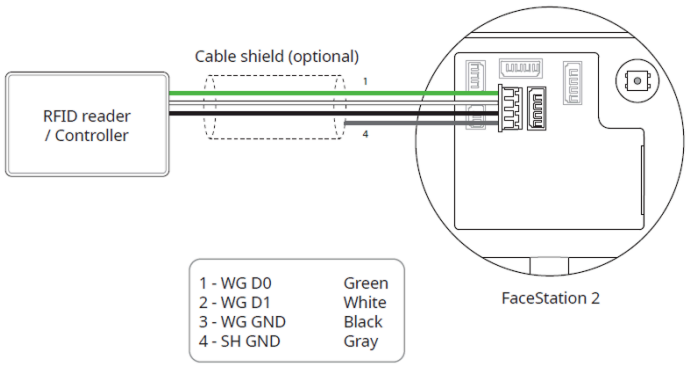


Info

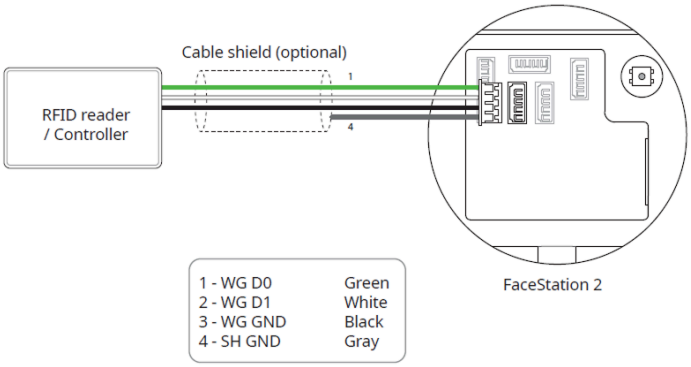
- The device can be used as a multi-door controller with the slave devices with the RS-485 cable. The slave devices are used as dummy readers and authentication is performed in the master device.
- If a fingerprint authentication device is configured as a slave device in FaceStation 2, you cannot add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

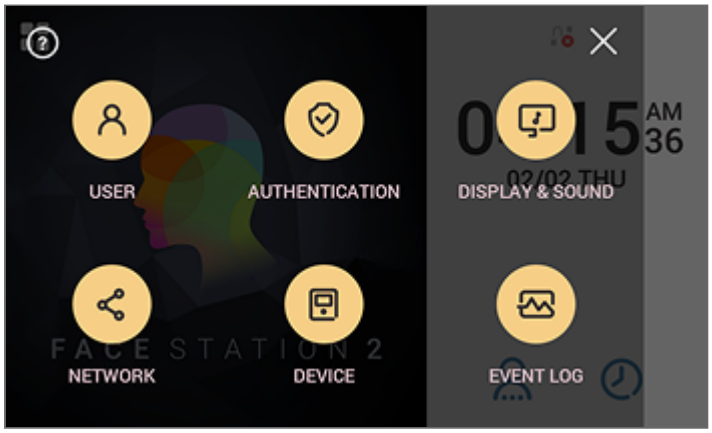
Provides guidance on how to use the main features of the device effectively.

Admin Menu

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

Full menu

1. Click and authenticate with administrator privileges.
2. Select your desired menu.



> **Info**
>
> If no administrator is specified, clicking will display the menu screen.

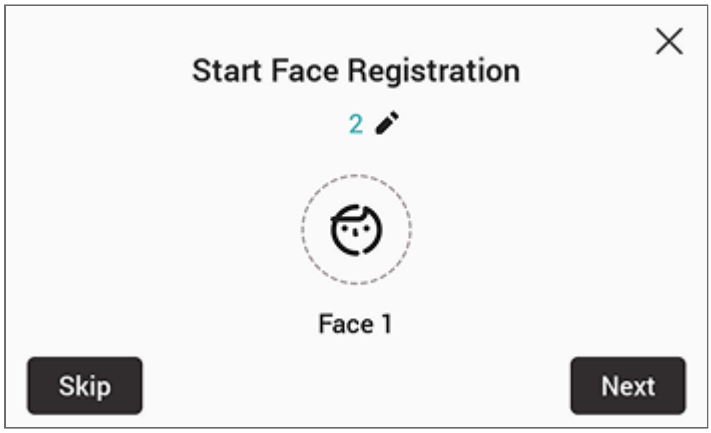
User

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

Registering user information

You can register user information that includes biometric authentication data.

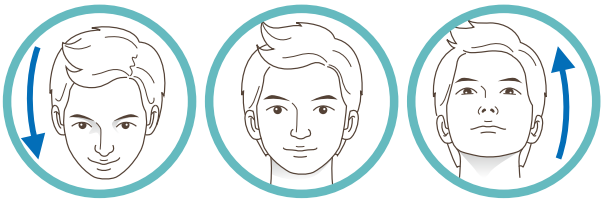
1. Click and authenticate with administrator privileges.
2. Click **USER** → . The face registration wizard will start.



3. Click **Next** to continue the face registration wizard. To skip, press **Skip** and verify step **5**.
4. If you pressed **Next**, follow the instructions on the screen to register your face. Face registration consists of a total of 3 steps.
    1. Front face registration

    2. Move face up and down

    3. Move face left and right

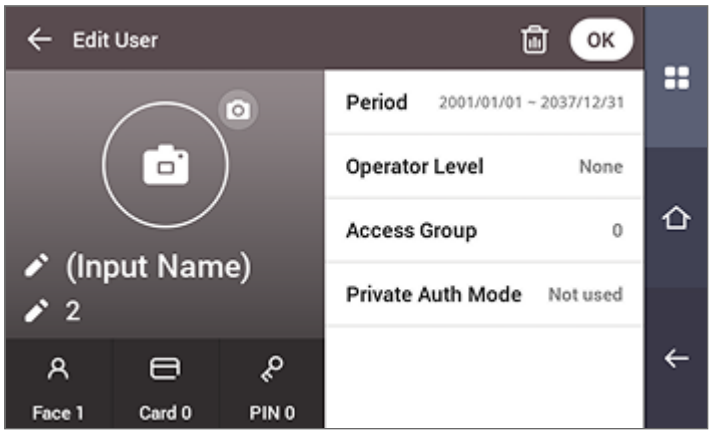
    

    Using the face registration wizard will only register the user's face. After face registration is completed, you can select the user to set additional information.

Please note the following when registering your face.

- Keep the distance between the device and your face at 40-80 cm when enrolling a 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.

5. If you pressed **Skip**, select the desired item and set it.



- : You can register a user photo.
- **Name**: Enter the user name.
- **ID**: Enter a number between 1 and 4294967295 to register a user ID. If **User ID Type** is set to **Alphanumeric**, you can use a combination of alphanumeric characters and symbols _ - as the ID, with a maximum of 32 characters.
- **Face**: You can enroll a face for user authentication. Press + and follow the instructions on the screen to register your face. To enroll more faces, click +.
- **Card**: You can enroll a card for user authentication. Press + and scan the card to assign it to the user in the RF card authentication section. To enroll more cards, click +.
- **PIN**: You can enter the PIN you want to use. Enter the PIN you want to use, then confirm by entering the PIN again, and press **OK**. To prevent leaks, input a PIN of 4 to 16 digits.
- **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**.

- **Face Group**: You can select a group for the user's face. Face groups can only be used if **Group Matching** is enabled and can only be registered in BioStar X.
- **Access Group**: You can check the user's access group. Access groups can only be registered in BioStar X.
- **Private Auth Mode**: You can set a personal authentication mode. Using personal authentication mode allows you to combine authentication methods including face authentication for each user. Otherwise, you can use the device's basic authentication mode.

6. Press **OK** to complete user information registration.

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. Click and authenticate with administrator privileges.
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.

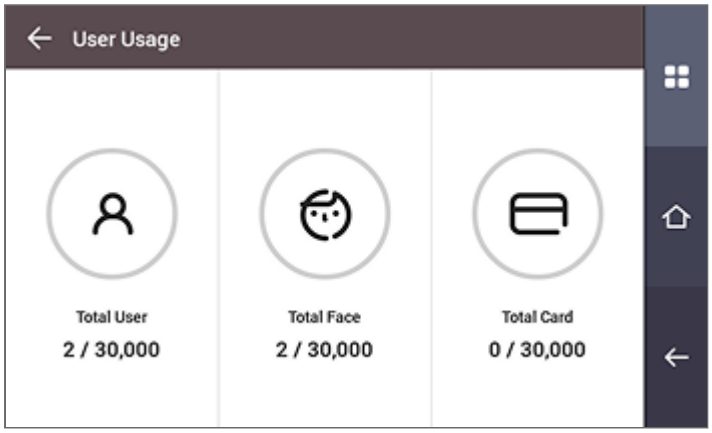
1. Click and authenticate with administrator privileges.
2. Select **USER** → .

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. Click and authenticate with administrator privileges.
2. Click **USER** → . User usage information appears.



Authentication

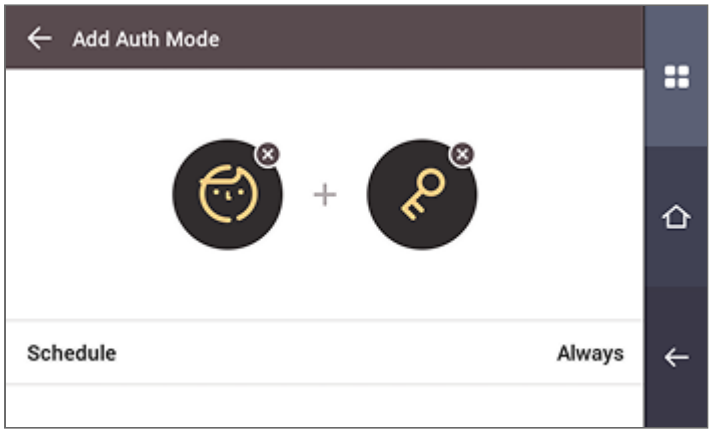
Describes the supported authentication methods and authentication procedures.

Authentication mode

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

Registering auth mode

1. Click and authenticate with administrator privileges.
2. Press **AUTHENTICATION** → **Auth Mode**.
3. Select .
4. Press to see the credentials that can be added on the screen. Select the credentials to add. You can delete the added credentials by pressing when credentials are added.



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

Category	Description
Face	- : This mode uses only facial authentication. - + : This mode authenticates with face and then enters the PIN.
Card	- : This mode uses only card authentication. - + : This mode authenticates with card and then with face. - + : This mode authenticates with card and then enters the PIN. - + / : This mode authenticates with card and then with face or enters the PIN. - + + : This mode uses both face authentication and PIN entry after authenticating with the card.
ID	- + : This mode enters the ID and then authenticates with face. - + : This mode enters the ID and then enters the PIN. - + / : This mode enters the ID and then either authenticates with face or enters the PIN. - + + : This mode uses both face authentication and PIN entry after entering the ID.

> **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.

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

Modifying auth mode

1. Click and authenticate with administrator privileges.
2. Press **AUTHENTICATION** → **Auth Mode**.
3. Select the authentication mode to modify.

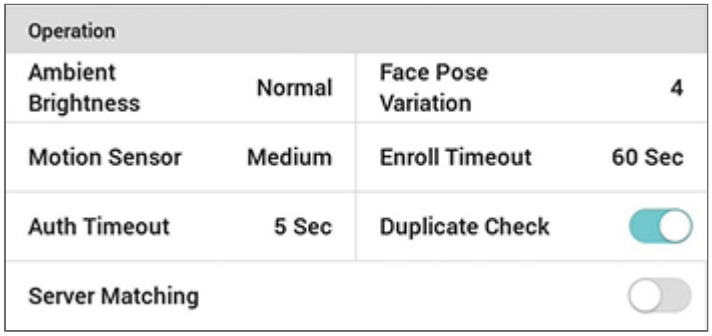
4. Modify the authentication mode by referring to Registering auth mode and press **OK**.

Delete auth mode

1. Click and authenticate with administrator privileges.
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

1. Click and authenticate with administrator privileges.
2. After pressing **AUTHENTICATION**, change the desired item in **Operation**.



- **Ambient Brightness**: Adjusts the intensity of the IR LED by detecting ambient brightness. Change settings according to the installation environment.
- **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.
- **Auth Timeout**: If authentication is not completed within the set time, authentication fails.
- **Server Matching**: When server matching is set, the device does not perform user authentication; BioStar X performs user authentication. It can be used when the device has too much user information or when the device is installed outside.

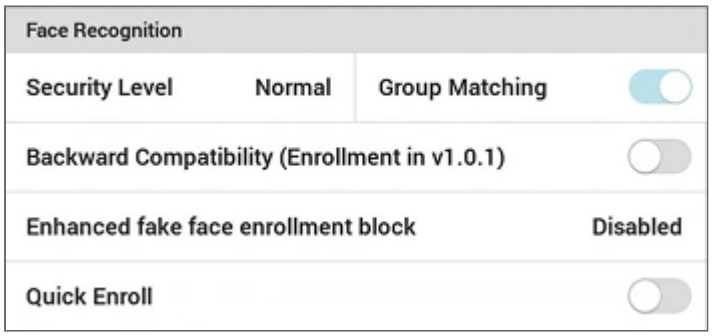
> **Info**
>
> – **Server Matching** can only use cards and IDs.
>
> – If you use **Server Matching**, you must enable server matching on both the device and BioStar X. For more information on BioStar X server matching settings, please refer to the BioStar X Administrator Guide.

- **Face Pose Variation**: Set the sensitivity for face position, angle, and distance when registering a face. Set high for precise face templates.
- **Enroll Timeout**: If the face is not enrolled within the set time, the face registration will be canceled.
- **Duplicate Check**: You can check for duplicate faces during face registration.

Facial recognition

You can change the configuration for facial authentication.

1. Click and authenticate with administrator privileges.
2. After pressing **AUTHENTICATION**, change the desired item in **Face Recognition**.



- **Security Level**: You can set the security level for 1:N: authentication.
- **Group Matching**: You can check whether group matching is used. Using group matching allows you to group multiple users' faces to increase authentication speed.
- **Backward Compatibility (Enrollment in v1.0.1)**: Enable this option if the firmware of the device that registers face templates is v1.0.1 or earlier.
- **Enhanced fake face enrollment block**: This can prevent user registration using spoofed faces such as photos. You can set the intensity from **Level 1** to **Level 3**, and as the level increases, the inspection intensity strengthens.
- **Quick Enroll**: You can set whether to use fast face registration. When fast face registration is enabled, the face registration process is set to one step, and when disabled, it is set to three steps.

> **Info**
>
> – **Group Matching** can be set in BioStar X.
>
> – If **Enhanced fake face enrollment block** is set to a high level, the registration of real faces may be rejected. If the registration fails, try again or lower the inspection intensity.
>
> – To register high-quality face templates, disable **Quick Enroll**.

Attendance Mode

You can set how to register T&A mode.

1. Click and authenticate with administrator privileges.
2. Click **AUTHENTICATION**, then change the desired item in **T&A Mode**.



- **T&A Mode**: Set how to use attendance mode.
- **T&A Code**: Register T&A events.
- **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.

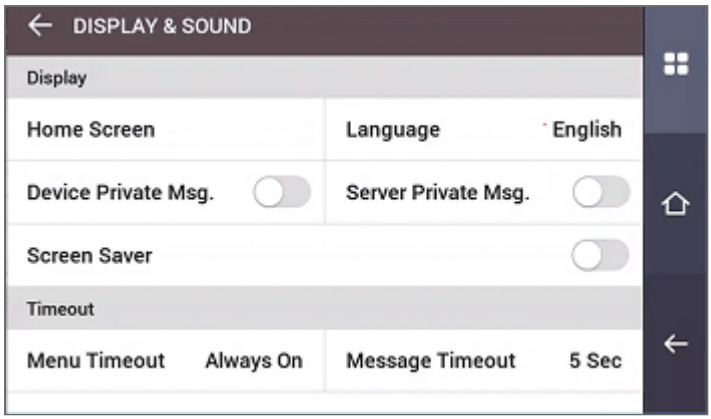
Settings

Provides instructions on how to set system and device configurations.

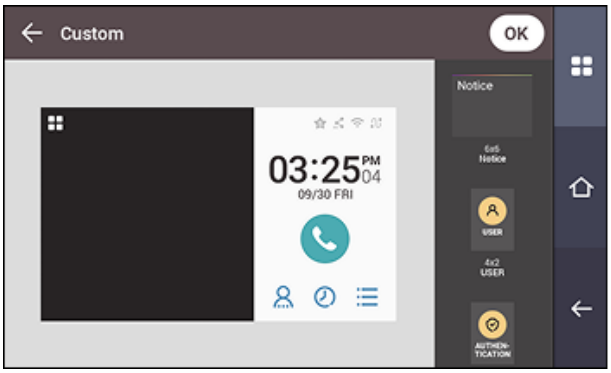
Display & Sound

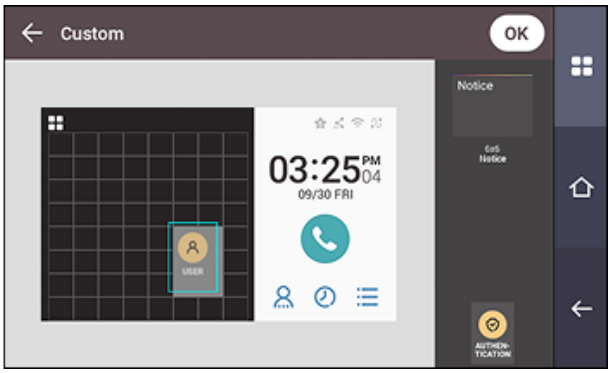
You can change the display and sound settings of the device.

1. Click and authenticate with administrator privileges.
2. Click **DISPLAY & SOUND**.
3. Change the desired item.



- **Home Screen**: You can choose items to display in the background of the home screen. Selecting the custom style allows you to modify the home screen directly. Long press the desired object and drag it to edit 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. It reduces unnecessary energy consumption by lowering the brightness of the screen 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.

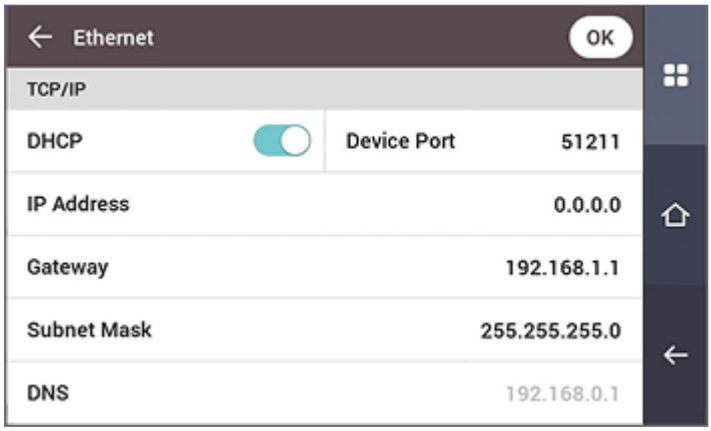
> **Info**
> For more information on the BioStar Device SDK, refer to the BioStar Device SDK page on the Suprema Knowledge Base.

Network

You can change the communication settings of devices such as Ethernet, server, and serial communication.

Ethernet

1. Click and authenticate with administrator privileges.
2. Select **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**.

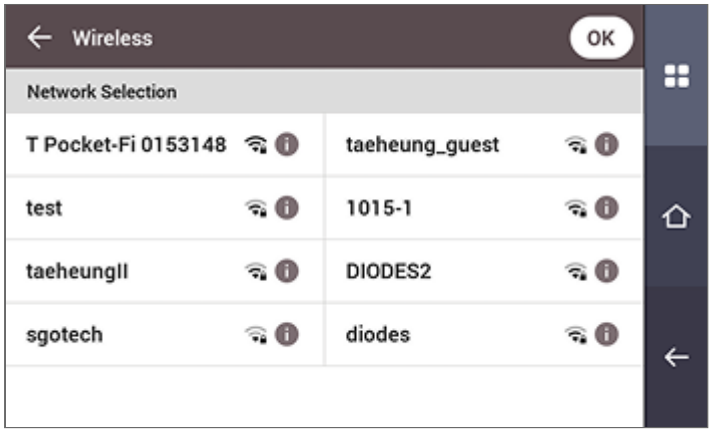
- **Device Port**: Set the device's port.
- **IP Address**: You can check the device's IP address. To modify, disable DHCP setting.
- **Gateway**: You can check the device's gateway. To modify, disable DHCP setting.
- **Subnet Mask**: You can check the device's subnet mask. To modify, disable DHCP setting.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

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

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

Wireless

1. Click and authenticate with administrator privileges.
2. Select **NETWORK** → **Wireless**.
3. The list of networks available to connect will be displayed.

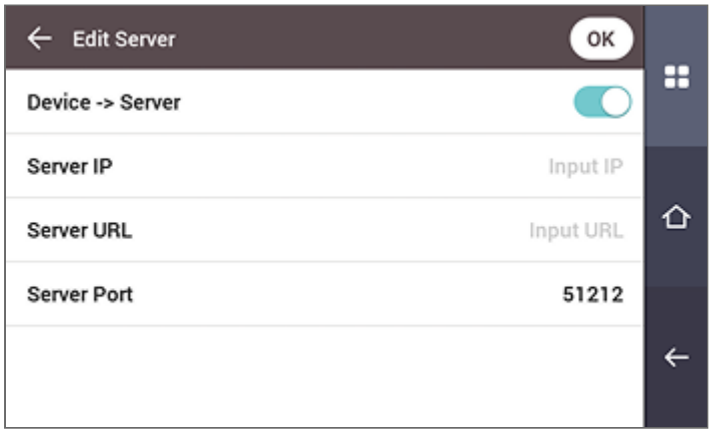


4. Select the network you wish to connect to and enter the password. When you press **OK**, the connection to the wireless network will be made.
5. Press for the wireless network you want to use, and turn off DHCP to modify **IP Address**, **Gateway**, and **Subnet Mask**.

> **Info**
> - **Wireless** is only available for the FS2-AWB 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. Click and authenticate with administrator privileges.
2. Select **NETWORK** → **Server**.
3. Change the desired item.

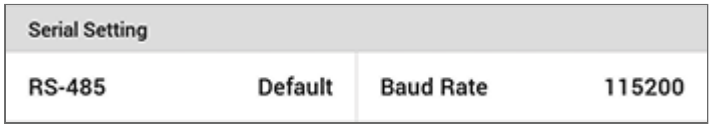


- **Device** → **Server**: You can send a connection signal from the device to a server with the input information directly. When **Device** → **Server** is enabled, the user can input **Server IP**, **Server URL**, and **Server Port**.
- **Server IP**: Enter the IP address of the PC on which BioStar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

Serial communication settings

1. Click and authenticate with administrator privileges.
2. Press **NETWORK** and change the desired item in **Serial Setting**.



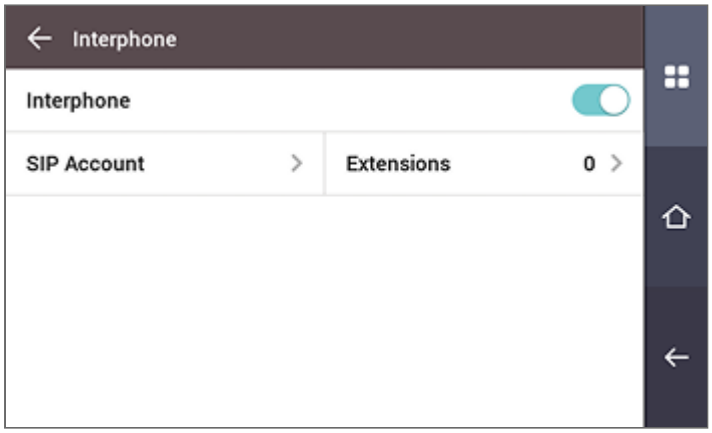
- **RS-485**: Select the RS-485 mode.
- **Baud Rate**: Select the desired baud rate.

Device

Intercom

You can configure the account and extensions of the SIP intercom.

1. Click and authenticate with administrator privileges.
2. Click **DEVICE** → **Interphone**.



- **Interphone**: You can set whether to enable the intercom. 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.
- **Extensions**: Add, delete, or edit extension numbers.

Relay

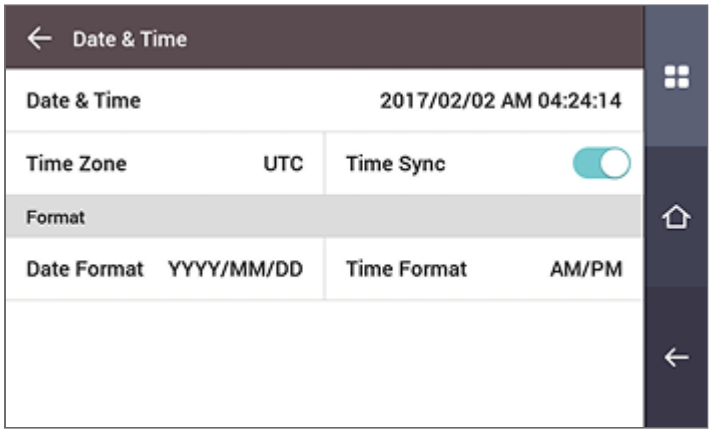
You can set the input ports of **Open Time** and **Exit Button** on the device.

1. Click and authenticate with administrator privileges.
2. Click **DEVICE** → **Relay**.
   - **Relay**: You can set whether relay is enabled or not. Enabling relay settings will allow you to configure **Open Time** and **Exit Button**.
   - **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 connected to the exit button.
   - **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. Click and authenticate with administrator privileges.
2. Click **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. Click and authenticate with administrator privileges.
2. Click **DEVICE** → **Daylight Saving Time**, then press to add daylight savings time.
3. Change the desired item.
   - **Name**: You can view the name of the daylight savings 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. Click and authenticate with administrator privileges.
2. Select **DEVICE** → **Device Info**. You can view the information for **Model Name**, **Device ID**, **Serial No.**, **HW**, **FW**, **Kernel**, **MAC**, and **WiFi MAC**.

> **Info**
> The **WiFi MAC** item is only available on the FS2-AWB model.

Memory information

View the status of memory usage.

1. Click and authenticate with administrator privileges.
2. Select **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. Click and authenticate with administrator privileges.
2. Select **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.

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. Click and authenticate with administrator privileges.
2. Select **DEVICE**.
3. Activate **Secure Tamper** to delete data of all registered users, all logs, and secure keys when a temper event occurs.

Restart device

The user can restart the device.

1. Click and authenticate with administrator privileges.
2. Select **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.

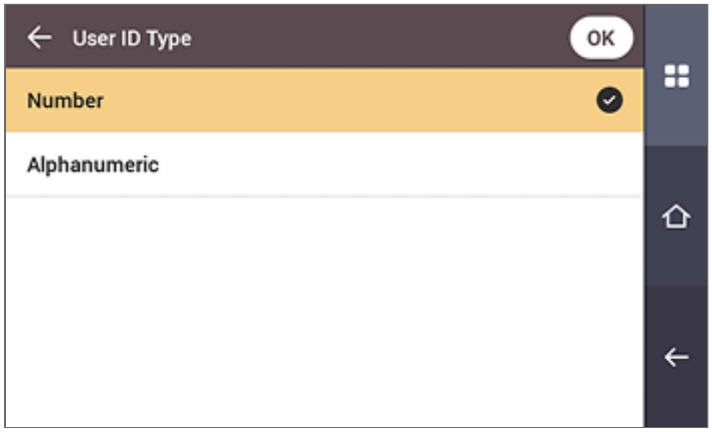
1. Click and authenticate with administrator privileges.
2. Select **DEVICE** → **Restore Default**.
   - **All settings**: Initializes all settings stored on the device. To initialize all device settings, press **OK** → **OK**. Press **Cancel** to return to the previous screen.
   - **Keep Network Settings**: Initializes all settings except for network settings. To initialize all settings except network settings, press **OK** → **OK**. 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. Click and authenticate with administrator privileges.
2. Select **DEVICE** → **User ID Type**.

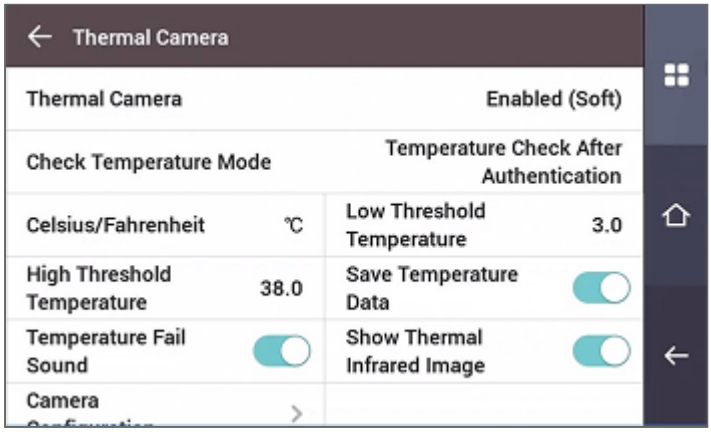


   - **Number**: You can enter a user ID with numbers only.
   - **Alphanumeric**: You can enter a user ID using alphanumeric characters and certain symbols _ -.
3. After changing to the desired item, press **OK**.

Thermal camera

The device can measure the temperature of users passing through the entrance by linking with the thermal camera and restrict access for users exceeding the reference temperature.

1. Click and authenticate with administrator privileges.
2. Select **DEVICE** → **Thermal Camera**.
3. Change the desired item.



- **Thermal Camera**: You can set whether to use the thermal camera. When set to **Enabled (Hard)**, users exceeding the reference temperature will be denied authentication, and the exceeding temperature event will be logged. When set to **Enabled (Soft)**, users exceeding the reference temperature can authenticate, but the exceeding temperature event will be logged.
- **Check Temperature Mode**: You can set the temperature check mode according to purpose.
  - **Temperature Check After Authentication**: Measures user's temperature after authentication is performed.
  - **Temperature Check Before Authentication**: Measures user's temperature and then performs authentication. In this mode, users exceeding the reference temperature cannot authenticate.
  - **Check Temperature Only**: The device can only be used for measuring temperature. In this mode, all users below the reference temperature can enter, regardless of authentication.
- **Celsius/Fahrenheit**: You can set the temperature display unit.
- **Low Threshold Temperature**: You can set the minimum reference temperature to restrict access. Users with a surface temperature lower than the minimum reference temperature will be denied authentication.
  The minimum reference temperature can be set in the range of 1 °C to 45 °C, and must be higher than the maximum reference temperature.
- **High Threshold Temperature**: You can set the maximum reference temperature to restrict access. Users with a surface temperature higher than the maximum reference temperature will be denied authentication.
  The maximum reference temperature can be set in the range of 1 °C to 45 °C, and must be lower than the minimum reference temperature.
- **Save Temperature Data**: You can set whether to save the user's temperature log. Using this option, both the success of authentication and the user's temperature value will be saved in the log; if not used, only the success of authentication will be logged.
- **Show Thermal Infrared Image**: You can set whether to display the thermal image on the device screen.
- **Camera Configuration**: You can set detailed options for accurate measurements for the camera.
  –

Distance(cm): Set the distance between the user and the thermal camera.

- **Emissivity**: Set the infrared emissivity.
- **ROI X(%)**, **ROI Y(%)**, **ROI Width(%)**, **ROI Height(%)**: If additional lighting is installed nearby, the thermal camera can be set to measure the user's temperature instead of that lighting. Adjust the position and size of the ROI (Region of Interest) to manually set the area where the thermal camera will measure the temperature.
- **Skin Temperature Compensation**: You can set the thermal camera to automatically calibrate the temperature based on the usage environment and ambient temperature.
- **Skin Temperature Correction**: You can adjust the temperature readings to a fixed value based on the usage environment. For example, in environments where the temperature is always measured as 0.1 °C higher, set the temperature calibration value to -0.1.

Info

- For optimal performance, it is recommended to use the default values for the sub-options of the camera settings. The default values of each option are as follows:
  - **Distance(cm)**: 100
  - **Emissivity**: 0.98
  - **ROI X(%)**: 47
  - **ROI Y(%)**: 45
  - **ROI Width(%)**: 15
  - **ROI Height(%)**: 10
- The thermal camera supports TCM10-FS2.

Event Logs

Describes how to view event logs generated by the device.

Search event logs

Set conditions to search logs.

1. Click and authenticate with administrator privileges.
2. Select **EVENT LOG**. All event logs appear.
3. Press to search a specific log and change the condition.

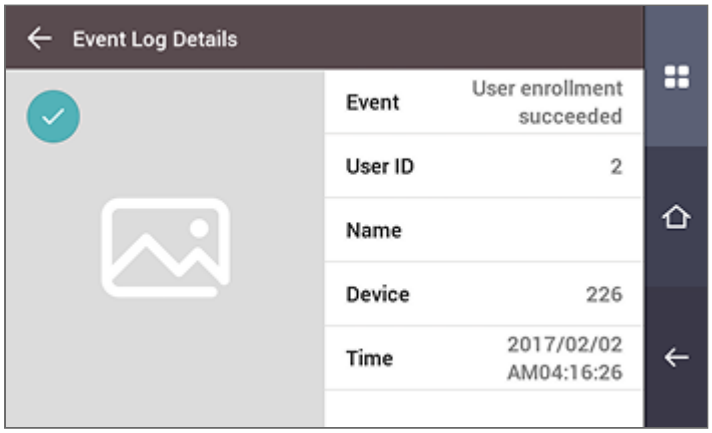


4. Set the search criteria and click **OK** to display logs that match the criteria.

View event log details

You can check the details of the logs.

1. Click and authenticate with administrator privileges.
2. Select **EVENT LOG**. All event logs appear.
3. Click the log to check the details.



Delete all logs

You can delete all saved logs.

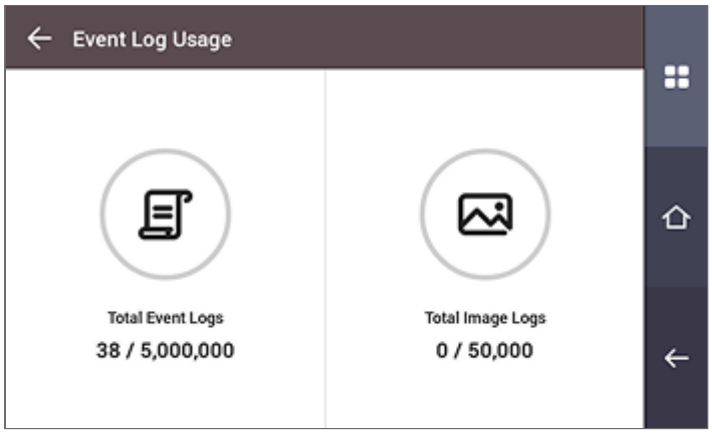
1. Click and authenticate with administrator privileges.
2. Select **EVENT LOG**. All event logs appear.
3. To delete all logs, select and click **OK**. Press **Cancel** to return to the previous screen.

View log usage

You can check the status of log usage.

1. Click and authenticate with administrator privileges.

2. Click **EVENT LOG** → . Check the device's event log and image log usage.



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 face 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. The thermal camera fails to measure temperature.

- Check if the thermal camera is properly connected to the terminal.
- Measure the temperature again without covering your forehead. If the problem persists, contact the installation company.

Q. The thermal camera measures lower temperature than actual temperature.

- If a user measures the temperature after being exposed to cold temperatures for a long time, the temperature may be measured lower than the actual temperature. Wait for 1 to 2 minutes indoors and try again. 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.

Product Specifications

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

Credentials

Biometric	**Face** • **Live Face Detection:Supported**	
RF Card	**FS2-D**	**125kHz EM & 13.56MHz MIFARE, MIFARE Plus, DESFire, DESFire EV1/EV2/EV3[1], FeliCa**
	FS2-AWB	**125kHz EM, HID Prox & 13.56MHz MIFARE, MIFARE Plus, DESFire, DESFire EV1/EV2/EV3[1], FeliCa, iCLASS SE/SR/Seos**
RF Read Range[2]	**EM/HID Prox/MIFARE/DESFire/HID iCLASS/FeliCa: 30 mm**	
Mobile	**FS2-D**	**NFC**
	FS2-AWB	**NFC, BLE**

General

CPU	**1.4 GHz Quad Core**
Memory	**8 GB Flash + 1 GB RAM**
Crypto Chip	**Supported**
Display	**4" TFT color touch**
Display Resolution	**800 x 480 pixels**
Sound	**24 bit/Voice DSP (echo cancel)**
Operating Temperature	**-20 °C ~ 50 °C**

Storage Temperature	**-40 °C ~ 70 °C**
Operating Humidity	**0 % ~ 80 %, non-condensing**
Storage Humidity	**0 % ~ 90 %, non-condensing**
Camera Type	**CMOS**
Camera Resolution	**720 x 480 pixels**
Camera Angle	• **Visual Lens: Diagonal 92.7°** • **IR Lens: Diagonal 58°**
Authentication	**CE, UKCA, KC, FCC, IC, RCM, BIS, SIG, RoHS, REACH, WEEE**

Capacity

Max. User	**30,000**[3)]
Max. Credentials (1:N)	**Face: 4,000**
Max. Credentials (1:1)	• **Face: 30,000** • **Card: 30,000** • **PIN: 30,000**
Max. Text logs	**5,000,000**
Max. Image logs	**50,000**

Interface

Ethernet	**Supported (10/100/1000 Mbps, auto MDI/MDI-X)**	
Wi-Fi	**FS2-D**	**Not supported**
	FS2-AWB	**Supported (Built-in, IEEE 802.11 b/g)**

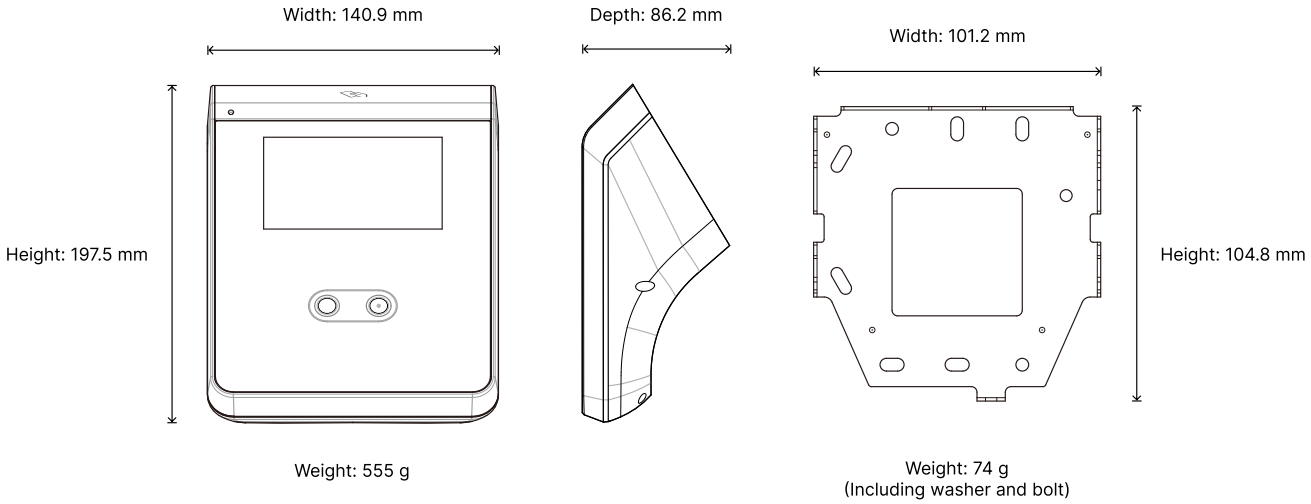
Network Protocol	**TCP, UDP**
RS-485	**1 ch Master / Slave (Selectable)**
RS-485 Communication Protocol	**OSDP V2 compliant**
Wiegand	**1 ch Input, 1 ch Output**
Input	**2 ch Inputs**
Relay	**1 relay**
Intercom	**Supported**
USB	**USB 2.0 (Host)**
Tamper	**Supported**

Electrical

Power	**24 Vdc**	**Current: Max. 1.2 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



1) DESFire EV2/EV3 cards are backward compatible with DESFire EV1 cards, supporting CSN and smart card features, including those of the DESFire EV1 card.

2) RF read range will vary depending on installation environment.

3) Based on users enrolled without credentials.

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:): 10,000
  - Max. Fingerprint Credentials (1:1:): 100,000

Regulatory Information

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

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: FS2-AWB 0.049 mW
- Bluetooth frequency: FS2-AWB 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 3.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.
- 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 AOSP included in this product follows the Apache License 2.0. For more information about Apache License 2.0, please see the Apache License.
- The source modified based on Linux kernel 3.x and AOSP source code 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.