X-Station 2

USER GUIDE

Version 1.11

English
EN 102.00.XS2

suprema
SECURITY & BIOMETRICS

CONTENTS

Safety Instructions 4

Compliance Information 4

Getting Started 8

Components 8

Name and function of each part 9

Notes on QR/Barcode and Device License 18

Installation 20

Fixing the bracket and the product 20

Power supply connection 23

Network Connection 24

Input connection 25

Relay Connection 26

Connecting as a Standalone 29

Connecting to Secure I/O 2 30

Wiegand Connection 31

How to Use 32

Admin Menu 32

User 32

Authentication 36

Settings 43

Event Logs 56

Troubleshooting 59

Check items before reporting a malfunction 59

Product Specifications 61

Credentials 61

General 61

Capacity 62

Interface 63

Electrical 63

Dimensions and Weight 64

Regulatory Information 67

FCC Compliance Information 67

IC information 68

EU Declaration of Conformity (CE) 68

Appendices 69

Disclaimers 69

Copyright Notice 70

Open Source License 70

Safety Instructions

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

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

Compliance Information

Warning

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

Caution

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

Info

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

Note

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

⚠ Warning

Install

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

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

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

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

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

- May cause fire or electric shock.

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

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

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

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

- May cause fire or electric shock due to overheating.

Do not install in damp places.

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

Do not install in places with electromagnetic interference.

- May cause electric shock or product damage.

Usage

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

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

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

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

Do not bend or break the power cord excessively.

- May cause fire or electric shock.

⚠ Caution

Install

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

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

- Devices may malfunction.

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

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

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

Do not leave power cables in passageways.

- May cause bodily injury or product damage.

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

- The device may malfunction.

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

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

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

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

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

- Devices may malfunction.

Do not connect the power supply and PoE power together.

- Devices may malfunction.

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

- Decreased waterproof and dustproof performance may cause malfunction.

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.

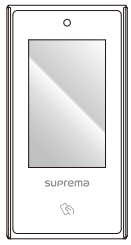
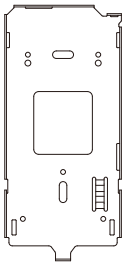
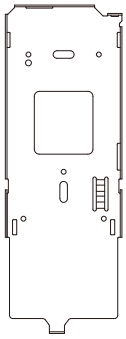
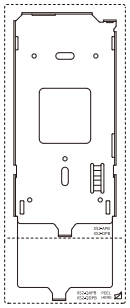
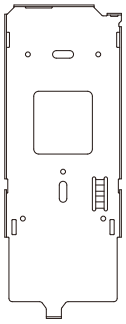
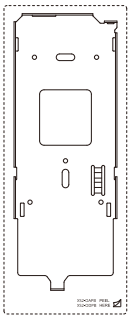
- The device may malfunction.

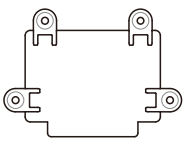
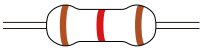
> **RTC Battery**
>
> Replacing with unauthorized or incorrect types of batteries may pose a risk of explosion. Dispose of batteries according to local or international waste regulations.

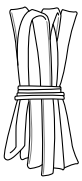
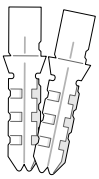
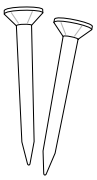
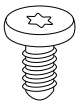
Getting Started

Provides initial procedures for getting started with the device.

Components

				
X-Station 2 (XS2-DPB, XS2-APB)	Wall Bracket (XS2-DPB, XS2-APB)	X-Station 2 (XS2-QDPB, XS2-QAPB)	Wall Bracket (XS2-QDPB, XS2-QAPB)	Drilling Template (XS2-DPB, XS2-APB, XS2-QDPB, XS2-QAPB)
				
X-Station 2 (XS2-ODPB, XS2-OAPB)	Wall Bracket (XS2-ODPB, XS2-OAPB)	Drilling Template (XS2-ODPB, XS2-OAPB)	Quick Guide	Open Source Software Guide

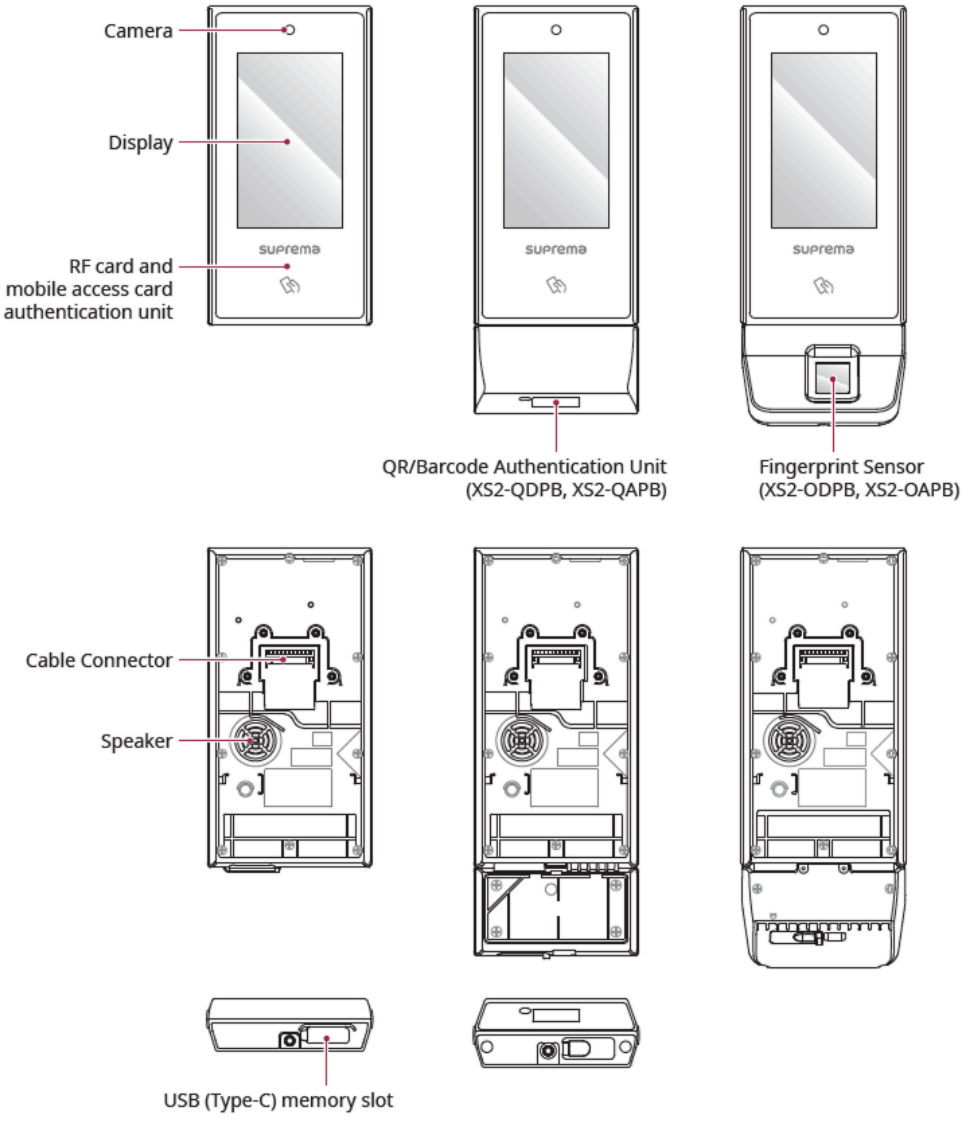
			
Connection Cables	Cable Cover	120 Ω Resistor	Diode

			
Shrink Tube	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.

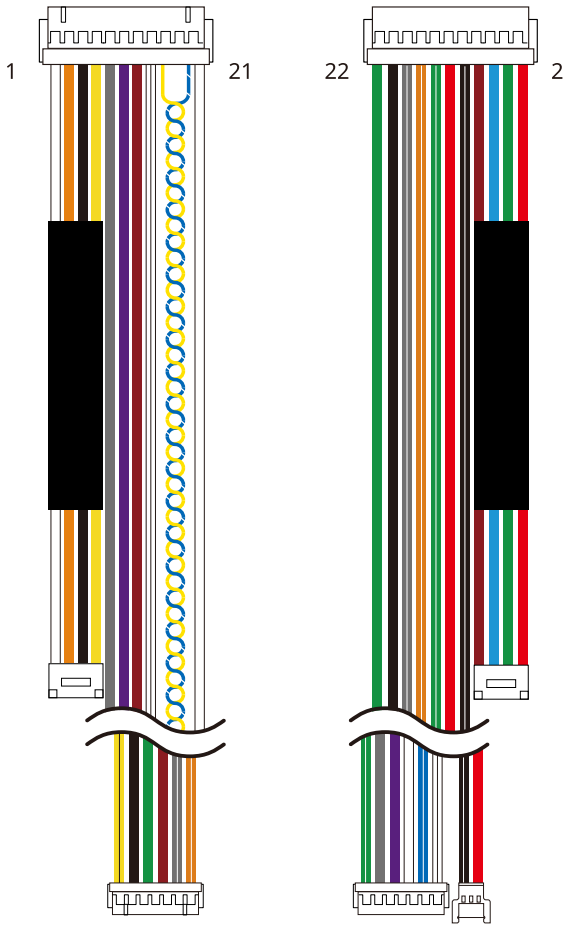
Name and function of each part



- **Camera**: You can register your photo or leave an image log.
- **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.
- **QR/Barcode Recognition Unit**: XS2-QDPB, XS2-QAPB Scans QR/Barcode credentials for access.
- **Fingerprint Recognition Unit**: XS2-ODPB, XS2-OAPB The part that recognizes the fingerprint for access.
- **Cable Connector**: Connects the cable.

  Power / RS-485 / Ethernet + PoE / Relay / Wiegand Input/Output / Input
- **Speaker**: Delivers sound.
- **USB (Type-C) Memory Slot**: Connects the USB memory.

Cables and connectors



Cable	Pin	Name	Color
RJ-45 (Ethernet + PoE)	1	ENET TXP	White
	3	ENET TXN	Orange
	5	ENET RXP	Black
	7	ENET RXN	Yellow
Input	9	INPUT GND	Gray
	11	INPUT0	Purple
	13	INPUT1	Brown
RS-485	15	485 GND	White (Black Stripe)
	17	485 TRXN	Yellow (Black Stripe)
	19	485 TRXP	Blue (White Stripe)
Wiegand	21	WG D1	White
	22	WG D0	Green
	20	WG GND	Black

Cable	Pin	Name	Color
Relay	18	RLY NO	Gray (White Stripe)
	16	RLY NC	Orange (White Stripe)
	14	RLY COM	Green (White Stripe)
Power	12	PWR +VDC	Red
	10	PWR GND	Black (White Stripe)
RJ-45 (Ethernet + PoE)	8	VB2	Brown
	6	VB2	Blue
	4	VB1	Green
	2	VB1	Red

Set Up Master Administrator CE model only

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

Info

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

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

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

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

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

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

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

Behavior Logic During Firmware Upgrade

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

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

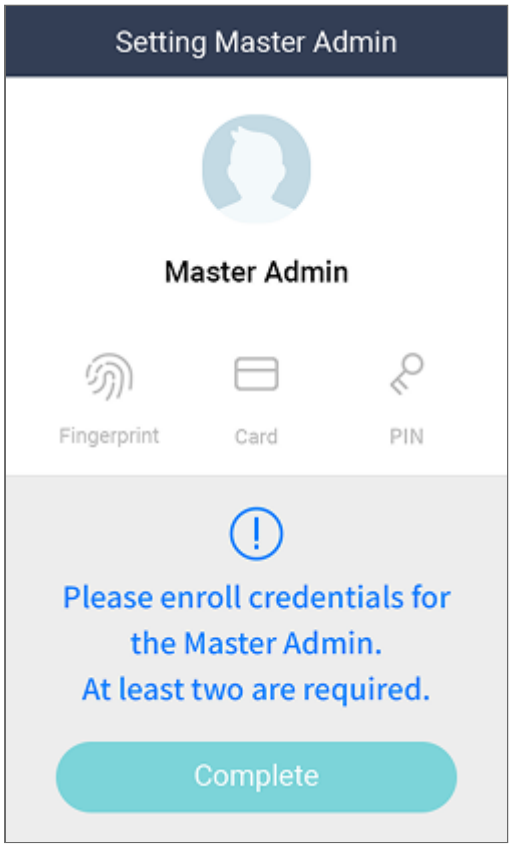
Enroll master administrator on a new device

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

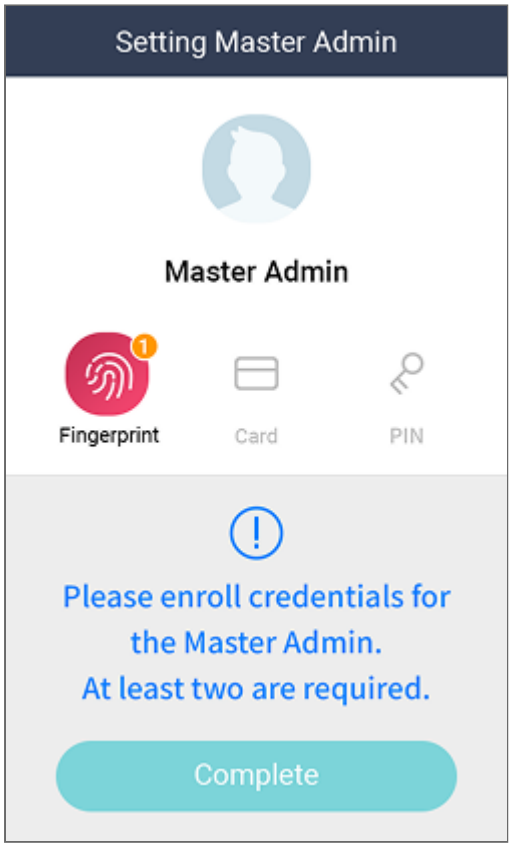
Info

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

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



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



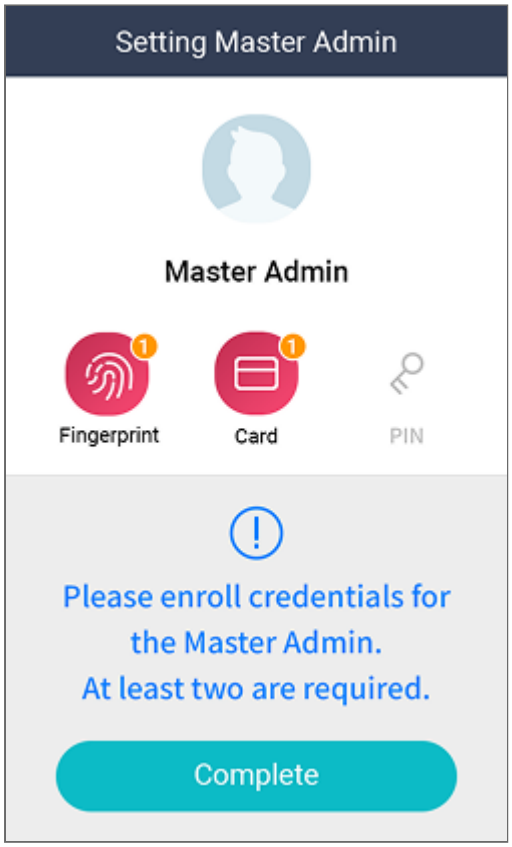
The credentials that can be enrolled for **Master Admin** are as follows.

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

Enrollment conditions

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

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



Additional Information

- **When enrolling PIN through BioStar software**

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

  – BioStar 2 v2.9.11 or later

  – BioStar X v1.0.0 to v1.0.2

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

- **Manual Device Hash Key Change**

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

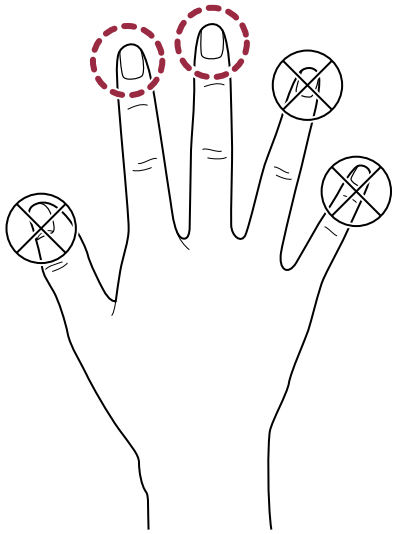
- **RS-485 Biometric Image Transmission Restriction**

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

Correct fingerprint input method XS2-ODPB, XS2-OAPB

In order to improve the fingerprint authentication rate, enroll the fingerprint correctly. This product can authenticate fingerprints even if the user's fingerprint input angle and position change. If you enroll the fingerprint with attention to the following matters, the authentication rate can be improved.

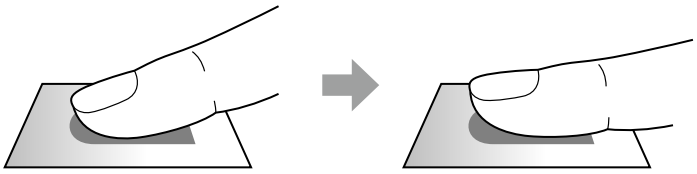
Selecting a finger for fingerprint input



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

Fingerprint enroll method

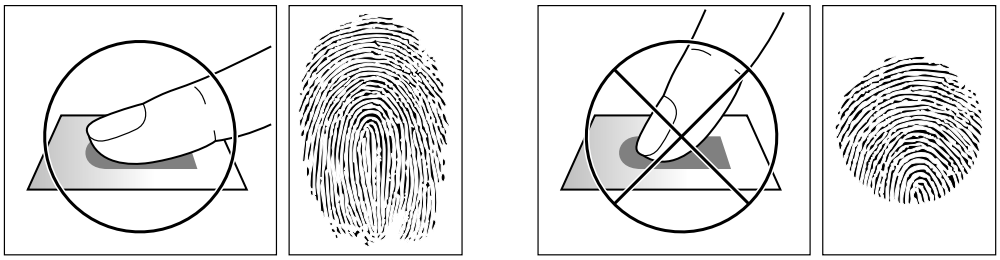
1. When the screen displays "Please input your fingerprint," place the finger you want to enroll on the fingerprint recognition unit and gently press it so that the fingerprint is authenticated well.



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

Cautions for fingerprint enrollment

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



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

If fingerprint authentication does not work well

This product can authenticate fingerprints regardless of seasonal changes or changes in the condition of the fingers. However, the authentication rate may vary according to the external environment or fingerprint input method. If the fingerprint authentication cannot be done smoothly, it is recommended to take the following measures.

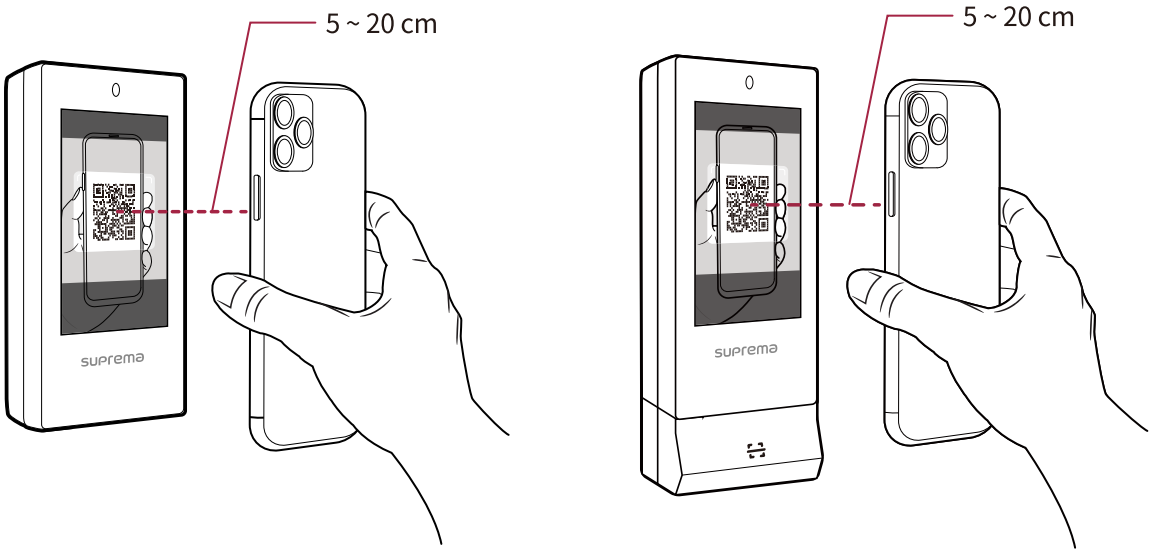
- If the finger is smeared with water or sweat, dry off the finger and then scan the finger.
- If the finger is too dry, blow your breath on the fingertips and then scan the finger.
- If the finger has a cut, enroll the fingerprint of another finger.
- Since the initially enrolled fingerprint is often not input correctly, please re-enroll the fingerprint according to the Cautions for fingerprint enrollment.

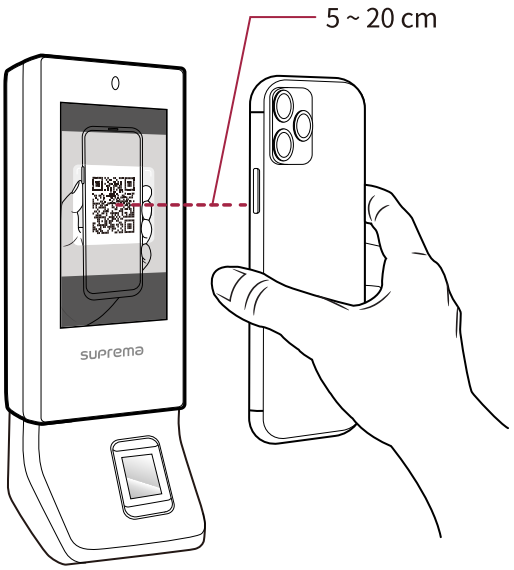
Notes on QR/Barcode and Device License

Correct QR/Barcode Authentication Method

You can issue a QR/barcode to the user for use as a means of authentication. To improve recognition rate, scan the QR/barcode correctly according to the guidance on the screen.

Camera

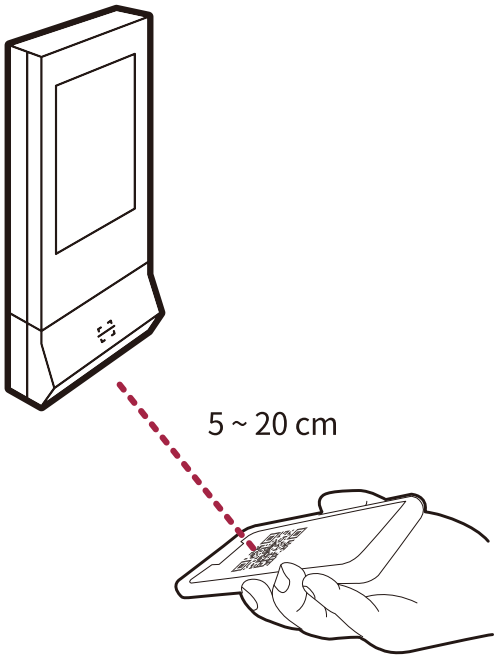




- Keep the distance between the device's camera and the QR/barcode at 5-20 cm.
- Position the QR/barcode so that it is centered in the device's scanning screen.

- If authenticating with a QR/barcode downloaded to a mobile device, adjust the brightness of the mobile device to ensure the screen is clearly visible.
- Failure to follow the instructions on the screen may result in slow recognition or failure of the QR/barcode.

QR/Barcode Scanner XS2-QDPB, XS2-QAPB



- Keep the distance between the device's QR/barcode recognition unit and the QR/barcode at 5-20 cm.
- Ensure the device's QR/barcode recognition unit is horizontal to the QR/barcode being scanned, and position the guide beam in the center of the QR/barcode.
- If authenticating with a QR/barcode downloaded to a mobile device, adjust the brightness of the mobile device to ensure the screen is clearly visible.
- Failure to follow the instructions on the screen may result in slow recognition or failure of the QR/barcode.

Notes for device license

- Using additional QR/Barcode authentication methods 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.

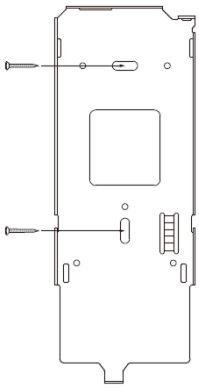
Installation

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

Fixing the bracket and the product

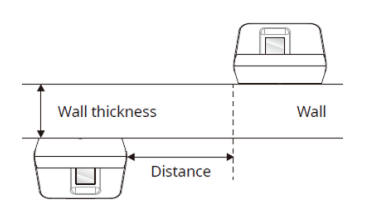
> **Info**
> This document explains the installation method based on the XS2-ODPB and XS2-OAPB form factor. Install the XS2-DPB, XS2-APB, XS2-QDPB, and XS2-QAPB models in the same way.

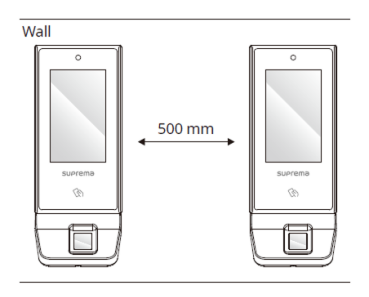
1. Determine the correct position to install the bracket using the provided drilling template. Secure the bracket tightly using the fixing screws at the location where the product will be mounted.



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.

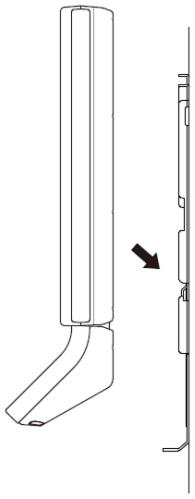




Wall thickness	Distance
100 mm	500 mm
120 mm	400 mm
150 mm	300 mm

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

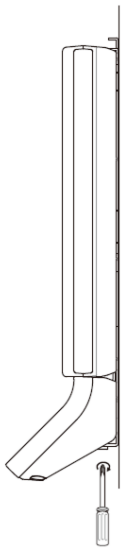
2. After attaching the cable cover, turn the four screws fitted in the cover to fasten it securely and mount the product on the fixed bracket.



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).

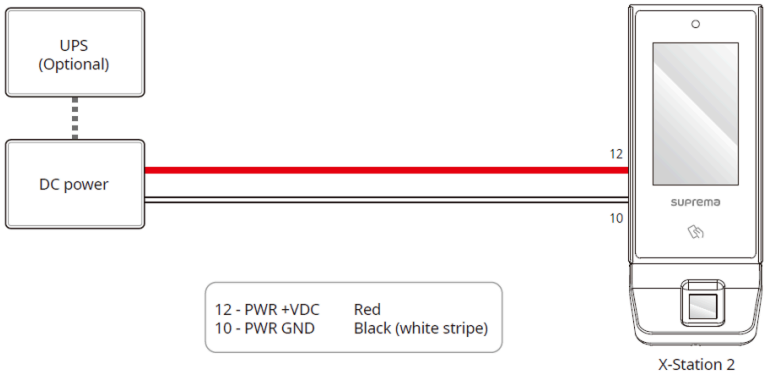
3. Rotate the fixing screws to assemble the product with the bracket.



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.

Power supply connection



Caution

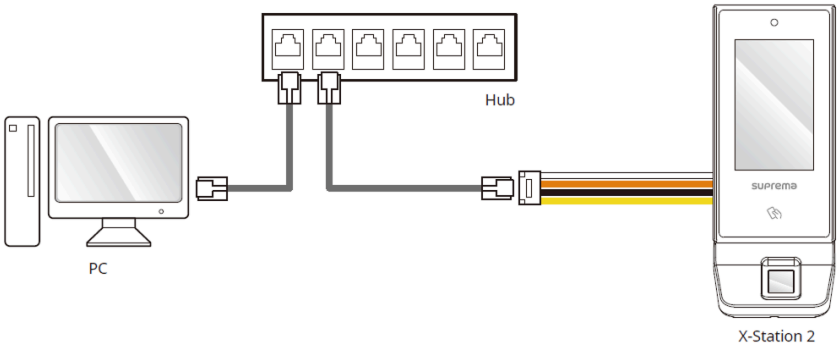
- DO NOT connect the device to the DC power supply (or adapter) and PoE power supply at the same time.
- Use the IEC/EN 62368-1 approved power adapter that supports higher power consumption than the product. If you wish to connect and use another device to the power supply adapter, you should use an 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.
- 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

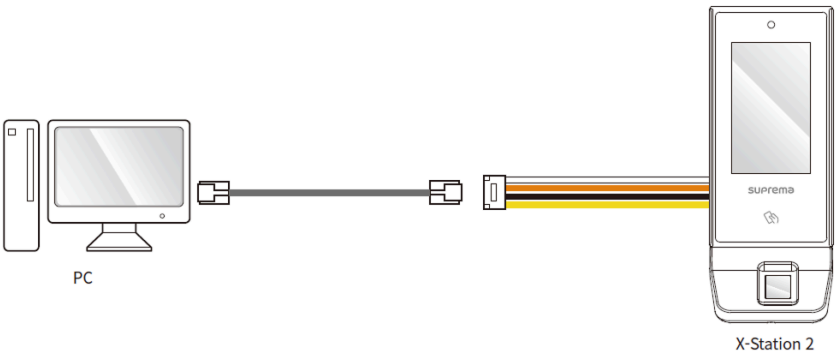
LAN connection (connecting to a hub)

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.



Network ports and services

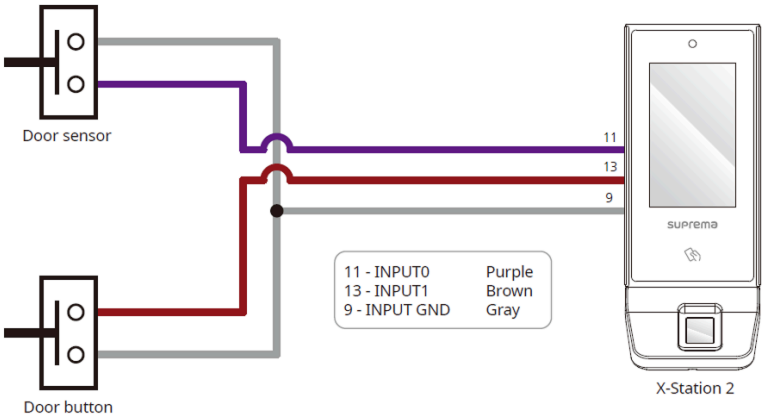
This device uses the following ports for network communication and stable service operation.

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.

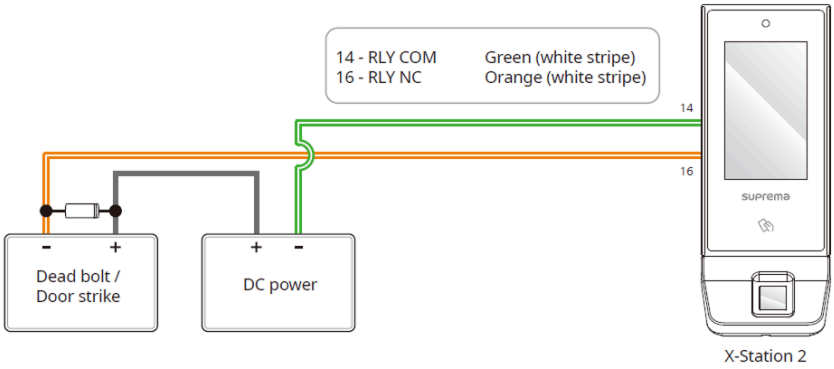
Input connection



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

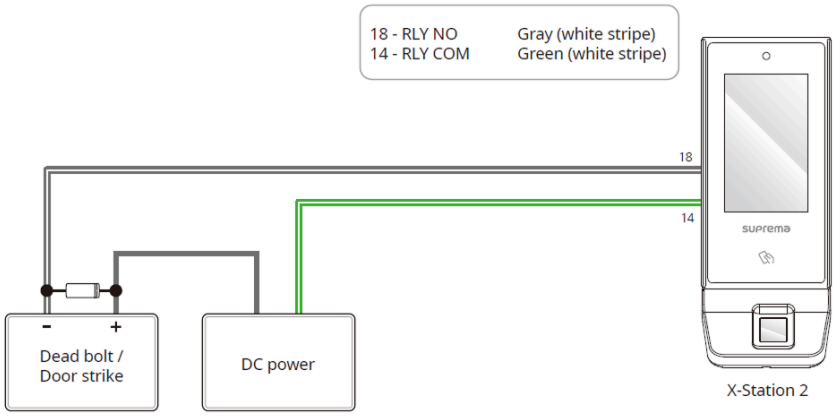
- Install a diode at both sides of the door lock wire as shown in the figure to protect the relay from the reverse current, which occurs when the door lock operates.
- Use a separate power supply for the product and the door lock.
- Suprema's standalone intelligent readers contain internal relays that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



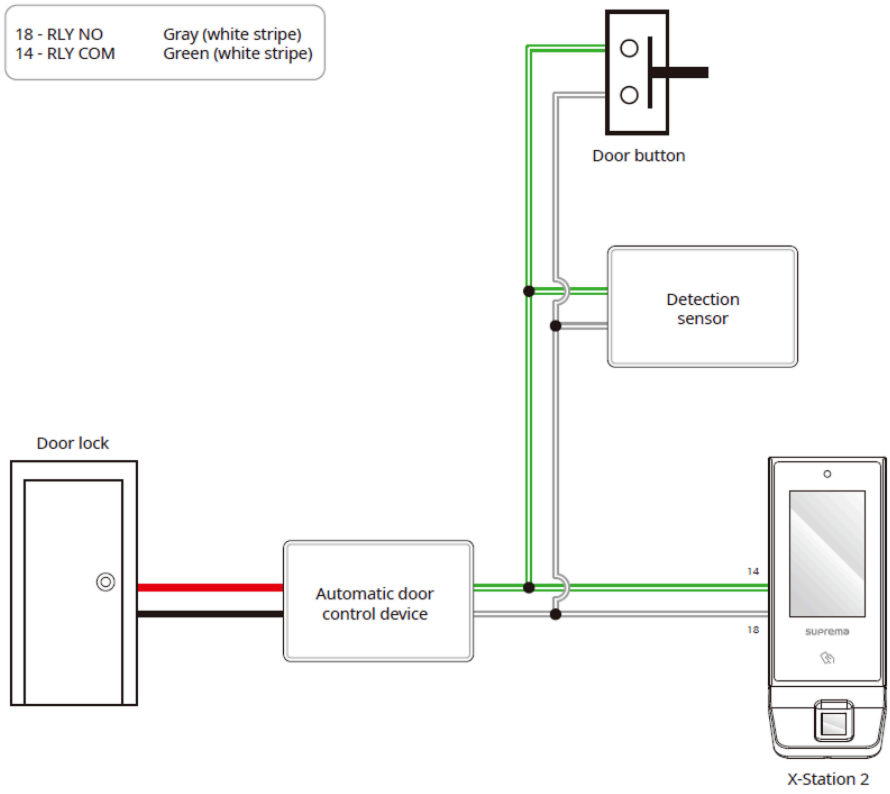
Caution

- 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

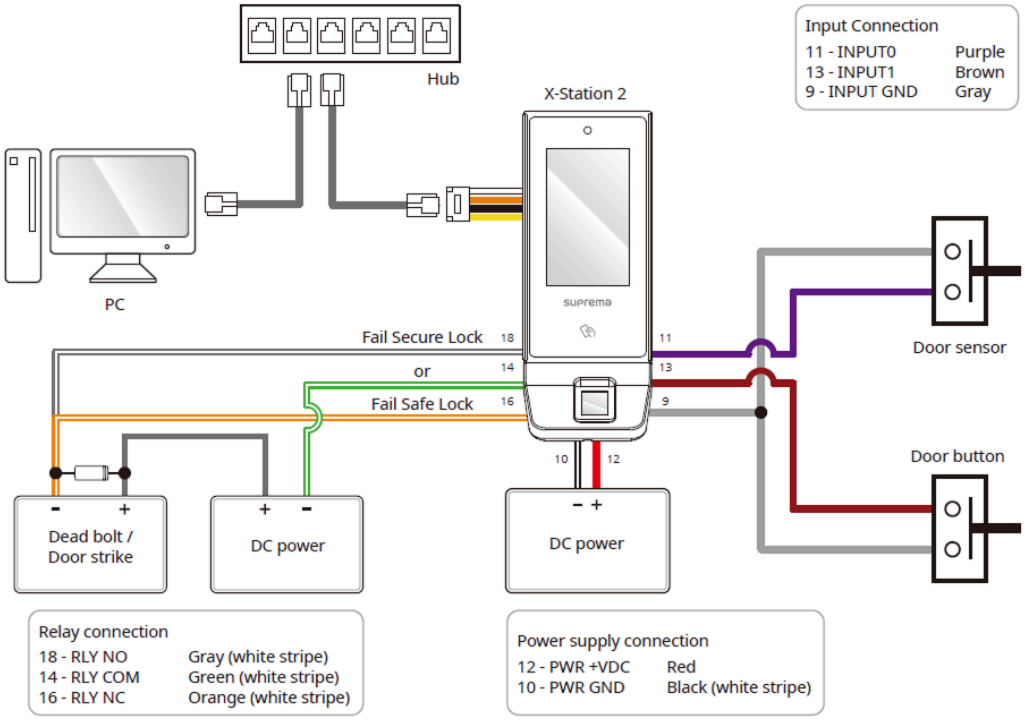
Take caution of the installation direction of the diode. Install the diode close to the door lock.

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.

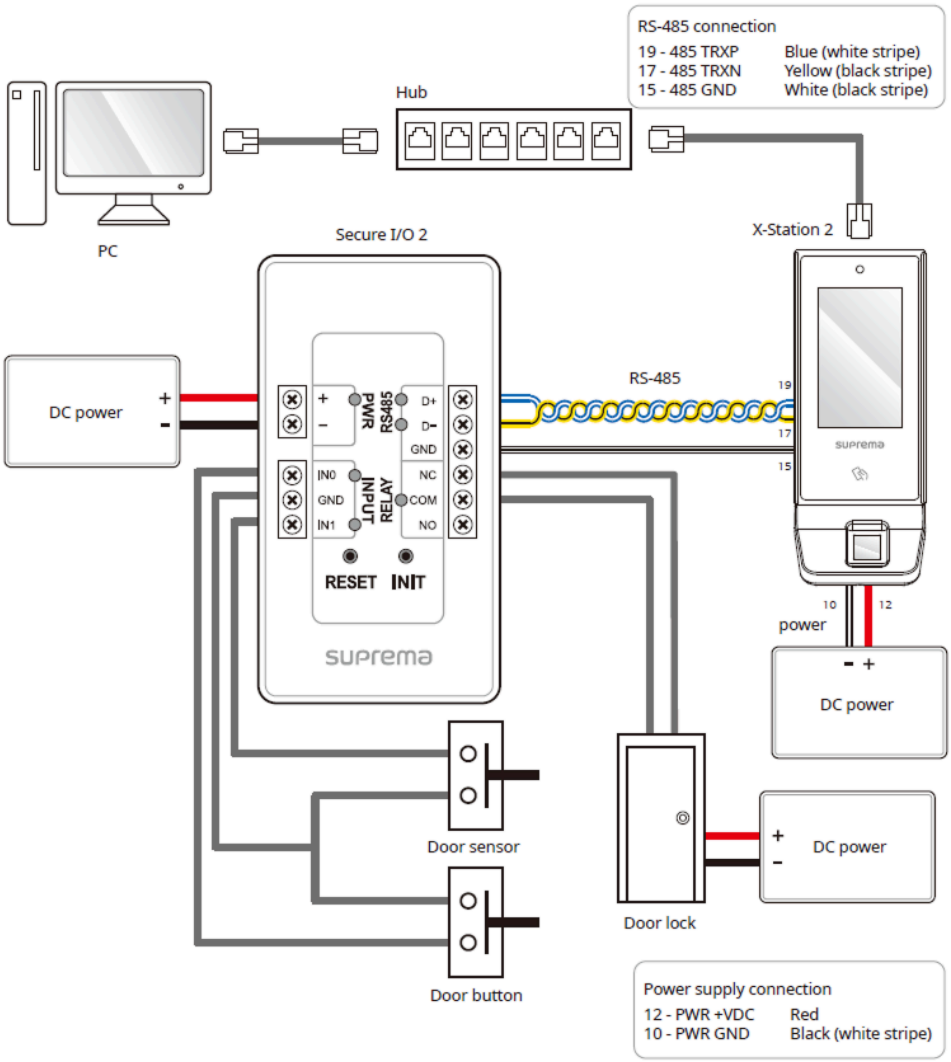
Info

- 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.
- 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.

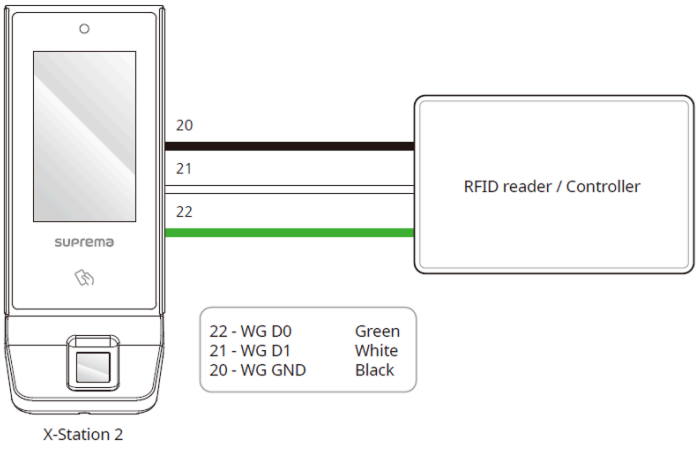


Info

- 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.
- 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

Use as a Wiegand input or output device.



How to Use

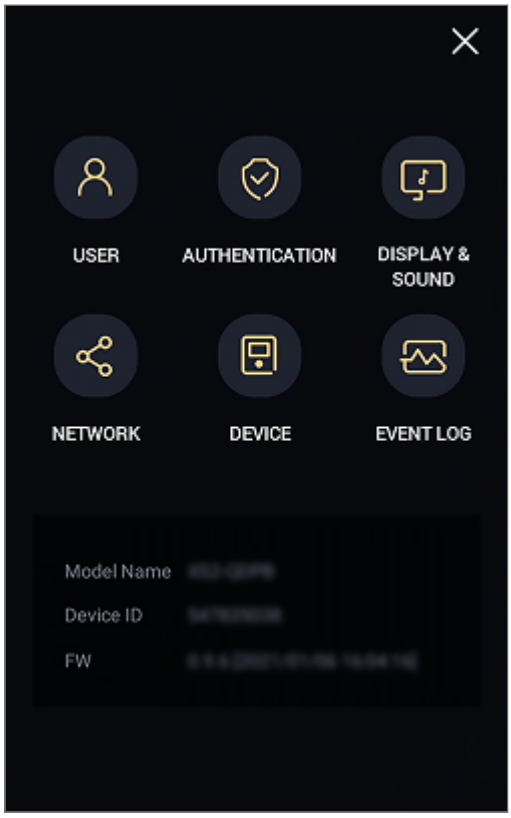
Provides guidance on how to use the main features of the device effectively.

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.

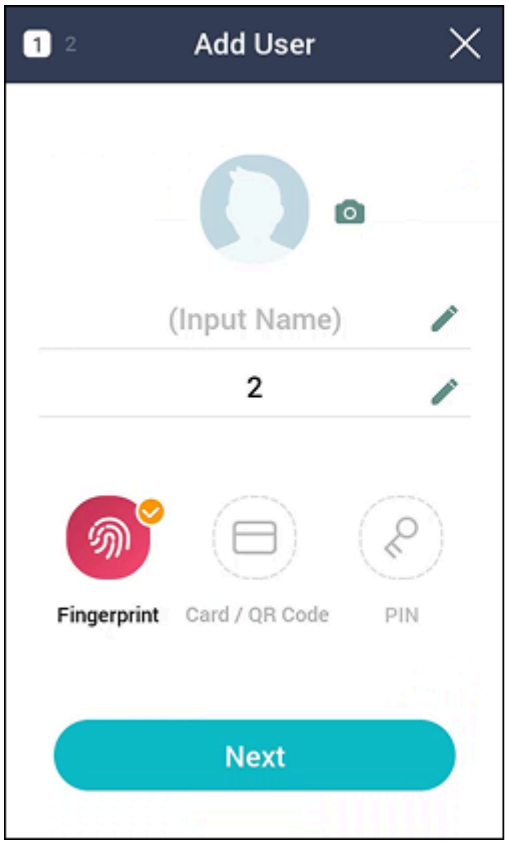
User

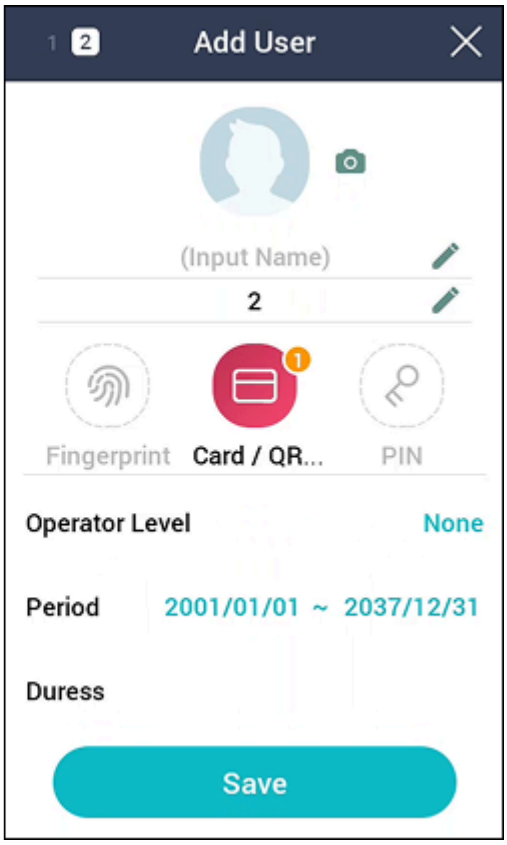
Describes how to register, edit, delete, and manage users.

Registering user information

You can register user information that includes biometric authentication data.

1. Click and authenticate with administrator privileges.
2. Select **USER** → and set the desired items. User usage information appears.





- : 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.
- **Fingerprint**: XS2-ODPB, XS2-OAPB You can enroll a fingerprint for user authentication. Press **Fingerprint** → **Next** and follow the on-screen instructions to enroll a fingerprint. To enroll more fingerprints, press . For more information on fingerprint registration, refer to User fingerprint enrollment.
- **Card / QR Code**: You can enroll a card for user authentication. Press **Card / QR Code** → **Next**, then scan the card to assign it to the user at the RF card authentication unit. To enroll more cards, click .
- **PIN**: You can enter the PIN you want to use. Press **PIN** → **Next** and enter the PIN you want to use. For confirmation, enter the PIN once more and then press **OK**. To prevent leaks, input a PIN of 4 to 16 digits.

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

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

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

- **Period**: You can set the duration for using the user account.
- **Duress**: XS2-ODPB, XS2-OAPB Select to enroll a duress fingerprint. If you are coerced by someone or need to open the door forcefully, authenticating with this fingerprint can send an alarm signal to BioStar X.
- **Private Auth Mode**: You can change the authentication method for each user.

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

User fingerprint enrollment XS2-ODPB, XS2-OAPB

1. Click and authenticate with administrator privileges.
2. Click **USER** → .
3. Select **Fingerprint** → **Next**.
4. After scanning the fingerprint of the finger to be enrolled, scan the same finger's fingerprint again.

> **Info**
> - Fingerprint enrollment is available only for XS2-ODPB and XS2-OAPB products.
> - Place the finger deep enough to contact with the sensor completely.
> - Place the center of the fingerprint in the center of the sensor.
> - If a finger has a cut or the fingerprint is blurry, select another finger for the fingerprint.
> - Enter accurately according to the on-screen instructions when authenticating fingerprints.
> - If you make the finger upright so that the contact area with the sensor is decreased or the angle of finger is warped, fingerprint authentication may not be performed.

Modifying User Information

User Management or Administrator can modify the registered user information. You can add the user's fingerprint or card and modify the PIN and permissions.

1. Click and authenticate with administrator privileges.

2. Click **USER** → .
3. Select your search terms. You can search for users with **All**, **User ID**, **Name**, **Fingerprint**, **Card / QR Code**.
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 press **OK**.

> **Info**
>
> - Fingerprint search is available only on XS2-ODPB and XS2-OAPB.
> - **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

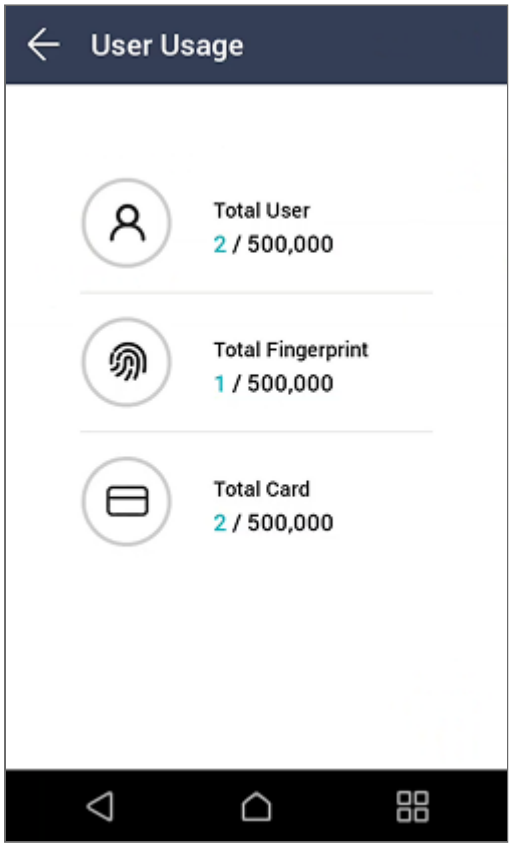
You can delete all registered users at once.

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 registered users and card counts at a glance.

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



Info

The number of fingerprints can only be verified on XS2-ODPB and XS2-OAPB products.

Authentication

Describes the supported authentication methods and authentication procedures.

Authentication mode

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

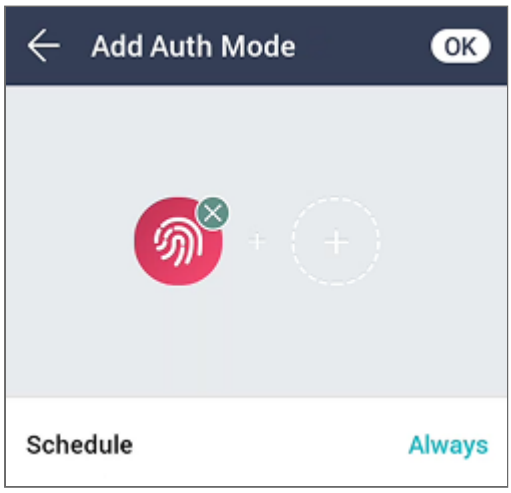
Info

Fingerprint authentication is only available for the XS2-ODPB and XS2-OAPB products.

Registering auth mode

1. Click and authenticate with administrator privileges.
2. Press **AUTHENTICATION** → **Auth Mode**.
3. Select .

4. Pressing (+) will display the credential that can be added on the screen. Select the credentials to add. Press the (×) while the credential is added, and the added credential will be deleted.



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

Category	Description
Fingerprint	- : This mode uses only fingerprint. - + : This mode requires entering a PIN after authenticating via fingerprint.
Card / QR Code	- : This mode uses only card / QR code authentication. - + : This mode requires authentication via card/QR code followed by fingerprint authentication. - + : This mode requires card / QR code authentication followed by PIN entry. - + / : This mode allows for authentication via card/QR code followed by either fingerprint or PIN entry. - + + : This mode uses both fingerprint authentication and PIN entry after authentication via card/QR code.
ID	- ID + : This mode requires entering an ID followed by fingerprint authentication. - ID + : This mode requires ID entry followed by PIN entry. - ID + / : This mode allows for entering an ID followed by either fingerprint authentication or entering a PIN. - ID + + : This mode uses both fingerprint authentication and PIN entry after entering an 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.
> - To use **QR/Barcode** authentication on XS2-DPB, XS2-APB, XS2-ODPB, and XS2-OAPB models, **QR/Barcode** must be activated in **AUTHENTICATION** → **QR/Barcode Operation**, and a separate device license is required. For more information, refer to License.

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**.



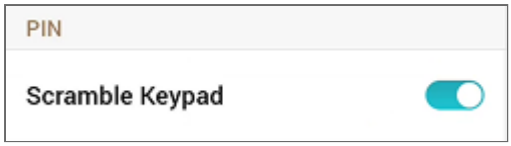
- **Auth Timeout**: If authentication is not completed within the set time, authentication will fail. It can be set to 3 to 20 seconds.
- **Server Matching**: When server matching is set, the device does not perform user authentication; BioStar X performs user authentication. It can be used when the device has too much user information or when the device is installed outside.

> **Info**
>
> 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.

PIN

Set whether to use the scramble keypad when entering passwords.

1. Click and authenticate with administrator privileges.
2. After pressing **AUTHENTICATION**, set whether to use **PIN** in **Scramble Keypad**.

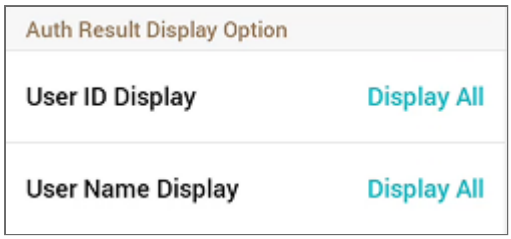


- **Scramble Keypad**: The positions of numeric keys can be scrambled randomly when entering a password to prevent password leaks.

Auth result display option

You can set the auth result display option.

1. Click and authenticate with administrator privileges.
2. After pressing **AUTHENTICATION**, change the desired items in **Auth Result Display Option**.



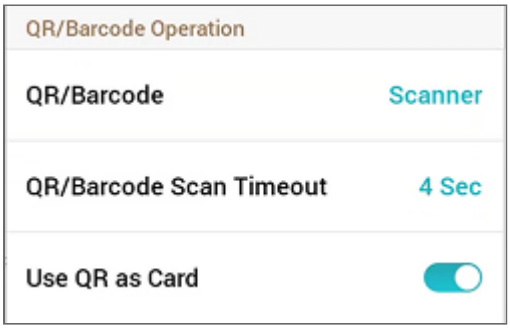
- **User ID Display**: You can select how the user ID is displayed on the authentication result screen of the device.
  - **Display All**: Displays the entire user ID.
  - **Mask All but First Letter**: Displays only the first letter of the user ID.
  - **Hide All**: Do not display the user ID.
- **User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

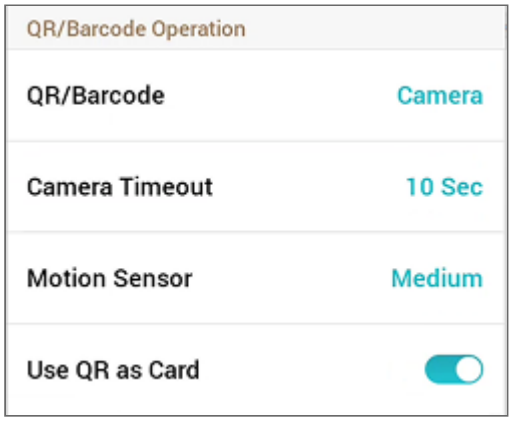
QR/Barcode Authentication Options

You can set QR/Barcode authentication.

1. Click and authenticate with administrator privileges.
2. After pressing **AUTHENTICATION**, set the QR/Barcode authentication method in **QR/Barcode Operation**.

XS2-QDPB, XS2-QAPB



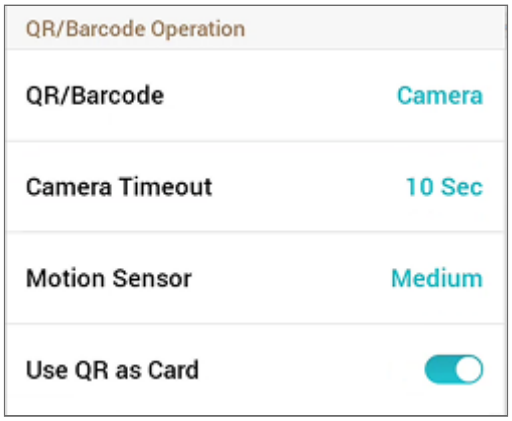


- **QR/Barcode**: Set the QR/Barcode authentication method. Select **Camera Frequency** or **Scanner** to authenticate with the device front camera or bottom QR/Barcode scanner, respectively. The default is **Scanner**.

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

- **QR/Barcode Scan Timeout**: If QR/Barcode is not scanned within the set time, authentication fails. Set between 4 and 10 seconds. Available when **QR/Barcode** is set to **Scanner**.
- **Camera Timeout**: If QR/Barcode is not scanned within the set time, authentication fails. Set between 3 and 20 seconds. Available when **QR/Barcode** is set to **Camera Frequency**.
- **Motion Sensor**: Set the sensitivity for detecting movement around the device. Available when **QR/Barcode** is set to **Camera Frequency**.
- **Use QR as Card**: You can set up authentication with a QR code that has the same data as the CSN card or Wiegand card issued to the user. Available when **QR/Barcode** is set to **Camera Frequency** or **Scanner**.

XS2-DPB, XS2-APB, XS2-ODPB, XS2-OAPB



- **QR/Barcode**: Set the QR/Barcode authentication method. Select **Camera Frequency** to authenticate with the device front camera. When **QR/Barcode** is set to **Camera Frequency**, you can use **Camera Timeout**, **Motion Sensor**, and **Use QR as Card**.

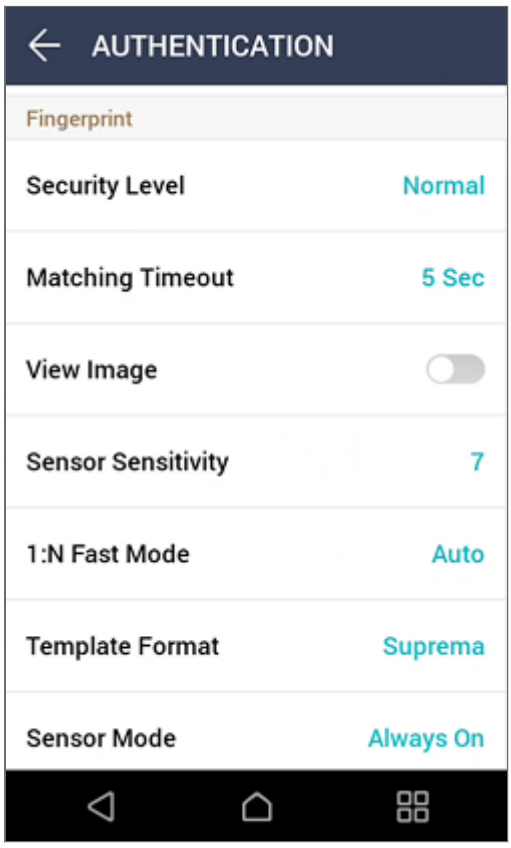
> **Info**
> A separate device license is required to use **Camera Frequency**. For more information, refer to License.

- **Camera Timeout**: If QR/Barcode is not scanned within the set time, authentication fails. Set between 3 and 20 seconds.
- **Motion Sensor**: Set the sensitivity for detecting movement around the device.
- **Use QR as Card**: You can set up authentication with a QR code that has the same data as the CSN card or Wiegand card issued to the user.

Fingerprint settings XS2-ODPB, XS2-OAPB

You can change the settings for fingerprint authentication.

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



- **Security Level**: You can set the security level for 1:N: authentication.
- **Matching Timeout**: Set the wait time for fingerprint matching. If authentication is not completed within the specified time, it will fail.
- **View Image**: The original image of the scanned fingerprint can be viewed.

- **Sensor Sensitivity**: Set the sensitivity of the fingerprint recognition sensor. Set the sensitivity higher to obtain precise fingerprint information.
- **1:N Fast Mode**: Set the speed of fingerprint authentication. When you select **Auto**, authentication speed is set according to the total number of fingerprint templates enrolled in the device.
- **Template Format**: Set the fingerprint template format. **SUPREMA** is set as default. Changing the template format will make all previously saved fingerprints unusable, so take care when changing.

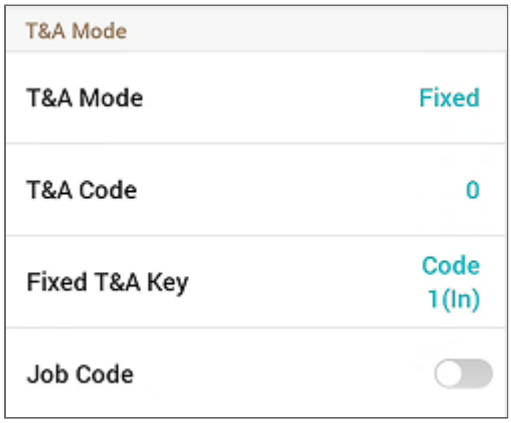
> **Info**
> Delete all user fingerprint information and then change the template format. If user fingerprint information is enrolled, you cannot change the template format.

- **Sensor Mode**: Set to **Auto On** to turn on the fingerprint sensor when it detects the user's finger. When set to **Always On**, the sensor remains on even when not scanning fingerprints.
- **Live Finger Detection**: Set the fake fingerprint detection level. Higher levels for fake fingerprint detection may also increase rejection rates for actual people's fingerprints.
- **Advanced Enrollment**: Assess the quality of scanned fingerprints to save high-quality fingerprint information. Enable to notify the user when fingerprint quality is low, helping them scan fingerprints correctly.
- **Duplicate Check**: Check for duplicate fingerprints when enrolling.

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. To register attendance events, select **T&A Code** → and set the icons to be displayed on the screen, **T&A Event Name**, and **Schedule**.
- **T&A Required**: Set to require a user to select a T&A event when authenticating. Available when **T&A Mode** is set to **By User**.
- **Fixed T&A Key**: Set to use only a T&A event selected by the administrator. Available when **T&A Mode** is set to **Fixed**.

- **Job Code**: Set whether to use the job code.

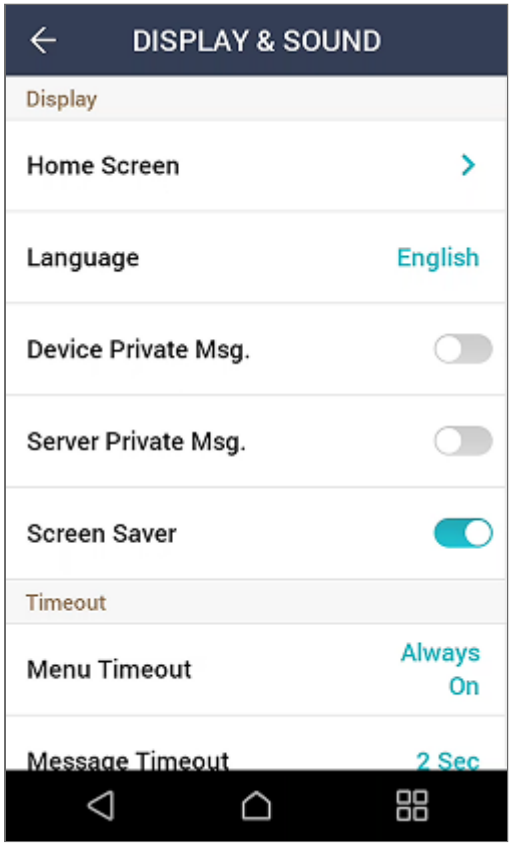
Settings

Provides instructions on how to set system and device configurations.

Display & Sound

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

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



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

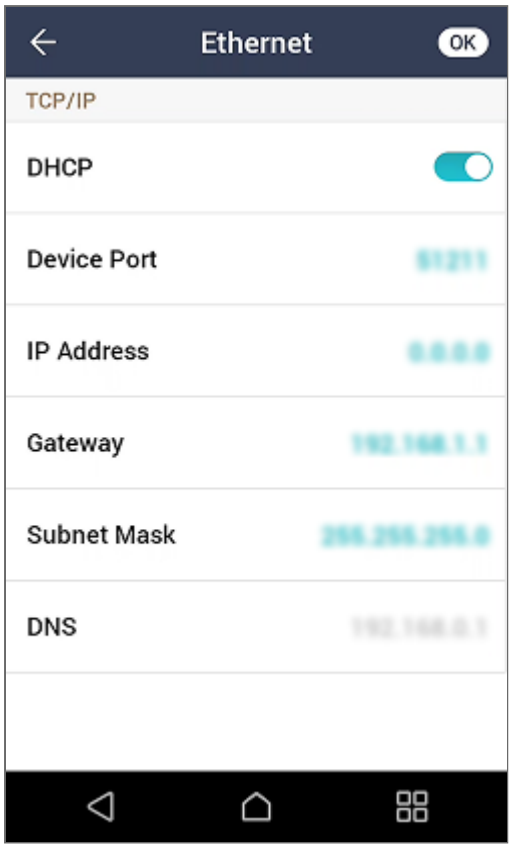
> **Info**
> For more information on the BioStar Device SDK, refer to the BioStar Device SDK page on the Suprema Knowledge Base.

Network

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

Ethernet

1. Click and authenticate with administrator privileges.
2. Select **NETWORK** → **Ethernet**.
3. Change the desired item.



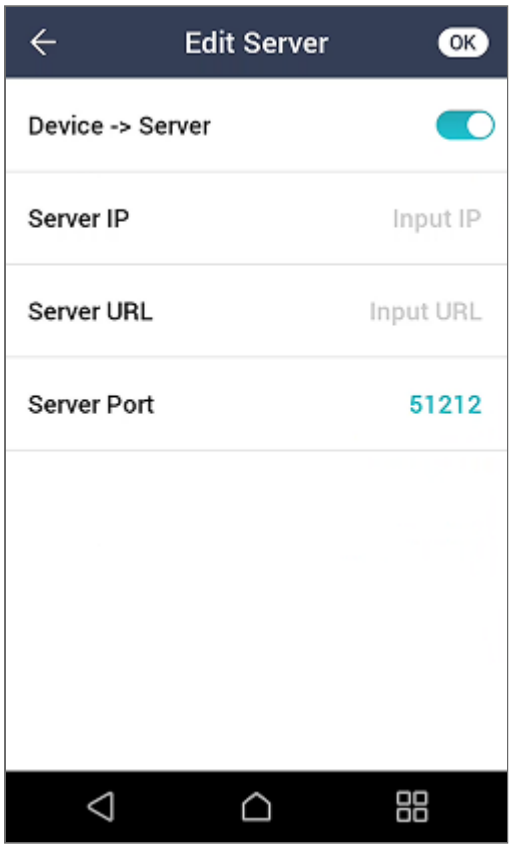
- **DHCP**: Set whether to use DHCP. If you disable the DHCP setting, users will be able to modify **Device Port**, **IP Address**, **Gateway**, and **Subnet Mask**.

- **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**.

Server

1. Click and authenticate with administrator privileges.
2. Select **NETWORK** → **Server**.
3. Change the desired item.

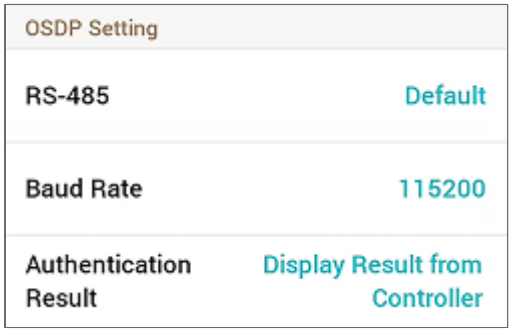


- **Device → Server**: You can send a connection signal from the device to a server with the input information directly. When **Device → Server** is enabled, the user can input **Server IP**, **Server URL**, and **Server Port**.
- **Server IP**: Enter the IP address of the PC on which BioStar X is installed.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

OSDP settings

1. Click and authenticate with administrator privileges.
2. Click **NETWORK** and set the desired item in **OSDP Setting**.



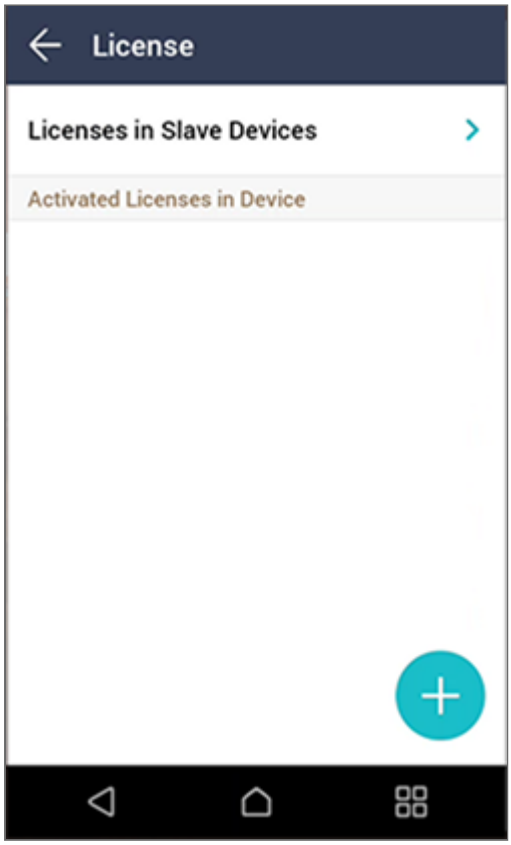
   - **RS-485**: Select the RS-485 mode.
   - **Baud Rate**: Select the desired baud rate.
   - **Authentication Result**: When using **Intelligent Slave**, select to display the authentication results of 3rd party controllers or devices on the screen. This option can be used when **RS-485** mode is set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

Device

License

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

1. Click and authenticate with administrator privileges.
2. Press **DEVICE** → **License**.
3. To activate the device license, connect the USB containing the license to the device and select .



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



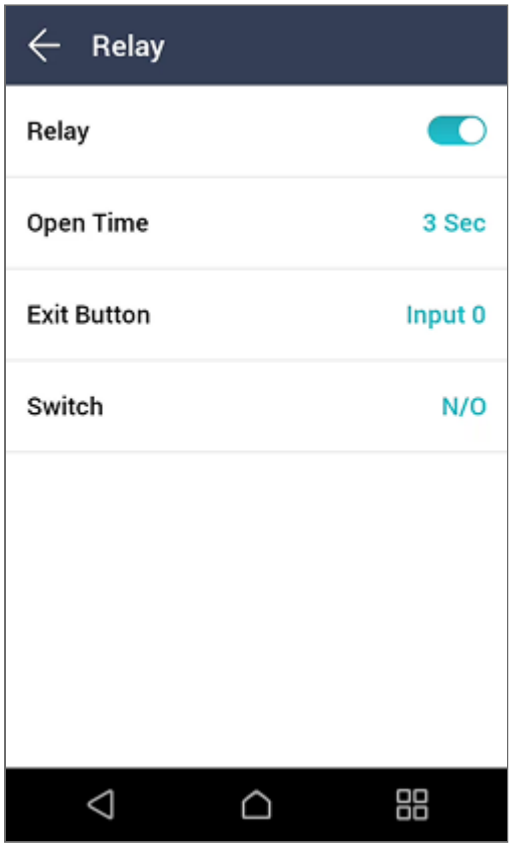
Info

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

Relay

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

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

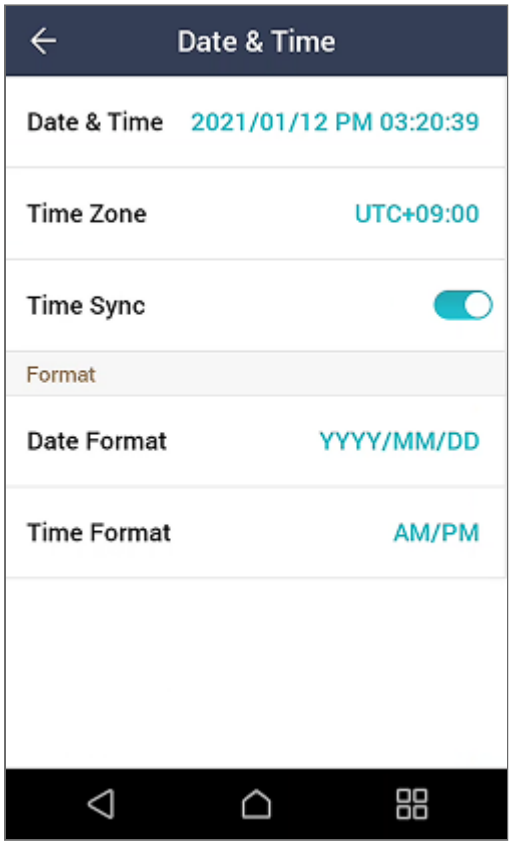


- **Relay**: You can set whether relay is enabled or not. Enabling relay settings will allow you to configure **Open Time** and **Exit Button**.
- **Open Time**: Set the duration for the door to remain open when standard user authentication has been carried out.
- **Exit Button**: Select the input port 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.

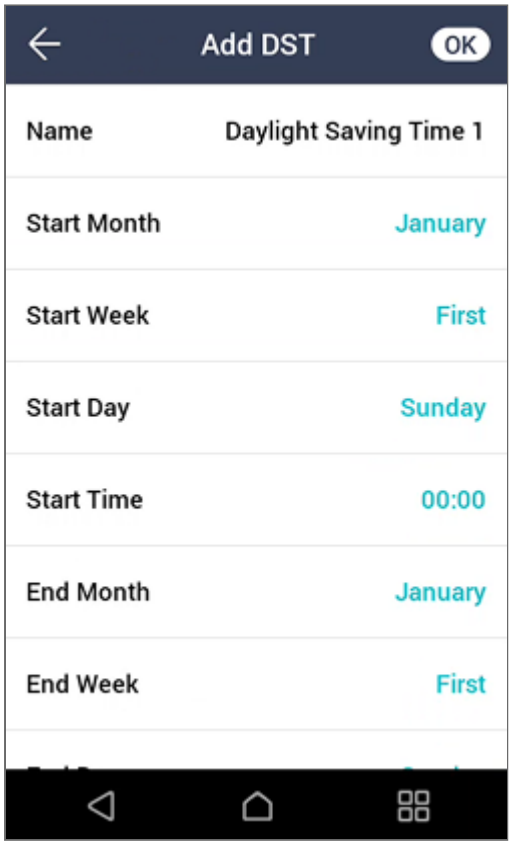


- **Date & Time**: Check the current date and time. To modify it manually, disable **Time Sync**.
- **Time Zone**: Set the time reference of the current location.
- **Time Sync**: Synchronize the server and the time. If you wish to synchronize the server and the time, enable **Time Sync**.
- **Date Format**: 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.



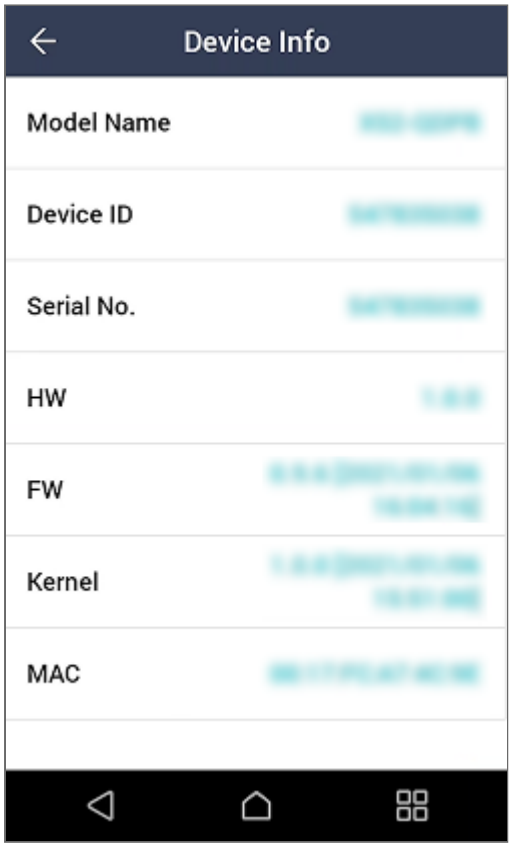
- **Name**: You can view the name of the daylight savings time.
- **Start Month** / **Start Week** / **Start Day** / **Start Time**: Set details of when daylight-saving time begins.
- **End Month** / **End Week** / **End Day** / **End Time**: Set details of when daylight-saving time ends.

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.

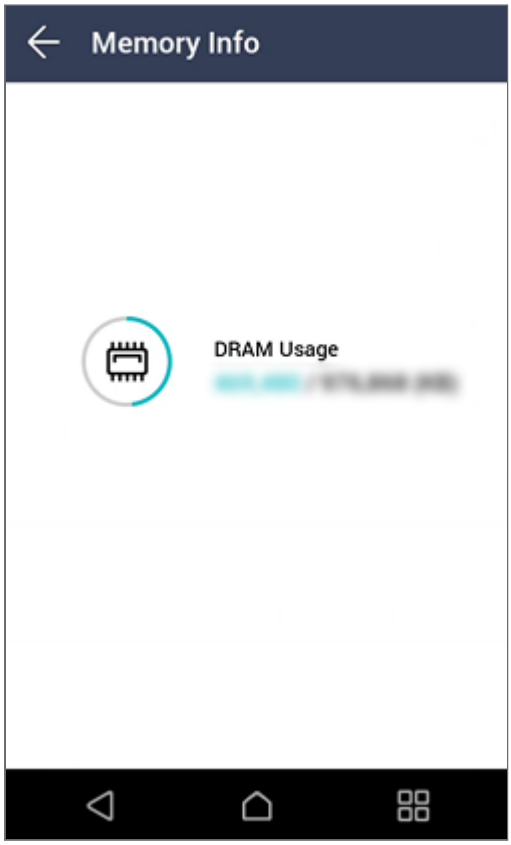
1. Click and authenticate with administrator privileges.
2. Select **DEVICE** → **Device Info**. You can check the information of **Model Name**, **Device ID**, **Serial No.**, **HW**, **FW**, **Kernel**, **MAC**.



Memory information

View the status of memory usage.

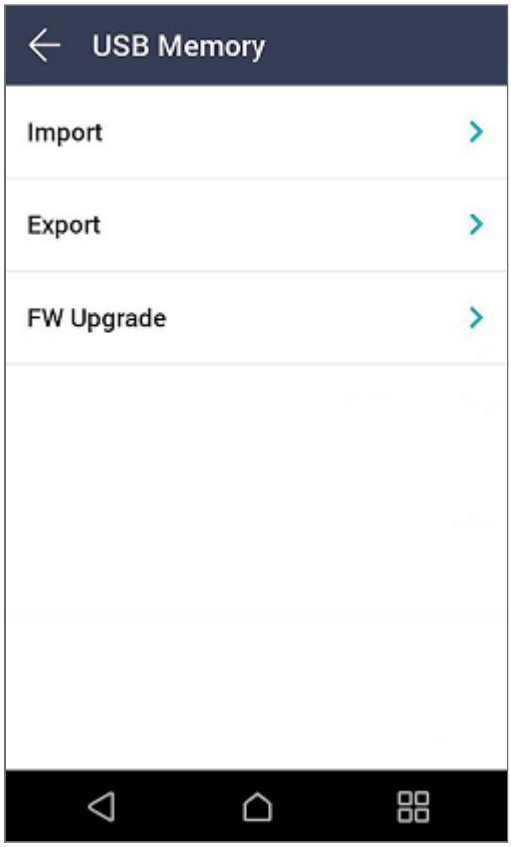
1. Click and authenticate with administrator privileges.
2. Select **DEVICE** → **Memory Info**. You can view the memory usage status of the device.



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.

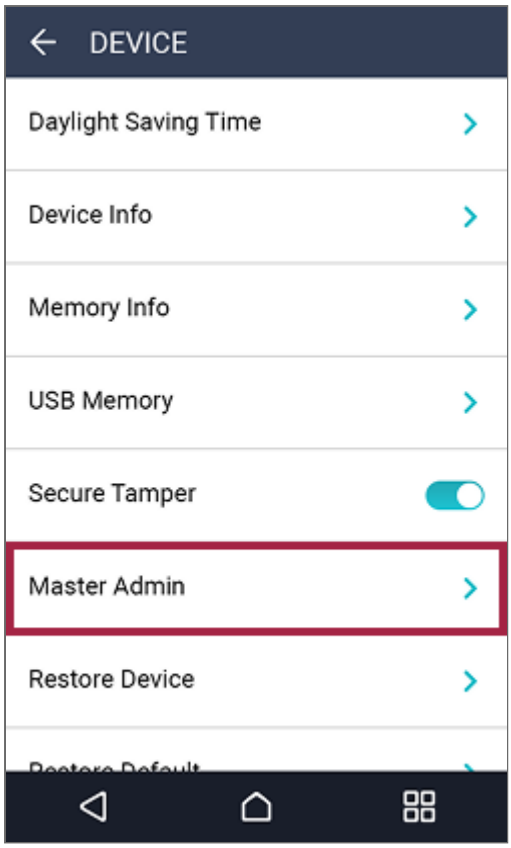
1. Click and authenticate with administrator privileges.
2. Select **DEVICE**.
3. Activate **Secure Tamper** to delete data of all registered users, all logs, and secure keys when a temper event occurs.

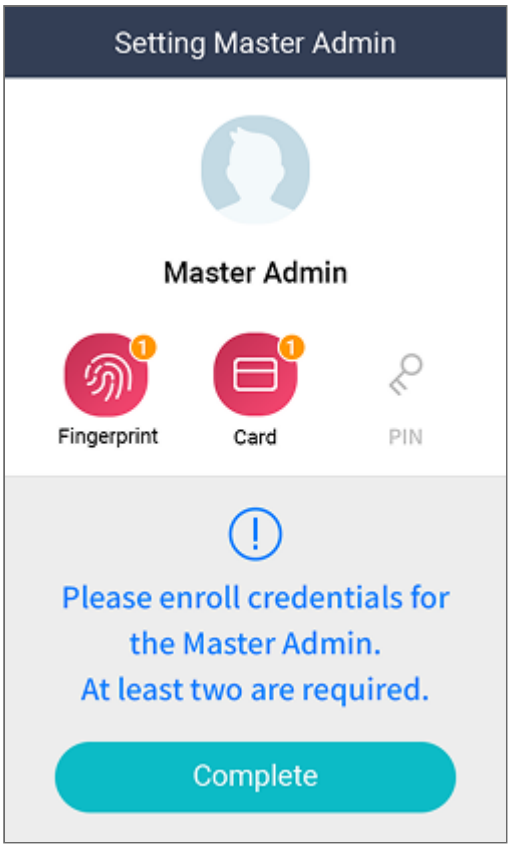
Master administrator CE products

You can change the authentication method of the Master Admin.

1. Click and authenticate with administrator privileges.
2. Select **DEVICE** → **Master Admin**.

3. Configure the desired authentication methods.





Info

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

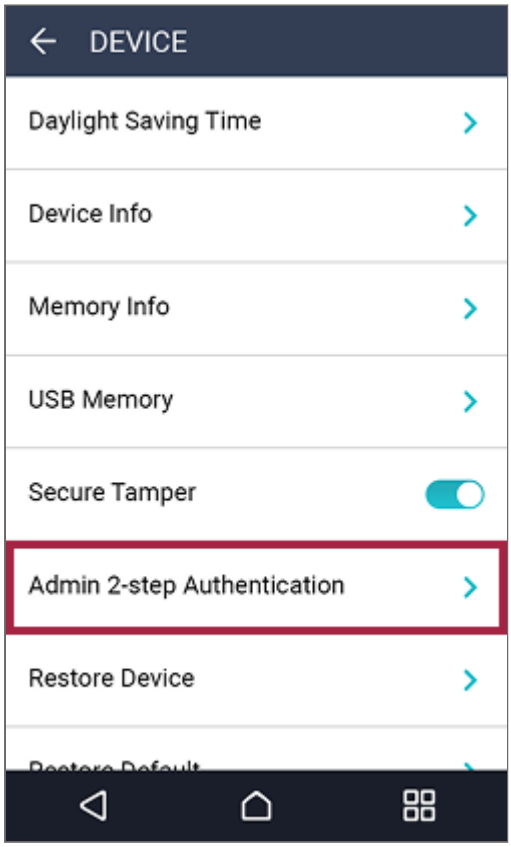
Administrator two-step authentication CE products

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

Info

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

1. Click and authenticate with administrator privileges.
2. Select **DEVICE** → **Admin 2-step Authentication**.

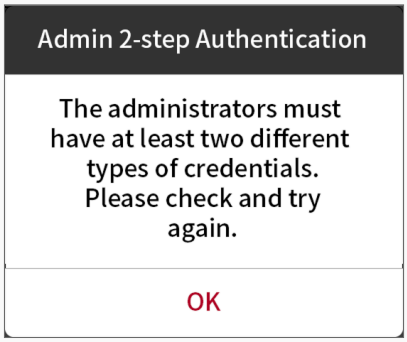


Info

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

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

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



Caution

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

Restart device

The user can restart the device.

1. 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. Press **OK** to initialize all device settings. Press **Cancel** to return to the previous screen.
   - **Keep Network Settings**: Initializes all settings except for network settings. Press **OK** to initialize all settings except for network settings. Press **Cancel** to return to the previous screen.
   - **Factory Default**: Deletes all information saved in the device and the root certificate, restoring settings to default.
   - **Delete the Root Certificate**: Deletes the root certificate saved in the device.
3. If you proceed with **Restore Default**, the device will restart.

> **Info**
>
> - When you reset, the operator level will be reset as well. After resetting, make sure to set the operator level again.
> - Language setting will not change after resetting.
> - The **Factory Default** menu can be used when the root certificate is saved in the device.
> - The **Delete the Root Certificate** menu can be used only when the root certificate is saved in the device and an administrator has been designated.

User ID type

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

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

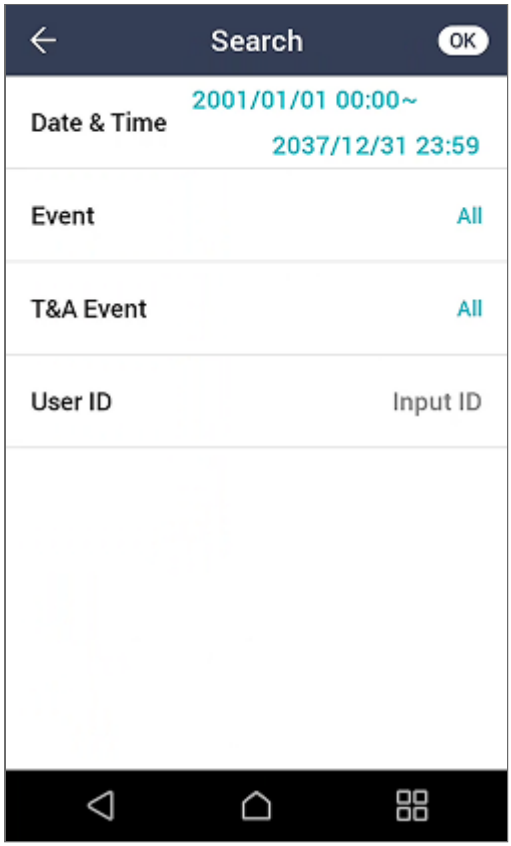
Event Logs

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.

Delete all logs

You can delete all saved logs.

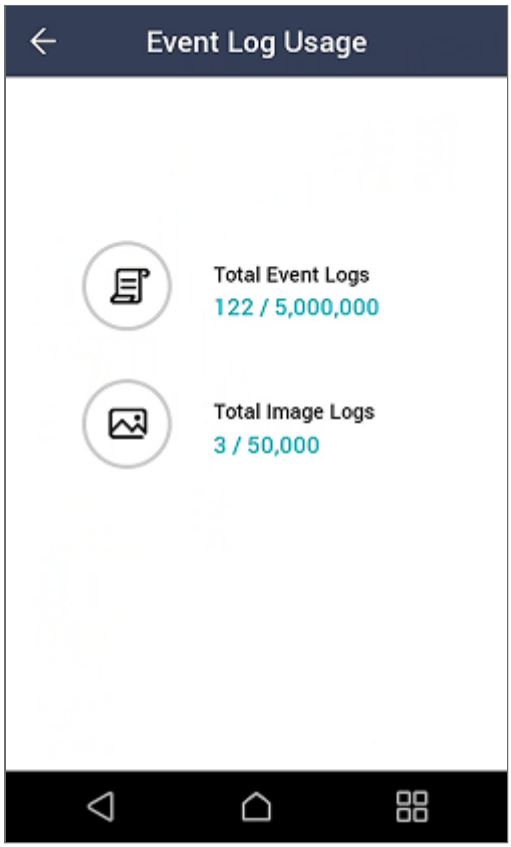
1. Click and authenticate with administrator privileges.
2. Select **EVENT LOG**. All event logs appear.
3. To delete all logs, select and click **OK**. Press **Cancel** to return to the previous screen.

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.

QR/Barcode

Q. It fails to scan a QR/Barcode.

- Refer to Correct QR/Barcode Authentication Method and try again.
- **XS2-QDPB**, **XS2-QAPB**: Place the guide beam at the center of the QR code.
- **XS2-DPB**, **XS2-APB**, **XS2-ODPB**, **XS2-OAPB**: Position the QR/Barcode in the center of the scan screen of the device.
- Adjust the brightness of your smartphone so that the device can read the QR/Barcode clearly and try again.
- If the problem persists, contact the administrator who issued the QR/Barcode.

Fingerprint

Q. The fingerprint has been enrolled but fingerprint authentication cannot be done smoothly and errors occur frequently.

- Check Correct fingerprint input method and enroll the fingerprint again.
- If your fingerprint has a cut, the device may recognize your fingerprint as someone else's fingerprint.
- If there are many enrolled fingerprints, change **Matching Timeout** and try again.

- The authentication rate may vary for each fingerprint due to different characteristics. Enroll the fingerprint of another finger.

Q. Suddenly fingerprint authentication cannot be done.

- Check if the finger or the fingerprint sensor is smeared with sweat, water or dust, and wipe the finger or the fingerprint sensor clean.
- Wipe your finger and the fingerprint sensor with a dry towel and then try again.
- If the fingerprint of your finger is too dry, blow on the fingerprint and then try again.

Q. The fingerprint sensor does not turn on.

- When **Sensor Mode** is set to **Auto On**, the sensor will only turn on when you place finger on the fingerprint sensor. If you want the fingerprint sensor to always be on, set **Sensor Mode** to **Always On**.

Door lock

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

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

Time

Q. Suddenly the time has become incorrect.

- The device is equipped with a built-in battery but if power is not supplied for a long time, the built-in battery may die, causing the time to become incorrect. You can correct the time by referring to Date & Time.

Admin access

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

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

Master Administrator (CE-oriented products)

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

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

Product Specifications

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

Credentials

Biometric	**Fingerprint** XS2-ODPB, XS2-OAPB • Image Dimension:300 x 400 pixels • Resolution:500 dpi • Template:SUPREMA / ISO19794-2 / ANSI-378 • Extractor / Matcher:MINEX certified and compliant • Sensor Certificates:FBI PIV and FBI Mobile ID FAP20 • Live Fingerprint Detection:Supported (SW-based)
RF Card	XS2-DPB, XS2-QDPB, XS2-ODPB: 125kHz EM & 13.56MHz MIFARE, MIFARE Plus, DESFire, DESFire EV1/EV2/EV3, FeliCa XS2-APB, XS2-QAPB, XS2-OAPB: 125kHz EM, HID Prox & 13.56MHz MIFARE, MIFARE Plus, DESFire, DESFire EV1/EV2/EV3, FeliCa, iCLASS SE/SR/Seos
RF Read Range[1)]	EM/HID Prox/MIFARE/DESFire/HID iCLASS: 50 mm, Felica: 30 mm
Mobile	NFC, BLE
Scramble Keypad (PIN)	Supported
QR/Barcode[2)]	Supported[3)]

General

CPU	1.5 GHz Quad Core
Memory	16 GB Flash + 1 GB RAM
Crypto Chip	Supported

Display	**4" IPS color LCD**	
Display Resolution	**480 x 800 pixels**	
Sound	**24 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 Type	**CMOS 2M pixels**	
Camera Resolution	**1600 x 1200 pixels**	
IP Rating	**IP65**	
Authentication	**XS2-DPB, XS2-APB, XS2-QDPB, XS2-QAPB**	**CE, UKCA, KC, FCC, IC, RCM, BIS, ANATEL, SIG, TELEC, RoHS, REACH, WEEE**
	XS2-ODPB, XS2-OAPB	**CE, UKCA, KC, FCC, IC, RCM, BIS, ANATEL, SIG, RoHS, REACH, WEEE**

Capacity

Max. User	**500,000**[4)]	
Max. Credentials (1:N)	**XS2-ODPB, XS2-OAPB**	**Fingerprint: 100,000**
Max. Credentials (1:1)	**XS2-DPB, XS2-APB, XS2-QDPB, XS2-QAPB**	• **Card: 500,000** • **PIN: 500,000**
	XS2-ODPB, XS2-OAPB	• **Fingerprint: 500,000** • **Card: 500,000** • **PIN: 500,000**

Max. Text logs	**5,000,000**
Max. Image logs	**50,000**

Interface

Ethernet	**Supported (10/100 Mbps, auto MDI/MDI-X)**
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 (Selectable)**
Input	**2 ch Inputs**
Relay	**1 relay**
USB	**USB 2.0 (Host)**
PoE	**Supported (IEEE 802.3af compliant)**
Tamper	**Supported**

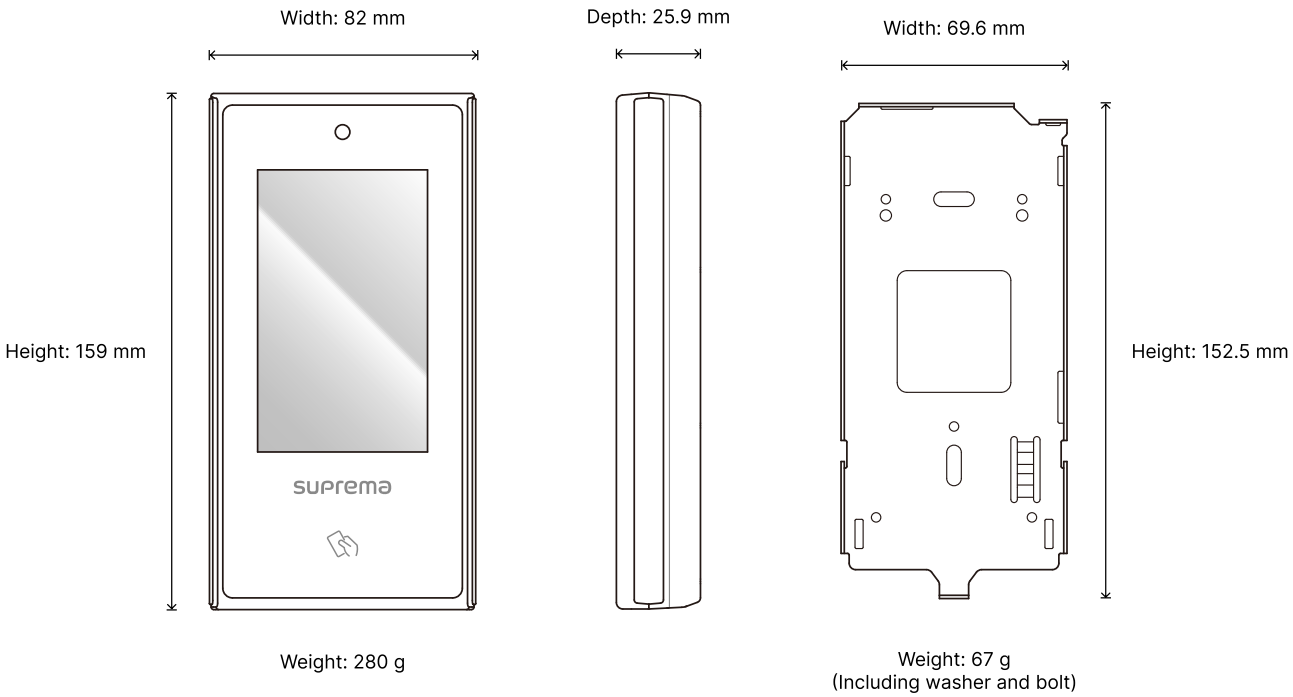
Electrical

Power	**12 Vdc**	**Current: Max. 0.8 A**
	24 Vdc	**Current: Max. 0.5 A**
Switch Input VIH	• **Min.: 3 V** • **Max.: 5 V**	

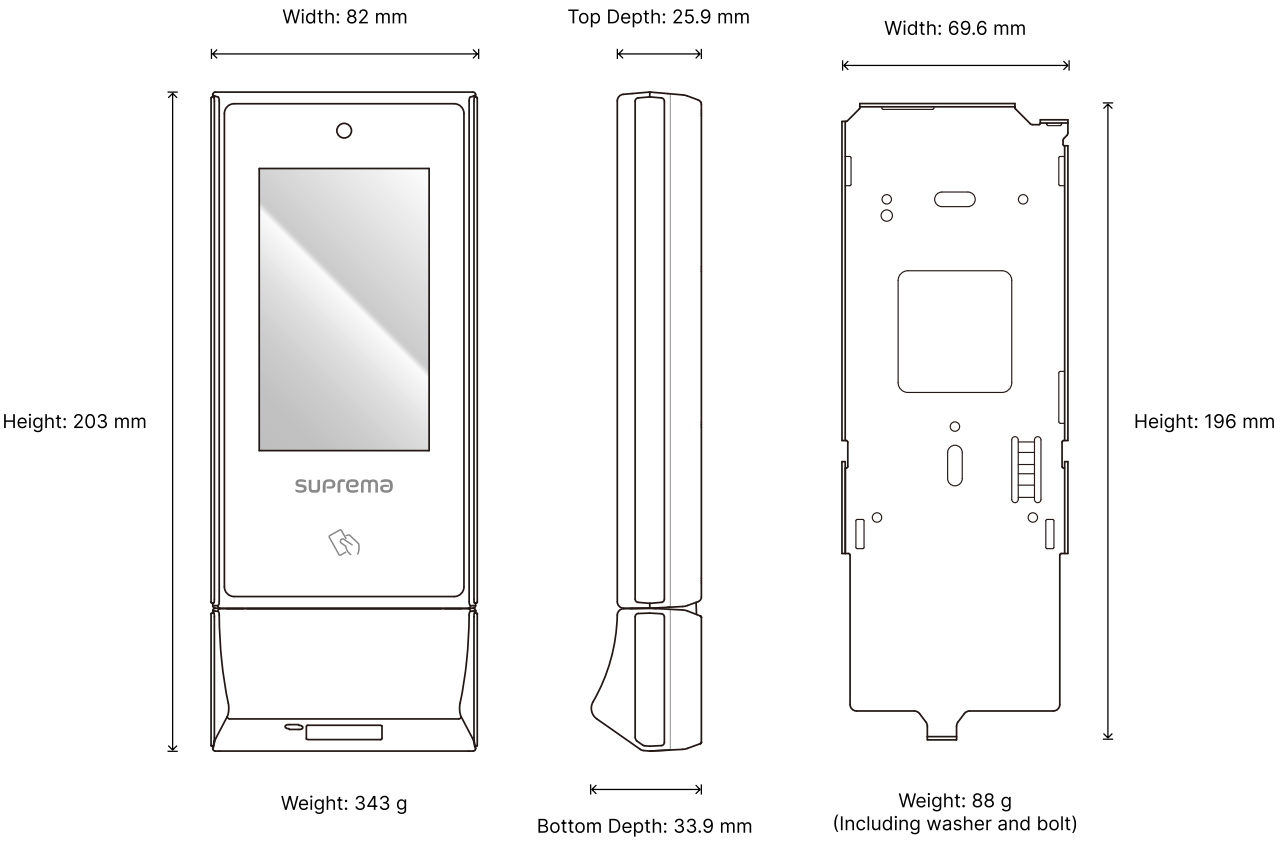
Switch Input VIL	**Max.: 1 V**
Switch Pull-up Resistance	**4.7 kΩ (The input ports are pulled up with 4.7 kΩ.)**
Wiegand Output VOH	**More than 4.8 V**
Wiegand Output VOL	**Less than 0.2 V**
Wiegand Output Pull-up Resistance	**Internally pulled up with 1 kΩ**
Relay	• **2 A @ 30 VDC Resistive load** • **1 A @ 30 VDC Inductive load**

Dimensions and Weight

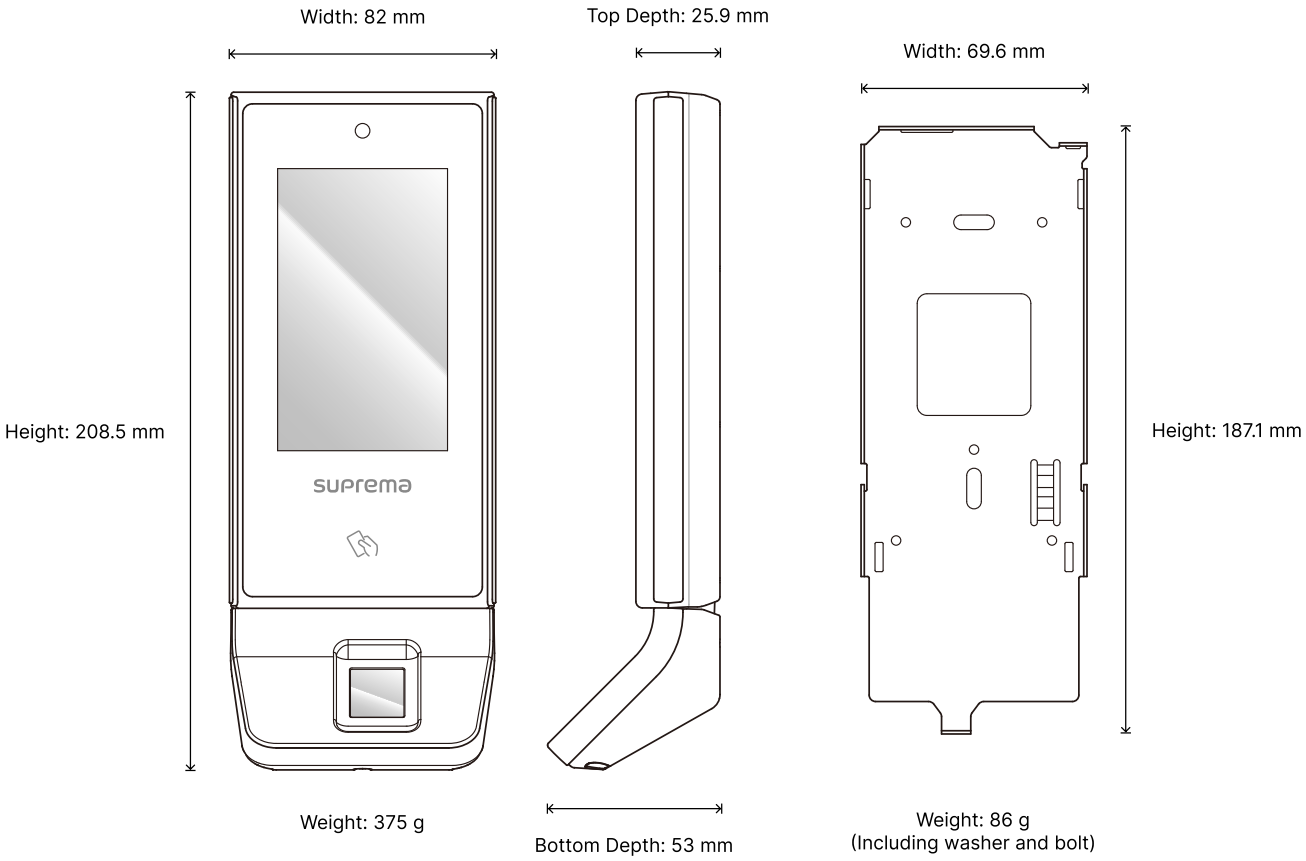
XS2-DPB, XS2-APB



XS2-QDPB, XS2-QAPB



XS2-ODPB, XS2-OAPB



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

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

3) Setting the **QR/Barcode** authentication method to **Camera Frequency** requires a separate device license.

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

Info

Product specifications are subject to change without notice for performance improvement.

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: -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 BoringSSL library included in this product follows the OpenSSL license and the Original SSLeay license. For more information about the BoringSSL license, please see the BoringSSL 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.
- Contact Suprema Technical Support Team to download the modified Linux kernel 4.x-based source and the BoringSSL, OpenSSL, Original SSLeay, and AOSP libraries included in this product.

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.