XPass Q2

INSTALLATION GUIDE

Version 1.03

English

EN 101.00.XPQ2

suprema

SECURITY & BIOMETRICS

CONTENTS

Safety Instructions 4

Compliance Information 4

Getting Started 8

Components 8

Name and function of each part 9

Cables and connectors 11

Notes on QR/Barcode and Device License 14

Installation 16

Fixing the bracket and the product 16

Power supply connection 18

Connect reader and lock power 19

Network Connection 21

Input connection 22

Relay Connection 23

Connecting as a Standalone 26

Connecting to Secure I/O 2 27

Wiegand Connection 28

Initialize Network Settings 28

Factory reset 29

Firmware upgrade 30

Product Specifications 31

Credentials 31

General 31

Capacity 32

Interface 32

Electrical 33

Dimensions and Weight 34

Regulatory Information 36

FCC Compliance Information 36

IC information 36

EU Declaration of Conformity (CE) 37

Appendices 38

Disclaimers 38

Copyright Notice 39

Open Source License 39

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.

Use the product within -20 °C ~ 60 °C and store it at appropriate temperatures, not too low or too high. Use only within -20 °C ~ 50 °C when using PoE.

- 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.

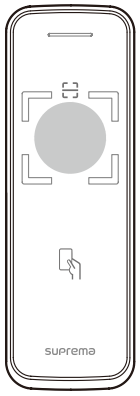
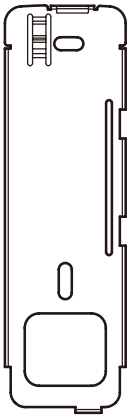
- The device may malfunction.

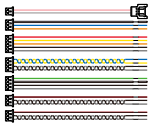
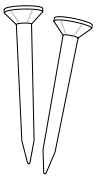
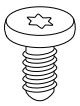
> **RTC Battery**
>
> Replacing with unauthorized or incorrect types of batteries may pose a risk of explosion. Dispose of batteries according to local or international waste regulations.

Getting Started

Provides initial procedures for getting started with the device.

Components

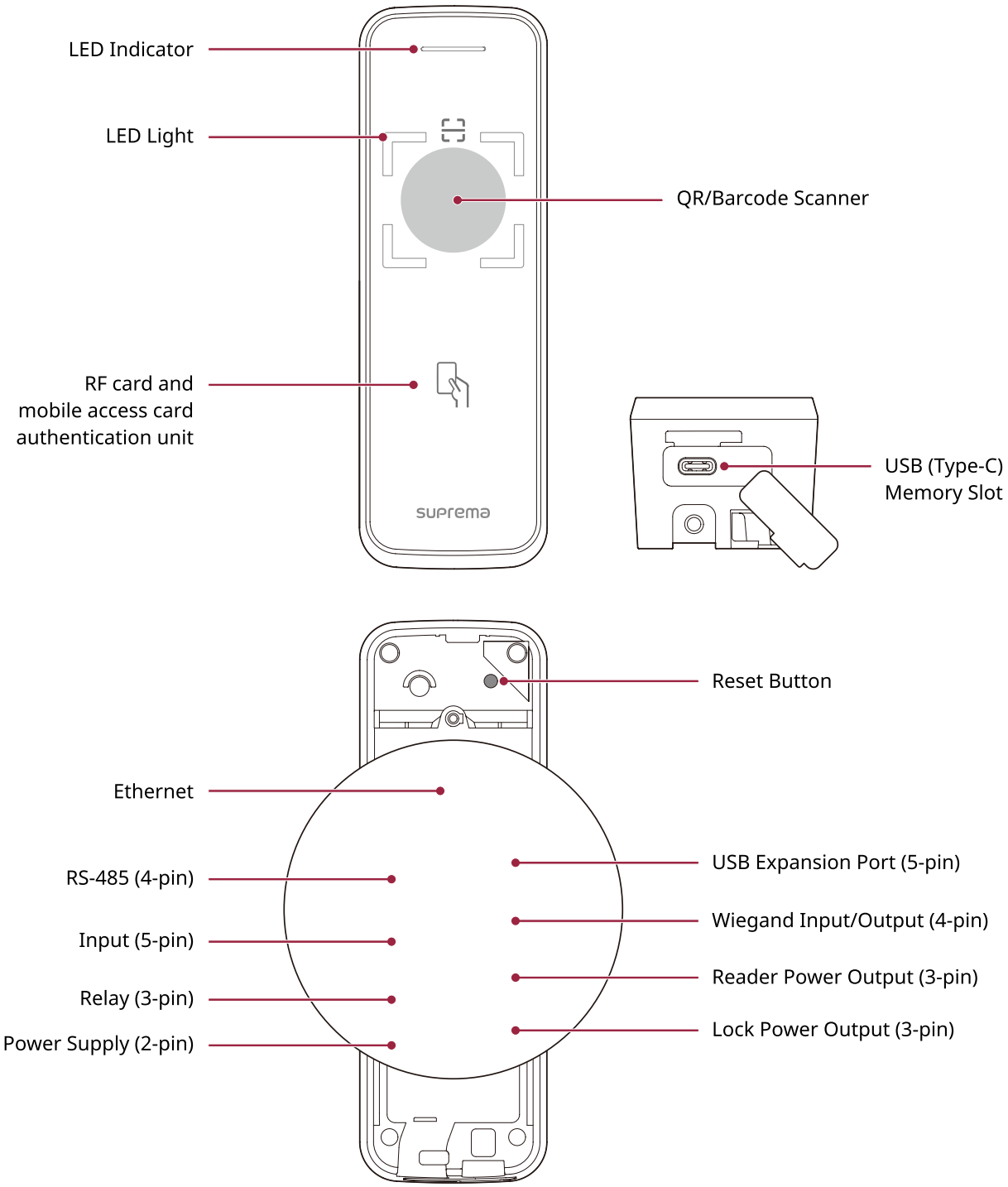
			
XPass Q2	Wall Bracket	Quick Guide	Open Source Software Guide

				
Connection Cables	Fixing Screws x2	Bracket Fixing Screw (Star Shaped)	Diode	120 Ω Resistor

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



- **LED Indicator**: Indicates the operational status of the device with the color of the LED.
  - Green: Authentication success.
  - Red: Authentication failure.
  - Blue/Cyan blinking: Normal operation.

  - Blue/Green blinking:
    - When setting **DHCP** to use, unable to retrieve IP address.
    - When in **Slave** mode, the connection to the master device is disconnected.
  - Red/Purple blinking: Device is locked.
  - Green blinking: Waiting for input.
- **LED Light**: The LED turns on automatically when motion is detected near the QR/Barcode scanner.
- **QR/Barcode Scanner**: Scans QR/Barcode credentials for access.
- **RF card and mobile access card authentication unit**: Part to scan a RFID card or mobile access card for entrance.
- **USB (Type-C) Memory Slot**: Connects the USB memory.
- **Reset Button**
  - Initializes network settings. For more information on initializing network settings, refer to Initialize Network Settings.
  - Deletes all information and certificates stored on the device and initializes the settings. For more information on factory initialization, refer to Factory reset.
- **Ethernet**: Connect the Ethernet cable.
- **RS-485 (4-pin)**: Connect the RS-485 cable.
- **Input (5-pin)**: Connect the input cable.
- **Relay (3-pin)**: Connect the Relay cable.
- **Power Supply (2-pin)**: Connects the power supply cable.
- **USB Expansion Port (5-pin)**: Connect other accessory products.
- **Wiegand Input/Output (4-pin)**: Connect the Wiegand Input/Output cable.
- **Reader Power Output (3-pin)**: Connect the reader power output cable.
- **Lock Power Output (3-pin)**: Connect the lock power 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	INPUT2	Orange
4	INPUT GND	Black
5	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

Reader/Lock Power Output

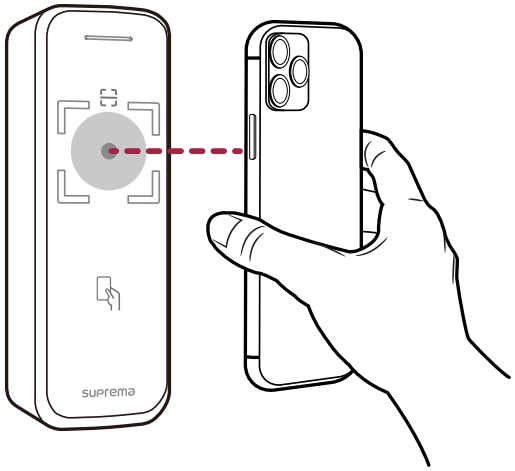


Pin	Name	Color
1	DC OUT	Red (black stripe)
2	DC GND	Black
3	DC GND	Gray

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. Scan the QR/Barcode as instructed to improve recognition.



- Maintain the recommended recognition distance between the device scanner and the QR/Barcode when scanning.
  - QR code: 5~15 cm
  - Barcode: 5~9 cm
- Position the QR/Barcode in the center of the scanner.
- 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.
- QR/Barcode scanning may take longer or fail if the position, distance, or lighting is inadequate.

Barcode types and minimum readable size

The following are examples of the minimum barcode sizes that can be read for each barcode type.

> **Info**
> Actual read rates may vary depending on print quality, encoding, lighting, camera resolution, shooting distance, and other conditions.

Basic support

This product natively supports QR Code.

Barcode type	Minimum readable size	Example value (character count)
QR Code	1 cm	32 alphanumeric characters

When the Camera QR license is applied

Barcode type	Minimum readable size	Example value (character count)
QR Code	1 cm	32 alphanumeric characters
Micro QR Code	1 cm	32 alphanumeric characters
Aztec	1 cm	32 alphanumeric characters
PDF417	3 cm	32 alphanumeric characters
Data Matrix	1 cm	32 alphanumeric characters
Code 39	5 cm	16 alphanumeric characters
Code 128	3 cm	16 alphanumeric characters
EAN-8	1.5 cm	8 digits (7 data + 1 checksum)
EAN-13	2 cm	13 digits (12 data + 1 checksum)
UPC-A	2 cm	12 digits (11 data + 1 checksum)
UPC-E	1.5 cm	8 digits (7 data + 1 checksum)

Notes for device license

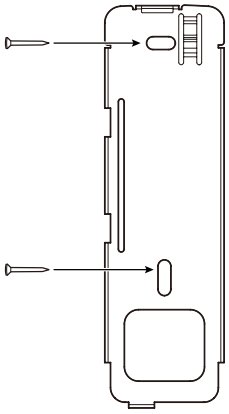
- Using additional QR/Barcode authentication methods requires a separate device license. Contact the place of purchase to issue a device license.
- The device license file is an encrypted file and cannot be modified arbitrarily.
- Device licenses are issued based on device ID. If the device ID is changed in an unusual way, the warranty service for the license is not provided.
- For detailed information on device licenses, please refer to the BioStar X Administrator Guide.

Installation

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

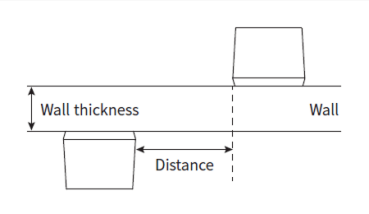
Fixing the bracket and the product

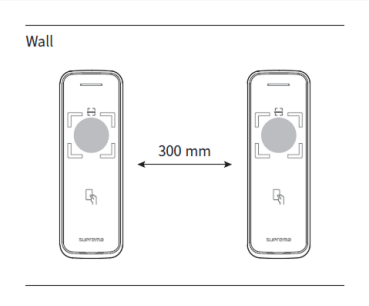
1. Secure the bracket tightly using the fixing screws at the location where the product will be mounted.



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.

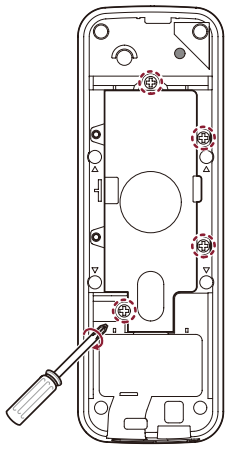




Wall thickness	Distance
100 mm	270 mm
120 mm	250 mm
150 mm	170 mm

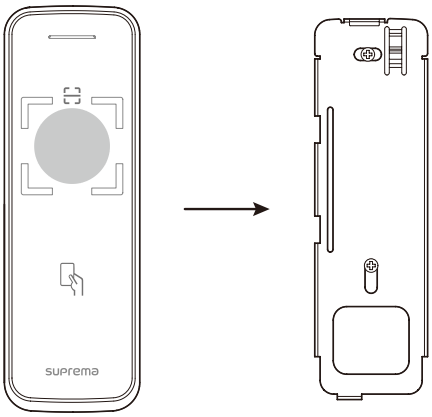
- When using a mobile access card, install devices maintaining a minimum distance of 1 m between devices to avoid BLE interference.

2. Tighten the four screws securing the cable cover.

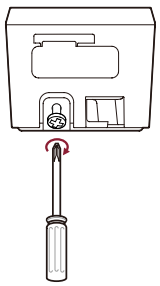


> **Info**
> Make sure that the cable cover is completely closed after connecting it to the product to maintain the water-resistant and dust-resistant features (IP65 rating).

3. Mount the product on the fixed bracket.

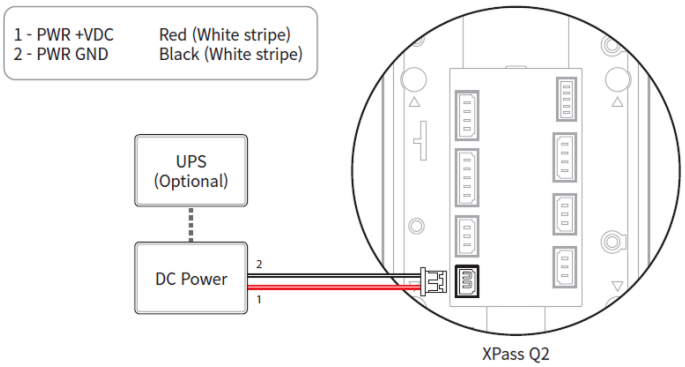


4. Rotate the fixing screws to assemble the product with the bracket.



> **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.

Power supply connection

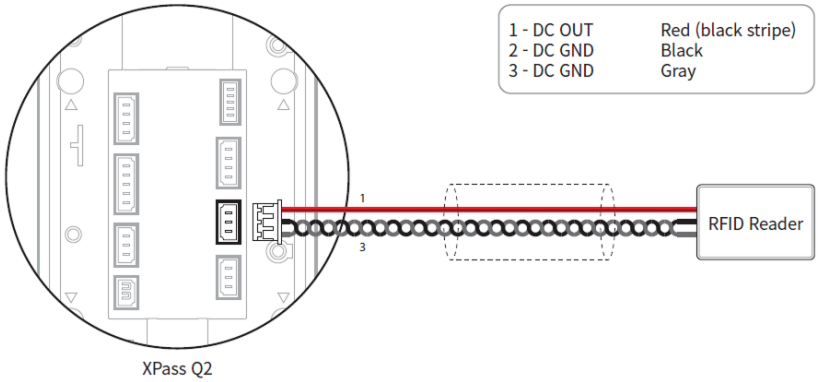


Caution

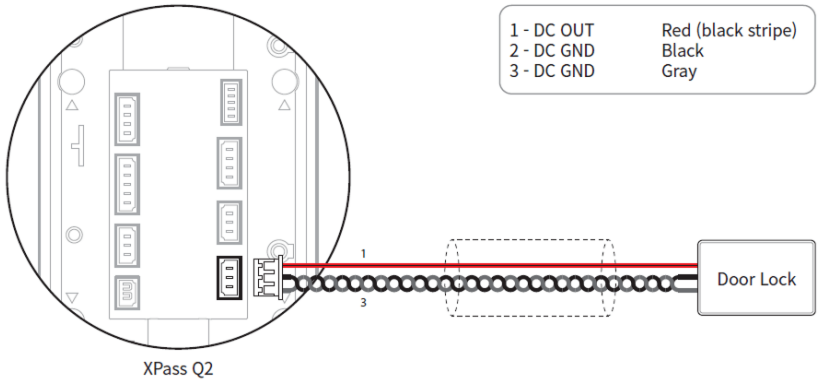
- DO NOT connect the device to the DC power supply (or adapter) and PoE power supply at the same time.
- Use the IEC/EN 62368-1 approved power adapter that supports higher power consumption than the product. If you wish to connect and use another device to the power supply adapter, you should use an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

Connect reader and lock power

Connect reader power



Connect lock power



Power output specifications for readers and locks by power source

Power	Maximum reader current	Maximum lock current
DC 12V	500 mA	1.2 A
DC 24V	250 mA	600 mA
PoE (12V out)	500 mA	Not supported

Maximum extension length for power output by cable specification

The distance that can be connected may vary depending on the cable specifications and installation environment used for power connection. If cable connections are made improperly it may cause the device to malfunction. The product supports DC 12 V, DC 24 V, and PoE. Check the maximum extension length for each cable gauge and connect the power correctly.

Cable specifications	DC 12V		DC 24V		PoE (12V output)
	Reader (500 mA)	Lock (1.2 A)	Reader (250 mA)	Lock (600 mA)	Reader (500 mA)
14 AWG	190 m	95 m	770 m	385 m	190 m
16 AWG	120 m	60 m	480 m	240 m	120 m
18 AWG	75 m	35 m	300 m	150 m	75 m

Info

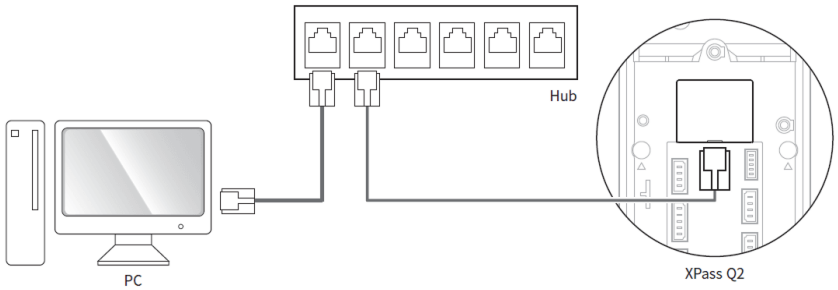
The actual maximum extension length can vary depending on the resistance of the cable manufacturer and model.

Network Connection

TCP/IP

LAN connection (connecting to a hub)

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

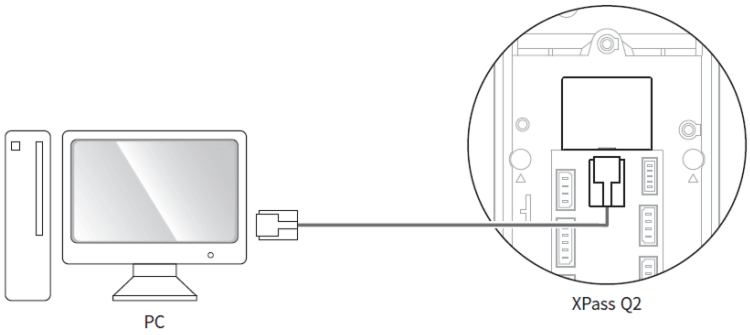


LAN connection (connecting to a PC directly)

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

> **Caution**
> Certain non-standard hubs/switches may not support automatic MDI/MDIX.

- XPQ2-DPB Supports PoE, which supplies power through an Ethernet cable.



Network ports and services

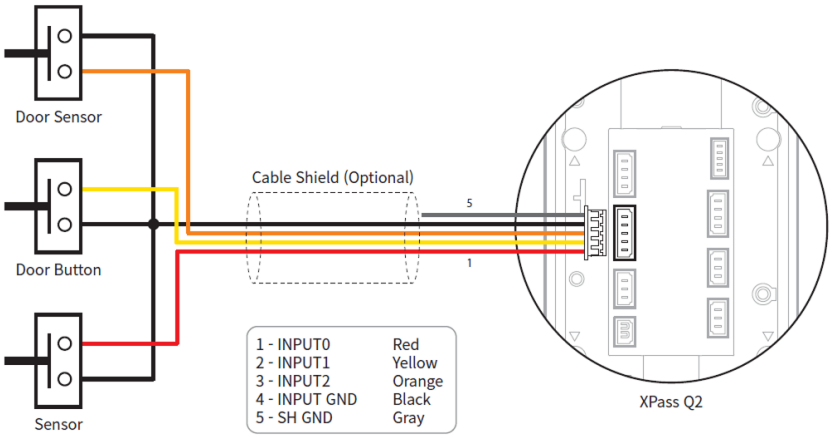
This device uses the following ports for network communication and stable service operation.

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

Info

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

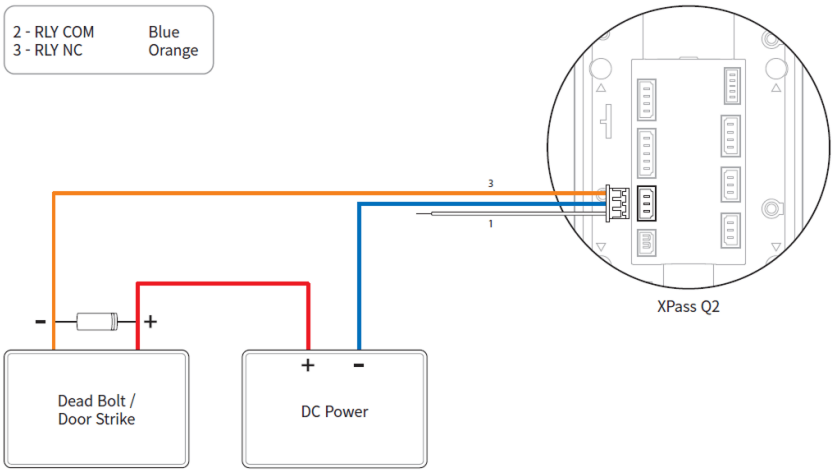
Input connection



Relay Connection

Fail Safe Lock

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



Caution

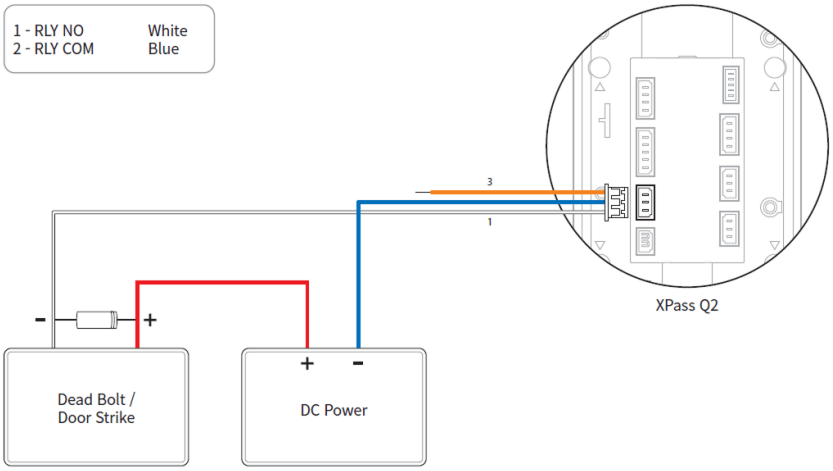
- Install a diode at both sides of the door lock wire as shown in the figure to protect the relay from the reverse current, which occurs when the door lock operates.
- Use a separate power supply for the product and the door lock.
- Suprema's standalone intelligent readers contain internal relays that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

Info

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

Fail Secure Lock

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



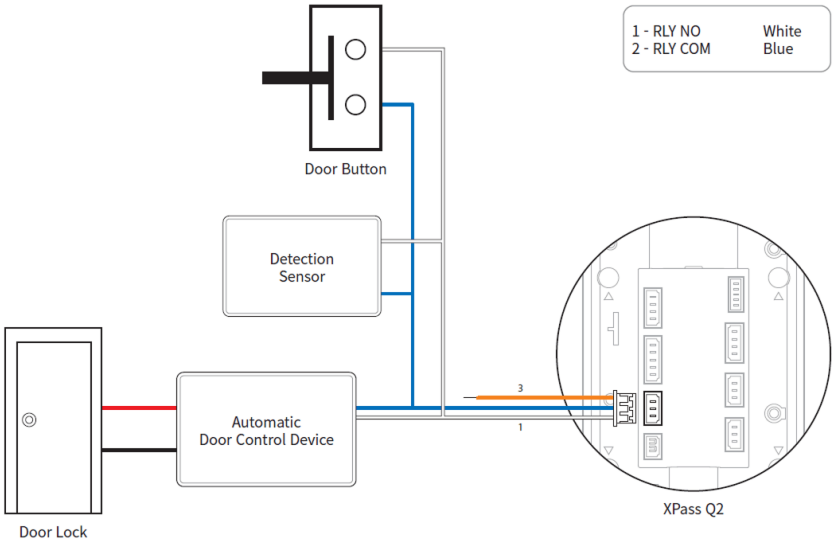
Caution

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

Info

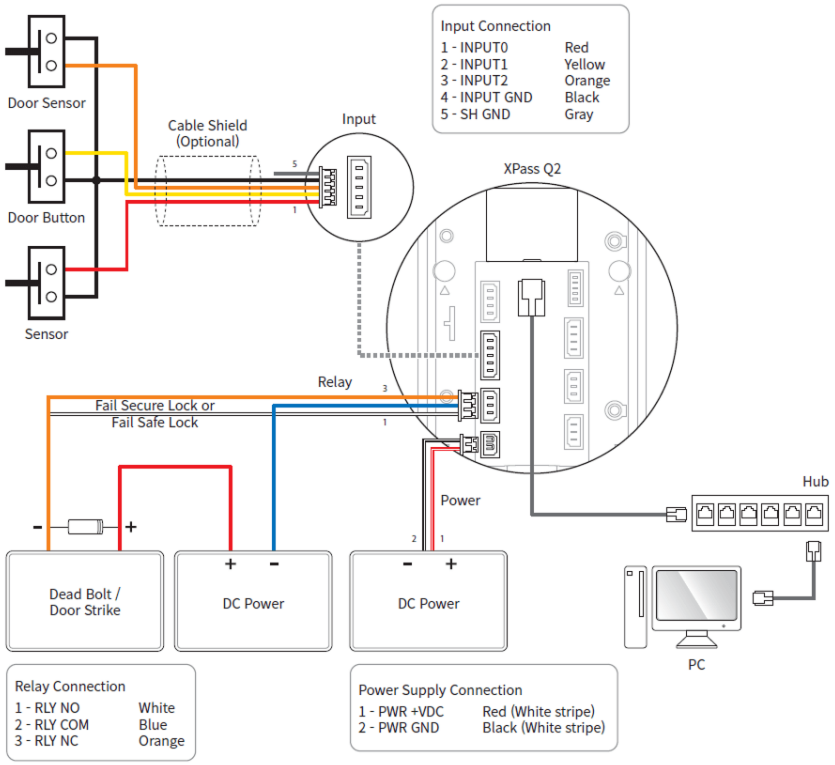
Take caution of the installation direction of the diode. Install the diode close to the door lock.

Automatic door connection



Connecting as a Standalone

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



Caution

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

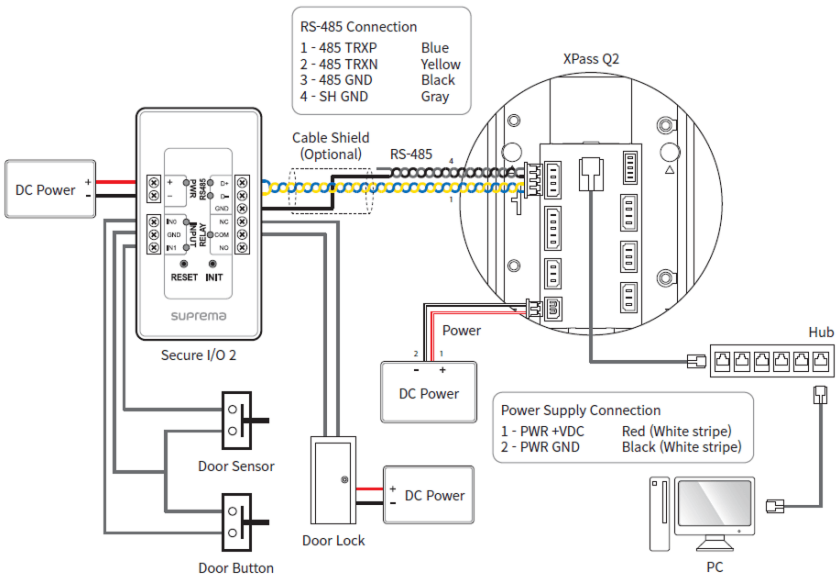
Info

- The device can be used as a multi-door controller with the slave devices with the RS-485 cable. The slave devices are used as dummy readers and authentication is performed in the master device.
- When this product operates as a master, only card or QR/Barcode authentication is available on the slave.
- Connect up to 31 slave devices to a master device.
- 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.

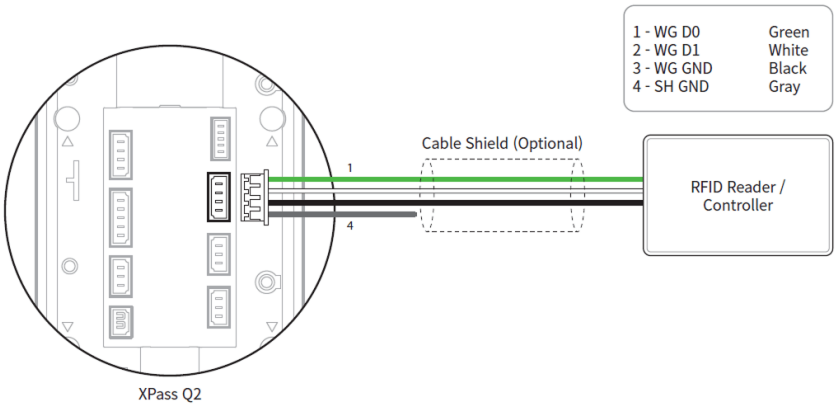


Info

- 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.
- When this product operates as a master, only card or QR/Barcode authentication is available on the slave.
- Connect up to 31 slave devices to a master device.
- For more information, contact the Suprema Technical Support Team.

Wiegand Connection

Use as a Wiegand input or output device.



Initialize Network Settings

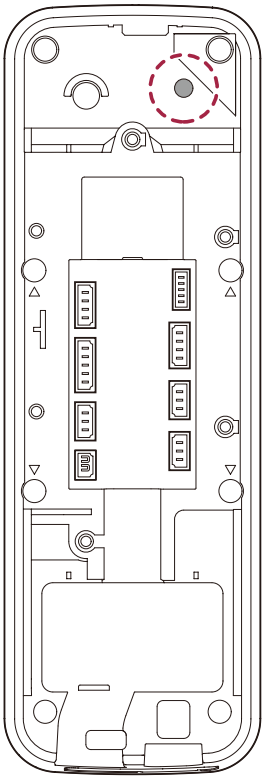
Initialize the device's network settings.

1. Power on.
2. Press the reset button until the device automatically reboots.
3. Connect the device using the initialized network information.
    - **TCP/IP Address**: DHCP address assignment (if DHCP address assignment fails, will be set to 169.254.x.x).
    - **Server Mode**: Disable
    - **RS-485**: Default, 115200 bps
4. Change the TCP/IP or RS-485 information.
5. Check if the network information is correctly set after turning the power off and on.

Factory reset

Delete all information stored on the device and initialize the settings.

1. Power on.
2. Quickly press the reset button three times.



3. Press the reset button once more when the device's LED blinks green.

Info

You can only use Factory Default when the root certificate is stored on the device.

Firmware upgrade

You can connect a USB memory stick to upgrade the firmware.

1. Save the firmware file to a USB memory stick for upgrade.

   Info
   It is recommended to save only one firmware file on the USB memory stick for the upgrade.

2. Connect the USB memory stick to the device.

   Info
   Authentication is temporarily suspended while the USB memory is being read.

3. When the LED/buzzer indicates an authentication request, authenticate with an administrator credential.

   Info

   - Register the administrator on BioStar X for the device. You cannot proceed with the firmware upgrade if an administrator is not registered on the device. For detailed instructions on how to register an administrator, please refer to the BioStar X Administrator Guide.
   - Only one authentication attempt is allowed per USB memory insertion.
   - If authentication fails, the LED/buzzer indicates the failure and USB reading ends. Disconnect the USB memory and reconnect it to the device.

4. After successful administrator authentication, the device performs a firmware upgrade and indicates the upgrade with the LED.

   Info
   If the firmware file is missing or corrupted, the upgrade does not proceed and the LED/buzzer indicates failure.

5. The device restarts automatically after the firmware upgrade is complete.

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

Product Specifications

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

Credentials

RF Card	**125kHz EM & 13.56MHz MIFARE, MIFARE Plus, DESFire, DESFire EV1/EV2/EV3, FeliCa**
RF Read Range[1)]	**EM/MIFARE/DESFire: 50 mm, FeliCa: 30 mm**
Mobile	**NFC, BLE**
QR/Barcode[2)]	**Supported**[3)]
QR/Barcode Read Range[4)]	• **QR code: 5 ~ 15 cm** • **Barcode: 5 ~ 9 cm**

General

Model Name	**XPQ2-DB, XPQ2-DPB**	
CPU	**1.2 GHz Single Core**	
Memory	**8 GB Flash + 256 MB RAM**	
Crypto Chip	**Supported**	
LED	**Multi-color**	
Sound	**Multi-tone Buzzer**	
Operating Temperature	**XPQ2-DB**	**-20 °C ~ 60 °C**
	XPQ2-DPB	• **DC Power: -20 °C ~ 60 °C** • **PoE Power: -20 °C ~ 50 °C**
Storage Temperature	**-40 °C ~ 70 °C**	

Operating Humidity	**0 % ~ 95 %, non-condensing**	
Storage Humidity	**0 % ~ 95 %, non-condensing**	
Camera	**1 Camera (QR only)**	
Dimensions (W x H x D)	**Device**	**50 x 150 x 40.2 (mm)**
	Bracket	**41.7 x 140.6 (mm)**
Weight	**Device**	• **XPQ2-DB: 208 g** • **XPQ2-DPB: 213 g**
	Bracket	**40 g (including washers and bolts)**
IP Rating	**IP65**	
Authentication	**CE, UKCA, KC, FCC, IC, RCM, SIG, RoHS, REACH, WEEE, EAC, TELEC**	

Capacity

Max. User	**200,000**[5)]
Max. Credentials (1:N)	**Card: 200,000**
Max. Credentials (1:1)	**Card: 200,000**
Max. Text logs	**1,000,000**

Interface

Ethernet	**Supported (10/100 Mbps, auto MDI/MDI-X)**
Network Protocol	**TCP, UDP**
RS-485	**1 ch Master / Slave (Selectable)**

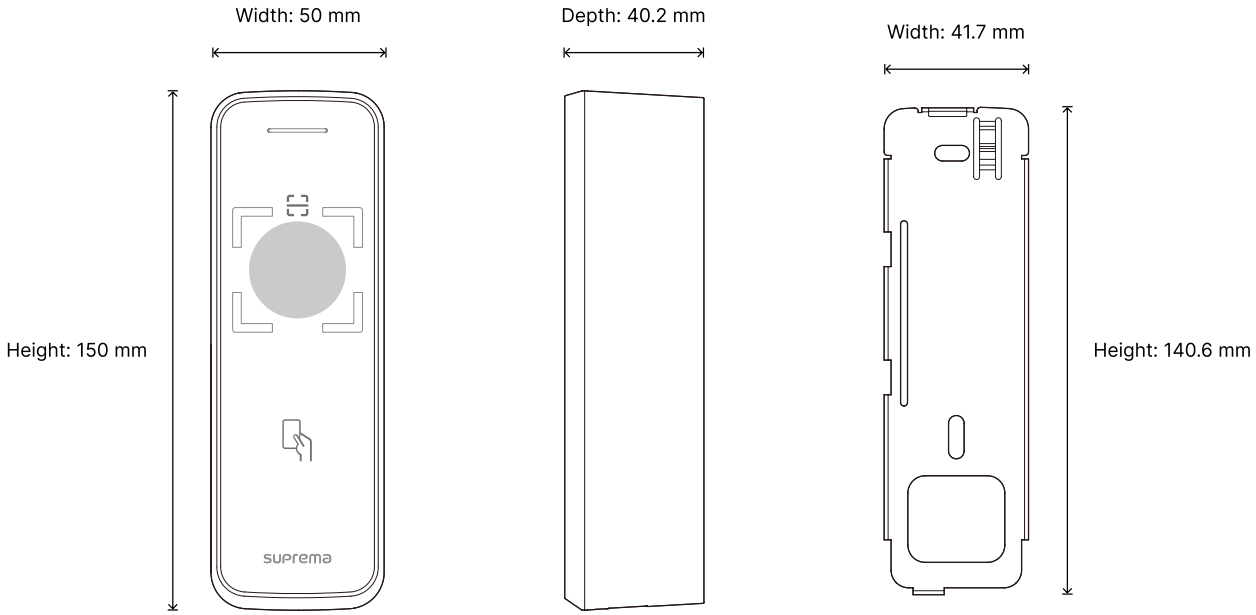
RS-485 Communication Protocol	**OSDP V2 compliant**	
Wiegand	**1 ch Input / 1 ch Output (Selectable)**	
Input	**3 ch Inputs**	
Relay	**1 relay**	
PoE	**XPQ2-DB**	**Not supported**
	XPQ2-DPB	**Supported (IEEE 802.3af compliant)**
USB	**USB 2.0 (Type C), only FW-Upgrade**	
USB Expansion Port	**Supported**	
Tamper	**Supported**	

Electrical

Power	**12 Vdc**	• **DC OUT not used Consumption Current: Max. 0.5 A** • **DC OUT used Consumption Current: Max. 2.6 A**
	24 Vdc	• **DC OUT not used Consumption Current: Max. 0.3 A** • **DC OUT used Consumption Current: Max. 1.4 A**
Power Output	**12 Vdc**	• **Reader: Max. 0.5 A** • **Lock: Max. 1.2 A**
	24 Vdc	• **Reader: Max. 0.25 A** • **Lock: Max. 0.6 A**
	PoE (12V out)	• **Reader: 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



Weight
- XPQ2-DB: 208 g
- XPQ2-DPB: 213 g

Weight: 40 g
(Including washer and bolt)

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

2) Supports QR codes with up to 32 ASCII characters.

3) Using a wider range of QR/Barcode authentication requires the Camera QR license. For detailed information on device licenses, please refer to the BioStar X Administrator Guide.

- Barcode types supported by the Camera QR license: QR Code, DataMatrix, Aztec, Micro QR Code, PDF417, Code39, Code128, UPC-A, UPC-E, EAN-8, EAN-13

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

5) 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: -1.83 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

- This product's software was created by modifying the Linux kernel, and the Linux kernel is licensed under the GPL. For more information about the GPL license, see the GNU General Public License.
- The uclibc library included in this product follows the LGPL. For more information about the LGPL license, see the GNU Lesser General Public License.
- This product uses the “OpenSSL”, which is licensed under the OpenSSL and Original SSLeay licenses. For more information about the OpenSSL and Original SSLeay licenses, please see the OpenSSL License and Original SSLeay License.
- ZXing included in this product follows the Apache License. For more information about the Apache license, please see the Apache License.
- The source modified based on Linux kernel 5.x and uclibc library included in this product can be downloaded by contacting the Suprema Technical Support Team.

Suprema Inc.

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

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

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

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