# BioLite N2 Suprema CLUe

## USER GUIDE

Version 1.02

English
EN 102.00.BLN2SC

suprema
SECURITY & BIOMETRICS

# CONTENTS


## Safety Instructions 4

Compliance Information 4

## Getting Started 8

Components 8

Name and function of each part 9

Correct fingerprint input method 11

## Installation 13

Fixing the bracket and the product 13

Power supply connection 16

Network Connection 17

Input connection 18

Relay Connection 19

Connecting as a Standalone 22

Connecting to Secure I/O 2 23

Wiegand Connection 25

## How to Use 26

Admin Menu 26

User 27

Authentication 29

Settings 34

Event Logs 39

## Troubleshooting 41

Check items before reporting a malfunction 41

## Product Specifications 43

Credentials 43

General 43

Capacity 44

Interface 45

Electrical 45

Dimensions and Weight 46

## Regulatory Information 47

FCC Compliance Information 47

IC information 48

EU Declaration of Conformity (CE) 48

## Appendices 49

Disclaimers 49

Copyright Notice 50

Open Source License 50

# 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 the product on a wall, do not seal around the product with silicone or similar materials.**

- 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.

**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 ~ 50 °C (BLN2-PAB: -10 °C ~ 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.**

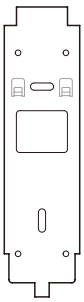
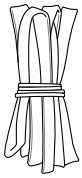
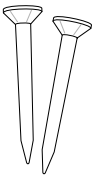
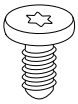
- The device may malfunction.

> **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.

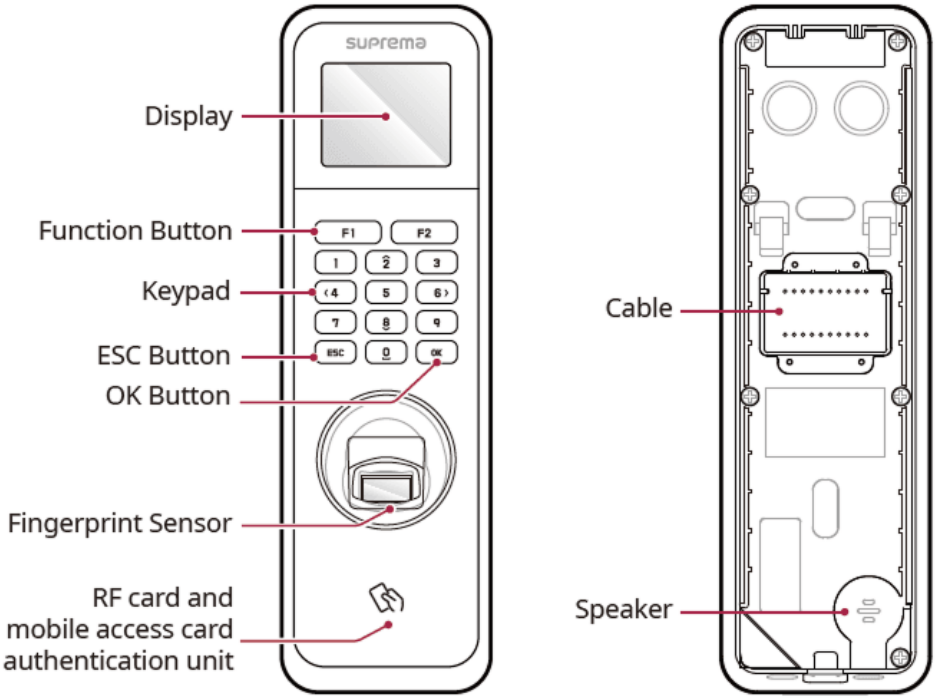
## Components

| | | |
|---|---|---|
|  |  |  |
| BioLite N2 | Wall Bracket | Shrink Tube |
|  |   |   |
| Fixing Screws x2 | Quick Guide | Open Source Software Guide |
|  |  |  |
| Bracket Fixing Screw (Star Shaped) | 120 Ω Resistor | Diode |

**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.

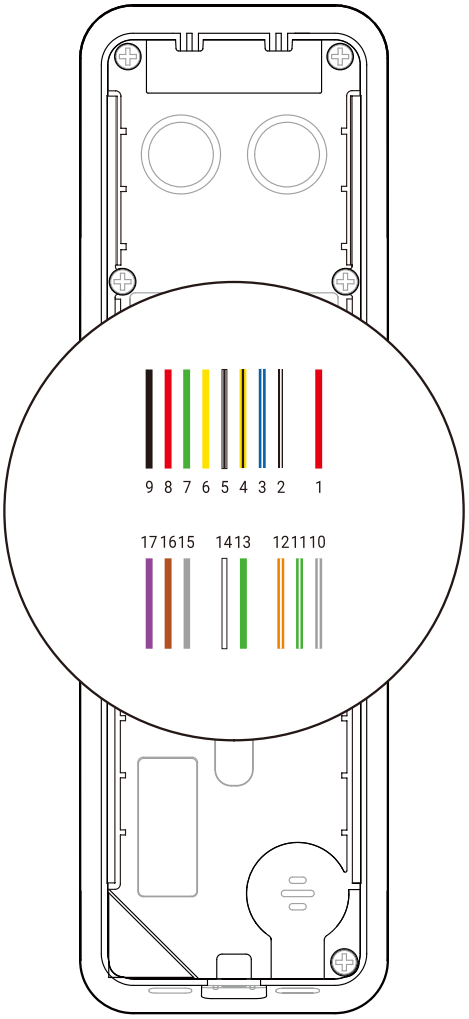
# Name and function of each part




- **Display**: Provides a UI for operation.
- **Feature Button**: Used for attendance key, text modification, etc.
- **Keypad**
  - **0-9**: Used to input numbers or characters.
  - **2, 4, 6, 8**: Used to navigate to the desired item.
- **OK Button**: Used to select attendance mode and save settings. If the work code is set, you can press and hold to change the user's work code.
- **ESC Button**: Used to open the menu, go back to the previous screen, and cancel input.
- **Fingerprint Recognition Unit**: The part that recognizes the fingerprint for access.
- **RF card and mobile access card authentication unit**: Part to scan a RFID card or mobile access card for entrance.
- **Cable**

  Power / RS-485 / Ethernet / Relay / Wiegand Input/Output / Input
- **Speaker**: Delivers sound.

## Cable

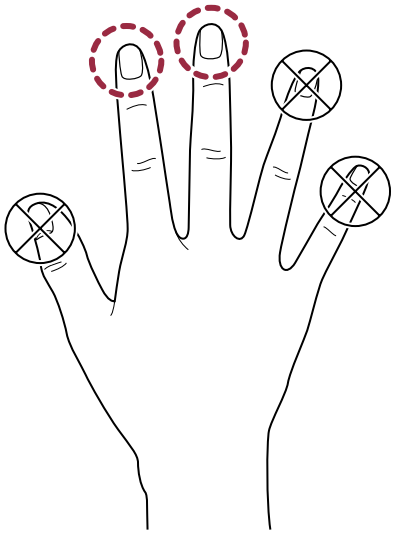



| Pin | Name | Color |
|---|---|---|
| 1 | PWR +VDC | Red |
| 2 | PWR GND | Black (White Stripe) |
| 3 | 485 TRXP | Blue (White Stripe) |
| 4 | 485 TRXN | Yellow (Black Stripe) |
| 5 | 485 GND | White (Black Stripe) |
| 6 | ENET RXN | Yellow |
| 7 | ENET RXP | Green |
| 8 | ENET TXN | Red |
| 9 | ENET TXP | Black |
| 10 | RLY NO | Gray (White Stripe) |
| 11 | RLY COM | Green (White Stripe) |
| 12 | RLY NC | Orange (White Stripe) |
| 13 | WG D0 | Green |
| 14 | WG D1 | White |
| 15 | INPUT GND | Gray |
| 16 | INPUT1 | Brown |
| 17 | INPUT0 | Purple |

# Correct fingerprint input method

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.

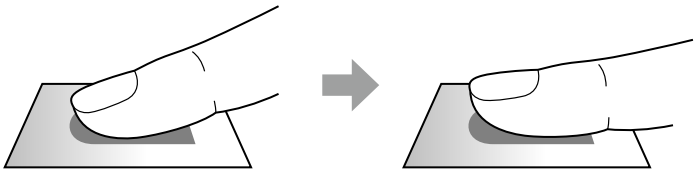
## Selecting a finger for fingerprint input



- 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

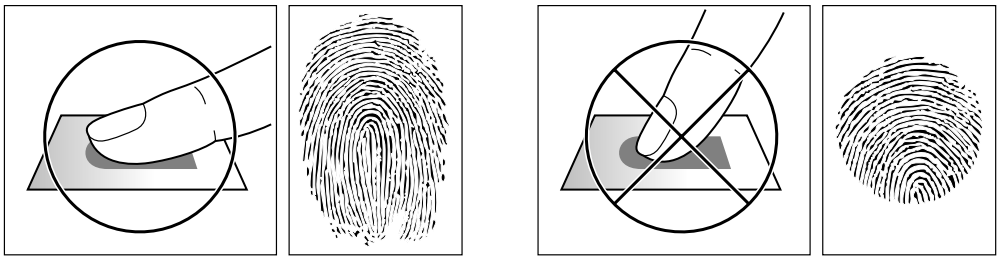
1. When the screen displays "Please input your fingerprint," place the finger you want to enroll on the fingerprint recognition unit and gently press it so that the fingerprint is authenticated well.



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.

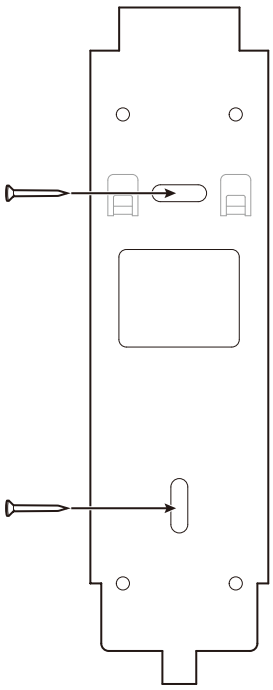
- If the finger is smeared with water or sweat, dry off the finger and then scan the finger.
- If the finger is too dry, blow your breath on the fingertips and then scan the finger.
- If the finger has a cut, enroll the fingerprint of another finger.
- Since the initially enrolled fingerprint is often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

# Installation

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

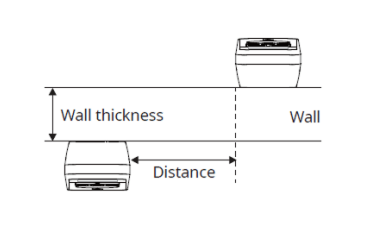
## Fixing the bracket and the product

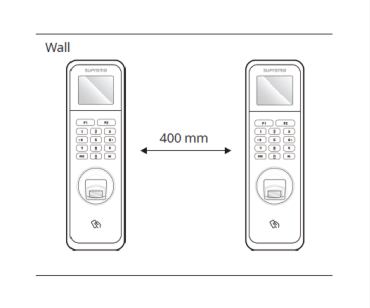
1. Secure the bracket tightly using the fixing screws at the location where the product will be mounted.



**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.

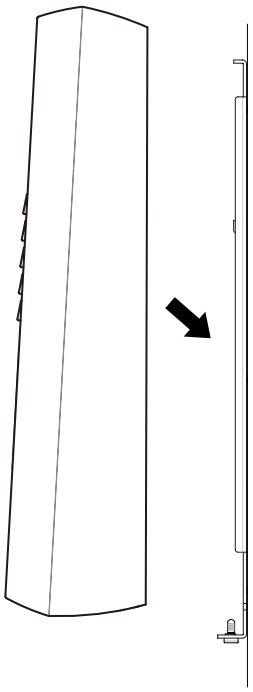


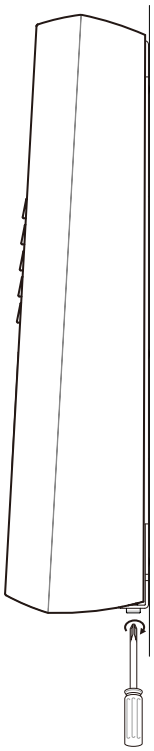

| Wall thickness | Distance |
|---|---|
| 100 mm | 350 mm |
| 120 mm | 350 mm |
| 150 mm | 300 mm |

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

2. Mount the product on the fixed bracket.



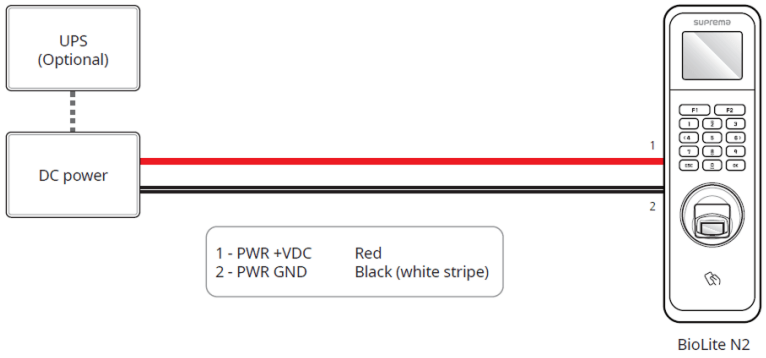
3. Rotate the fixing screws to assemble the product with the bracket.



**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**

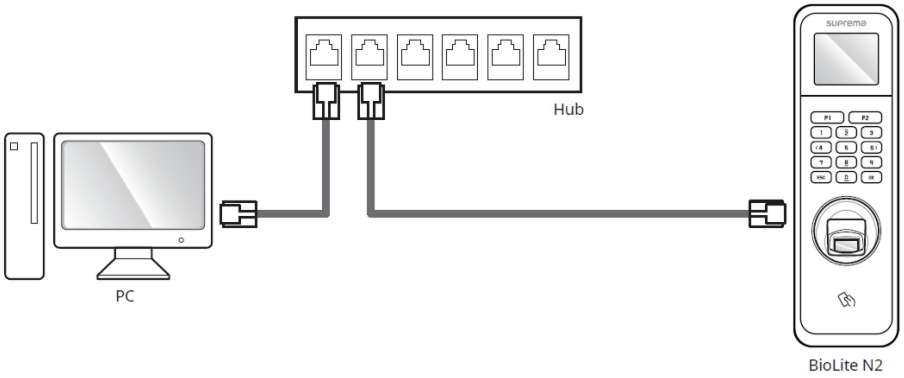
- Use the IEC/EN 62368-1 approved power adapter that supports higher power consumption than the product. If you wish to connect and use another device to the power supply adapter, you should use an adapter with a current capacity which is the same or larger than the total power consumption required for 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.

# 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.



### Network ports and services

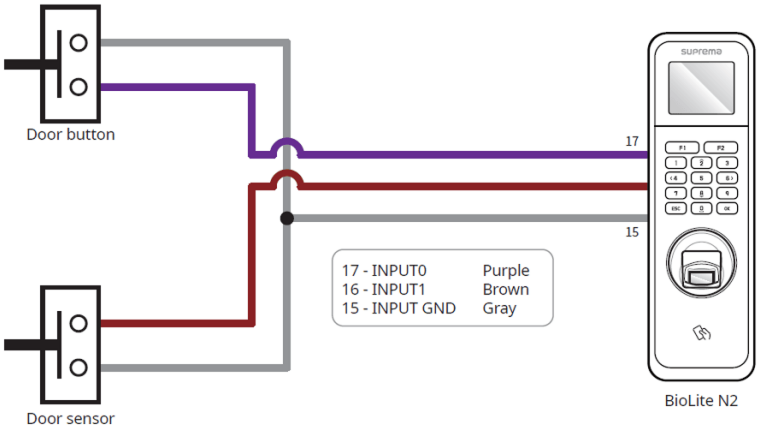
This device uses the following ports for network communication and stable service operation.

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

**Info**

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

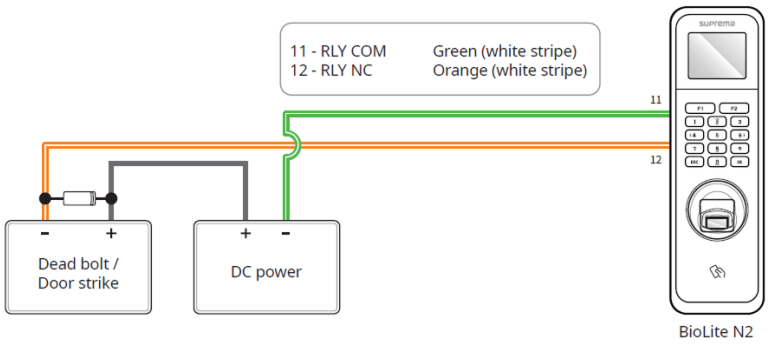
# Input connection



# Relay Connection

## Fail Safe Lock

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




**Caution**

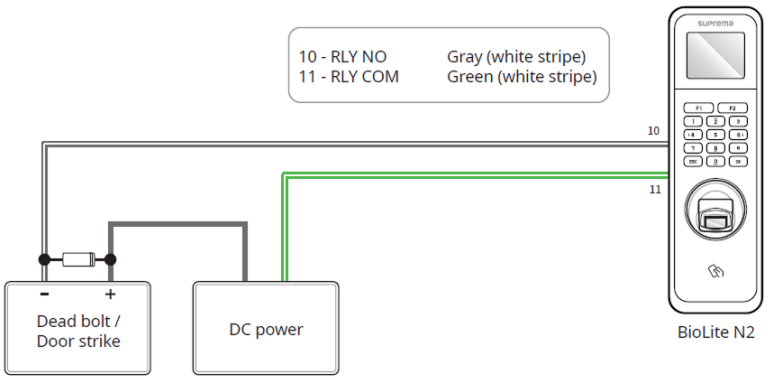
- Install a diode at both sides of the door lock wire as shown in the figure to protect the relay from the reverse current, which occurs when the door lock operates.
- Use a separate power supply for the product and the door lock.
- Suprema's standalone intelligent readers contain internal relays that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

**Info**

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

## Fail Secure Lock

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



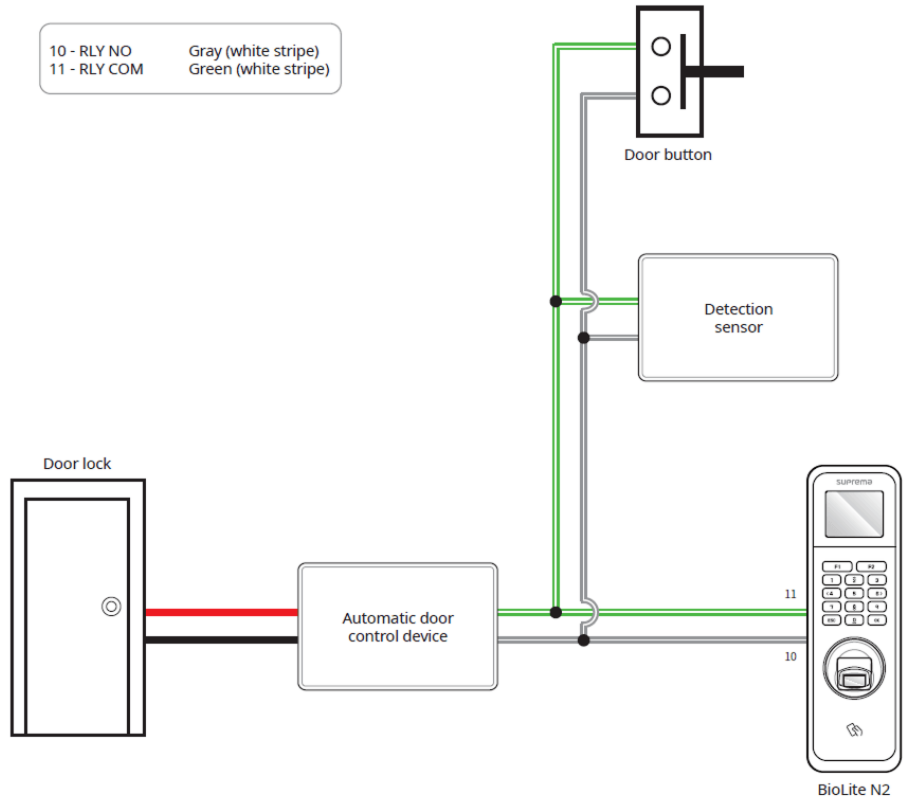

**Caution**

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

**Info**

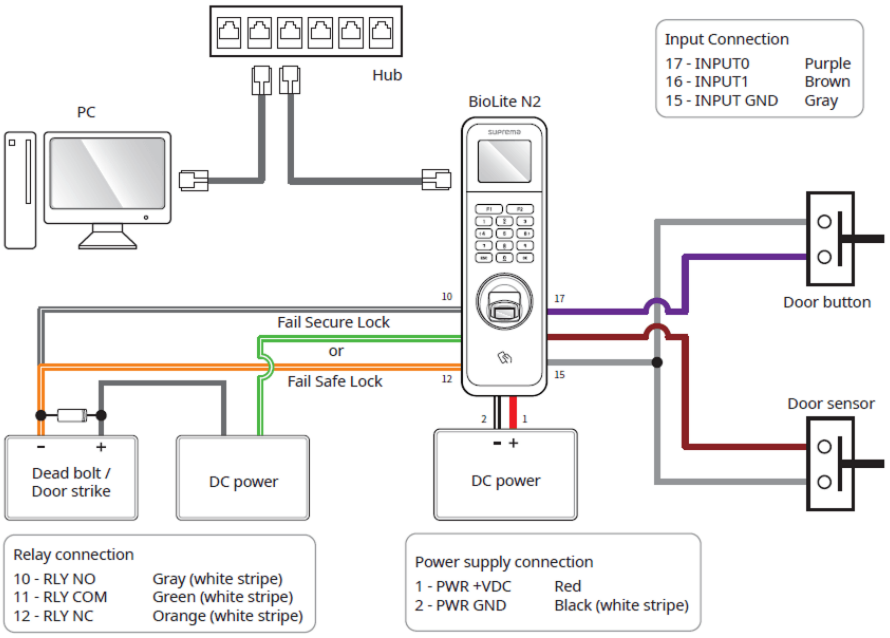
Take caution of the installation direction of the diode. Install the diode close to the door lock.

## Automatic door connection



# Connecting as a Standalone

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




**Caution**

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

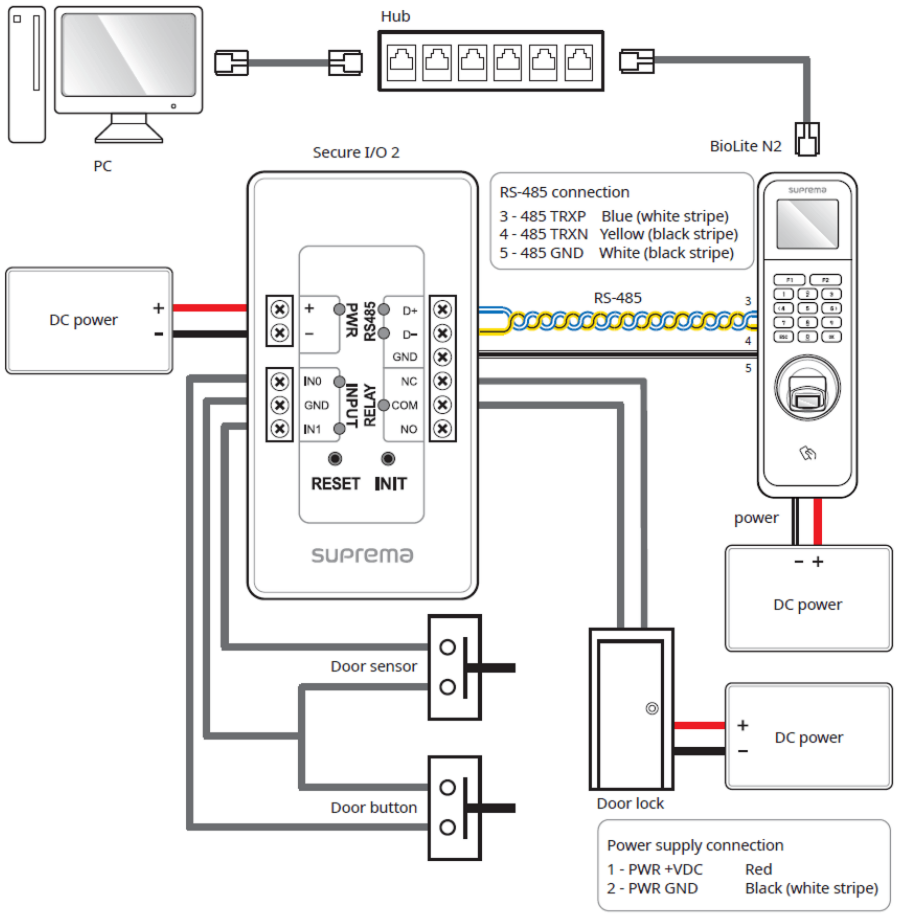
**Info**

- The device can be used as a multi-door controller with the slave devices with the RS-485 cable. The slave devices are used as dummy readers and authentication is performed in the master device.
- If XPass or XPass 2 is connected to the master device, only card authentication can be used.
- The maximum number of slave devices available to connect varies according to the authentication method, number of users, and number of devices. Also note that the number of slave devices affects the authentication performance.
- Connect up to 31 slave devices to a master device. The bandwidth of RS-485 allows for up to 7 fingerprint authentication devices to be connected.
- For more information, contact the Suprema Technical Support Team.

# Connecting to Secure I/O 2

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

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

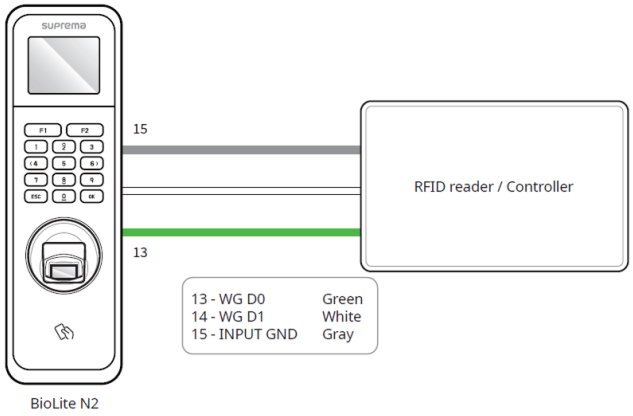


**Info**

- The device can be used as a multi-door controller with the slave devices with the RS-485 cable. The slave devices are used as dummy readers and authentication is performed in the master device.
- If XPass or XPass 2 is connected to the master device, only card authentication can be used.
- 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.



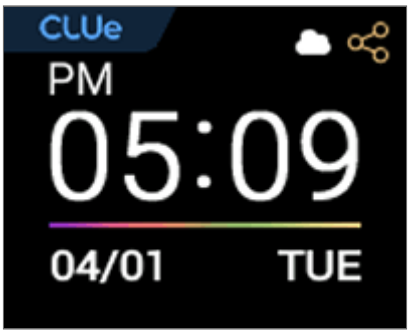
# How to Use

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.

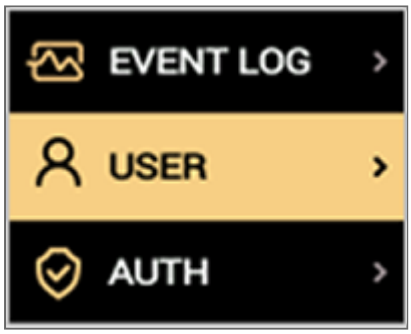
### Top icon




| Name | Feature description |
|---|---|
| (Connecting to Suprema CLUe) | Icon indicating that the device is connecting to Suprema CLUe |
| (Suprema CLUe) | Icon indicating that the device is connected to Suprema CLUe |
| (RS-485) | Icon indicating that RS-485 communication is connected |
| (TCP/IP) | Icon indicating the TCP/IP communication connection status |

### Full menu

1. Press **ESC**, enter the password, and access the menu.
2. Select your desired menu.



> **Info**
>
> If **Menu Password** is not set, press **ESC** to open the menu screen. For details on how to set the password, refer to Menu password.

# User

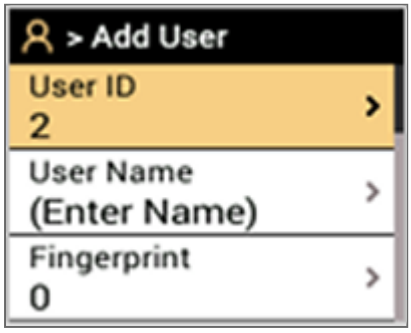
Describes how to register, edit, delete, and manage users.

> **Info**
>
> When using Suprema CLUe mode, user enrollment, editing, and deletion are available only on the Suprema CLUe server, not on the device.

## Registering user information

You can register user information that includes biometric authentication data.

1. Press **ESC**, enter the password, and access the menu.
2. Select **USER** → **Add User** and then press **6**.




3. Select the desired item and press **4** or **6** to set it. Press **OK** to register user information.
   - **ID**: Enter a number between 1 and 4294967294 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.
   - **Name**: You can enter a username using numeric and function buttons.
   - **Fingerprint**: You can enroll a fingerprint for user authentication. After scanning the fingerprint of the finger to be enrolled, scan the same finger's fingerprint once more. Select the fingerprint to be deleted and press **4** to delete the fingerprint, or press **6** to scan the fingerprint again. To add more fingerprints, select **+ Add Finger** and then press **6**.
   - **Card**: You can enroll a card for user authentication. Scan the card to be assigned to the user at the RF card recognition unit.
   - **PIN**: You can enter the PIN you want to use. After entering the desired PIN, enter the PIN again for confirmation. 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.
> – **Normal User**: This is a regular user level and cannot access the menu.
> – **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**.

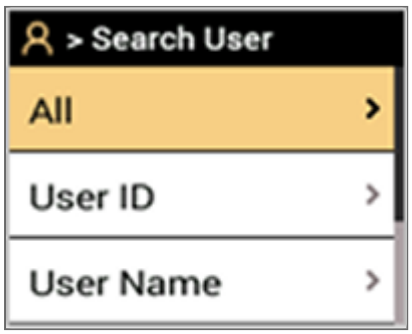
- **Start Date**: You can set the date to start using the user account.
- **Expiration Date**: You can set the date to stop using the user account.
- **1:1 Security Level**: You can set the security level for 1:1 authentication.
- **Duress**: You can select the fingerprint number to be used as a threat fingerprint. At least 2 fingerprints must be enrolled to use this function.
- **Private Auth Mode**: You can change the authentication method for each user.

4. Press **OK** to save the settings.

## 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. Press **ESC**, enter the password, and access the menu.
2. Select **USER** → **Search User** and then press **6**.
3. Select your search terms. You can search for users using **All**, **ID**, **Name**, **Fingerprint**, **Card**.




4. Select the user you want to modify and then press **6**. Refer to Registering user information to modify the information.
   - To delete a user, select **4** and then press **OK**.

> **Info**
> **Access Group** can be enrolled on the Suprema CLUe server.

### Delete All Users

You can delete all registered users at once.

1. Press **ESC**, enter the password, and access the menu.
2. Select **USER** → **Delete All Users** and then press **6**.
3. Press **OK** to delete all registered users.

### View User Usage

You can view the number of enrolled users, fingerprints, and cards at a glance.

1. Press **ESC**, enter the password, and access the menu.
2. Select **USER** → **User Usage** and then press **6**. User usage information appears.

## Authentication

Describes the supported authentication methods and authentication procedures.

> **Info**
> If you use Suprema CLUe mode, you can set the authentication mode only on the Suprema CLUe server, not on the device.

### Authentication mode

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

### Fingerprint authentication mode

You can set schedules for each authentication method that uses fingerprints.

1. Press **ESC**, enter the password, and access the menu.
2. Press **6** after selecting **AUTHENTICATION** → **Auth Mode** → **Fingerprint Mode**.
3. Select the desired item and press **4** or **6** to set the schedule.




- : This mode uses only fingerprints.
- + : This mode authenticates with a fingerprint followed by entering a PIN.

4. Press **OK** to save the settings.

> **Info**
> **Schedule** can be set on the Suprema CLUe server. If you have no scheduled settings, you can only select **Never** and **Always**.

## Card Authentication Mode

You can set schedules for each authentication method that uses cards.

1. Press **ESC**, enter the password, and access the menu.
2. Press **6** after selecting **AUTHENTICATION** → **Auth Mode** → **Card Mode**.
3. Select the desired item and press **4** or **6** to set the schedule.




- : This mode uses only cards.
- + : This mode authenticates with a card followed by fingerprint authentication.
- + : This mode uses a card for authentication followed by entering a PIN.
- + / : This mode authenticates with a card followed by either fingerprint or PIN entry.
- + + : This mode uses a card followed by both fingerprint authentication and PIN entry.

4. Press **OK** to save the settings.

> **Info**
>
> **Schedule** can be set on the Suprema CLUe server. If you have no scheduled settings, you can only select **Never** and **Always**.

## ID Authentication Mode

You can set schedules for each authentication method that uses IDs.

1. Press **ESC**, enter the password, and access the menu.
2. Press **6** after selecting **AUTHENTICATION** → **Auth Mode** → **ID Mode**.
3. Select the desired item and press **4** or **6** to set the schedule.




- + : This mode authenticates with an ID followed by a fingerprint.
- + : This mode uses an ID followed by entering a PIN.
- + / : This mode uses an ID followed by either fingerprint authentication or entering a PIN.
- + + : This mode uses an ID followed by both fingerprint authentication and entering a PIN.

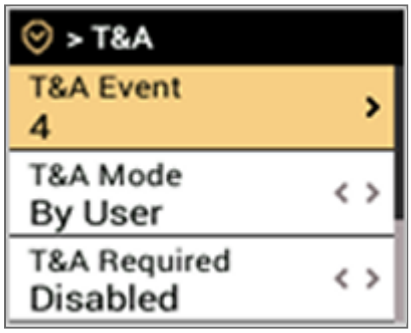
4. Press **OK** to save the settings.

> **Info**
>
> **Schedule** can be set on the Suprema CLUe server. If you have no scheduled settings, you can only select **Never** and **Always**.

# Attendance Mode

You can set how to register T&A mode.

1. Press **ESC**, enter the password, and access the menu.
2. Select **AUTHENTICATION** → **T&A**, then press **6**.
3. Select the desired item and press **4** or **6** to set the schedule.




- **T&A Event**: You can check attendance events.
- **T&A Mode**: Set how to use attendance mode.
- **T&A Required**: Set to require a user to select a T&A event when authenticating. Setting **Enabled** allows you to require selecting a time and attendance event when authenticating.
- **T&A Fixed**: You can configure to use only time and attendance events selected by an administrator. Available when **T&A Mode** is set to **Fixed**.
- **Job Code**: Set whether to use the job code.

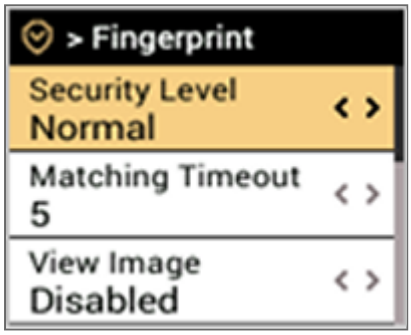
4. Press **OK** to save the settings.

> **Info**
>
> Set **Job Code** to **Enabled** to change the user's action code. Long press **OK** then authenticate to select the desired work code.

## Fingerprint Settings

You can change the settings for fingerprint authentication.

1. Press **ESC**, enter the password, and access the menu.
2. Press **6** after selecting **AUTHENTICATION** → **Fingerprint**.
3. Select the desired item and press **4** or **6** to set the schedule.




- **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.
- **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.
- **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.

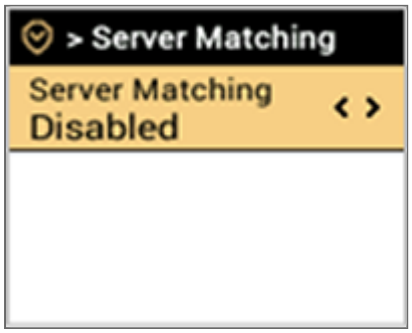
- **Sensor Mode**: Set to **Auto On** to turn on the fingerprint sensor when it detects the user's finger. When set to **Always On**, the sensor remains on even when not scanning fingerprints.
- **Advanced Enrollment**: Assess the quality of scanned fingerprints to save high-quality fingerprint information. Enable to notify the user when fingerprint quality is low, helping them scan fingerprints correctly.
- **Duplicate Check**: Check for duplicate fingerprints when enrolling.

4. Press **OK** to save the settings.

## Server matching

When you enable server matching, the device authenticates users or Suprema CLUe users according to the set authentication mode. It can be used when the device has too much user information or when the device is installed outside.

1. Press **ESC**, enter the password, and access the menu.
2. Press **6** after selecting **AUTHENTICATION** → **Server Matching**.




3. Press **4** or **6** to change the settings.
4. Press **OK** to save the settings.

> **Info**
>
> - If you use **Server Matching**, enable server matching on both the device and the Suprema CLUe server.
> - If you use Suprema CLUe mode, **Server Matching** is enabled automatically.

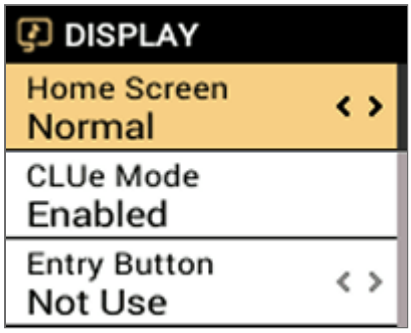
# Settings

Provides instructions on how to set system and device configurations.

## Display & Sound

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

1. Press **ESC**, enter the password, and access the menu.
2. Select **DISPLAY & SOUND** and press **6**.
3. Select the desired item and press **4** or **6** to set the schedule.




- **Home Screen**: You can choose items to display in the background of the home screen.
- **CLUe Mode**: Indicates the CLUe mode status.
- **Entry Button**: Select whether to use the entry button.
- **Backlight Timeout**: Set the time (sec) to turn off the lighting of the screen.
- **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.
- **Language**: You can select the language that will be displayed on the screen.
- **Voice Instruction**: You can use voice guidance instead of notification tones.
- **Volume**: Set the volume.

4. Press **OK** to save the settings.

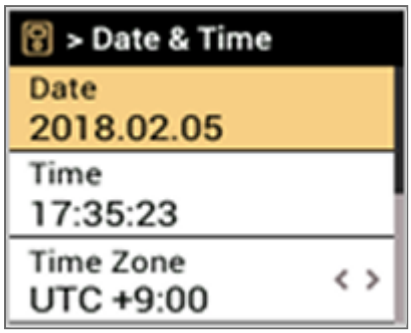
## Device

### Date & Time

You can set date and time. Set the date and time accurately in order to collect accurate log data.

1. Press **ESC**, enter the password, and access the menu.
2. Select **DEVICE** → **Date & Time** and press **6**.

3. Select the desired item and press **4** or **6** to set the schedule.




   - **Date**: You can check the current date. To modify it manually, disable **Time Sync**.
   - **Time**: You can check the current 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 **24-Hour** and **AM/PM**.

4. Press **OK** to save the settings.

## Daylight saving time

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

1. Press **ESC**, enter the password, and access the menu.
2. Select **DEVICE** → **Daylight Saving Time** and press **6**.
3. Select the desired item and press **4** or **6** to change settings.
   - **Name**: Set the name of daylight-saving time.
   - **Start Month** / **Start Week** / **Start Day** / **Start Time**: Set details of when daylight-saving time begins.
   - **End Month** / **End Week** / **End Day** / **End Time**: Set details of when daylight-saving time ends.
4. Press **OK** to save the settings.

## Relay

You can set the input ports of **Open Time** and **Exit Button** on the device. Useful when used as a standalone.

1. Press **ESC**, enter the password, and access the menu.
2. Select **DEVICE** → **Relay** and press **6**.
   - **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.

3. Press **OK** to save the settings.

## Device Information

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

1. Press **ESC**, enter the password, and access the menu.
2. Select **DEVICE** → **Device Info** and press **6**. You can check the information of **Model Name**, **Device ID**, **Serial No.**, **HW**, **FW**, **Kernel**, **MAC**.
3. Press **ESC** to return to the previous screen.

## Memory usage

View the status of memory usage.

1. Press **ESC**, enter the password, and access the menu.
2. Select **DEVICE** → **Memory Usage** and press **6**. You can view the memory usage status of the device.
3. Press **ESC** to return to the previous screen.

## Secure Tamper

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

1. Press **ESC**, enter the password, and access the menu.
2. Select **DEVICE** → **Secure Tamper** and press **4** or **6** to change settings.
3. Press **OK** to save the settings.

## Restart device

The user can restart the device.

1. Press **ESC**, enter the password, and access the menu.
2. Select **DEVICE** → **Restart Device** and press **6**.
3. Press **OK** to restart the device. Press **ESC** to cancel.

## Restore default

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

1. Press **ESC**, enter the password, and access the menu.
2. Select **DEVICE** → **Restore Default** and press **6**.
   - **Reset All Settings**: Initializes all settings saved on the device. Press **OK** to initialize all device settings. Press **ESC** to return to the previous screen.

- **Quick Reset**: Initializes all settings except for network settings. Press **OK** to initialize all settings except for network settings. Press **ESC** to return to the previous screen.
- **Factory Default**: Deletes all information saved in the device and the root certificate, restoring settings to default.
- **Delete the Root Certificate**: Deletes the root certificate saved in the device.

3. If you proceed with **Restore Default**, the device will restart.

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

### User ID type

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

1. Press **ESC**, enter the password, and access the menu.
2. Select **DEVICE** → **User ID Type** and press **4** or **6** to change settings.
   - **Number**: You can enter a user ID with numbers only.
   - **Alphanumeric**: You can enter a user ID using alphanumeric characters and certain symbols `_` `-`.
3. Press **OK** to save the settings.

### Menu password

Set the device password.

1. Press **ESC**, enter the password, and access the menu.
2. Select **DEVICE** → **Menu Password**, and then press **6**.
3. Set the password, and press **OK** to save.

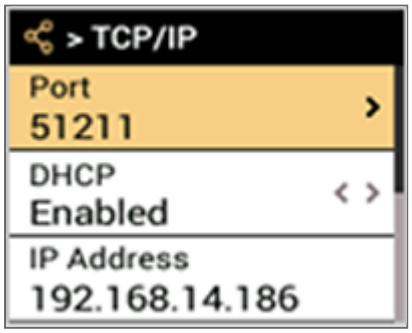
> **Info**
>
> - Set the device password to 4~16 digits.
> - Be careful not to lose the device password. If you lose the password, initialize the device to connect to it.

## Network

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

## TCP/IP

1. Press **ESC**, enter the password, and access the menu.
2. Select **NETWORK** → **TCP/IP** and press **6**.
3. Select the desired item and press **4** or **6** to change settings.



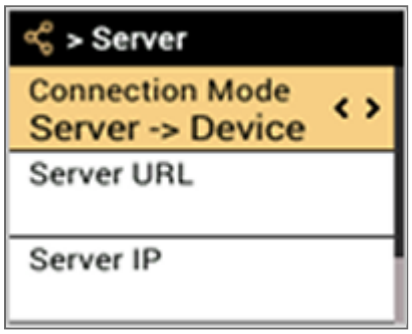

- **PORT**: You can set the ports of the device.
- **DHCP**: Set whether to use DHCP. If DHCP setting is disabled, the user can modify **IP Address**, **Gateway**, and **Subnet Mask**.
- **IP Address**: You can check the device's IP address. To modify, disable DHCP setting.
- **Gateway**: You can check 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**: You can set the domain name server address.
- **Ping Test**: Starts the Ping test.

> **Info**
> Select a DNS server below to run the Ping test.

4. Press **OK** to save the settings.

## Server

1. Press **ESC**, enter the password, and access the menu.
2. Select **NETWORK** → **Server** and press **6**.
3. Select the desired item and press **4** or **6** to change settings.



- **Connection Mode**: Selecting **Device → Server** sends a direct connection signal to the server with the information entered on the device. Users can input **Server URL**, **Server IP**, and **Server Port**.

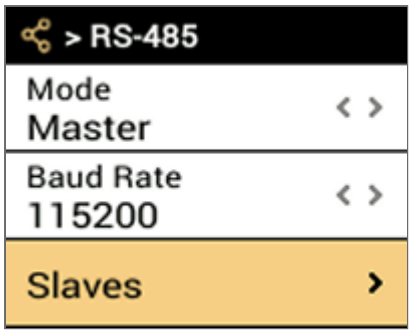
> **Info**
> When you use Suprema CLUe mode, the **Device → Server** setting is fixed.

- **Server URL**: You can enter **Server URL** instead of **Server IP**.
- **Server IP**: To connect to Suprema CLUe, enter `127.0.0.1`.
- **Server Port**: To connect to Suprema CLUe, enter `51212`.

4. Press **OK** to save the settings.

### Serial communication settings

1. Press **ESC**, enter the password, and access the menu.
2. Select **NETWORK → RS-485** and press **6**.
3. Select the desired item and press **4** or **6** to change settings.




- **Operation Mode**: You can select the RS-485 operation mode.
- **Baud Rate**: You can select the desired communication performance.
- **Slave**: Displays a list of devices connected as slaves. > **Search** and then press **6** to search for new slave devices and add them to the list automatically.

> **Info**
> The **Slave** menu is available only on the master device.

4. Press **OK** to save the settings.

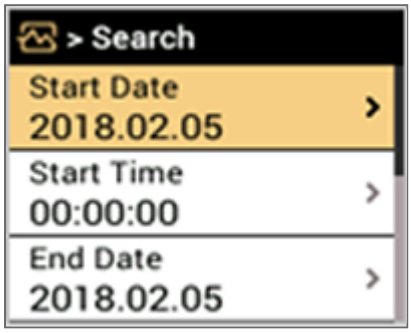
# Event Logs

Describes how to view event logs generated by the device.

## Search event logs

Set conditions to search logs.

1. Press **ESC**, enter the password, and access the menu.
2. Select **EVENT LOG** → **Search** and press **6**.
3. Select the desired item and press **6** to change the setting.




4. Set the search conditions and press **OK** to display the logs that match the conditions.
5. Press **ESC** to return to the previous screen.

## Delete all logs

You can delete all saved logs.

1. Press **ESC**, enter the password, and access the menu.
2. Select **EVENT LOG** → **Delete All Logs** and press **6**.
3. Press **OK** to delete all logs. Press **ESC** to cancel.

## View log usage

You can check the status of log usage.

1. Press **ESC**, enter the password, and access the menu.
2. Select **EVENT LOG** → **Log Usage** and press **6**.
3. You can check the log usage of the device.
4. Press **ESC** to return to the previous screen.

# 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.

- If you lose your 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.

### 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.

# Product Specifications

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

## Credentials

| | | |
|---|---|---|
| Biometric | **Fingerprint**<br>• **Image Dimension:272 x 320 pixels**<br>• **Image Bit Depth:8 bits, 256 grayscale**<br>• **Resolution:500 dpi**<br>• **Template:SUPREMA / ISO19794-2 / ANSI-378**<br>• **Extractor / Matcher:MINEX certified and compliant**<br>• **Live Fingerprint Detection:Supported (SW-based)** | |
| RF Card | **BLN2-OD, BLN2-ODB** | **125kHz EM & 13.56MHz MIFARE, MIFARE Plus, DESFire, DESFire EV1/EV2/EV3, FeliCa** |
| | **BLN2-OA, BLN2-OAB, BLN2-PAB** | **125kHz EM, HID Prox & 13.56MHz MIFARE, MIFARE Plus, DESFire, DESFire EV1/EV2/EV3, FeliCa, iCLASS SE/SR/Seos** |
| RF Read Range[1)] | **MIFARE/DESFire/HID iCLASS: 50 mm, EM/HID Prox/FeliCa: 30 mm** | |
| Mobile | **BLN2-ODB, BLN2-OAB, BLN2-PAB** | **NFC, BLE** |
| | **BLN2-OD, BLN2-OA** | **NFC** |

## General

| | |
|---|---|
| Model Name | **BLN2-ODB, BLN2-OAB, BLN2-PAB** |
| CPU | **1.2 GHz** |
| Memory | **4 GB Flash + 64 MB RAM** |
| Crypto Chip | **Supported** |

| | | |
|---|---|---|
| Display | **1.77" color TFT LCD** | |
| Display Resolution | **160 x 128 pixels** | |
| Sound | **16 bit** | |
| Operating Temperature | **BLN2-ODB, BLN2-OAB, BLN2-OD, BLN2-OA** | **-20 °C ~ 50 °C** |
| | **BLN2-PAB** | **-10 °C ~ 50 °C** |
| Storage Temperature | **BLN2-ODB, BLN2-OAB, BLN2-OD, BLN2-OA** | **-40 °C ~ 70 °C** |
| | **BLN2-PAB** | **-20 °C ~ 60 °C** |
| Operating Humidity | **0 % ~ 80 %, non-condensing** | |
| Storage Humidity | **0 % ~ 90 %, non-condensing** | |
| IP Rating | **IP65, IP67** | |
| Authentication | **CE, UKCA, KC, FCC, IC, RCM, BIS, SIG, RoHS, REACH, WEEE** | |

# Capacity

| | |
|---|---|
| Max. User | **10,000** |
| Max. Credentials (1:N) | **Fingerprint: 10,000** |
| Max. Credentials (1:1) | • **Fingerprint: 10,000**<br>• **Card: 10,000**<br>• **PIN: 10,000** |
| Max. Text logs | **1,000,000** |

# Interface

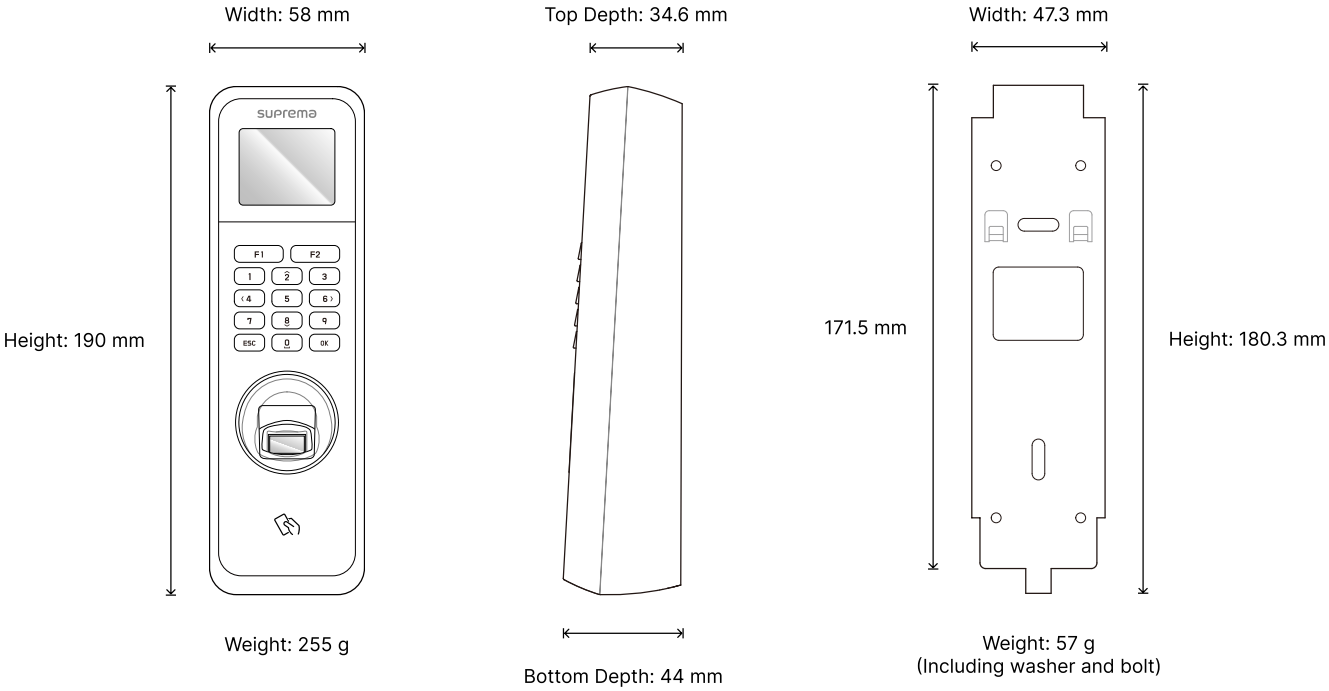
| | |
|---|---|
| Ethernet | **Supported (10/100 Mbps, auto MDI/MDI-X)** |
| Network Protocol | **TCP, UDP** |
| RS-485 | **1 ch Master / Slave (Selectable)** |
| RS-485 Communication Protocol | **OSDP V2 compliant** |
| Wiegand | **1 ch Input / 1 ch Output (Selectable)** |
| Input | **2 ch Inputs** |
| Relay | **1 relay** |
| Tamper | **Supported** |

# Electrical

| | | |
|---|---|---|
| Power | **12 Vdc** | **Current: Max. 0.4 A** |
| Switch Input VIH | • **Min.: 3 V**<br>• **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**<br>• **1 A @ 30 VDC Inductive load** |

# Dimensions and Weight




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

**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: -7.9 dBm
- Bluetooth frequency: 2402~2480 MHz
- NFC frequency: 129.2 MHz
- RFID frequency: 13.56 MHz

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

Suprema Inc.

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

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

# Appendices

Includes legal notices contained in the product.

## Disclaimers

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

# Copyright Notice

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

# Open Source License

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