BioStation 3

USER GUIDE

Version 1.09
English
EN 102.00.BS3

suprema
SECURITY & BIOMETRICS

CONTENTS

Safety Instructions 3

Instructional Icons 3

Introduction 6

Components 6

Name and Function of Each Part 7
- Cables and Connectors 9

Master Admin Settings 11

Correct Face Enrollment and Authentication Method 14

Note for QR Code Usage and Device License 15

Admin Menu 16

DASHBOARD 16

User 17

Registering User Information 17

Modifying User Information 19

Delete All Users 19

View User Usage 20

Authentication 21

Auth Mode 21
- Registering Auth Mode 21
- Modifying Auth Mode 22
- Delete Auth Mode 22

Operation 23

PIN 24

Auth Result Display Option 24

Face 25

T&A Mode 27

Settings 28

Display & Sound 28

Network 29
- Ethernet 29
- Wireless 30
- Server 31
- OSDP Setting 31

Devices 32
- Intercom 32
- License 33
- Relay 34
- Date & Time 35
- Daylight Saving Time 36
- Device Information 37
- Memory Information 38
- USB Memory 39
- Secure Tamper 39
- RTSP 40
- Master Admin 41
- Admin 2-step Authentication 42
- Restart Device 43
- Restore Default 43
- User ID Type 43

CONTENTS

Event Logs 44

Search Event Logs 44

Delete All Logs 44

View Log Usage 45

Troubleshooting 46

Product Specifications 47

Dimensions 49

Regulatory Information 50

Regulatory & Licenses 50

FCC Compliance Information 51

EU Declaration of Conformity (CE) 51

Appendices 52

Disclaimers 52

Copyright Notice 53

Open Source License 53

- GNU General Public License 54
- GNU Lesser General Public License 62
- OpenSSL License 65
- Original SSLeay License 66

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.

Instructional Icons

Warning: This symbol indicates situations that could result in death or severe injury.

Caution: This symbol indicates situations that may result in moderate injury or property damage.

Note: This symbol indicates notes or additional information.

Warning

Installation

When using a high-capacity power supply, please pay special attention to avoid miswiring.

- Miswiring may result in serious fire, electric shock, or product damage.

Do not install or repair the product arbitrarily.

- This may result in electric shock, fire, or product damage.
- Damages caused by any modifications or failure to follow installation instructions can void your manufacturer's warranty.

Do not install the product in a place with direct sunlight, moisture, dust, soot, or a gas leak.

- This may result in electric shock or fire.

Install the product in a well-ventilated and cool place away from direct sunlight to prevent overheating when installing it outside.

Do not place the product inside the sealed enclosure when installing it outside.

- It increases the internal temperature of the enclosure and this may result in electric shock, fire, or malfunction.

Do not install the product in a location with heat from an electric heater.

- This may result in fire due to overheating.

Install the product in a dry location.

- Humidity and liquids may result in electric shock or product damage.

Do not install the product in a location where it will be affected by radio frequencies.

- This may result in fire or product damage.

Operation

Keep the product dry.

- Humidity and liquids may result in electric shock, fire, or product damage.

Do not use damaged power supply adapters, plugs, or loose electrical sockets.

- Unsecured connections may cause electric shock or fire.

Do not bend or damage the power cord.

- This may result in electric shock or fire.

Caution

Installation

Please read this manual before installing the product to ensure a safe and correct installation.

When wiring the power cable and other cables, make sure to connect them with the power turned off for all devices involved.

- The product may malfunction.

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

Do not install the product under direct sunlight or UV light.

- This may result in product damage, malfunction, discoloration, or deformation.

Do not install the power supply cable in a location where people pass by.

- This may result in injury or product damage.

Do not install the product near magnetic objects, such as a magnet, TV, monitor (especially CRT), or speaker.

- The product may malfunction.

Keep the minimum distance between products when installing multiple products.

- The product may be affected by radio frequencies emitted by other products and the product may malfunction.

Use the IEC/EN 62368-1 approved power adapter that supports higher power consumption than the product. It is highly recommended to use the power adapter sold by Suprema.

- If the right power supply is not used, the product may malfunction.
- Refer to the Power in the product specifications for maximum current consumption specifications.

Use a separate power supply for the Secure I/O 2, electric lock, and the product.

- If connecting and using the same power supply, the product may malfunction.

Do not connect and use the power supply and Power over Ethernet (PoE+) simultaneously.

- The product may malfunction.

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). It is recommended to use the enclosure if the product is installed outside.

- The product may malfunction if the water-resistant and dust-resistant features are damaged.

When connecting PoE+ power, always use PoE+ or PoE++ standards only.

- Using standard PoE may cause unstable operation and can potentially damage the device permanently.

Caution

Operation

Do not drop the product or cause impacts to the product.

- The product may malfunction.

Do not disconnect the power supply while upgrading the firmware of the product.

- The product may malfunction.

Do not disclose the password to others and change it regularly.

- This may result in illegal intrusion.

Do not press buttons(touch pad) on the product by force or do not press them with a sharp tool.

- The product may malfunction.

Do not store your product in very hot or very cold places. It is recommended to use your product at temperatures from -20 °C to 50 °C.

- The product may malfunction.

When cleaning the product, mind the following.

- Wipe the product with a clean and dry towel.
- If you need to sanitize the product, moisten the cloth or the wipe with a proper amount of rubbing alcohol and gently clean all exposed surfaces. Use rubbing alcohol (containing 70 % Isopropyl alcohol) and a clean, non-abrasive cloth like lens wipe.
- Do not apply liquid directly to the surface of the product.

Do not use the product for anything other than its intended use.

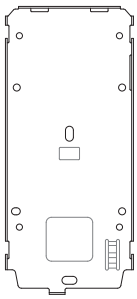
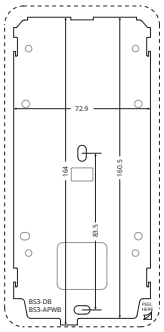
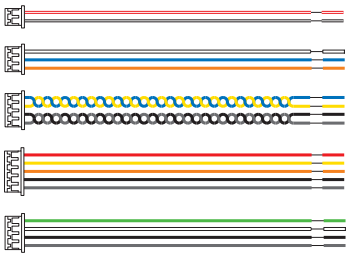
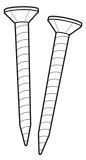
- The product may malfunction.

RTC Battery

Use of an unapproved or incorrect type of battery may result in a risk of explosion. Discard the battery according to the appropriate regional or international waste regulations.

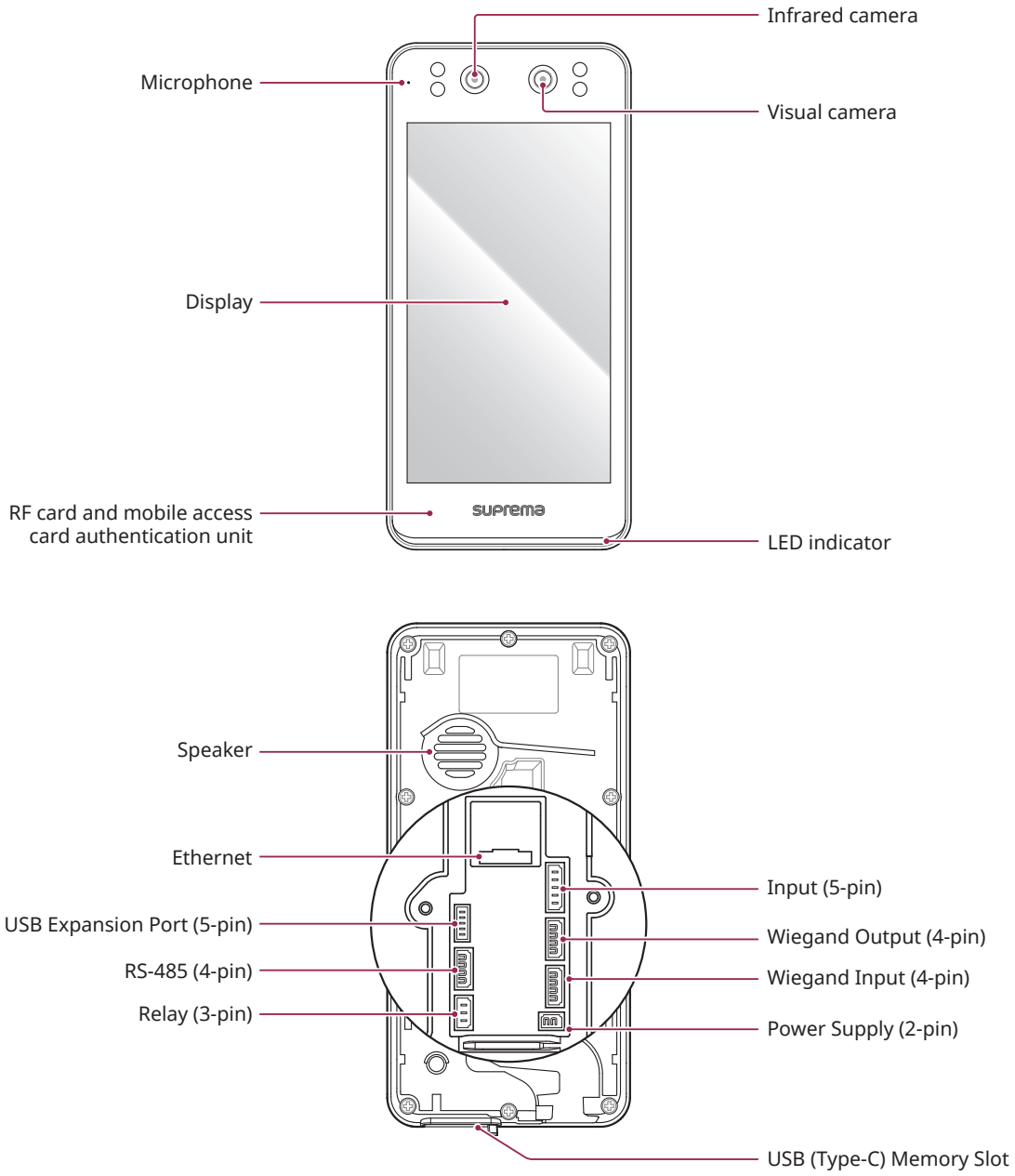
Introduction

Components

		
BioStation 3	Wall Bracket	Drilling Template
		
Connection Cables	Diode	120 Ω Resistor
			
PVC Anchor x2	Fixing Screw x2	Bracket Fixing Screw (Star Shaped)	Quick Guide

- 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.
- For more details regarding the product installation, visit the Suprema Download Center (https://download.supremainc.com) and refer to the installation guide.

Name and Function of Each Part



Name	Description
Microphone	Transmits the voice of the user when the interphone is connected. • Covering or blocking the microphone may interfere with voice transmission.
Infrared Camera	Capture the infrared face image.
Visual Camera	Capture an actual face image.
Display	Provides a UI for operation.
RF card and mobile access card authentication unit	Part to scan a RFID card or mobile access card for entrance.

Name	Description

LED Indicator	Indicates the operational status of the device with the color of the LED.
	• Green: Authentication success.
	• Red: Authentication failure.
	• Blue: Normal operation.
	• Blue/Green blinking:
	  – Fails to receive an IP address when **DHCP** is enabled.
	  – Disconnection with the master device when in **Slave** mode.
	• Red/Purple blinking: Device is locked.
	• Yellow blinking: Waiting for an input.

Speaker	Delivers sound.
Ethernet	Connect the Ethernet cable.
Input (5-pin)	Connect the Input cable.
USB Expansion Port (5-pin)	Connect other accessory products.
Wiegand Output (4-pin)	Connect the Wiegand Output cable.
Wiegand Input (4-pin)	Connect the Wiegand Input cable.
RS-485 (4-pin)	Connect the RS-485 cable.
Relay (3-pin)	Connect the Relay cable.
Power Supply (2-pin)	Connects the power supply cable.
USB (Type-C) Memory Slot	Connects the USB memory.

Cables and Connectors

Power supply

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

Relay

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

RS-485

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

Input

Pin	Name	Color
1	INPUT0	Red
2	INPUT1	Yellow
3	INPUT2	Orange
4	INPUT GND	Black
5	SH GND	Gray

Wiegand Input

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

Wiegand Output

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

Master Admin Settings

The **Master Admin** feature is designed to enhance device security by strengthening overall administrator privileges and preventing unauthorized access and configuration changes.

With this feature, you must **register a Master Admin** on the device, and only registered Master Admins can access the administrator menu and change device settings.

What is a Master Admin?

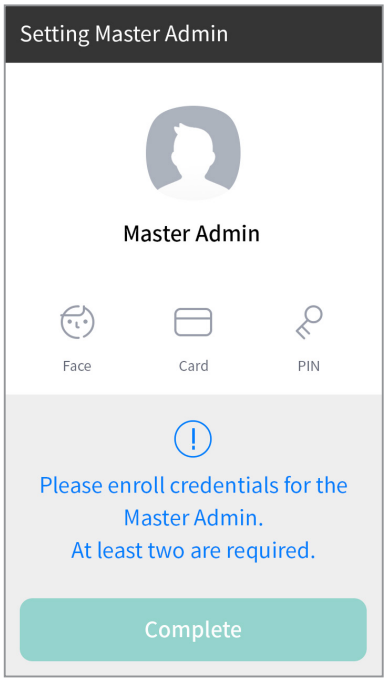
- If you use the device without setting up a Master Admin, anyone can access the administrator menu and change device settings. The Master Admin feature addresses this security vulnerability by enforcing the setup of an overall administrator.
- The Master Admin cannot be deleted directly, and they are deleted only through **Factory Reset**.

Registering Master Admin on a New Device

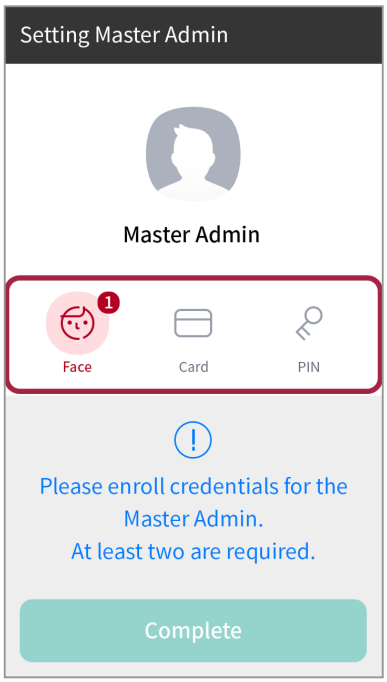
For new devices, registering a Master Admin is mandatory. If you do not register a Master Admin, device usage will be restricted.

- On new devices, the **Master Admin** registration screen appears upon initial boot. You cannot proceed to the next screen unless you register a Master Admin.
- Even if you assign an overall device administrator via BioStar 2, you must register a **Master Admin** to use all device functions.
- The new device cannot be downgraded to a lower version.

1 When you boot a new device for the first time, the **Master Admin** registration screen appears.



2 To register a **Master Admin**, you must enroll at least two types of credentials. Select and enroll your preferred two credential types.



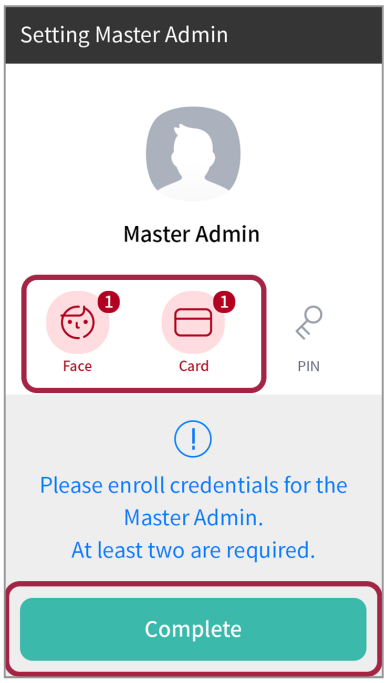
Credentials that can be enrolled for **Master Admin** are as follows:

Credential Type	Max Quantity	Details
Card	Up to 4	Supports CSN and Wiegand type only No duplicate enrollment within the same type
Face	Up to 2	Available only on devices with the same algorithm
Fingerprint	Up to 2	-
PIN	1	Minimum 8 digits

Enrollment Conditions:

- At least two different types of credentials must be enrolled.
- The same conditions apply to both new and upgraded devices.
- All credentials supported by the device can be used for authentication.

3 After enrolling at least two types of credentials, press the **Complete** button to finish **Master Admin** registration.



Additional Information

- **Manual Device Hash Key Change**

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

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

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

Correct Face Enrollment and Authentication Method

Cautions for enrolling a faces

- When enrolling a face, maintain a distance of 60 ~ 100 cm between the device and the face.
- Do not change your face expression.
- Do not wear masks, hats, or eye patches.
- Do not enroll a face wearing a mask. It may increase the False Acceptance Rate (FAR) if both faces with and without a mask are enrolled.
- Do not raise head up or lower head.
- Do not wear thick makeup.
- Do not close your eyes.
- Make sure that both of your shoulders correctly appear on the screen.
- Stand still and enroll your face by staring at the screen.
- Be careful not to display two faces on the screen. Enroll one person at a time.
- If you do not follow the instructions on the screen, the face enrollment may take longer or may fail.

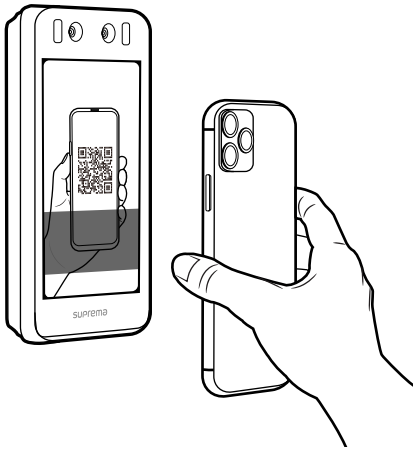
Cautions for authenticating a face

- Ensure that the face appears in the center of the device's screen. When the guideline is displayed, follow the instructions shown on the screen to authenticate the face.
- If a part of the face is covered with a hat, a mask, an eye patch, or sunglasses authentication may fail. Do not cover the face; allow the device to recognize both the eyebrows and the face.
- Authenticate your face at a distance of 60 ~ 100 cm from the device.
- Make sure that both of your shoulders correctly appear on the screen. Authentication may fail if your shoulders are not at the same height. Stand still, and then authenticate your face.

Note for QR Code Usage and Device License

How to scan a QR code

You can issue a QR code to a user and use it as an authentication method. Scan the QR code properly by following the instructions on the screen to increase the recognition rate.



- Keep 30 ~ 40 cm of distance between the device's camera and the QR code.
- Position the QR code in the center of the scan screen of the device.
- When authenticating with the QR code downloaded to your smartphone, adjust the brightness of your smartphone so that the device can read the QR code clearly.
- If do not follow the instructions on the screen, it may take a long time to scan the QR code, or it may fail.

Notes for Device License

- Using the QR Code authentication requires a separate device license. Contact the place of purchase to issue a device license.
- The device license file is an encrypted file and cannot be modified arbitrarily.
- Device licenses are issued based on device ID. If the device ID is changed in an unusual way, the warranty service for the license is not provided.

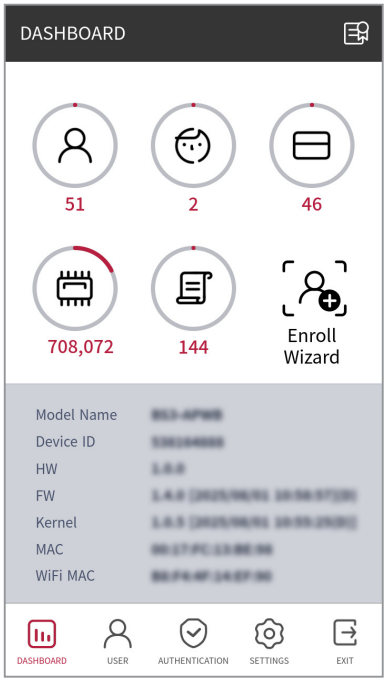
Admin Menu

DASHBOARD

1 Press ⊞ and authenticate with the Admin level credential.

Check current device usage and information on the **DASHBOARD**. Or select the **Enroll Wizard** to immediately register a user.

2 To Enroll a user or set up a device, select the desired menu from the bottom of the dashboard.



- If the administrator has not been designated, the **DASHBOARD** screen will be displayed when you press ⊞.
- The **WiFi MAC** is only available on the BS3-APWB model.

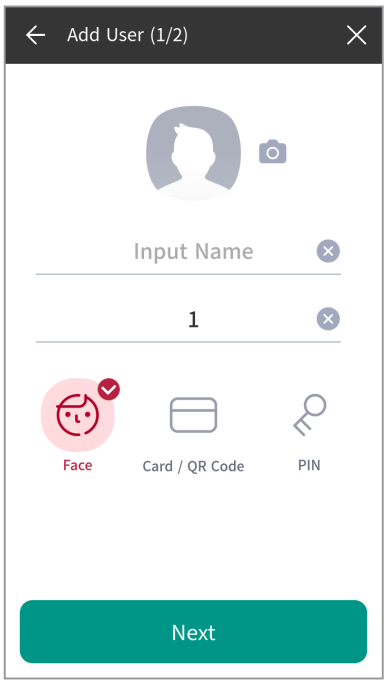
User

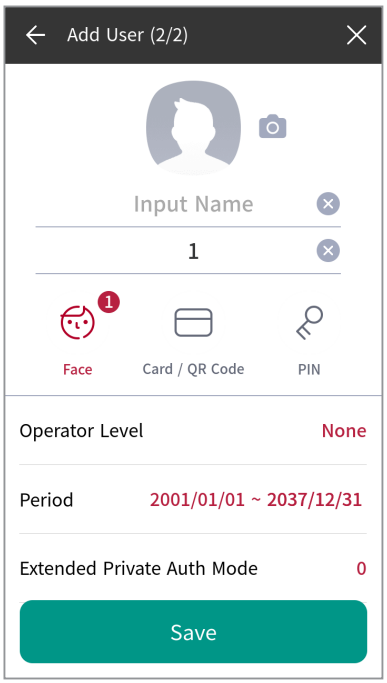
Registering User Information

The user information including credentials can be registered.

1 Press ⊞ and authenticate with the Admin level credential.

2 Select **USER** → ⊕, and choose a credential you want to enroll.
There are two steps for the user registration. Some options are available after the credential has been registered.





- 📷 : Register a user photo.
- **Name**: Enter the user name.
- **ID**: Enter a number between 1 and 4294967295 to register as the user ID. If **User ID Type** set to **Alphanumeric**, a combination of alphanumeric characters and symbols (_, -) can be used for the ID. Up to 32 characters can be input.
- **Face**: Enroll a face for user authentication. Press **Face** → **Next** and enroll a face according to the instructions on the screen. To add more faces, press ⊕. Please refer to Enrolling User Faces to learn more about face enrollment.
- **Card / QR Code**: Enroll a card for user authentication. Press **Card / QR Code** → **Next** and scan the card that will be assigned to the user. To enroll an additional card, press **Card / QR Code** → ⊕.
- **PIN**: Enter the PIN you wish to use. Enter the PIN you wish to use, and then enter the same PIN again for confirmation. Enter a number between 8 and 16 digits to prevent leaking.

- **Operator Level**: Select the level you wish to assign to a user.

> Available menus vary according to the set user level.
> - **None**: This is the general user level and menus cannot be accessed.
> - **Administrator**: All menus can be accessed.
> - **Configuration**: **AUTHENTICATION**, **DISPLAY & SOUND**, **DEVICE**, **NETWORK** and **EVENT LOG** menus can be accessed.
> - **User Management**: **USER** and **EVENT LOG** menus can be accessed.

- **Period**: Set an expiry date to use the user account.
- **Extended Private Auth Mode**: Change the authentication method according to the user. You can set extended private auth mode. This mode allows you to combine user authentication methods, including both faces. Otherwise, you can use the device's basic authentication mode.

3 To complete the registration of user information, press **Save**.

Enrolling User Faces

1 Press ⊞ and authenticate with the Admin level credential.

2 Select **USER** → ⊕.

3 Select **Face** → **Next**.

4 Adjust a distance between the face and screen and look straight at the camera of the device.

5 Once your face is captured successfully, press **OK** → **Save**. To retake a photo, press **Re-Shot**.

> - The visual face data of BioStation 3 are not compatible with face templates of FaceStation 2 or FaceLite.
> - You can enroll visual face not only directly from BioStation 3 but from the BioStar 2 by uploading photos or importing CSV files. You can also enroll visual face with your smartphone via a link sent from BioStar 2. To learn more about how to enroll visual face for each method, please refer to the BioStar 2 Administrator Guide.
> - To use a Visual Face feature correctly, take a picture by following instructions below.
> - When enrolling a face, maintain a distance of 60–100 cm between the device and the face.
> - Do not change your face expression.
> - Do not wear a masks, hats, or eye patches.
> - Do not enroll a face wearing a mask. It may increase the False Acceptance Rate (FAR) if both faces with and without a mask are enrolled.
> - Do not raise head up or lower head.
> - Do not wear thick makeup.
> - Do not close your eyes.
> - Make sure that both of your shoulders correctly appear on the screen.
> - Stand still and enroll your face by staring at the screen.
> - Be careful not to display two faces on the screen. Enroll one person at a time.
> - If you do not follow the instructions on the screen, the face enrollment may take longer or may fail.

Modifying User Information

User Management or Administrator can modify the registered user information. A card or face can be added, and PIN and level can be modified.

1 Press ⊞ and authenticate with the Admin level credential.

2 Select **USER** → 🔍.

3 Select your search terms. You can search for a user by **All**, **User ID**, **Name**, **Face** and **Card**.

4 Select the user to modify.

5 Modify the information by referring to Registering User Information and press **OK**.

- To delete a user, select 🗑 and then press **OK**.

> The **Access Group** can be registered in BioStar 2. For detailed contents regarding registering an access group, refer to the BioStar 2 Administrator Guide.

Delete All Users

You can delete all registered users at once.

1 Press ⊞ and authenticate with the Admin level credential.

2 Select **User** → 🗑.

3 Check **Delete All** to delete all registered users and press **OK**.

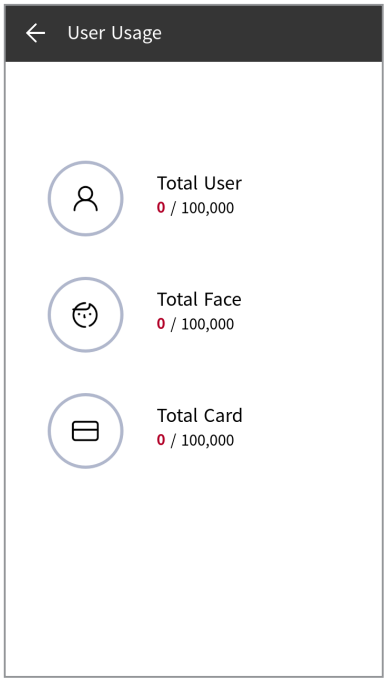
4 When you press **OK**, all registered users will be deleted.

View User Usage

You can see the number of registered users, faces, and cards at a glance.

1 Press ⊞ and authenticate with the Admin level credential.

2 Select **USER** → ⓘ. User usage information appears.



Authentication

Auth Mode

Set the authentication mode. You can make a combination of **Face**, **PIN**, **Card / QR Code**, or **ID** and you can also set a schedule for each authentication mode.

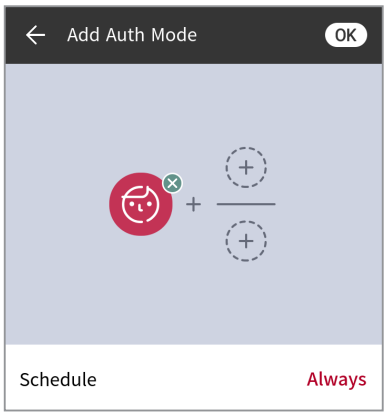
Registering Auth Mode

1 Press ⊞ and authenticate with the Admin level credential.

2 Select **AUTHENTICATION** → **Auth Mode**.

3 Press ⊕.

4 Pressing ⊕ will display the credential that can be added on the screen. Select the credentials to add. Press the ⊗ while the credential is added, and the added credential will be deleted.



5 Set the authentication mode as desired and configure the **Schedule**.

Category	Description
Face	• : Mode to use a face only • + : Mode to authenticate with a face and then enter PIN
Card / QR Code	• : Mode to use a card / QR code only • + : Mode to authenticate with a card / QR code and then authenticate with a face • + : Mode to authenticate with a card / QR code and then enter PIN • + / : Mode to authenticate with a card / QR code and then authenticate with a face or enter PIN • + + : Mode to authenticate with a card / QR code and then use both face authentication and PIN input.
ID	• ID + : Mode to enter ID and then authenticate with a face • ID + : Mode to enter ID and then enter PIN • ID + / : Mode to enter ID and then authenticate with a face or enter PIN • ID + + : Mode to enter ID and then use both face authentication and PIN input

- The **Schedule** can be set in BioStar 2. If there is no set schedule, only **Always** can be selected.
- For detailed contents regarding setting a **Schedule**, refer to the BioStar 2 Administrator Guide.
- To use **QR Code** authentication, **QR Authentication** must be activated in **AUTHENTICATION** → **Operation**, and a separate device license is required. For more information, refer to License.

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

Modifying Auth Mode

1 Press and authenticate with the Admin level credential.

2 Select **AUTHENTICATION** → **Auth Mode**.

3 Select the authentication mode to modify.

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

Delete Auth Mode

1 Press and authenticate with the Admin level credential.

2 Select **AUTHENTICATION** → **Auth Mode**.

3 Press and select the authentication mode to delete. You can select multiple options.

4 To delete the selected option, press **OK**.

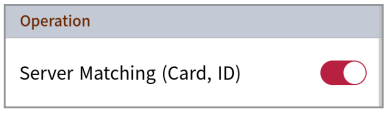
Operation

Server Matching

You can set up server matching.

1 Press ⊞ and authenticate with the Admin level credential.

2 Select **AUTHENTICATION** and activate **Server Matching (Card, ID)** in **Operation**.



- **Server Matching (Card, ID)**: When this option is activated, it performs user authentication matching in BioStar 2, not in the device. It can be used when the device has too much user information or when the device is installed outside.

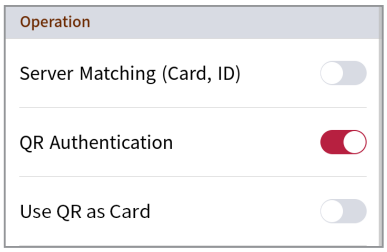
- **Server Matching** is only available for card and ID options.
- When you use the **Server Matching** option, you need to activate the option in both Biostar 2 and the device. Refer to the Administrator Guide of BioStar 2 to learn how to set the server matching settings in BioStar 2.

QR Authentication

You can activate QR code authentication.

1 Press ⊞ and authenticate with the Admin level credential.

2 Select **AUTHENTICATION** and activate **QR Authentication** in **Operation**.



- **QR Authentication**: Set whether to use QR Code authentication through the device's camera.
- **Use QR as Card**: Allows authentication with a QR code of the same data as the issued CSN card or Wiegand card. It can be set only when **QR Authentication** is activated.

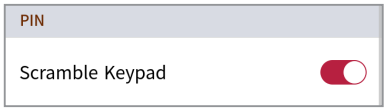
Using the **QR Authentication** requires a separate device license. For more information, refer to License.

PIN

Set whether to use the scramble keypad when entering passwords.

1 Press ⊞ and authenticate with the Admin level credential.

2 Select **AUTHENTICATION**, and set whether to use the **Scramble Keypad** in the **PIN**.



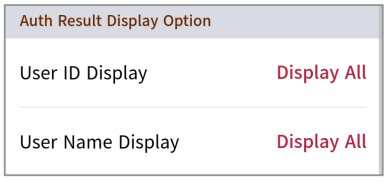
- **Scramble Keypad**: When entering a password, the positions of the number keys are randomly shuffled to prevent password leakage.

Auth Result Display Option

You can set the auth result display option.

1 Press ⊞ and authenticate with the Admin level credential.

2 Select **AUTHENTICATION** and set the desired item in the **Auth Result Display Option**.



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

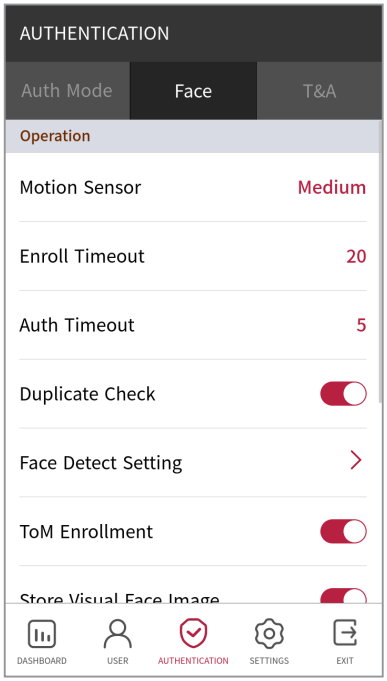
Face

You can change the configuration for facial authentication.

1 Press ⊞ and authenticate with the Admin level credential.

2 Select **AUTHENTICATION** → **Face**.

3 Select and set the desired item.



- **Motion Sensor**: Set the sensitivity for detecting motion near the device. If **Motion Sensor** is set to **Off**, tap the screen to authenticate the face.
- **Enroll Timeout**: If a face is not enrolled during the set time, the face enrollment will be canceled.
- **Auth Timeout**: If the authentication is not completed during the set time, the authentication will fail.
- **Duplicate Check**: When enrolling a face, you can check duplicates.
- **Face Detect Setting**: Set the face authentication area by adjusting the size and position of the detected area.

- It is recommended to maintain the default values of options under **Face Detect Setting**. The default values of each option are as follows:
  - Maximum Head Pose Angle: 15
  - Detection Distance: Min 30 cm, Max 100 cm
  - Wide Search: Deactivated

- **ToM Enrollment**: Enabling **ToM Enrollment** can be enrolled the **Template on Mobile** issued by BioStar 2. **Template on Mobile** is a Mobile Access card in which the user's biometric templates can be stored so you can still use biometric authentication although your biometric information is not stored in BioStar 2 server, Airfob Portal, or device.

For detailed contents regarding **Template on Mobile**, refer to the BioStar 2 Administrator Guide.

- **Store Visual Face Image**: Set whether to store both the actual image and the template in the visual face or to store only the template without storing the actual image. If disabled, all stored images of visual faces will be deleted, and newly enrolled visual faces will store templates excluding images.

After disabling this setting, please use BioStar 2 v2.9.7 or higher.

- **Security Level**: Set the security level for 1:N authentication.
- **Operation Mode**: Set the operation mode of the device when the face is authenticated.
  - **Fusion Matching**: Use both visual and infrared cameras to increase the face authentication accuracy.
  - **Fast Matching**: The device authenticates users who pass an access point without a pause within the authentication distance.
- **Fake Detection**: The device prevents user authentication using fake faces, such as photos. It is available when **Operation Mode** is set to **Fusion Matching**.

- Face anti-spoofing performance has been improved to pass the iBeta Level 1 ISO 30107-3 Presentation Attack Detection Test.
- We recommend using the **Fake Detection** feature set to **Normal** in environments with strong sunlight.

- **Advanced Settings**: Set the settings of the face authentication, such as mask detection.
  - **Mask Detection**: Set the mask detection mode to detect whether a user is wearing a mask or not.
  - **Detection Mode**: Set the method for verifying whether a mask is being worn. This is activated when the **Mask Detection** is set to **Enabled**.

- **Require Mask (Hard)**: Users not wearing a mask will be denied authentication and a mask non-compliance event logs.
- **Require Mask (Soft)**: Users not wearing a mask can be authenticated, but a mask non-compliance event logs.
- **Require No Mask**: Only users not wearing a mask can be authenticated, and when this mode is used, the mask check mode is fixed to **Check Before Authentication**.

  - **Mask Detection Level**: Set the sensitivity to detect wearing a mask. This is activated when the **Mask Detection** is set to **Enabled**.
  - **Check Mode**: Set the check mode depending on the usage.

- **Check After Authentication**: Authenticate and then detect whether the user is wearing a mask.
- **Check Before Authentication**: Detect whether the user is wearing a mask and then authenticates.
- **Check Only**: Detect whether a user is wearing a mask without authentication. When this mode is activated, any user wearing a mask can access it regardless of authentication.

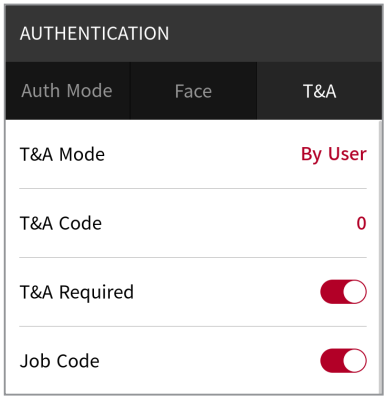
T&A Mode

You can set how to register T&A mode.

1 Press ⊞ and authenticate with the Admin level credential.

2 Select **AUTHENTICATION** → **T&A**.

3 Select and set the desired item.



- **T&A Mode**: Set the method to use T&A mode.
- **T&A Code**: You can register T&A events. Select **T&A Code** → ⊕ to register a T&A event and set an icon, **T&A Event Name** and **Schedule**.
- **T&A Required**: Set to require a user to select a T&A event when authenticating. This option can be used when **T&A Mode** is set to **By User**.
- **Fixed T&A Key**: Set to use only a T&A event selected by the administrator. This option can be used when **T&A Mode** is set to **Fixed**.
- **Job Code**: Select whether to use **Job Code**.

Settings

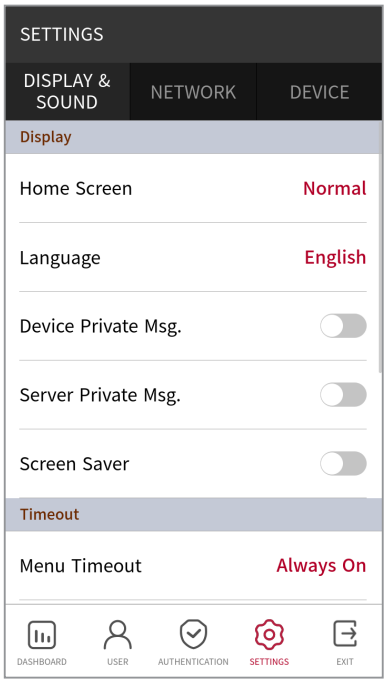
Display & Sound

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

1 Press ⊞ and authenticate with the Admin level credential.

2 Select **SETTINGS** → **DISPLAY & SOUND**.

3 Change the desired item.



- **Home Screen**: Select items to be displayed in the background of the home screen.
- **Language**: Select the language that will be displayed on the screen.
- **Device Private Msg.**: Set whether to use a Private Message, which will be displayed on the screen when the user authenticates. The **Device Private Msg.** can be set using the BioStar 2 Device SDK. If not set, does not display a message when authentication is successful even if **Device Private Msg.** is enabled on the device.
- **Server Private Msg.**: Set whether to use a Private Message, which will be displayed on the screen when the user authenticates. The **Server Private Msg.** can be set using the BioStar 2 API. If not set, does not display a message when authentication is successful even if **Server Private Msg.** is enabled on the device.

For more detailed information about the BioStar 2 Device SDK, visit the BioStar 2 Device SDK web page on the Suprema Knowledge Base (kb.supremainc.com/bs2sdk/).

- **Screen Saver**: Set this option to use the screen saver feature. It reduces unnecessary energy consumption by lowering the brightness of the screen when the device is not in use.
- **Menu Timeout**: Set the time (sec) for the menu screen to disappear automatically. If there is no button input during a set time, the screen will return to the home screen.

- **Message Timeout**: Set the time (sec) for a setting complete message or information message to disappear automatically.
- **Backlight Timeout**: Set the time (second) to turn off the lighting of screen.
- **Voice Instruction**: Set to use the voice instruction instead of alarm sounds.
- **Volume**: Set the volume.
- **Intercom Speaker Volume**: Adjust the speaker's output volume when using intercom.
- **Intercom Microphone Volume**: Adjust the microphone's input volume when using intercom.

Network

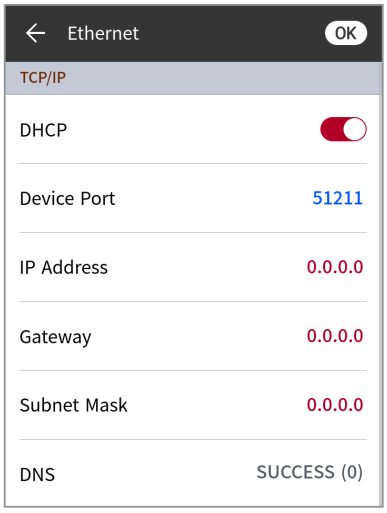
You can change the network settings of the device, such as Ethernet, server, OSDP, etc.

Ethernet

1 Press ⊞ and authenticate with the Admin level credential.

2 Select **SETTINGS** → **NETWORK** → **Ethernet**.

3 Change the desired item.



- **DHCP**: Set whether to use DHCP. If DHCP setting is disabled, the user can modify **IP Address**, **Gateway**, and **Subnet Mask**.
- **Device Port**: Set the device port.
- **IP Address**: View the IP address of the device. To modify, disable DHCP setting.
- **Gateway**: View the gateway of the device. To modify, disable DHCP setting.
- **Subnet Mask**: View the subnet mask of the device. To modify, disable DHCP setting.
- **DNS**: Set the DNS server address.

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

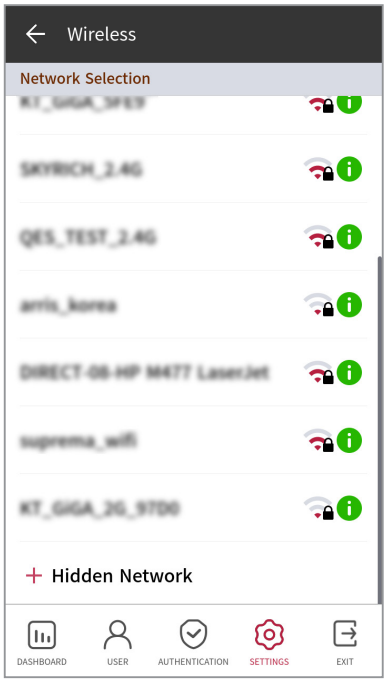
Ethernet cannot be used with **Wireless** at the same time.

Wireless

1 Press ⊞ and authenticate with the Admin level credential.

2 Select **SETTINGS** → **NETWORK** → **Wireless**.

3 The list of networks available to connect will be displayed.



- **Hidden Network**: Add and connect to a wireless network by entering network information manually.
  - **SSID**: Enter the SSID. The SSID may be up to 32 characters long and include alphanumeric (case-sensitive), and special characters.
  - **Password**: Enter the password. The password can include alphanumeric and special characters only.

4 Select the network you wish to connect to and enter the password. When you press **OK**, the connection to the wireless network will be made.

5 Press ⓘ the wireless network you wish to use and then disable DHCP settings to allow users to modify the **IP Address**, **Gateway** and **Subnet Mask**.

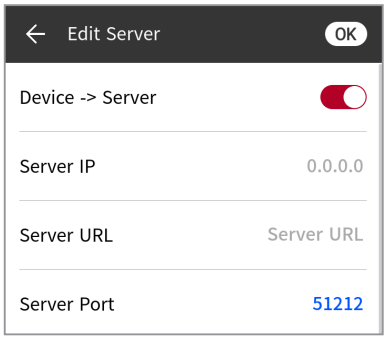
- **Wireless** is only available for BS3-APWB model.
- **Wireless** cannot be used with **Ethernet** at the same time.
- To connect to **Wireless**, a wireless router is required. For content regarding the installation and configuration of wireless router, refer to the user's manual of the wireless router.

Server

1 Press ⊞ and authenticate with the Admin level credential.

2 Select **SETTINGS** → **NETWORK** → **Server**.

3 Change the desired item.



- **Device** → **Server**: You can send a connection signal from the device to a server with the input information directly. When the **Device** → **Server** is enabled, the user can enter the **Server IP**, **Server URL**, and **Server Port**.
- **Server IP**: Enter the IP address of the PC on which BioStar 2 is installed.
- **Server URL**: Enter the **Server URL** instead of **Server IP**.
- **Server Port**: Enter the port of the PC on which BioStar 2 is installed.

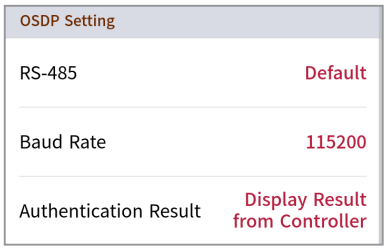
4 To save the settings, press **OK**.

OSDP Setting

1 Press ⊞ and authenticate with the Admin level credential.

2 Select **SETTINGS** → **NETWORK**.

3 Change the desired item in the **OSDP Setting**.



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

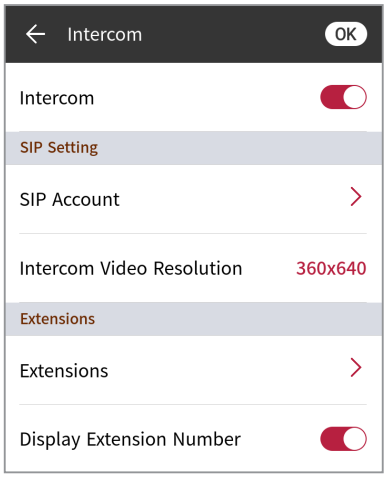
Devices

Intercom

Set the account and extensions of intercom.

1 Press ⊞ and authenticate with the Admin level credential.

2 Select **SETTINGS** → **DEVICE** → **Intercom**.



- **Intercom**: Set whether the intercom is enabled or not. To set the **SIP Account** and the **Extensions**, activate this option.
- **SIP Account**: Enter each item so that the device can be registered on the SIP server.
- **Intercom Video Resolution**: Select the resolution of the intercom video output from the device.
- **Extensions**: Add, delete, or edit extension numbers.
- **Display Extension Number**: Set whether to display the extension number.

- If **Display Name** is not set, it will not be possible to distinguish receivers.
- Extension numbers can only enter alphanumeric (case sensitive), and special characters (+, -, @, .).

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

License

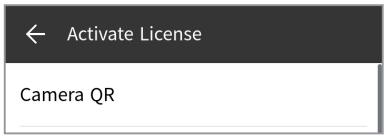
You can activate device licenses or view **Licenses in Slave Devices** and **Activated Licenses in Device**.

1 Press ⊞ and authenticate with the Admin level credential.

2 Select **SETTINGS** → **DEVICE** → **License**.

3 To activate the device license, connect the USB with the license to the device and select ⊕.

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



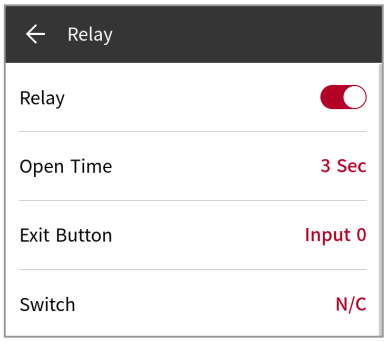
- Contact the place of purchase to issue a device license.
- One feature is available per device license.
- You can include multiple device licenses in one device license file. (Supports up to 100)
- The device license file is an encrypted file and cannot be modified arbitrarily.
- Device licenses are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

Relay

You can set the **Open Time** and the input port of the **Exit Button** in the device.

1 Press ⊞ and authenticate with the Admin level credential.

2 Select **SETTINGS** → **DEVICE** → **Relay**.



- **Relay**: You can set whether relay is enabled or not. To set the **Open Time** and the input port of the **Exit Button**, activate this option.
- **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 where the exit button is connected.
- **Switch**: Select the type of switch (**N/O** or **N/C**) for the Exit Button's input port.

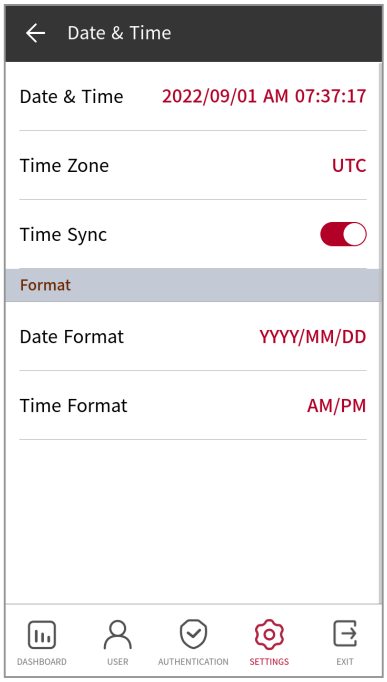
Date & Time

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

1 Press ⊞ and authenticate with the Admin level credential.

2 Select **SETTINGS** → **DEVICE** → **Date & Time**.

3 Change the desired item.



- **Date & Time**: Check the current date and time. To modify it manually, disable **Time Sync**.
- **Time Zone**: Set the time reference of the current location.
- **Time Sync**: Synchronize the server and the time. If you wish to synchronize the server and the time, enable **Time Sync**.
- **Date Format**: Set the date format. You can select among **YYYY/MM/DD**, **MM/DD/YYYY** and **DD/MM/YYYY**.
- **Time Format**: Set the time format. You can select either **AM/PM** or **24-Hour**.

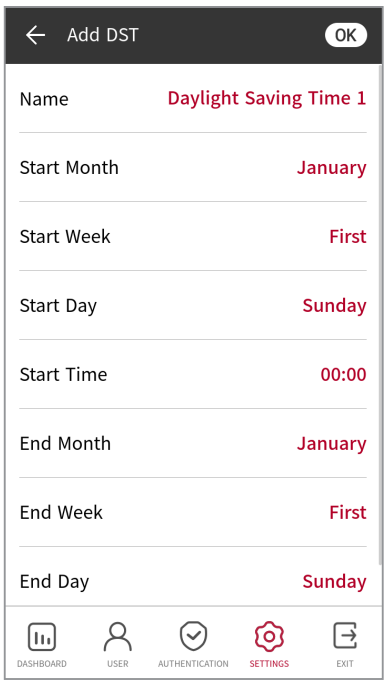
Daylight Saving Time

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

1 Press ⊞ and authenticate with the Admin level credential.

2 Select **SETTINGS** → **DEVICE** → **Daylight Saving Time** and then press ⊕ to add additional daylight-saving time.

3 Select the desired item and change the setting.



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

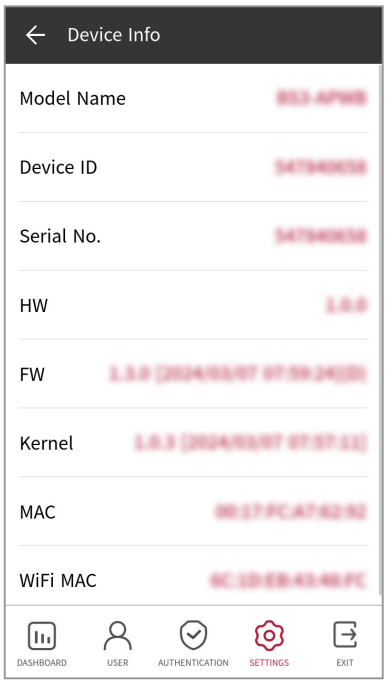
4 To save the settings, press **OK**.

Device Information

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

1 Press ⊞ and authenticate with the Admin level credential.

2 Select **SETTINGS** → **DEVICE** → **Device Info**. You can view the information including **Model Name**, **Device ID**, **Serial No.**, **HW**, **FW**, **Kernel**, **MAC** and **WiFi MAC**.



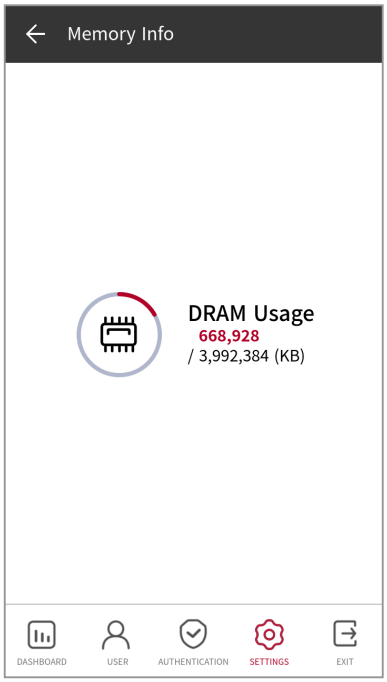
- When long-pressing the **MAC**, **FAS_IR_SP** will be displayed, showing the version of the face anti-spoofing algorithm. If press **FAS_IR_SP** to check the entire hash value in a pop-up message.
- The **WiFi MAC** is only available on the BS3-APWB model.

Memory Information

View the status of memory usage.

1 Press ⊞ and authenticate with the Admin level credential.

2 Select **SETTINGS** → **DEVICE** → **Memory Info**. You can view the memory usage status of the device.



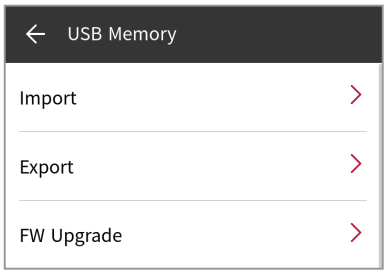
USB Memory

Connect USB Memory and import user information to the device or export log and user information from the device. You can also upgrade the firmware.

1 Press ⊞ and authenticate with the Admin level credential.

2 Select **SETTINGS** → **DEVICE** → **USB Memory**.

3 Select the desired item and change the setting.



- **Import**: Import user information from the connected USB memory.
- **Export**: Select information you wish to export to the connected USB memory.
- **FW Upgrade**: Upgrade the firmware if the firmware files are saved in the connected USB memory.

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

- It is recommended to use a USB flash drive formatted in exFAT. USB flash drives in FAT32 format may malfunction when more than 50,000 face credentials are stored.
- Check the amount of free space on your USB flash drive. To save 100,000 face credentials, a minimum of 15 GB of free space is required.
- The type of supported USB memory is as follows. If you use a different type of USB memory, the function may not operate normally.
  - Samsung Electronics: SUM-BSG 32GB
  - LG Electronics: MU 1 USB 32GB, MU28GBC 32GB
  - SanDisk: Cruzer Blade CZ50 32GB, CZ48 Ultra USB 3.0 64GB, CZ80 USB3.0 64GB, CZ52 64GB, Cruzer Glide Z60 128GB, Cruzer Force CZ71 32GB
  - Sony: USM-SA1 32GB
  - Transcend: JetFlash 760 32GB

  The supported USB flash drives listed above were all tested with USB Type-A. To connect these USB flash drives to BioStation 3, a separate USB Type-C gender is required.

Secure Tamper

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

1 Press ⊞ and authenticate with the Admin level credential.

2 Select **SETTINGS** → **DEVICE**.

3 Activate **Secure Tamper** to delete data of all registered users, all logs, and secure keys when a temper event occurs.

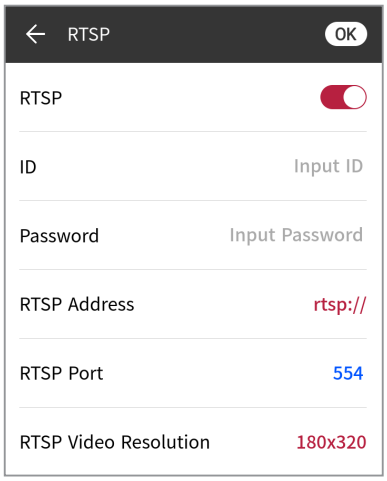
RTSP

A video management system (VMS) of another brand may be connected to monitor videos filmed with the BioStation 3 visual camera.

1 Press ⊞ and authenticate with the Admin level credential.

2 Select **SETTINGS** → **DEVICE** → **RTSP**.

3 Select the desired item and change the setting.



- **RTSP**: You can set whether **RTSP** is enabled or not. To set the **ID**, **Password**, **RTSP Address**, **RTSP Port**, and **RTSP Video Resolution** activate this option.
- **ID**: Enter the ID. The ID may have up to 32 characters, in a combination of alphanumeric (case-sensitive) characters and certain symbols (_, -).
- **Password**: Enter the password. The password may have 8–32 characters in a combination of alphabetic (capital and lowercase letters) and numeric characters.
- **RTSP Address**: Enter the RTSP address.
- **RTSP Port**: Enter the RTSP Port number.
- **RTSP Video Resolution**: Select the resolution of the RTSP video output from the device.

When the device is configured as a slave device, the RTSP function may not be available.

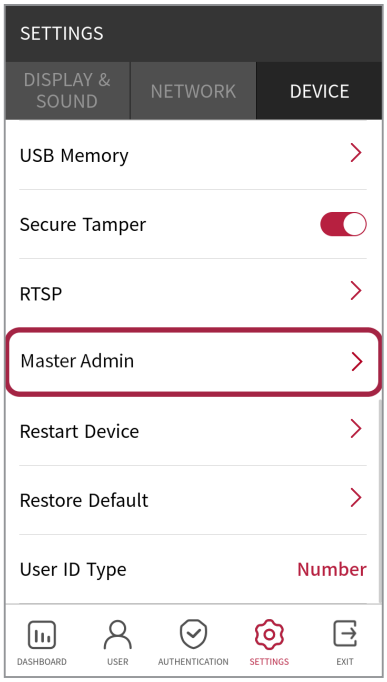
Master Admin

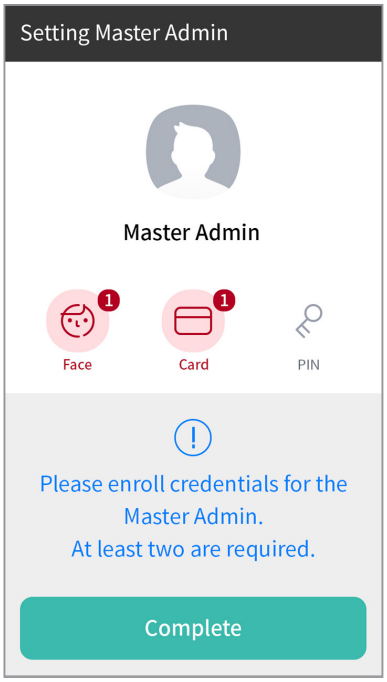
Change the authentication methods for the Master Admin.

1 Press ⊞ and authenticate with the Admin level credential.

2 Select **SETTINGS** → **DEVICE** → **Master Admin**.

3 Select the desired authentication methods.





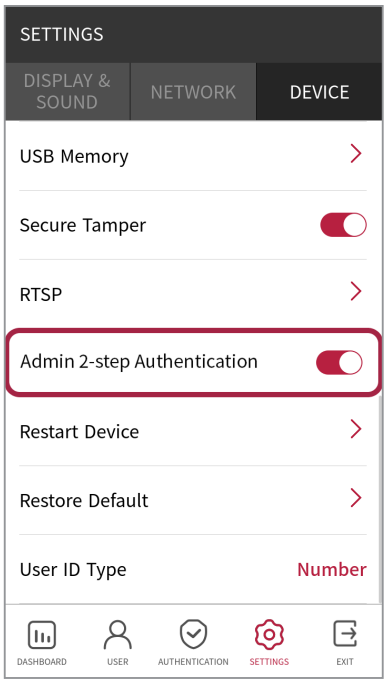
- At least two different types of credentials must be enrolled.
- This feature is available only on new devices with firmware version v1.4.0 or higher.

Admin 2-step Authentication

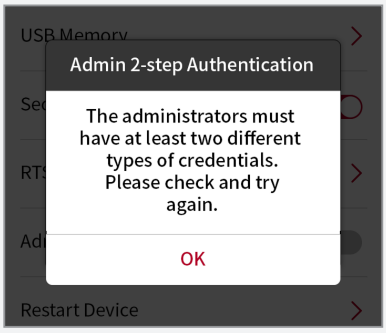
Devices upgraded via firmware do not provide **Master Admin** settings, but you can enhance administrator security by enabling the **Admin 2-step Authentication** option.

1 Press ⊞ and authenticate with the Admin level credential.

2 Select **SETTINGS** → **DEVICE** → **Admin 2-step Authentication**.



- **Admin 2-step Authentication** is available after upgrading the firmware to v1.4.0 or higher. Once upgraded to v1.4.0 or higher, you cannot downgrade to a lower version.
- The default value for **Admin 2-step Authentication** is single-step authentication.
- If not all administrators have at least two types of credentials, activation will fail and an error message will appear. Enroll at least two types of credentials for all administrators, and then try again.



If you activate **Admin 2-step Authentication** and then delete credentials so that all administrators have fewer than two types, you will not be able to access the administrator menu if BioStar 2 connection is also unavailable. Therefore, exercise caution when deleting administrator credentials.

Restart Device

The user can restart the device.

1 Press ⊞ and authenticate with the Admin level credential.

2 Select **SETTINGS** → **DEVICE** → **Restart Device**.

3 To restart the device, press **OK**. To return to the previous screen, press **Cancel**.

Restore Default

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

1 Press ⊞ and authenticate with the Admin level credential.

2 Select **SETTINGS** → **DEVICE** → **Restore Default**.

- **All settings**: Reset all settings stored on the device. To reset all device settings, press **OK**. To return to the previous screen, press **Cancel**.
- **Keep Network Settings**: Reset all settings except for the network settings. To reset all settings except for the network settings, press **OK**. To return to the previous screen, press **Cancel**.
- **Factory Default**: Delete all the information saved in the device and the root certificate and restore default settings.
- **Delete the Root Certificate**: Delete the root certificate saved in the device.

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

- 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.
- **Factory Default** menu can be used when the root certificate is saved in the device.
- **Delete the Root Certificate** menu can be used only when the root certificate is saved in the device and Administrator has been designated.

User ID Type

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

1 Press ⊞ and authenticate with the Admin level credential.

2 Select **SETTINGS** → **DEVICE** → **User ID Type**.

- **Number**: You can register a user ID with numbers only.
- **Alphanumeric**: You can register a user ID with alphanumeric characters and symbols (_, -).

3 Select to the desired item.

Event Logs

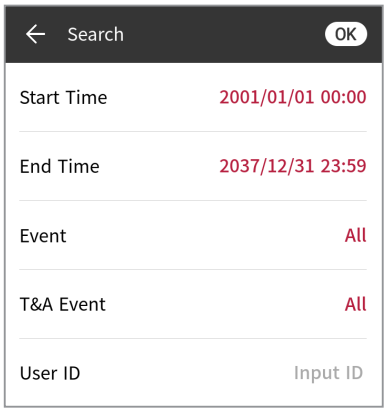
Search Event Logs

Set conditions to search logs.

1 Press ⊞ and authenticate with the Admin level credential.

2 On the **DASHBOARD**, select (📄). All event logs appear.

3 Press 🔍 to search a specific log and change the condition.



4 Set the condition and press **OK** to log that matches the condition will be displayed on the screen.

Delete All Logs

You can delete all saved logs.

1 Press ⊞ and authenticate with the Admin level credential.

2 On the **DASHBOARD**, select (📄). All event logs appear.

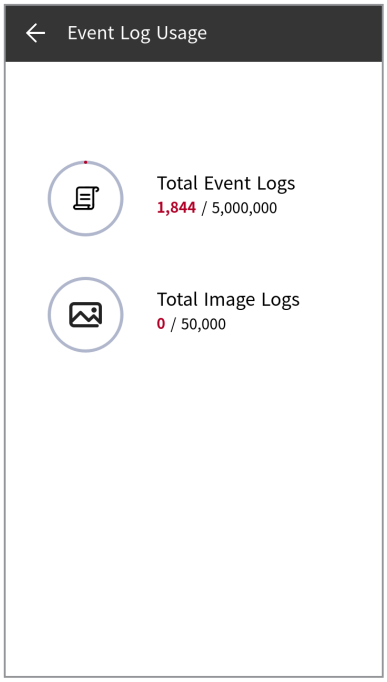
3 To delete all logs, select 🗑 and then press **OK**. To return to the previous screen, press **Cancel**.

View Log Usage

You can check the status of log usage.

1 Press ⊞ and authenticate with the Admin level credential.

2 On the **DASHBOARD**, select → . Check the device's event log and image log usage.



Troubleshooting

This troubleshooting provides information to solve unexpected issues that you may encounter when using the device.

Category	Problem	Solution
Power	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.
	The terminal reboots abnormally.	• Upgrade the terminal's firmware to the latest version.
PIN	I lost my PIN.	• For a normal user PIN, request it from the administrator and enter it again. • If you have lost the Admin PIN, contact the installation company.
	I entered my PIN and pressed the **OK** button, but I still cannot open the door.	• Check if you have entered the registered PIN correctly. • Check if you have changed the PIN recently. • If you cannot remember the PIN, request it from the administrator and enter it again.
Face	The face has been registered but face authentication cannot be done smoothly, and errors occur frequently.	• Check Cautions for enrolling a faces and enroll the face again. • If there are a large number of enrolled faces, change **Matching Timeout** and try again.
	Face authentication has suddenly stopped working.	• Check Cautions for authenticating a face and try again.
	Mask Detection is set to **Enabled**, but face authentication cannot be done smoothly when wearing a mask.	• Authenticate your face twice with the mask pull down on the tip of your nose. Then, authenticate your face again wearing a mask that covers your nose completely. If the problem persists, contact the installation company.
Door lock	The door cannot be locked when I close the door.	• The electric lock may be malfunctioning. Have an inspection through the installation company.
Time	Suddenly the time has become incorrect.	• BioStation 3 is equipped with a built-in battery but if power is not supplied for a long time, the built-in battery may die, causing the time to become incorrect. You can correct the time by referring to Date & Time.
Admin Access	I lost my Admin PIN, so I cannot access the Admin mode.	• The administrator grants an access permission in BioStation 3, so only the administrator can access the Admin menu. • If you have lost the Admin PIN, contact the installation company.
Master Admin	After upgrading the firmware on existing devices, the Master Admin setting does not appear.	• Devices upgraded with firmware from existing devices do not support master administrator configuration. You can enhance device security by strengthening the permissions of all administrators through the **Admin 2-Step Authentication** option. For more detailed information, refer to Admin 2-step Authentication.

Product Specifications

Category	Feature	Specifications
Credentials	Biometric	Face
	RF Card	• **BS3-DB**: 125kHz EM & 13.56MHz MIFARE, MIFARE Plus, DESFire, DESFire EV1/EV2/EV3[1], FeliCa • **BS3-APWB**: 125kHz EM, HID Prox & 13.56MHz MIFARE, MIFARE Plus, DESFire, DESFire EV1/EV2/EV3[1], FeliCa, iCLASS SE/SR/Seos
	RF Read Range[2]	EM/HID Prox/MIFARE/DESFire/HID iCLASS: 30 mm, FeliCa: 15 mm
	Mobile	NFC, BLE
	Scramble Keypad (PIN)	Supported
	QR/Barcode[3]	Supported[4]
General	CPU	1.5 GHz Quad Core
	Memory	32 GB Flash + 4 GB RAM
	Crypto Chip	Supported
	Display	5.5" IPS color LCD
	Display Resolution	720 x 1280 pixels
	Sound	16 bit
	Operating Temperature	-20 °C ~ 50 °C
	Storage Temperature	-40 °C ~ 70 °C
	Operating Humidity	0 % ~ 80 %, non-condensing
	Storage Humidity	0 % ~ 90 %, non-condensing
	Camera	• IR: 2M pixels • Visual: 2M pixels
	Dimensions (W x H x D)	82.5 x 171 x 23.4 (mm)

	Weight	• Device
		  – **BS3-DB**: 370 g
		  – **BS3-APWB**: 380 g
		• Bracket: 90 g (Including washers and bolts)

	IP Rating	IP65
	IK Rating	IK06
	Certifications	CE, UKCA, KC, FCC, IC, RCM, BIS, SIG, RoHS, REACH, WEEE, MIC, TELEC
Face	Authentication Distance[5]	0.3 ~ 1.0 m
	Authentication Height	1.4 ~ 1.9 m
	Matching Speed	Within 0.2 seconds
	Live Face Detection	Supported
Capacity	Max. User	100,000[6]
	Max. Credentials (1:N)	• Face: 50,000
	Max. Credentials (1:1)	• Face: 100,000 • Card: 100,000 • PIN: 100,000
	Max. Text logs	5,000,000
	Max. Image logs	50,000

Category	Feature	Specifications
Interfaces	Ethernet	Supported (10/100/1000 Mbps, auto MDI/MDI-X)
	Wi-Fi	• **BS3-DB**: Not supported • **BS3-APWB**: Supported (802.11 b/ g/ n 2.4 GHz)
	Network Protocol	TCP, UDP
	RS-485	1 ch Master / Slave (Selectable)
	RS-485 Communication Protocol	OSDP V2 compliant
	Wiegand	1 ch Input, 1 ch Output
	Input	3 ch Inputs
	Relay	1 Relay
	PoE+[7)]	• **BS3-DB**: Not supported • **BS3-APWB**: Supported (IEEE 802.3at compliant)
	Intercom	Supported
	RTSP	Supported
	USB	USB 2.0 (Host)
	USB Expansion Port	Supported
	Tamper	Supported
Electrical	Power	• Voltage: 12 Vdc • Current: Max. 1 A
		• Voltage: 24 Vdc • Current: Max. 0.7 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
	Wiegnad Output Pull-up Resistance	Internally pulled up with 1 kΩ
	Relay	2 A @ 30 VDC Resistive load 1 A @ 30 VDC Inductive load

1) DESFire EV2/EV3 cards are supported by having backward compatibility of DESFire EV1 cards. CSN and smart card functions are compatible with BioStation 3.

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

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

4) Requires a separate license.

5) The minimum face authentication distance shown is the default setting for the product, and the recommended face authentication distance is 0.6 to 1.0 m.

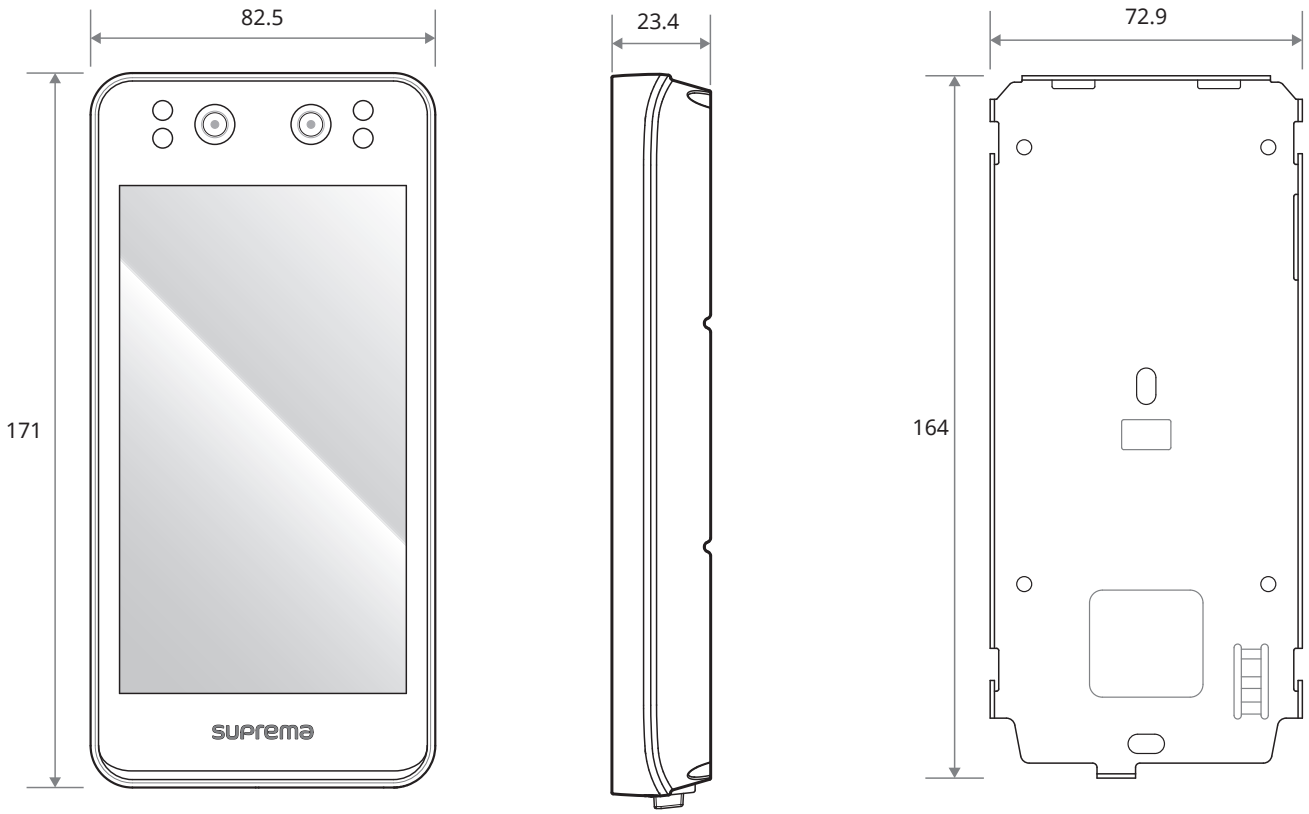
6) The number of users registered without having any credential data.

7) The device requires PoE+ (IEEE 802.3at, 30W) or PoE++ (IEEE 802.3bt, 60~100W). It does not support standard PoE (IEEE 802.3af, 15.4W). Using standard PoE may cause unstable operation and can potentially damage the device permanently. Always verify that your network switch or PoE injector supports PoE+ or PoE++ before connecting the device.

- If BioStation 3 is a master device and a device with a fingerprint sensor is connected as a slave, the slave device can be used for fingerprint authentication.
  - Max. Fingerprint Credentials (1:N): 100,000
  - Max. Fingerprint Credentials (1:1): 100,000

Dimensions

(Unit: mm)



Regulatory Information

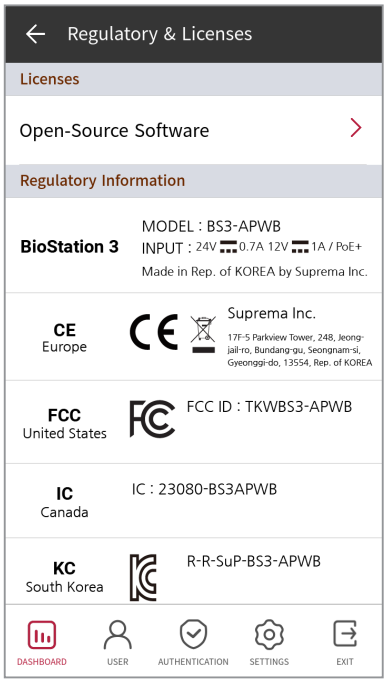
Regulatory & Licenses

Licenses, Regulatory Information, certifications, and compliance marks specific to BioStation 3 are available from the device.

- **CE / FCC / IC / KC / UKCA / RCM / MIC / TELEC**

1 Press ⊞ and authenticate with the Admin level credential.

2 You can view **Regulatory & Licenses** press the ⊟ on the upper right corner of **DASHBOARD**.



If the administrator has not been designated, the **DASHBOARD** screen will be displayed when you press ⊞.

FCC Compliance Information

THIS DEVICE COMPLIES WITH PART 15 OF THE FCC RULES.

Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and

(2) This device must accept any interference received, including interference that may cause undesired operation.

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. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

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.

- Bluetooth transmit power: -0.1 dBm
- Bluetooth frequency: 2402–2480 MHz
- NFC frequency: 13.56 MHz
- RFID frequency: 13.56 MHz + 125 kHz

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

Suprema Inc.

Website: https://www.supremainc.com

Address: 17F-5, Parkview Office Tower, 248, Jeongjail-ro, Seongnam-si, Gyeonggi-do, 13554, Republic of Korea

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

Appendices

Disclaimers

- Information in this document 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 document.
- 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 of this document is vested in Suprema. The rights of other product names, trademarks and registered trademarks are vested in each individual or organization that owns such rights.

Open Source License

- The software of this product is based on “Linux Kernel 4.x”, which is licensed under GPL. As for GPL, please refer to the GNU General Public License in this manual.
- This product uses the “glibc”, which is licensed under the LGPL. As for LGPL, please refer to the GNU Lesser General Public License in this manual.
- This product uses the “OpenSSL”, which is licensed under the OpenSSL and Original SSLeay licenses. As for the OpenSSL and Original SSLeay licenses, please refer to OpenSSL License and Original SSLeay License in this manual.
- To request the modified source code based on Linux Kernel 4.x and the source code of glibc library, which are included in this product, please contact us at support.supremainc.com.

GNU General Public License

Version 3, 29 June 2007

Copyright © 2007 Free Software Foundation, Inc. <https://fsf.org/>

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

“This License” refers to version 3 of the GNU General Public License.

“Copyright” also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

“The Program” refers to any copyrightable work licensed under this License. Each licensee is addressed as “you”. “Licensees” and “recipients” may be individuals or organizations.

To “modify” a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a “modified version” of the earlier work or a work “based on” the earlier work.

A “covered work” means either the unmodified Program or a work based on the Program.

To “propagate” a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To “convey” a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays “Appropriate Legal Notices” to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The “source code” for a work means the preferred form of the work for making modifications to it. “Object code” means any non-source form of a work.

A “Standard Interface” means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The “System Libraries” of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A “Major Component”, in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The “Corresponding Source” for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to “keep intact all notices”.

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an “aggregate” if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A “User Product” is either (1) a “consumer product”, which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, “normally used” refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

“Installation Information” for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An “entity transaction” is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A “contributor” is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's “contributor version”.

A contributor's “essential patent claims” are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, “control” includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a “patent license” is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To “grant” such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. “Knowingly relying” means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is “discriminatory” if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License “or any later version” applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

GNU Lesser General Public License

Version 3, 29 June 2007

Copyright © 2007 Free Software Foundation, Inc. <https://fsf.org/>

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

This version of the GNU Lesser General Public License incorporates the terms and conditions of version 3 of the GNU General Public License, supplemented by the additional permissions listed below.

0. Additional Definitions.

As used herein, “this License” refers to version 3 of the GNU Lesser General Public License, and the “GNU GPL” refers to version 3 of the GNU General Public License.

“The Library” refers to a covered work governed by this License, other than an Application or a Combined Work as defined below.

An “Application” is any work that makes use of an interface provided by the Library, but which is not otherwise based on the Library. Defining a subclass of a class defined by the Library is deemed a mode of using an interface provided by the Library.

A “Combined Work” is a work produced by combining or linking an Application with the Library. The particular version of the Library with which the Combined Work was made is also called the “Linked Version”.

The “Minimal Corresponding Source” for a Combined Work means the Corresponding Source for the Combined Work, excluding any source code for portions of the Combined Work that, considered in isolation, are based on the Application, and not on the Linked Version.

The “Corresponding Application Code” for a Combined Work means the object code and/or source code for the Application, including any data and utility programs needed for reproducing the Combined Work from the Application, but excluding the System Libraries of the Combined Work.

1. Exception to Section 3 of the GNU GPL.

You may convey a covered work under sections 3 and 4 of this License without being bound by section 3 of the GNU GPL.

2. Conveying Modified Versions.

If you modify a copy of the Library, and, in your modifications, a facility refers to a function or data to be supplied by an Application that uses the facility (other than as an argument passed when the facility is invoked), then you may convey a copy of the modified version:

a) under this License, provided that you make a good faith effort to ensure that, in the event an Application does not supply the function or data, the facility still operates, and performs whatever part of its purpose remains meaningful, or

b) under the GNU GPL, with none of the additional permissions of this License applicable to that copy.

3. Object Code Incorporating Material from Library Header Files.

The object code form of an Application may incorporate material from a header file that is part of the Library. You may convey such object code under terms of your choice, provided that, if the incorporated material is not limited to numerical parameters, data structure layouts and accessors, or small macros, inline functions and templates (ten or fewer lines in length), you do both of the following:

a) Give prominent notice with each copy of the object code that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the object code with a copy of the GNU GPL and this license document.

4. Combined Works.

You may convey a Combined Work under terms of your choice that, taken together, effectively do not restrict modification of the portions of the Library contained in the Combined Work and reverse engineering for debugging such modifications, if you also do each of the following:

a) Give prominent notice with each copy of the Combined Work that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the Combined Work with a copy of the GNU GPL and this license document.

c) For a Combined Work that displays copyright notices during execution, include the copyright notice for the Library among these notices, as well as a reference directing the user to the copies of the GNU GPL and this license document.

d) Do one of the following:

0) Convey the Minimal Corresponding Source under the terms of this License, and the Corresponding Application Code in a form suitable for, and under terms that permit, the user to recombine or relink the Application with a modified version of the Linked Version to produce a modified Combined Work, in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.

1) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (a) uses at run time a copy of the Library already present on the user's computer system, and (b) will operate properly with a modified version of the Library that is interface-compatible with the Linked Version.

e) Provide Installation Information, but only if you would otherwise be required to provide such information under section 6 of the GNU GPL, and only to the extent that such information is necessary to install and execute a modified version of the Combined Work produced by recombining or relinking the Application with a modified version of the Linked Version. (If you use option 4d0, the Installation Information must accompany the Minimal Corresponding Source and Corresponding Application Code. If you use option 4d1, you must provide the Installation Information in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.)

5. Combined Libraries.

You may place library facilities that are a work based on the Library side by side in a single library together with other library facilities that are not Applications and are not covered by this License, and convey such a combined library under terms of your choice, if you do both of the following:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities, conveyed under the terms of this License.

b) Give prominent notice with the combined library that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

6. Revised Versions of the GNU Lesser General Public License.

The Free Software Foundation may publish revised and/or new versions of the GNU Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library as you received it specifies that a certain numbered version of the GNU Lesser General Public License “or any later version” applies to it, you have the option of following the terms and conditions either of that published version or of any later version published by the Free Software Foundation. If the Library as you received it does not specify a version number of the GNU Lesser General Public License, you may choose any version of the GNU Lesser General Public License ever published by the Free Software Foundation.

If the Library as you received it specifies that a proxy can decide whether future versions of the GNU Lesser General Public License shall apply, that proxy's public statement of acceptance of any version is permanent authorization for you to choose that version for the Library.

OpenSSL License

Copyright (c) 1998-2017 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

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

© 2025 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.