



FaceStation

User Manual

Version V1.0

www.supremainc.com

Safety Information

Please ensure that the warnings and cautions below are followed in order to prevent risk and damage to property by correctly using the product.

Warning

Violation of the instructions may lead to serious injury or death.

Installation

Avoid places with direct sunlight, high humidity, dust or soot.

- This may cause fire or electric shock.

Install in a dry place.

- Moisture may cause damage to the product or electric shock.

Install in a place with no heat such as a heater.

- Overheating may cause fire or electric shock.

Install in a place without electromagnetic interference.

- This may cause damage to the product or electric shock.

Usage

Do not disassemble, repair or remodel this product.

- This may cause fire, electric shock or injury.

Do not place a wet object or any object on the vent.

- There is a risk of electric shock or fire; the product may malfunction if the vent is covered.

Avoid liquids such as water, beverages and drugs from leaking into the product.

- There is a risk of electric shock or fire; the product may be damaged.

Caution

Violation of the instructions may lead to minor injury or damage to the product.

Installation

Do not leave a power cable or other cables in the passage way.

- This may damage the product or cause injury.

Usage

Do not press the touchscreen hard.

- This may cause malfunction.

Do not place the product near objects with a strong magnetic field such as a magnet, CRT, TV, monitor, or speaker.

- This may cause malfunction.

Clean the product with a dry cloth; avoid benzene or alcohol.

- Using chemicals or cleaning agents may deform the product.

Do not drop or apply physical shock.

- This may cause malfunction.

Contents

| | | | |
|--|-----------|---------------------------------------|-----------|
| 1 Getting Started | 6 | Connecting Fail Secure Lock | 19 |
| Features..... | 7 | Connecting with Automatic Doors | 19 |
| Components..... | 8 | Connecting Inputs | 20 |
| Name of Parts | 9 | Connecting Wiegand | 20 |
| | | Connecting Wiegand Input | 20 |
| | | Connecting Wiegand Output | 21 |
| 2 Installation | 11 | Connecting Mini USB | 21 |
| Installation | 12 | Connecting USB | 22 |
| Precautions for Installation | 13 | Connecting Video Phone | 22 |
| | | | |
| 3 Connection | 14 | | |
| Connecting Power | 15 | 4 Easy Use | 23 |
| Connecting with Wireless LAN | 15 | Registering Face | 24 |
| Connecting with Ethernet | 16 | Authenticating Face | 26 |
| Connecting with a PC | 16 | | |
| Connecting with Hub | 16 | | |
| Connecting RS485 | 17 | 5 Settings | 27 |
| Connecting with a PC..... | 17 | Setting Menu Overview | 28 |
| Connecting with Secure I/O and Other Devices | 17 | User Management | 30 |
| Connecting RS232 | 18 | Entering Administrator's Menu | 31 |
| Connecting Relays | 19 | Registering New User | 32 |
| Connecting Fail Safe Lock | 19 | Modifying User Information | 33 |
| | | Deleting User | 33 |

Contents

| | | | |
|--|-----------|--|-----------|
| Deleting All Users | 34 | Checking Device Information | 46 |
| Searching Users | 34 | Checking Memory Status | 47 |
| Checking User Capacity Information | 35 | TouchScreen Calibration | 47 |
| Setting Network | 35 | Device Reset..... | 48 |
| Setting TCP/IP | 36 | Reset to Default..... | 48 |
| Setting Server..... | 36 | Setting Display and Sound | 49 |
| Setting Serial Communication | 37 | Theme | 49 |
| Setting USB | 37 | Background | 49 |
| Using USB Memory Device | 38 | Voice Instruction | 49 |
| Using WLAN (Only for Wireless model)..... | 38 | Menu Timeout | 49 |
| Setting Operation Mode | 39 | Pop-Up Time | 49 |
| Setting Face Authentication | 39 | Backlight Timeout | 50 |
| Setting Card Authentication | 40 | Volume | 50 |
| Setting ID Authentication | 40 | Language | 50 |
| Setting Operations | 41 | Central Time Display..... | 50 |
| Setting Time and Attendance | 41 | Date Display | 50 |
| Setting Device | 42 | Viewing Logs..... | 50 |
| Setting Face..... | 43 | Log List | 51 |
| Setting Door..... | 43 | Log Search | 51 |
| Setting Interphone..... | 44 | Delete All Log | 52 |
| Setting Time..... | 46 | Log Info..... | 52 |

6 How to Use53

- Basic Screen View 54
 - Face Authentication Screen 54
 - Home Screen 54
 - Device Status Screen55
 - When Face Authentication is Set 56
 - When Card Authentication is Set..... 56
 - When ID Authentication is Set 56
 - Face Authentication Types 57
 - Card Authentication Types 57
 - ID Authentication Types 58
- Authenticating Time and Attendance 58
- Checking Time and Attendance59

Appendix..... 60

- Specifications.....61
 - Product Specifications61
 - Electric Specifications61
 - Optional Accessories.....61
- Cable Specifications62
 - Power Cable 62
 - 232 Cable..... 62
 - Relay Cable 62
 - RS485 Cable 62
 - Wiegand Cable..... 63
 - Video Phone Cable..... 63
 - Switch Cable 63
- Troubleshooting..... 64
- FCC Rules 64
- Device Font License..... 64
- Quality Assurance..... 66
- Index67

1 Getting Started







Features

Components

Name of Parts

Getting Started

Features

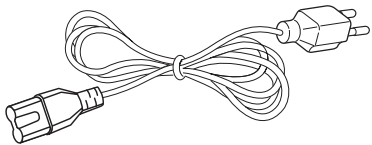
| | | |
|--|--|--|
| 4.3" Touchscreen LCD |  | The 4.3" WVGA touchscreen LCD is mounted on the front of the product and provides an intuitive GUI. It makes the user management easy while displaying various information including the time and attendance as well as notifications. |
| Next Generation Face Recognition Technology |  | The state-of-the-art technology with Suprema's proprietary algorithms stores both facial stamps using the visual camera and facial templates using the IR camera. The seamless combination of the information gathered makes Suprema's FaceStation the ultimate in facial recognition technology with query speeds of up to 1:1000 matches per second. |
| Various Interface Supported |  | You can connect with a PC and configure the network through various interfaces such as PoE, WiFi, TCP/IP, and RS485/232. Also, you can configure various access control systems through Wiegand and input/output ports. |
| Video Phone |  | FaceStation's built-in camera, microphone, and speaker provides the device the ability to be integrated with conventional analogue based videophones or IP based videophones to create a simple interphone system. |
| Various RF Cards Supported |  | Mifare Classic, Mifare Plus, and Mifare DesFire (CSN) cards are supported. |
| Powerful Dual-CPU Architecture |  | A powerful 1.1GHz DSP is dedicated to handling facial template operations and a 667MHz RISC processor ensures uninterrupted device operations. |

Components

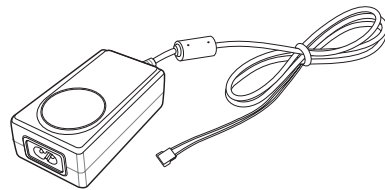
Device



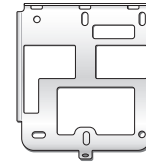
AC Power Cable (1)



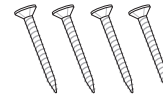
DC Power Supply (1)



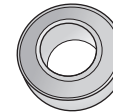
Wall Mounting Bracket (1)



Screws (4)



Ferrite Core (1)



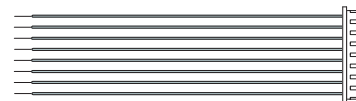
232 Cable (1)



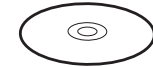
RS485 Cable (2)



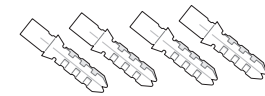
Switch Cable (1)



Software CD (1)



PVC Anchors (4)



Power Cable (1)



Relay Cable (2)



Wiegand Cable (1)



Video Phone Cable (1)



Name of Parts

Front



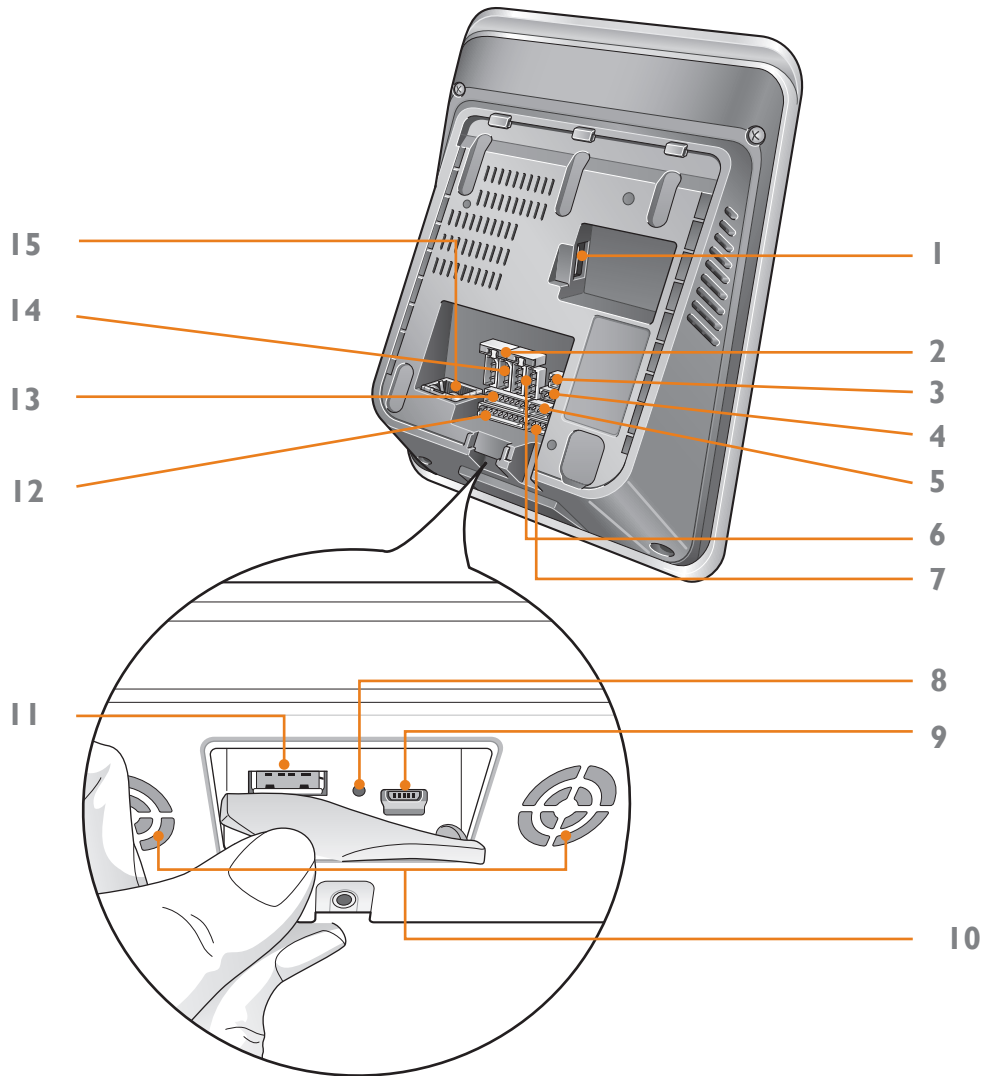
| | | |
|---|----------------------------|---|
| 1 | LCD Touchscreen | Used to display the device operating status and device operation. |
| 2 | Call Button | Used to place a call on the interphone. |
| 3 | Light LED | Used as a general lighting. |
| 4 | Infrared (IR) LED | Used as an IR light. |
| 5 | Camera | Detects and captures a face image. |
| 6 | Proximity Sensor | Determines the user's proximity. |
| 7 | Basic T&A Button (F1 - F4) | Selects Time and Attendance events. |
| 8 | Microphone | Used for speaking while connected via the interphone. |

Note

The RF cameras built in around the IR LED are used to detect an RF card.

Getting Started

Rear and Bottom



| | | |
|----|-----------------------------|--|
| 1 | USB Wireless LAN Terminal | Connects the USB wireless LAN. |
| 2 | Termination Resistor Switch | Activates the RS485 terminal resistance. |
| 3 | PWR IN Terminal | Connects the power cable. |
| 4 | RS232 Terminal | Connects the RS232 3-pin connector. |
| 5 | Debug Terminal | |
| 6 | RS485 Terminal | Connects the RS485 4-pin connector. |
| 7 | Wiegand Terminal | Connects the Wiegand 5-pin connector. |
| 8 | Reset Button | Resets the device. |
| 9 | Mini USB Connect Terminal | Connects with a PC. |
| 10 | Speaker | Outputs a voice on the device. |
| 11 | USB Connect Terminal | Connects a USB memory device. |
| 12 | Switch Input Terminal | Connects an input switch cable. |
| 13 | Phone Terminal | Connects a video phone cable. |
| 14 | Output Relay 1/2 Terminal | Connects Door Lock and output devices. |
| 15 | Ethernet Terminal | Connects an Ethernet cable. |



2 Installation

Installation

Precautions for Installation

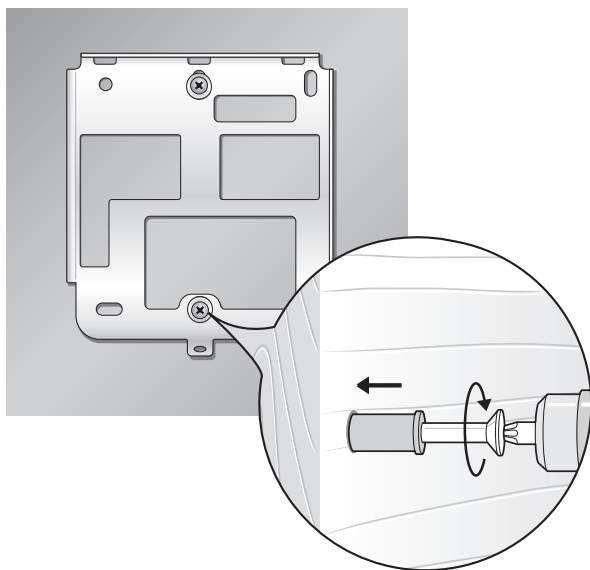
Installation

Installation

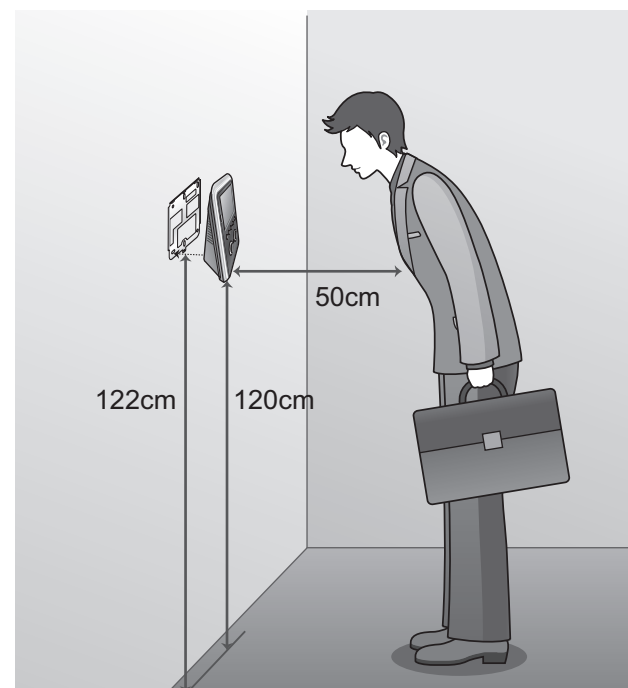
Since FaceStation has a built-in camera for face recognition and video interphone, the installation height needs to be considered. Select a location to install the device by considering the face capturing.

Installation

- 1 Fix the bracket at the desired location.
- 2 Drill a hole by using a drill and tools, insert anchors, and tightly fasten screws.



- 3 Mount the device on the fixed bracket.
- 4 Fix the fixing screws on the bottom of the device.



Note

- When installing the device for the first time, make sure to remove the transparent film from it. Otherwise, it may affect adversely on the face recognition.

Installation

Precautions for Installation

Recommended Installation Height

- The optimal installation height is 120cm.
(Based on the user's height between 155cm - 205cm)
- It is recommended that you adjust the installation height based on the shortest person of all the users.
- If you install devices for a same user group in many places, it is recommended that you make all of them all the same height.
- It is recommended that you install the device by considering the recommended installation height based on the bottom heights of device and bracket.

| Recommended Installation Height | | Range of User's Height | |
|---------------------------------|-----------------------|------------------------|---------|
| Bottom of the device | Bottom of the bracket | Minimum | Maximum |
| 90cm | 92cm | 125cm | 175cm |
| 100cm | 102cm | 135cm | 185cm |
| 115cm | 117cm | 145cm | 195cm |
| 120cm | 122cm | 155cm | 205cm |

Installation Location

- The device must be installed indoors.
- When installing the device near a window, install the device at least 3 meters away from the window.
- Avoid a place where there is direct sunlight on the face or from behind.
- Make sure not to install the device under incandescent light bulbs.

3 Connection

Connecting Power

Connecting with Wireless LAN

Connecting with Ethernet

Connecting RS485

Connecting RS232

Connecting Relays

Connecting Switch

Connecting Wiegand

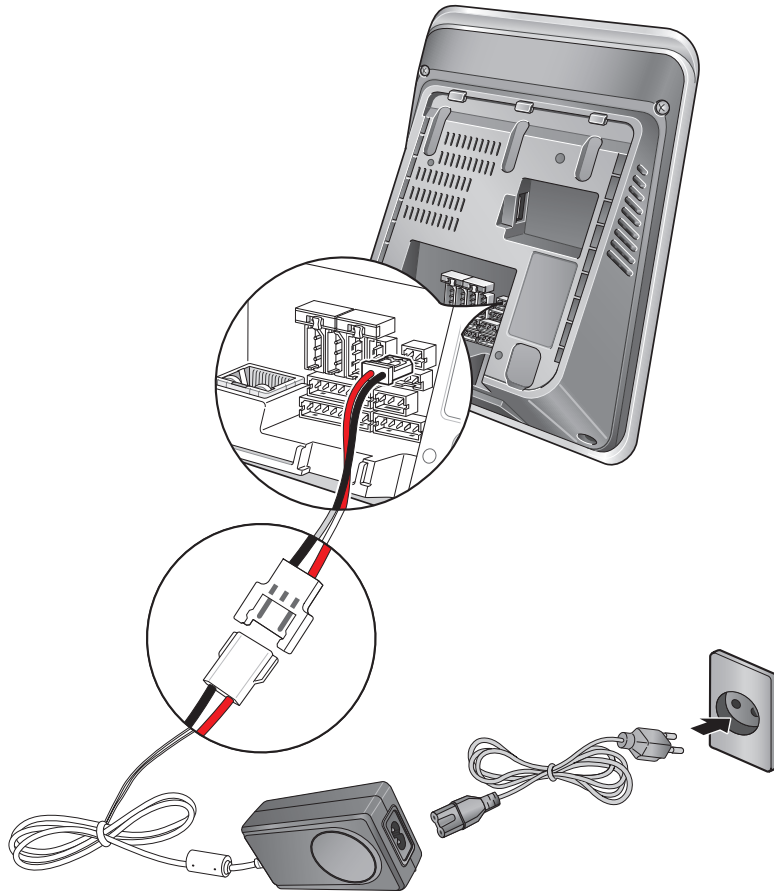
Connecting Mini USB

Connecting USB

Connecting Video Phone

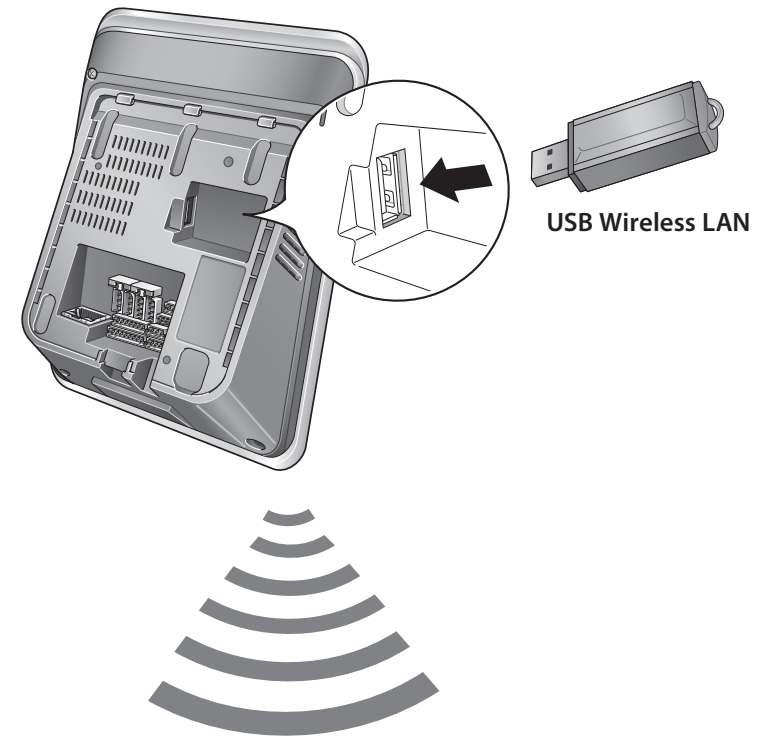
Connection

Connecting Power



Connecting with Wireless LAN

A model supporting the wireless LAN (WLAN) is equipped with a USB WLAN module upon shipment.



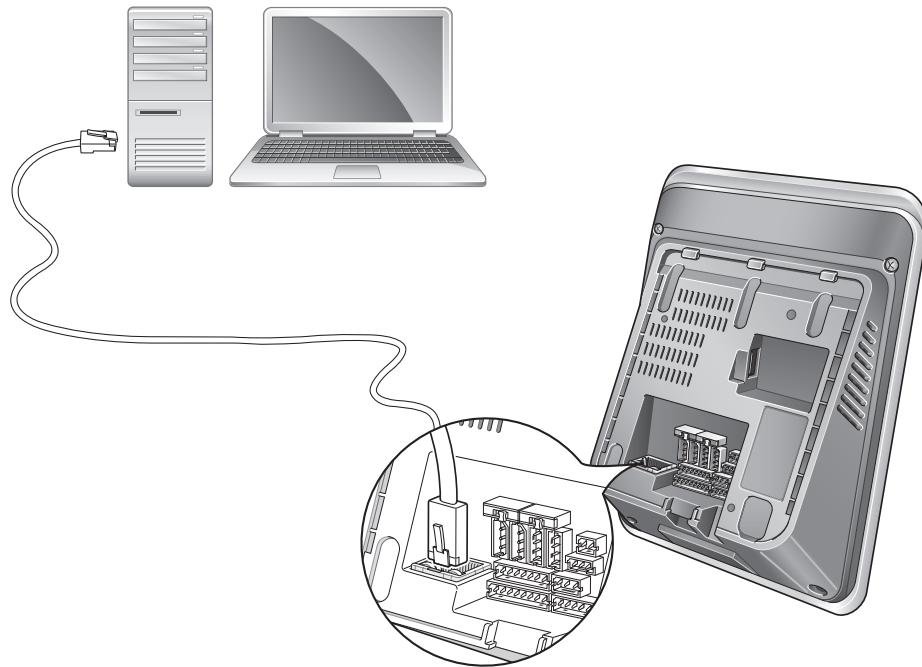
Note

- The performance of WLAN is greatly affected by the surroundings and the type of the access point (AP) in use.
- Some wireless AP may cause a problem when connecting with WLAN due to a hardware compatibility issue.

Connecting with Ethernet

Connecting with a PC

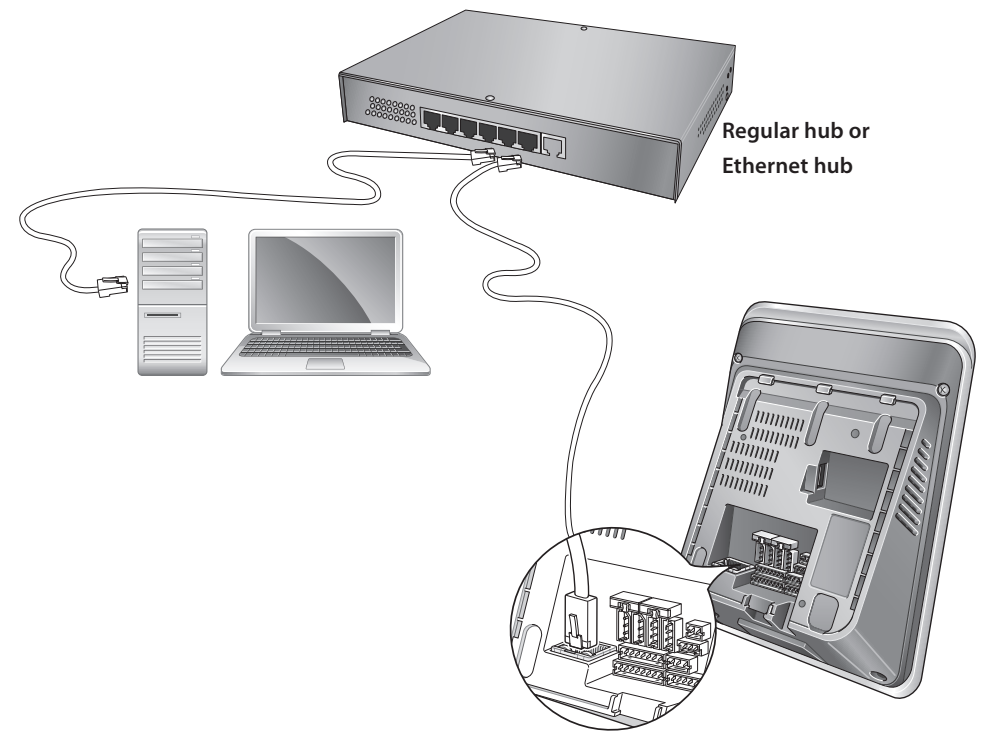
The device can communicate with a PC by directly connecting with the Ethernet cable.



Connecting with Hub

The device can be connected with a regular hub or PoE hub by connecting the Ethernet cable to the Ethernet terminal.

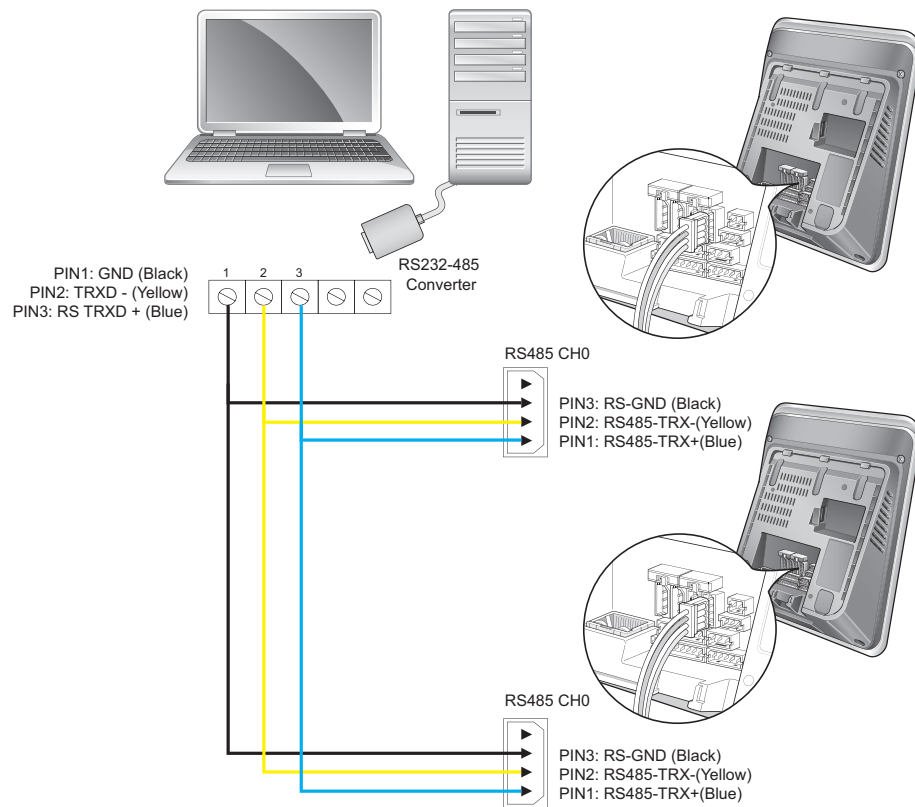
PoE (Power over Ethernet) is an Ethernet connection of which the power is supplied from PSE (Power Sourcing Equipment) satisfying the IEEE802.3af standard.



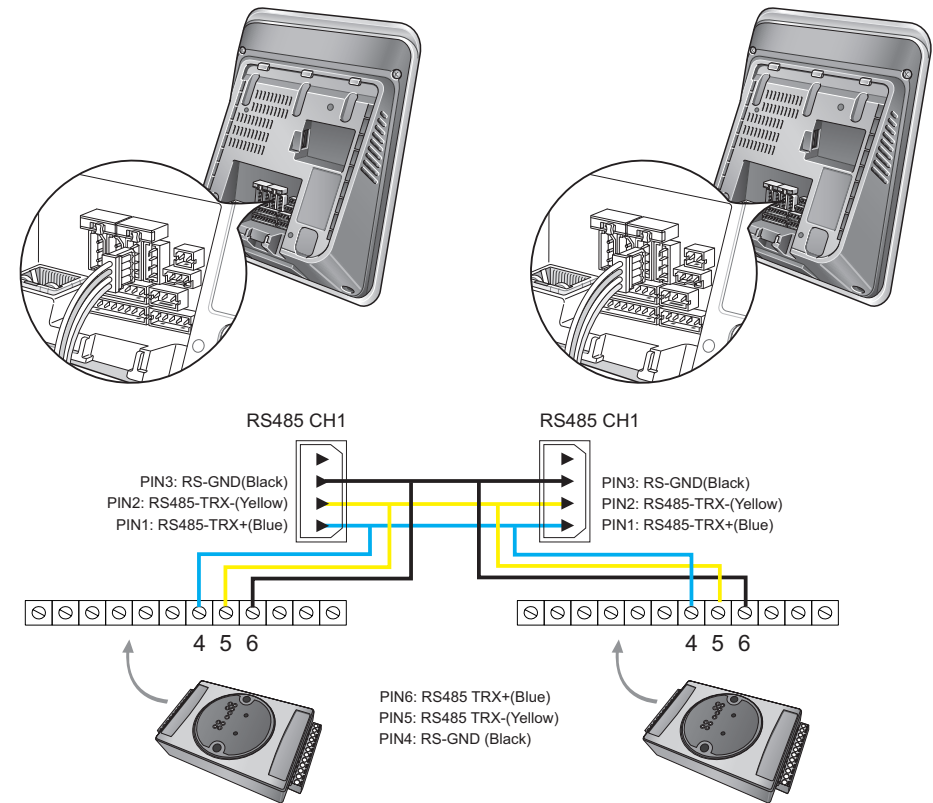
Connecting RS485

By using the RS485 wiring, several devices can be connected with a PC or a device can be connected with a secure I/O or another device.

Connecting with a PC



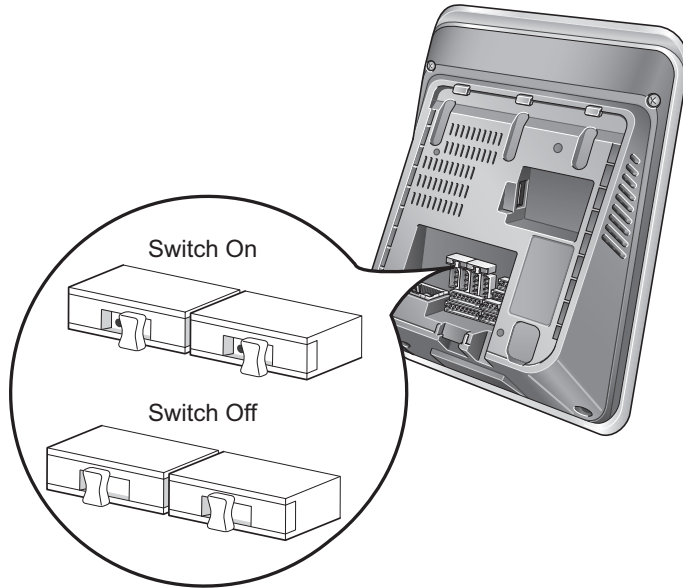
Connecting with Secure I/O and Other Devices



Connection

Note

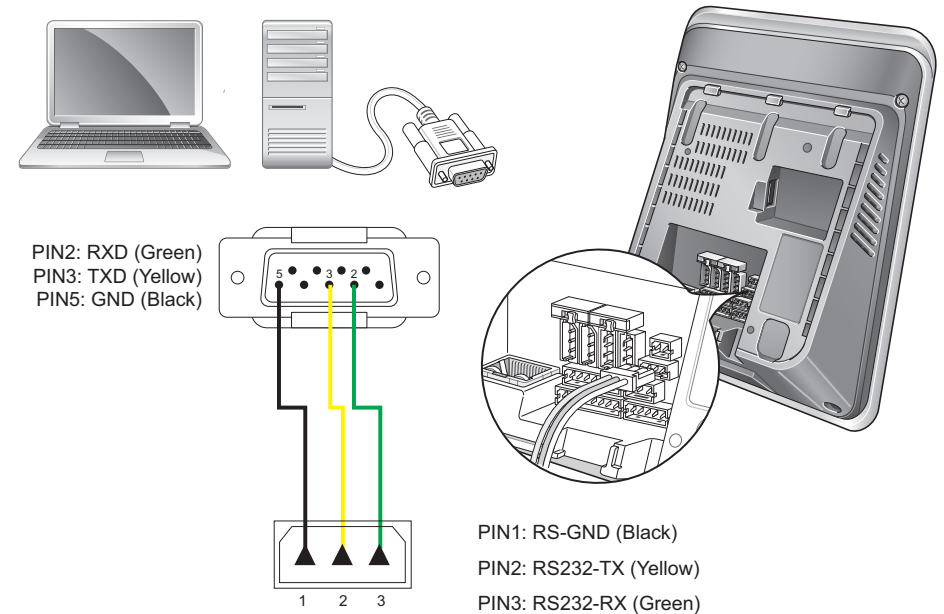
- When the RS485 wiring is long, turn on the dip switch to add terminating resistance in order to prevent weakening of the signal and to properly deliver the signal.



- When the wiring is too short, adding resistance affects the signal. By considering the length of the cable and signal status, turn on/off the termination resistor switch.
- If GND is not connected, either the RS485 chip may be damaged or it may not properly communicate.
- The RS485 communication between devices can be configured with 1 host device and up to 7 slave devices. When configuring such communication, up to 4 Secure I/O can be connected.

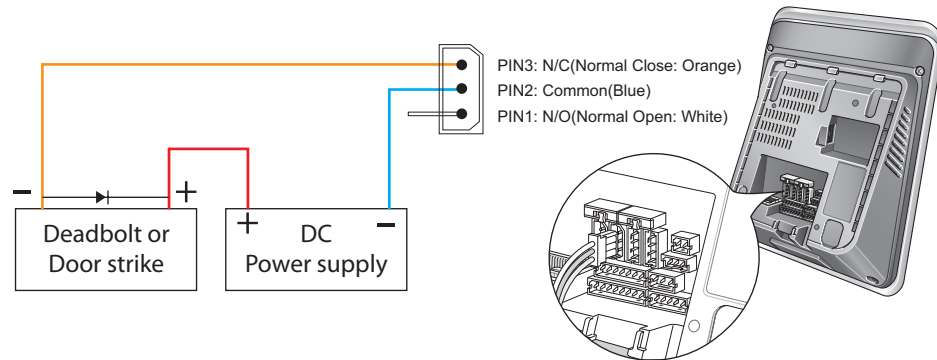
Connecting RS232

The device can be connected with a PC through RS232 wiring.

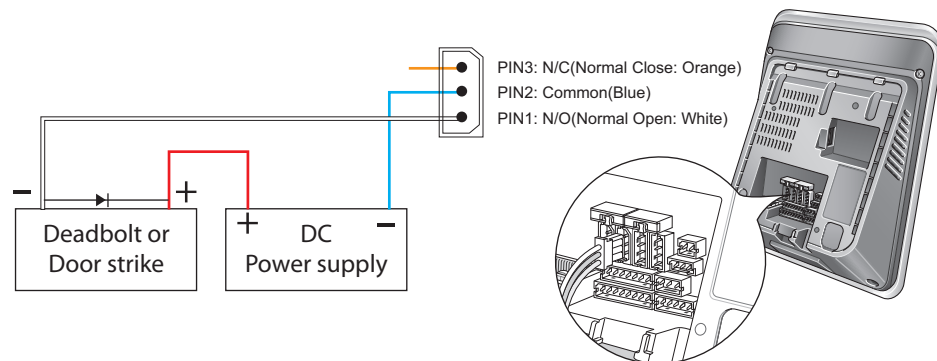


Connecting Relays

Connecting Fail Safe Lock



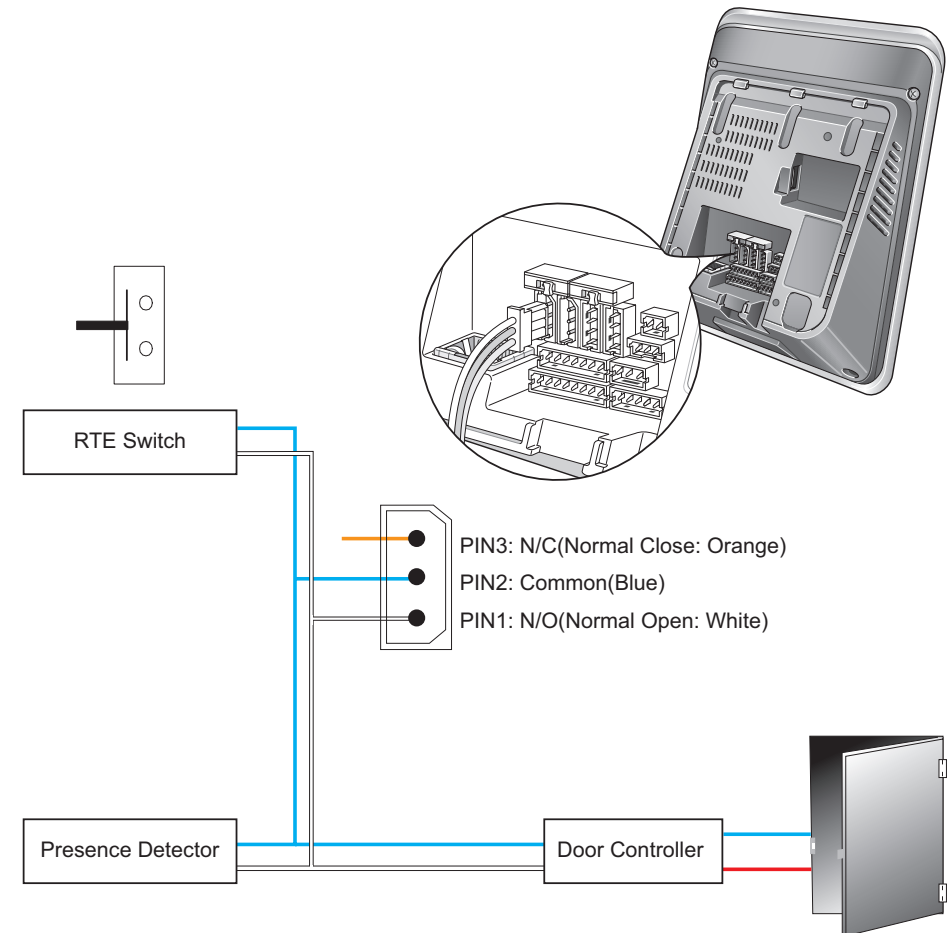
Connecting Fail Secure Lock



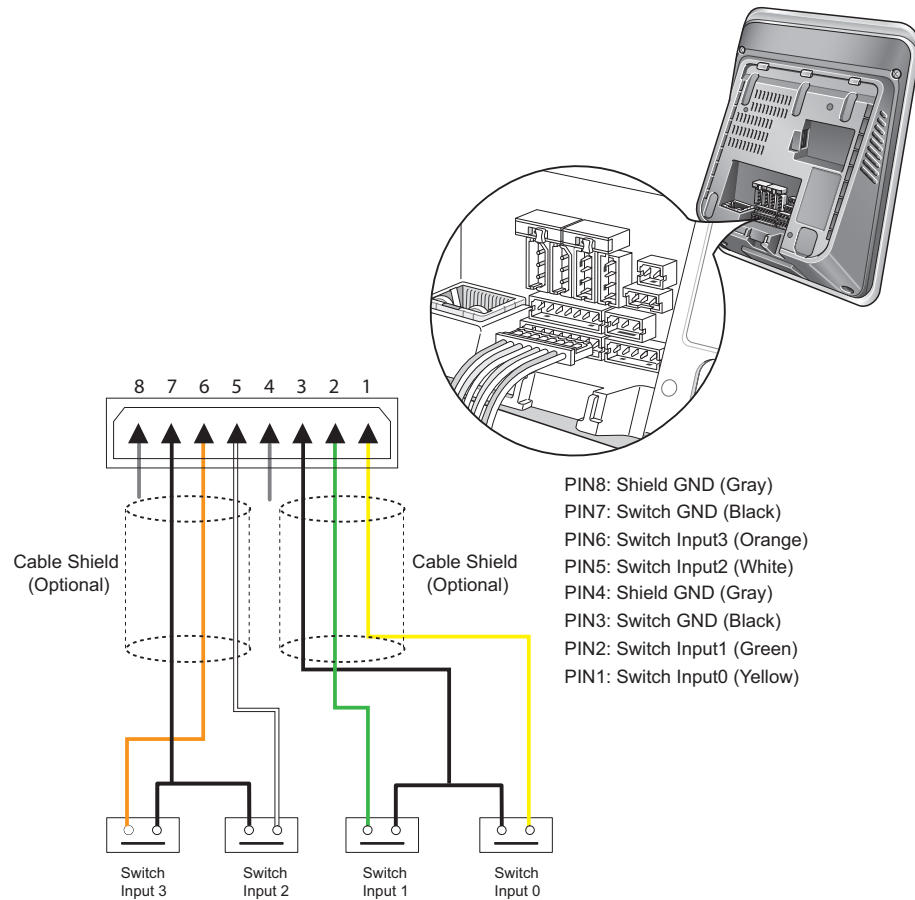
Note

- Normally Open/N.O: The electricity does not flow when there is no control signal but flows when there is a control signal.
- Normally Close/N.C: The electricity flows when there is no control signal but does not flow when there is a control signal.

Connecting with Automatic Doors

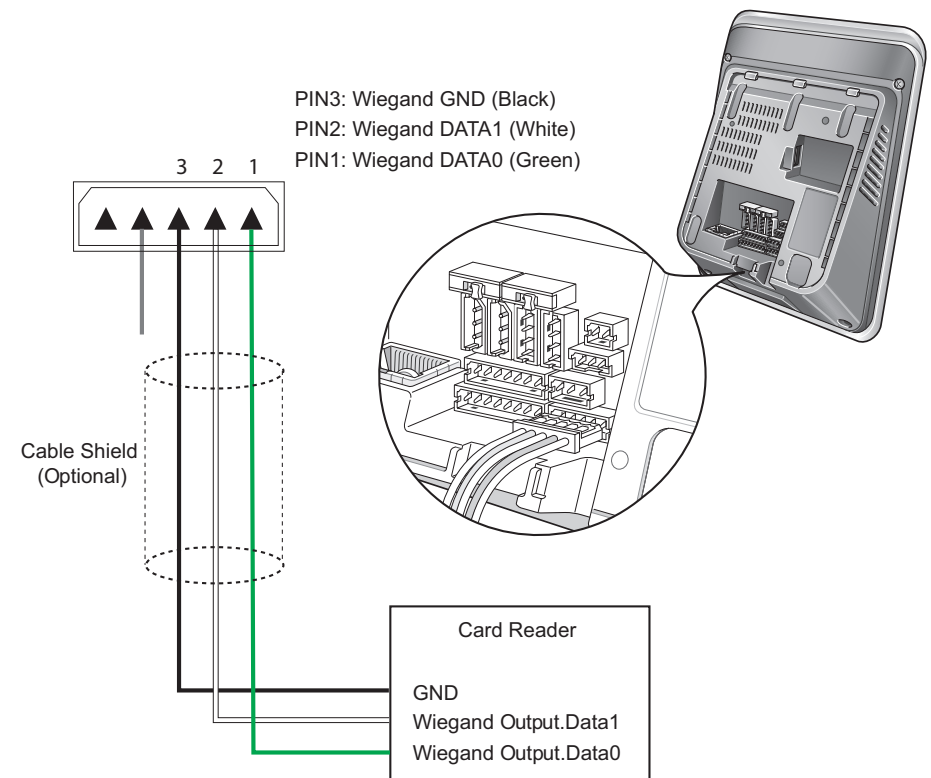


Connecting Inputs



Connecting Wiegand

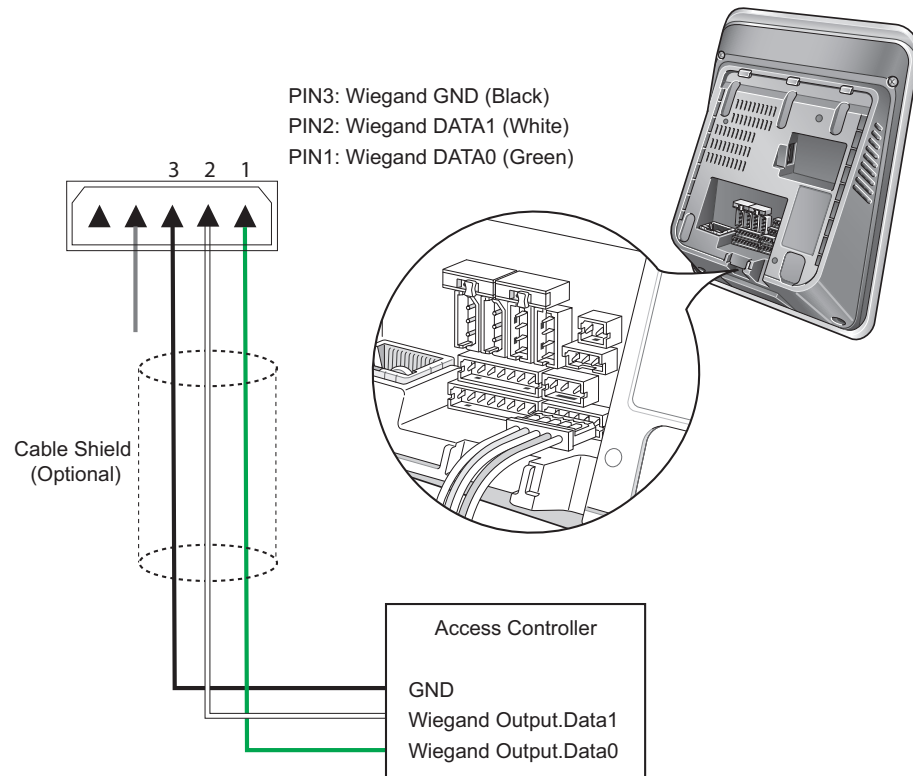
Connecting Wiegand Input



Note

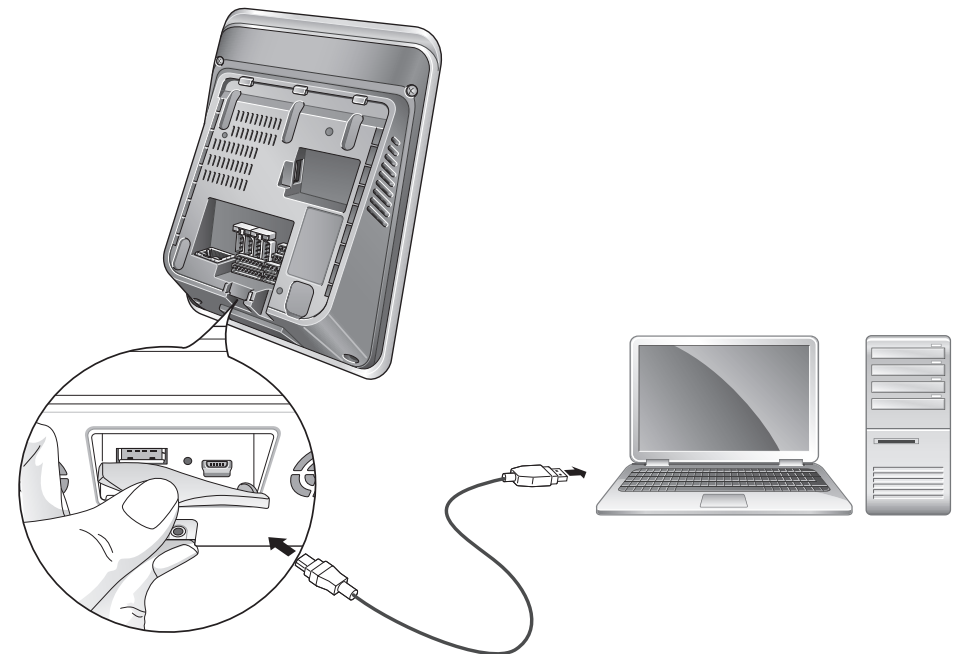
- Since there is a single Wiegand port, set to either input mode or output mode on the BioStar software.

Connecting Wiegand Output



Connecting Mini USB

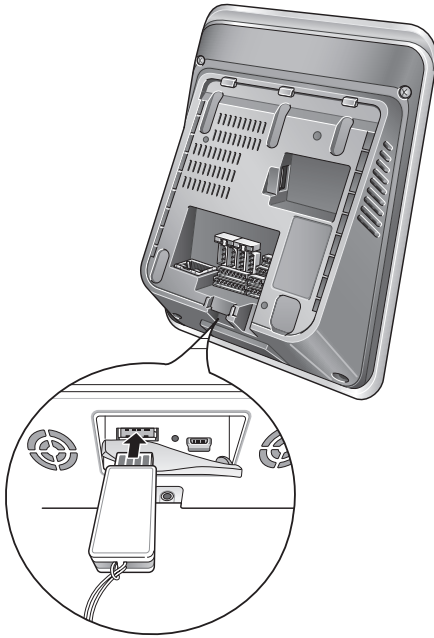
The device can be directly connected with a PC through the mini USB port.



Connection

Connecting USB

You can upload or download data from a USB memory device.

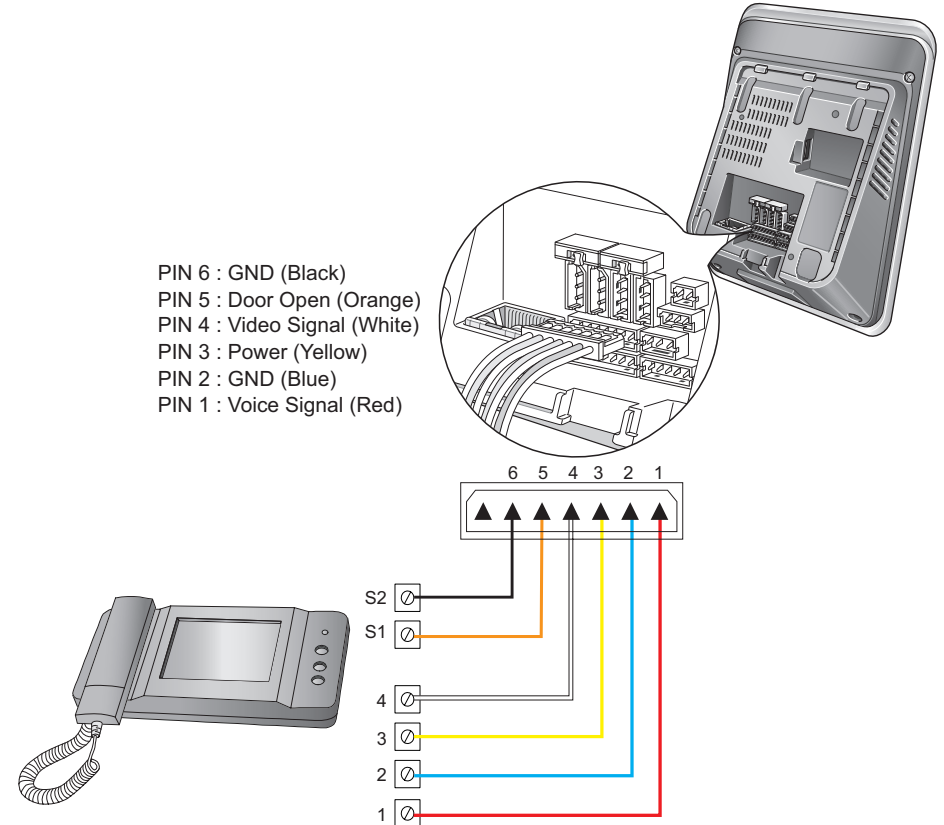


Note

- Some USB memory devices may not be recognized due to a hardware compatibility issue.

Connecting Video Phone

- PIN 6 : GND (Black)
- PIN 5 : Door Open (Orange)
- PIN 4 : Video Signal (White)
- PIN 3 : Power (Yellow)
- PIN 2 : GND (Blue)
- PIN 1 : Voice Signal (Red)



Note

- The videophones compatible with FaceStaion are as below;
COMMAX/ CAV-35N, COMMAX/ CAV-50H, COMMAX/ CAV-50P

4 Easy Use

Registering Face

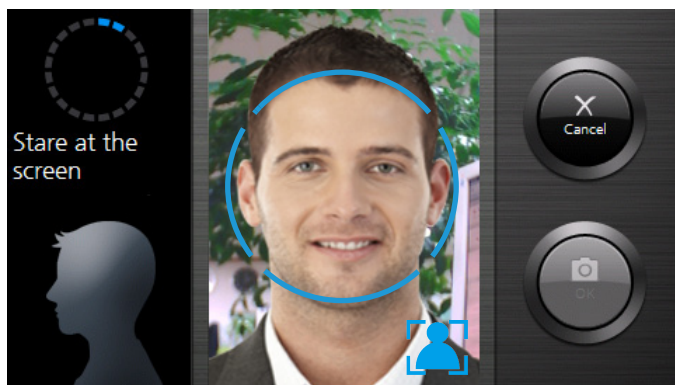
Authenticating Face

Registering Face

Go to **Menu > User > Enroll User** and press **Face** in order to register a face for authentication.

Registration Method

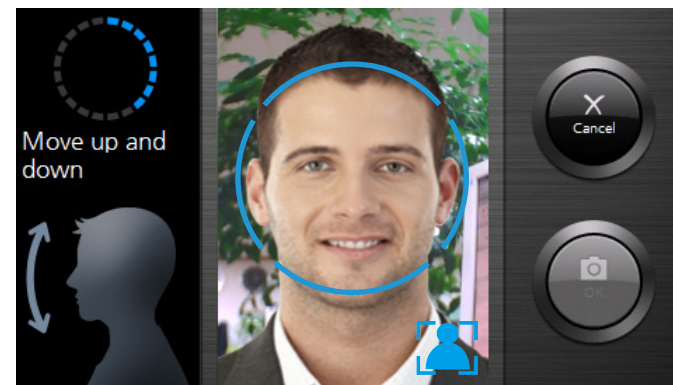
1 Stare at the screen.



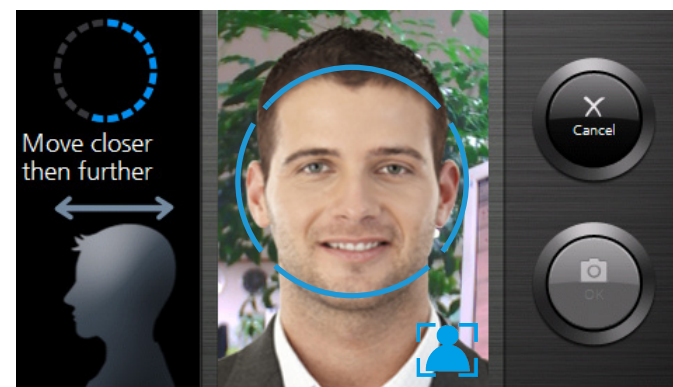
Note

- When a face is detected on the sensor of the device, the orange guide line turns to blue.
- Follow the face recognition instructions until the dotted circle on the left of the screen is completed.

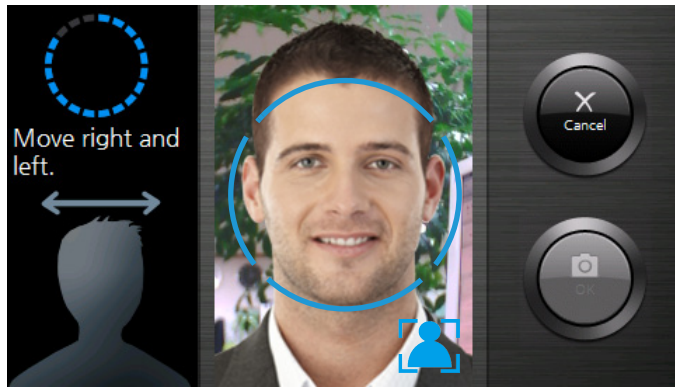
2 Move your face up and down.



3 Move your face back and forth.



4 Move your face right and left.

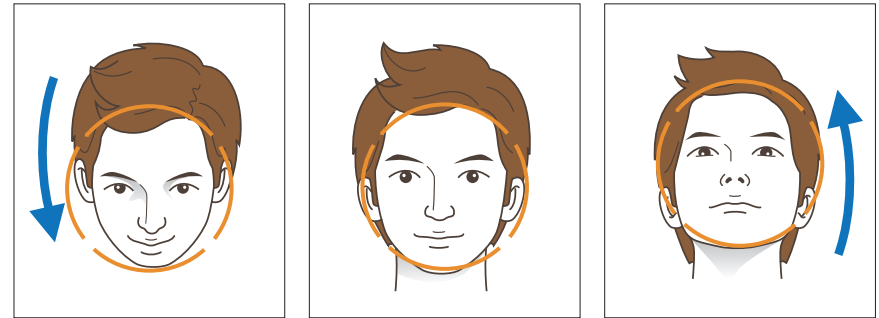


5 Press **OK** to complete the registration.
Press **Cancel** to cancel the face registration.

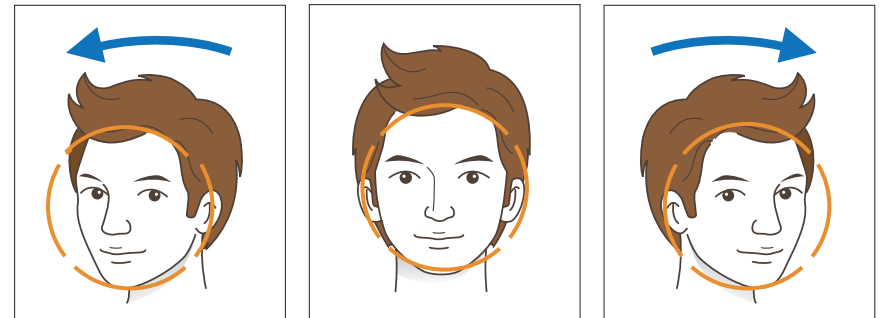
Precautions for Registration

- It is recommended that you register your face at the installation site.
- Register an expressionless face.
- It is recommended that you keep the distance of about 40 to 80 cm from the device screen when registering your face.
- When initially registering the front of the face, the authentication performance may be deteriorated if you face up. Make sure to stare at the screen.
- When initially registering the front of the face, the registration may take longer if no movement is detected. When registering the front of the face, slightly move the face.
- When moving the face back and forth, step back and forth in order to improve the authentication performance.
- Make sure to take off a hat and to make the face with the eyebrows exposed in order not to cover the lower part of the face with hairs.
- If a user frequently switches between wearing glasses and no glasses, change the look of wearing glasses when registering left and right images.
- Make sure that more than two people's faces should not be registered on the screen at the same time.
- If the face moves up, down, left, or right or if the instructions for moving the face forward or backward are not followed while registering, the registration may take longer. Please follow the registration instructions.

• When moving your face up and down



• When moving your face left and right



• When moving your face back and forth



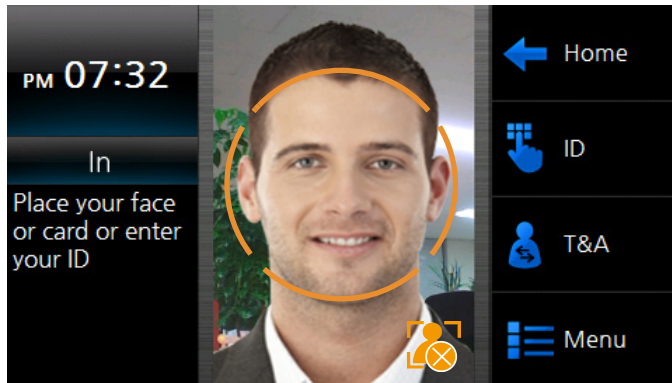
Authenticating Face

When **Menu > Mode > Face Auth Mode > Face** is set as **Always**, the authentication screen is activated when the user is in close proximity to the device.

Authentication Method

Align your face with the orange guide line turns to blue, circular line on the authentication screen.

When the orange guide line turns to blue, keep your face still while aligned with the blue line and wait until the authentication is complete.

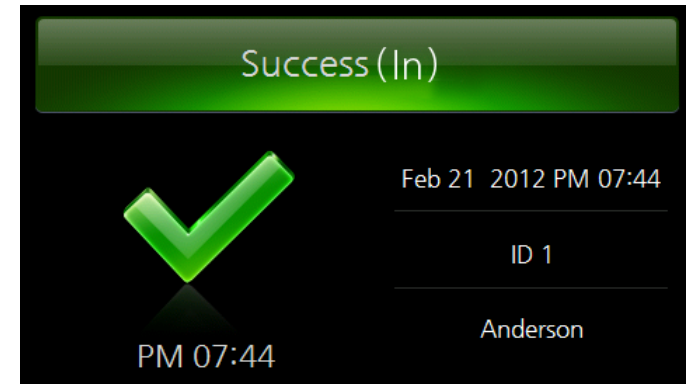


Note

- When a face is detected on the sensor of the device, the orange guide line turns to blue on the authentication screen. Do not move your face while the authentication is in progress.
- Make sure to keep the distance of 50cm from the device when authenticating the face.

2

The authentication completion screen is displayed if the user authentication is completed.



Note

- When authentication is completed on the face authentication screen after you press **Menu**, you can enter the Administrator's menu.

Precautions for Authentication

- Position the face within the orange circle on the screen.
- If the authentication takes too long, either move the chin up and down or step back and forth.
- If hairs on the side covers a part of the face including the eyebrows, the authentication may not perform well. It is recommended that you authenticate the face with the eyebrows exposed.
- If the user changes glasses, the authentication may fail. It is recommended to re-enroll the user's face with new glasses.
- When wearing sunglasses, the authentication is not possible. It is recommended you take it off before authentication.

Precautions for Usage

- It is recommended you set the Authentication mode to '**Card+Face**' or '**ID+Face**' in order to strengthen the authentication security.
- It is recommended you set the Authentication mode to '**Card+Face**' since the authentication for twin users may not be correct.
- If the user's facial appearance has changed dramatically (such as plastic surgery or shaving bushy beard), it is recommended to re-enroll the user.

5 Settings

Setting Menu Overview

Setting Users

Setting Network

Using WLAN

Setting Operation Mode

Setting Device

Setting Display and Sound

Viewing Logs

Setting Menu Overview

| | | |
|---------|--------------------|------------------|
| User | Enroll User | |
| | Edit User | |
| | Search | |
| | User Capacity Info | |
| | Delete All Users | |
| Network | TCP/IP | LAN Type |
| | | Port |
| | | Max Conn |
| | | DHCP |
| | | IP Address |
| | | Gateway |
| | | Subnet |
| | Server | Use Server |
| | | Server IP |
| | | Port |
| | Serial | RS485-PC |
| | | RS485-NET |
| | | RS232 |
| | USB | USB |
| | | USB Memory |
| | USB Memory | Import |
| | | Export |
| | | Firmware Upgrade |
| | WLAN | |

| | | |
|--------------|----------------|---------------------|
| Mode | Face Auth Mode | Face |
| | | Face+Pin |
| | | T&A Key > Face |
| | | T&A Key > Face+PIN |
| | | Face > T&A Key |
| | | Face+Pin > T&A Key |
| | Card Auth Mode | Card Only |
| | | Card+PIN |
| | | Card+Face |
| | | Card+Face/PIN |
| | | Card+Face+PIN |
| | | |
| | ID Auth Mode | ID+PIN |
| | | ID+Face |
| | | ID+Face/PIN |
| | | ID+Face+PIN |
| | Operation | Face Detection |
| | | Dual Authentication |
| | | Card Mode |
| | | Individual Auth |
| | | Match Timeout(sec) |
| T&A | | |
| Camera Event | | |

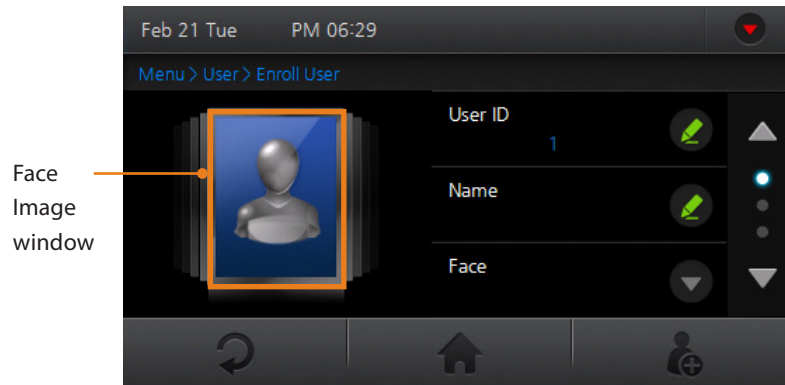
| | | |
|---------------|-------------------------|------------------------|
| Device | Face | Security Level |
| | | Enrollment Sensitivity |
| | Door | Relay |
| | | Driven By |
| | | Duration |
| | | RTE(Exit SW) |
| | | RTE Type |
| | | Door Sensor |
| | | Door Sensor Type |
| | | Held Open Period(sec) |
| | | Unlock Time |
| | | Lock Time |
| | | Exit Relay Device ID |
| | | Interphone |
| | VoIP Setting | |
| | BS VideoPhone Setting | |
| | Date & Time | Date |
| | | Time |
| | | Time Sync |
| | Device Info | |
| | Memory Info | |
| | Touchscreen Calibration | |
| | Reset | |
| | Factory Default | |

| | | |
|----------------|----------------------|------------|
| Display | Theme | |
| | Background | |
| | Voice Instruction | |
| | Menu Timeout | |
| | Pop-Up Time | |
| | Backlight Timeout | |
| | Volume | |
| | Language | |
| | Central Time Display | |
| | Date Display | |
| | Log | Log List |
| | | Log Search |
| Delete All Log | | |
| Log Info | | |

Settings

User Management

After the device installation, register the administrator before use. The administrator can register and delete users and set preferences.



Registering Administrator

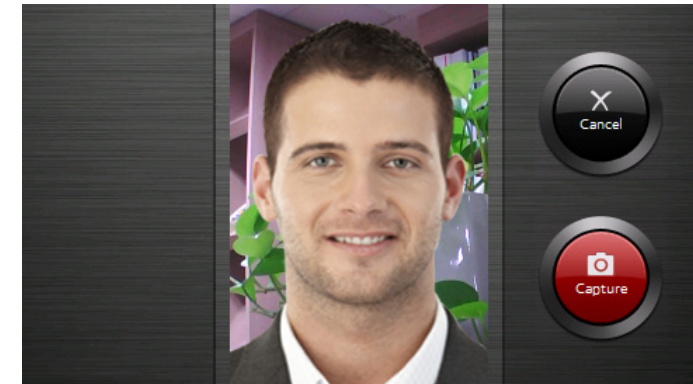
Setup

1 Go to **Menu > User > Enroll User**.

Register the administrator's picture.

- 1) Press the Face image window for registering the administrator's face picture.
- 2) Align your face in the screen and press **Capture**. The captured face image will be registered.
Press **Cancel** to cancel the registration.

2



3

- **User ID** Enter the user ID.
- **Name** Enter your name and press **OK**.
- **Faces** Register your face. For details regarding face registration, please refer to '**Registering Face**(page 24)'
- **Card** Enter the ID and press **OK**.
- **PIN** Enter the pin number and press **OK**.
- **Administrator** Select the administrator level.

4

Press . The administrator will be registered.

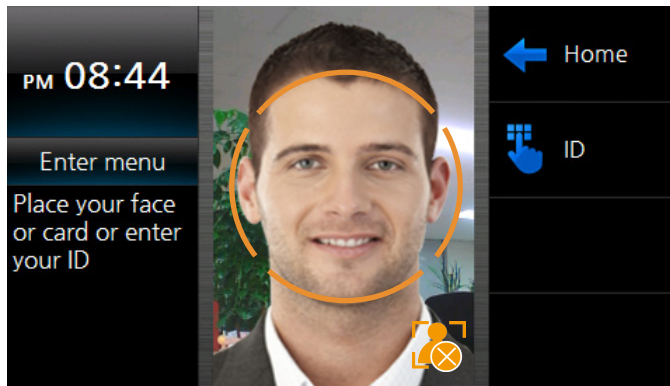
Entering Administrator's Menu

Setup

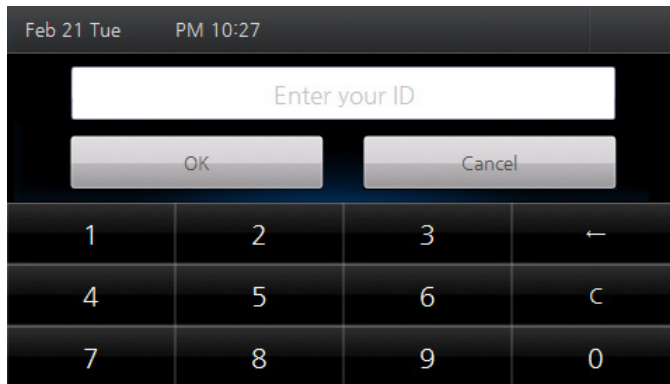
1) Press **Menu** on the Home screen. The administrator's menu is displayed.

1) Scan the face or enter the card.

2

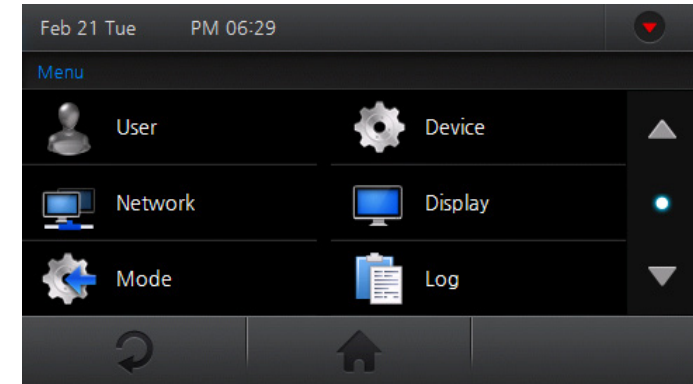


2) Enter the ID. And enter the pin number or face.



Go to the administrator's menu and set each item.

3

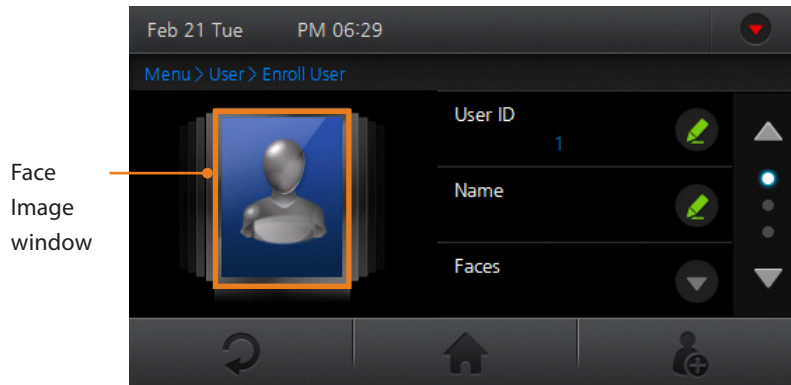


Note

- If you press **Menu** while no user is registered, the administrator's menu is displayed without any authentication process.
- When a general user follows the process to enter the administrator's menu, the user can view the event log for the time and attendance.
- Regardless of a previously set authentication mode, you can move to the administrator's menu by Face authentication, Card authentication, and ID + Face/Pin authentication.

Registering New User

You can register a new user on the device.

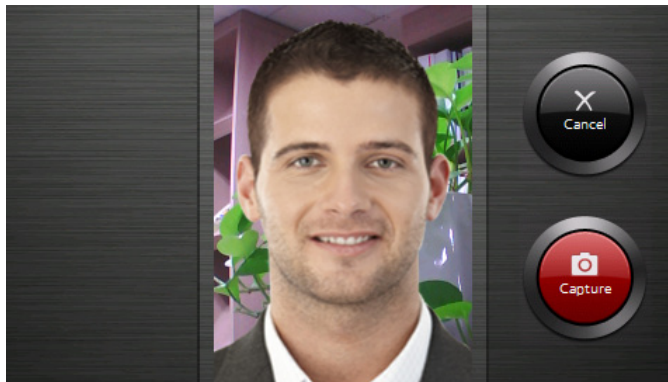


Go to **Menu > User > Enroll User**.

Register the user's picture.

- 1) Press Face Image window for registering the user's picture.
- 2) Align your face in the screen and press **Capture**. The captured facial image will be registered.
Press **Cancel** to cancel the registration.

2



3

- **User ID** Enter the user ID.
- **Name** Enter your name and press **OK**.
- **Faces** Register your face. For details regarding face registration, please refer to '**Registering Face**(page 24)'
- **Card** Enter the card **ID** by placing the card on the device.
- **PIN** Enter the pin number and press **OK**.
- **Administrator** Check on the administrator level to register as the administrator.
Uncheck if registering as a general user.
- **Bypass Card** If Bypass Card is checked when registering a user, the user is always authenticated regardless of the authentication mode on the device.
- **Individual Auth** A user registered with this mode is authenticated with the individually selected authentication mode instead of the device authentication mode.
The set individual authentication mode works only for the relevant authentication method. For higher security, it is recommended to set either '**Card+Face**' or '**ID+Face**'. For twins, it is recommended to set either '**Card+Face**' or '**ID+Face**'. After setting the mode, press **OK**.
- **Group** The access of group users can be set. A group can be selected from Access groups transferred from the BioStar software to the relevant device. After setting, press **OK**.

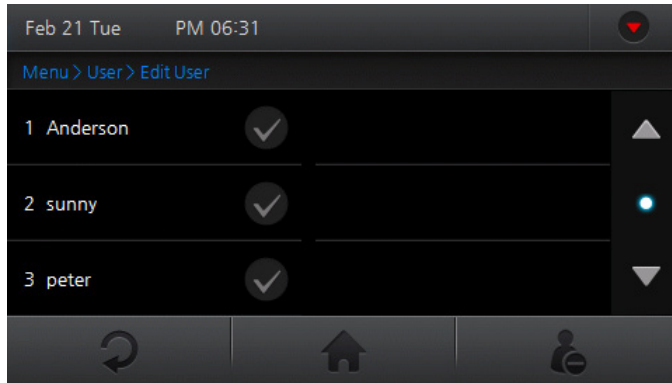
4

Press . You can register a new user.




Press or to exit without saving the changes. You can go to the previous screen or Home screen.

Modifying User Information

You can modify the registered user information.



Setup

- 1 Go to **Menu > User > Edit User**.
- 2 Select a user by pressing the user name field.
Modify the desired information.
- 3 Press  to save the modified information.
Press  or  to exit without saving the changes. You can go to the previous screen or Home screen.


Note

- The user ID cannot be modified.

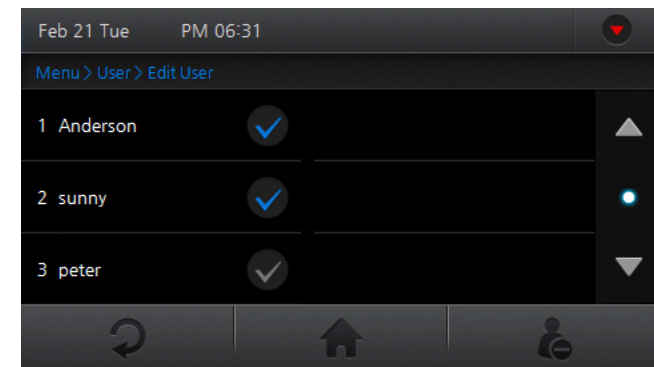
Deleting User

You can delete the desired user.

Setup

- 1 Go to **Menu > User > Edit User**.
- 2 Check a user to delete.
Press .

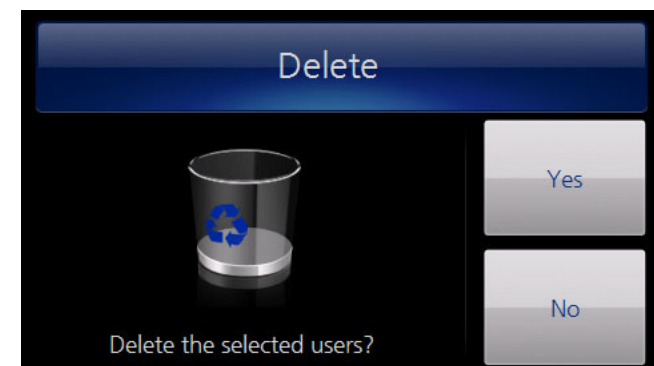
3



Press **Yes** to delete the selected user.

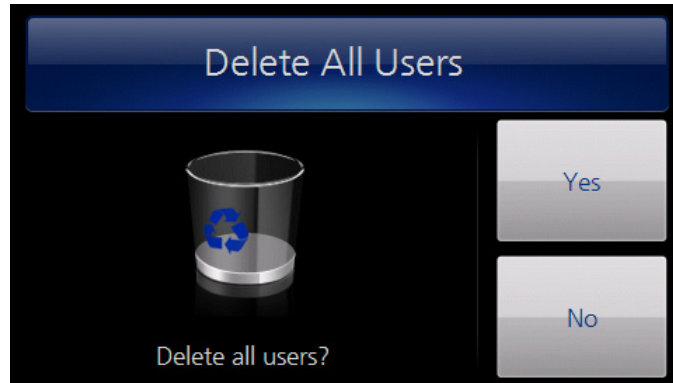
Press **No** to cancel the deletion.

4



Deleting All Users

You can delete all registered users.



Setup

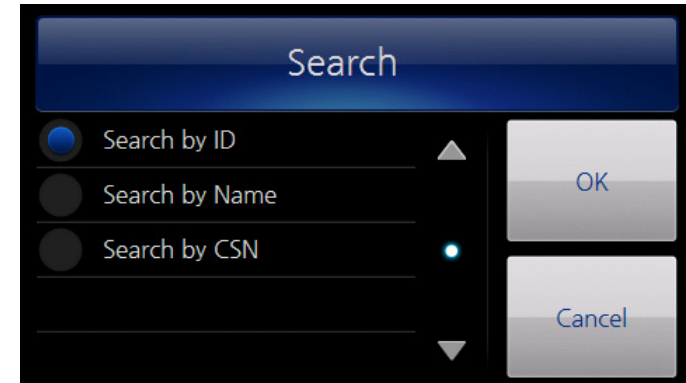
- 1 Press **Menu** > **User** > **Delete All Users**.
- 2 Press **Yes** to delete all registered users.
Press **No** to cancel the deletion.

Note

- When a user is deleted while not saved on the BioStar software database, the user cannot be restored.

Searching Users

You can search the registered users.

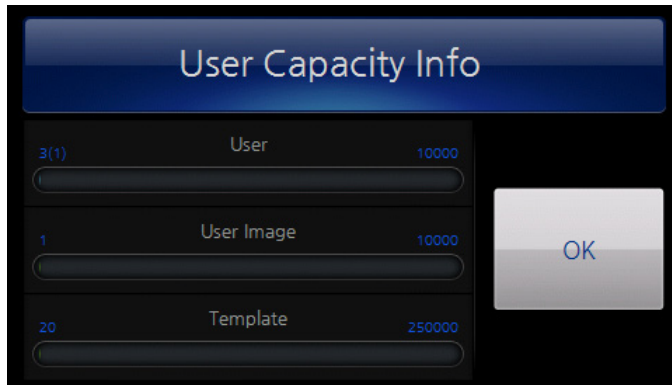


Setup

- 1 Go to **Menu** > **User** > **Search**.
- 2
 - **Search by ID** Enter an ID and press **OK**.
 - **Search by Name** Enter a name and press **OK**.
 - **Search by CSN** Enter the card.
- 3 Press **OK** to display the search results.
Press **Cancel** to cancel the search.

Checking User Capacity Information

You can view the registration information (total number of registered users, total number of registered user's images, and number of templates).



Setup

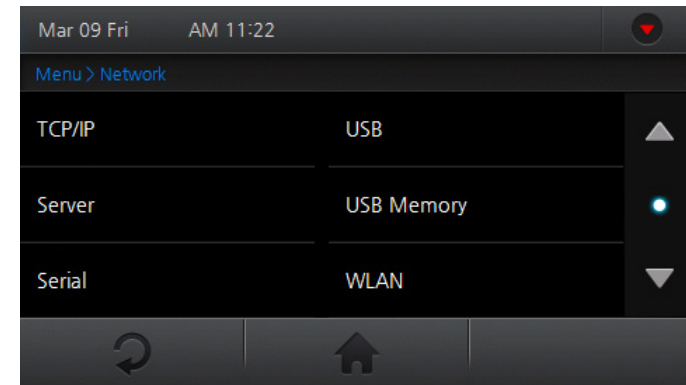
- 1 Go to **Menu > User > User Capacity Info**.
- 2 Press **OK** to return to the previous screen.

Note

- Up to 10,000 users along with their images can be stored.

Setting Network

You can set the communication method of the device.



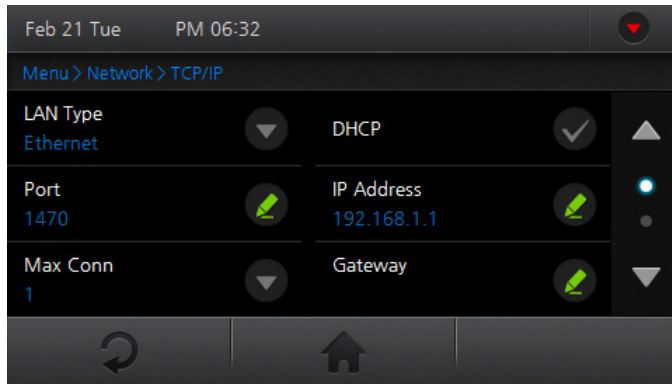
Setup

- 1 Go to **Menu > Network**.
- 2 Set the options.
- 3 Press **↶** or **🏠** to go to the previous screen or Home screen.

Settings

Setting TCP/IP

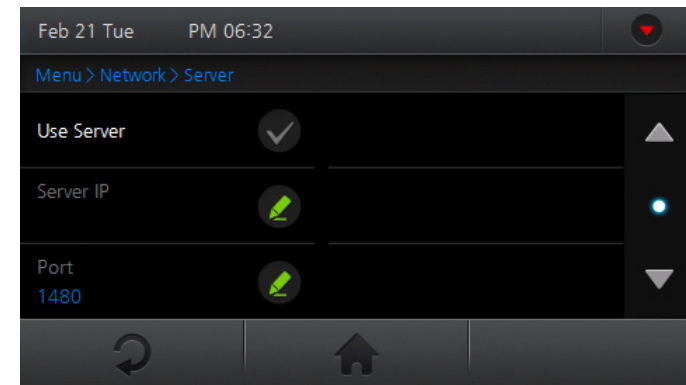
When the device and BioStar software is connected via TCP/IP method, you can set the relevant settings.



- 1 Go to **Menu > Network > TCP/IP**.
- 2 Set the options.
 - **LAN Type** Set the connection method and press **OK**.
 - **Port** Enter the port and press **OK**.
 - **Max Conn** Set the maximum number of clients to be concurrently connected with the device and press **OK**.
 - **DHCP** Check to enable DHCP.
 - **IP Address** Enter an IP address if a static IP address is used and press **OK**. If DHCP is checked, this item is not activated.
 - **Gateway** Enter a gateway address if a static IP address is used and press **OK**. If DHCP is checked, this item is not activated.
 - **Subnet** Enter the subnet mask if a static IP address is used and press **OK**. If DHCP is checked, this item is not activated.
- 3 Press or to go to the previous screen or Home screen.

Setting Server

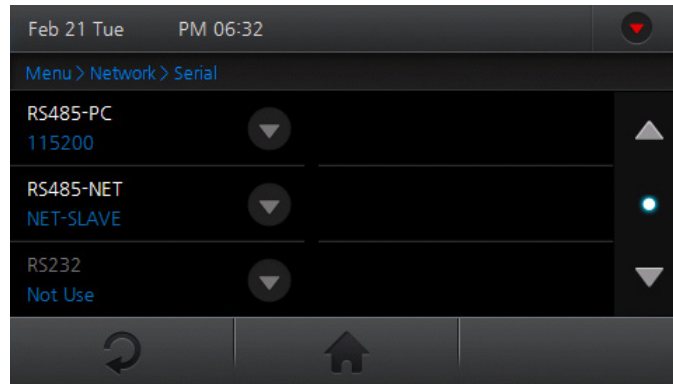
You should set the IP address and port of the server to connect in order to communicate with it.



- 1 Go to **Menu > Network > Server**.
- 2 Set the options.
 - **User Server** Check to use the server.
 - **Server IP** Enter the server's IP address and press **OK**. It can be set if User Server is checked.
 - **Port** Enter the server's port and press **OK**. It can be set if User Server is checked.
- 3 Press or to go to the previous screen or Home screen.

Setting Serial Communication

When the device is connected by RS485 or RS232, you can set the connection-related options.



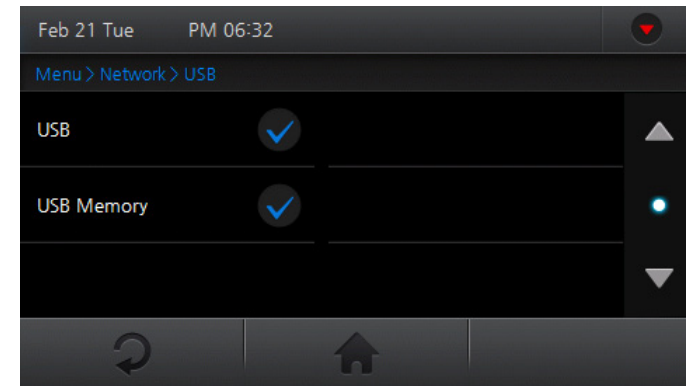
Setup

- 1 Go to **Menu > Network > Serial**.
- 2 Set the options and press **OK**.
 - **RS485-PC** You can enable/disable the RS485 port to connect with a PC and set the communication speed.
 - **RS485-NET** Enable or disable the RS485 port for communications between devices and set the communication mode. You can add the device as a host by setting **RS485-NET** to **NET-HOST**, and as a slave by setting it to **NET-SLAVE**.
 - **RS232** It can be set if RS485 is disabled. You can enable/disable the RS232 port to connect with a PC and set the communication speed.
- 3 Press **↶** or **🏠** to go to the previous screen or Home screen.

Note

- The RS485 communication between devices can be configured with 1 host device and up to 7 slave devices including up to 4 Secure I/O.

Setting USB



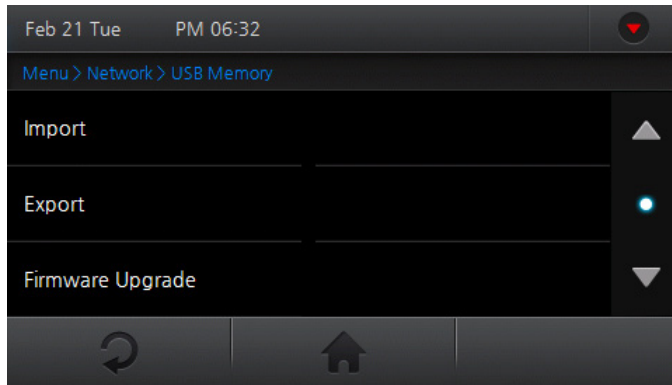
Setup

- 1 Go to **Menu > Network > USB**.
- 2 Set the options.
 - **USB** Set to allow the connection with a PC via USB.
 - **USB Memory** Set to allow the connection with a USB memory device.
- 3 Press **↶** or **🏠** to go to the previous screen or Home screen.

Settings

Using USB Memory Device

When setting to make USB available, you can select options to conduct the desired operations with the USB memory device.



Setup

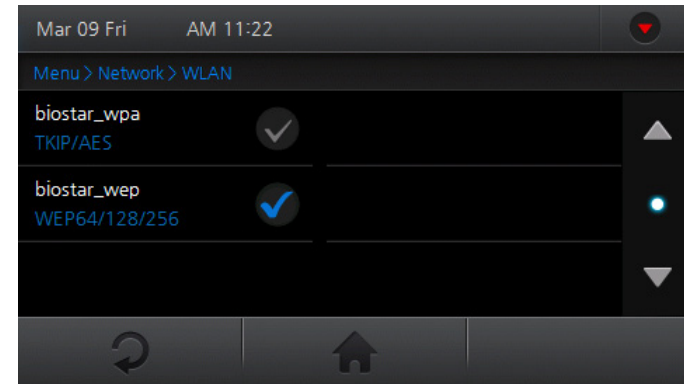
- 1 Go to **Menu > Network > USB Memory**.
- 2 Select an option.
 - **Import** Select a device ID to import data and press **OK**.
 - **Export** Press **Export** and wait until the job is completed.
 - **Firmware Upgrade** Select firmware to upgrade and press **OK**.
- 3 Press or to go to the previous screen or Home screen.

Note

- The USB Memory needs to be checked from **Menu > Network > USB** in order to activate the **USB Memory** menu.

Using WLAN (Only for Wireless models)

You can select one of 4 WLAN preset options previously saved from BioStar. On BioStar, you can set the preset options including SSID, encryption method, encryption key, etc.

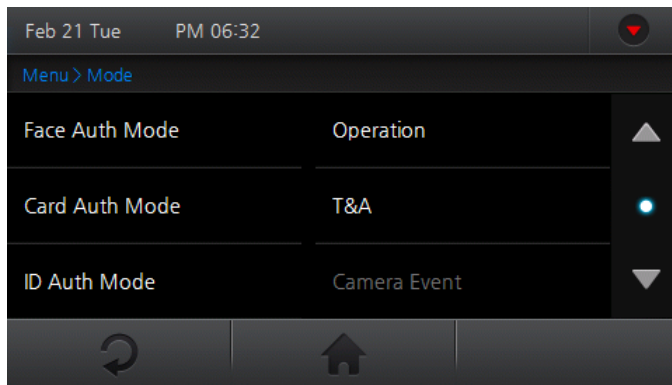


Setup



- 1 Go to **Menu > Network > WLAN**.
- 2 Check the preset option to use for WLAN connection.
- 3 Press or to go to the previous screen or Home screen.

Setting Operation Mode

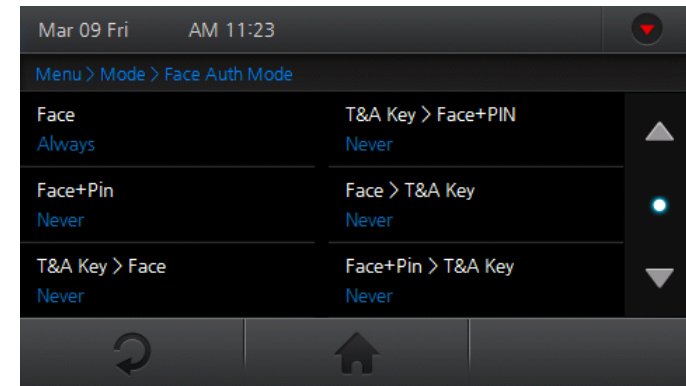
You can set operations related to each authentication or view the Time and Attendance events. The authentication mode operates according to the set timezone. Up to 128 timezones for setting authentication mode can be set on BioStar.





Setup

- 1 Go to **Menu > Mode**.
- 2 Set the options.
- 3 Press  or  to go to the previous screen or Home screen.

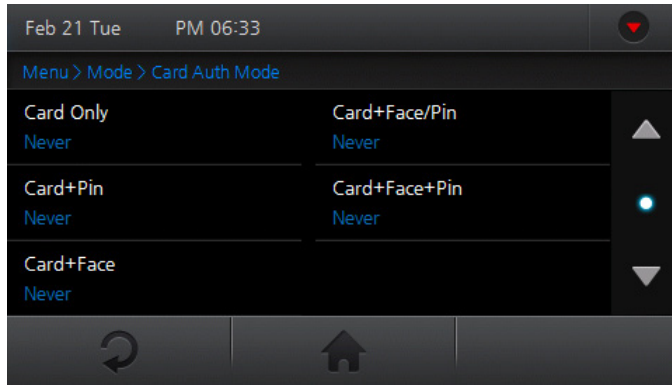
Setting Face Authentication



Setup

- 1 Go to **Menu > Mode > Face Auth Mode**.
- 2 Select a desired option.
 - **Face** Authenticates with a face only.
 - **Face + Pin** Authenticates with both face and pin number.
 - **T&A Key > Face** Authenticates with both the T&A key and the face.
 - **T&A Key > Face + Pin** Authenticates with the T&A key, face, and pin number.
 - **Face > T&A Key** Authenticates with both the face and the T&A key.
 - **Face + Pin > T&A Key** Authenticates with face, pin number, and the T&A key.
- 3 Check **Never** or **Always** to set the apply time.
- 4 Press  or  to go to the previous screen or Home screen.

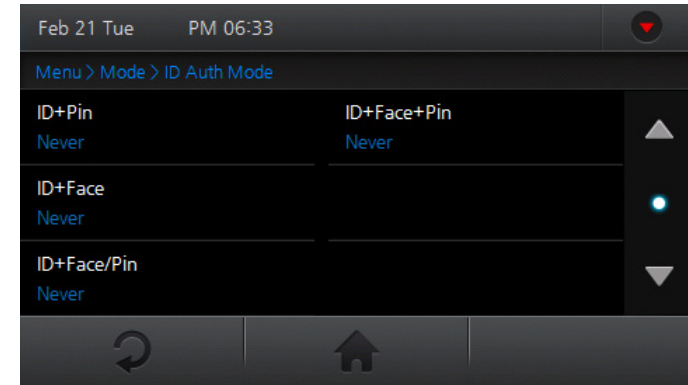
Setting Card Authentication



Setup

- 1 Go to **Menu > Mode > Card Auth Mode**.
- 2 Select a desired option.
 - **Card Only** Authenticates with a card only.
 - **Card + Pin** Authenticates with both card and pin number.
 - **Card + Face** Authenticates with both card and face.
 - **Card+ Face/Pin** Authenticates with both card and either face or pin number.
 - **Card + Face + Pin** Authenticates with card, face, and pin number.
- 3 Check **Never** or **Always** to set the apply time.
- 4 Press or to go to the previous screen or Home screen.

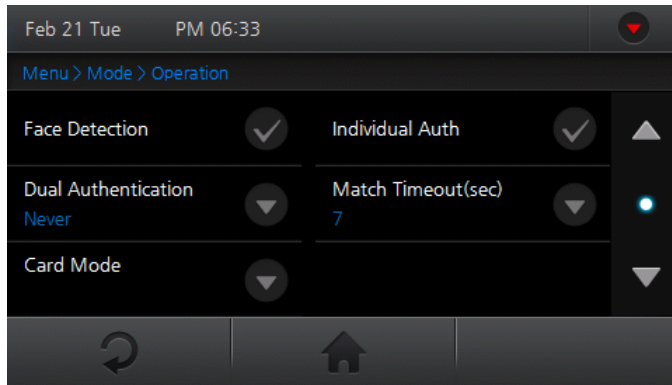
Setting ID Authentication



Setup

- 1 Go to **Menu > Mode > ID Auth Mode**.
- 2 Select a desired option.
 - **ID + Pin** Authenticates with both ID and pin number.
 - **ID + Face** Authenticates with both ID and face.
 - **ID + Face/Pin** Authenticates with both ID and either face or pin number.
 - **ID + Face + Pin** Authenticates with ID, face, and pin number.
- 3 Check **Never** or **Always** to set the apply time.
- 4 Press or to go to the previous screen or Home screen.

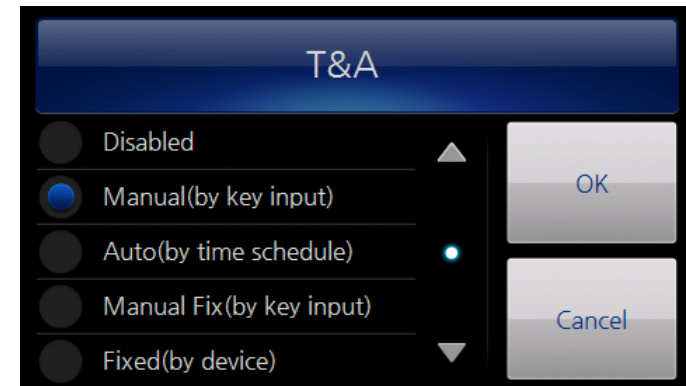
Setting Operations



Setup

- 1 Go to **Menu > Mode > Operation**.
- 2 Check, or set the options and press **OK**.
 - **Face Detection** On face authentication, stores the detected face image as an image log. On ID or card authentication, additionally authenticates and stores the detected face image as an image log. If no face is detected, the authentication will end up in failure.
 - **Dual Authentication** Authenticates with faces, cards, and IDs of two people. The entry relay operates only when two different users are authenticated, and the second user should be authenticated within 15 seconds after the first user is authenticated. If 15 seconds has passed after the first authentication, the authentication is invalidated and the status is initialized.
 - **Card Mode** Sets whether to use the CSN card for authentication.
 - **Individual Auth** Authenticates by customized methods for each individual. When registering a new user from **Menu > User > Enroll User**, the private authentication can be set. Please refer to 'Registering New User(page 32)' for details.
 - **Match Timeout(sec)** Sets the authentication time-out period. If a user is not authenticated within the set period, the authentication fails.
- 3 Press or to go to the previous screen or Home screen.

Setting Time and Attendance



Setup

- 1 Go to **Menu > Mode > T&A > T&A**.
- 2 Set the T&A options.
 - **Disabled** Select to use the access authentication without using Time and Attendance. The the T&A button disappears on the Home menu and the **CALL** button is activated.
 - **Manual(by key input)** For every authentication, press either the T&A buttons (F1 - F4) or the T&A event button (T&A) to select an event. The selected Time and Attendance event is deselected after the authentication.

Settings

- **Auto(by time schedule)** The Time and Attendance event of the corresponding timezone is automatically applied when authenticating. When changing to a different event instead of the event of the corresponding timezone, press the T&A button (F1 - F4) to select a particular event.
- **Manual Fix(by key input)** Select a Time and Attendance event by pressing either one of F1 - F4 buttons or an additional T&A event button (👤 T&A) when authenticating. The selected event is maintained until another event is selected, while the event is deselected after the authentication when manually changing.
- **Fixed(by device)** A user can be authenticated with a fixed Time and Attendance event but cannot select other events.

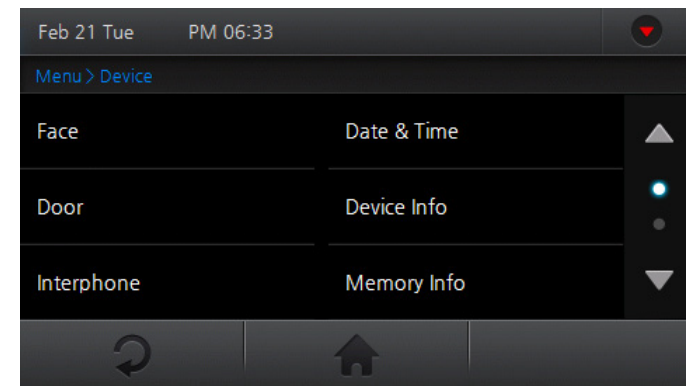
3

Press **OK** to save the changes.

Press **Cancel** to cancel any changes.

Setting Device

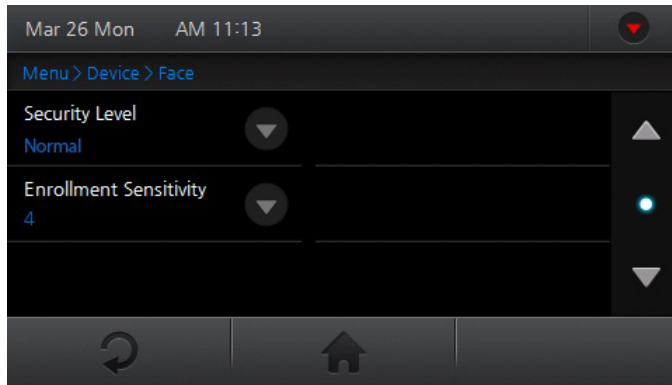
You can set options for the device authentication and operations.





Setup

- 1 Go to **Menu > Device**.
- 2 Set the options.
- 3 Press 🔄 or 🏠 to go to the previous screen or Home screen.

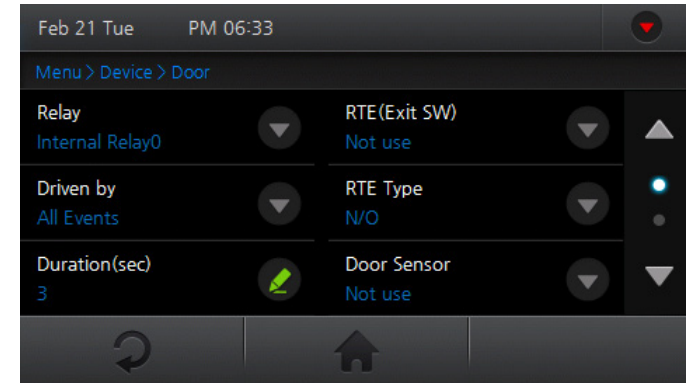
Setting Face



Setup

- 1 Go to **Menu > Device > Face**.
- 2 Set the options.
 - **Security Level** Increasing the security level will indirectly increase the FRR(False Reject Rate, probability that the system will incorrectly reject an access attempt by an authorized user) because the stricter authentication protocols will reject more inconsistencies. Select the desired security level and press **OK**.
 - **Enrollment Sensitivity** Select the desired enrollment speed and press **OK**.
- 3 Press  or  to go to the previous screen or Home screen.

Setting Door



Setup

- 1 Go to **Menu > Device > Door**.
- 2 Set the options and press **OK**.
 - **Relay** Sets a relay to use for the door when authenticating a user.
 - **Driven by** Sets an event to open the door.
 - **All Events:** Opens the door for all authentication modes.
 - **Authentication:** Opens the door only for regular authentication but not for the Time and Attendance authentication.
 - **T&A Event:** Opens the door for an event with a relay enabled during the Time and Attendance authentication.

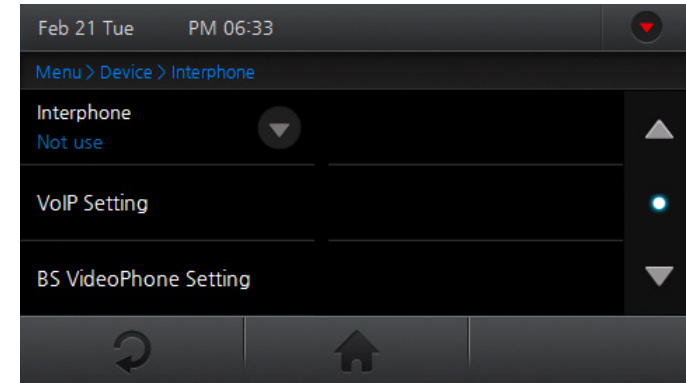
Settings

- **Authentication + T&A Event** : Opens the door for an event with a relay enabled during both general authentication and Time and Attendance authentication.
- **Disabled**: Sets to disable opening the door for all Time and Attendance events.
- **Duration(sec)** Sets the opening time of the door relay when an event occurs. The door relay closes after the set time.
- **RTE(Exit SW)** Select the input to be used for the door opening switch.
- **RTE Type** Select the operation method for the door opening switch. (N/C: Normally Closed; N/O: Normally Open)
- **Door Sensor** Select the input to be used for detecting the door opening.
- **Door Sensor Type** Select the operation method for the door opening switch. (N/C: Normally Closed; N/O: Normally Open)
- **Held Open Period(sec)** Sets a period of time from opening the door to displaying the opening warning event.
- **Unlock Time** Sets a period of time to leave the door open. During this period, the door does not close. The period can be set on BioStar software.
- **Lock Time** Sets a period of time to lock the door. The period can be set on BioStar software.

3 Press ↶ or 🏠 to go to the previous screen or Home screen.

Setting Interphone

When the interphone is set, you can make a video call by pressing the **CALL** button.

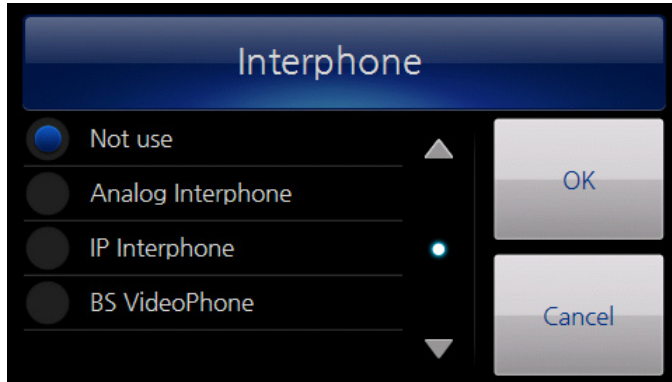


Setup

- 1 Go to **Menu > Device > Interphone**.
- 2 Set the options.
- 3 Press ↶ or 🏠 to go to the previous screen or Home screen.

Interphone

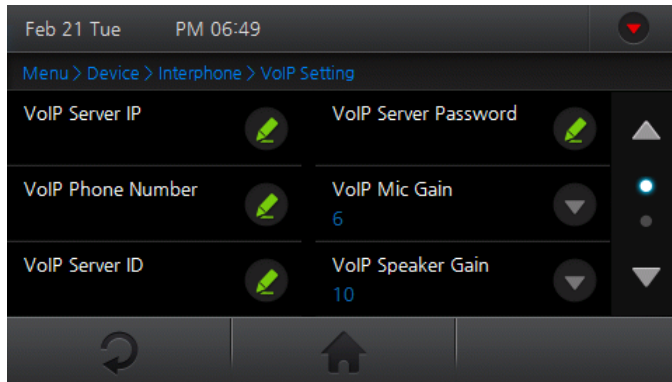
Select an interphone to use and press **OK**.



- **VoIP Server IP:** Enter the VoIP IP address and press **OK**.
- **VoIP Phone Number:** Enter the VoIP phone number and press **OK**.
- **VoIP Server ID:** Enter a VoIP server ID and press **OK**. Korean, English, number, and special characters can be used for an ID.
- **VoIP Server Password:** Enter a VoIP server password and press **OK**.
- **VoIP Mic Gain:** Adjusts the VoIP microphone volume. (0 - 10)
- **VoIP Speaker Gain:** Adjusts the VoIP speaker volume. (0 - 10)
- **VoIP Display Name:** Enter the VoIP name to be displayed on the screen and press **OK**.

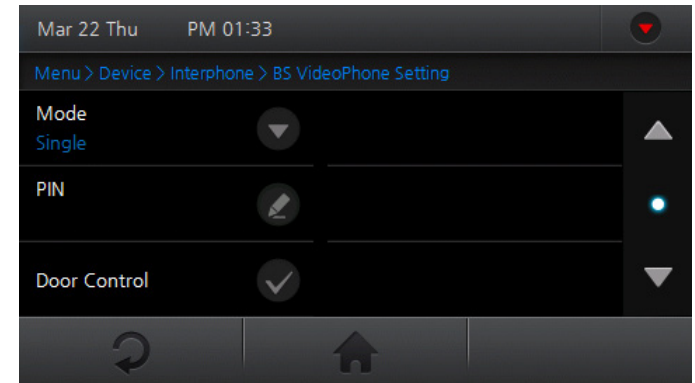
VoIP Setting

When the IP interphone is set, the relevant options can be set.



BS VideoPhone Setting

When the BioStar Video Phone is set, the relevant options can be set.

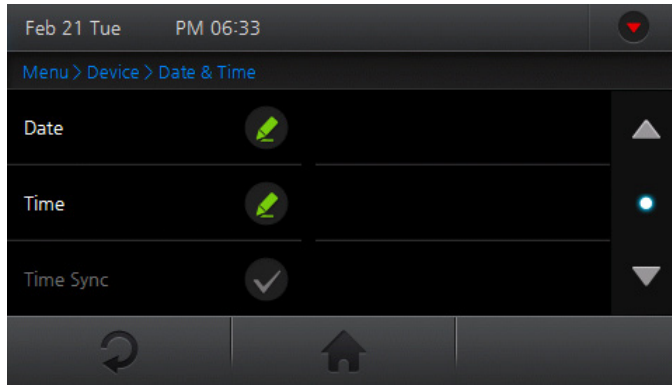


- **Mode:** Select either single or extension mode and press **OK**.
- **PIN:** Enter a pin number for the BioStar video phone and press **OK**.
- **Door Control:** Enables or disables the door control on the BioStar video phone.

3

Press or to go to the previous screen or Home screen.

Setting Time



Setup

- 1 Go to **Menu > Device > Date & Time**.
- 2 Set the options.
 - **Date** Set the year, month, and day, and press **OK**.
 - **Time** Set AM/PM, hour, minute, and second, and press **OK**.
 - **Time Sync** Can be set only if the device is connected with a server. You can synchronize the time on the device with the server. The time is synchronized every hour when the difference between the BioStar server and device is more than 5 seconds.
- 3 Press or to go to the previous screen or Home screen.

Checking Device Information

You can view the device information such as the model name, device ID, hardware version, firmware version, kernel version, MAC, face module version, face module (FD) version, and face module (LDA) version.

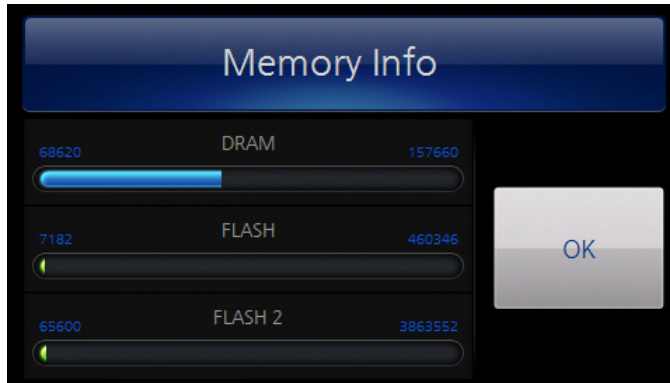


Setup

- 1 Go to **Menu > Device > Device Info**.
- 2 View the option.
- 3 Press or to go to the previous screen or Home screen.

Checking Memory Status

You can check the memory status of DRAM, FLASH, and FLASH2.



Setup

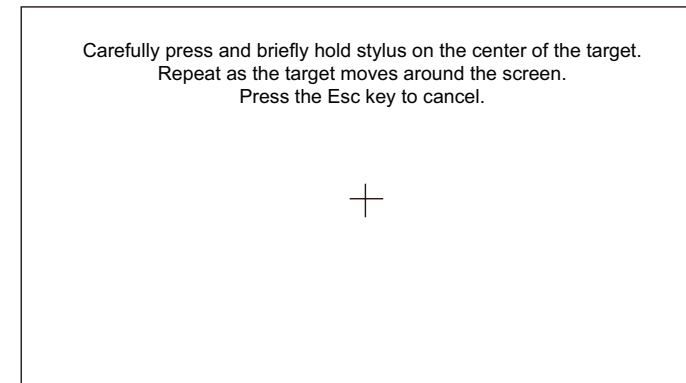
- 1 Go to **Menu > Device > Memory Info**.
- 2 View the option.
- 3 Press **OK** to return to the previous screen.

TouchScreen Calibration

If the screen does not function when touched or a touch point does not correctly correspond, you can calibrate the screen.

Setup

- 1 Go to **Menu > Device > Touch Calibration**.
- 2 Press and hold the center of the touch point on the screen until the completion message appears.



- 2 Press **OK**. The screen calibration is complete.



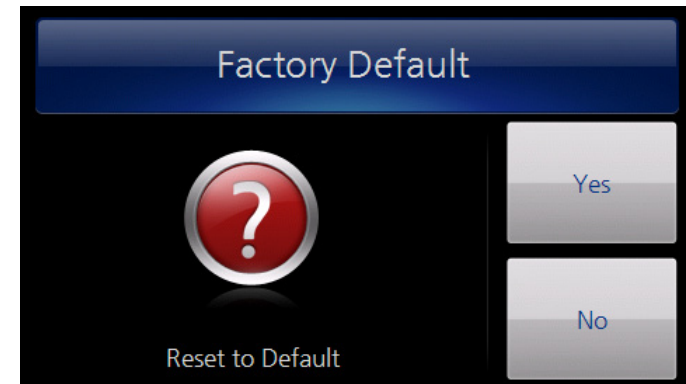
Device Reset



Setup

- 1 Go to **Menu > Device > Reset**.
- 2 Press **Yes** to restart the device.
Press **No** to return to the previous screen.

Reset to Default



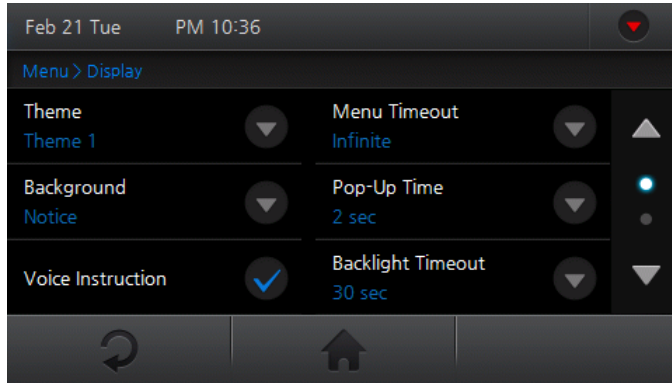
Setup

- 1 Go to **Menu > Device > Factory Default**.
- 2 Press **Yes** to initialize the device.
Press **No** to return to the previous screen.



Note

- Please note that initializing the device will delete all information such as downloaded backgrounds and sounds through BioStar software as well as announcements. The initialization does not delete the registered user information and log data.

Setting Display and Sound



Setup

- 1 Go to **Menu > Display**.
- 2 Set or check by pressing the relevant option.
- 3 Press  or  to go to the previous screen or Home screen.

Theme

You can set the background theme of the device.

Select among **Red**, **Blue**, **Black**, **Rainbow**, and **Custom**, and press **OK**.

Background

You can set the device background to be displayed.

Select among **Logo**, **Notice**, **Slide Show**, and **PDF**, and press **OK**.

Note

- When the background is set for **Logo**, **Slide**, or **PDF**, the logo screen is displayed during the authentication and other operations while the announcement, slide show or PDF screen appears after the menu time-out period (30 seconds if set to Always On). When touching the screen while an announcement or slide show is on, the LCD backlight turns on if it was off or a logo screen is displayed if the LCD backlight was on.

Voice Instruction

You can enable the voice guide on the device.

Menu Timeout

You can set the amount of idle time (sec) before the menu disappears.

Select among **Infinite**, **10 sec**, **20 sec**, and **30 sec**, and press **OK**.

Pop-Up Time

You can set the duration (sec) before the popup window disappears.

Select among **0.5 sec**, **1 sec**, **2 sec**, **3 sec**, **4 sec**, and **5 sec**, and press **OK**.

Settings

Backlight Timeout

You can set the amount of idle time before the backlight turns off.

Select among **Infinite**, **10 sec**, **20 sec**, **30 sec**, **40 sec**, **50 sec**, and **60 sec**, and press **OK**.

Volume

You can set the volume output of the device.

Select among **0**, **10**, **20**, **30**, **40**, **50**, **60**, **70**, **80**, **90**, and **100**, and press **OK**.

Language

You can set the display language.

Select among **Korean**, **English**, and **Custom**, and press **OK**.

Central Time Display

You can set to enable or disable the time on the screen.

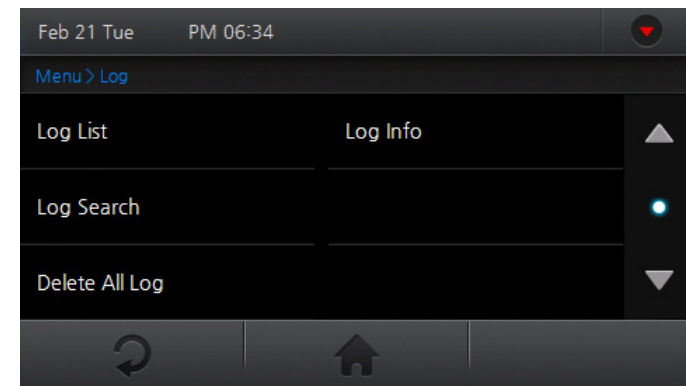
Date Display

You can set the date format.



Select **MM/DD** or **DD/MM**, and press **OK**.

Viewing Logs

You can view, search or delete the event log.



Setup



- 1 Go to **Menu > Log**.
- 2 Press and view the option.
- 3 Press  or  to go to the previous screen or Home screen.

Log List

You can select and view the desired event log.

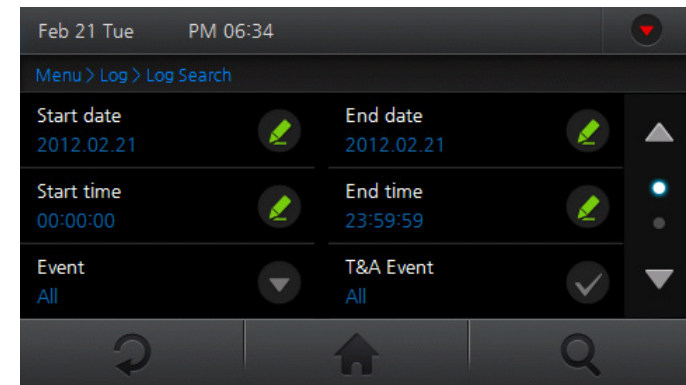


Setup




- 1 Go to **Menu > Log > Log List**.
- 2 View a desired log.
- 3 Press  or  to go to the previous screen or Home screen.

Log Search

You can search and view logs by starting date, starting time, ending date, ending time, event, Time and Attendance event, or user ID.



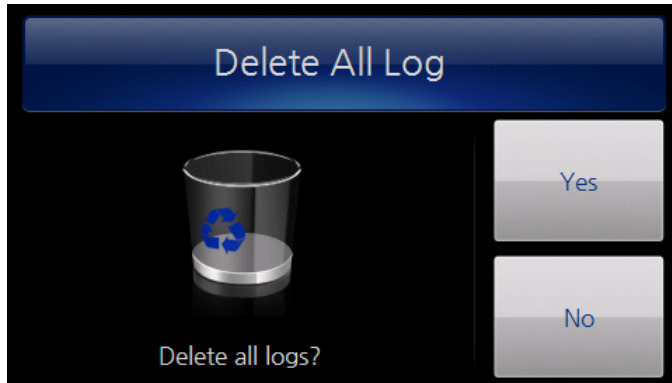
Setup

- 1 Go to **Menu > Log > Log Search**.
- 2 Set the search items and press **OK**.
- 3 Press  to display the searched log.
- 4 Press  or  to go to the previous screen or Home screen.

Settings

Delete All Log

You can delete the entire log at once.

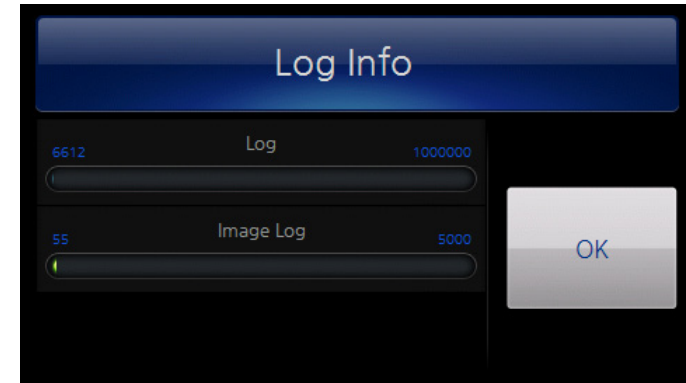


Setup

- 1 Go to **Menu > Log > Delete All Log**.
- 2 Press **Yes** to delete all logs.
Press **No** to cancel the log deletion.

Log Info

You can view the log and face image log currently stored on the device.



Setup

- 1 Go to **Menu > Log > Log Info**.
- 2 Press **OK** to return to the previous screen.

Note

- Up to 1,000,000 regular logs and up to 5,000 face image logs can be stored.

6 How to Use

Basic Screen View

Authenticating Time and Attendance

Checking Time and Attendance

How to Use

Basic Screen View

Face Authentication Screen

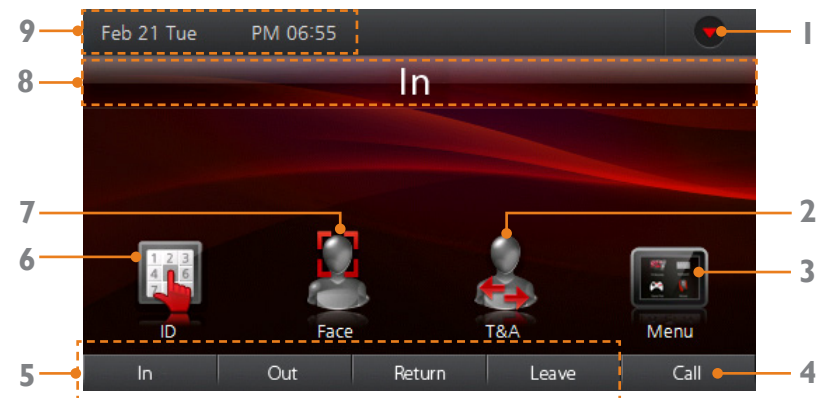
If face authentication is set, the screen as shown below appears.



| | | |
|----|---------------------------|---|
| 1 | Home | Goes to the Home screen. |
| 2 | ID | Goes to the ID authentication screen. |
| 3 | T&A | Selects Time and Attendance options. |
| 4 | Menu | Goes to the Administrator's menu. |
| 5 | Face Detection Icon | Displays the face detection availability. |
| 6 | Image Display Screen | Displays an image from the camera as well as the face. |
| 7 | Authentication Guide | Displays available authentication methods. |
| 8 | T&A Event | Displays the set Time and Attendance event. When entering the administrator's menu, a message 'Enter the administrator's menu' appears. |
| 9 | Current Time | Displays the current time on the device. |
| 10 | Face Detection Guide Line | Displays the guide line for face detection. |

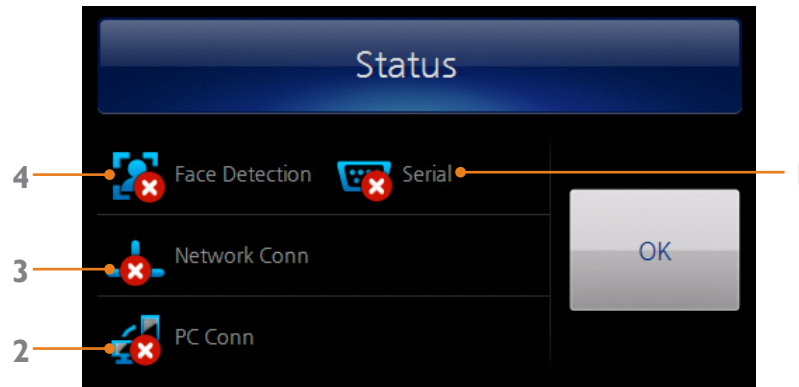
Home Screen

If face authentication is not set from the operation mode or the camera does not detect any motion, the Home screen is displayed.



| | | |
|---|----------------------------|--|
| 1 | Status Button | Checks for the connection status of the device and whether or not the face recognition is enabled. |
| 2 | Additional T&A Button | Selects 12 Time and Attendance buttons in addition to 4 basic Time and Attendance. |
| 3 | Menu Button | Enter the Administrator's Menu. |
| 4 | Call Button | Used for a video phone call. |
| 5 | Basic T&A Button | Displays basic Time and Attendance events. |
| 6 | ID Authentication Button | Enter the ID input window for ID authentication. |
| 7 | Face Authentication Button | Goes to the face authentication screen. |
| 8 | T&A Event | Displays the Time and Attendance event. |
| 9 | Status Bar | Displays the current date and time on the device. |

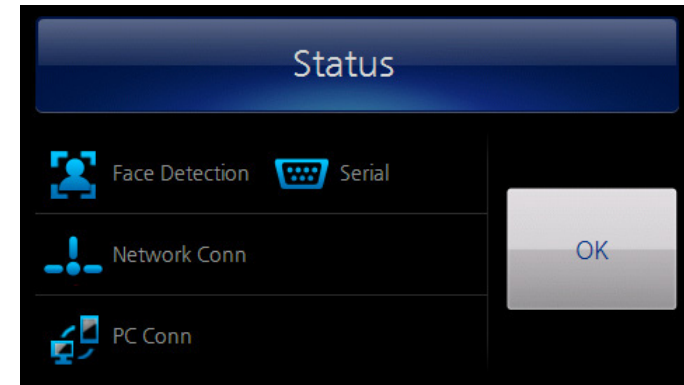
Device Status Screen



| | | |
|---|--------------------|--|
| 1 | Serial | Displays the connection status with a host when in RS485 slave mode. |
| 2 | PC Connection | Displays the connection status with a PC through Ethernet or WLAN. |
| 3 | Network Connection | Displays the connection status of the Ethernet or WLAN. |
| 4 | Face Detection | Displays whether or not the face recognition is enabled. |

Note

When the face recognition and all connection status are successfully set, a screen as shown below is displayed.



Access Authentication

FaceStation supports the face, card (RFID), and ID (PIN) authentication. The authentication mode operates according to the set timezone, and each authentication timezone does not overlap. Up to 128 timezones for setting authentication mode can be set on BioStar PC software.

When Face Authentication is Set

When the face is set as the authentication option from **Menu > Mode > Face Auth Mode**, the face authentication is operated during the corresponding timezone.

For details regarding the face authentication, please refer to '**Authenticating Face**(page 26)'.

When Card Authentication is Set

When the card is set as the authentication option from **Menu > Mode > Card Auth Mod**, the card authentication is operated during the corresponding timezone.

For details regarding the card authentication settings, please refer to '**Setting Card Authentication**(page 40)'.



When ID Authentication is Set

When the ID is set as the authentication option from **Menu > Mode > ID Auth Mod**, the ID authentication is operated during the corresponding timezone.

Please refer to '**Setting ID Authentication**(page 40)' for details regarding ID authentication settings.

Face Authentication Types

Face

- 1 Scan the face.

Face + Pin

- 1 Scan the face.
- 2 Enter the pin number and press **OK**.

T&A Key > Face

- 1 Press the T&A button.
- 2 Scan the face.

T&A Key > Face + Pin

- 1 Press the T&A button.
- 2 Scan the face.
- 3 Enter the pin number and press **OK**.

Face > T&A Key

- 1 Scan the face.
- 2 Press the T&A button.

Face + Pin > T&A Key

- 1 Scan the face.
- 2 Enter the pin number and press **OK**.
- 3 Press the T&A button.

Card Authentication Types

Card Only

- 1 Enter the card ID by placing the card on the device.

Card + Pin

- 1 Enter the card ID by placing the card on the device.
- 2 Enter the pin number and press **OK**.

Card + Face

- 1 Enter the card ID by placing the card on the device.
- 2 Scan the face.

Card+ Face/Pin

- 1 Enter the card ID by placing the card on the device.
- 2 Scan the face.
Or, enter the pin number and press **OK**.

Card + Face + Pin

- 1 Enter the card ID by placing the card on the device.
- 2 Scan the face.
- 3 Enter the pin number and press **OK**.

ID Authentication Types

ID + Pin

- 1 Enter the ID and press **OK**.
- 2 Enter the pin number and press **OK**.

ID + Face

- 1 Enter the ID and press **OK**.
- 2 Scan the face.

ID + Face/Pin

- 1 Enter the ID and press **OK**.
- 2 Scan the face.
Or enter the pin number and press **OK**.

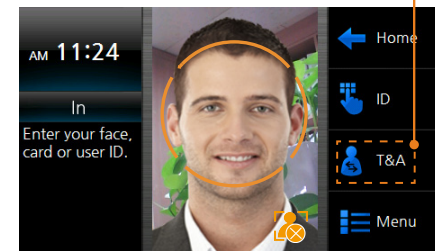
ID + Face + Pin

- 1 Enter the ID and press **OK**.
- 2 Scan the face.
- 3 Enter the pin number and press **OK**.

Authenticating Time and Attendance

Setup

- 1 Either press the T&A key(F1 - F4) or select an event on the screen.



- 2 Perform the authentication process.
- 2 Please refer to '**Access Authentication(page 56)**' for details regarding the face, card and ID authentication processes.

Note

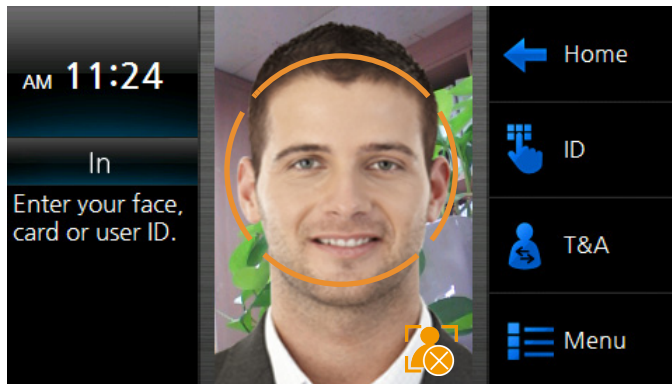
- If the Time and Attendance is set as fixed or manual, the Time and Attendance event does not need to be separately selected. Please refer to '**Setting Time and Attendance(page 41)**' for details regarding Time and Attendance.

Checking Time and Attendance

The user can view the access and attendance records.

Setup

1 Press **Menu**.



2

Enter the registered face, card and/or ID. The Time and Attendance log list is displayed.



Note

- The general user can view the Time and Attendance log through the said method, while the administrator can go to the administrator's menu through the said method.

Appendix

Specifications

Cable Specifications

Troubleshooting

FCC Rules

Device Font License

Quality Assurance

Index

Specifications

Product Specifications

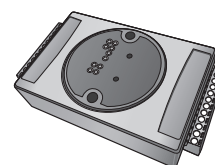
| | | | |
|---------|--------------------|---|--------------------------------------|
| System | Max Users | 10,000 | |
| | Log Capacity | 1,000,000 | |
| | Image Log Capacity | 10,000 | |
| | CPU | 1.1GHz DSP, 667MHz RISC | |
| | LCD | 4.3" WVGA Touchscreen | |
| | Memory | 4GB Flash + 512MB RAM | |
| | RF Options | 13.56MHz Mifare | |
| | Interfaces | TCP/IP, RS485(2ch), RS232, USB, Wiegand, WiFi | |
| | Power | 12VDC, PoE (Power over Ethernet) | |
| General | Dimensions | FaceStation (W x H x D) | 132 x 165 x 60 mm |
| | | Wall Bracket (W x H) | 97 x 107.8 mm (screw joint included) |

Electric Specifications

| | | Min. | Avr. | Max. | Description |
|--------------|-----------------------------|------|------|---------------|--|
| Power | Voltage(V) | 10.8 | 12 | 13.2 | Make sure to use only the supplied power supply. |
| | Current(mA) | - | | 1500 | |
| Switch Input | VIH(V) | - | TBD | - | The input ports are pulled up with 4.7K resistors. |
| | VIL(V) | - | TBD | | |
| | Pullup Resistor | - | 4.7K | - | |
| Relay | Switching Capacity(A) | - | - | 2 0.3 | 30V DC 125 AC |
| | Switching Power (resistive) | - | - | 30W 37.5VA | DC AC |
| | Switching Voltage(V) | - | - | 110 125 | DC AC |

Optional Accessories

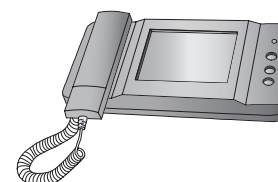
Secure I/O



Mifare reader/writer



Video phone



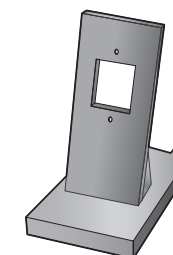
Wireless AP



RF Card

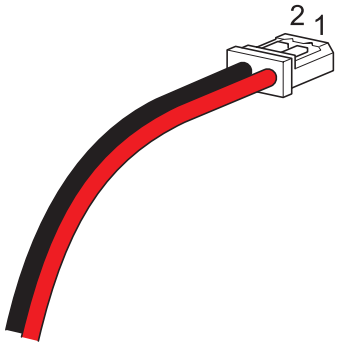


Plastic Stand



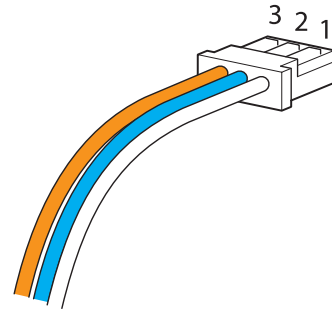
Cable Specifications

Power Cable



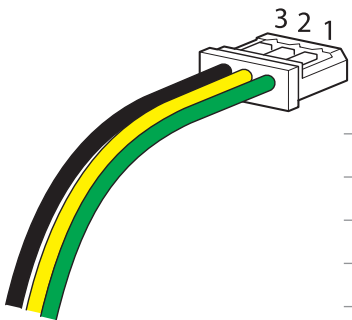
| Pin | Name | Cable Type | Color |
|-----|-------|------------|-------|
| 1 | POW + | AWG24 | RED |
| 2 | POW - | | BLACK |

Relay Cable



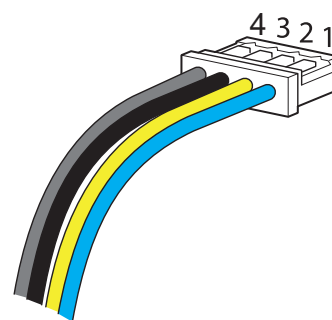
| Pin | Name | Cable Type | Color |
|-----|--------------------|------------|--------|
| 1 | RELAY NORMAL OPEN | AWG24 | WHITE |
| 2 | RELAY COMMON | | BLUE |
| 3 | RELAY NORMAL CLOSE | | ORANGE |

232 Cable



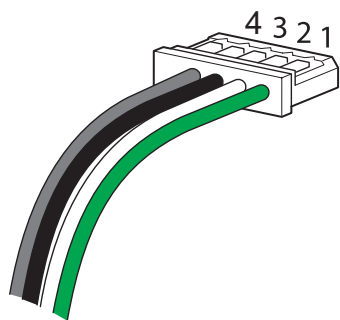
| Pin | Name | Cable Type | Color |
|-----|-------|------------|--------|
| 1 | 232RX | AWG26 | GREEN |
| 2 | 232TX | | YELLOW |
| 3 | GND | | BLACK |

RS485 Cable



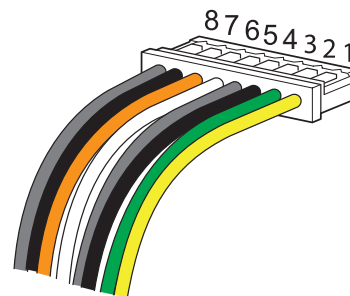
| Pin | Name | Cable Type | Color |
|-----|------------|------------|--------|
| 1 | RS485 TRX+ | AWG26 | BLUE |
| 2 | RS485 TRX- | | YELLOW |
| 3 | GND | | BLACK |
| 4 | SHIELD GND | | GRAY |

Wiegand Cable



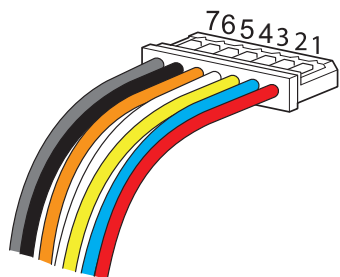
| Pin | Name | Cable Type | Color |
|-----|------------|------------|-------|
| 1 | DATA0 | AWG26 | GREEN |
| 2 | DATA1 | | WHITE |
| 3 | GND | | BLACK |
| 4 | SHIELD GND | | GRAY |

Switch Cable



| Pin | Name | Cable Type | Color |
|-----|---------------|------------|--------|
| 1 | SWITCH INPUT0 | AWG26 | YELLOW |
| 2 | SWITCH INPUT1 | | GREEN |
| 3 | SWITCH GND | | BLACK |
| 4 | SHIELD GND | | GRAY |
| 5 | SWITCH INPUT2 | | WHITE |
| 6 | SWITCH INPUT3 | | ORANGE |
| 7 | SWITCH GND | | BLACK |
| 8 | SHIELD GND | | GRAY |

Video Phone Cable



| Pin | Name | Cable Type | Color |
|-----|------------------|------------|--------|
| 1 | VOICE SIGNAL | AWG26 | RED |
| 2 | GND | | BLUE |
| 3 | POWER | | YELLOW |
| 4 | VIDEO SIGNAL | | WHITE |
| 5 | DOOR OPEN SIGNAL | | ORANGE |
| 6 | GND | | BLACK |
| 7 | SHIELD GND | | GRAY |

Troubleshooting

When any issues arise while using the device, you can request technical support from the local distributor or dealer you purchased the product from or Suprema via email (support@supremainc.com). When you send an email to Suprema, please include the following information:

- The F/W version of FaceStation that you are using
- The Model no. that you are using
- A detailed error message if an error message appears
- A brief description regarding the issue
- Your company name, contact information and the purchase information

FCC Rules

Caution

Changes or modifications not expressly approved by the manufacturer responsible for compliance could void the user's authority to operate the equipment.

Warning

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

Information to User

This equipment has been tested and found to comply with the limit of a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, user and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation; if this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more the following measures:

1. Reorient / Relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help.

Device Font License

Copyright (c) 2010, NHN Corporation (<http://www.nhncorp.com>), with Reserved Font Name Nanum, Naver Nanum, NanumGothic, Naver NanumGothic, NanumMyeongjo, Naver NanumMyeongjo.

This Font Software is licensed under the SIL Open Font License, Version 1.1.

This license is copied below, and is also available with a FAQ at: <http://scripts.sil.org/OFL>

SIL OPEN FONT LICENSE

Version 1.1 - 26 February 2007

PREAMBLE

The goals of the Open Font License (OFL) are to stimulate worldwide development of collaborative font projects, to support the font creation efforts of academic and linguistic communities, and to provide a free and open framework in which fonts may be shared and improved in partnership with others.

The OFL allows the licensed fonts to be used, studied, modified and redistributed freely as long as they are not sold by themselves.

The fonts, including any derivative works, can be bundled, embedded, redistributed and/or sold with any software provided that any reserved names are not used by derivative works.

The fonts and derivatives, however, cannot be released under any other type of license.

The requirement for fonts to remain under this license does not apply to any document created using the fonts or their derivatives.

DEFINITIONS

“Font Software” refers to the set of files released by the Copyright Holder(s) under this license and clearly marked as such.

This may include source files, build scripts and documentation.

“Reserved Font Name” refers to any names specified as such after the copyright statement(s).

“Original Version” refers to the collection of Font Software components as distributed by the Copyright Holder(s).

“Modified Version” refers to any derivative made by adding to, deleting, or substituting ? in part or in whole ?

any of the components of the Original Version, by changing formats or by porting the Font Software to a new environment.

“Author” refers to any designer, engineer, programmer, technical writer or other person who contributed to the Font Software.

PERMISSION & CONDITIONS

Permission is hereby granted, free of charge, to any person obtaining a copy of the Font Software, to use, study, copy, merge, embed, modify, redistribute, and sell modified and unmodified copies of the Font Software, subject to the following conditions:

- 1) Neither the Font Software nor any of its individual components, in Original or Modified Versions, may be sold by itself.
- 2) Original or Modified Versions of the Font Software may be bundled, redistributed and/or sold with any software, provided that each copy contains the above copyright notice and this license. These can be included either as stand-alone text files, human-readable headers or in the appropriate machine-readable metadata fields within text or binary files as long as those fields can be easily viewed by the user.
- 3) No Modified Version of the Font Software may use the Reserved Font Name(s) unless explicit written permission is granted by the corresponding Copyright Holder. This restriction only applies to the primary font name as presented to the users.
- 4) The name(s) of the Copyright Holder(s) or the Author(s) of the Font Software shall not be used to promote, endorse or advertise any Modified Version, except to acknowledge the contribution(s) of the Copyright Holder(s) and the Author(s) or with their explicit written permission.
- 5) The Font Software, modified or unmodified, in part or in whole, must be distributed entirely under this license, and must not be distributed under any other license. The requirement for fonts to remain under this license does not apply to any document created using the Font Software.

TERMINATION

This license becomes null and void if any of the above conditions are not met.

DISCLAIMER

THE FONT SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF COPYRIGHT, PATENT, TRADEMARK, OR OTHER RIGHT. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, INCLUDING ANY GENERAL, SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF THE USE OR INABILITY TO USE THE FONT SOFTWARE OR FROM OTHER DEALINGS IN THE FONT SOFTWARE.

Quality Assurance

Warranty

Suprema warrants the performance of the product specified in the specifications within the limitations set forth for a warranty period of one year from the date of delivery to the purchaser. If the purchaser claims any defects covered in this warranty in writing within the warranty period, then Suprema will repair or replace and deliver the defective product that is returned within the warranty period; provided that the purchaser shall be responsible for any transportation cost (including insurance for overseas shipping). This warranty does not apply to: (1) damage caused by strong external physical impact, overcurrent, misuse, abuse, or negligence; (2) damage to the product that has been improperly repaired, remodeled, or modified without the written permission of the provider; or (3) damage to the product that has been installed or used contrary to the manual provided by Suprema.

Claims for any defects must be submitted to Suprema in writing by using the Return Material Authorization Report provided by Suprema within 30 days of the finding of the defect or within 1 year from the date of delivery. The Return Material Authorization Report must include the detailed information, model number, invoice number, and serial number of the defective product. A product without the return authorization number issued by Suprema is not considered to be eligible for the warranty; all defects must be reproducible.

Excluding the above-mentioned warranties and remedies, this product is provided as-is without any expressed or implied warranties regarding product warranty, commercial viability, or availability for a particular purpose.

Disclaimer

The information in this document is provided in connection with Suprema products. The license is granted only for products covered by Suprema's Terms and Conditions of Sale. No license, express or implied, by estoppels or otherwise, to any intellectual property rights is granted by this document. Suprema assumes no liability whatsoever and Suprema disclaims any express or implied warranty, relating to sale and/or use of Suprema products, including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright, or other intellectual property right. Suprema products are not intended for use in medical, life saving, or 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 Buyer purchase or use Suprema products for any such unintended or unauthorized application, Buyer shall indemnify and hold Suprema and its officers, employees, subsidiaries, affiliates, and distributors harmless against all claims, costs, damages, 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. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Supreme reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them.

Index

A

- Access Authentication 56
- Authenticating Face 26
- Authenticating Time and Attendance 58

C

- Card Authentication 56, 57
- Checking Device Information 46
- Checking Memory Status 47
- Checking Time and Attendance 59
- Checking User Capacity Information 35
- Checking User Registration Status 35
- Connecting Mini USB 21
- Connecting Power 15
- Connecting Relays 19
- Connecting Switch 20
- Connecting USB 22
- Connecting Video Phone 22
- Connecting Wiegand 20
- Connecting with Ethernet 16
- Connecting with Wireless LAN 15

D

- Delete All Log 52

- Delete All Users 34

- Delete User 33

- Device Reset 48

- Device Status Screen 55

- Display and Sound 49

E

- Entering Administrator's Menu 31

F

- Face Authentication 56, 57
- Face Authentication Screen 54

H

- Home Screen 54

I

- ID Authentication 56, 58
- Installation 12

L

- Log Info 52
- Log List 51
- Log Search 51

M

- Modifying User Information 33

P

- Precautions for Installation 13

R

- Registering Administrator 30
- Registering Face 24
- Registering New User 32
- Reset to Default 48
- RS232 18
- RS485 17

S

- Searching Users 34
- Setting Card Authentication 40
- Setting Door 43
- Setting Face 43
- Setting Face Authentication 39

- Setting ID Authentication 40

- Setting Interphone 44

- Setting Menu Overview 28

- Setting Operations 41

- Setting Serial Communication 37

- Setting Server 36

- Setting TCP/IP 36

- Setting Time and Attendance 41

- Setting USB 37

T

- TouchScreen Calibration 47

U

- Using USB Memory Device 38



Suprema Inc.

(463-863) 16F Parkview Office Tower, Jeongja-dong, Bundang-gu, Seongnam, Gyeonggi, Korea

Tel: +82-31-783-4502 | Fax: +82-31-710-4503

Email: sales@supremainc.com | Homepage: www.supremainc.com