suprema

FaceStation

User Manual

Version V1.24

Important Safety Information

Carefully review the information within the user manual before installing/operating the device.
Pay careful attention to the warning and cautions below as they are here to prevent any risk/damage to any person(s) or property associated with the device.

⚠ **Warning**
Failure to heed these warnings may lead to serious injury or even death!

Installation

- Do not install the device near areas with direct sunlight, high humidity, soot or dust.
- Do not install the device near heat sources such as radiators, heat registers, and stoves.
- Do not install the device near areas of large electromagnetic interference.

Usage

- Do not disassemble, repair or reconstruct the device.
  Contact your nearest Suprema dealer for technical support.
- Do not obstruct or place wet objects near/on the vent.
- Do not place liquids such as water, beverages and other solutions near/on the device.
- Only use the device its intended use.

⚠ **Caution**
Failure to heed these cautions may lead to minor injury or damage the device.

Installation

- Do not leave cables (especially power cables) exposed to the outer environment.
- Do not install the device near objects with a strong magnetic field such as magnets, computer monitors (especially CRT), TV screens, and speakers.

Usage

- Do not apply heavy pressure to or use sharp objects with the touchscreen LCD.
- Do not drop or apply any physical shock/impact to the device.
- Regularly clean the product with a soft dry cloth; avoid benzene or alcohol.

Contents

Contents

1 Getting Started

Features

Components

Product Description

Dimensions

Features

4.3" Touchscreen LCD		The 4.3" WVGA touchscreen LCD provides a robust and precise interface to an intuitive GUI allowing for easy operation and access to the device.
Next Generation Face Recognition Technology		By combining state-of-the-art technology with Suprema's proprietary algorithms, FaceStation provides querying speeds of up to 1:1000 matches per second. Using twin camera technology FaceStation is able to store both facial stamps using a visual camera as well as complex facial templates using the IR camera.
Various Interface Supported		FaceStation comes with a variety of network interfaces such as TCP/IP, WiFi, RS485, RS232, Wiegand, and USB.
Video Phone		FaceStation's built-in camera, microphone and speaker provide the device with the ability to be integrated with conventional analogue video phones, VoIP video phones or PC software to create.
RF Card Support		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

FaceStation

Wall Mounting Bracket (1)
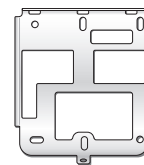
Software CD (1)

Wall Mount Screws (4)
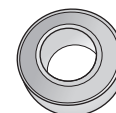
PVC Anchors (4)

Ferrite Core (1)

Diode (2)

RS232 Cable (1)
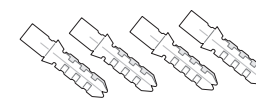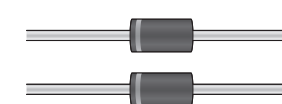
Relay Cable (2)

RS485 Cable (2)

Wiegand Cable (1)

Switch Cable (1)

Video Phone Cable (1)

Power Cable (1)

Optional Accessories

Power Adapter

Secure I/O

RF Card

RF
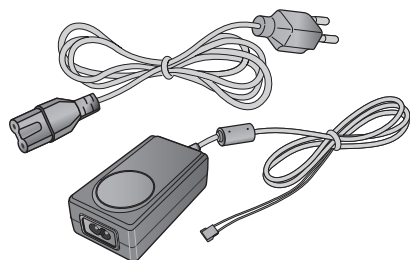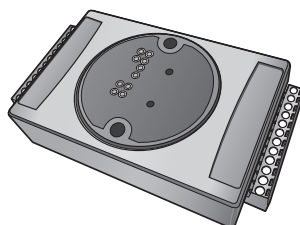
Plastic Stand
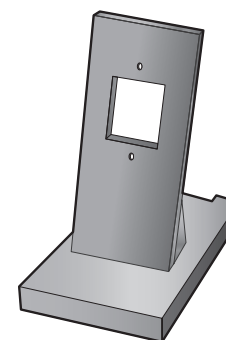
Mifare reader/writer
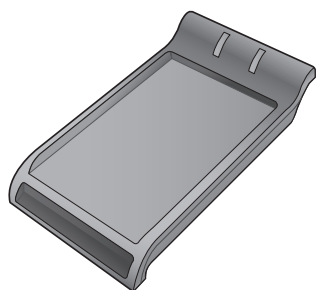
Video phone
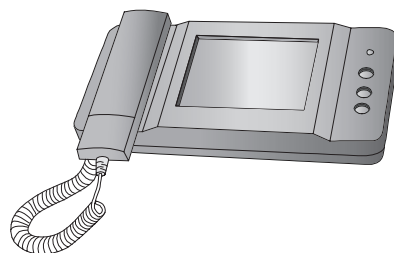
**Wireless Access Point
(For Wireless Models Only)**

Product Description

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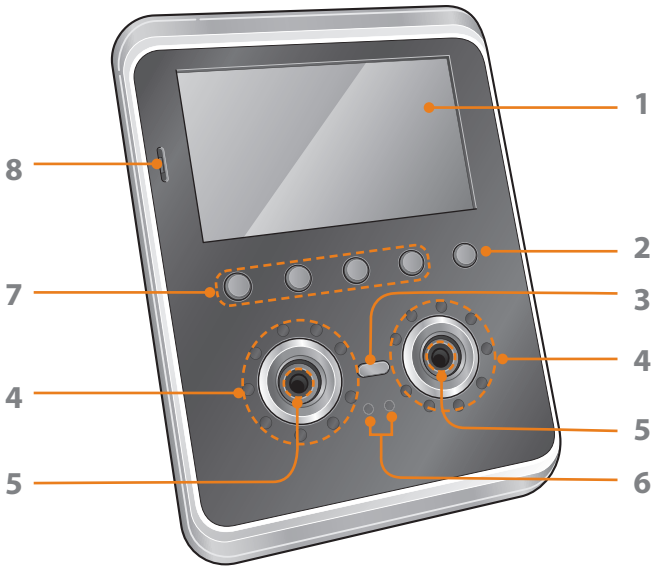
1	LCD Touchscreen	Used to display the device operating status and device operation.
2	Call Button	Used to place a call on the interphone.
3	Light LED	Used as a general lighting.
4	Infrared (IR) LED	Used as an IR light.
5	Camera	Detects and captures a face image.
6	Proximity Sensor	Determines the user's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

Note

The RF antenna, used to scan RFID cards, is built around the IR LEDs.

Rear and Bottom
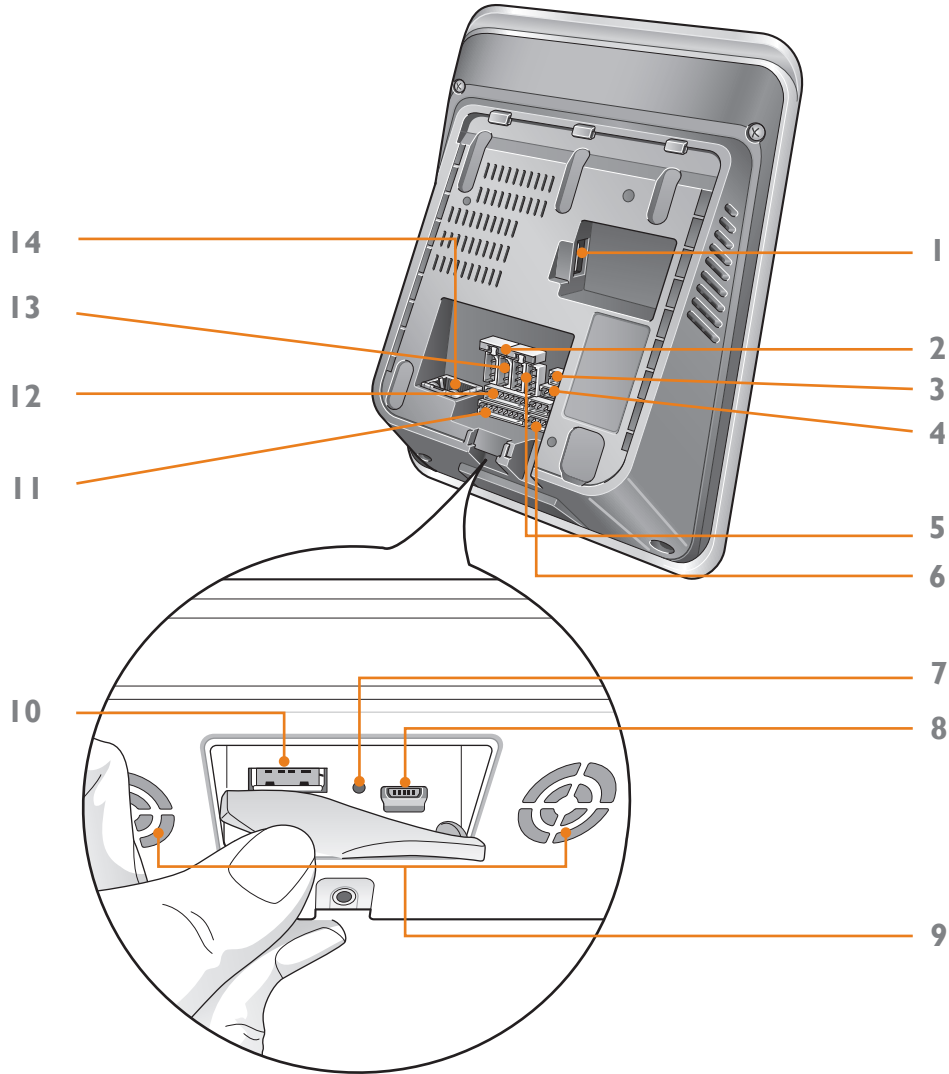
1	USB Wireless LAN Port	Used for the wireless LAN module.
2	Termination Switch	Enables RS485 termination.
3	PWR Connectors	Connects to the 2-pin power cable.
4	RS232 Connectors	Connects to the 3-pin RS232 cable.
5	RS485 Connectors	Connects to the 4-pin RS485 cable.
6	Wiegand Connectors	Connects to the 5-pin Wiegand cable.
7	Reset Button	Resets the device.
8	Mini USB Port	Connects with a PC.
9	Speaker	Audio output from the device
10	USB type A Port	Connects to a USB memory device.
11	Input Terminal	Connects to the 8-pin input cable.
12	Analogue Video	Connects to the 7-pin analogue video phone cable.
13	Output Relay Terminal	Connects to two 3-pin relay cables.
14	Ethernet Port	Connects an Ethernet cable.

Dimensions

FaceStation
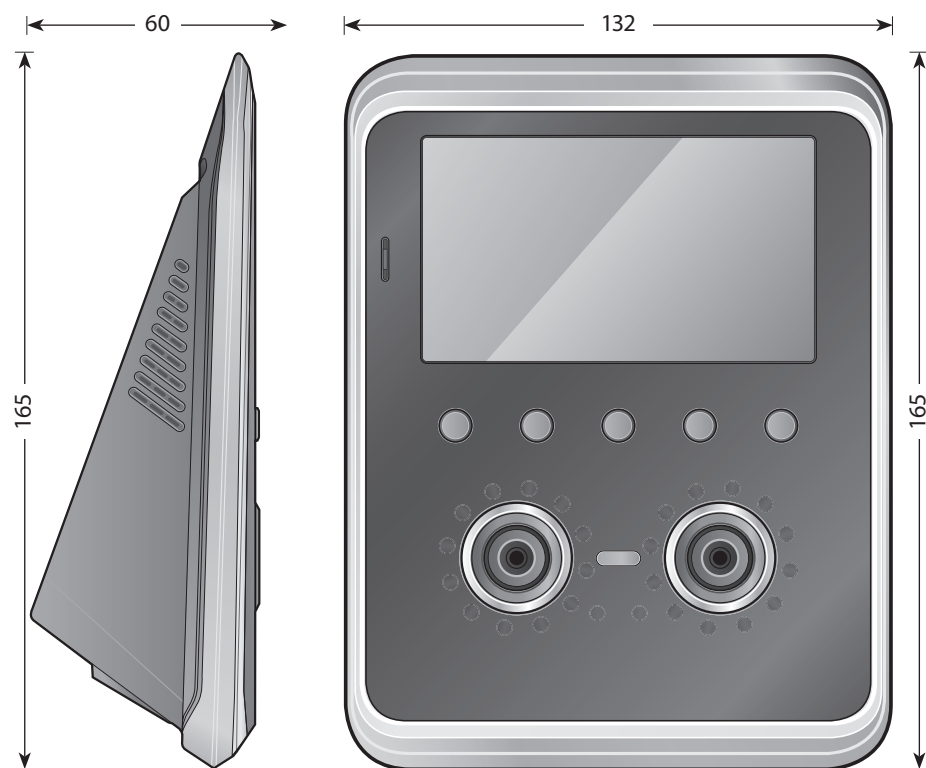
Wall Bracket
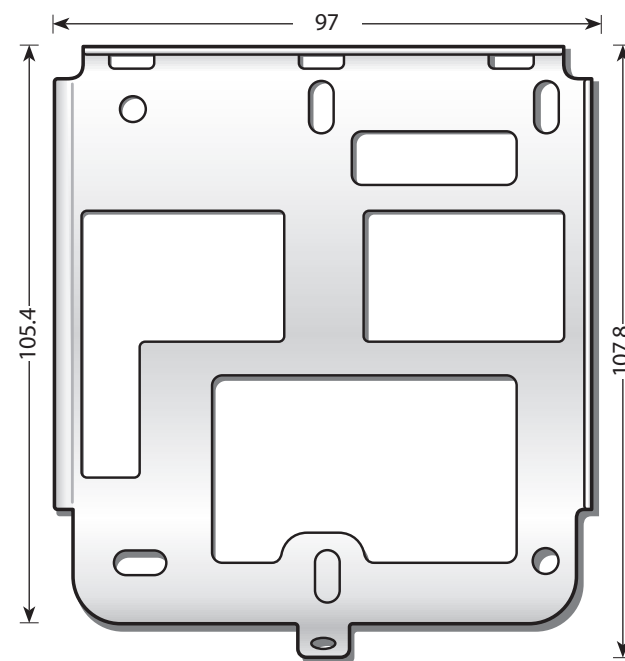
2 Installation

Installation Precautions

Basic Installation

Installation Precautions

FaceStation is a state-of-the-art face recognition terminal using Suprema's advanced adaptive IR illumination technology.
Please pay care attention to the precautions and instructions to maximize its performance.

Installation Location

- Optimal Installation Height: 120cm (Ideal for user height's between 155cm - 205cm)

- It is recommended to determine the installation height based on the shortest user.

- A uniform installation height must be maintained when installing multiple devices for the same user group.

- The device is designed for indoor use.

- When installing the device near a window, install the device at least 3 meters from the window.

- Avoid installation locations where there is direct sunlight on or behind the face.

Recommended Installation Height

Recommended Installation Height	User Height Range	
Bottom of the bracket	Minimum	Maximum
90cm	125cm	175cm
100cm	135cm	185cm
110cm	145cm	195cm
120cm	155cm	205cm

※ The recommended installation height refers to the distance from the ground to the bottom of the bracket.

Basic Installation

As FaceStation two built-in cameras for face recognition, the correct installation height is extremely important to maximize the performance of the device.
Select the optimal installation height for all users.

Installation

| 1 | Place the bracket on the desired location. |
| 2 | Fix the bracket to the location using the insert anchors and screws. |

3	Mount the device onto the bracket.
4	Fix the device to the bracket using the device mount screw.
5	Remove the transparent protective film from the device.

50cm

120cm
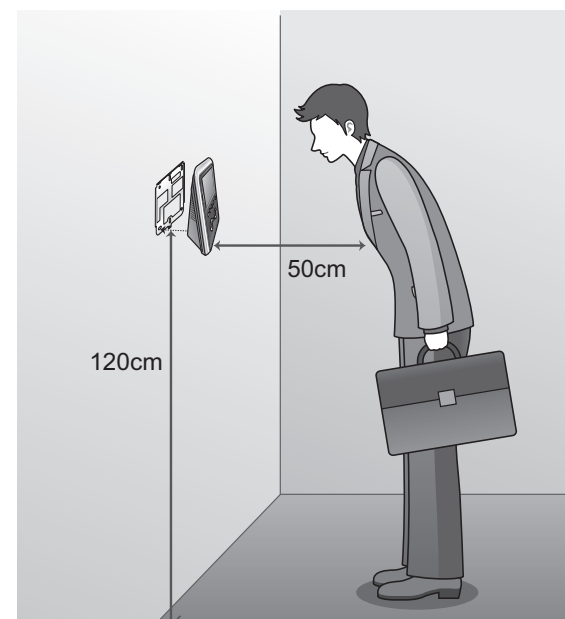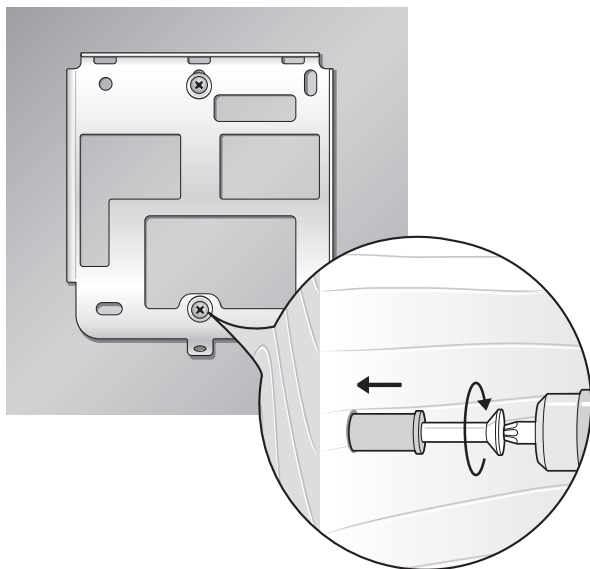
3 Connections

Cable Specifications

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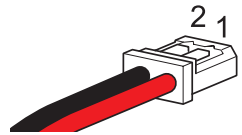
Pin	Name	Cable Type	Color
1	POW +	AWG24	RED
2	POW -		BLACK

RS232 Cable
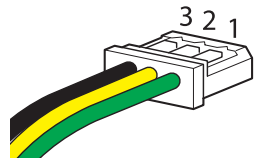
Pin	Name	Cable Type	Color
1	RS232 RX	AWG26	GREEN
2	RS232 TX		YELLOW
3	GND		BLACK

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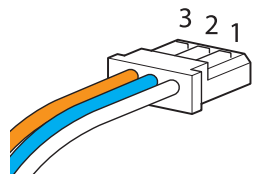
Pin	Name	Cable Type	Color
1	RELAY NORMAL OPEN	AWG24	WHITE
2	RELAY COMMON		BLUE
3	RELAY NORMAL CLOSE		ORANGE

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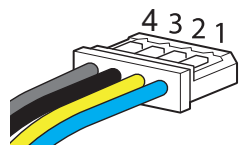
Pin	Name	Cable Type	Color
1	RS485 TRX+	AWG26	BLUE
2	RS485 TRX-		YELLOW
3	GND		BLACK
4	SHIELD GND		GRAY

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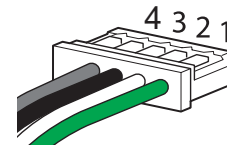
Pin	Name	Cable Type	Color
1	DATA0	AWG26	GREEN
2	DATA1		WHITE
3	GND		BLACK
4	SHIELD GND		GRAY

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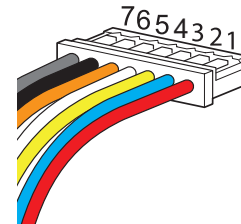
Pin	Name	Cable Type	Color
1	VOICE SIGNAL	AWG26	RED
2	GND		BLUE
3	POWER		YELLOW
4	VIDEO SIGNAL		WHITE
5	DOOR OPEN SIGNAL		ORANGE
6	GND		BLACK
7	SHIELD GND		GRAY

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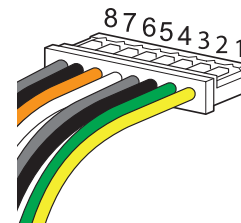
Pin	Name	Cable Type	Color
1	SWITCH INPUT0	AWG26	YELLOW
2	SWITCH INPUT1		GREEN
3	SWITCH GND		BLACK
4	SHIELD GND		GRAY
5	SWITCH INPUT2		WHITE
6	SWITCH INPUT3		ORANGE
7	SWITCH GND		BLACK
8	SHIELD GND		GRAY

Connections
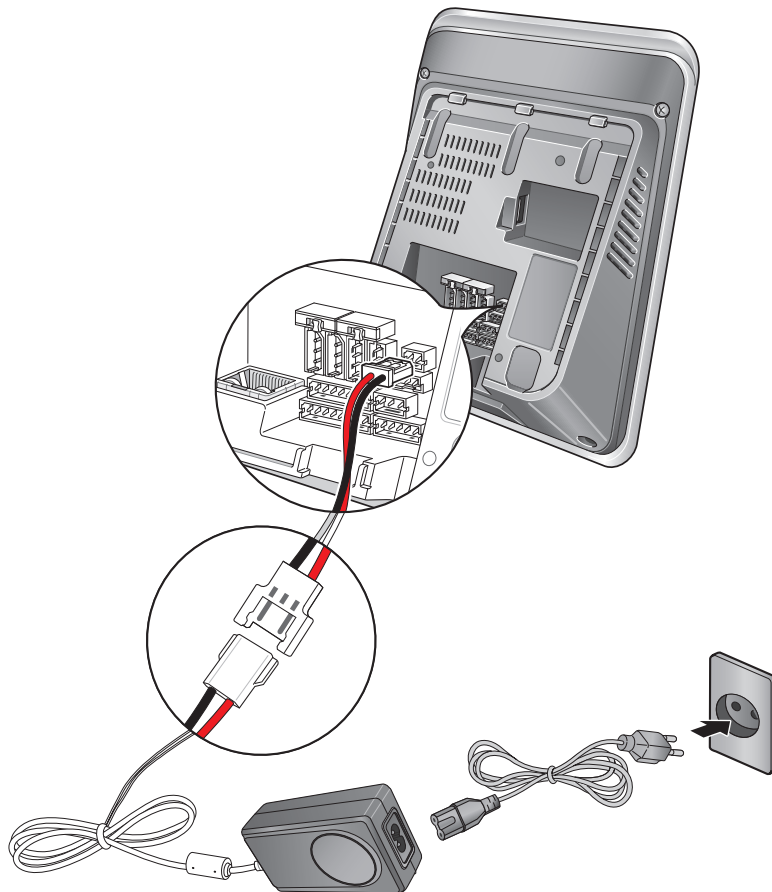
Power Connection

Note
- Use a 12VDC IEC/EN 60950-1 certified power adapter.
- It is recommended not to share FaceStation's power with other devices such as Secure I/O and/or locks.

Wireless LAN Connection

Wireless LAN FaceStation models come pre-installed with a USB WLAN module.

USB Wireless LAN
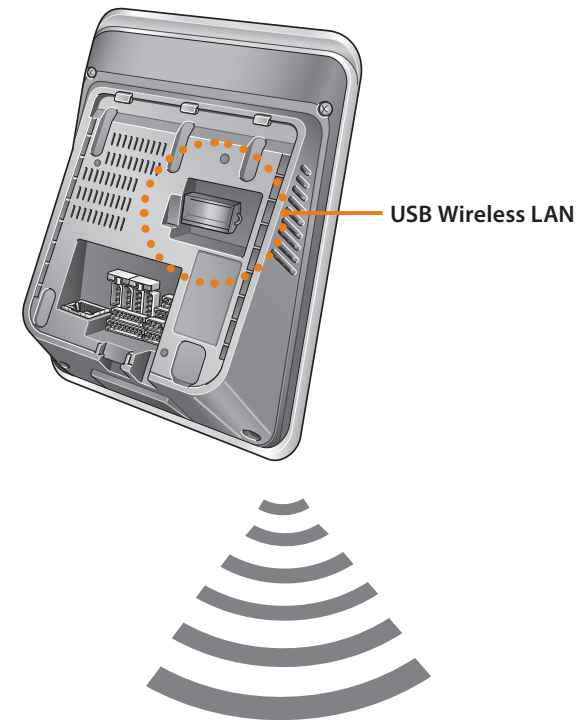
Note
- The performance of WLAN is greatly affected by the surroundings and the type of the access point (AP) used.
- Compatibility issues may cause connection difficulties with some wireless access point brands.

Ethernet Connections

Connecting with a PC

FaceStation can communicate with a PC through a direct connection using an Ethernet cable.
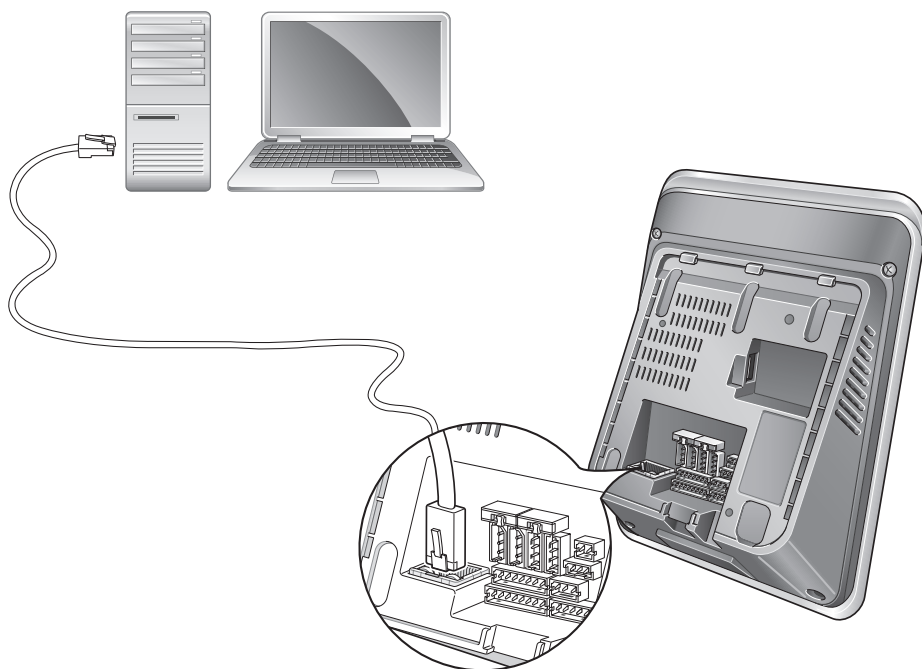
Connecting with Hub

FaceStation can be connected to a network using a regular Ethernet hub or PoE hub. PoE (Power over Ethernet): Power is provided through the Ethernet connection by an IEEE802.3af compliant PSE (Power Sourcing Equipment).

Ethernet Hub
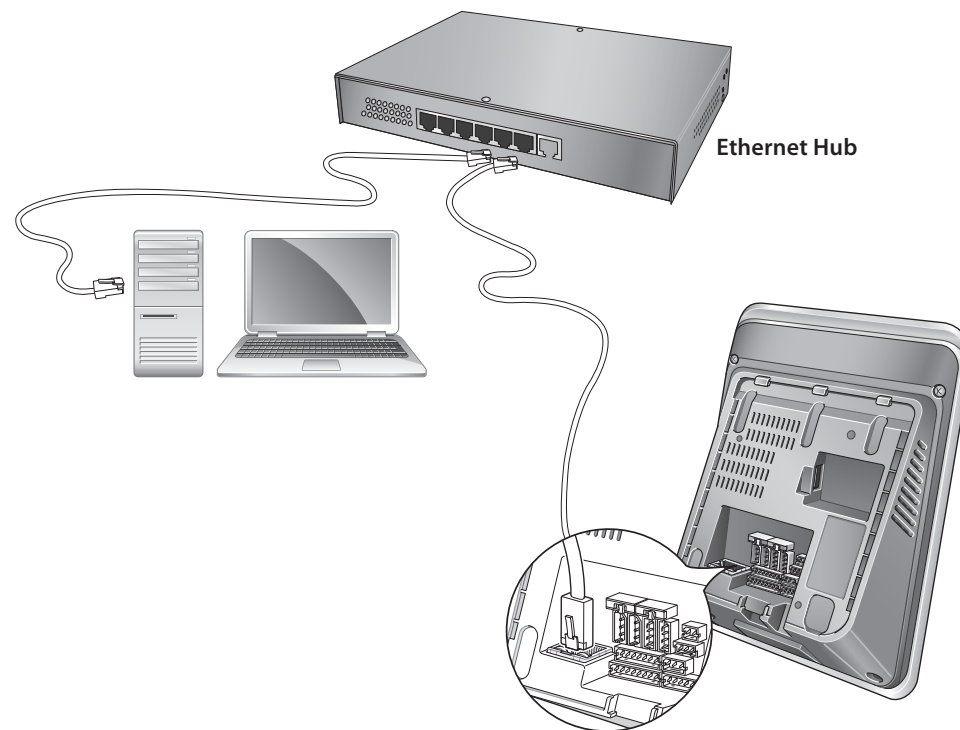
RS485 Connections

FaceStation can communicate with a PC, Secure I/O, or other devices via an RS485 connection.

Connecting with a PC

PIN1: GND (Black)
PIN2: TRXD - (Yellow)
PIN3: RS TRXD + (Blue)

1 2 3

RS232-485 Converter

RS485 CH0

PIN3: RS-GND (Black)
PIN2: RS485-TRX-(Yellow)
PIN1: RS485-TRX+(Blue)

RS485 CH0

PIN3: RS-GND (Black)
PIN2: RS485-TRX-(Yellow)
PIN1: RS485-TRX+(Blue)
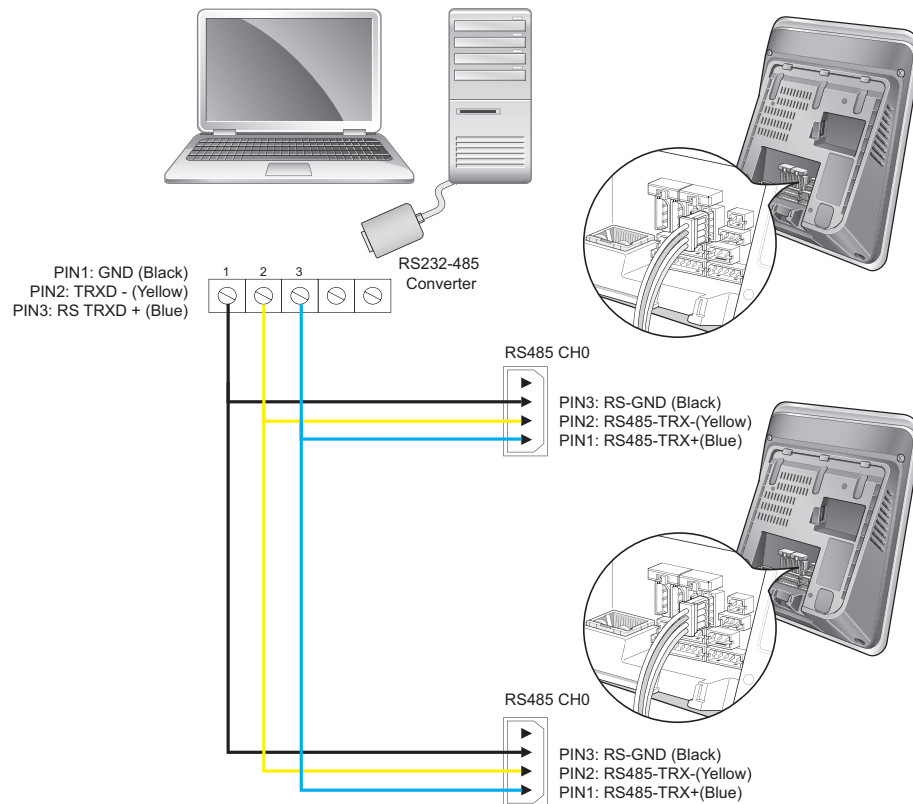
Connecting with Secure I/O

Master

RS485 CH1

PIN3: RS-GND(Black)
PIN2: RS485-TRX-(Yellow)
PIN1: RS485-TRX+(Blue)

4 5 6

Slave

PIN6: RS485 TRX+(Blue)
PIN5: RS485 TRX-(Yellow)
PIN4: RS-GND (Black)
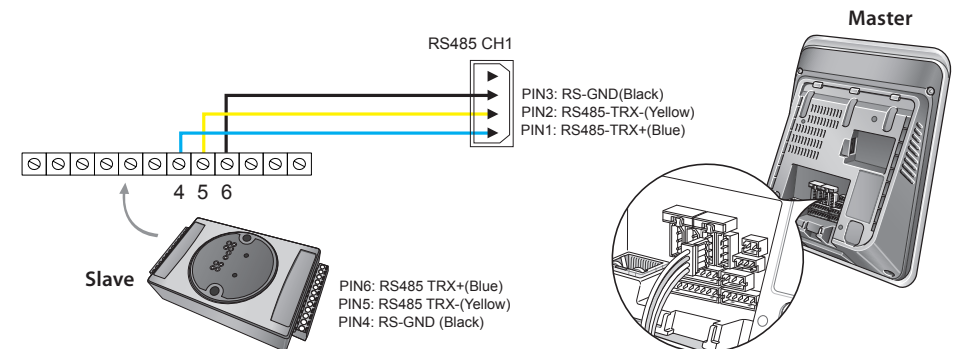
📑 Note

- For added security, a Secure I/O is recommended as the door relay interface.

Connecting with Other Devices

Master   RS485 CH1   RS485 CH1   Slave

PIN3: RS-GND(Black)
PIN2: RS485-TRX-(Yellow)
PIN1: RS485-TRX+(Blue)
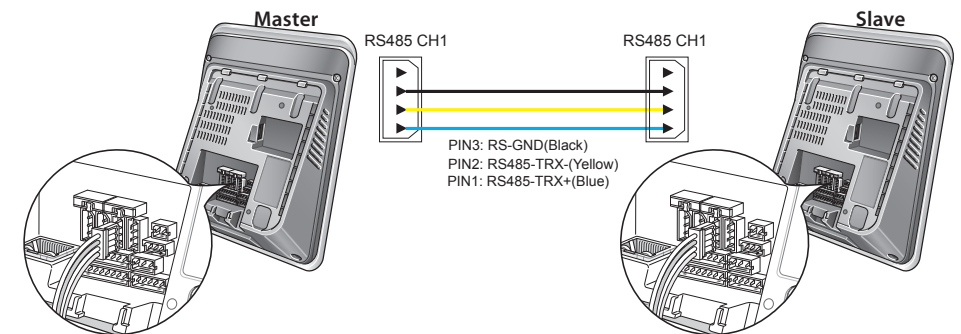
Note

- For long RS485 connections, enable the dip switch to terminate the line and prevent signal degradation.

Switch On

Switch Off
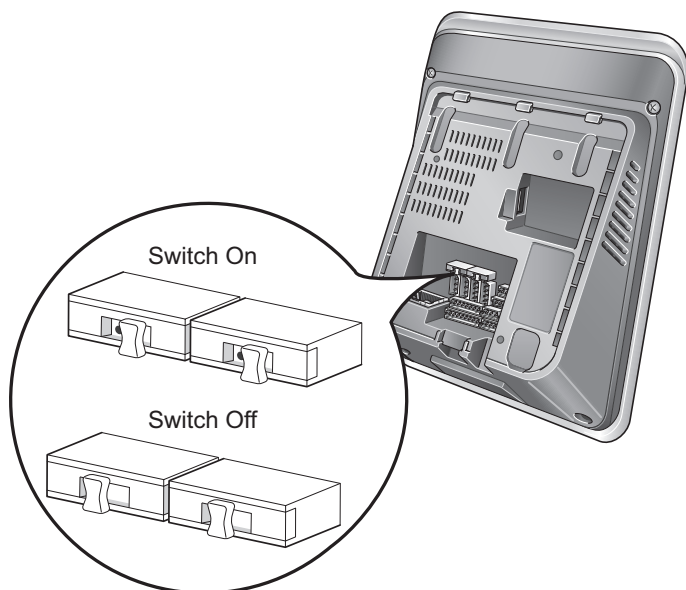
- Do not use the termination for short RS485 connections.
- If GND is not connected, the RS485 chip may malfunction.
- RS485 communication can support 2 host device and up to 7 slave devices.
- A maximum of 4 Secure I/O can be connected to one FaceStation.

RS232 Connection

FaceStation can communicate with a PC via an RS232 connection.

PIN2: RXD (Green)
PIN3: TXD (Yellow)
PIN5: GND (Black)

PIN1: RS-GND (Black)

PIN2: RS232-TX (Yellow)

PIN3: RS232-RX (Green)
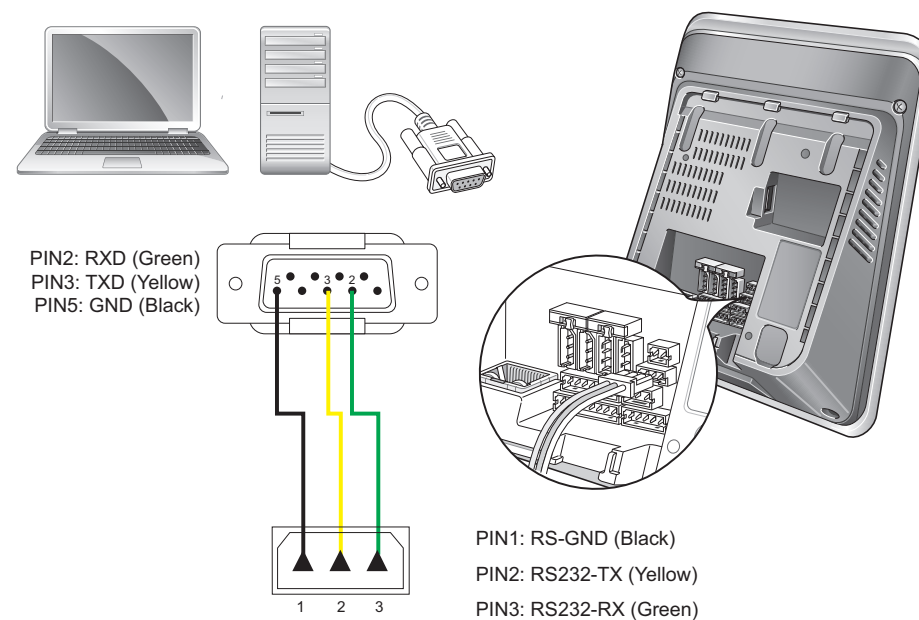
Relay Connections

Connecting with a Fail Safe Lock

PIN3: N/C(Normal Close: Orange)
PIN2: Common(Blue)
PIN1: N/O(Normal Open: White)

Deadbolt or Door strike

DC Power supply
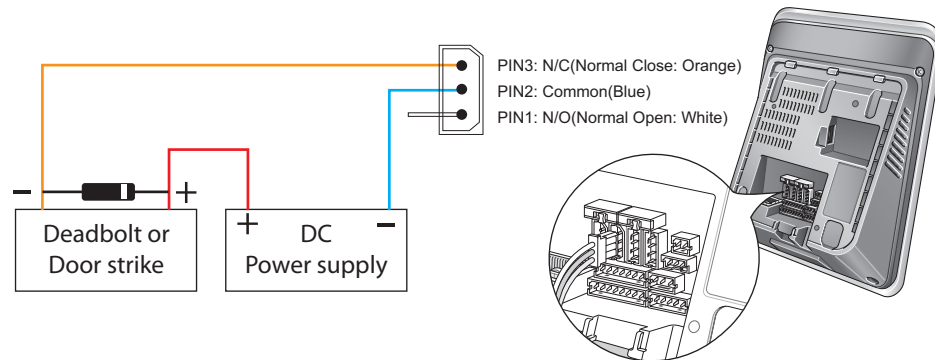
Connecting with a Fail Secure Lock

PIN3: N/C(Normal Close: Orange)
PIN2: Common(Blue)
PIN1: N/O(Normal Open: White)

Deadbolt or Door strike
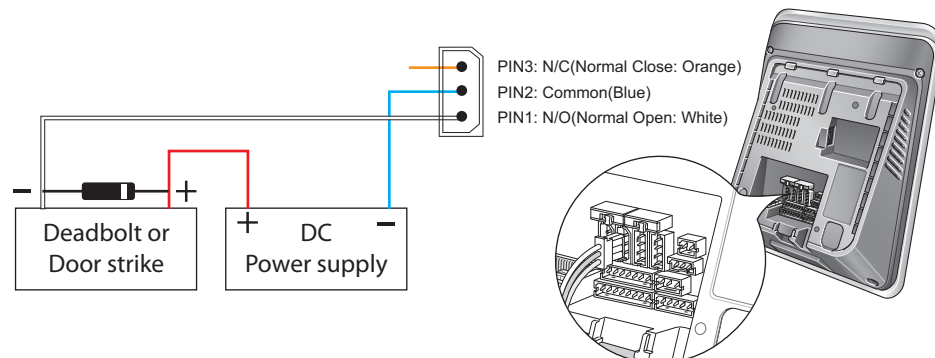
DC Power supply

Note

- N.O. (Normally Open): A control signal closes the circuit.
- N.C. (Normally Closed): A control signal opens the circuit.
- Take care of the direction of the diode.
- Make sure to install the diode near to the door lock.
- Make sure to use different power supplies for the FaceStation and the door lock.
- Make sure to install the diode at both ends of the circuit as shown in the figure left in order to protect the relay contact from the reverse current that occurs when the door lock works.

Connecting with Automatic Doors

RTE Switch

PIN3: N/C(Normal Close: Orange)
PIN2: Common(Blue)
PIN1: N/O(Normal Open: White)

Presence Detector

Door Controller

Input Connection

8 7 6 5 4 3 2 1

Cable Shield (Optional)

Cable Shield (Optional)

PIN8: Shield GND (Gray)
PIN7: Switch GND (Black)
PIN6: Switch Input3 (Orange)
PIN5: Switch Input2 (White)
PIN4: Shield GND (Gray)
PIN3: Switch GND (Black)
PIN2: Switch Input1 (Green)
PIN1: Switch Input0 (Yellow)

Switch Input 3   Switch Input 2   Switch Input 1   Switch Input 0

Wiegand Connections

Connecting a Wiegand Input

PIN3: Wiegand GND (Black)
PIN2: Wiegand DATA1 (White)
PIN1: Wiegand DATA0 (Green)

3 2 1

Cable Shield (Optional)

Card Reader

GND
Wiegand Output.Data1
Wiegand Output.Data0
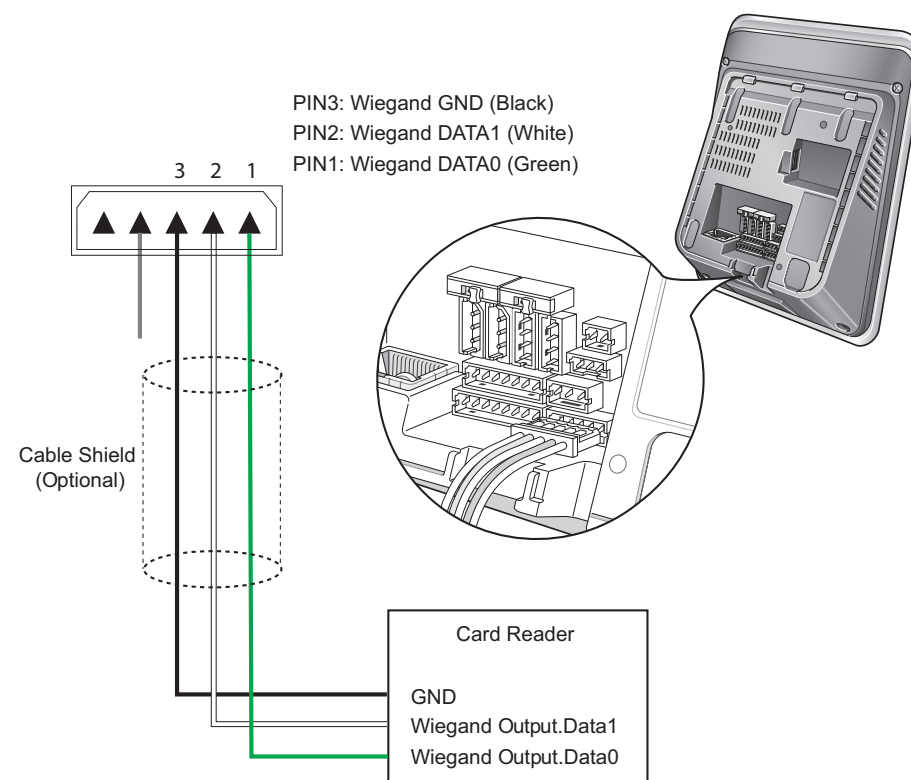
📄 Note

• The Wiegand port can be set as either input or output via the BioStar software.

Connections

Connecting a Wiegand Output

PIN3: Wiegand GND (Black)
PIN2: Wiegand DATA1 (White)
PIN1: Wiegand DATA0 (Green)

3 2 1

Cable Shield
(Optional)

Access Controller

GND
Wiegand Output.Data1
Wiegand Output.Data0
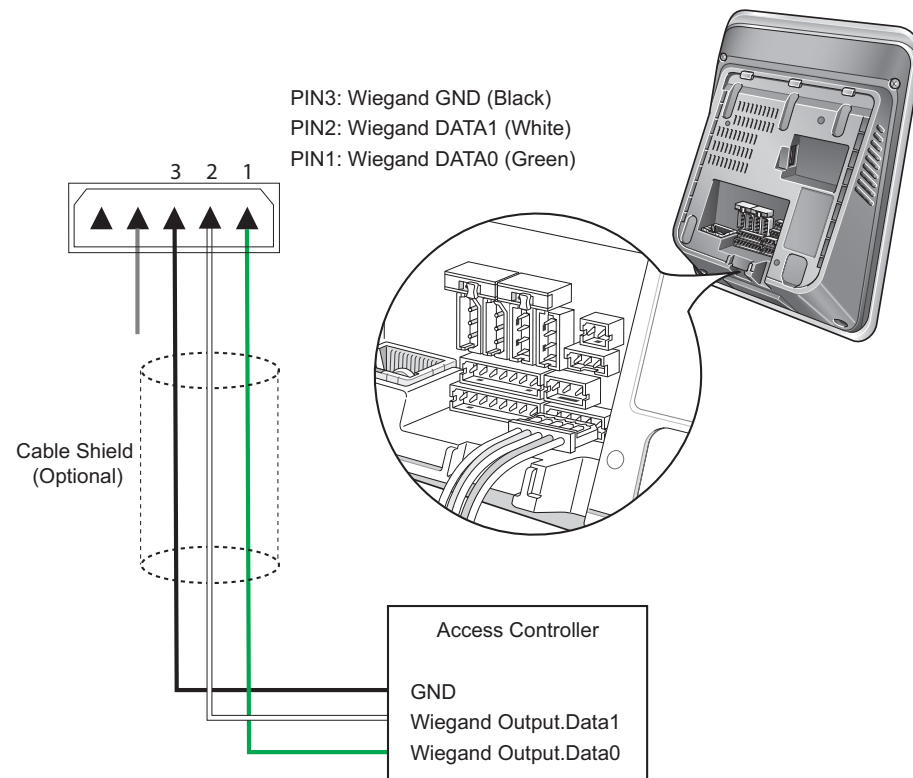
Mini USB Connection

FaceStation can communicate with a PC via the mini USB port.
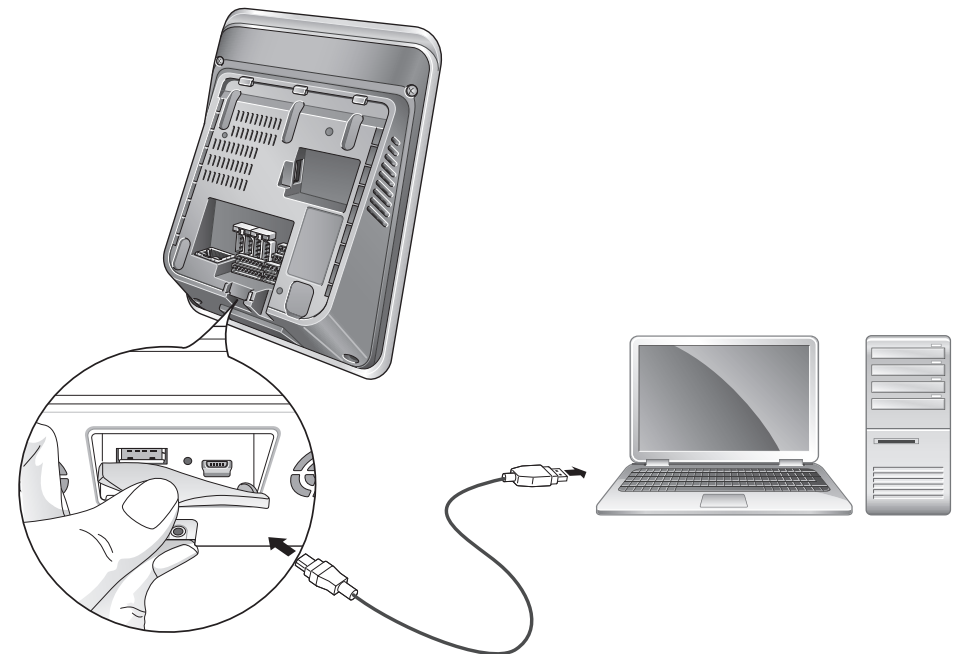
USB Connection

The USB port can be used to upload/download data to/from a USB memory device.
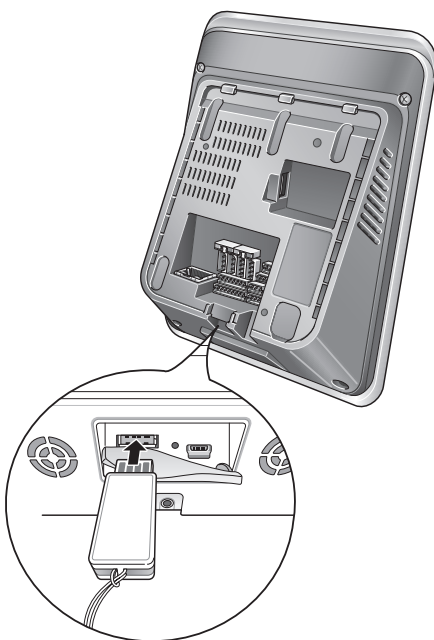
▤ Note

- Compatibility issues may cause recognition difficulties with some USB memory devices.

Analogue Video Phone Connection

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)
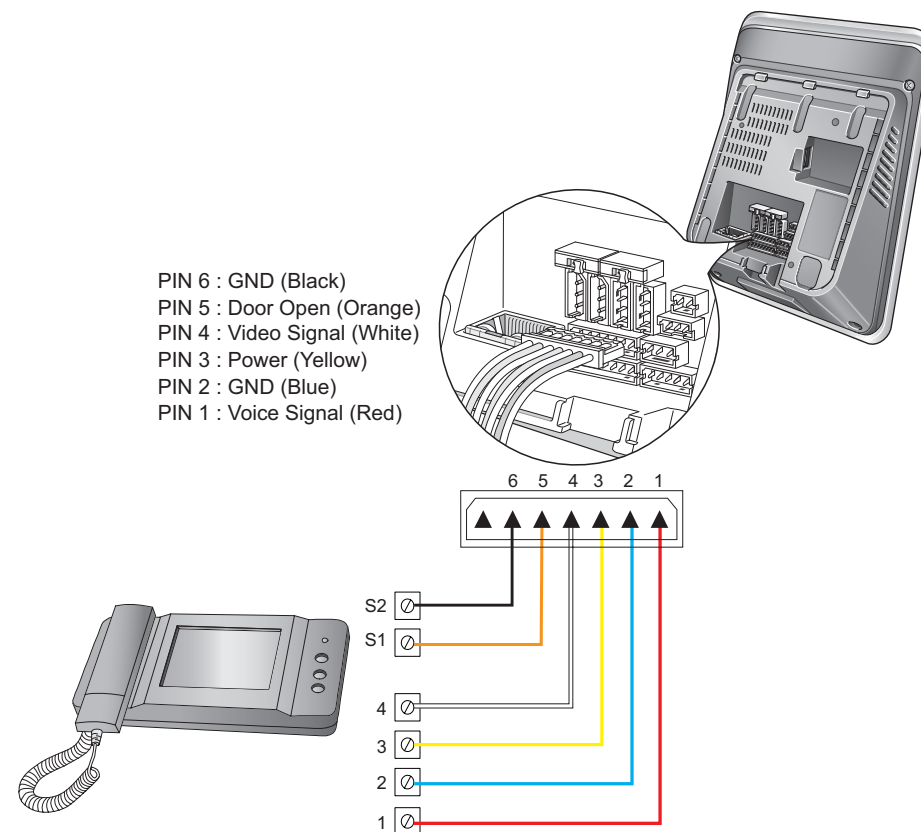
▤ Note

- Compatible Analogue Video Phone Models:
  COMMAX/ CAV-35N, COMMAX/ CAV-50H, COMMAX/ CAV-50P

25

4 Device Configuration

FaceStation Menu Tree

Network Settings

Operation Mode Settings

Device Settings

Display and Sound Settings

FaceStation Menu Tree

1. User
- Enroll User
- Edit User
- Search
- User Capacity Info
- Delete All Users

2. 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

3. 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

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

5. Display
- Theme
- Background
- Voice Instruction
- Menu Timeout
- Pop-Up Time
- Backlight Timeout
- Volume
- Language
- Central Time Display
- Date Display
- Authentication Alert

6. Log
- Log List
- Log Search
- Delete All Log
- Log Info

27

Network Settings

Setup various communication interfaces with the device.
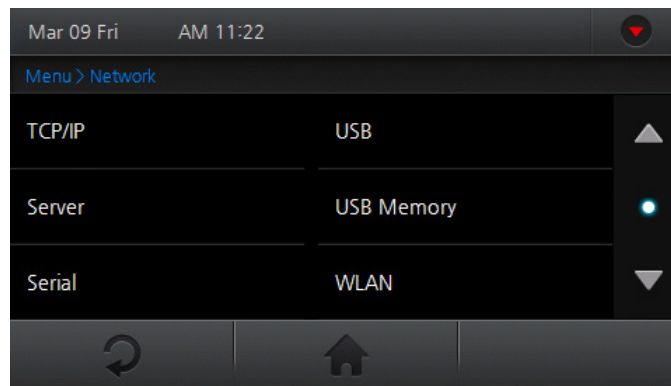
1   Go to **Menu** > **Network**.

2   Navigate to the desired interface.

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

Setting TCP/IP

Setup the TCP/IP network settings of the device.
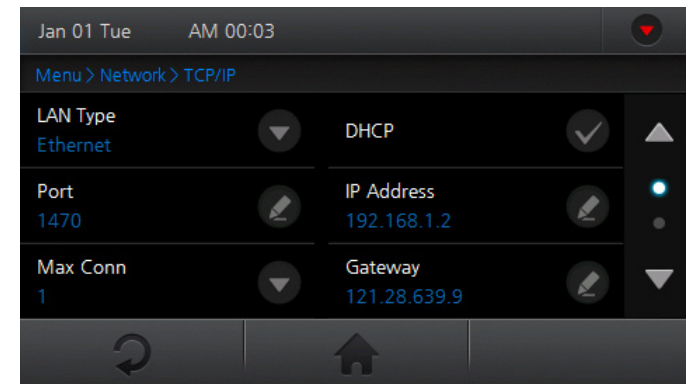
1   Go to **Menu** > **Network** > **TCP/IP**.

2   Set the options.

- **LAN Type**   Select the net type 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 the desired IP address and press **OK**. (Only available with DHCP disabled)

- **Gateway**   Enter the desired gateway address and press **OK**. (Only available with DHCP disabled)

- **Subnet**   Enter the desired subnet address and press **OK**. (Only available with DCHP disabled)

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

Setting Server

Setup the TCP/IP settings of the server to be connected with the device.
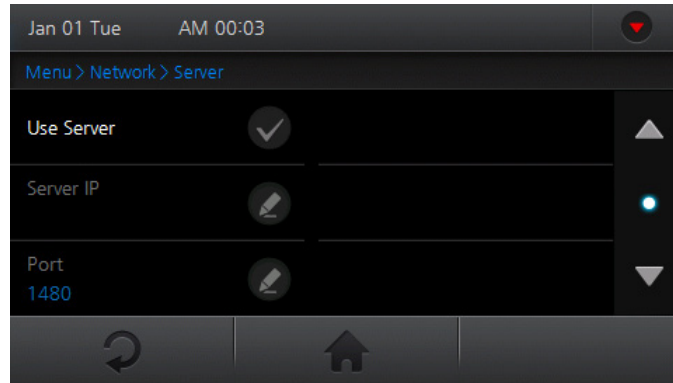
1	Go to **Menu** > **Network** > **Server**.
2	Set the options.

- **User Server**   Check to use the "Server mode".
- **Server IP**   Enter the server's IP address and press **OK**.
  (Only available if **Use Server** is enabled)
- **Port**   Enter the server's port and press **OK**.
  (Only available if **Use Server** is enabled)

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

Setting Serial Communication

Setup the serial network settings of the device.
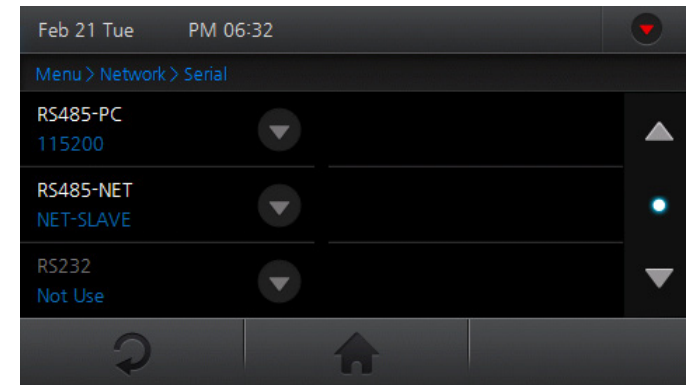
1	Go to **Menu** > **Network** > **Serial**.
2	Set the options and press **OK**.

- **RS485-PC**   You can enable/disable the RS485 port to connect with a PC and set the communication speed.
- **RS485-NET**   Set the desired RS485 communication mode. (**NET-HOST**: allows slave devices to be connect to the device; **NET-SLAVE**: allows the device to connect to a host)
- **RS232**   Set to communicate with a PC using RS232.
  (Only available if RS485 is disabled)

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

📄 **Note**

- The RS485 network supports up to 1 host devices and 7 slave devices (including up to 4 Secure I/O).

Setting USB
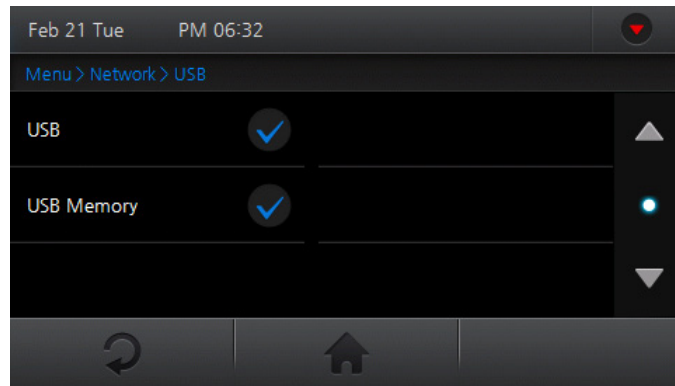
1   Go to **Menu** > **Network** > **USB**.

2   Set the options.

- **USB**   Setup the USB port to connect with a PC.

- **USB Memory**   Setup the USB port to connect with a USB memory device.

3   Press ⟳ to go to the previous screen or ⌂ to go to the Home screen.

Using USB Memory Device

Contains various options associated with the USB memory device.
(Only available if **USB Memory** is enabled)
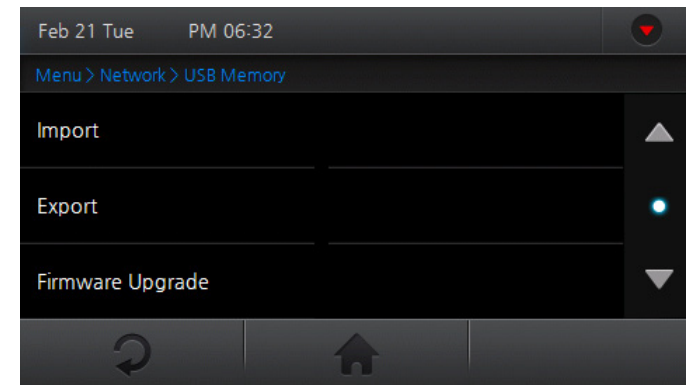
1   Go to **Menu** > **Network** > **USB Memory**.

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 ⟳ to go to the previous screen or ⌂ to go to the Home screen.

▤ Note

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

Setting WLAN (Only for wireless models)

Setup one of the four WLAN network presets to communicate with BioStar. The preset details can be configured via BioStar.
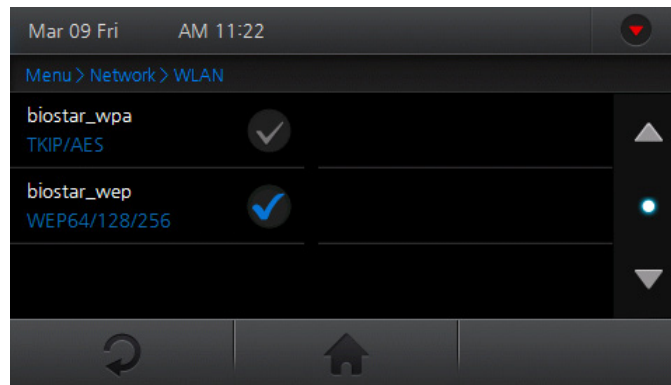
1	Go to **Menu** > **Network** > **WLAN**.
2	Check the preset option to use for WLAN connection.
3	Press ↻ to go to the previous screen or ⌂ to go to the Home screen.

Operation Mode Settings

Setup the various authentication modes, operation modes, and/or time & attendance triggers for the device. The authentication modes will operate according to the schedule set via BioStar.
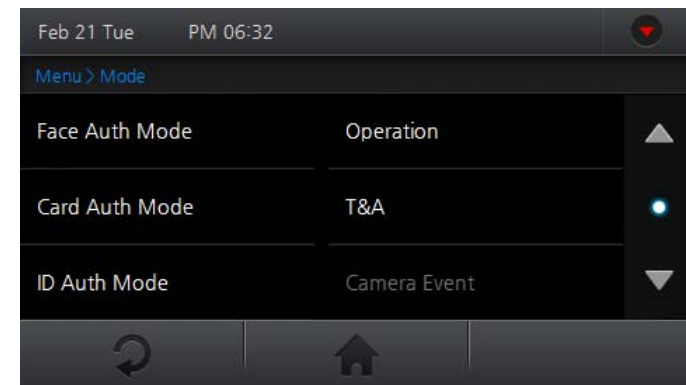
1	Go to **Menu** > **Mode**.
2	Set the options.
3	Press ↻ to go to the previous screen or ⌂ to go to the Home screen.

31

Face Authentication Mode
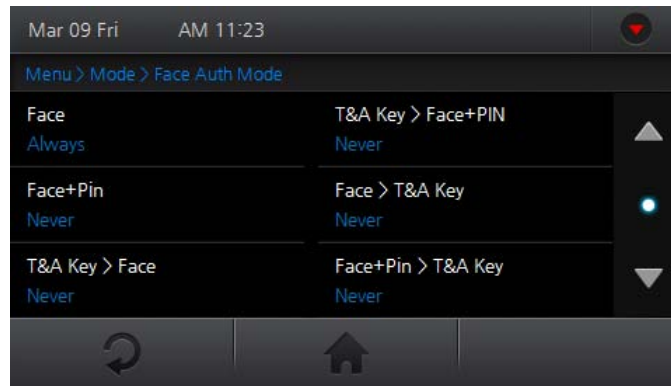
1	Go to **Menu** > **Mode** > **Face Auth Mode**.
2	Select a desired option.

- **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 schedule.
4	Press ↻ to go to the previous screen or 🏠 to go to the Home screen.

Card Authentication Mode
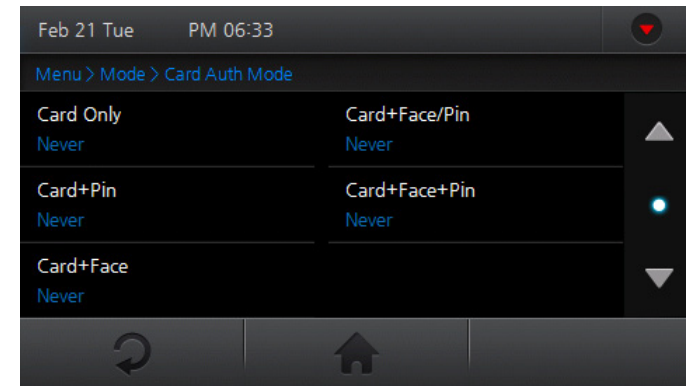
1	Go to **Menu** > **Mode** > **Card Auth Mode**.
2	Select a desired option.

- **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 schedule.
4	Press ↻ to go to the previous screen or 🏠 to go to the Home screen.

ID Authentication Mode

Feb 21 Tue   PM 06:33

Menu > Mode > ID Auth Mode

ID+Pin	ID+Face+Pin
Never	Never
ID+Face	
Never	
ID+Face/Pin	
Never	
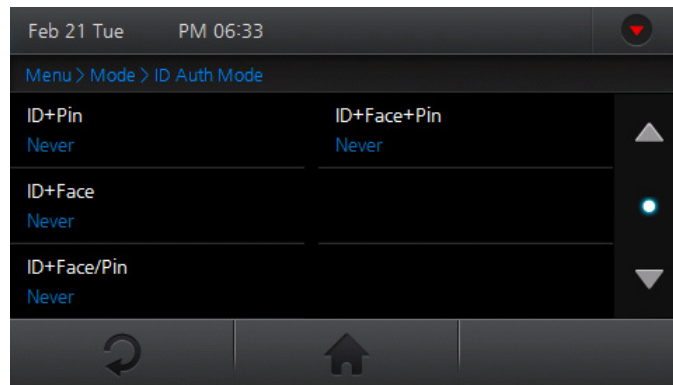
1 Go to **Menu** > **Mode** > **ID Auth Mode**.

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 schedule.

4 Press ↻ to go to the previous screen or ⌂ to go to the Home screen.

Setting General Operational Parameters

Feb 21 Tue   PM 06:33

Menu > Mode > Operation

Face Detection	Individual Auth
Dual Authentication	Match Timeout(sec)
Never	7
Card Mode	
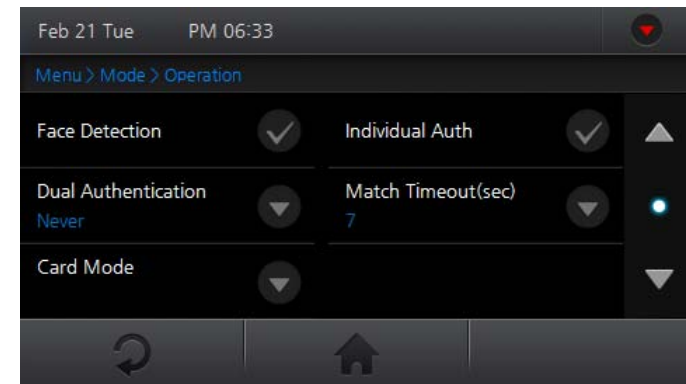
1 Go to **Menu** > **Mode** > **Operation**.

2 Check, or set the options and press **OK**.

- **Face Detection**   Check to use 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**   Requires the authentication of two different users within 15 seconds and operates the associate relay.

- **Card Mode**   Select whether or not to use the CSN card for authentication.

- **Individual Auth**   Check to enable individual authentication within the device. Seer **'User Registration(page 45)'** for more details.

- **Match Timeout(sec)**   Sets the time-out period for an authentication attempt.

3 Press ↻ to go to the previous screen or ⌂ to go to the Home screen.

Time and Attendance Mode
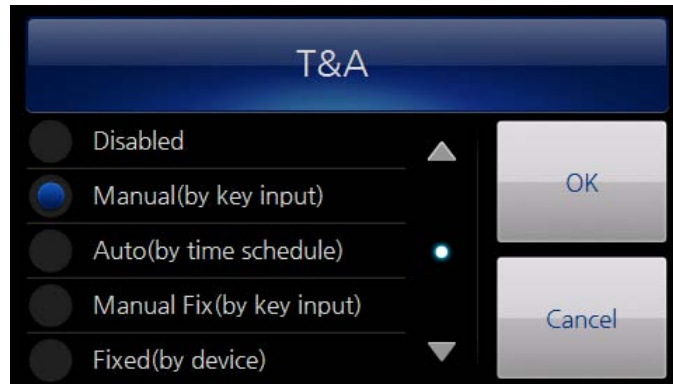
1 Go to **Menu** > **Mode** > **T&A** > **T&A**.

2 Set the T&A options.

- **Disabled** — Disables the T&A buttons. The Home menu and the **CALL** button remain active.

- **Manual(by key input)** — T&A events must by manually selected using the T&A buttons before authentication.

- **Auto(by time schedule)** — T&A events are automatically applied during authentication. The schedule can be created using BioStar.

- **Manual Fix(by key input)** — T&A events can be must be manually selected used the T&A buttons. The selected T&A event will remain until another event has been selected.

- **Fixed(by device)** — A T&A event will be fixed by the device.

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

Press **Cancel** to cancel any changes.

Device Settings

Sets system related features of the device.
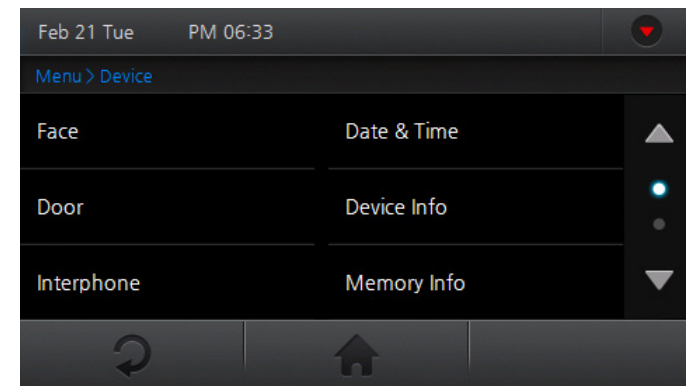
1 Go to **Menu** > **Device**.

2 Select the desired submenu and configure the corresponding settings.

3 Press ↻ to go to the previous screen or ⌂ to go to the Home screen.

34

Setting Face Authentication Settings

Dec 13 Fri   PM 01:53

Menu > Device > Face

Security Level	Proximity Level
Normal	Far
Enrollment Sensitivity	
4	
Enable SubImage	

1   Go to **Menu** > **Device** > **Face**.

2   Set the options.

- **Security Level**   Select the desired security level and press **OK**.

- **Enrollment Sensitivity**   Select the desired enrollment speed and press **OK**.

- **Enable SubImage**   Check **Enable SubImage** to capture then display a thumbnail image for each newly enrolled face SubID.

- **Proximity Level**   Sets the desired level that the sensor can recognize a face according to the proximity distance. Select **Far** or **Near** and press **OK**. When the option is set to **Far**, the sensor recognition rate gets higher.

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

Note

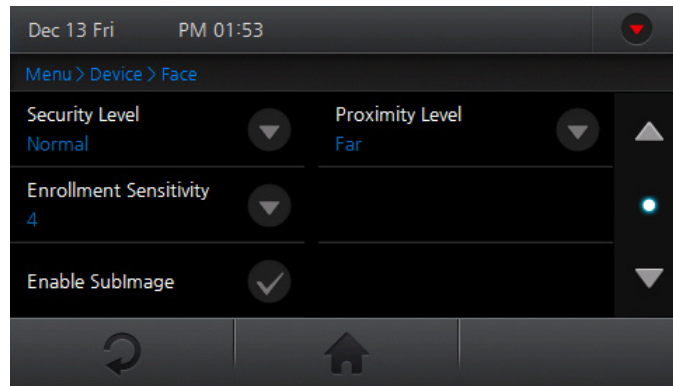- Increasing the security level will indirectly increase the FRR (False Rejection Rate), the probably that the system will reject access for an authorized user, because stricter authentication protocols will reject more inconsistencies.
- Decreasing the Enrollment Sensitivity will allow for easier enrollment.
- Each user can hold up to five face SubIDs, which can be used for advanced progressive enrollment for individuals with glasses or beards.

Setting Door Control

Jan 01 Tue   AM 00:03

Menu > Device > Door

Relay	RTE(Exit SW)
Internal Relay0	Not use
Driven by	RTE Type
All Events	N/O
Duration(sec)	Door Sensor
3	Not use
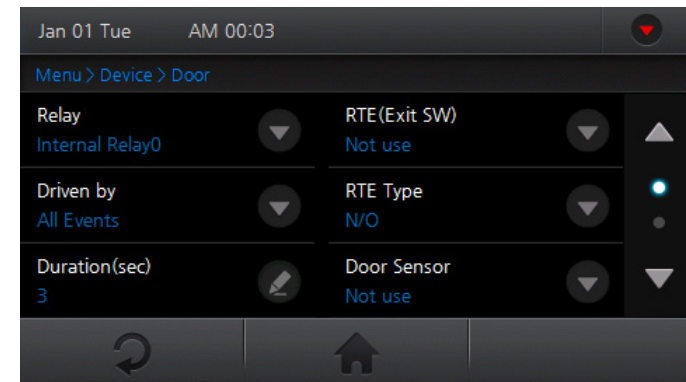
1   Go to **Menu** > **Device** > **Door**.

2   Set the options and press **OK**.

- **Relay**   Sets a relay to be used with the door.

- **Driven by**   Sets a trigger to activate the relay.

  - **All Events**:   Opens the door for all authentication modes.

  - **Authentication**:   Triggers the relay when a general authentication occurs.

  - **T&A Event**:   Triggers the relay when a time and attendance authentication occurs.

- **Authentication** : Triggers the relay only when both
  + T&A Event general authentication and time &
  attendance authentication are set
  to trigger the relay.

- **Disabled** : Disables all triggers for the relay.

- **Duration(sec)** Sets the activation time of the relay.
  (Period in which the door will remain open)

- **RTE (Request to Exit)** Sets an input to be used as an exit switch.

- **RTE Type** Set the default state of the switch.
  (N/O: Normal Open; N/C: Normal Closed)

- **Door Sensor** Sets an input to be used for detecting the door
  status.

- **Door Sensor Type** Set the default state of the switch.
  (N/O: Normal Open; N/C: Normal Closed)

- **Held Open** Sets the duration that a door must be held open
  Period(sec) before an alarm is triggered.

- **Unlock Time** Sets a schedule for which the door will remain open.
  The schedule can be set using the BioStar software.

- **Lock Time** Sets a schedule for which the door will remain locked.
  The schedule can be set using the BioStar software.

3 Press ⟲ to go to the previous screen or ⌂ to go to the Home screen.

Setting Interphone

Enables the device to act as an interphone.
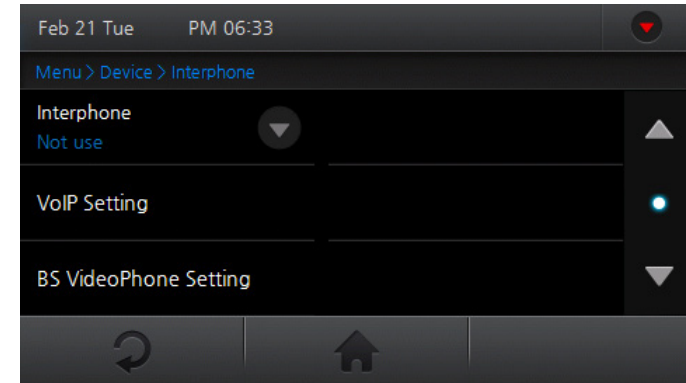
1 Go to **Menu** > **Device** > **Interphone**.

2 Select the desired interphone type and configure the corresponding settings.

Interphone Select the desired interphone type and press **OK.**

VoIP Setting   Set the desired VoIP settings for the IP Interphone.

- **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 the 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**.

BS VideoPhone Setting   Set the desired BioStar VideoPhone settings.
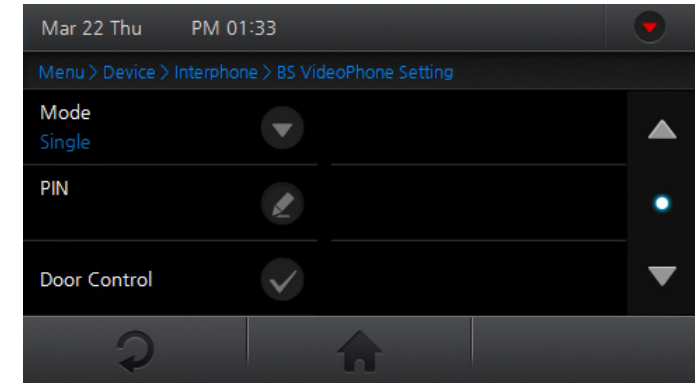
- **Mode**   Select either single or extension mode and press **OK**.

- **PIN**   Enter a pin number for the BioStar VideoPhone and press **OK**.

- **Door Control**   Enables or disables the door control on the BioStar VideoPhone.

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

Device Configuration

Setting Time

Sets the date/time options for the device.
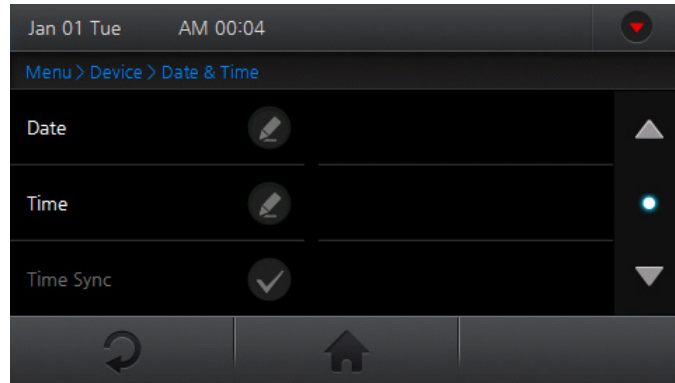
1 Go to **Menu** > **Device** > **Date & Time**.

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** Synchronizes the time on the device with the BioStar server. (Only available in "Server Mode")

3 Press ⟳ to go to the previous screen or ⌂ to go to the Home screen.

Checking Device Information

Displays information such as the model name, device ID, hardware version, firmware version, kernel version, MAC address and more.

1 Go to **Menu** > **Device** > **Device Info**.

2 Press ⟳ to go to the previous screen or ⌂ to go to the Home screen.

Checking Memory Status

Display the status of the DRAM, FLASH and FLASH2 memory.

1 Go to **Menu** > **Device** > **Memory Info**.

2 Press **OK** to return to the previous screen.

TouchScreen Calibration

Recalibrates the touchscreen to coordinate the point of contact with the user interface.

1   Go to **Menu** > **Device** > **Touch Calibration**.

2   Press the center of each point until the completion message appears.

Carefully press and briefly hold stylus on the center of the target.
Repeat as the target moves around the screen.
Press the Esc key to cancel.

+

3   Press **OK** to complete the touchscreen calibration.

Note

 • There is no "Esc" key so the process must be completed to exit the touchscreen calibration.

Device Reset

1   Go to **Menu** > **Device** > **Reset**.

2   Press **Yes** to restart the device.

 Press **No** to return to the previous screen.

Factory Default

1   Go to **Menu** > **Device** > **Factory Default**.

2   Press **Yes** to initialize the device.

 Press **No** to return to the previous screen.

Note

 • A factory default will only affect the device configurations. The user information and log data will remain intact.

Camera

1   Go to **Menu** > **Device** > **Camera** > **Power Line Frequency**.

2   Select the corresponding power line frequency setting.

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

 Press **Cancel** to cancel the setting.

Note

 • Make sure to set the correct power line frequency to avoid the image flickering.

Display and Sound Settings

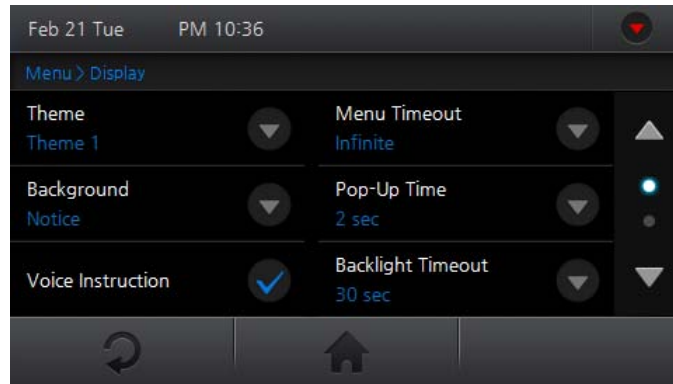|	
1	Go to **Menu** > **Display**.
2	Set or check by pressing the relevant option.
3	Press ↻ to go to the previous screen or ⌂ to go to the Home screen.

Theme

Sets the graphical theme of the device.

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

Background

Sets the background of the device.

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

> 📄 **Note**
> • The Logo screen is displayed during authentication.

Voice Instruction

Enables voice instructions from the device.

Menu Timeout

Sets the amount of idle time required before returning to the home menu.

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

Pop-Up Time

Sets the duration before the pop-up window disappears.

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

Backlight Timeout

Sets the amount of idle time required before turning off the LCD.

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

Volume

Sets the volume output of the device.

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

Language

Sets the displayed language on the device.

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

Central Time Display

Enables or disables the clock located in the center of the screen.

Date Display

Sets the desired date format.

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

Authentication Alert

Enables or disables the authentication alert that is outputted when the face authentication screen is displayed. When the authentication alert is enabled and the face authentication screen is displayed, corresponding alert sounds for an authentication mode is outputted. When the authentication alert is disabled and the face authentication screen is displayed, a beep is outputted.

5 Device Operation

Basic Screen Views

User Management

Authentication Modes

Viewing Logs

Basic Screen Views

Face Authentication Screen

The following screen is displayed during face authentication.

|		
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 status.
6	Image Display Screen	Displays an image from the camera.
7	Authentication Method	Displays the authentication method.
8	T&A Event	Displays the current T&A mode.
9	Current Time	Displays the current time on the device.
10	Face Detection Guide Line	Displays the guide line for face detection. (Blue circle: Face Detected/ Orange: Face Not Found)

Home Screen

The following screen is the default home screen.
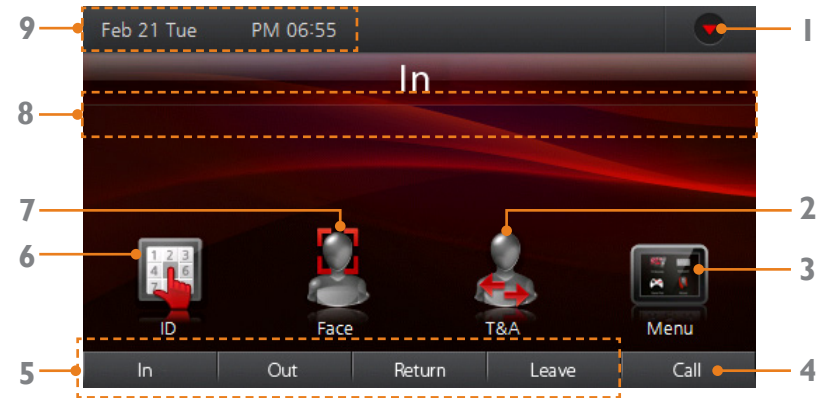
1	Status Button	Click to display the status of the device.
2	Additional T&A Button	Click to select up to 12 time & attendance options in addition to the 4 basic time & attendance buttons.
3	Menu Button	Click to enter the administrator menu.
4	Call Button	Click to use the selected video phone.
5	Basic T&A Button	Displays 4 basic time & attendance events
6	ID Authentication Button	Click to initiate the ID authentication mode.
7	Face Authentication Button	Click to initiate the face authentication mode.
8	T&A Event	Displays the current T&A mode.
9	Status Bar	Displays the date and time on the device.

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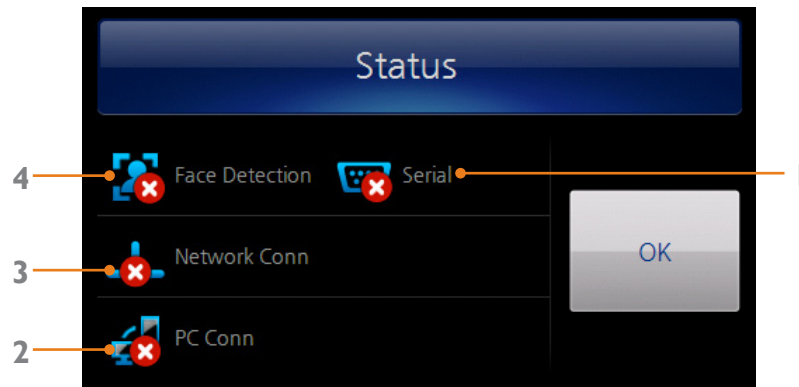
1	Serial	Displays the connection status with a host when in RS485 slave mode.
2	PC Connection	Displays the connection status with a PC through Ethernet or WLAN.
3	Network Connection	Displays the connection status of the Ethernet or WLAN.
4	Face Detection	Displays whether or not the face recognition is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

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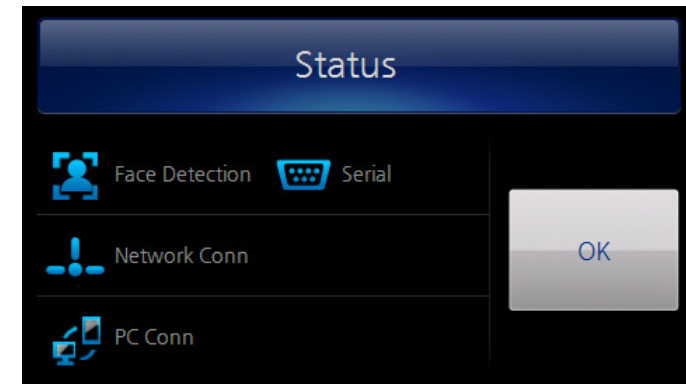
When the face recognition and all connection status are successfully set, a screen as shown above is displayed.

User Management

User Registration

After the device installation, register the administrator before use.
Check the "Administrator" option within the enroll user window to create an administrator.
The administrator can register and delete users and set preferences.

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

2 | Register the user's picture.

1) Press the Profile Image 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.
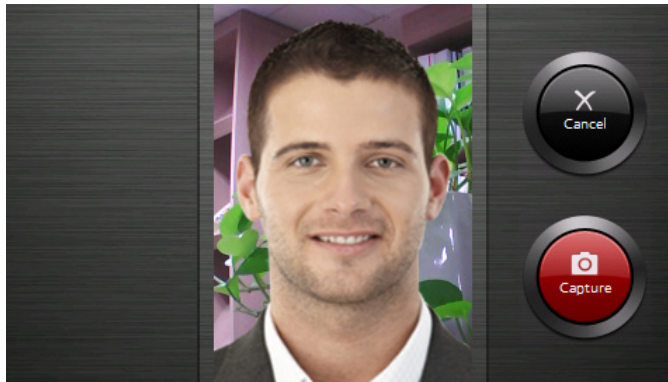
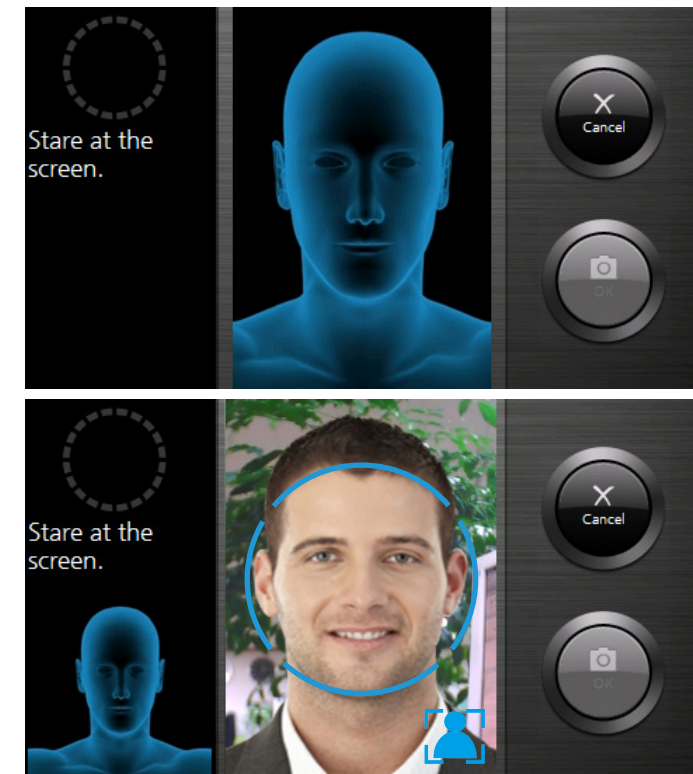**3** | Press **User ID** to enter the user ID and press **OK**.

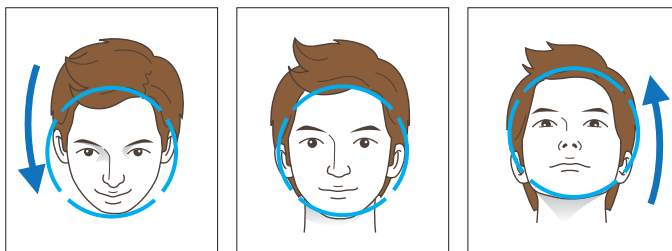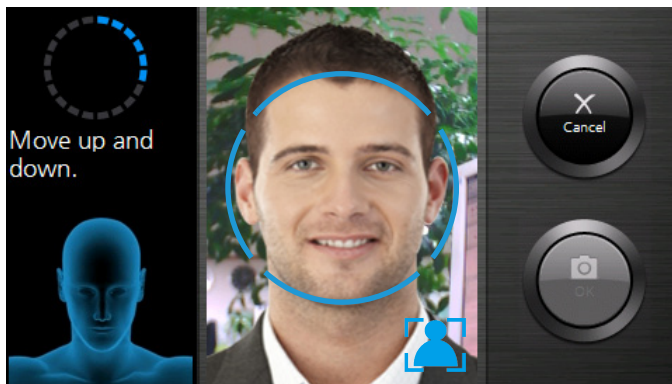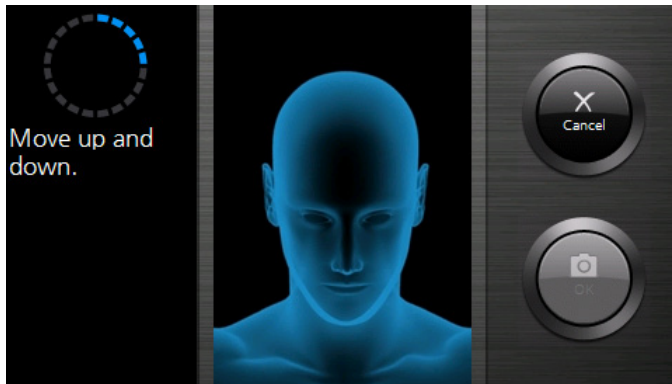**4** | Press **Name**, and enter a name press **OK**.

5 | Press **Face** to enroll a face.

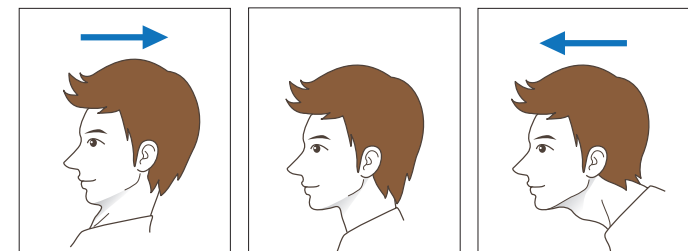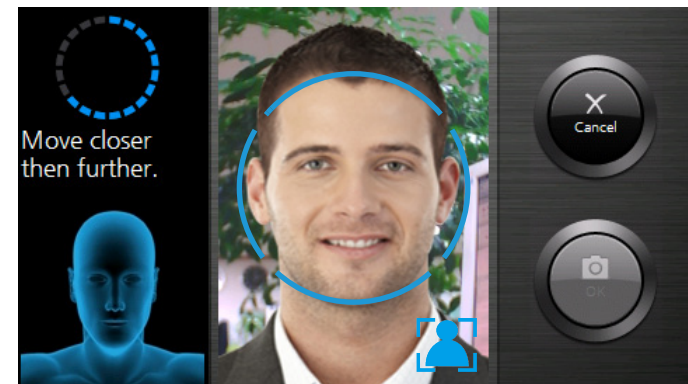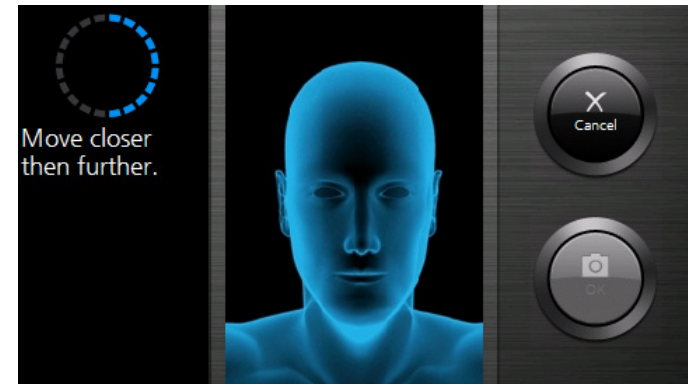Up to five different versions of the user's face may be enrolled.
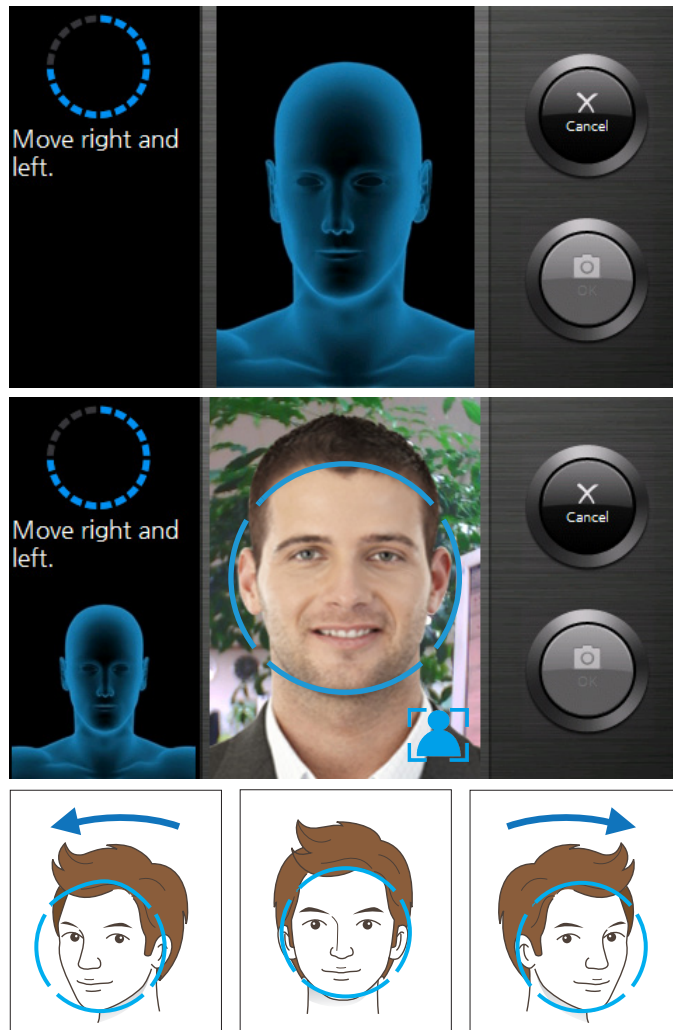
1) Stare directly at the screen.

2) Move your head up and down.

3) Move your face back and forth.

46

4) Move your face right and left.

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

6) Press **Face** to enroll another version of the individual's face.

6	Press **Card** to enter the ID and press **OK**.
7	Press **PIN** to enter the pin number and press **OK**.
8	Check **Administrator** to register as the administrator. Uncheck **Administrator** if registering as a general user.
9	Check or uncheck **Bypass Card**. If **Bypass Card** is checked when registering a user, the user is always authenticated regardless of the authentication mode on the device.
10	Press **Individual Auth** and set the authentication mode. 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**.
11	Select **Group** and set the access of group users. A group can be selected from Access groups transferred from the BioStar software to the relevant device. After setting, press **OK**.
12	Press 👤⊕. You can register a new user. Press ↻ to go to the previous screen or 🏠 to go to the Home screen without saving the changes.

▤ **Precautions for Registration**

- If there is no progress in registration, slightly move your face.
- It is recommended to register your face at the installation site.
- Register an expressionless face.
- It is recommended to keep a distance of 40~80cm from the device when registering your face.
- If a user wears glasses, you may replace step 4 "Move your face left and right" with "take off your glasses and stare directly at the screen".
- Remove any obstacles obstructing your face. The eyes and eyebrows must be exposed.
- Only one person can use the device at a time.
- Do not wear sunglasses when using the device.
- Re-enroll users that have undergone major changes in facial appearance.
- Multiple versions of an individual's face are extremely useful for individuals wearing glasses or individuals with beards.
- Individuals wearing glasses can enroll their face with and without glasses.
- Individual with beards can progressively enroll various stages of a beard cycle. Once the beard cycle has been completed, the individual will not have to register again.

▤ **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.

Modifying User Information

Use the following steps to modify the information of a registered user.
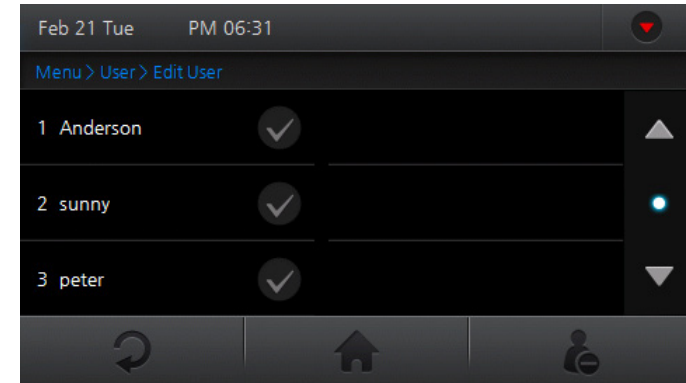
1   Go to **Menu** > **User** > **Edit User**.

2   Select a user by pressing the user name field.

Press **Face** to enroll or delete a face.

3
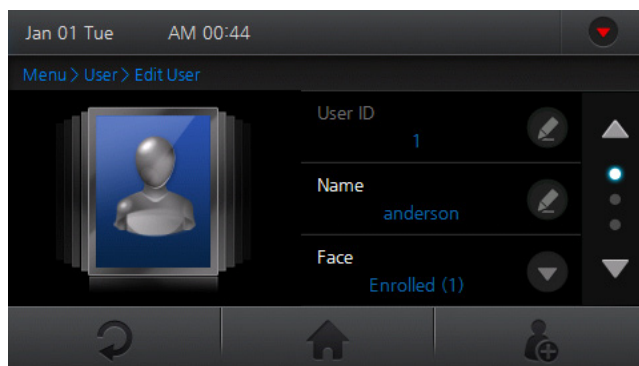
1) Press [icon] to register a new face.
For details regarding the information modification, please refer to **'Step 5 of User Registration(page 45)'**.

2) Press [icon] to delete a face.
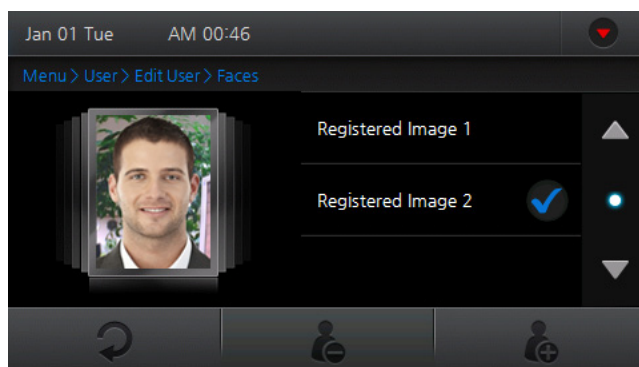
4

Modify the desired other information.

For details regarding the information modification, please refer to **'User Registration(page 45)'**.

5

Press [icon] to save the modified information.

Press [icon] to go to the previous screen or [icon] to go to the Home screen without saving the changes.

📄 Note

- The user ID cannot be modified.

Deleting a User

Use the following steps to remove user(s) from the FaceStation's database.

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

2   Select the user(s) to be deleted.

3

Press [icon] .

4

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

Press **No** to cancel the deletion.

Deleting All Users

Use the following steps to delete all the users within the database.

1	Go to **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 for a User

Use the following steps to search for a registered user.
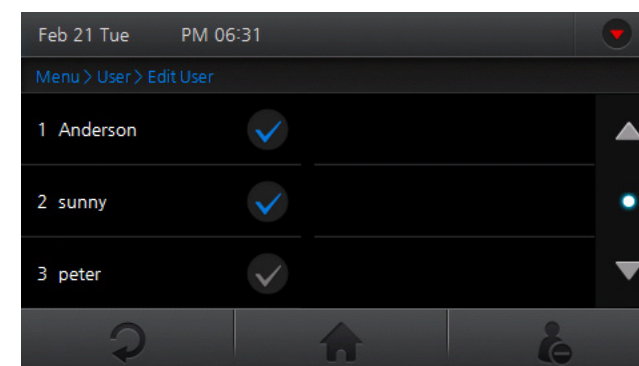
1	Go to **Menu** > **User** > **Search**.
2	• **Search by ID**　　Enter an ID and press **OK**. • **Search by Name**　Enter a name and press **OK**. • **Search by CSN**　Enter the card.
3	Press **OK** to display the search results. Press **Cancel** to cancel the search.

Checking User Capacity

Use the following steps to view the memory status of the user DB.

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

Note

- FaceStation can store up to 10,000 users (1:1).

Authentication Modes

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.

Face Authentication Procedure

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

1   Align your face within the orange guideline until it turns blue.
And keep your face still until the authentication is complete.
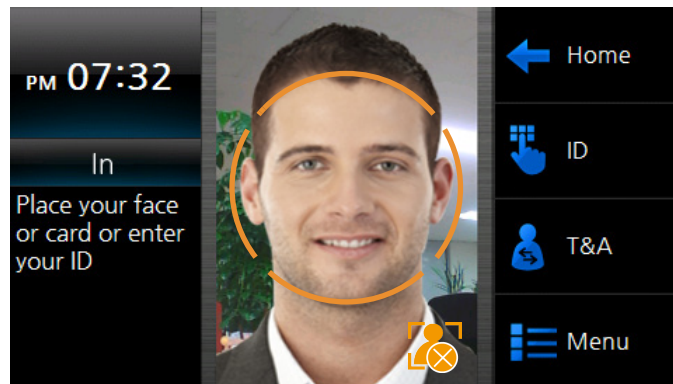
Note
- Make sure to keep the distance of 50cm from the device when authenticating the face.

2   The follow screen will be displayed upon a successful authentication.
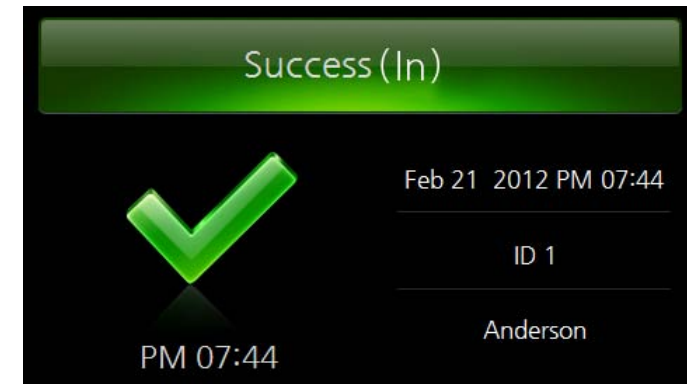
Precautions for Authentication
- If authentication takes too long, slightly move your face.
- Remove any obstacles obstructing your face. The eyes and eyebrows must be exposed.
- Only one person can use the device at a time.
- Do not wear sunglasses when using the device.
- Re-enroll users that have undergone major changes in facial appearance.

Face Authentication Modes

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 Modes

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 Modes

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.
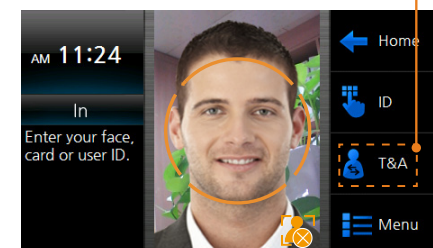
ID + Face/Pin

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**.

Using Time and Attendance

1   Press one of the T&A keys (F1 ~ F4) or click the T&A button and select an event on screen.

T&A key

AM **11:24**

In
Enter your face,
card or user ID.

Home

ID

T&A

Menu

Perform the authentication process.

2   Please refer to **'Authentication Modes(page 51)'** for details regarding the face, card and ID authentication processes.
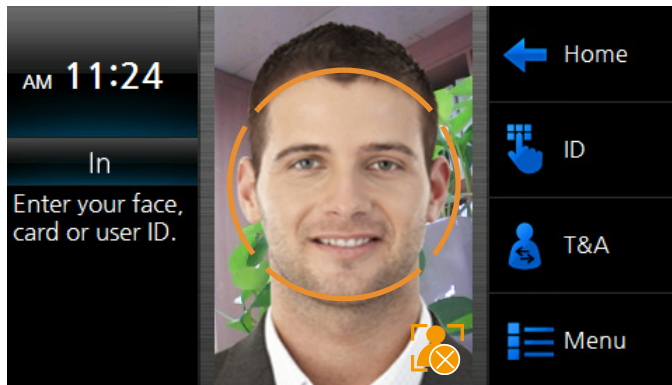
▤ Note

- 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 **'Time and Attendance Mode(page 34)'** for details regarding Time and Attendance.

Checking Time and Attendance

A general user can view their access and attendance records.

1 Press **Menu**.

2 Successfully authenticate a general user.

Viewing Logs

View, search, or delete all logs.
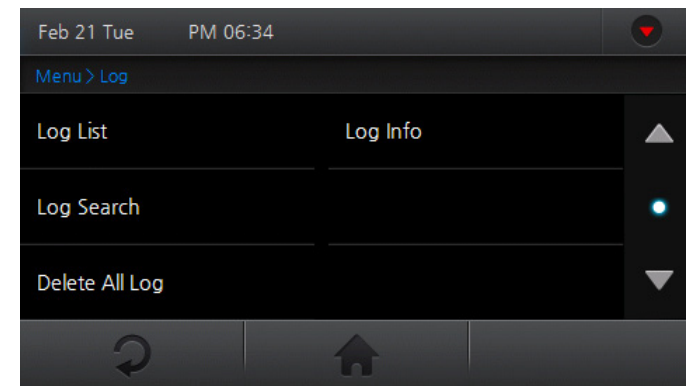
1 Go to **Menu** > **Log**.

2 Select the desired option.

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

Log List

You can select and view the desired event log.

1 Go to **Menu** > **Log** > **Log List**.

2 View the logs within the device.

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

Log Search

Search logs by event, date, time and user ID.

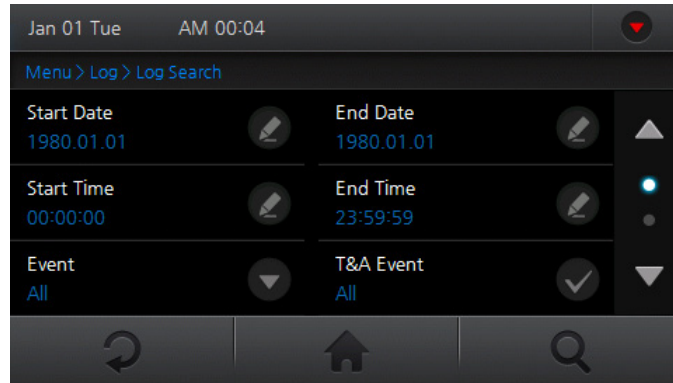| **1**	Go to **Menu** > **Log** > **Log Search**.
2	Set the search filters and press **OK**.
3	Press 🔍 to display the search results.
4	Press ↺ to go to the previous screen or 🏠 to go to the Home screen.

Delete All Logs

All logs will be deleted from the device's memory.

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

Log Info

View log events stored on the device.

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

📄 **Note**

- FaceStation can store up to 1,000,000 logs and 5000 image logs.

Appendix

Specifications

Product Specifications

System	Max Users	1000 (1:N), 10,000 (1:1)
	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 (Optional)
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	Use certified power adapters that meet the specifications.
	Current(mA)	-		1500	
Switch Input	VIH(V)	-	TBD	-	
	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

Troubleshooting

Please contact your local dealer/distributor for support or contact Suprema at support@supremainc.com. Please submit the following information and we will coordinate support with your local dealer/distributor.

- Device model
- F/W version of the device
- H/W version of the device
- Detailed information regarding the issue
- Error messages / screenshots, if possible
- Contact information (Company, Name, Telephone, Email)

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 difference 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 as a 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