www.supremainc.com

suprema

D-Station

Multi-Biometric Fusion Technology
with Dual Finger & Face Recognition

User Guide

Ver 1.0

Contents

Chapter 1. Product Information 4

1.1 Features....4

1.2 Terms....4

1.3 Safety Tips....5

1.4 Fingerprint Recognition....6

Fingerprint Recognition....6

The Process....6

Fingerprint Recognition Method....6

1.5 Face Recognition....8

The Process....8

Face Recognition Method....8

Chapter 2. Installation 9

2.1 Package Contents....9

Basic Contents....9

Optional Accessories....9

2.2 Product Parts Description....10

Front / Bottom....10

Rear....11

2.3 Dimensions....12

2.4 Installation of Wall Mount Bracket....13

Planning the installation position of D-Station....13

Adjusting the camera angle....14

Fixing the wall mount bracket....15

2.5 Connector connection part....15

2.6 Cable Specifications....16

1) Power Supply....17

2) USB Cable Connection....17

3) LAN Connection....18

4) LAN Connection (Direct connection with PC)....18

5) PoE Hub Connection....19

6) Wireless LAN Connection(Wireless Version Only)....19

7) USB Memory Connection....20

8) RS485 Network Connection....20

9) RS485 Connection for Secure I/O....21

10) RS232 Connection....21

Contents

11) Videophone Connection 22
12) Relay Connection – Fail-Safe Lock 22
13) Relay Connection – Fail-Secure Lock 23
14) Relay Connection – Automatic Door 23
15) Switch Input Connection – for RTE, door sensor and alarm inputs 24
16) Wiegand Input Connection – When Using a Separate Wiegand Reader 24
17) Wiegand Output Connection – When Using a Separate Access Controller 24

2.7 System Configurations 25

Chapter 3. Admin Menu 27

3.1 Start-up Screen 27
Start-up Screen Menu 27
Administrator Registration 28
Opening the Admin Menu 30
Admin Menu Functions 31
Authentication Mode 32

3.2 User Information Management 34
User Registration 34
Deleting User Information 36
Changing User Information 37
User Search 38
Checking Memory Information 39

3.3 Using the User Menu 39
DB Initialization 39
DB Error Check 40
Card Format 40

3. 4 Network Management 41
TCP / IP Setting 41
Server Configuration 42
Serial Configuration 43
USB 44
USB Memory 45

3.5 Operation Management 46
Setting Authentication Mode 46
Time and Attendance Configuration 48
Confirming Time and Attendance Events 50

3.6 Terminal Management 50
Configuring Fingerprint Authentication 50

Contents

Setting the Door Operation 53

Configuring the Camera 56

Setting the Time 57

Terminal Management 57

Memory Check 58

3.7 Display / Sound Management 59

Setting Display / Sound 59

3.8 Log Management 60

Log Management 60

Chapter 4. User Menu 62

4.1 Access Authentication 62

1 : N Access by Fingerprint Recognition 62

Access Through 1:1 Authentication 62

Fingerprint Authentication 63

Card Recognition 63

ID + Fingerprint Input 64

ID + PIN Input 65

Face Fusion Recognition 66

Forced Face Detection 67

4. 2 Time and Attendance Management 68

Time and Attendance Management using 1:N fingerprint recognition 68

Time and Attendance Management through 1:1 Authentication 69

Checking Users' Access / T&A Record 70

4.3 Interphone Use 70

Chapter 5. Appendix 71

5.1 Troubleshooting 71

5.2 Product Specifications 72

5.3 Electrical Specification 73

5.4 FCC Rules 74

5.5 License 75

Chapter 1. Product Information

Chapter 1. Product Information

1.1 Features

The D-Station features a 16 megapixel, 5.0 inch-wide LCD panel and an 18-bit sound system, and is the first of its kind to provide diverse real-time multimedia content.

The Tri-CPU facilitates the world's fastest fingerprint recognition. It is capable of matching 10,000 fingerprints within 1 second and boasts the largest storage capacity (storing up to 200,000 fingerprints and 1,000,000 logs).

Wi-Fi wireless LAN enables real-time access checking and logging of time and attendance on a PC (optional).

The D-Station allows convenient transfer of registered fingerprint information, access, and time and attendance data to other D-Stations with a USB flash drive.

The D-Station adopts core algorithm technology recognized for its excellence in recognition rate, recognition speed and memory efficiency to make it the world's most reliable solution.

The D-Station adopts the RF reader function to enable each user's choice of among four methods of authentication: fingerprint, card, PIN, face fusion (optional).

1.2 Terms

- Administrator

Administrator refers to the person(s) who has the authority to manage user information. This may include registering or deleting users, or setting and changing various values of the terminal's configuration. A user who has the authority of the administrator, or knows the terminal's PIN, can control and manage all functions of the terminal.

- 1:1 Authentication

1:1 authentication is the process of matching the input information to the stored information when a user enters their ID and the corresponding PIN or fingerprint.

- 1:N Recognition

1:N recognition is the process of matching the input fingerprint to stored fingerprint information when the fingerprint is read without an ID.

- Fingerprint Registration

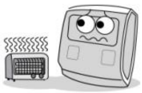
Fingerprint registration is the process of extracting and storing the unique features of each fingerprint to the fingerprint recognition database. These features are obtained from images taken by the fingerprint sensor. The fingerprint recognition information stored in the process is used repeatedly so proper input of fingerprints determines the quality of fingerprint recognition.

1.3 Safety Tips

The following instructions ensure your safety and prevent any property damage. Be sure to read the following and use the product correctly.

Do not install the terminal in a place affected by direct sunlight, humidity, dust or soot.

Keep the terminal away from magnets or anything containing magnetic material such as CRT, TV sets, computer monitors and speakers. They may harm the product.



Keep the terminal away from heating products.

Do not let any liquids (water, soda or solution) get into the terminal.

Clean the terminal regularly to prevent dust settling on it.

Use a soft cloth or towel when cleaning the terminal. Do not spray water on the terminal.

- Wipe the dust or dirt on the fingerprint application area with a dry soft cloth. Cleaning solutions, gas or thinner harm the surface of the fingerprint application area resulting in malfunction in fingerprint input.

Do not drop the terminal or subject it to heavy impact.

Do not apply too much pressure to the touch screen.

Do not disassemble, repair or reconstruct the terminal.

Keep the terminal out of reach of children.

Do not use the terminal for any purposes other than its original use.

In cases of product malfunction or any other problems, please contact a service center.

1.4 Fingerprint Recognition

Fingerprint Recognition

Fingerprints are an individual’s unique biometric information and this information does not change throughout a lifetime. Fingerprint recognition technology uses this fingerprint information for authentication and identification purposes.

This technology eliminates the risks associated with loss or fraudulent use which are common to PIN or card technology. This reliable and convenient technology is now adopted in various fields as next-generation security technology.

The Process

1. Fingerprints consist of ridges which protrude from the surface, and valleys which are the spaces between these ridges. Each individual has a different pattern of ridges and valleys. Fingerprint recognition utilizes this unique quality of an individual’s fingerprints.
2. Fingerprint sensors detect the ridges of the finger and turn these ridges into a two-dimensional fingerprint image. Fingerprint sensors are available in various types according to their mechanism. These mechanisms include optical, semi-conductor, and scan sensors.
3. The process of identifying each fingerprint’s features from the constructed image produces the fingerprint recognition information. The fingerprint recognition information is hundreds of bytes of data, which is stored in the terminal’s database and used for authentication.

Note) Protection of individual biometric information

Suprema’s fingerprint recognition products are designed not to store fingerprint images, which are an individual’s private biometric information, in any circumstances and thus prevent the leaking of private information.

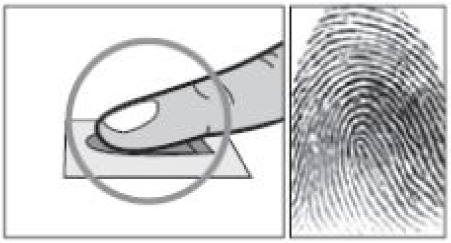
Fingerprint Recognition Method

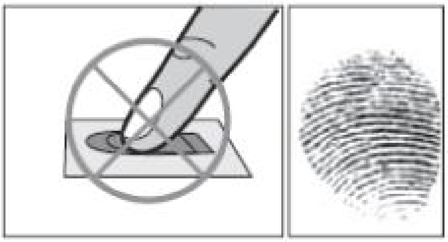
1. Select a finger for fingerprint input.

- We recommend the index finger or middle finger of your dominant hand.
- Thumbs, ring fingers and little fingers are relatively hard to place on the center of the sensors and may cause unstable posture when applying these fingerprints to the sensor.

2. Correctly apply fingerprints to the sensor.

- Place the finger squarely on the sensor so that the finger covers a large area of the sensor.
- Place the fingerprint core (the area with the most features) on the center of the sensor.
- The fingerprint core has the most ridges and is usually located on the opposite side of the lunula (the white part) of a nail.
- Many users wrongly put the fingertip on the sensor. Place the finger on the sensor so that the lunula aligns with the center of the sensor.
- Raising the finger upright on the sensor inputs only the print of fingertip, and results in failed registration or authentication.





3. Coping with various finger conditions

- Suprema’s fingerprint recognition products are designed for easy fingerprint input regardless of weather or finger conditions. In cases of input failure because of external conditions, please refer to the following:
- When the finger is sweaty or wet, remove the sweat or water before you try to input your fingerprint.
- When the finger is dusty or dirty with any substances, shake or clean the finger before you try to input your fingerprint.
- When the finger is too dry, blow on the fingertip before input.

4. Recommendations

- Proper registration is very important for accurate fingerprint recognition. So take care to properly input the fingerprint in the fingerprint registration process.
- When failed recognition cases increase, the following measures are recommended:
- Delete the registered fingerprint and register your fingerprint again.
- Register the same fingerprint in addition to the original registration.
- If a scar prevents a finger from being registered, register another finger.
- Two or more fingerprints per person can be registered for cases when you cannot use your usual fingerprint because of injury or because the hand is used to carry something.

1.5 Face Recognition

Face is one of the most widely used biometrics such as fingerprints and eye iris. Face recognition technology exploits these facial features to automatically identify or verify a person. This technology is an alternative to fingerprint or eye iris for authentication in that face can be indirectly captured and freely used in unconstrained environment compared to other biometrics.

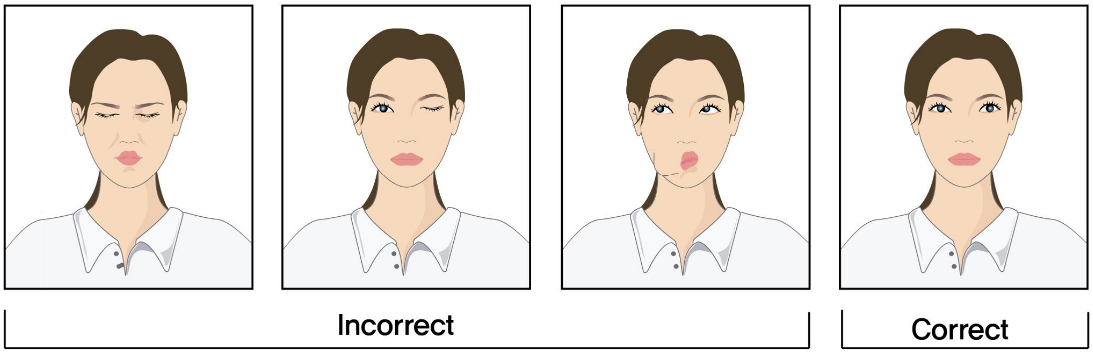
The Process

1. Face is a well-structured object consisting of lots of facial features. The inherent structure and facial features robust to some variations characterize an individual. Face recognition employs these unique characteristics.
2. Face sensors create a digital image or the sequence of video frames from a video. Various types of illumination source such as visible light ray or IR can be utilized for sensing a face.
3. The face region is necessarily detected. The process of identifying each face produces face information in that region. This information is stored in terminal’s database and used for authentication.

Face Recognition Method

1. Correctly apply a face to the sensor

- Stare at the face sensor so that the captured face is placed in the center of an image.
- We recommend the frontal face similar to ID picture.
- Locate the face at an appropriate distance from the face sensor so that whole parts of a face is captured in an image.
- Many users change their pose abruptly. Maintain the pose for capturing a face although our solution provides the unique solution to minimize necessary time to capture a face steadily.
- Facial features can be severely distorted by expression changes including smile, cry and wink. Maintain the facial expression for capturing a face. We recommend the normal expression similar to ID picture.



2. Recommendations

- Proper registration is very important for accurate face recognition. So take care to properly input the face in the face registration process.
- Face information can be severely varied for illumination environment. It is recommend that matching process take place under the same illumination as registration process.

Chapter 2. Installation

Chapter 2. Installation

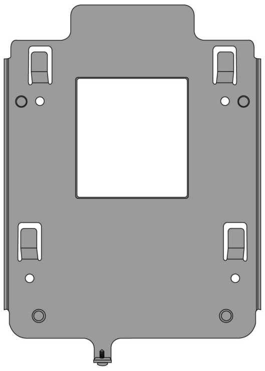
2.1 Package Contents

Check the product package contains the following items. If any of the following items is damaged or missing, contact your retailer.

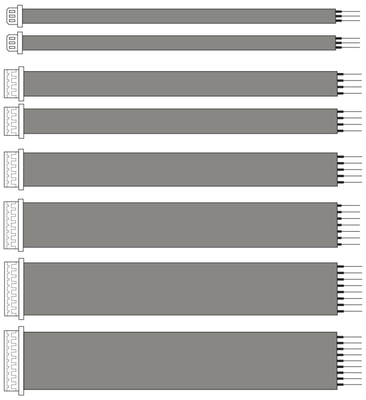
Basic Contents

F1
F2
F3
F4
CALL
suprema

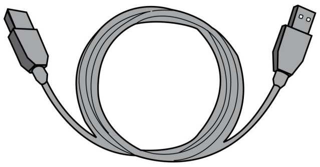
D-Station terminal



Bracket



Cables (8)

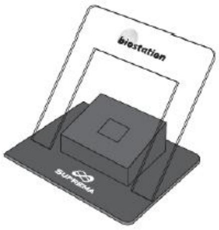


USB cable

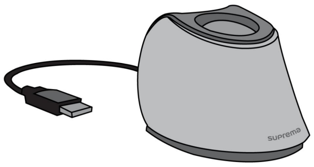
Screws and holders (4 each)

Software CD

Optional Accessories

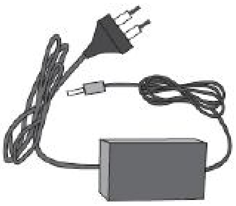


Plastic stand



USB fingerprint scanner

Wireless LAN access point

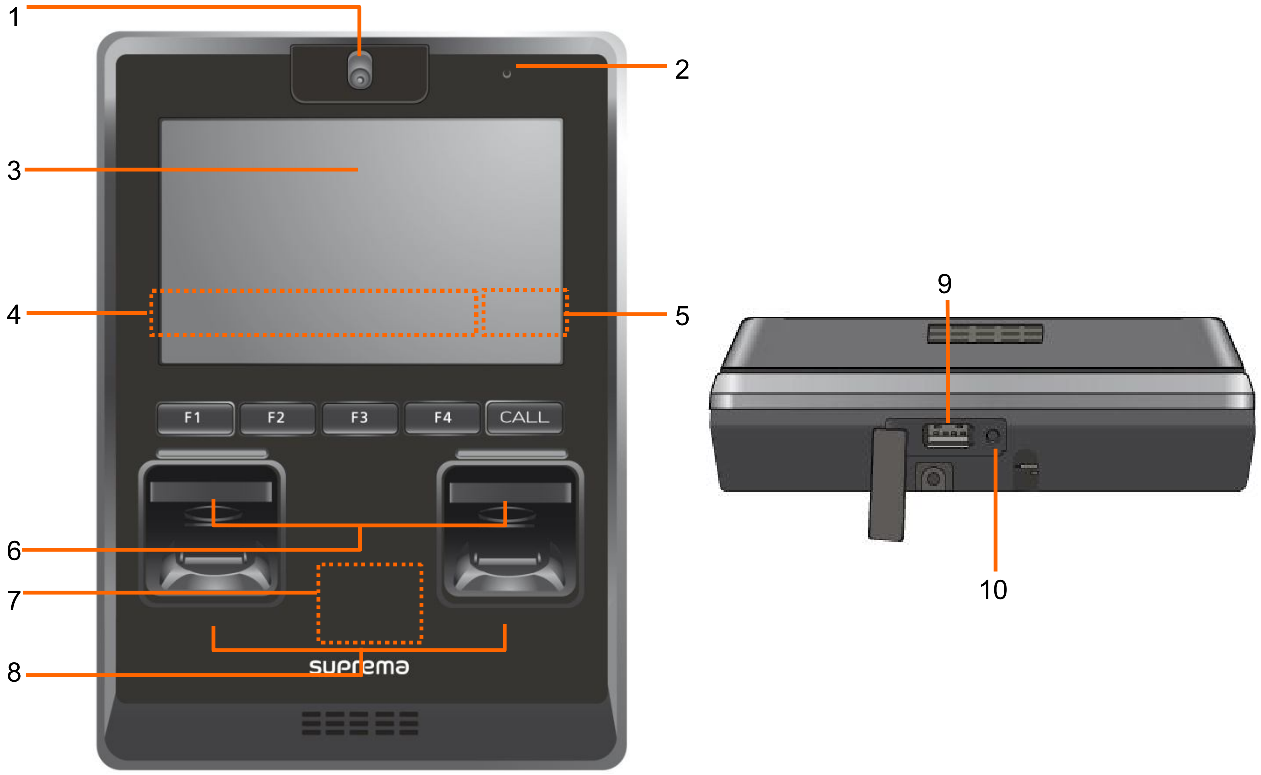


12 V adaptor

2.2 Product Parts Description

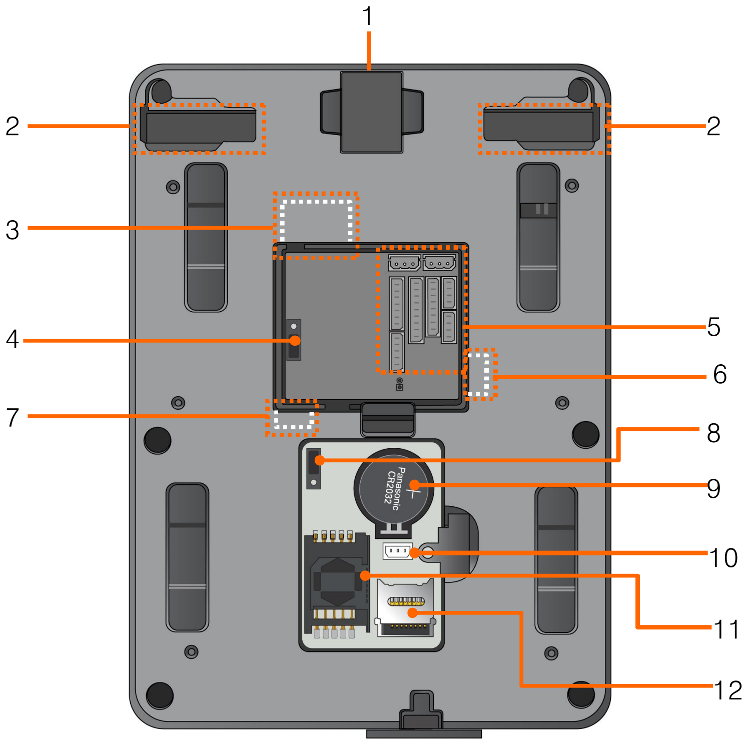
Front / Bottom

The following shows the name and function of the D-Station parts.



No.	Name	Function	No.	Name	Function
1	Camera	Allows face recognition or video calling.	6	LED Indicator	Power on: Blue LED on Awaiting fingerprint input: Blue LED flashes
2	Microphone	Provides audio for video calling.	7	RF card reading part	Reads RF card.
3	LCD screen	Displays current status (time and attendance, notices, etc.) and the time.	8	Fingerprint sensor	Inputs fingerprint from finger placed here.
4	Function Keys	Uses function keys as the time and attendance event keys.	9	USB Port	Connect a flash drive or a USB cable to a PC.
5	Call Key	Makes a call when the video phone is on.	10	Reset button	Restarts the terminal.

Rear

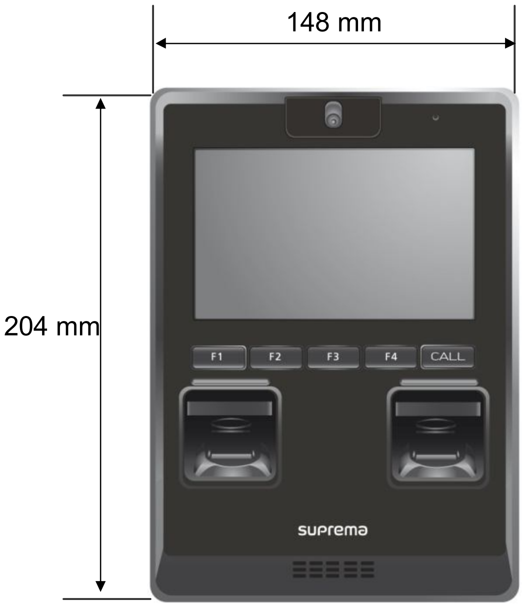


No.	Name	Function
1	Camera adjustment lever	Adjusts the camera.
2	USB port	Connects USB WLAN.
3	Ethernet cable terminal (RJ 45)	Connects Ethernet cables.
4	Power supply selection jumper	- POE IN: POE (Power Over Ethernet) using UTP cable - DC IN: uses a power adaptor (The default setting is DC IN)
5	Cable ports	Connects cables. Refer to 2.2. Cable Specifications
6	SW3	Selection switch for RS485 termination.

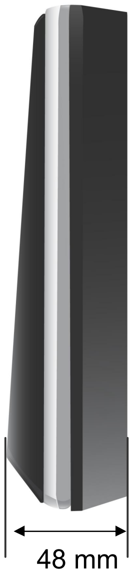
No.	Name	Function
7	Power supply port	Connects 12 V power adaptor.
8	Booting mode selection jumper	Selects between NORMAL or ADMIN MODE. Because Admin mode is used for maintenance, you must set it 'normal' for operation.(The default setting is NORMAL mode.)
9	RTC Battery	RTC (Real Time Clock) battery. (Battery for clock operation)
10	Debug	Debug port for maintenance
11	SAM	Insert the security application module here.(To be supported)
12	Micro SD	Insert Micro SD memory card. (To be supported)

2.3 Dimensions

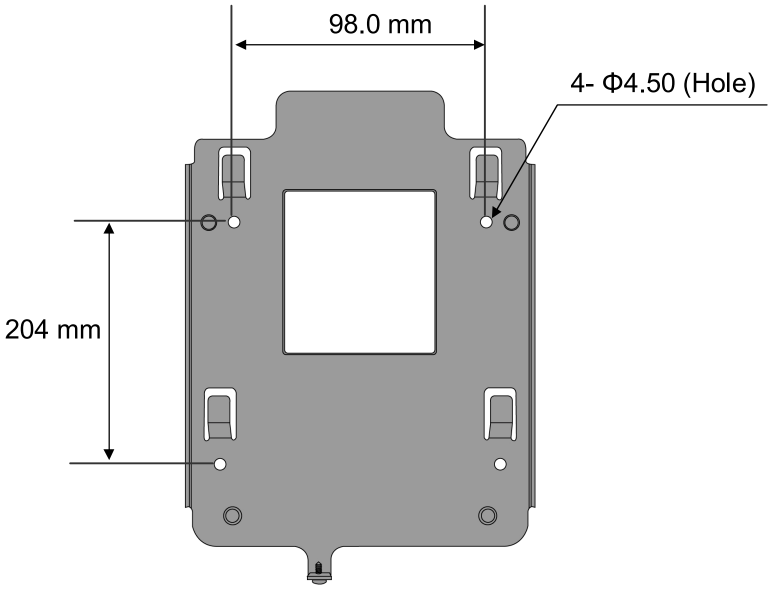
- Product dimension: 148mm(W) x 204mm(H) x 48mm(D)



[Front View]



[Side View]



[Bracket]

2.4 Installation of Wall Mount Bracket

Installation procedures of wall mount bracket are as follows:

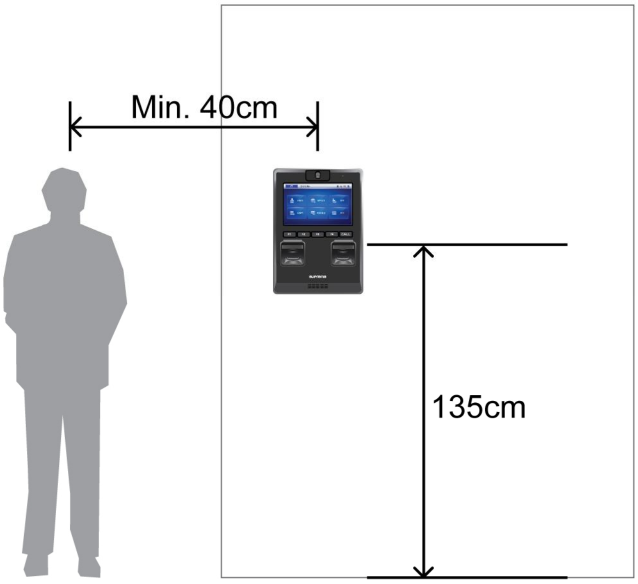
1) Planning the installation position of D-Station
2) Adjusting the camera angle
3) Fixing the wall mount bracket

Planning the installation position of D-Station

Because D-Station is product for face recognition, you must consider the installation height and camera angle before installation of wall mount bracket

You can decide the installation position of product considering to the face recognition and fingerprint input.

Optimum installation height is 135cm, minimum distance between person and product is 40cm.

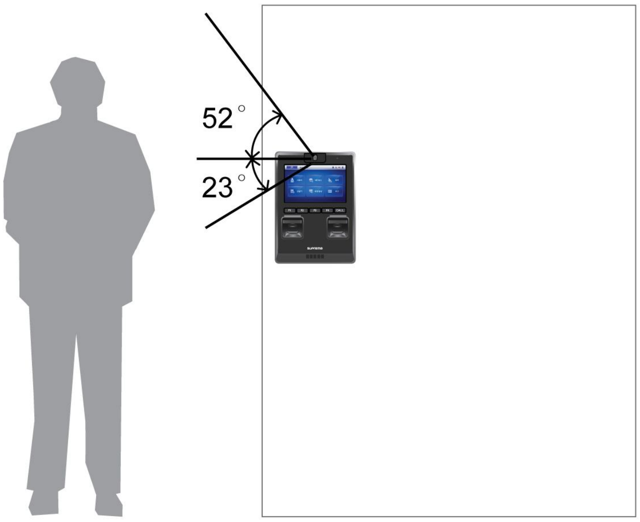


Chapter 2. Installation

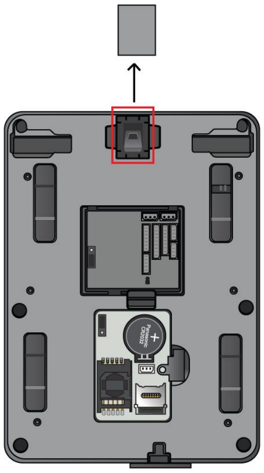
Adjusting the camera angle

Adjustment lever of camera angle is located in product's rear side, you must adjust camera angle before fixing the wall mount bracket.

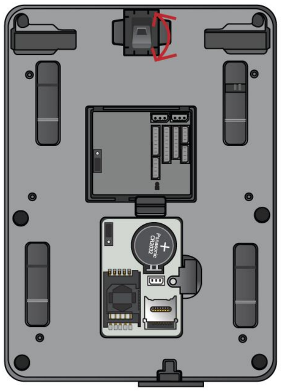
1. You can decide the installation position considering to face recognition. You can adjust the camera angle only up/down direction based on product's front view, 52degree(max. angle) to up direction and 23degree(min. angle).



2. Detached the rubber cap of camera's angle adjustment lever.

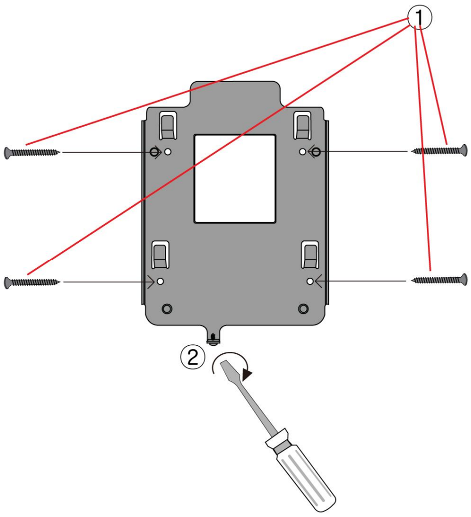


3. Adjusts the camera's angle adjustment lever to face is located in camera's center for face recognition.



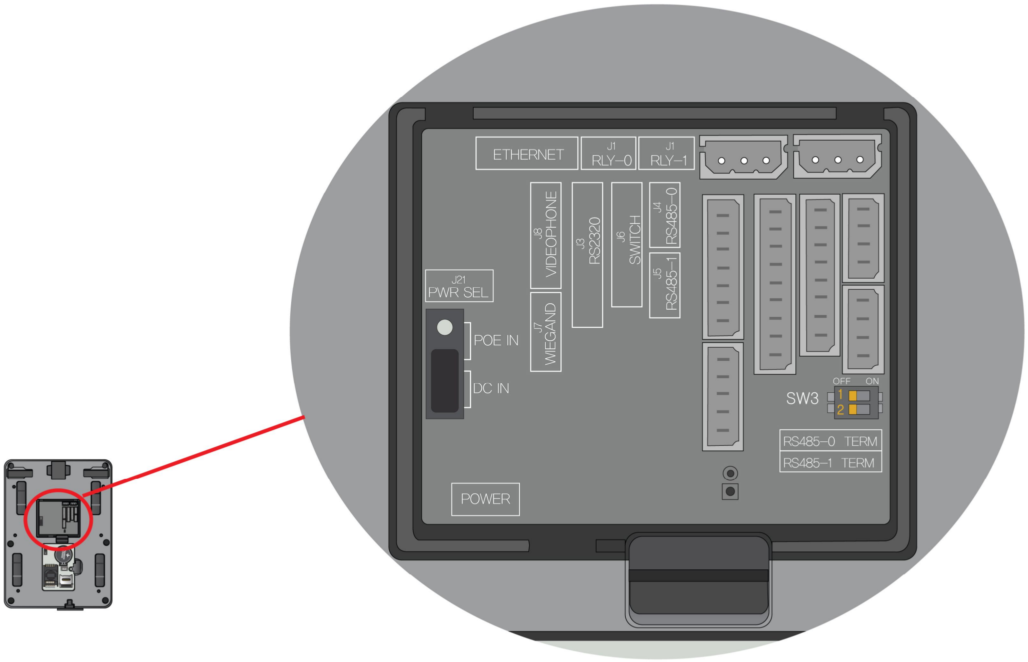
Fixing the wall mount bracket

First, adjusts the wall mount bracket using the four screws as following figure. Locates the product on wall mount bracket, adjusts the product using screw in the bottom of wall mount bracket.



2.5 Connector connection part

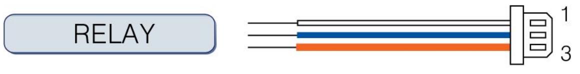
There is the connector connection part in product rear side as following figure:



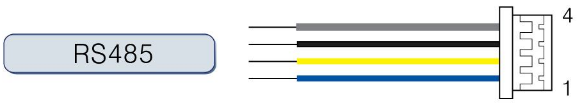
Note

- ■ RS485-0(J4) to be used for connection between PC and a device
  >> PC Only
- ■ RS485-1(J5) to be used for connection between devices
  >> Device Type: Secure I/O, BST, BEPL, BLN, Xpass, DST, XST

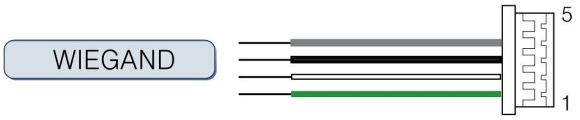
2.6 Cable Specifications



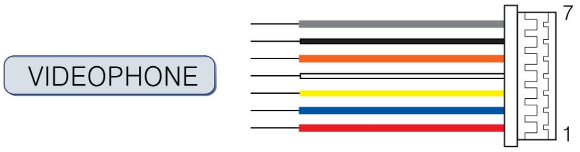
PIN	PIN DESCRIPTION	WIRE
1	Relay Normal Open	WHITE
2	Relay Common	BLUE
3	Relay Normal Close	ORANGE



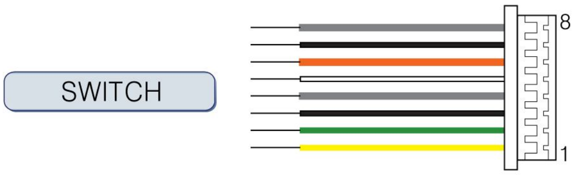
PIN	PIN DESCRIPTION	WIRE
1	485 TRX+	BLUE
2	485 TRX-	YELLOW
3	GND	BLACK
4	SHIELD GND	GRAY



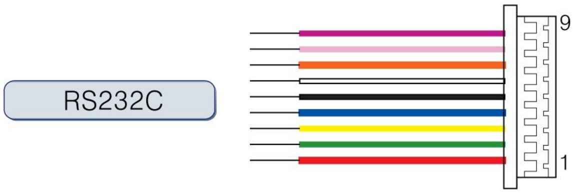
PIN	PIN DESCRIPTION	WIRE
1	DATA0	GREEN
2	DATA1	WHITE
3	GND	BLACK
4	SHIELD GND	GRAY
5	-	



PIN	PIN DESCRIPTION	WIRE
1	VOICE SIGNAL	RED
2	GND	BLUE
3	POWER	YELLOW
4	VIDEO SIGNAL	WHITE
5	DOOR OPEN SIGNAL	ORANGE
6	GND	BLACK
7	SHIELD GND	GRAY

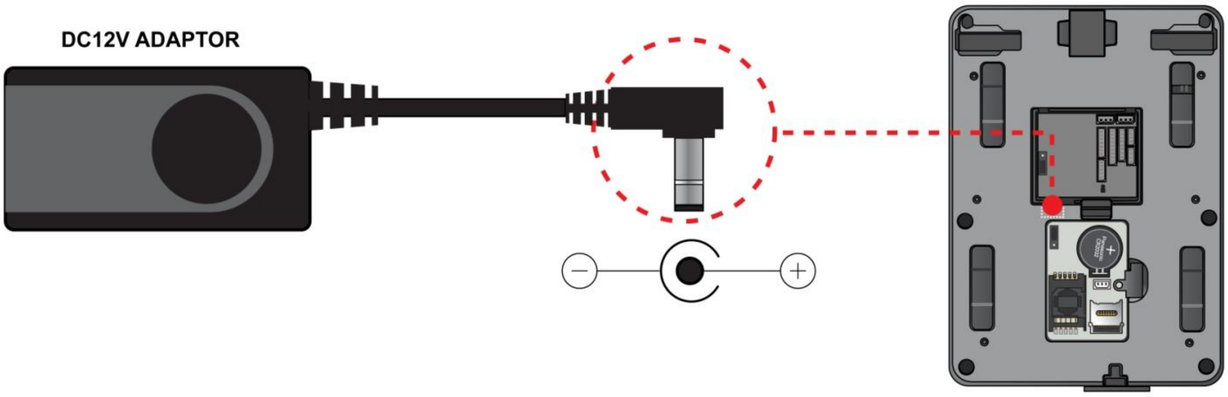


PIN	PIN DESCRIPTION	WIRE
1	SWITCH INPUT0	YELLOW
2	SWITCH INPUT1	GREEN
3	SWITCH GND	BLACK
4	SHIELD GND	GRAY
5	SWITCH INPUT2	WHITE
6	SWITCH INPUT3	ORANGE
7	SWITCH GND	BLACK
8	SHIELD GND	GRAY



PIN	PIN DESCRIPTION	WIRE
1	232 DCD	RED
2	232 RXD	GREEN
3	232 TXD	YELLOW
4	232 DTR	BLUE
5	232 GND	BLACK
6	232 DSR	WHITE
7	232 RTS	ORANGE
8	232 CTS	PINK
9	232 RI	PURPLE

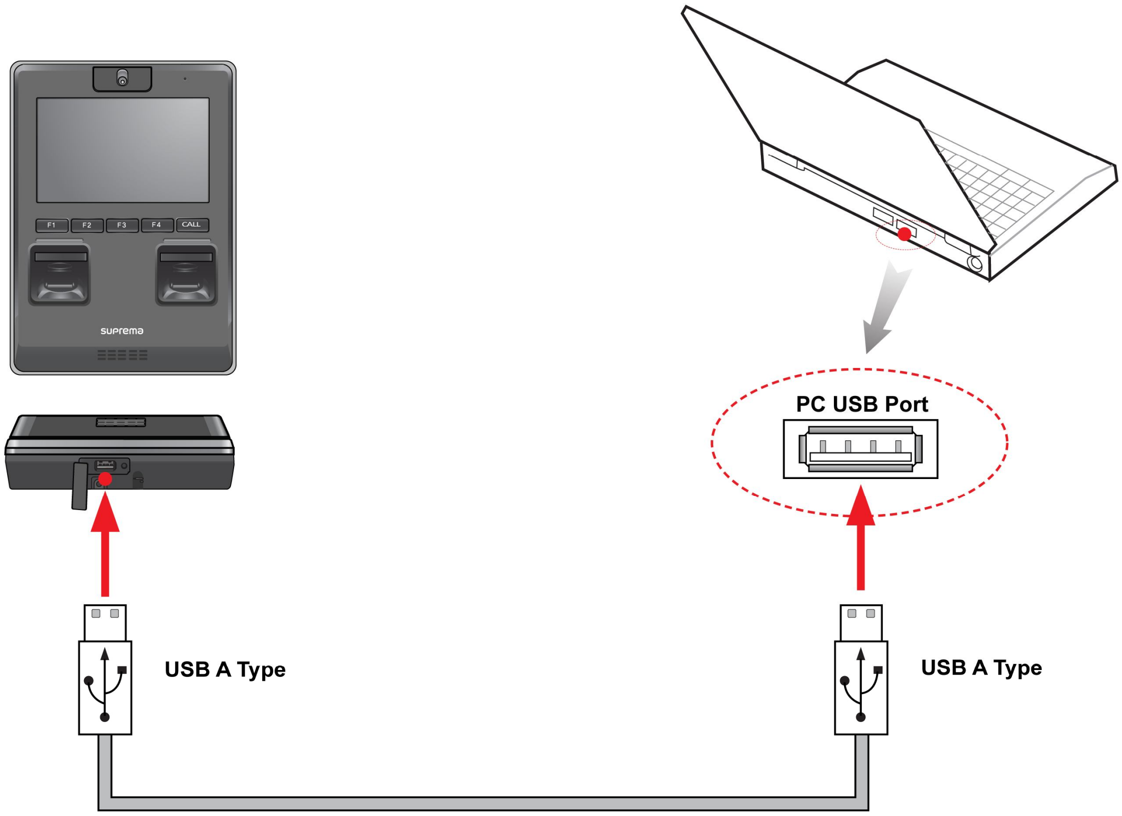
1) Power Supply



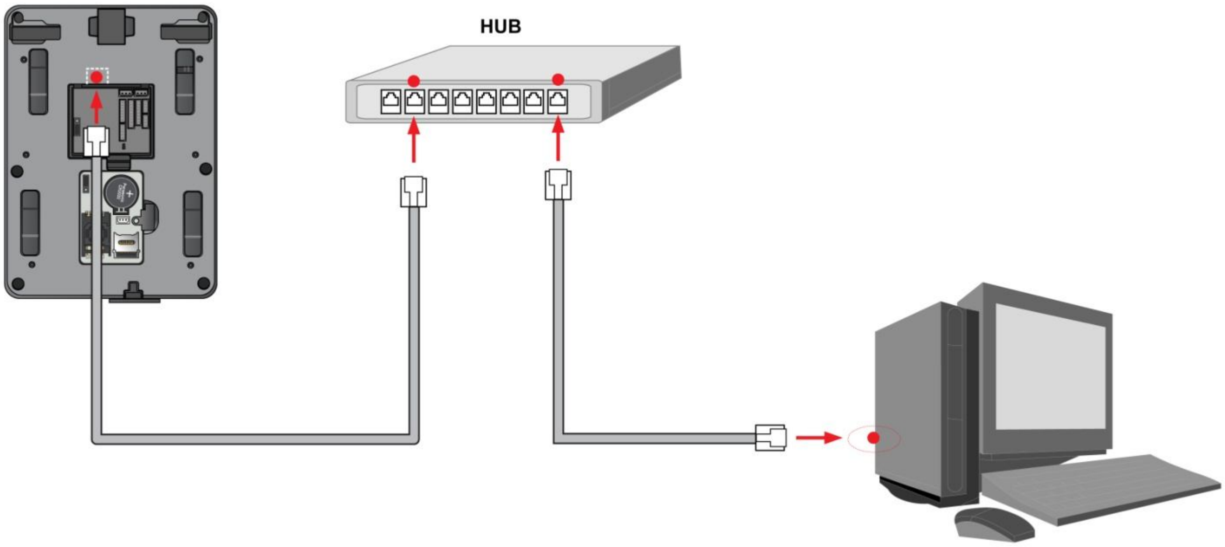
Recommended Power Supply

- DC 12 V adaptor: 12 V ± 10%, 1500 mA or above, IEC / EN 60950-1 compliance
- When sharing power supply with other appliances, we recommend you use adaptors of more than 1500 mA.

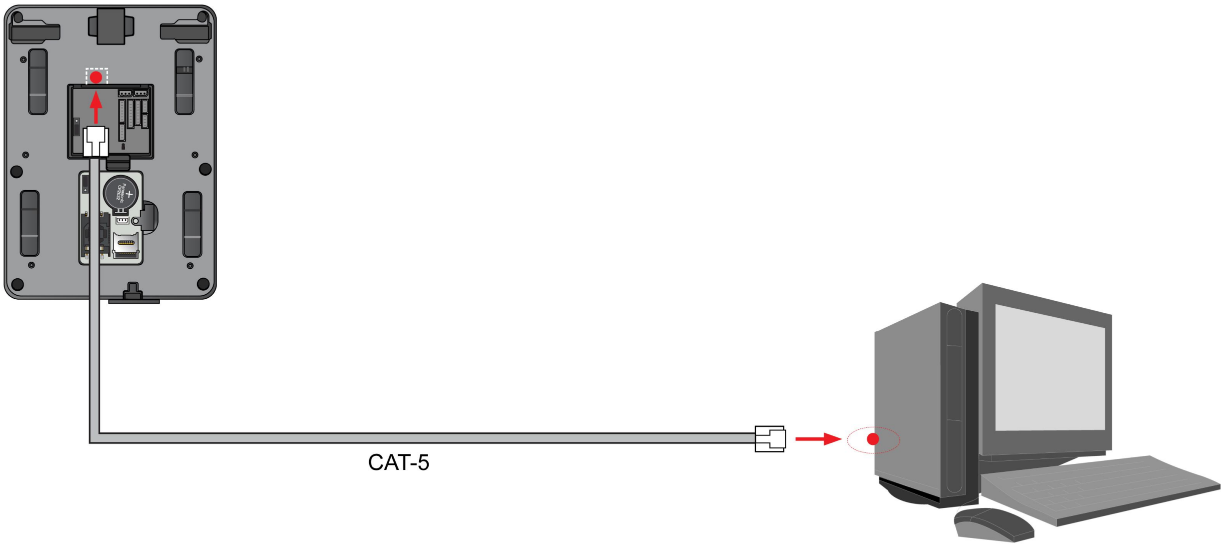
2) USB Cable Connection



3) LAN Connection

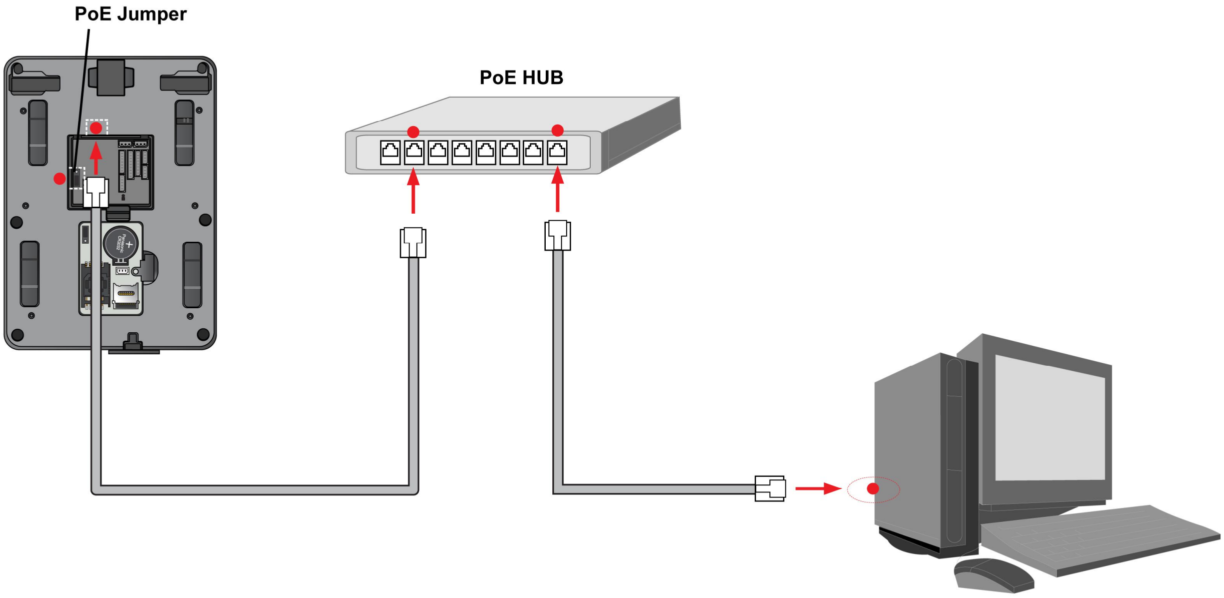


4) LAN Connection (Direct connection with PC)



5) PoE Hub Connection

PoE(Power over Ethernet) is used to connect Ethernet by PSE(Power sourcing Equipment) complies with IEEE802.3 standard.

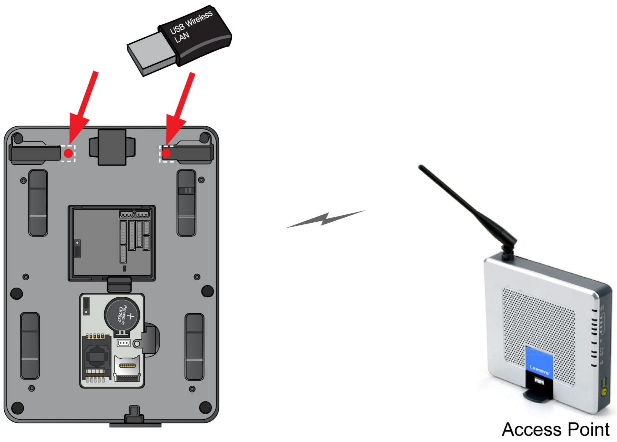


- Please use the distance of LAN cable within 100m in case of POE power.
- PoE Jumper : Sets the jumper of PWR SEL as ‘POE IN’ in the product’s rear side.

6) Wireless LAN Connection(Wireless Version Only)

The performance of wireless LAN is influenced by the surrounding environment and the access point. You must insert the USB Wireless LAN module using only the products of our company. You can select the port position from among right and left side port, according to installation conditions.

The access points compatible with D-Station are as follows:



Access points compatible with D-Station:

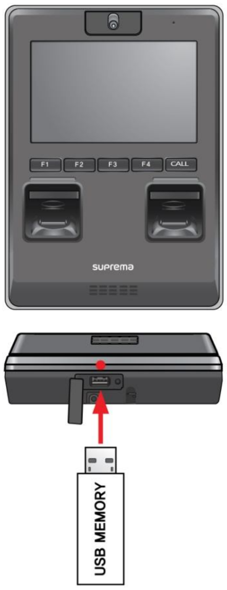
- Buffalo WHR-HP-G54
- IP Time G104

(Using other access points may cause the wireless LAN to function incorrectly.)

7) USB Memory Connection

Some USB flash drives may not connect to the product because of hardware compatibility. You can download or upload the user information and log data using the USB memory.

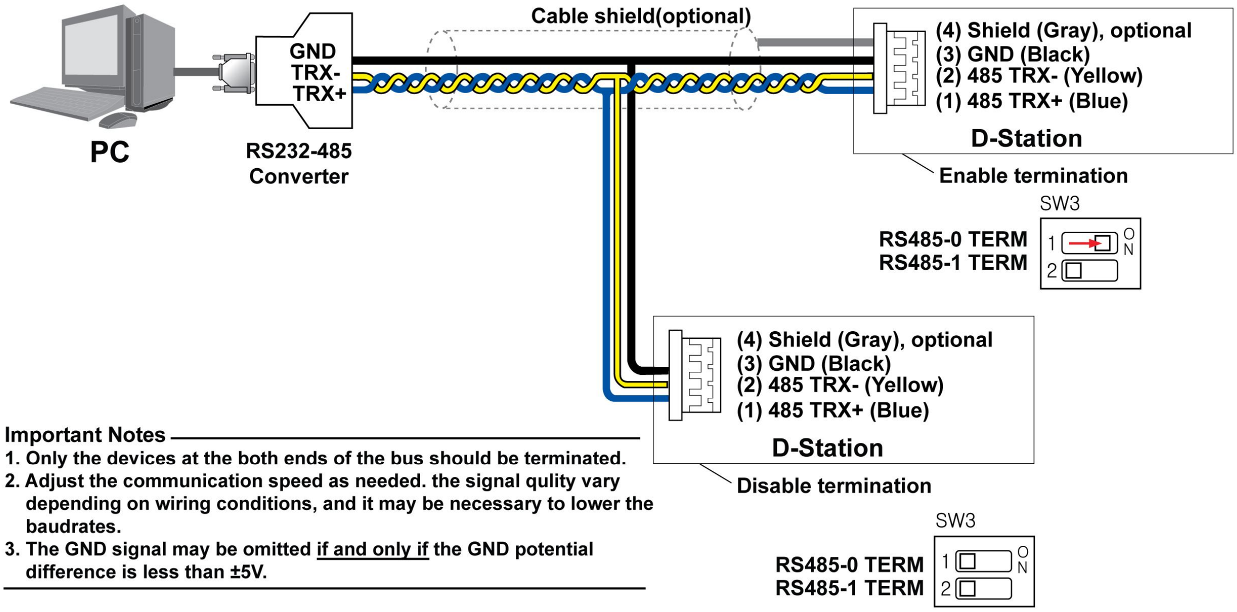
The following is a list of USB flash drives that are verified to work properly on D-Station.



USB memory drives compatible with D-Station:

- [IMATION] Flash Drive Nano 4GB
- [LG Elecronics] X TICK M4 4GB
- [LG Electronics] X TICK MOBY J1 2GB
- [PQI] Traveling Disk U173 4GB
- [SAMSUNG C&T] PLEOMAX PUB-S100 4GB
- [SAMSUNG Electronics] SUB-4G MLC 4GB
- [SAMSUNG Electronics] SUM-M2GSD (2GB)
- [SONY] MicroVault Slide USM4GJ 4GB

8) RS485 Network Connection



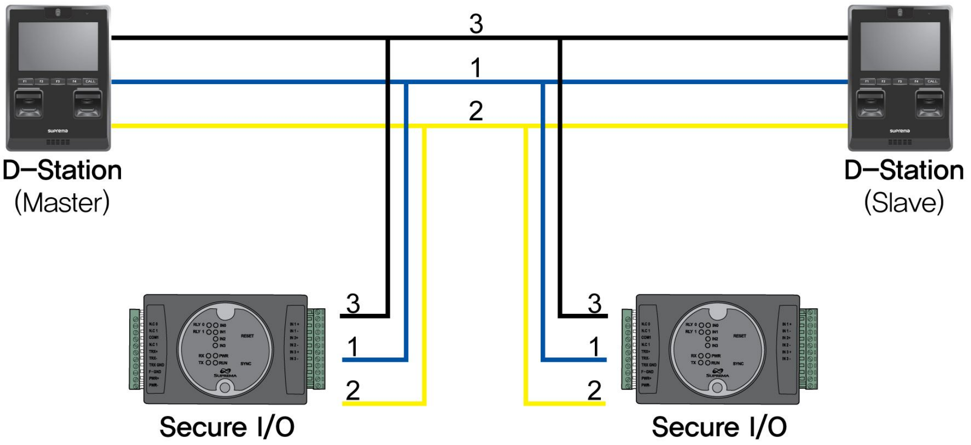
Important Notes

1. Only the devices at the both ends of the bus should be terminated.
2. Adjust the communication speed as needed. the signal qulity vary depending on wiring conditions, and it may be necessary to lower the baudrates.
3. The GND signal may be omitted if and only if the GND potential difference is less than ±5V.

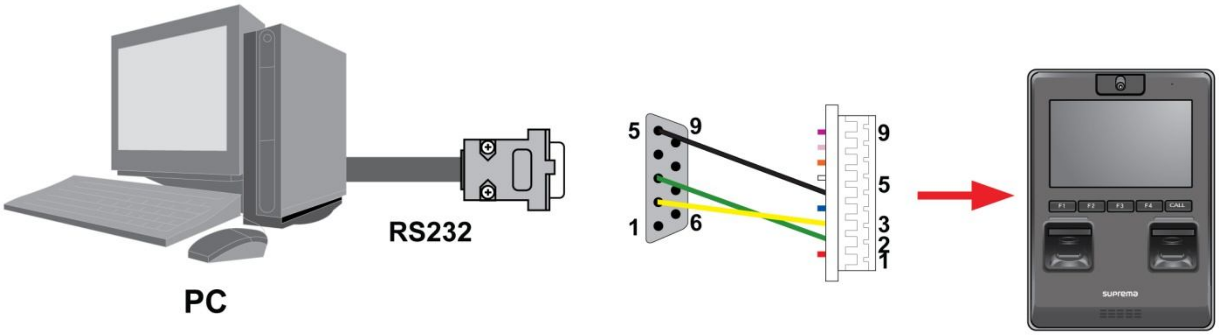
SW3(Selection switch for RS 485 termination): If it is long for the wire length between source and destination, signal decrease may be occurred. Then dip switch is set 'ON'(e.g. Pull up the RS485 termination resistance), signal is sent normally. Inversely, if it is short for the wire length between source and destination, signal is not sent when the RS485 termination resistance is pulled up. Therefore, you must consider wire length and signal quality, whether pull up the RS485 termination resistance or not.

9) RS485 Connection for Secure I/O

PIN	PIN DESCRIPTION	COLOR
1	485 TRX+ ↵	BLUE
2	485 TRX– ↵	YELLOW
3	GND	BLACK

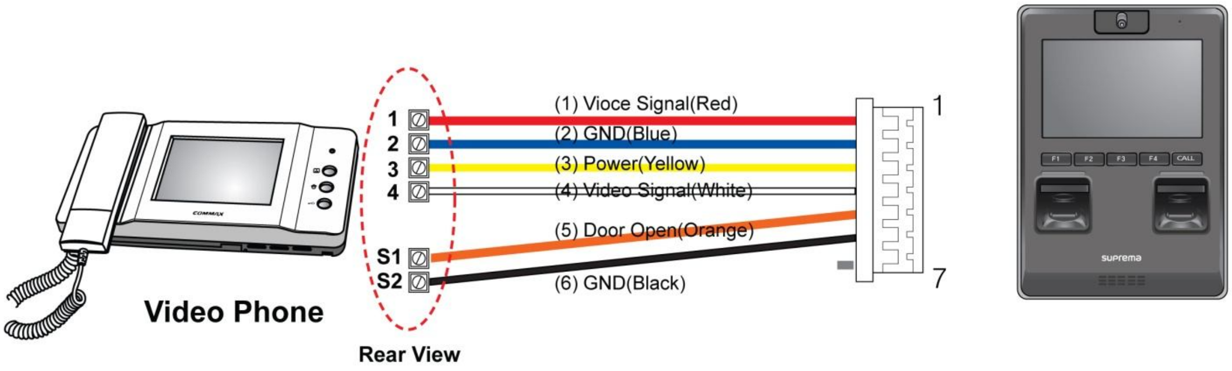


10) RS232 Connection



- D-Station is supported the serial printer or wireless modem connection.

11) Videophone Connection

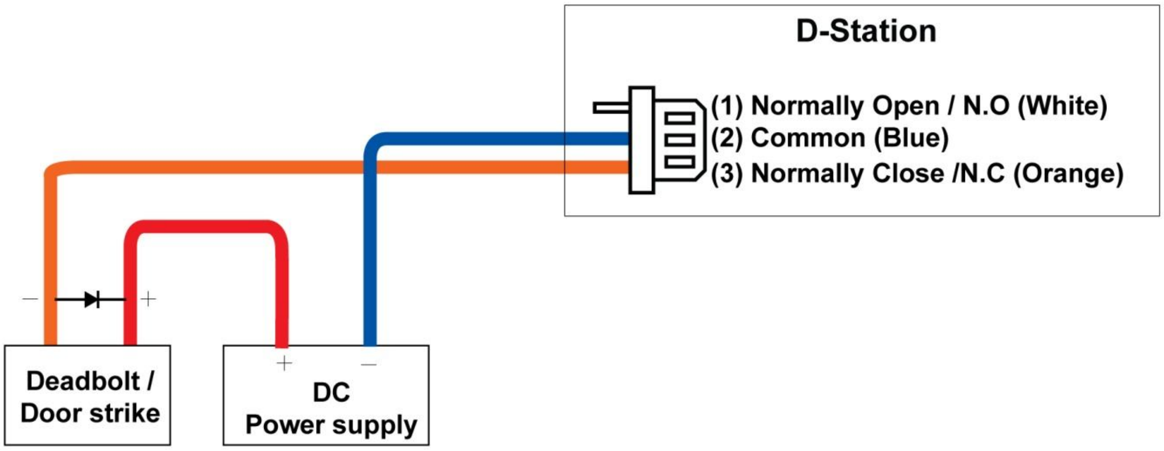


Videophone models compatible with D-Station:

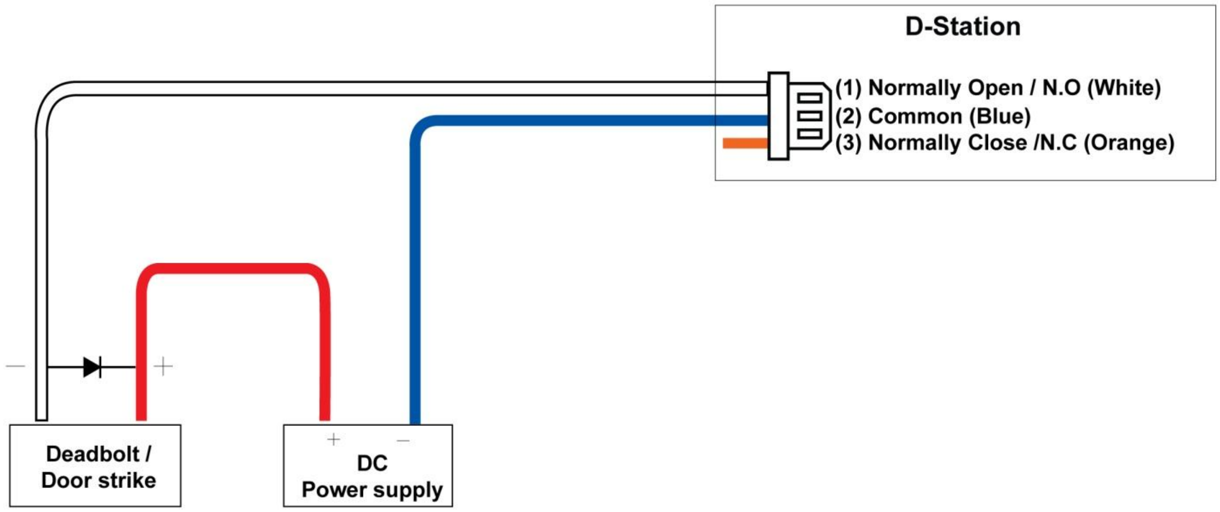
- COMMAX / CAV-35N
- COMMAX / CAV-50H
- COMMAX / CAV-50P

(To purchase the videophone, please contact supremaic’s dealer or headquarter.)

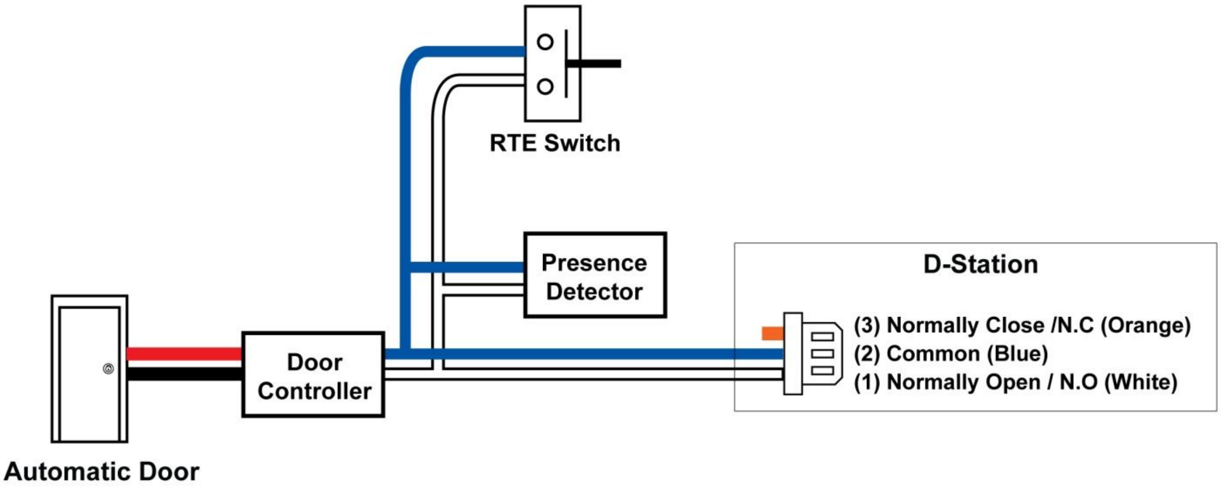
12) Relay Connection – Fail-Safe Lock



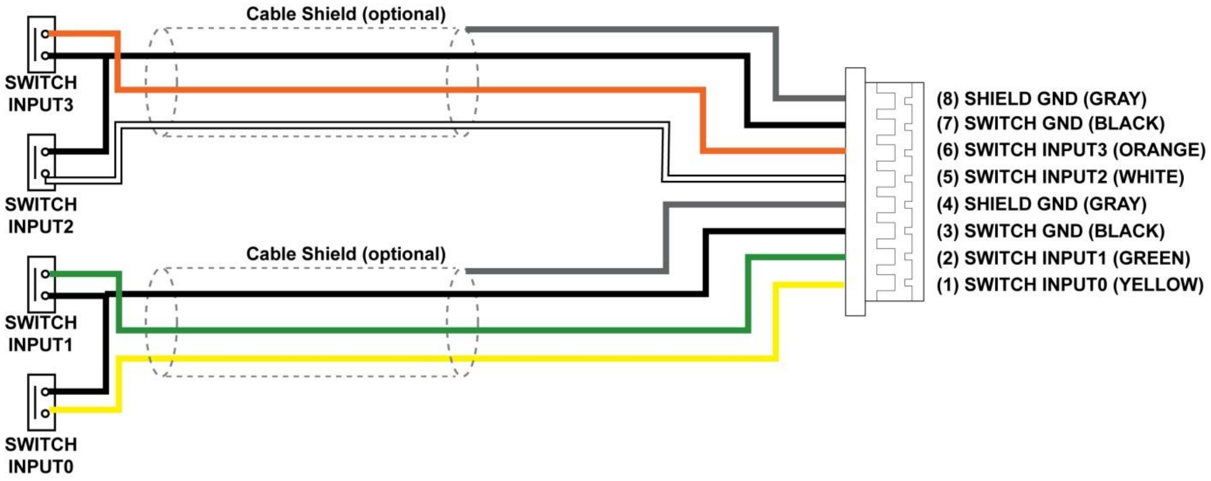
13) Relay Connection – Fail-Secure Lock



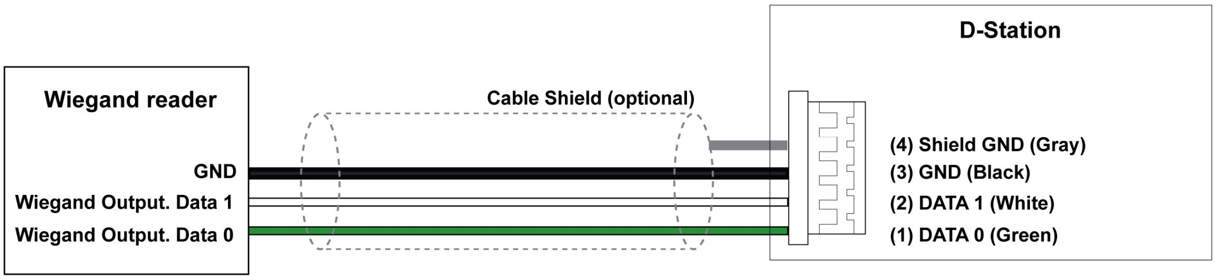
14) Relay Connection – Automatic Door



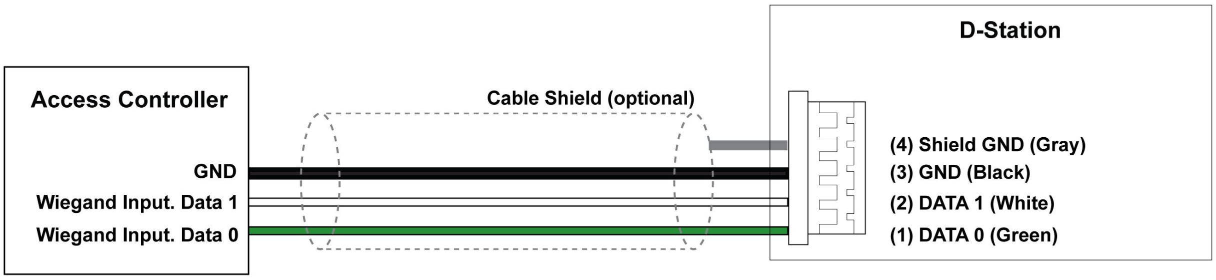
15) Switch Input Connection – for RTE, door sensor and alarm inputs



16) Wiegand Input Connection – When Using a Separate Wiegand Reader

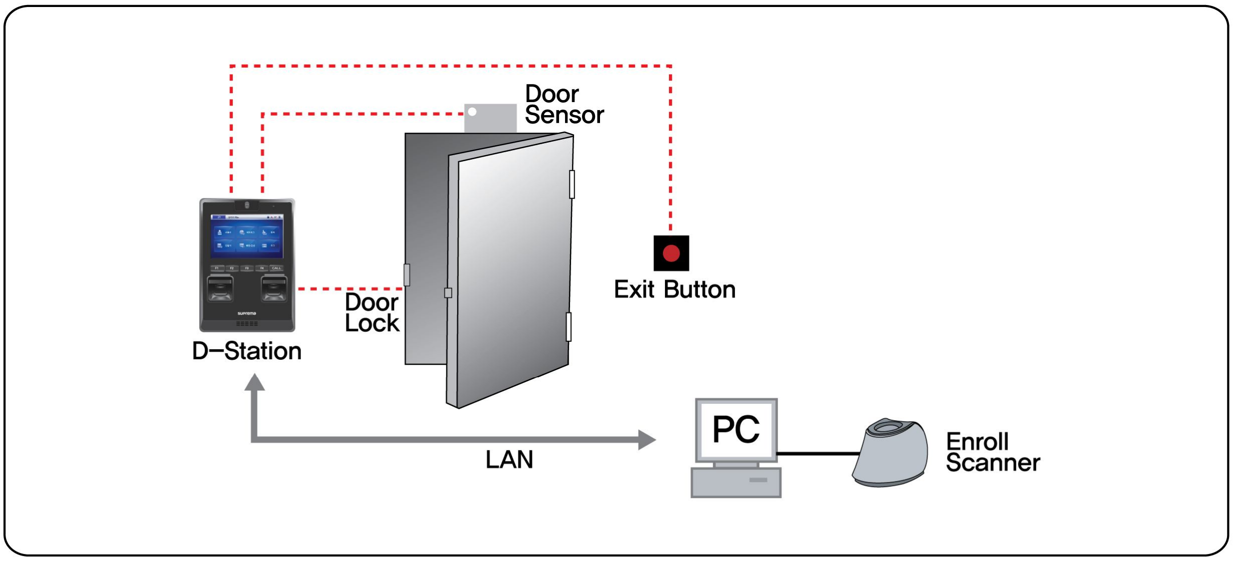


17) Wiegand Output Connection – When Using a Separate Access Controller

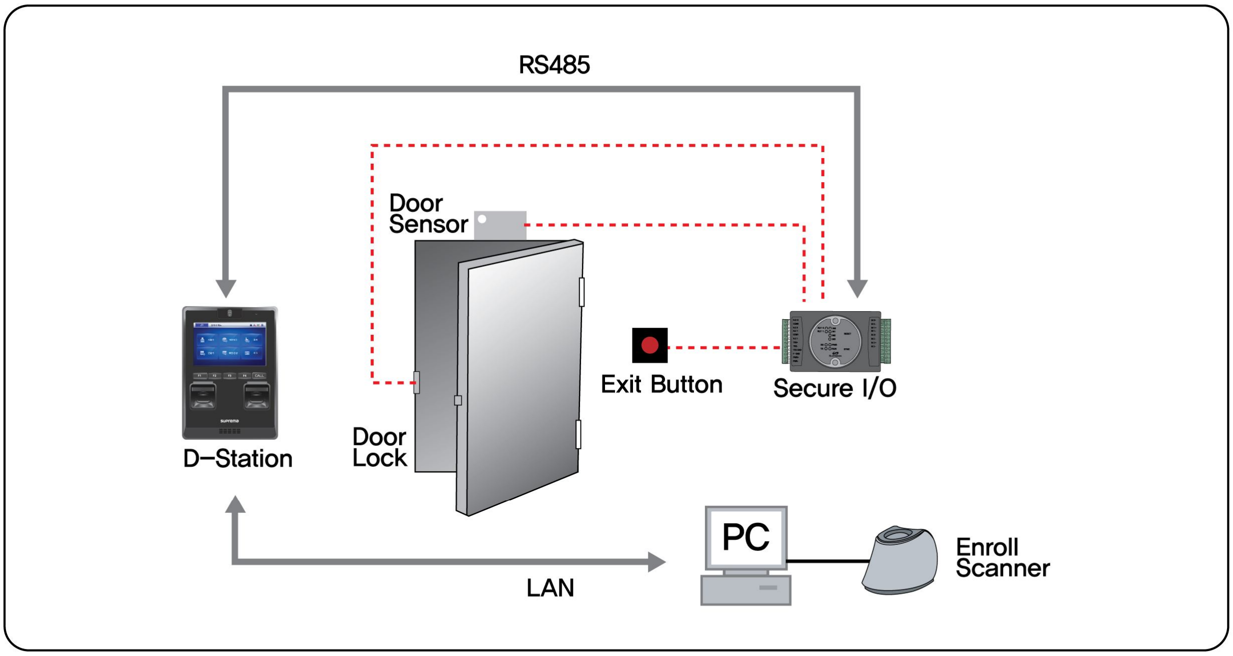


2.7 System Configurations

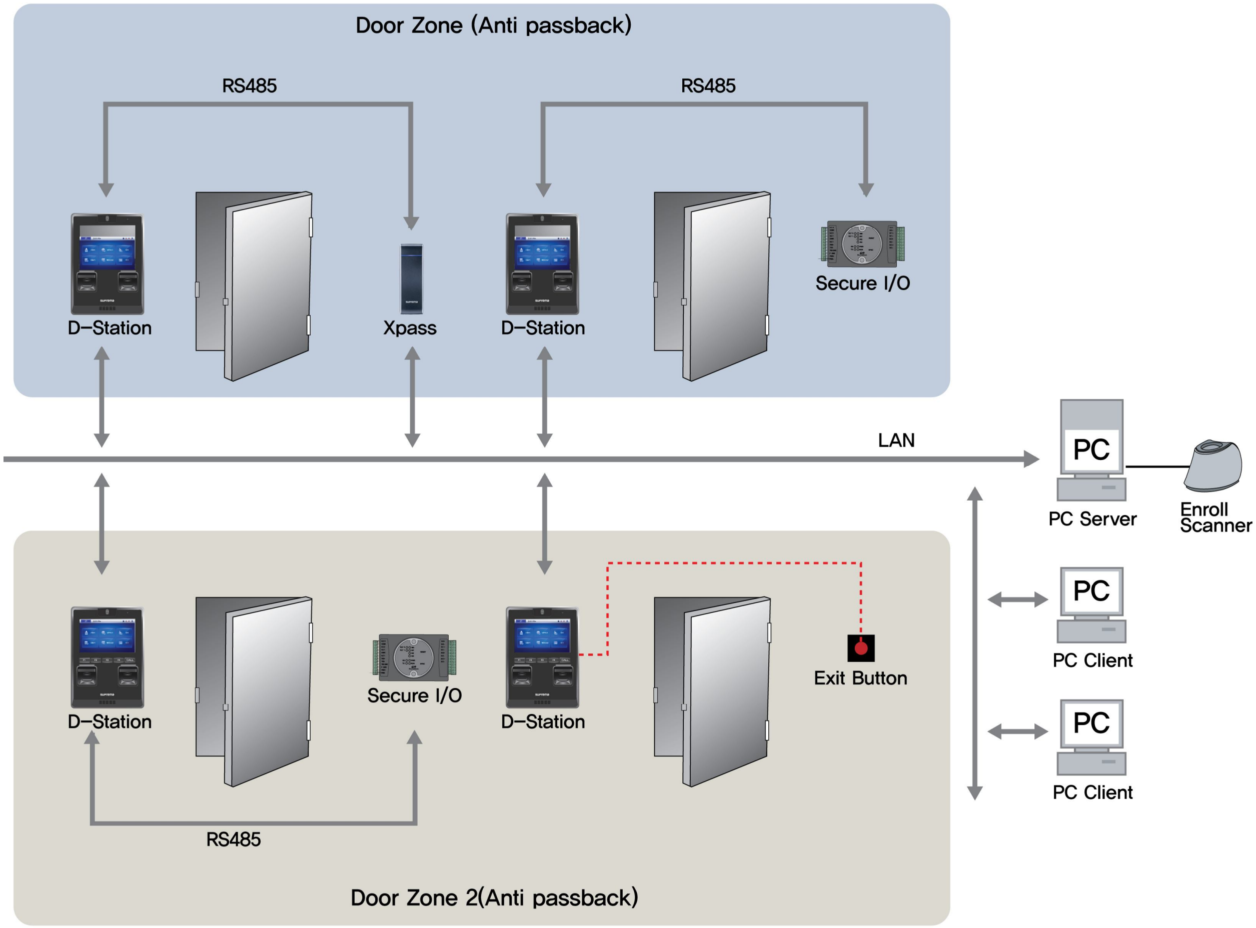
■ Standalone



■ Standalone (Secure)



Network Installation (TCP / IP or RS485)

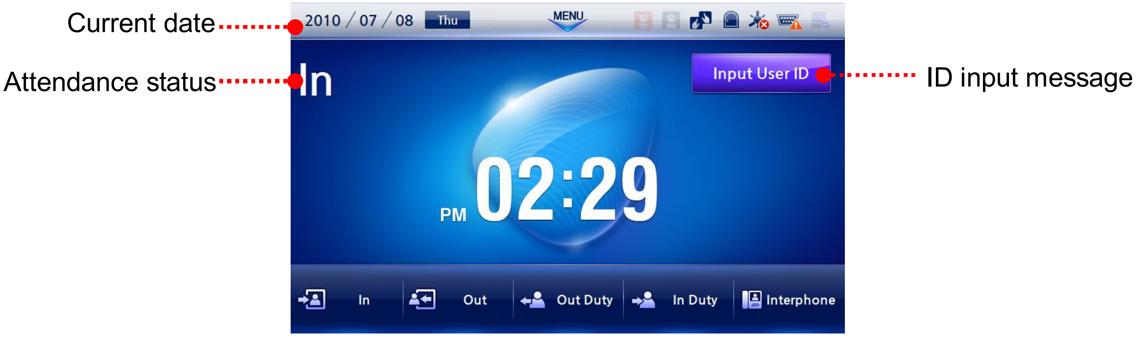


Chapter 3. Admin Menu

Chapter 3. Admin Menu

3.1 Start-up Screen

Start-up Screen Menu



Key / Icon	Function
Current date	Displays the day and date.
Attendance	Displays the current attendance event.
In	Press on arrival.
Out	Press on leaving.
In Duty	Press on returning .
Out Duty	Press on leaving (temporarily).
Interphone	Press to use the videophone.
Input User ID	Input ID for authentication.

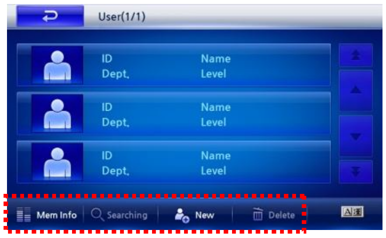
Key / Icon	Function
	Detect Face function is on.
	Face Fusion function is on. (Fusion mode)
	Fingerprint Recognition Mode FAST Fast mode Fusion mode TWIN Twin mode
	Door opening and closing
	Ethernet connection
	RS485 connection
	Connection to PC
MENU	Opens Admin menu.

Administrator Registration

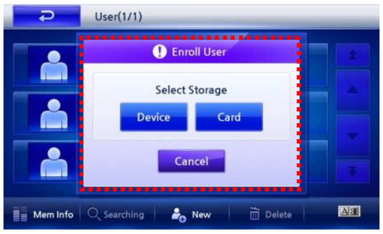
There is no registered user immediately after purchasing the product. Please register the administrator right after installation.

The administrator registration process is as follows:

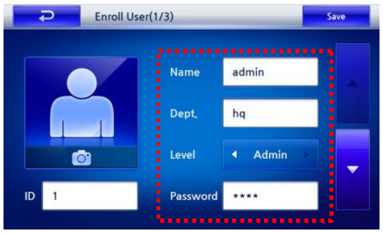
1. Open [Admin Menu] ▸ [User] ▸ [User Management]
   - Searching: Searches for user information.
   - New: Registers user
   - Delete: Deletes user information



2. For new user registration, select [Device] or [Card]

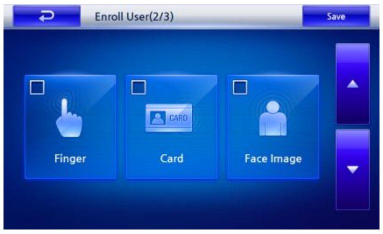


3. Input Name, Dept., Level and Password, and press [▾].
   - Select Admin for Level
   - Input Password twice with the number keys.

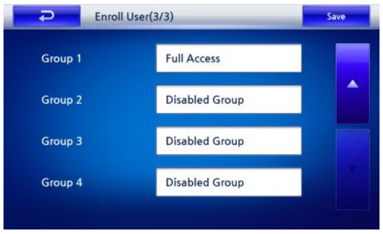


Name: admin
Dept.: hq
Level: Admin
Password: ****
ID: 1

4. Select among Finger, Card and Face Image, and input the administrator’s corresponding information. There is no requirement for the number of information options you use, nor necessary order in which to register Finger, Card and Face Image. You can register only the information option you want.



5. Press [▾] and select user group. User group selection is optional and you can use this function when you want to divide users into different groups and manage them accordingly.
   - Set values: Disabled Group / No Access / Full Access



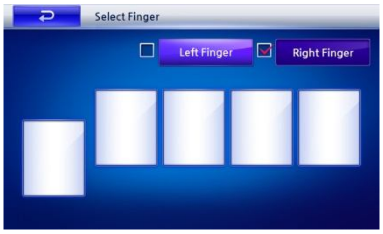
Group 1: Full Access
Group 2: Disabled Group
Group 3: Disabled Group
Group 4: Disabled Group

Chapter 3. Admin Menu

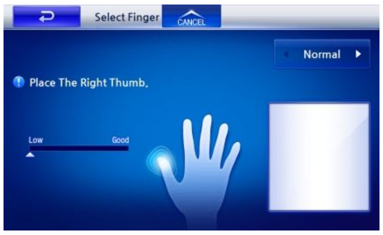
Fingerprint Registration

We recommend you register at least two fingerprints for every ID. Users experiencing repeated failure in fingerprint recognition may improve the recognition performance by registering the same fingerprint several times.

Select the hand and finger to register.



Input the fingerprint. (You can choose between a normal and duress finger.)

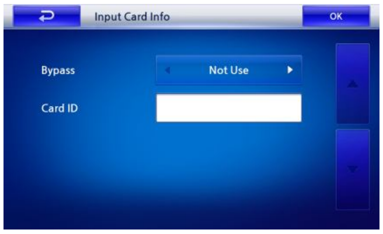


Place The Right Thumb.

- Normal finger: Registers the fingerprint information to be used for access or basic authentication purposes.
- Duress finger: Is useful for dangerous situations such as being threatened by a thief. By registering a duress finger, you can set the terminal to trigger an alarm or emergency call configured as an output port. The door opens normally. A duress finger must be different to the one used for the normal finger.

Card Registration

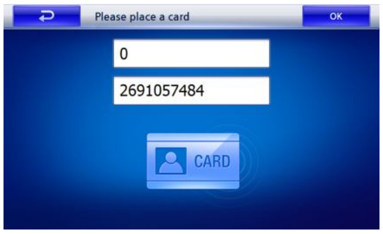
Select whether or not to use Bypass, and then enter the card ID



Bypass: Not Use

Card ID

Place the card against the screen, and then press [OK].



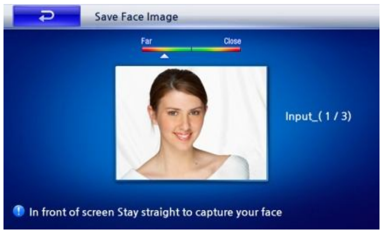
0

2691057484

- The terminal reads the Custom ID and Card ID from an ID card and automatically fills in the corresponding ID fields. (Above: Custom ID, Below: Card ID)

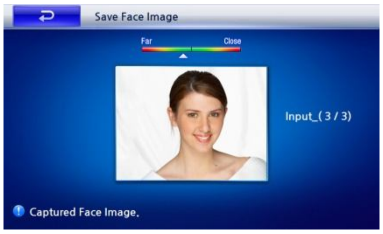
Face Image Registration

Register the face image.



In front of screen Stay straight to capture your face

Input the image three consecutive times.



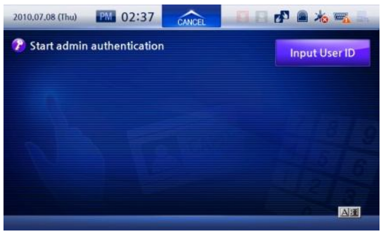
Captured Face Image.

Chapter 3. Admin Menu

Opening the Admin Menu

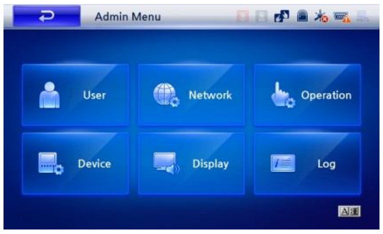
Admin configures User, Network, Operation, Device, Display and Log settings.

1. Press [Admin Menu], and the Admin authentication screen appears. Then get the administrator’s registered card or recognized fingerprint. Admin Menu screen appears after authentication.



2. The Admin Menu start-up screen is shown on the right. You can select the menu and set the configuration.

- User: Register or delete user information, or initialize the DB.
- Network: Set TCP / IP / server configuration and determine whether or not to use USB.
- Operation: Select between time and attendance mode and authentication mode.
- Device: Configure fingerprint authentication, the door and the time displayed on the terminal.
- Display: Select wallpapers and the screen theme, configure LCD lights, and adjust the volume of the automated voice.
- Log: Check access / operation log information.

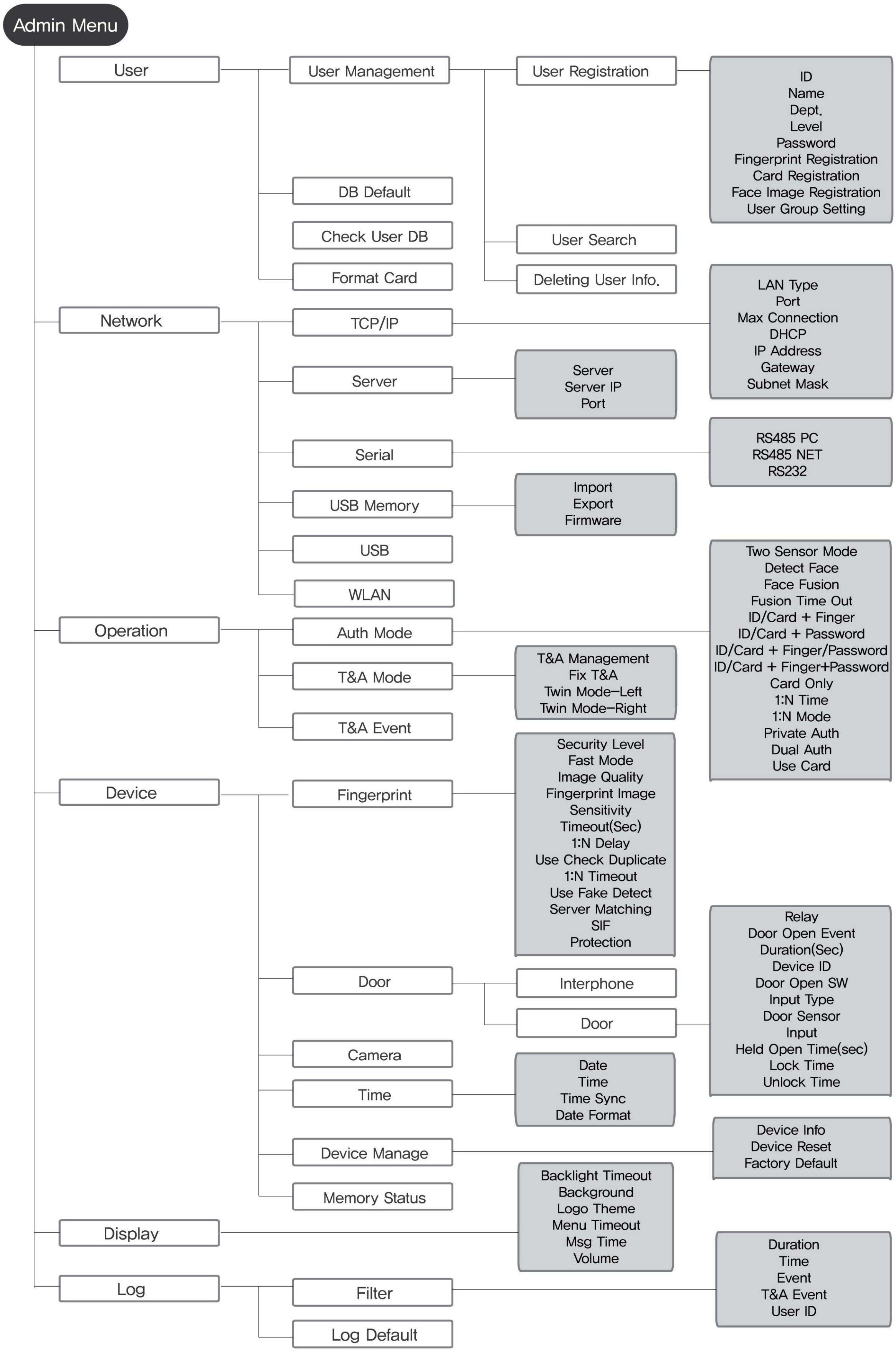


Note

■ Press ↩ to return the screen to the previous page.
■ Use [▼] / [▲] to go to the sub-menus.
■ Absence of activity for a certain period of time on the Admin Menu automatically returns the screen to the start-up screen for security reasons. If you do not want to use this function, or want to change the standby time, refer to ‘**3.7 Display / Sound Management**’ of the manual.

Chapter 3. Admin Menu

Admin Menu Functions



- Admin Menu
  - User
    - User Management
      - User Registration
        - ID
        - Name
        - Dept.
        - Level
        - Password
        - Fingerprint Registration
        - Card Registration
        - Face Image Registration
        - User Group Setting
      - User Search
      - Deleting User Info.
    - DB Default
    - Check User DB
    - Format Card
  - Network
    - TCP/IP
      - LAN Type
      - Port
      - Max Connection
      - DHCP
      - IP Address
      - Gateway
      - Subnet Mask
    - Server
      - Server
      - Server IP
      - Port
    - Serial
      - RS485 PC
      - RS485 NET
      - RS232
    - USB Memory
      - Import
      - Export
      - Firmware
    - USB
    - WLAN
  - Operation
    - Auth Mode
      - Two Sensor Mode
      - Detect Face
      - Face Fusion
      - Fusion Time Out
      - ID/Card + Finger
      - ID/Card + Password
      - ID/Card + Finger/Password
      - ID/Card + Finger+Password
      - Card Only
      - 1:N Time
      - 1:N Mode
      - Private Auth
      - Dual Auth
      - Use Card
    - T&A Mode
      - T&A Management
      - Fix T&A
      - Twin Mode–Left
      - Twin Mode–Right
    - T&A Event
  - Device
    - Fingerprint
      - Security Level
      - Fast Mode
      - Image Quality
      - Fingerprint Image
      - Sensitivity
      - Timeout(Sec)
      - 1:N Delay
      - Use Check Duplicate
      - 1:N Timeout
      - Use Fake Detect
      - Server Matching
      - SIF
      - Protection
    - Door
      - Interphone
      - Door
        - Relay
        - Door Open Event
        - Duration(Sec)
        - Device ID
        - Door Open SW
        - Input Type
        - Door Sensor
        - Input
        - Held Open Time(sec)
        - Lock Time
        - Unlock Time
    - Camera
    - Time
      - Date
      - Time
      - Time Sync
      - Date Format
    - Device Manage
      - Device Info
      - Device Reset
      - Factory Default
    - Memory Status
  - Display
    - Backlight Timeout
    - Background
    - Logo Theme
    - Menu Timeout
    - Msg Time
    - Volume
  - Log
    - Filter
      - Duration
      - Time
      - Event
      - T&A Event
      - User ID
    - Log Default

Authentication Mode

1:1 Mode

- ID/Card+Finger,
- ID/Card+PIN,
- ID/Card+Finger/PIN,
- ID/Card+Finger+PIN,
- Card Only

  - After entering ID on 1:1 mode, set whether you will use fingerprint, PIN, or either for authentication. In case of card, using card only enables users to access just by placing the card.

1:1 Time

- Set schedules to apply the above 1:1 mode.
- Select “All Time”, “No Time” or a specific schedule set by BioStar program.

1:N Mode

- Setting: Auto / OK / T&A Key / Disabled
- Auto : Fingerprint sensor is always on standby. So, if a finger is placed, identification starts automatically.
- OK / T&A key : After pressing OK key or T&A function key, fingerprint sensor is turned on to scan a fingerprint.
- Disabled : 1:N identification is not used. In order to enhance the security level of your system, you can use 1:1 mode in which users should enter their ID first.

1:N Time

- Set schedules to apply the above 1:N mode.
- Select “All Time”, “No Time” or a specific schedule set by BioStar.

Private Auth

- Use or Not Use for private authentication.

Dual

- Dual Authentication needs consecutive authentications from two different users within 15 seconds for high security.
- If only the first user is authenticated, the device signals authentication success but does not activate a relay.

Two Sensor Mode

Two fingerprint sensors and two CPUs work for user authentication.

Fast Mode	Two CPUs perform simultaneous authentication of one fingerprint input.
Fusion Mode	Authentication process is performed by a fusion algorithm on two fingerprints. This allows simultaneous input of two fingerprints. Using the combination of features from both fingerprints, fusion mode increases the authentication rate for users who have a low authentication rate for each fingerprint and may experience repeated failed authentication with other authentication modes.
Twin Mode	Two sensors perform authentication processes independently. One terminal of D-Station can process two persons simultaneously.
Demo Mode	Demonstration mode for face fusion how to be used. Authentication will succeed nevertheless face recognition is failed, if only finger authentication succeeds. Do not apply this mode to real operation, but only to test and demonstration.

Detect Face

Select whether or not to photograph the face on authentication. After a successful authentication, the user's face image is detected automatically and that image is stored as a log.

Face Fusion

The user's face image is also included in authentication. It increases the authentication rate in users who have low authentication rate with fingerprint recognition.

- The authentication modes which apply the face fusion feature are fast mode and fusion mode. The combinations of fast mode and face fusion, and fusion mode and face fusion are possible.

Fusion Time Out

The time-out against the total required time for a successful fusion authentication when operating in fusion mode.

3.2 User Information Management

User Registration

User registration involves inputting basic information, authentication information and group information. User information can be registered on the terminal or the card.

1) Basic information comprises ID, Name, Dept., Level and Password.

2) Authentication information comprises fingerprints, a card and face image.

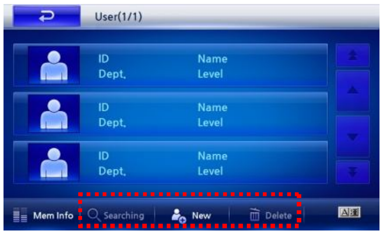
3) Group information

1. Registering on the terminal

The following is an illustration of registering user information on the terminal.

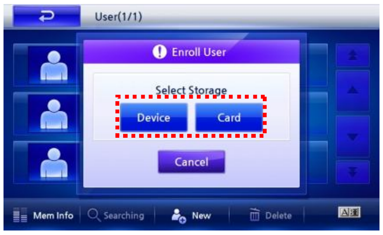
1. Open [Admin Menu] ▸ [User] ▸ [User Management]

- Searching: Search for user information.
- New: Register a user.
- Delete: Delete user information.



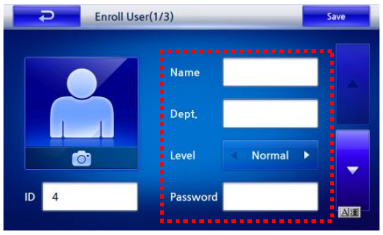
2. For new user registration, select [Device] or [Card].

- Device: Store the user information on D-Station.
- Card: Store the user information on the card.



3. Input Name, Dept., Level and Password, and press [▾].

- Face Image: Press the camera key (showing a human figure) on the bottom of the screen and store the face image.
- Select Normal for Level.
- Input Password twice with the number keys.
- The lowest number available is given as user ID. But users can input the numbers they want manually, from 1 to 4,294,967,295.

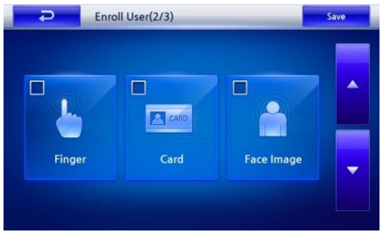


Level Normal

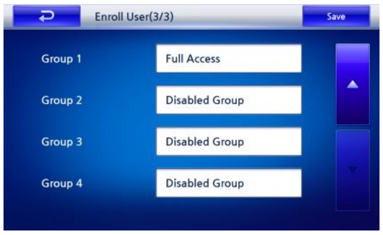
ID 4

4. Select among Finger, Card and Face Image, and input the administrator’s corresponding information. There is no requirement for the number of information options you use, nor necessary order in which to register Finger, Card and Face Image. You can register only the information option you want.

- For information on the registration of Finger, Card, and Face Image, refer to page. 24.



5. Press [▾] and select user group. User group selection is optional and you can use this function when you want to divide users into different groups and manage them accordingly.
    - Set values: No Access / Full Access / Access Group generated by BioStar.
    - Editing access groups should be done through the BioStar program, and the set values for the primary access group are No Access / Full Access. (The authentication time period set in the Operation Menu is irrelevant.)

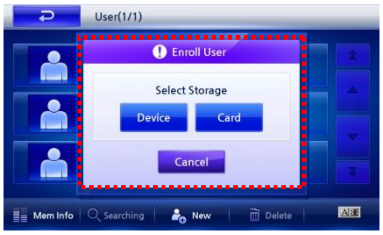


Group 1 Full Access
Group 2 Disabled Group
Group 3 Disabled Group
Group 4 Disabled Group

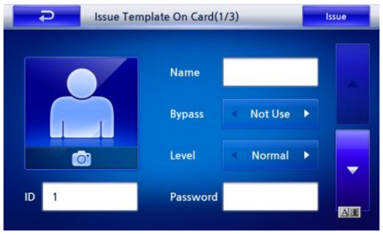
2. Registering on the card

The following is an illustration of how to register user information on a card.

1. Press [New] on the user information management screen, choose [Card], and register.
    - Device: Store the user information on D-Station.
    - Card: Store the user information on the card.

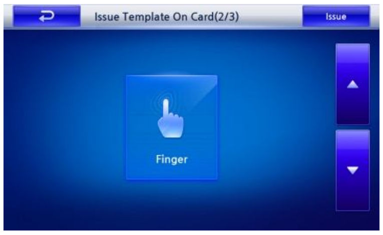


2. Input Name, Bypass, Level and Password, and then press [▾].
    - Select Normal for Level.
    - Input Password twice with the number keys.

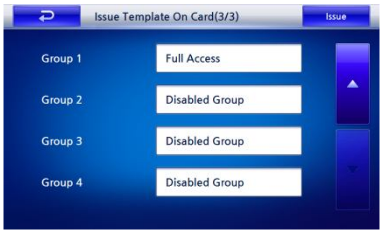


Name
Bypass Not Use
Level Normal
ID 1
Password

3. Select Finger and input the administrator’s corresponding information.
    - For fingerprint registration, refer to page 24.

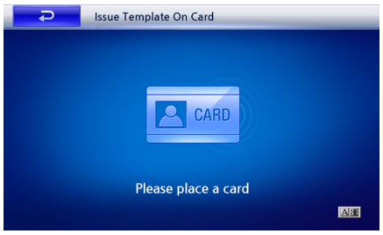


4. Press [▾] and select user group. User group selection is optional and you can use this function when you want to divide users into different groups and manage them accordingly.
    - Set values: No Access / Full Access / access group generated by BioStar
    - Editing access groups should be done through the BioStar program, and the set values for the primary access group are No Access and Full Access. (The authentication time period set in the Operation Menu is irrelevant.)



Group 1 Full Access
Group 2 Disabled Group
Group 3 Disabled Group
Group 4 Disabled Group

5. Pressing [Issue] will open the card registration screen. Put the card to the screen (let them touch).


Issue Template On Card

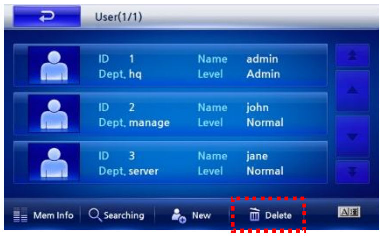
Please place a card

Deleting User Information

Search for currently registered users, and delete the information from the terminal.

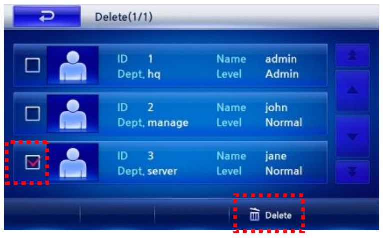
Caution!
Deleted user information cannot be restored if it is not stored in the BioStar Database.

1. Press [Delete] on the user information management screen.


User(1/1)

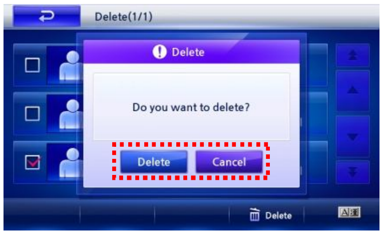
ID		Name	
ID 1	Dept. hq	Name admin	Level Admin
ID 2	Dept. manage	Name john	Level Normal
ID 3	Dept. server	Name jane	Level Normal

2. Select the user to delete (check the box next to the figure) and press [Delete].


Delete(1/1)

☐	ID 1 Dept. hq	Name admin	Level Admin
☐	ID 2 Dept. manage	Name john	Level Normal
☑	ID 3 Dept. server	Name jane	Level Normal

3. When a dialogue box pops up, press [Delete]. Pressing [Cancel] returns the screen to the previous page.


Delete(1/1)

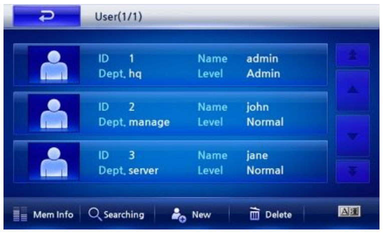
Delete

Do you want to delete?

Changing User Information

Find a registered user and change information such as PIN or fingerprints.

1. Open [Admin Menu] ▸ [User] ▸ [User Management].



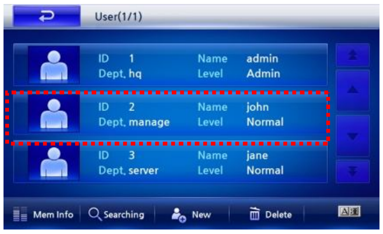
ID 1 Name admin Dept. hq Level Admin

ID 2 Name john Dept. manage Level Normal

ID 3 Name jane Dept. server Level Normal

2. Select from the user list or press [Searching] and enter his / her ID.

Selecting from the user list

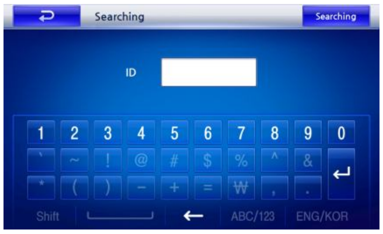


ID 1 Name admin Dept. hq Level Admin

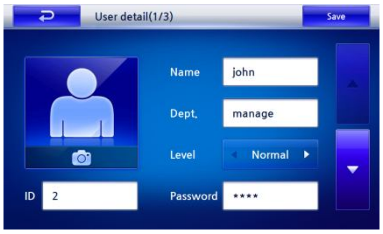
ID 2 Name john Dept. manage Level Normal

ID 3 Name jane Dept. server Level Normal

Using [Searching] function



3. Change the desired information and press [▾].



Name john

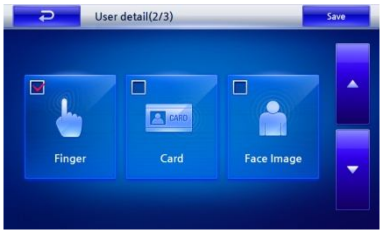
Dept. manage

Level Normal

ID 2

Password ****

4. Select among Finger, Card, and Face Image.
For procedure to change this, refer to the registration procedure on page 24.

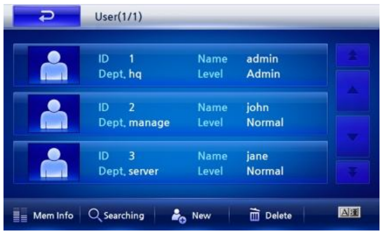


5. After finishing all the changes, press [Save] to store the new information.

User Search

Search for a current registered user.

1. Open [Admin Menu] ▸ [User] ▸ [User Management].



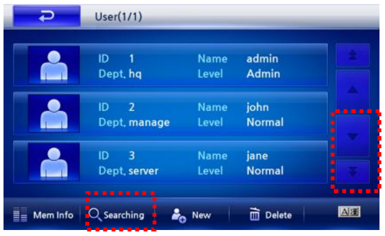
User(1/1)

ID 1 Name admin
Dept. hq Level Admin

ID 2 Name john
Dept. manage Level Normal

ID 3 Name jane
Dept. server Level Normal

2. Use [▾ / ▴] keys on the user list, or press [Searching] and then enter the desired user ID.



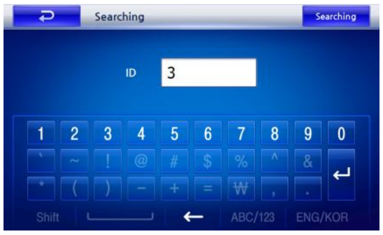
User(1/1)

ID 1 Name admin
Dept. hq Level Admin

ID 2 Name john
Dept. manage Level Normal

ID 3 Name jane
Dept. server Level Normal

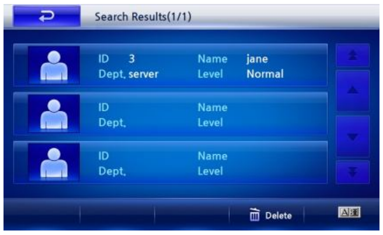
Entering ID after [Searching]



Searching

ID 3

3. The result is displayed on the screen. You can change or delete the user information here.



Search Results(1/1)

ID 3 Name jane
Dept. server Level Normal

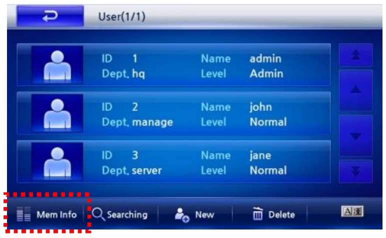
ID Name
Dept. Level

ID Name
Dept. Level

Checking Memory Information

This function checks the amount of the terminal's memory currently in use.

1. Open [Admin Menu] ▸ [User] ▸ [User Management], and select [Mem Info].

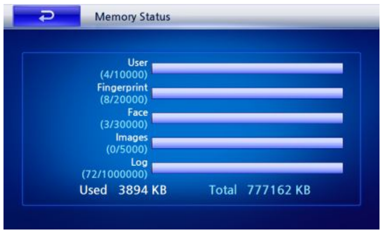

User(1/1)

ID 1 Name admin
Dept. hq Level Admin

ID 2 Name john
Dept. manage Level Normal

ID 3 Name jane
Dept. server Level Normal

2. You can see the currently used memory here.


Memory Status

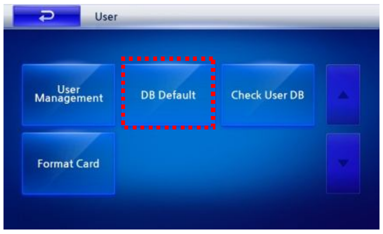
User (4/10000)
Fingerprint (8/20000)
Face (3/30000)
Images (0/5000)
Log (72/1000000)
Used 3894 KB Total 777162 KB

3.3 Using the User Menu

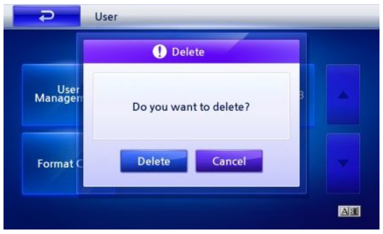
DB Initialization

DB initialization deletes all registered user data. As this process also deletes the Admin information, you must register Admin first after initialization.

1. Open [Admin Menu] ▸ [User], and select [DB Default].



2. Select [Delete] on the dialogue box.
   - This process deletes all the users and Admin information and it cannot be restored.


User

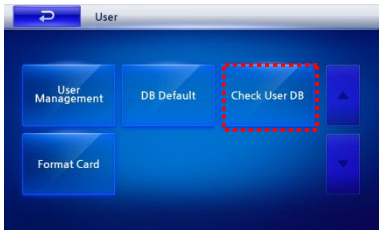
Delete

Do you want to delete?

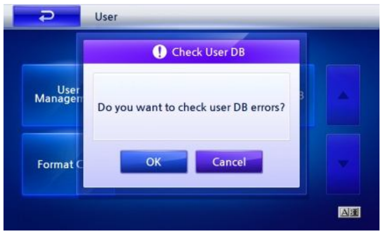
DB Error Check

An error in the User DB may cause failed authentication, even when the user is registered. Running a DB error check examines the DB record and repairs it if any error is detected.

1. Open [Admin Menu] ▸ [User], and select [Check User DB].



2. The result is displayed on the screen.
   - If any error is detected in the user DB, the DB is automatically repaired. If the repair fails, an error message will pop up.

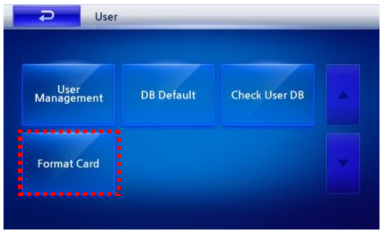


Do you want to check user DB errors?

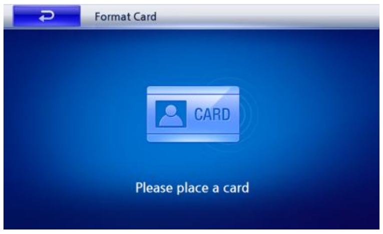
Card Format

User information can be stored on the terminal or MIFARE card. Formatting the card will delete the user information stored on it.

1. Open [Admin Menu] ▸ [User] and Select [Format Card].



2. The screen shown on the right appears. Then put the card to the image on the screen. After formatting is complete, a confirmation window appears.



Please place a card

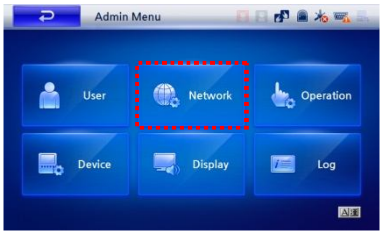
3. 4 Network Management

If you wish to connect the terminal to a PC after installation, you are required to set the network configuration according to the connection mode you choose.

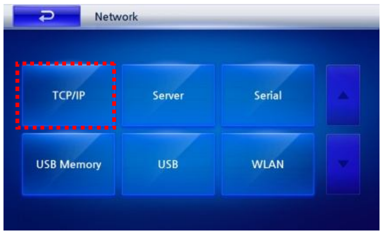
TCP / IP Setting

Select TCP / IP for connecting the terminal and BioStar.

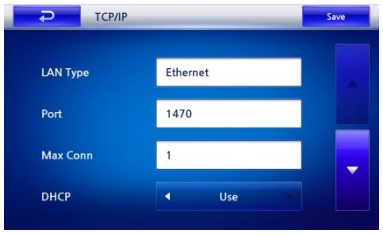
1. Open [Admin Menu] and select [Network].



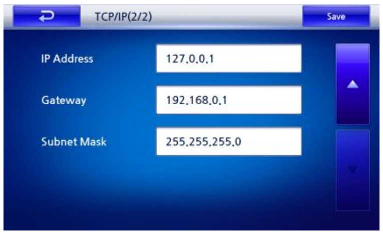
2. Select [TCP / IP] on the screen shown on the right.



3. Enter connection type, port, etc., and press [▾]. On the next screen, enter IP address, gateway and subnet mask. Then press [Save].
   - LAN Type: Connection to a PC through Ethernet via the RJ45 connector located on the rear of the terminal, or using wireless LAN. (Set values: Ethernet / Wireless LAN / Disabled)
   - Port: Assigns the terminal's TCP / IP port. The default value is 1470.
   - Max Conn: Sets the number of BioStars that can be connected to the terminal. (Set values: 1, 4, 6, 8 and 16)
   - DHCP: Sets whether or not to use DHCP protocol. (Set values: Enabled / Disabled)
   - IP Address: Enter the IP address when adopting a fixed IP instead of DHCP protocol. Ask your network administrator for the IP address.
   - Gateway: Enter the gateway address when adopting a fixed IP instead of DHCP protocol. Ask your network administrator for the address.
   - Subnet Mask: Enter the Subnet Mask address when adopting a fixed IP instead of DHCP protocol. Ask your network administrator for the address.



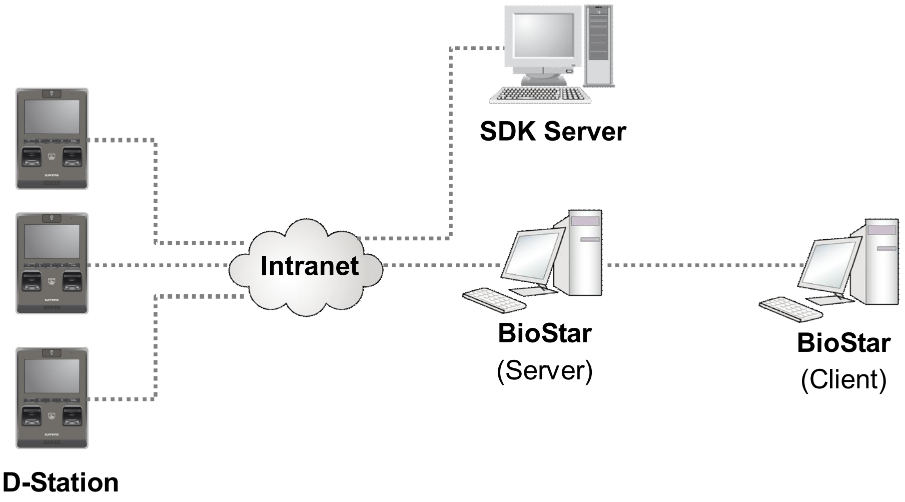
LAN Type: Ethernet
Port: 1470
Max Conn: 1
DHCP: ◂ Use



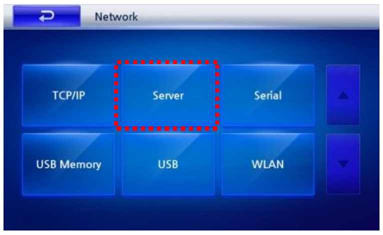
IP Address: 127.0.0.1
Gateway: 192.168.0.1
Subnet Mask: 255.255.255.0

Server Configuration

The terminal can communicate with the BioStar server or SDK server. Configure the IP and ports of the server to connect to the terminal.

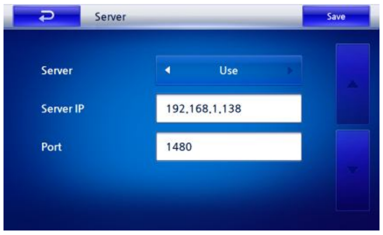


1. Open [Admin Menu], and select [Server].



2. Configure the server information and press [Save].

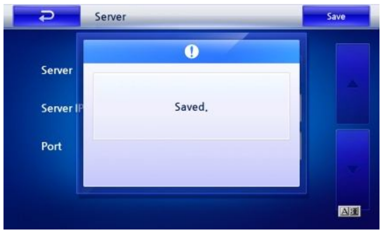
- Server: Set whether or not to use a host server.
  To make a direct connection from the BioStar client to D-station without connecting to a server, select 'Server - Disabled'.
- Server IP: Enter the IP address of the host server.
- Port: Enter the port of the host server.



Server: Use
Server IP: 192.168.1.138
Port: 1480

3. The configuration confirmation window appears.

- Running this process displays D-Station on the BioStar Client program which is connected to the server.

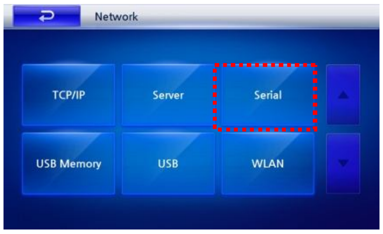


Saved.

Serial Configuration

Configure the communication type and the network speed when connecting the terminal to BioStar or a PC.

1. Open [Admin Menu] and select [Serial].



2. Configure the serial information and press [Save].

- RS485: Set the network speed between the terminal and a PC in RS485 communication. (Set values: Not Use / 9600 / 19200 / 38400 / 57600 / 115200)

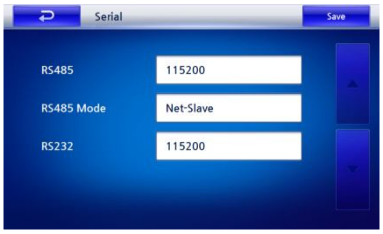
- The default value is ‘115200’, but you can change to a lower speed if a communication error occurs.
- RS485 port is on the back of the terminal.

- RS485 mode: Set the environment of RS485 communication. (Set values: Disabled, Net-Slave, Net-Host)
  RS485 mode allows communication between a server terminal and up to 7 slave terminals.

- Net-Slave: When connecting several terminals, sets the terminal as a slave.
- Net-Host: When connecting several terminals, sets the terminal as the host.

- RS232: Set the network speed between the terminal and a PC in RS232 communication.

- Select when connecting the terminal to a PC through 9-pin connectors on the back of the terminal in RS232 communication.

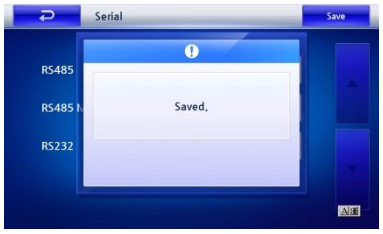


RS485 115200

RS485 Mode Net-Slave

RS232 115200

3. The configuration confirmation window appears.



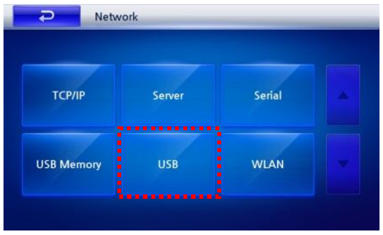
Saved.

USB

Set the USB port on ‘Enable’ only when a USB flash drive is connected to the terminal for use.

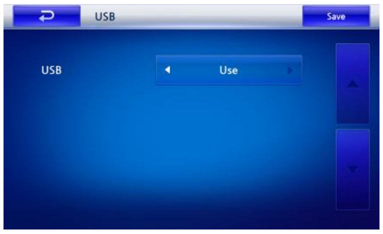
Caution!
Use the USB port on the bottom of the terminal when connecting to a PC. For security purposes, the port is set on ‘Disabled’. Make sure to change the setting to ‘Enabled’ when connecting the terminal and a PC using a USB flash drive.

1. Open [Admin Menu] and select [USB].



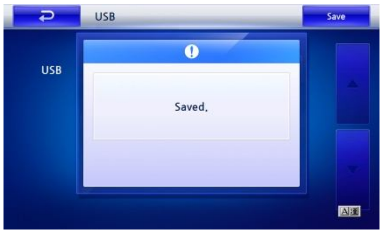
2. Select whether or not to use USB and press [Save].

- Enabled: When connecting to a PC using the USB port.
- Disabled: For normal operation of the terminal not using the USB port.



USB Use

3. The configuration confirmation window appears.



Saved.

USB Memory

You can export user information and log data stored on the terminal to a USB flash drive. Alternatively, you can import information on the USB memory to the terminal. This is particularly convenient for regular data exchange with the PC's BioStar program.

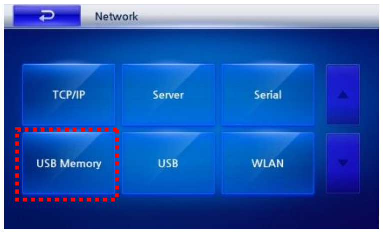
If you wish to connect a PC to the terminal's USB port after terminal installation, first set the USB port to 'Enabled'. (Refer to the previous page.)

Before configuring USB settings, plug the USB flash drive into the USB port.

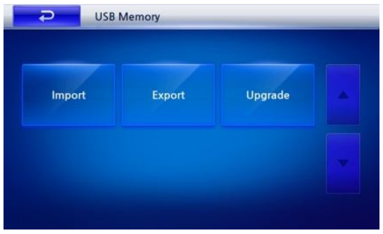
Caution!

Importing rewrites all the user information and set values.

1. Open [Admin Menu], and select [USB Memory].

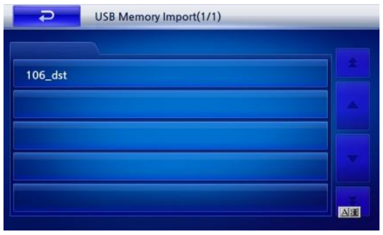


2. Select among Import, Export or Upgrade. The process may take from just a few seconds to a couple of hours.
   - Import: Copy the user information and various set values stored in the USB memory on the terminal.
   - Export: Copy the user information and set values stored on the terminal to a USB flash drive.
   - Upgrade: Upgrade the terminal's firmware with that stored in a USB memory.



■ Import (Example)

- Select the name of the file to import, and the user information and log data in the USB memory are copied to the terminal.

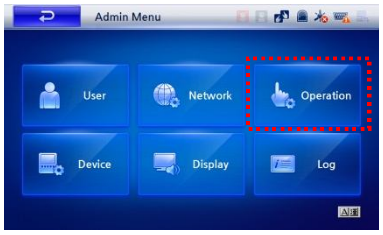


3.5 Operation Management

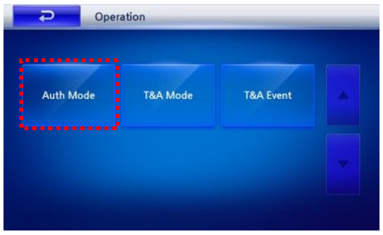
Configure terminal operation, time and attendance and access control.

Setting Authentication Mode

1. Open [Admin Menu], and select [Operation].



2. The screen shown on the right appears. Select [Auth Mode] on it.

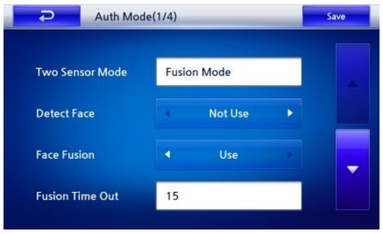


3. Configure the authentication mode you want to use and press [▾]

- Two-sensor mode: Two fingerprint sensors and two CPUs work for user authentication. (Set values: Fast Mode / Fusion Mode / Twin Mode)

- Fast mode: Two CPUs perform simultaneous authentication of one fingerprint input.
- Fusion mode: Authentication process is performed by a fusion algorithm on two fingerprints. This allows simultaneous input of two fingerprints. Using the combination of features from both fingerprints, fusion mode increases the authentication rate for users who have a low authentication rate for each fingerprint and may experience repeated failed authentication with other authentication modes.
- Twin mode: Two sensors perform authentication processes independently. One terminal of D-Station can process two persons simultaneously.
- Demo Mode: Demonstration mode for face fusion how to be used. Authentication will succeed nevertheless face recognition is failed, if only finger authentication succeeds. Do not apply this mode to real operation, but only to test and demonstration.

- Detect Face: Select whether or not to photograph the face on authentication. After a successful authentication, the user's face image is detected automatically and that image is stored as a log.
- Face Fusion: The user's face image is also included in authentication. It increases the authentication rate in users who have low authentication rate with fingerprint recognition.



Two Sensor Mode: Fusion Mode
Detect Face: Not Use
Face Fusion: Use
Fusion Time Out: 15

- The authentication modes which apply the face fusion feature are fast mode and fusion mode. The combinations of fast mode and face fusion, and fusion mode and face fusion are possible.

• Fusion Time Out: The time-out against the total required time for a successful fusion authentication when operating in fusion mode.

4. Set the access authentication mode and press [▾]. Set only one of the five authentication modes as on 'Always' with the other modes set to 'Disabled'.

• ID / card+finger: Users input ID / card and fingerprints consecutively for authentication.

• ID / card+password: Users input ID / card and PIN consecutively for authentication.

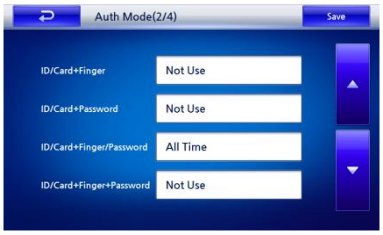
• ID / card+finger / password: Users input ID / card and a fingerprint or PIN for authentication.

• ID / card+finger+password: Users input ID / card, fingerprints, and PIN consecutively for authentication.

• Card Only: Users input only cards for authentication. In this mode, the card type should be set on the [Use Card] menu.

• Authentication mode set values

- Default access time: Always / Disabled



ID/Card+Finger Not Use
ID/Card+Password Not Use
ID/Card+Finger/Password All Time
ID/Card+Finger+Password Not Use

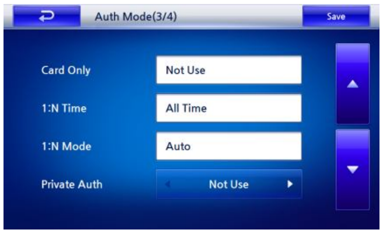
5. Set the authentication mode and press [▼].

• 1:N Time: Set the time schedule of 1:N authentication mode, for which only fingerprints are used. (Set values: Always / Disabled / the access time generated by BioStar)

- When setting 'Always', the access time should be set beforehand on the BioStar program's Access Control menu.

• 1:N mode: Set the operation mode of 1:N authentication mode, for which only fingerprints are used. (Set values: Disabled / Auto / T&A key)

• Private Auth: Select whether or not to use the authentication mode set for an individual. (Set values: Disabled / Enabled)

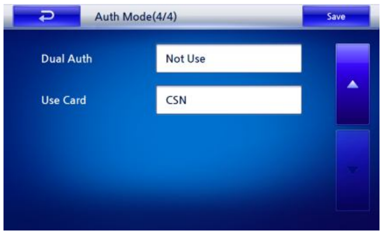


Card Only Not Use
1:N Time All Time
1:N Mode Auto
Private Auth Not Use

6. Set the authentication mode and press [Save].

• Dual Auth: Select whether or not to use dual authentication. (Set values: Disabled / Always)

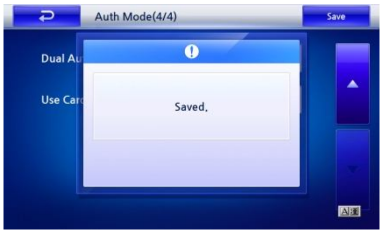
- When set for 'Always', the fingerprints or cards of two different persons should be input within a 15 seconds of interval for successful authentication. The door does not open when the first person's authentication is finished. Without another authentication within 15 seconds, the first authentication becomes invalid and the process of dual authentication must be started again.



Dual Auth Not Use
Use Card CSN

- Use Card: Select the card type used for authentication. (Set values: Disabled / Use Template / CSN)
  - Use Template: Store the user information and fingerprint information directly on the card.
  - CSN: Stores the unchangeable card serial number (CSN) assigned to each user. Users can input the CSN in person.

7. The configuration confirmation window appears.

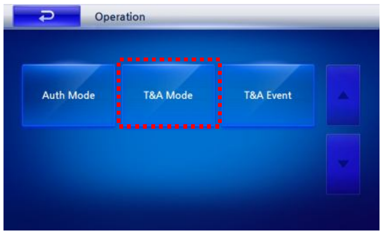


Saved.

Time and Attendance Configuration

Configuration of time and attendance input method.

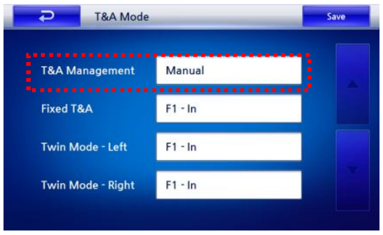
1. Open [Admin Menu] ▸ [Operation] Select [T&A Mode].



2. Set the function key usage for each item on [T&A Mode].

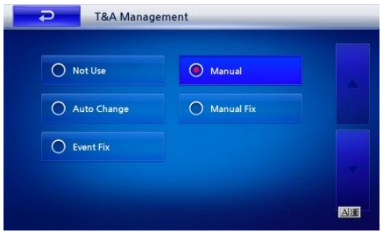
■ T&A Management

T&A Mode Screen



T&A Management: Manual
Fixed T&A: F1 - In
Twin Mode - Left: F1 - In
Twin Mode - Right: F1 - In

T&A Management Screen



○ Not Use ● Manual
○ Auto Change ○ Manual Fix
○ Event Fix

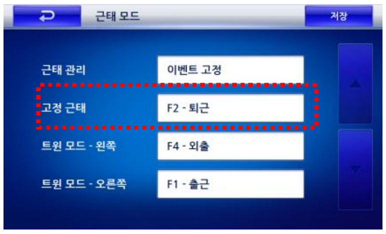
- Set values: Disabled / Manual / Auto Change / Manual Fix / Event Fix
  - Manual: Usually the time and attendance function is inactivated, but you can select attendance status when pressing a designated function key. The log of selected attendance status is recorded if user authentication is successful at the time.
  - Auto Change: 'Auto Change' is convenient when applying the attendance events (getting to work, outside duty, etc.) and time periods set on BioStar unconditionally to all users using the door.
    For 'Auto Change', you can set a corresponding time period for each attendance event. During such a time period, the activated attendance status is recorded.
  - Manual Fix: The activated attendance status is shown on the screen and users can change it by pressing a function key. When it is changed, the status remains as it is until another

status is input. The attendance log is recorded for every successful authentication. 'Manual Fix' is convenient when applying changed attendance events unconditionally to all users using the door.

- Event Fix: A specific attendance status is maintained, and a successful user authentication is followed by logging such attendance status. When set for Event Fix, other function keys' input is ignored.
- Select among Attendance F1 to EXT12. The set values for Attendance F1 to EXT12 should be set on the BioStar program.

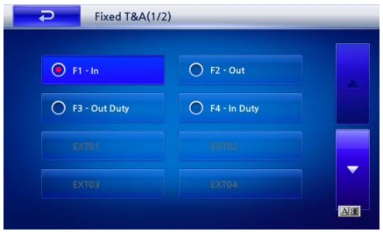
Fixed Time and Attendance

T&A Mode Screen



근태 관리: 이벤트 고정
고정 근태: F2 - 퇴근
트윈 모드 - 왼쪽: F4 - 외출
트윈 모드 - 오른쪽: F1 - 출근

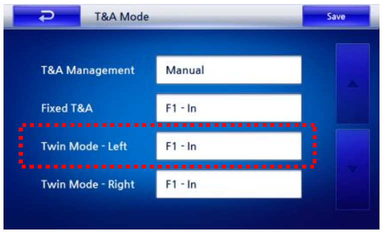
Fixed T&A Screen



- In the Fixed Time and Attendance field, select the fixed attendance event to use on authentication when Time and Event is set for 'Event Fix'. You can select from F1 to EXT12.

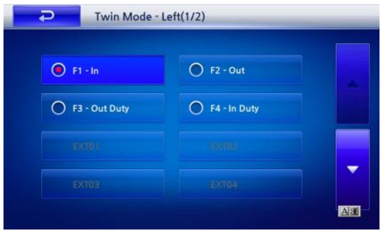
Twin Mode – Left

T&A Mode Screen



T&A Management: Manual
Fixed T&A: F1 - In
Twin Mode - Left: F1 - In
Twin Mode - Right: F1 - In

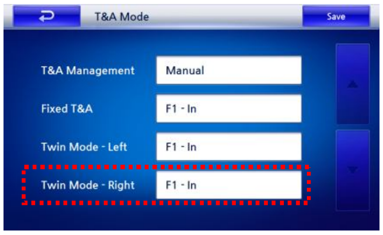
[Twin Mode-Left] Screen



- Set the key to use when selecting the left sensor in Twin mode.
- Select the fixed attendance event to use for authentication on the left sensor when Time and Attendance is set for 'Event Fix' and the sensor is set to Twin mode.
- You can select from F1 to EXT12.

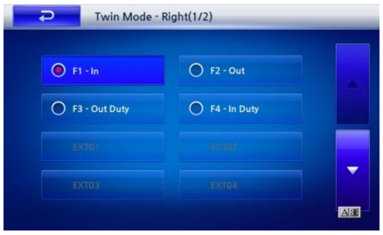
Twin Mode – Right

T&A Mode Screen



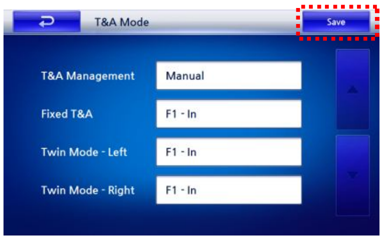
T&A Management: Manual
Fixed T&A: F1 - In
Twin Mode - Left: F1 - In
Twin Mode - Right: F1 - In

[Twin Mode-Right] Screen



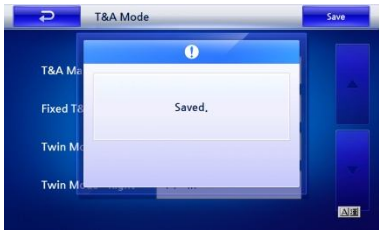
- Set the key to use when selecting the right sensor in Twin mode.
- Select the fixed attendance event to use for authentication on the right sensor when Time and Attendance is set for 'Event Fix' and the sensor is set to Twin mode.
- You can select from F1 to EXT12.

3. Press [Save] after setting configuration.



T&A Management: Manual
Fixed T&A: F1 - In
Twin Mode - Left: F1 - In
Twin Mode - Right: F1 - In

4. The configuration confirmation window appears.



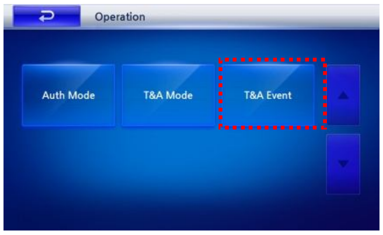
Saved.

Confirming Time and Attendance Events

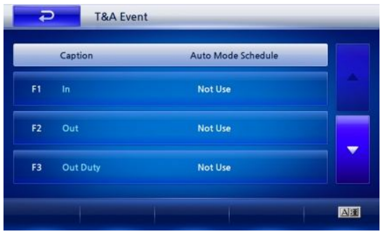
In the Time and Attendance Event menu, set specific events assigned to F1 to F4 or EXT01 to12 and their automatic application time on BioStar.

You can check the above setting conditions on the Time and Attendance setting screen, but you cannot add, change or delete them from the terminal.

1. Open [Admin Menu] ▶ [Operation] and select [T&A Event].



2. Use [▾] / [▴] to check the time set on BioStar. (Set values: F1-F4, EXT01- 12)
   - If Time and Attendance is in ‘Auto Change’ mode, and its automatic application time is set for ‘Enable’, the Time and Attendance function key automatically selected at a given time is applied.



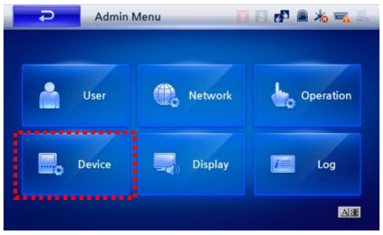
Caption		Auto Mode Schedule
F1	In	Not Use
F2	Out	Not Use
F3	Out Duty	Not Use

3.6 Terminal Management

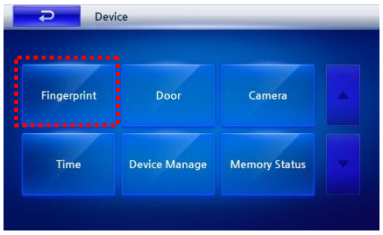
Set the terminal’s basic conditions, time and attendance, access control, etc.

Configuring Fingerprint Authentication

1. Open [Admin Menu] and select [Device].



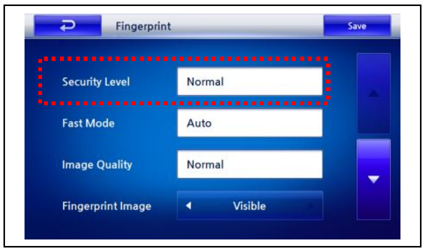
2. Select [Fingerprint] on a screen shown on the right.



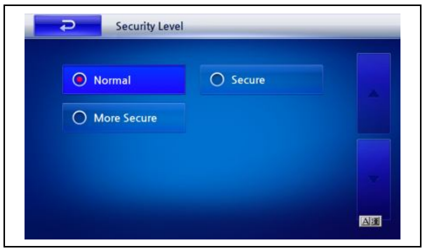
3. Set the detailed conditions of fingerprint authentication.

■ Security Level

The following describes the security level regarding fingerprint recognition rate under the conditions of access by fingerprint authentication.



Security Level: Normal
Fast Mode: Auto
Image Quality: Normal
Fingerprint Image: Visible



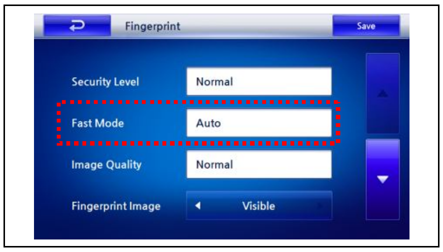
● Normal ○ Secure
○ More Secure

- Set values: Normal / Secure / More Secure

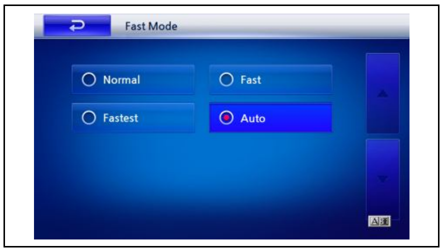
  - The security level is determined by the false acceptance ratio (FAR). A lower security level allows easier user authentication, while a higher security level requires the exact input of fingerprints. Therefore, select ‘Secure’ or ‘More Secure’ for circumstances demanding strict access control and security, and select ‘Normal’ otherwise.

■ Fast Mode

Set the user recognition speed under condition of access by fingerprint authentication.



Security Level: Normal
Fast Mode: Auto
Image Quality: Normal
Fingerprint Image: Visible



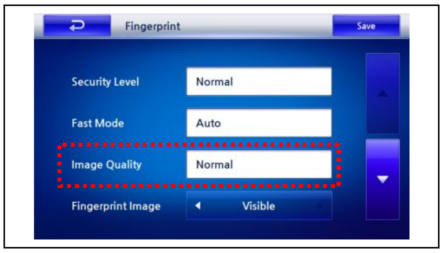
○ Normal ○ Fast
○ Fastest ● Auto

- Set values: Normal / Fast / Fastest / Auto

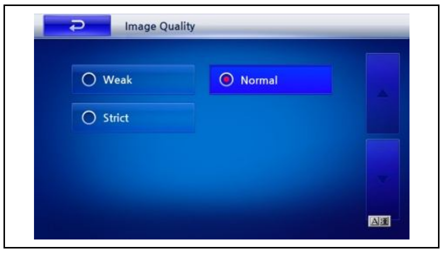
  - With more than hundreds of users, faster recognition speed saves time but it may raise the false reject rate (FRR). ‘Auto’ determines the recognition speed according to the number of fingerprint templates stored on the device.

■ Image Quality

Set the standard for the input fingerprints quality.



Security Level: Normal
Fast Mode: Auto
Image Quality: Normal
Fingerprint Image: Visible

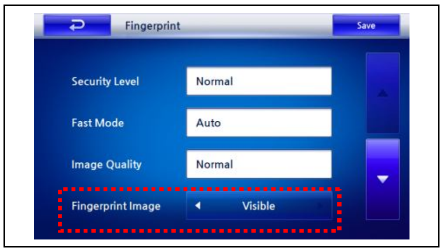


○ Weak ● Normal
○ Strict

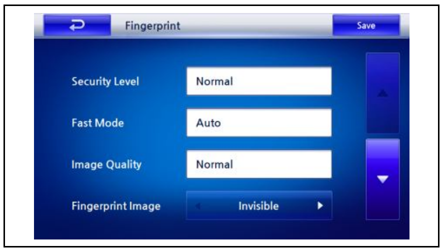
- Set values: Weak / Normal / Strict
  - In the 'Weak' setting, users who experience frequent authentication failures will otherwise easily pass the process.

Fingerprint Image

Select whether or not to display users' fingerprints on the screen when registering them.



Security Level: Normal
Fast Mode: Auto
Image Quality: Normal
Fingerprint Image: Visible

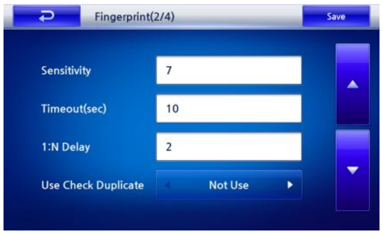


Security Level: Normal
Fast Mode: Auto
Image Quality: Normal
Fingerprint Image: Invisible

- Set values: Visible / Invisible
  - Setting 'Visible' allows the user to check his fingerprint on the LCD screen, thus providing assistance for proper input.

4. Press [▾] and set detailed conditions.

- Sensitivity: Sets the sensors' sensitivity when reading fingerprints.
  - Lower sensitivity allows easier fingerprint input while higher sensitivity produces high quality images of fingerprints input. The highest value is recommended for ordinary circumstances. When optical models are affected by sunlight, setting the sensitivity at lower values helps mitigate these effects.
- Timeout (Sec): Set the standby time in seconds. (Set values: 1 / ….20)
  - Failing to input fingerprints within a certain time leads to failed authentication.
- 1:N Delay: Sets the standby time (to 10 sec) during fingerprint authentication. (Set values: 1 / ….10)
  - Setting the delay time prevents repeated authentication of the same fingerprints when users keep their finger on the sensor.
- Check Duplicate: Checks if the fingerprint being registered is already in the database, and shows the result. (Set values: Disabled / Enabled)
  - If the device determines the fingerprint to have been previously registered, the registration process is cancelled.



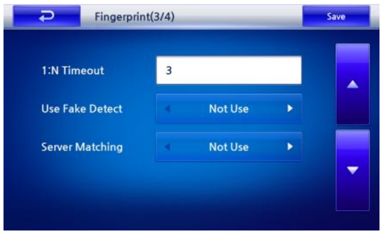
Sensitivity: 7
Timeout(sec): 10
1:N Delay: 2
Use Check Duplicate: Not Use

5. Press [▾] and set detailed conditions.

- 1:N Timeout: Set the user recognition speed under the condition of access by fingerprint authentication.
  (Set values: 1 / 2 / 3 / … / 19 / 20)

- Failure to find a matching fingerprint in the set matching time is processed as an authentication failure.

- Fake Detection: Select whether or not to use the fake fingerprint detection function. (Set values: Disabled / Enabled)
- Server Matching: Select whether or not to compare the fingerprints to those registered on the server. (Set values: Disabled / Enabled)


Fingerprint(3/4)

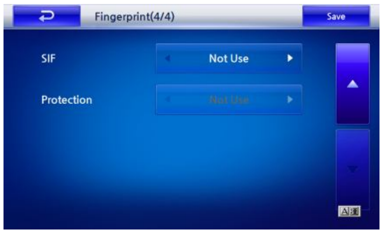
1:N Timeout 3

Use Fake Detect Not Use

Server Matching Not Use

6. Press [▾] and set detailed conditions.

- SIF: Select whether or not to use ISO / IEC compatible data format. (Set values: Disabled / Enabled)
- Protection: Select whether or not to use user information protection function. (Set values: Disabled / Enabled)


Fingerprint(4/4)

SIF Not Use

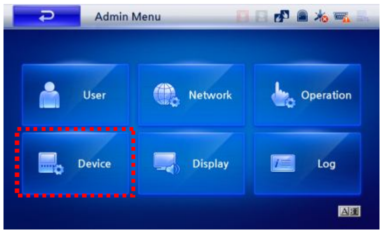
Protection Not Use

7. Press [Save], and then [↩].

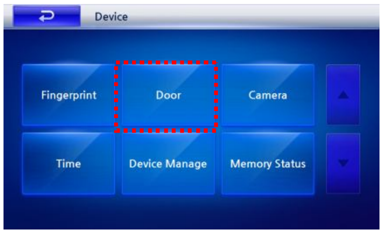
Setting the Door Operation

The following describes how to configure the settings of the interphone, door relay and event occurrence.

1. Open [Admin Menu], and select [Device].



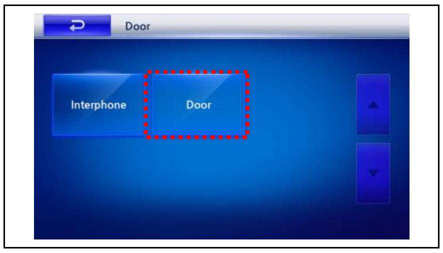
2. Select [Door] on the screen shown on the right.

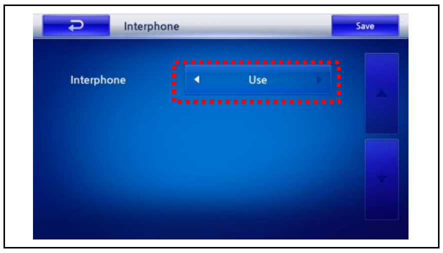


3. Configure the interphone and door separately.

■ Interphone

Select whether or not to use [Interphone] and press [Save].



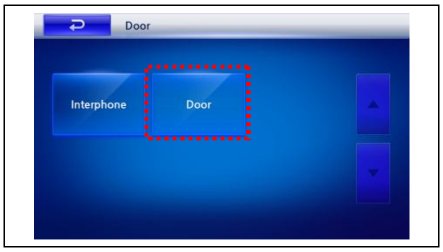


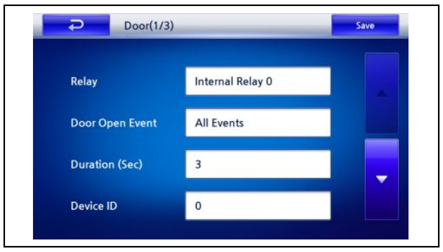
Interphone ◂ Use ▸

- Set [Interphone] to [Enable] to use the [CALL] button and interphone.

■ Door

① Set the conditions of the [Door] and press [▾].



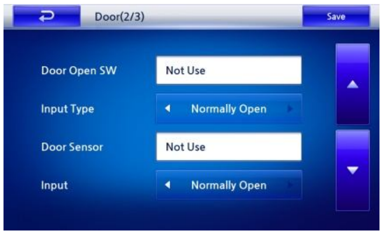


Relay: Internal Relay 0
Door Open Event: All Events
Duration (Sec): 3
Device ID: 0

- Relay: Select relay to open the door on authentication. (Set values: Disabled / Internal Relay 0 / Internal Relay 1 / External Relay 0 / External Relay 1 / SIO0 Relay 0 / SIO0 Relay 1 / SIO1 Relay 0 / SIO1 Relay 1 / SIO2 Relay 0 / SIO2 Relay 1 / SIO3 Relay 0 / SIO3 Relay 1)
  - Set values: Disabled
- Door Open Event: Determine events to open the door. (Set values: All Events / Auth+T&A Event / Auth Event / T&A Event / Disabled)
  - All Events: The door opens for all successful authentication events (1:1 PIN authentication, PIN authentication, 1:1 fingerprint authentication, 1:1 fingerprint recognition).
  - Auth+T&A Event: The door opens for T&A events for which door access is selected. The door also opens on authentication without T&A events.
  - T&A Event: The door opens for certain T&A events for which door access is selected.
  - Auth Event: The door opens on authentication without T&A events.
  - Disabled: The door does not open for any authentication or event.
- Duration (Sec): Set the duration to open the door on event occurrence. The door closes after the set duration.
- Device ID: Input the terminal ID which is used when going out from inside. (Set values: 0 / Terminal ID)

② Press [▾] and set the following conditions:

- Door Open SW: Select whether or not to use the door open switch. (Set values: Disabled, Input 0, Input 1, SIO0 Input 0 to 3, SIO1 Input 0 to 3, SIO2 Input 0 to 3, SIO3 Input 0 to 3)
- Input Type: Select the door open switch’s operation mode. (Set values: N / O, N / C)
- Door Sensor: Set the detection mechanism for door opening. (Set values: Disabled, Input 0, Input 1, SIO0 Input 0 to 3, SIO1 Input 0 to 3, SIO2 Input 0 to 3, SIO3 Input 0 to 3)
- Input: (Set values: N / O, N / C)



Door Open SW: Not Use
Input Type: Normally Open
Door Sensor: Not Use
Input: Normally Open

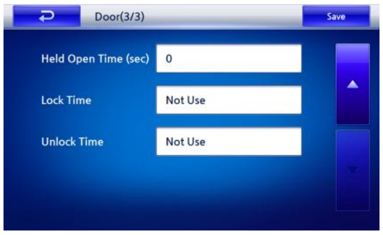
③ Press [▾] and set the following conditions.

- Held Open Time (Sec): Sets the duration of time for the alarm to go off after the door opens.
- Lock Time: Set the time to keep the door forcibly locked. (Set values: Disabled / Enabled)

- During Lock Time, only the administrator can access the door while ordinary users cannot. The lock time is set only on the BioStar program.

- Unlock Time: Set the time to keep the door forcibly open.

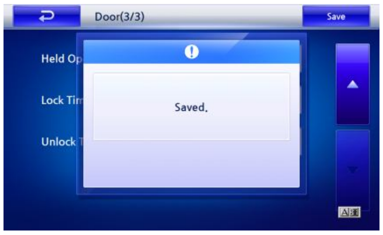
- Set values: Disabled / Enabled
  (During the Unlock Time, no event will close the door.)
- Unlock Time is set only on the BioStar program.



Door(3/3) Save

Held Open Time (sec)	0
Lock Time	Not Use
Unlock Time	Not Use

④ Press [Save], and [↩].



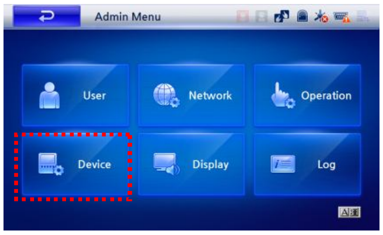
Door(3/3) Save

Saved.

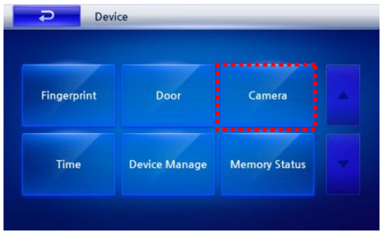
Configuring the Camera

Check the authentication camera is working at the door. And the terminal is applied automatically by the setting of the Biostar.

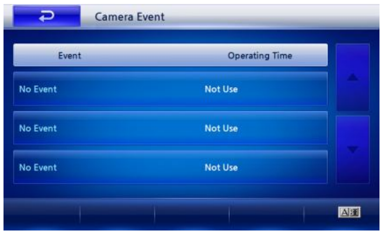
1. Open [Admin Menu], and select [Device].



2. Select [Camera] on the screen shown on the right.



3. The [Camera Event] screen appears. Press [↩] to close it.



Camera Event

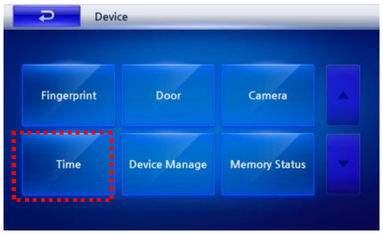
Event	Operating Time
No Event	Not Use
No Event	Not Use
No Event	Not Use

Chapter 3. Admin Menu

Setting the Time

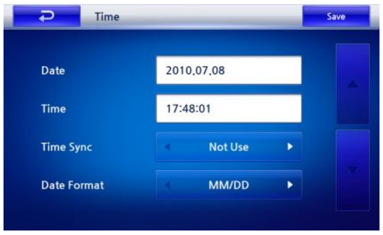
You can set the time shown on the terminal. Setting the time of the terminal ensures the recording of accurate access time and log data.

1. Open [Admin Menu] ▸ [Device], and select [Time].



2. Set detailed conditions and select [Save] on the screen shown on the right.
   - Date: Enter the date (YYYYMMDD).
   - Time: Enter the time (hhmmss).
   - Time Sync: Select the terminal's time reference. (Set values: Enabled, Disabled)

   - Disabled: The time set on the terminal itself becomes the reference.
   - Enabled: Synchronize to the server time.
   - Date Format: Select the date display order. (MM / DD or DD / MM)

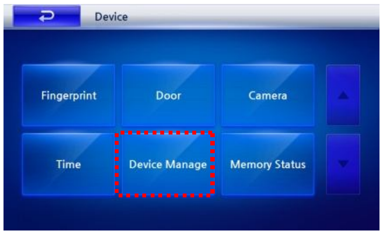


Date 2010,07,08
Time 17:48:01
Time Sync Not Use
Date Format MM/DD

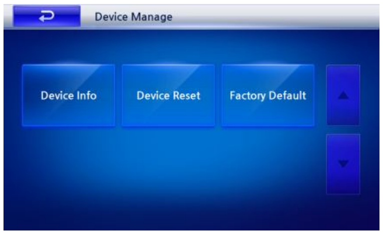
Terminal Management

You can check information, reset or initialize the terminal.

1. Open [Admin Menu] ▸ [Device] and select [Device Manage].

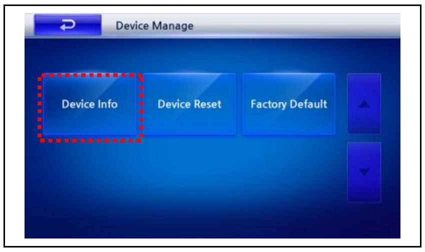


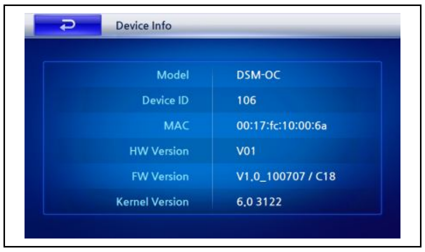
2. Select the menu on the [Device Manage] screen shown on the right.



■ Device Info

Device Info shows basic information. This includes the model and hardware version.

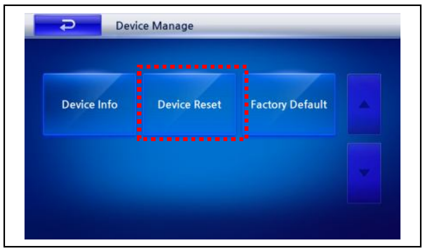


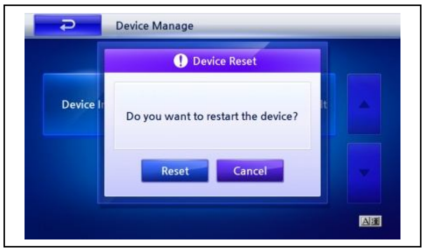

Device Info

Model	DSM-OC
Device ID	106
MAC	00:17:fc:10:00:6a
HW Version	V01
FW Version	V1.0_100707 / C18
Kernel Version	6.0 3122

■ Device Reset

Device Reset resets the terminal if there is any instability in its functioning.




Device Manage

Device Reset

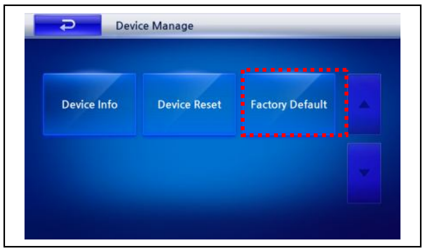
Do you want to restart the device?

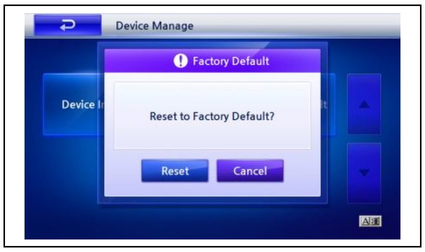
Caution!
Initializing deletes all the information including downloaded screen themes, sounds, notices, etc., along with the set values.

■ Factory Default

Factory Default initializes all the set values of the terminal to factory defaults.

.




Device Manage

Factory Default

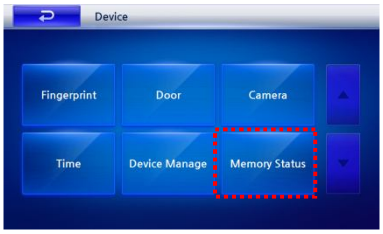
Reset to Factory Default?

Note
Initializing does not delete registered user information and log data. To delete user information or log data, Refer to page29. **Deleting User Information** and page53. **Log Initializing**.

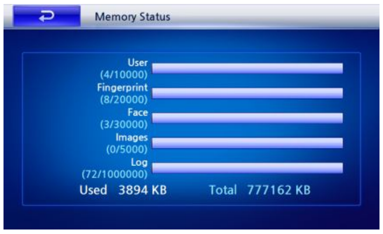
Memory Check

Memory Check checks the terminal's current memory use.

1. Open [Admin Menu] ▸ [Device], and select [Memory Status].



2. The memory use information is shown on the screen.


Memory Status

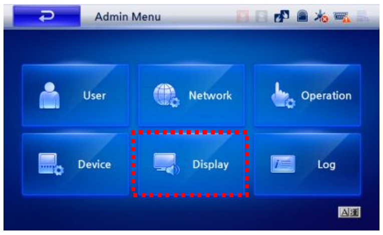
User (4/10000)
Fingerprint (8/20000)
Face (3/30000)
Images (0/5000)
Log (72/1000000)
Used 3894 KB Total 777162 KB

3.7 Display / Sound Management

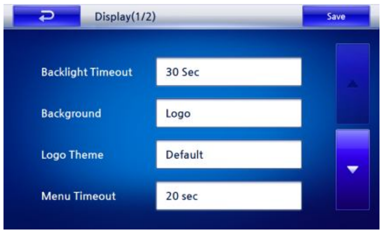
You can set the terminal's screen theme, sound volume, etc.

Setting Display / Sound

1. Open [Admin Menu], and select [Display].

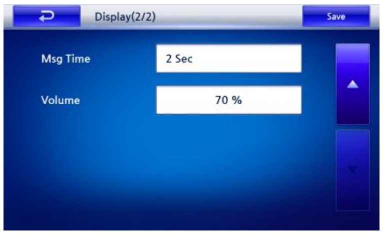


2. Press [▾] and set detailed conditions.
   - Backlight Timeout: The duration of time after which without any key input, the backlight is turned off. (Set values: Infinite / 10 sec to 60 sec)
   - Background: Select the screen theme for the start-up screen. (Set values: Logo / Notice)
   - You can upload screen themes through the BioStar program.
   - Logo theme: Select the logo theme to use. (Set values: Theme 1 to 20 / Default / Custom)
   - Menu Timeout: The duration of time after which without any key input, the screen returns to the start-up screen. (Set values: Infinite / 10 sec / 20 sec / 30 sec)



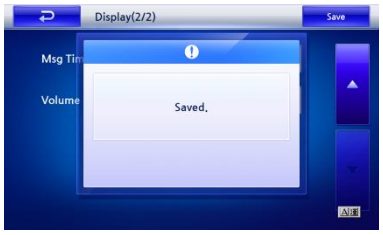
Backlight Timeout: 30 Sec
Background: Logo
Logo Theme: Default
Menu Timeout: 20 sec

3. Press [▾] and set detailed conditions.
   - Msg Time: The time for which the message on the screen during authentication shows. (Set values: 0.5 sec / 1 sec / 2 sec / 3 sec / 4 sec / 5 sec)
   - Volume: Sets the sound volume. (Set values: 0% / 10% / 20% / … / 100%) 0% volume does not produce any sound.



Msg Time: 2 Sec
Volume: 70 %

4. Press [Save] and [↩].



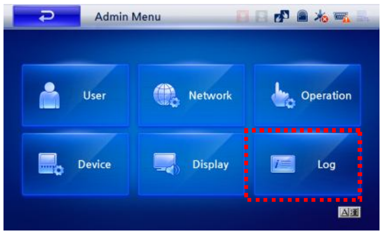
Saved.

3.8 Log Management

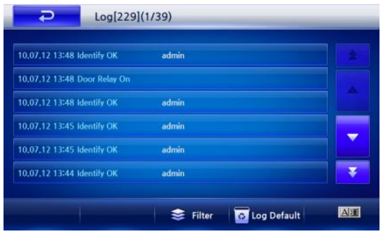
You can check or remove access and T&A information recorded on the terminal.

Log Management

1. Open [Admin Menu], and select [Log].



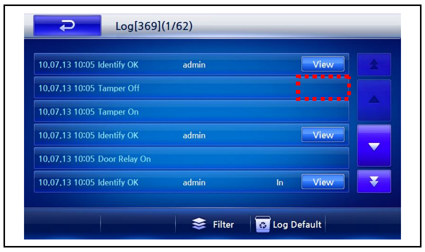
2. Press [▼] to check the log or set [Filter] or [Log Default].


Log[229](1/39)

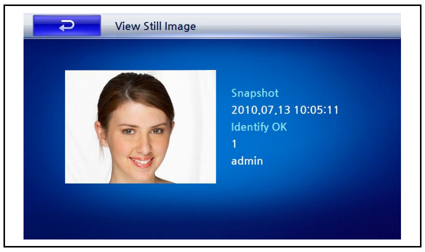
```
10.07.12 13:48 Identify OK      admin
10.07.12 13:48 Door Relay On
10.07.12 13:48 Identify OK      admin
10.07.12 13:45 Identify OK      admin
10.07.12 13:45 Identify OK      admin
10.07.12 13:44 Identify OK      admin
```

■ Visual Log View

Select [View] on the log list to see the photographed log.


Log[369](1/62)

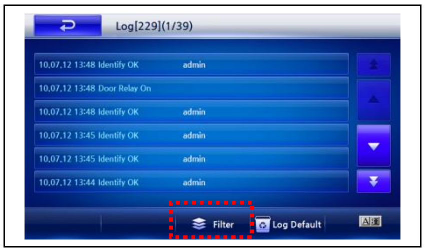
```
10.07.13 10:05 Identify OK      admin          View
10.07.13 10:05 Tamper Off
10.07.13 10:05 Tamper On
10.07.13 10:05 Identify OK      admin          View
10.07.13 10:05 Door Relay On
10.07.13 10:05 Identify OK      admin      In  View
```


View Still Image

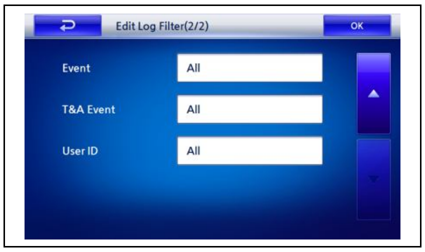
Snapshot
2010.07.13 10:05:11
Identify OK
1
admin

■ Log Filter

Select [Filter] and set event, T&A event and User ID to edit the log filter.


Log[229](1/39)

```
10.07.12 13:48 Identify OK      admin
10.07.12 13:48 Door Relay On
10.07.12 13:48 Identify OK      admin
10.07.12 13:45 Identify OK      admin
10.07.12 13:45 Identify OK      admin
10.07.12 13:44 Identify OK      admin
```

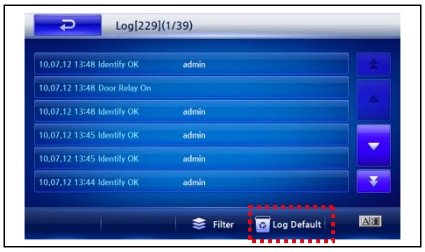

Edit Log Filter(2/2)

Event	All
T&A Event	All
User ID	All

- Event: Designate the events to filter.
- T&A Event: Designate the T&A events to filter.
- User ID: Designate the user ID to filter. To set for all users, enter 0.

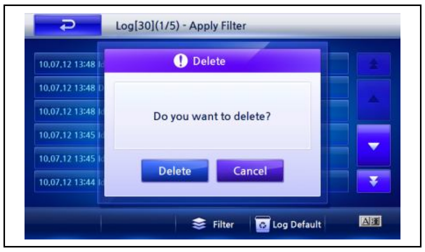
Log Initializing

Select [Log Default] to delete all logs. Selecting [Delete] on the dialogue box deletes all log information.



Log[229](1/39)

```
10.07.12 13:48 Identify OK      admin
10.07.12 13:48 Door Relay On
10.07.12 13:48 Identify OK      admin
10.07.12 13:45 Identify OK      admin
10.07.12 13:45 Identify OK      admin
10.07.12 13:44 Identify OK      admin
```



Log[30](1/5) - Apply Filter

Delete

Do you want to delete?

Chapter 4. User Menu

4.1 Access Authentication

Access is permitted on the input of fingerprint / card / ID / PIN according to the authentication mode.

1 : N Access by Fingerprint Recognition

When 1:N recognition mode is set to 'Auto' or 'T&A', the door opens with only the fingerprint.

1. When 1:N recognition mode is set to 'Auto'

- Fingerprint input without a single key stroke shows the access authentication message and opens the door.

2. When 1:N recognition mode is set on 'T&A' function keys

- Pressing the set T&A function keys makes the blue LED blink and subsequent input of registered input within a certain time opens the door.

Access Through 1:1 Authentication

Open the door by inputting the fingerprint or PIN after ID input.

1:1 Authentication Mode	ID Input	Authentication Method
Fingerprint or PIN	Enter ID or use the card	Fingerprint authentication or PIN entry
Fingerprint	Enter ID or use the card	Fingerprint authentication
PIN	Enter ID or use the card	PIN entry
Card only	Card authentication	
Fingerprint and PIN	Enter ID or use the card	PIN entry after fingerprint authentication

1. When 1:1 authentication mode is set to fingerprint

- Fingerprint input opens the door.

2. When 1:1 authentication mode is set to PIN.

- PIN entry opens the door.

3. When 1:1 authentication mode is set to fingerprint or PIN

- Fingerprint or PIN input opens the door.

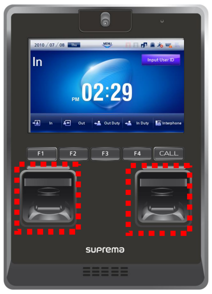
4. When using an RF card in 1:1 authentication

- When 1:1 authentication mode is set to 'Card Only', authentication is performed without fingerprint or PIN input.
- When 1:1 authentication mode is not set to 'Card Only', the card plays the role of ID input, and a fingerprint or PIN is required for authentication.

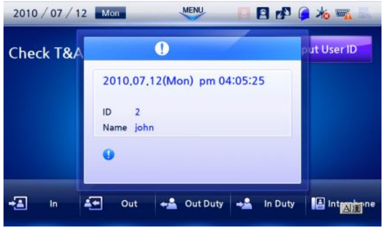
Fingerprint Authentication

In 1:N recognition mode, a fingerprint opens the door.

1. Place a finger on a sensor.



2. Successful authentication opens the door and the confirmation window pops up on the screen.



2010,07,12(Mon) pm 04:05:25

ID 2

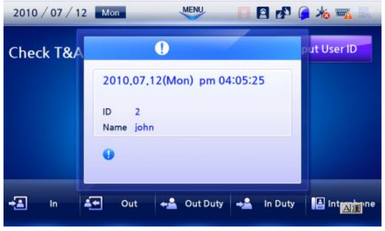
Name john

Card Recognition

Card recognition is used in ‘Card Only’ authentication mode.

1. Put the card close to the sensor.

2. Successful authentication opens the door and the confirmation window pops up on the screen.



2010,07,12(Mon) pm 04:05:25

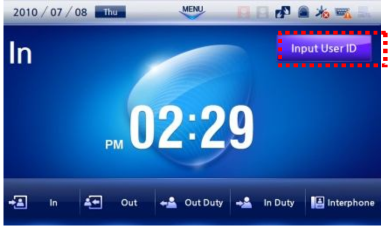
ID 2

Name john

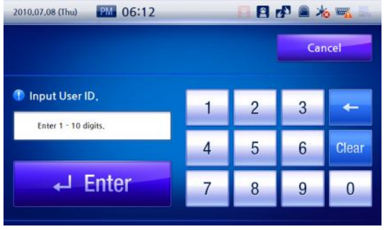
ID + Fingerprint Input

In 1:1 authentication mode, first enter ID and then input a fingerprint to open the door.

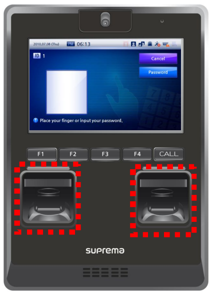
1. Press [Input User ID] on the start-up screen.



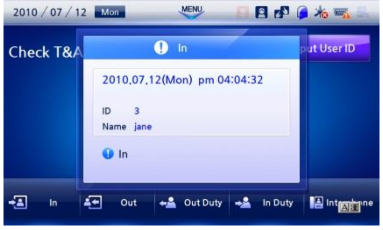
2. Enter ID with the number keys on the ID input screen shown on the right, and then press [Enter].



3. Place the finger on the sensor.



4. Successful authentication opens the door and the confirmation window pops up on the screen.



2010.07.12(Mon) pm 04:04:32

ID 3

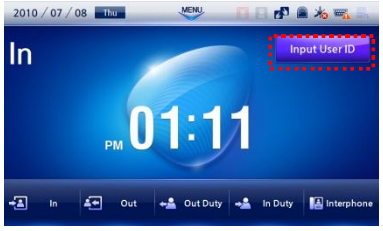
Name jane

In

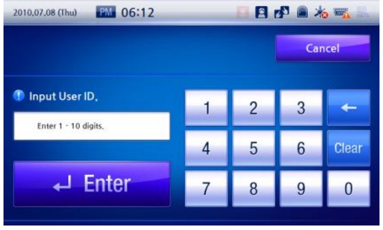
ID + PIN Input

In 1:1 authentication mode, first enter ID, and then PIN to open the door.

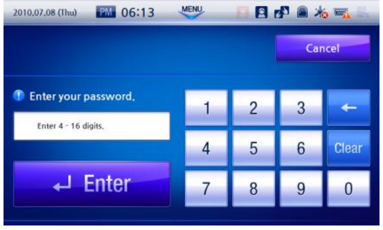
1. On the start-up screen, press [Input User ID].



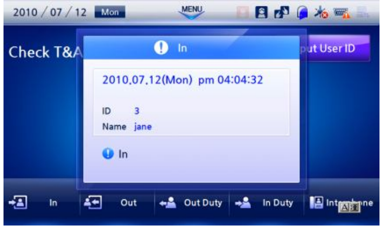
2. Enter ID with the number keys on the ID input screen shown on the right, and then press [Enter].



3. Enter PIN with the number keys on the screen, and press [Enter].



4. Successful authentication opens the door and the confirmation window pops up on the screen.



In

2010.07.12(Mon) pm 04:04:32

ID 3

Name jane

In

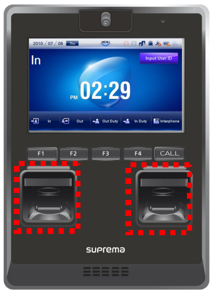
Face Fusion Recognition

Face Fusion Recognition is supported only in 1:N authentication mode.

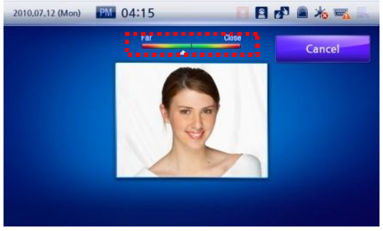
Face recognition alone does not support user authentication. It is used as a complement to fingerprint authentication in the fusion method.

Face fusion recognition is possible when the sensor is set to high speed and fusion mode, but not possible when the sensor is in twin mode. (Refer to page 39 ‘Setting Authentication Mode’.)

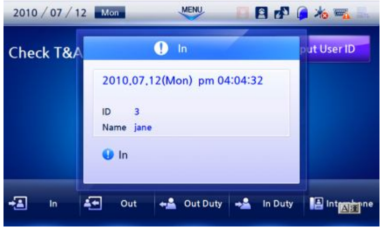
1. Put the finger on a sensor.



2. Face recognition screens such as the one on the right appear only when fingerprint recognition fails. Adjust the distance to the camera so that the arrow comes to the center of the gauge.



3. Successful face recognition opens the door and the confirmation window pops up on the screen.


2010 / 07 / 12 Mon

Check T&A

In

2010.07.12(Mon) pm 04:04:32

ID 3

Name jane

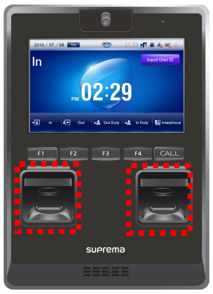
In

Forced Face Detection

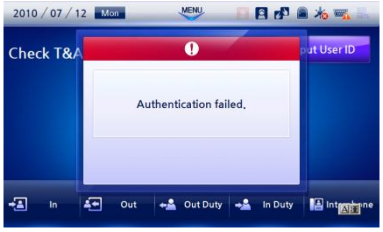
When forced face detection is on, the face image is forcibly taken in a successful authentication case and stored as a log.

If the face image is not stored properly, the door will not open.

1. Put the finger on a sensor.

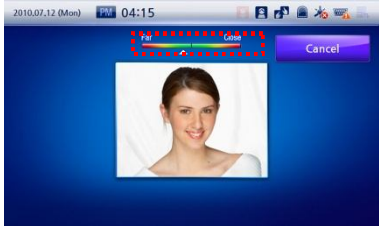


2. If the fingerprint authentication fails, the confirmation (of failed authentication) window pops up.

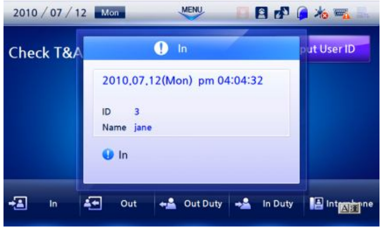


Authentication failed.

3. The face image store window pops up if the authentication is successful. Adjust the distance from the camera so that the arrow comes to the center of the gauge.



4. When storing the face image is complete, the confirmation window pops up and the door opens.



In

2010.07.12(Mon) pm 04:04:32

ID 3

Name jane

In

4. 2 Time and Attendance Management

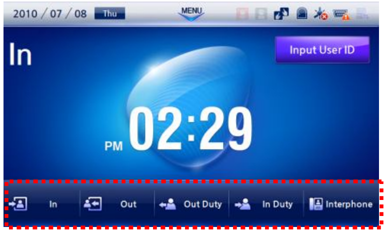
Manage Time and Attendance using 1:N fingerprint recognition or 1:1 authentication.

Time and Attendance Management using 1:N fingerprint recognition

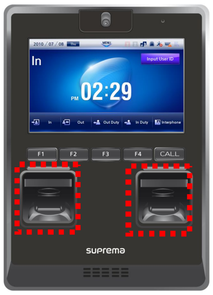
You can search for a matching fingerprint in the stored fingerprint DB when only a fingerprint is input without ID. Press one of F1 to F4 keys and input a registered fingerprint within a certain time, and the time and attendance event set for the user is applied.

If the door open event is set for an applicable T&A event, or an applicable T&A event is set for the door to open, the T&A event is applied and the door opens.

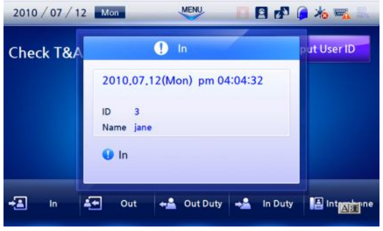
1. Select among [In / Out / Out Duty / In Duty] on the start-up screen, or one of F1 to F4 keys on the terminal.



2. Put the finger on the sensor.



3. Successful authentication opens the door and the confirmation window pops up on the screen.



In

2010.07.12(Mon) pm 04:04:32

ID 3

Name jane

In

Note

To set the door open function on a T&A event, use the BioStar program on a PC.

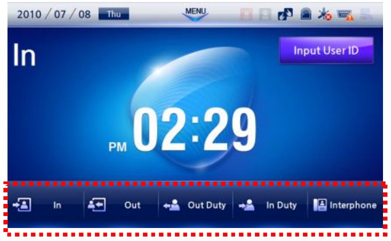
Time and Attendance Management through 1:1 Authentication

Input ID first, followed by the corresponding PIN or fingerprints. The device compares the stored information and input information.

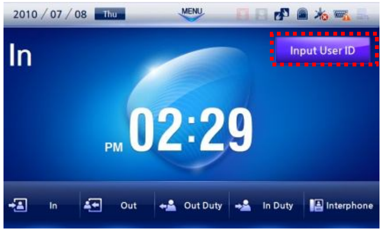
When 1:1 authentication mode is set to ‘Card Only’, authentication is performed through the card without fingerprint or PIN input.

When 1:1 authentication mode is not set to ‘Card Only’, the card plays the role of ID input, and a fingerprint or PIN is required for authentication.

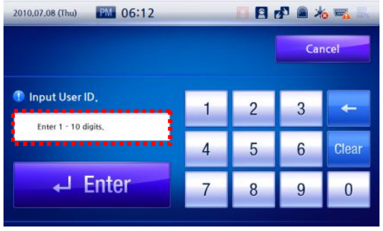
1. Select among [In / Out / Out Duty / In Duty] on the start-up screen, or one of F1 to F4 keys on the terminal.



2. Press [Input User ID] on the start-up screen.



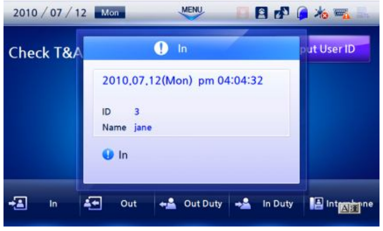
3. Enter ID with the number keys on the ID input screen shown on the right, and then press [Enter].



Input User ID.

Enter 1 - 10 digits.

4. If authentication is successful, whether by fingerprint or PIN, the T&A pop-up appears.



In

2010.07.12(Mon) pm 04:04:32

ID 3

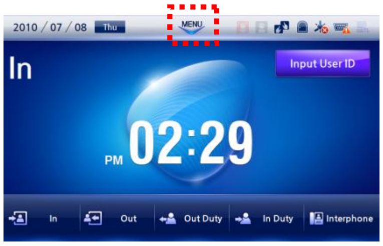
Name jane

In

Checking Users' Access / T&A Record

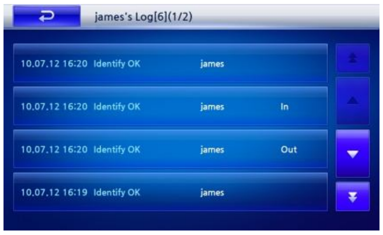
Inputting a user's fingerprint shows them their own record of access, and time and attendance.

1. Press the Menu button (MENU) on the start-up screen.



2. Perform user authentication with a fingerprint or the card.

3. Successful authentication shows his / her logs on the screen.



james's Log[6](1/2)

10.07.12 16:20 Identify OK james

10.07.12 16:20 Identify OK james In

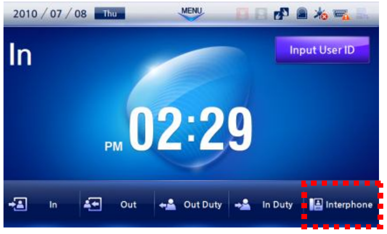
10.07.12 16:20 Identify OK james Out

10.07.12 16:19 Identify OK james

4.3 Interphone Use

Make a call to the administrator with the terminal's interphone function.

1. Press [Interphone] on the start-up screen or the [CALL] button on the terminal.



or

2. Use the terminal's microphone and speaker.

Chapter 5. Appendix

5.1 Troubleshooting

Symptoms	Suggestions
Fingerprint input fails or takes too long.	• Check if the finger or the sensor is stained with dust, dirt, sweat or any liquid. • Try again after wiping the finger and the sensor clean. • If the fingerprint is too dry, blow on it before input.
Inputting the fingerprint is OK but authentication fails repeatedly.	• Check if the user is restricted by access group or access time conditions. • Check with the administrator if the fingerprint is registered.
The card does not register.	• Check if the authentication mode is set [Card Use]. • Confirm that the card is compatible with the device before trying again.
Face recognition fails.	• During the face image authentication, have the face area from forehead to jaw fit into the screen.
Authentication is successful but the door does not open.	• Check if the time is within the time period set for closed hours. • Check the door open event on the Admin menu. If it is set to 'Disabled' or 'Selected T&A Event', the door may not open.
The LCD screen does not respond to touch.	• If the LCD screen and the blue LED are not lit, the power may be off. Check the power supply. • If it is a temporary technical problem, pressing the reset button on the bottom of the device will solve it. If resetting does not solve the problem, contact the retailer for assistance.
Some keys are not entered or the device is unstable.	• If the device is unstable for any reason, press the reset button on the bottom of the device. • If resetting does not solve the problem, contact the retailer for assistance.

5.2 Product Specifications

Item	Specification	
Sensor	Optical fingerprint sensor x 2 Face recognition camera	
Matching Speed (1:N)	1:10,000 < 1 sec)	
Card Options	13.56 MHz ISO 14443 A/B (MIFARE)	
Capacity	Template Capacity	400,000 (1:1) 20,000 (1:N)
	Max. User	200,000
	Log Capacity	1,000,000
Interfaces	Communication Interfaces	Wireless LAN TCP/IP RS485 x 2ch, RS232 USB (Slave)
	Wiegand	IN & OUT
	TTL I/O	4 inputs
	Built-in Relay	2
	Memory Slot	USB host, Micro SD Card
Hardware	CPU	667MHz RISC x 1 400MHz DSP x 2
	Memory	1GB flash + 256MB RAM (with SD card slot)
	LCD Display	5.0" WVGA touch screen
	LED Indicator	Multi-color x 2
	Sound Indication	18-bit Hi-Fi sound
	Voice Instruction	18-bit Hi-Fi sound
	Operating Temperature	-20℃ ~ 50℃
	Humidity	90%
	Tamper	Accelerometer, switch
	Operating Voltage	12V DC
	Dimensions	148mm(W) x 204mm(H) x 48mm(D)

5.3 Electrical Specification

	Min.	Typ.	Max.	Notes
Power				
Voltage (V)	10.8	12	13.2	Use regulated DC power adaptor only
Current (mA)	-		1500	
Switch Input				
VIH (V)	-	TBD	-	
VIL (V)	-	TBD		
Pull-up resistance (Ω)	-	4.7K	-	The input ports are pulled up with 4.7KΩ resistors
Wiegand Output				
VOH (V)	-	5	-	
VOL (V)	-	0.8	-	
Pull-up resistance (Ω)	-	4.7K	-	
Relay				
Switching capacity (A)	-	-	2 0.3	30V DC 125V AC
Switching power (resistive)	-	-	30W 37.5VA	DC AC
Switching voltage (V)	-	-	220 250	DC AC

5.4 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

5.5 License

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.

Suprema Inc.

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

TEL : 82-31-710-2400
FAX : 82-31-783-4506

Online Customer Support : support@supremainc.com
Company Website : www.supremainc.com

The specifications and functions of D-Station are subject to change without prior notice for continuous function or quality improvement. For more information on the product, contact Suprema Inc.