iomo

Workplace Intelligence

USER MANUAL

FCA-3000

Facial + Card + Access control

Touchless biometric facial recognition
5 Inch Touchscreen with id card scan
Fully access control system

empeo CERTIFIED

FOLLOW US
www.iomotech.com

Document Conventions

Conventions used in this manual are listed below:

GUI Conventions

For Software	
Convention	**Description**
Bold font	Used to identify software interface names e.g. **OK**, **Confirm**, **Cancel**
>	Multi-level menus are separated by these brackets. For example, File > Create > Folder.
Convention	**Description**
< >	Button or key names for devices. For example, press <OK>
[ ]	Window names, menu items, data table, and field names are inside square brackets. For example, pop up the [New User] window
/	Multi-level menus are separated by forwarding slashes. For example, [File/Create/Folder].

Symbols

Convention	Description
	This implies about the notice or pays attention to, in the manual
	The general information which helps in performing the operations faster
	The information which is significant
	Care taken to avoid danger or mistakes
	The statement or event that warns of something or that serves as a cautionary example.

Table of Contents

1 Safety Measures

The below instructions intend to ensure that the user can use the product correctly to avoid danger or property loss. The following precautions are to keep users safe and prevent any damage. Please read carefully before installation.

⚠ Noncompliance with instructions could lead to product damage or physical injury (may even cause death).

1. **Read**, **follow**, **and retain instructions** - All safety and operational instructions must be properly read and followed before bringing the device into service.
2. **Do not ignore warnings** - Adhere to all warnings on the unit and in the operating instructions.
3. **Accessories** - Use only manufacturer-recommended or product-sold accessories. Please do not use any other components other than manufacturer suggested materials.
4. **Precautions for the installation** – Do not place this device on an unstable stand or frame. It may fall and cause serious injury to persons and damage to the device.
5. **Service** - Do not try to service this unit yourself. Opening or removing covers may expose you to hazardous voltages or other hazards.
6. **Damage requiring service** - Disconnect the system from the Mains AC or DC power source and refer service personnel under the following conditions:
    - When cord or connection control is affected.
    - When the liquid spilled or an item dropped into the system.
    - If exposed to water or due to inclement weather (rain, snow, and more).
    - And if the system is not operating normally, under operating instructions.

    Just change controls defined in operating instructions. Improper adjustment of the controls may result in damage and involve a qualified technician to return the device to normal operation.

    And do not connect multiple devices to one power adapter as adapter overload can cause over-heat or fire hazard.
7. **Replacement parts** - When replacement parts are needed, service technicians must only use replacement parts provided by the supplier. Unauthorized substitutes can result in a burn, shock, or other hazards.
8. **Safety check** - On completion of service or repair work on the unit, ask the service technician to perform safety checks to ensure proper operation of the device.
9. **Power sources** - Operate the system only from the label's power source form. If the sort of power supply to use is unclear, call your dealer.

10. **Lightning** - Can install external lightning conductors to protect against electrical storms. It stops power-ups from destroying the system.

    Recommended installing the devices in areas with limited access.

Electrical Safety

- Before connecting an external cable to the device, complete grounding properly, and set up surge protection; otherwise, static electricity will damage the mainboard.
- Please make sure that the power has been disconnected before you wire, install, or dismantle the device.
- Ensure that the signal connected to the device is a weak-current (switch) signal; otherwise, components of the device will get damaged.
- Ensure that the standard voltage applicable in your country or region is applied. If you are not sure about the endorsed standard voltage, please consult your local electric power company. Power mismatch may cause a short circuit or device damage.
- In the case of power supply damage, return the device to the professional technical personnel or your dealer for handling.
- To avoid interference, keep the device far from high electromagnetic radiation devices, such as generators (including electric generators), radios, televisions, (especially CRT) monitors, or speakers.

Operation Safety

- If smoke, odor, or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.
- Transportation and other unpredictable causes may damage the device hardware. Check whether the device has any intense damage before installation.
- If the device has major defects that you cannot solve, contact your dealer as soon as possible.
- Dust, moisture, and abrupt temperature changes can affect the device's service life. You are advised not to keep the device under such conditions.
- Do not keep the device in a place that vibrates. Handle the device with care. Do not place heavy objects on top of the device.
- Do not apply rosin, alcohol, benzene, pesticides, and other volatile substances that may damage the device enclosure. Clean the device accessories with a piece of soft cloth or a small amount of cleaning agent.
- If you have any technical questions regarding usage, contact certified or experienced technical personnel.

Note

- Make sure whether the positive polarity and negative polarity of the DC 12V power supply is connected correctly. A reverse connection may damage the device. It is not advisable to connect the AC 24V power supply to the DC 12V input port.
- Make sure to connect the wires following the positive polarity and negative polarity shown on the device's nameplate.
- The warranty service does not cover accidental damage, damage caused by mis-operation, and damage due to independent installation or repair of the product by the user.

2 Overview

FCA-6000 uses **Facial Recognition** algorithms and the latest **Computer Vision Technology**. It supports both facial and palm verification with large capacity and speedy recognition, as well as improves security performance in all aspects.

It adopts touchless recognition technology and new functions namely **Masked Individual Identification** which eliminates hygiene concerns effectively. It is also equipped with the ultimate **Ant Spoofing** algorithm for facial recognition against almost all types of fake photos and videos attack. It has 3-in-1 palm recognition (Palm Shape, Palm Print, and Palm Vein) is performed in 0.35 sec per hand; the palm data acquired is compared with a maximum of 3,000 palm templates.

The terminal with temperature and mask detection is a perfect device to help reduce the spread of germs and help prevent infections at each access point of any premises and public areas such as hospitals, factories, schools, commercial buildings, stations during the recent global public health issue with its fast and accurate body temperature measurement and masked individual identification functions during facial and palm verification.

Features

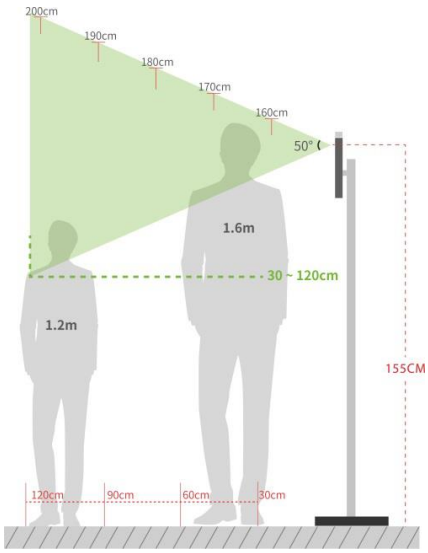
- Visible Light Facial Recognition.
- Better hygiene with touchless biometric authentication, temperature detection and masked individual identification.
- Anti-spoofing algorithm against print attack (laser, color and B/W photos), videos attack and 3D mask attack.
- Multiple Verification Methods: **Face / Palm / Password / Card**

3 Instruction for Use

Before getting into the Device features and its functions, it is recommended to be familiar to the below fundamentals.

3.1 Standing Position, Posture and Facial Expression

- **The recommended distance**



The distance between the device and a user whose height is in a range of 1.55m-1.85m is recommended to be 0.3-2.5m. Users may slightly move forward or backward to improve the quality of facial images captured.

- **Recommended Standing Posture and Facial Expression**

Standing Posture

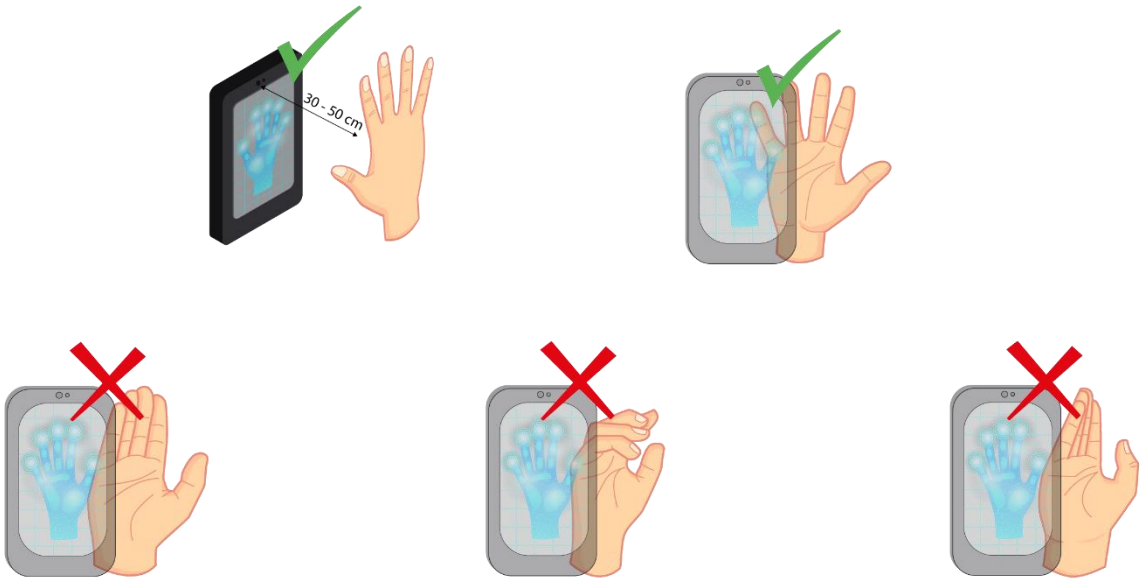
Facial Expression

NOTE: Please keep your facial expression and standing posture natural while enrolment or verification.

3.2 Palm Registration

Place your palm in the palm multi-mode collection area, such that the palm is placed parallel to the device.

Make sure to keep space between your fingers.



NOTE: Place your palm within 30-50cm of the device.

3.3 Face Registration

Try to keep the face in the centre of the screen during registration. Please face towards the camera and stay still during face registration. The screen should look like this:

Correct face registration and authentication method

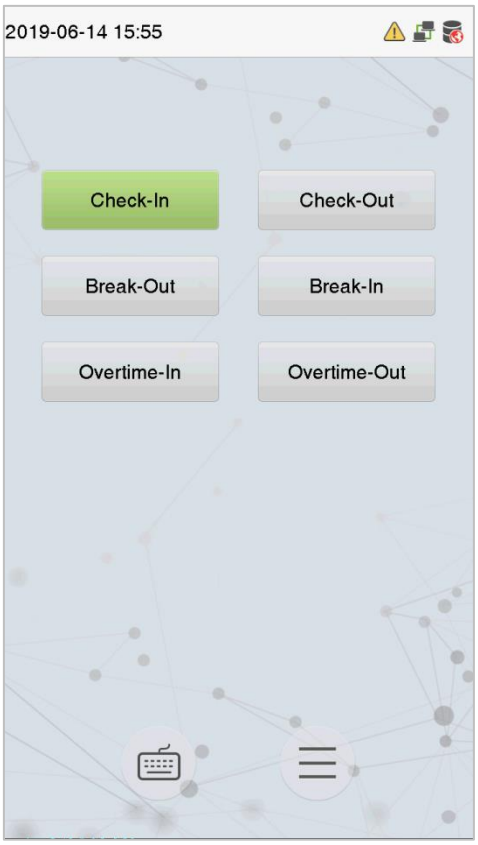
- **Recommendation for registering a face**
  - When registering a face, maintain a distance of 40cm to 80cm between the device and the face.
  - Be careful not to change your facial expression. (smiling face, drawn face, wink, etc.)
  - If you do not follow the instructions on the screen, the face registration may take longer or may fail.
  - Be careful not to cover the eyes or eyebrows.
  - Do not wear hats, masks, sunglasses, or eyeglasses.
  - Be careful not to display two faces on the screen. Register one person at a time.
  - It is recommended for a user wearing glasses to register both faces with and without glasses.

- **Recommendation for authenticating a face**
  - Ensure that the face appears inside the guideline displayed on the screen of the device.
  - If the glasses have been changed, authentication may fail. If the face without glasses has been registered, authenticate the face without glasses further. If the face with glasses has been registered, authenticate the face with the previously worn glasses.
  - If a part of the face is covered with a hat, a mask, an eye patch, or sunglasses, authentication may fail. Do not cover the face, allow the device to recognize both the eyebrows and the face.

3.4 Standby Interface

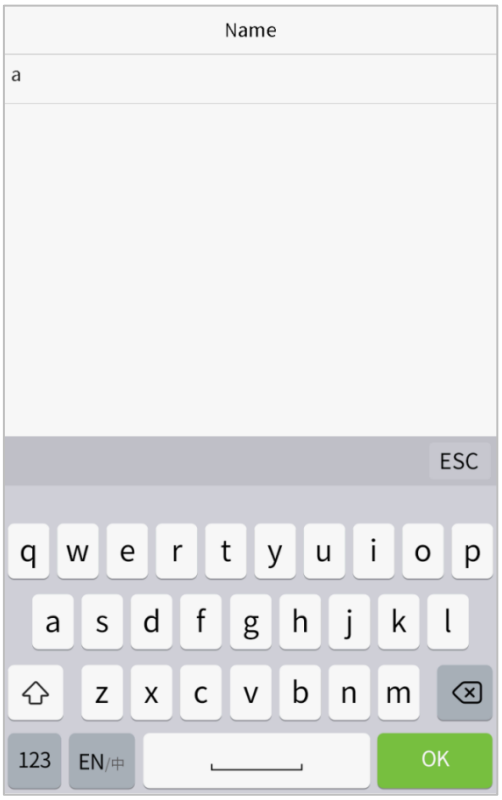
After connecting the power supply, the following standby interface is displayed:

- Click  to enter the User ID input interface.
- When there is no Super Administrator set in the device, tap  to go to the menu.
- After setting the Super Administrator on the device, it requires the Super Administrator's verification before entering the menu functions.
  NOTE: For the security of the device, it is recommended to register super administrator the first time you use the device.
- The punch state options can also be displayed and used directly on the standby interface. Click anywhere on the screen apart from the icons, and six shortcut keys appears on the screen, as shown in the figure below:



- Press the corresponding punch state key to select your current punch state, which is displayed in green.

3.5 Virtual Keyboard



NOTE:

The device supports the input in Chinese language, English language, numbers, and symbols.

- Click [**En**] to switch to the English keyboard.
- Press [**123**] to switch to the numeric and symbolic keyboard.
- click [**ABC**] to return to the alphabetic keyboard.
- Click the input box, virtual keyboard appears.
- Click [**ESC**] to exit the virtual keyboard.

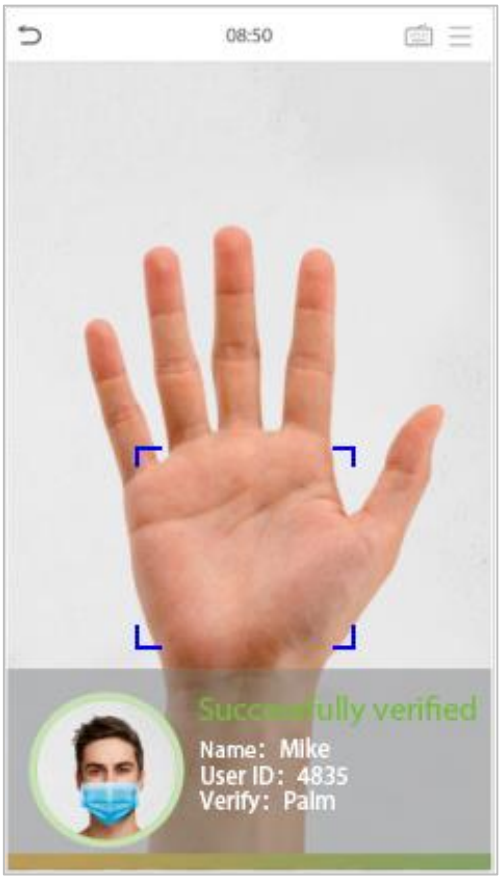
3.6 Verification Mode

3.6.1 Palm Verification

- **1: N Palm Verification mode**

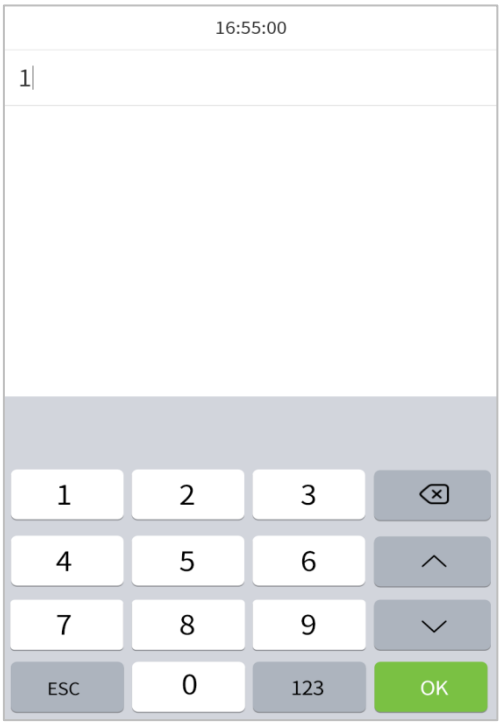
In this verification mode, the device compares the palm image collected by the palm collector with all the palm data in the device.

The device automatically distinguishes between the palm and the face verification mode as the user places his/her palm in the scanning area. Then the palm image is collected by the palm collector, and the device matches the collected palm image with all the registered palm and returns an output.



- **1: 1 Palm Verification mode**

Click the button on the main screen to enter 1:1 palm verification mode and input the user ID and press [OK], as shown in image below.



If the user has registered the fingerprint, face, and password in addition to his/her palm, and the verification method is set to palm/ fingerprint/ face/ password verification, the following screen will appear. Select the palm icon to enter palm verification mode. Then place your palm for verification.

3.6.2 Facial Verification

- **1:N Facial Verification**

1. **Conventional verification**

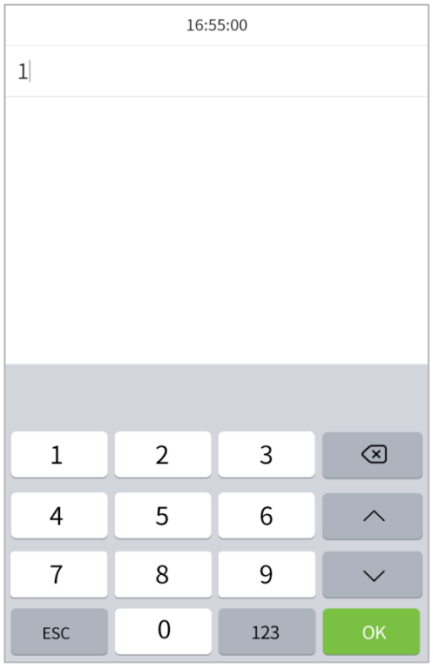
In this verification mode, the device compares the collected facial images with all face data registered in the device. The following is the pop-up prompt of a successful comparison result.

2. Enable mask detection

When the user enables the **Enable mask detection** function, the device will identify whether the user is wearing a mask or not while verification. The following are the popups of the comparison result prompt interface. (Note: This function is only applicable to products with temperature measurement module.)

- **1:1 Facial Verification**

In this verification mode, the device compares the face captured by the camera with the facial template related to the entered user ID. Press on t ain interface and enter the 1:1 facial verification mode and enter the user ID and click [**OK**].



If the user has registered palm, fingerprint, and password in addition to face, and the verification method is set to palm/ fingerprint/ face /password verification, the following screen will appear. Select the icon to ter the face verification mode.

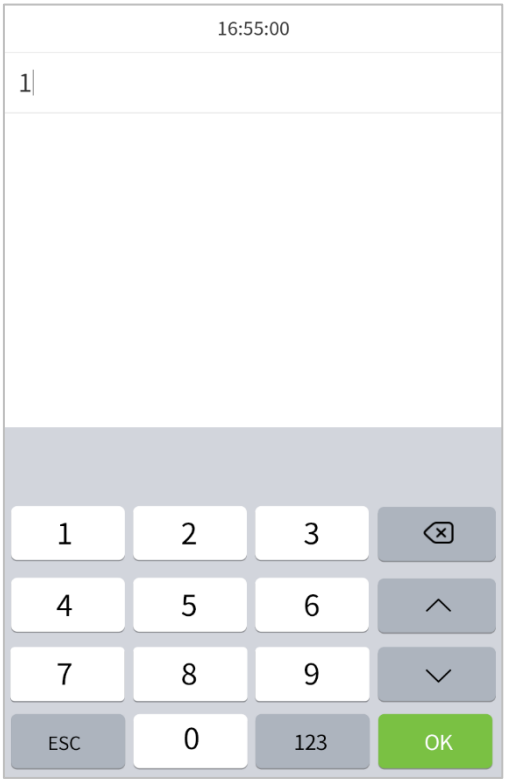
After successful verification, the prompt box displays "Successfully verified", as shown below:

If the verification is failed, it prompts “Please adjust your position!”.

3.6.3 Password Verification

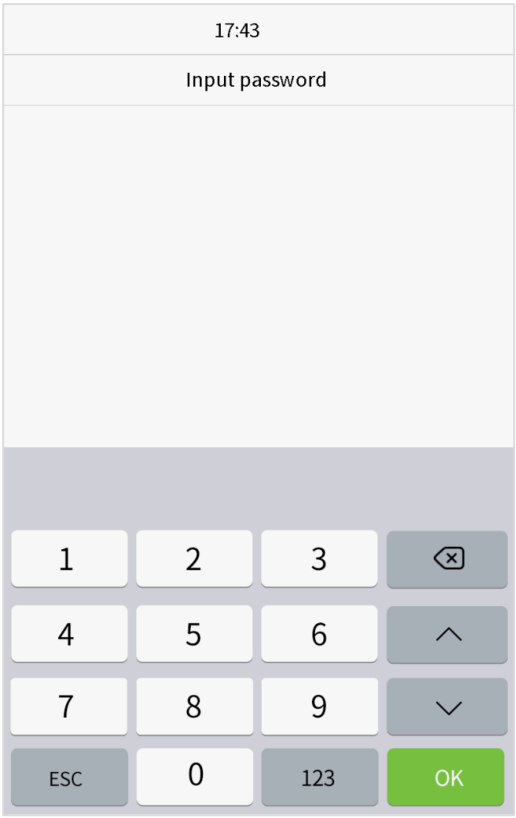
The device compares the entered password with the registered password by the given User ID.

Click the button on the main screen to enter the 1:1 password verification mode. Then, input the user ID and press [**OK**].



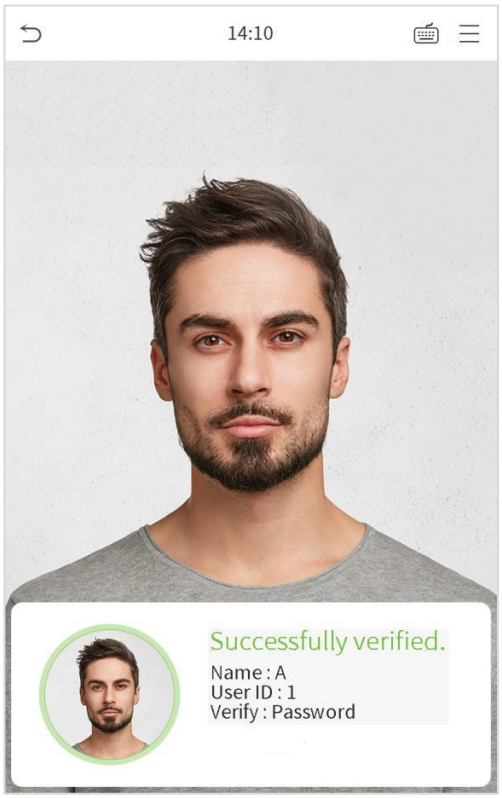
If the user has registered palm, fingerprint, and face in addition to password, and the verification method is set to palm/ fingerprint/ face /password verification, the following screen will appear. Select the icon  to enter password verification mode.

Input the password and press [**OK]**.

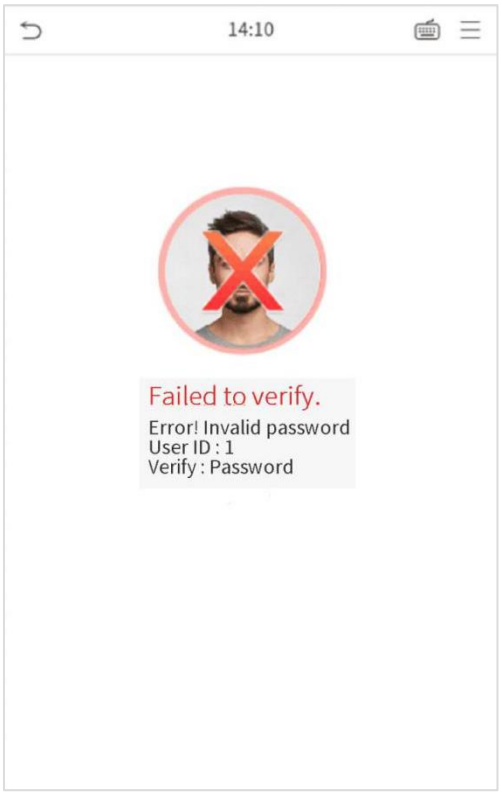


Following are the display screen after a inputting a correct password and a wrong password respectively.

Verification is successful:



Verification is failed:

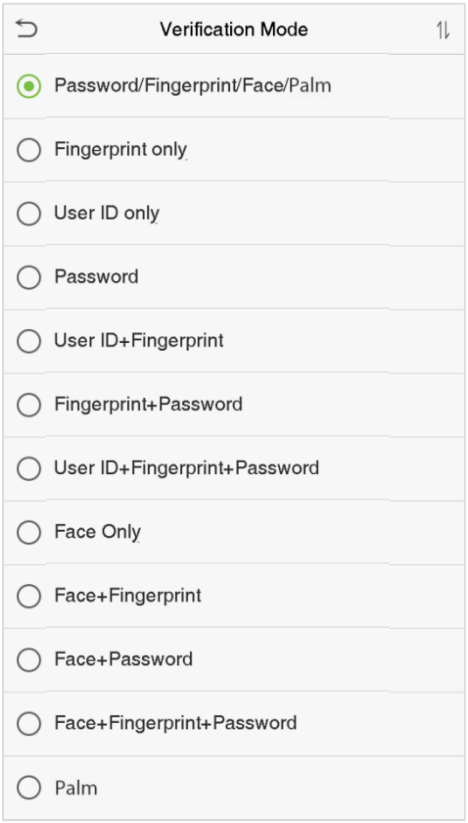


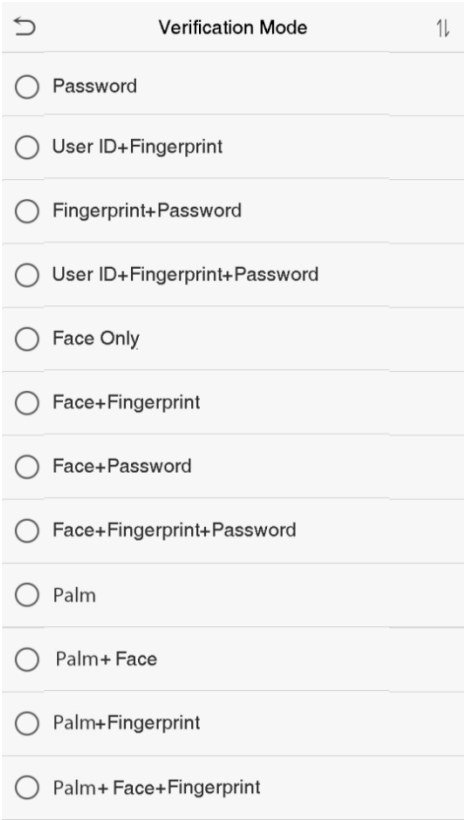
3.6.4 Combined Verification

To increase security, this device offers the option of using multiple forms of verification methods. A total of 15 different verification combinations can be used, as shown below:

Combined Verification Symbol Definition

Symbol	Definition	Explanation
/	or	This method compares the entered verification of a person with the related verification template previously stored to that Personnel ID in the Device.
+	and	This method compares the entered verification of a person with all the verification template previously stored to that Personnel ID in the Device.





Procedure to set for Combined Verification Mode

- Combined verification requires personnel to register all the different verification method. Otherwise, employees will not be able to successfully verify the combined verification process.
- For instance, when an employee has registered only the fingerprint data, but the Device verification mode is set as "Fingerprint + Password", the employee will not be able to complete the verification process successfully.
- This is because the Device compares the scanned fingerprint template of the person with registered verification template (both the Fingerprint and the Password) previously stored to that Personnel ID in the Device.

- But as the employee has registered only the Fingerprint but not the Password, the verification will not get completed and the Device displays “Verification Failed”.

4 Main Menu

Press n the Standby interface to enter the **Main Menu**, the following screen will be displayed:

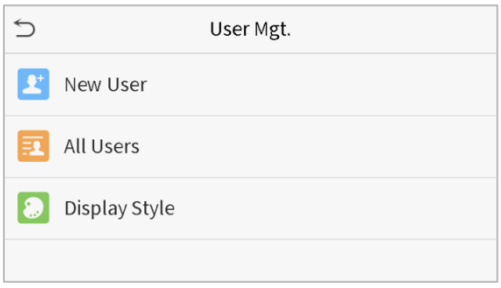
Function Description

Menu	Descriptions
User Mgt.	To Add, Edit, View, and Delete basic information of a User.
User Role	To set the permission scope of the custom role and enroller for the users, that is, the rights to operate the system.
COMM.	To set the relevant parameters of Network, Serial Comm., PC Connection, Wireless Network, Cloud Server and Wiegand.
System	To set parameters related to the system, including Date & Time, Access Logs Setting, Face, Fingerprint, and Palm parameter, Resetting to factory settings and Detection Management.
Personalize	This includes User Interface, Voice, Bell Schedules, Punch State Options and Shortcut Key Mappings settings.
Data Mgt.	To delete all relevant data in the device.
Access Control	To set the parameters of the lock and the relevant access control device including options like Time schedule, Holiday Settings, Combine verification, Anti-passback Setup, and Duress Option Settings.
Attendance Search	To query the specified Attendance record, check Attendance Photos and Blocklist attendance photos.
Autotest	To automatically test whether each module functions properly, including the LCD Screen, Audio, Camera, Fingerprint sensor, and real-time clock.
System Info	To view Data Capacity and Device and Firmware information of the current device.

5 User Management

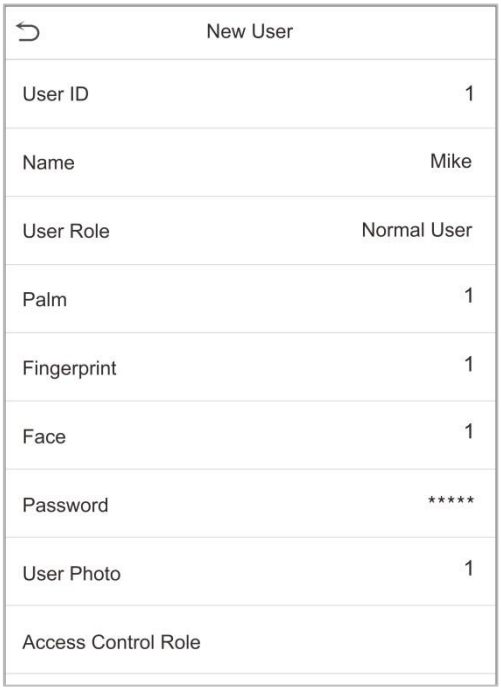
5.1 User Registration

Click **User Mgt.** on the main menu.



5.1.1 User ID and Name

Tap **New User.** Enter the **User ID** and **Name.**



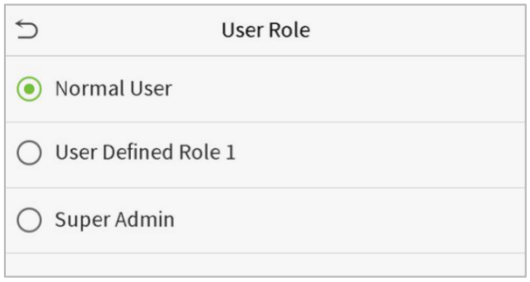
Notes:

1. A name can take up to 17 characters.
2. The user ID may contain 1-9 digits by default.
3. During the initial registration, you can modify your ID, which cannot be modified after registration.
4. If a message "**Duplicated!**" pops up, you must choose another ID as the enter User ID already exists.

5.1.2 User Role

On the New User interface, tap on **User Role** to set the role for the user as either **Normal User** or **Super Admin**.

- **Super Admin:** The Super Administrator owns all management privileges in the Device.
- **Normal User:** If the Super Admin is already registered in the Device, then the Normal Users will not have the privileges to manage the system and can only access authentication verifications.
- **User Defined Roles:** The Normal User can also be set with **User Defined Role** which are the custom roles that can be set to the Normal User.



Note: If the selected user role is the Super Admin, the user must pass the identity authentication to access the main menu. The authentication is based on the authentication method(s) that the super administrator has registered. Please refer to 3.7 Verification Method.

5.1.3 Palm

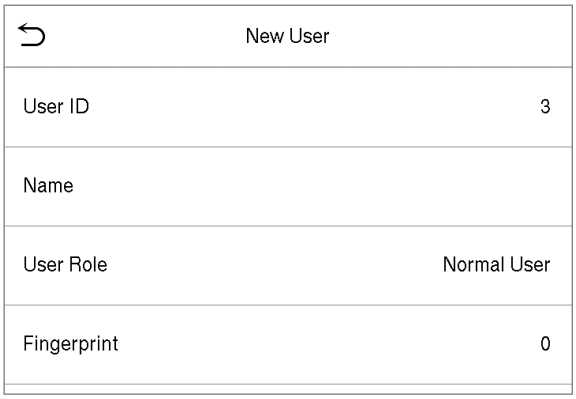
Tap **Palm** in the **New User** interface to enter the palm registration page.

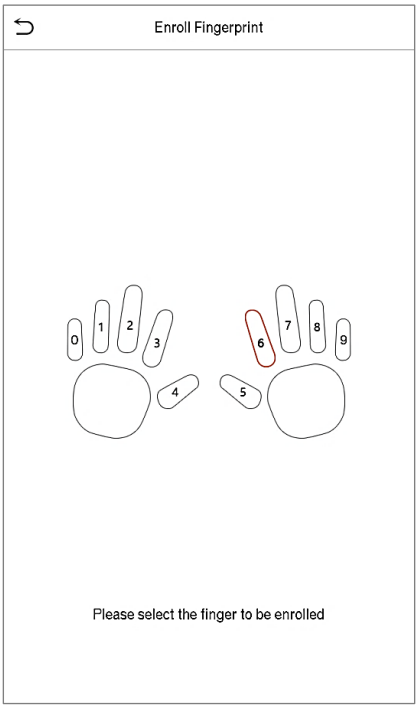
- Select the palm to be enrolled.
- Please place your palm inside the guiding box and keep it still while registering.
- A progress bar shows up while registering the palm and a **"Enrolled Successfully"** is displayed as the progress bar completes.
- If the palm is registered already then, the **"Duplicate Palm"** message shows up. The registration interface is as follows:

5.1.4 Fingerprint (Only avaiable model)

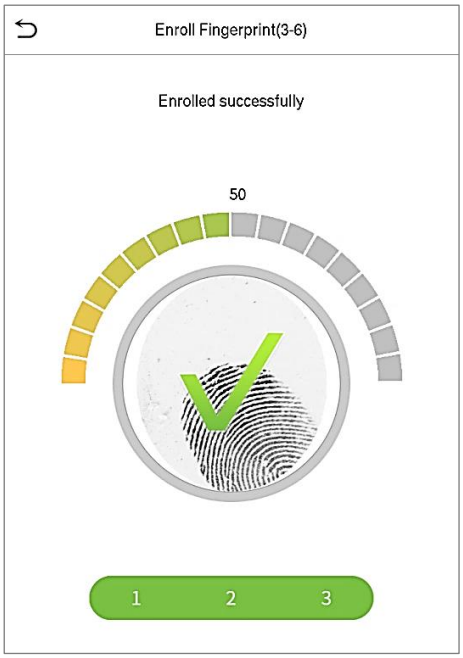
On the **New User** interface, tap on **Fingerprint** to go to the fingerprint registration page.

- On the **Enroll Fingerprint** interface, select the finger to be enrolled.





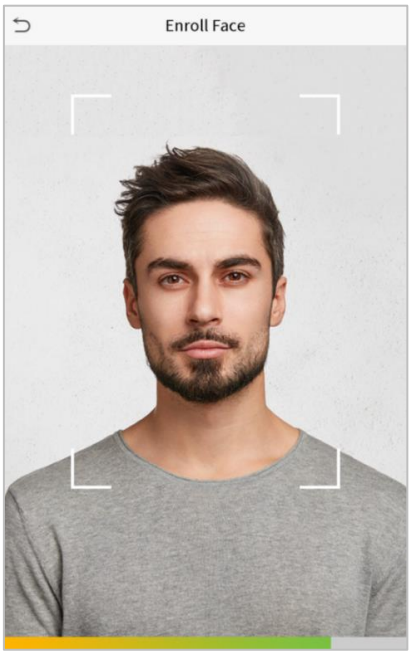
- After the selecting the required finger, press the same finger on the fingerprint reader three times.
- Green indicates that the fingerprint was enrolled successfully.



5.1.5 Face

Tap **Face** in the **New User** interface to enter the face registration page.

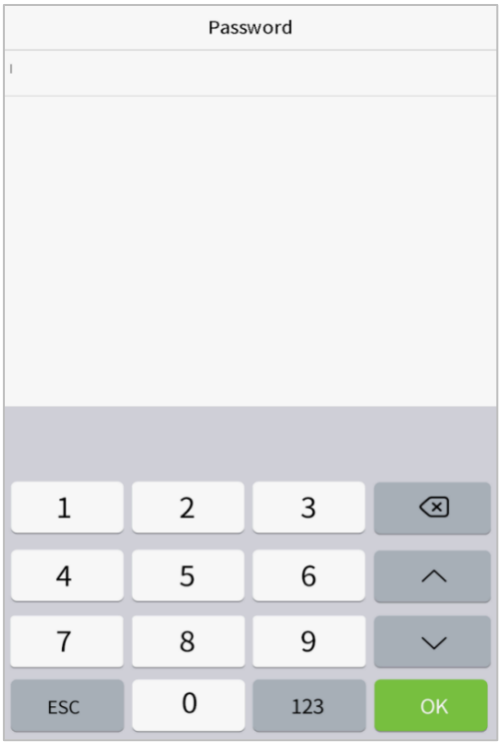
- Please face towards the camera and position your face inside the white guiding box and stay still during face registration.
- A progress bar shows up while registering the face and a **"Enrolled Successfully"** is displayed as the progress bar completes.
- If the face is registered already then the **"Duplicate Face"** message shows up. The registration interface is as follows:



5.1.6 Password

Tap **Password** in the **New User** interface to enter the password registration page.

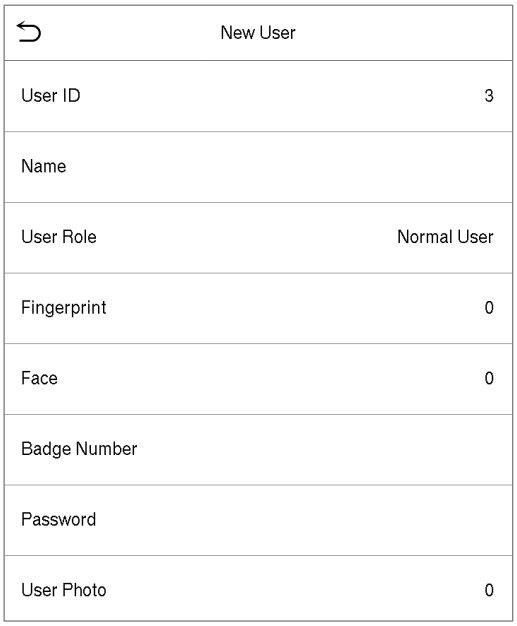
- On the Password interface, enter the required password and re-enter to confirm it and tap **OK**.
- If the re-entered password is different from the initially entered password, then the device prompts the message as "**Password not match!**", where the user needs to re-confirm the password again.



Note: The password may contain 1 to 8 digits by default.

5.1.7 User photo

Tap on **User Photo** in the **New User** interface to go to the User Photo registration page.



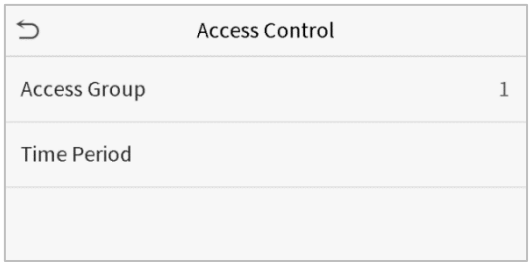
- When a user registered with a photo passes the authentication, the registered photo will be displayed.
- Tap **User Photo**, the device's camera will open, then tap the camera icon to take a photo. The captured photo is displayed on the top left corner of the screen and the camera opens up again to take a new photo, after taking the initial photo.

Note: While registering a face, the system automatically captures a picture as the user photo. If you do not register a user photo, the system automatically sets the picture captured while registration as the default photo.

5.1.8 Access Control Role

The **Access Control Role** sets the door access privilege for each user. This includes the access group, verification mode, fingerprint privilege and also facilitates to set the group access time-period.

- Tap **Access Control Role** > **Access Group**, to assign the registered users to different groups for better management. New users belong to Group 1 by default and can be reassigned to other groups. The device supports up to 99 Access Control groups.
- Tap **Time Period**, to select the time period to use.



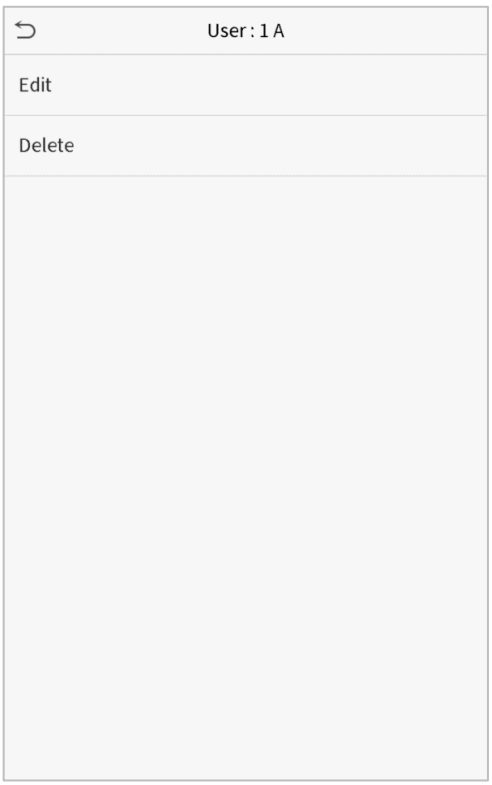
5.2 Search for Users

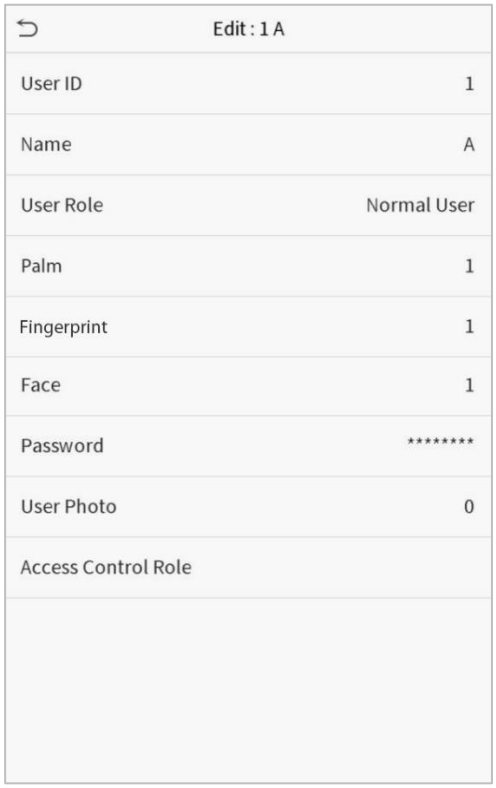
On the **Main Menu**, tap **User Mgt.,** and then tap **All Users** to search for a User.

- On the **All Users** interface, tap on the search bar on the user's list to enter the required retrieval keyword (where the keyword may be the user ID, surname or full name) and the system will search for the related user information.

5.3 Edit User

On **All Users** interface, tap on the required user from the list and tap **Edit** to edit the user information.





NOTE: The process of editing the user information is the same as that of adding a new user, except that the User ID cannot be modified when editing a user. The process in detail refers to "5.1 User Management".

5.4 Delete User

On **All Users** interface, tap on the required user from the list and tap **Delete** to delete the user or a specific user information from the device. On the **Delete** interface, tap on the required operation and then tap OK to confirm the deletion.

Delete Operations

Delete User: Deletes all the user information (deletes the selected User as a whole) from the Device.

Delete Fingerprint Only: Deletes the fingerprint information of the selected user.

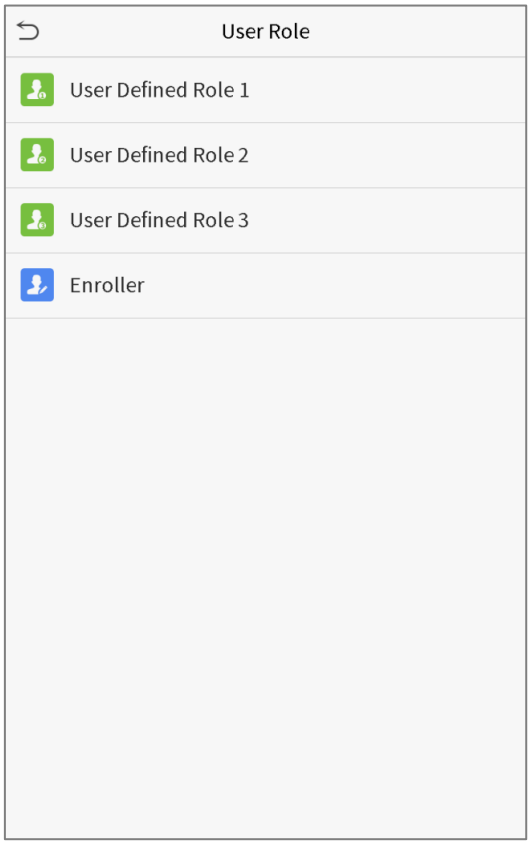
Delete Password Only: Deletes the password information of the selected user.

Delete Face Only: Deletes the Face information of the selected user.

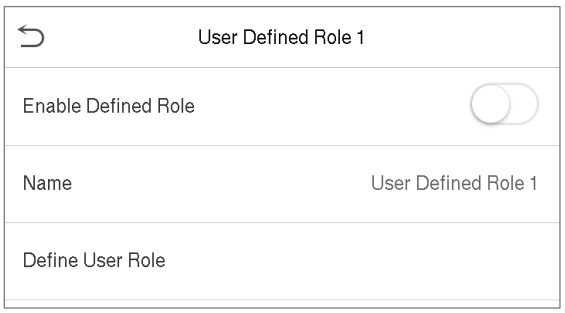
6 User Role

User Role facilitates to assign some specific permissions to certain users, based on the requirement.

- On the **Main** menu, tap **User Role**, and then tap on the **User Defined Role** to set the user defined permissions.
- The permission scope of the custom role can be set up to 3 roles, that is, the custom operating scope of the menu functions of the user.

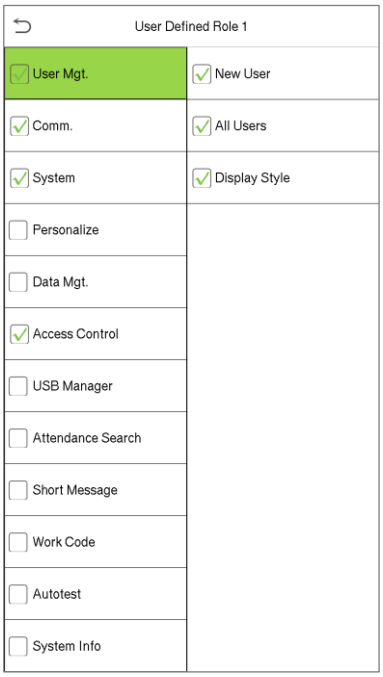


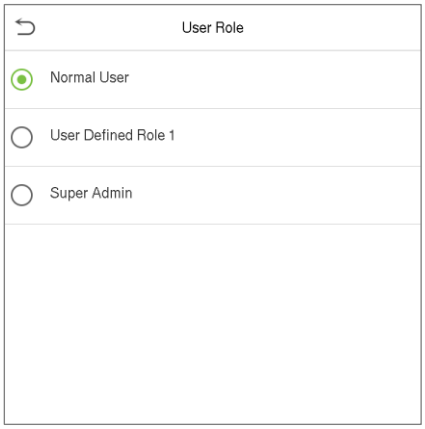
- On the **User Defined Role** interface, toggle **Enable Defined Role** to enable or disable the user defined role.
- Tap on **Name** and enter the custom name of the role.



- Then, tap on **Define User Role** and select the required privileges to assign to the new role, and then tap on the **Return** button.

- During privilege assignment, the main menu function names will be displayed on the left and its sub-menus will be listed on its right.
- First tap on the required **Main Menu** function name, and then select its required sub-menus from the list.

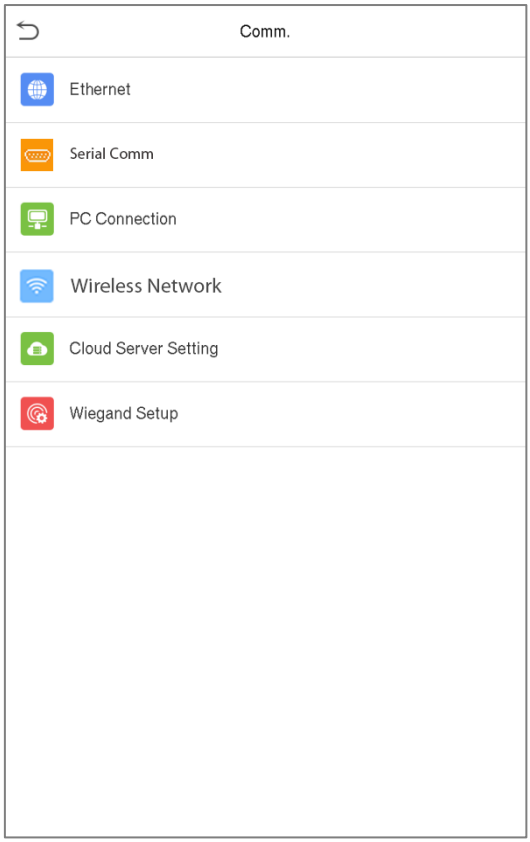




Note: If the User Role is enabled for the Device, tap on **User Mgt. > New User > User Role** to assign the created roles to the required users. But if there is no super administrator registered in the Device, then the device will prompt "Please enroll super admin first!" when enabling the User Role function.

7 Communication Settings

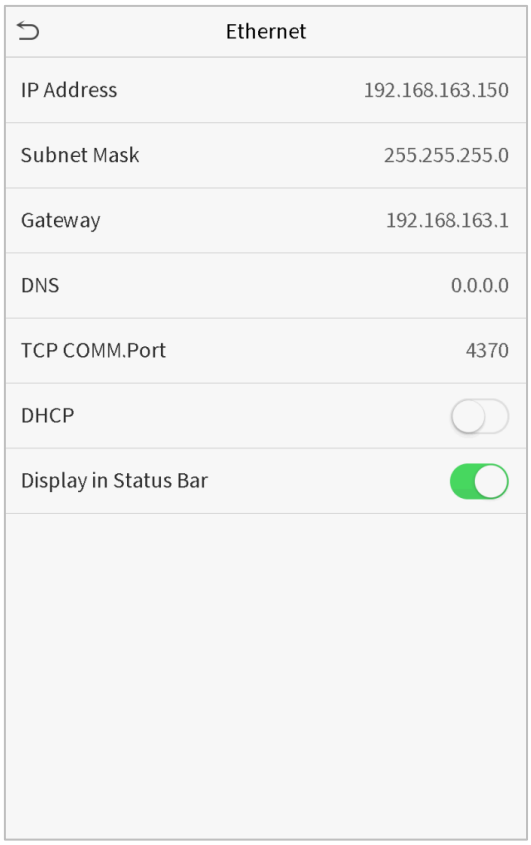
Tap **COMM.** on the **Main Menu** to set the Ethernet PC connection, Cloud Server setting and Wiegand.



7.1 Network Settings

When the device needs to communicate with a PC over the Ethernet, you need to configure network settings and ensure that the device and the PC are connecting to the same network segment.

Tap **Ethernet** on the **Comm**. Settings interface to configure the settings.



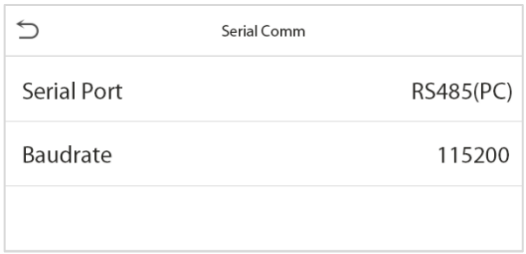
Function Description

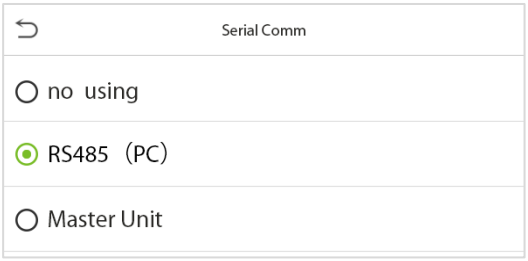
Function Name	Descriptions
IP Address	The default IP address is 192.168.1.201. It can be modified according to the network availability.
Subnet Mask	The default Subnet Mask is 255.255.255.0. It can be modified according to the network availability.
Gateway	The default Gateway address is 0.0.0.0. It can be modified according to the network availability.
DNS	The default DNS address is 0.0.0.0. It can be modified according to the network availability.
TCP COMM. Port	The default TCP COMM Port value is 4370. It can be modified according to the network availability.
DHCP	Dynamic Host Configuration Protocol is to dynamically allocate IP addresses for clients via server.
Display in Status Bar	Toggle to set whether to display the network icon on the status bar.

7.2 Serial Comm

Serial Comm function facilitates to establish communication with the device through a serial port (/RS485/ Master Unit).

Tap **Serial Comm.** on the **Comm.** Settings interface.





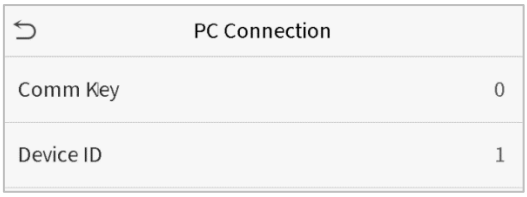
Function Description

Function Name	Descriptions
Serial Port	**Disable:** Do not communicate with the device through the serial port. **RS485(PC):** Communicates with the device through RS485 serial port. **Master Unit:** When RS485 is used as the function of "**Master unit**", the device will act as a master unit, and it can be connected to RS485 fingerprint & card reader.
Baud Rate	The rate at which the data is communicated with PC, there are 4 options of baud rate: 115200 (default), 57600, 38400, and 19200. The higher is the baud rate, the faster is the communication speed, but also the less reliable. Hence, a higher baud rate can be used when the communication distance is short; when the communication distance is long, choosing a lower baud rate would be more reliable.

7.3 PC Connection

Comm Key facilitates to improve the security of data by setting the communication between the device and the PC. Once the Comm Key is set, its connection password must be provided before the device gets connected to the PC software.

Tap **PC Connection** on the **Comm.** Settings interface to configure the communication settings.



Function Description

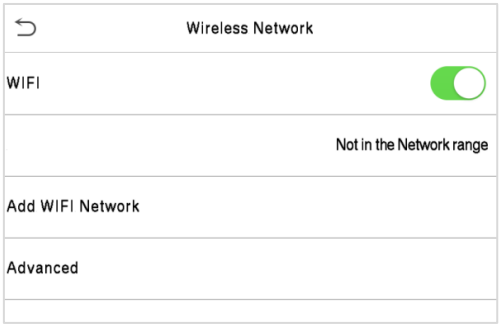
Function Name	Descriptions
Comm Key	The default password is 0, which can be changed. The Comm Key can contain1-6 digits.
Device ID	Identity number of the device, which ranges between 1 and 254. If the communication method is RS232/RS485, you need to input this device ID in the software communication interface.

7.4 Wireless Network (Only avaiable model)

The device provides a Wi-Fi module, which can be built-in within the device mould or can be externally connected.

The Wi-Fi module enables data transmission via Wi-Fi (Wireless Fidelity) and establishes a wireless network environment. Wi-Fi is enabled by default in the device. If you don't need to use the Wi-Fi network, you can toggle the Wi-Fi to disable button.

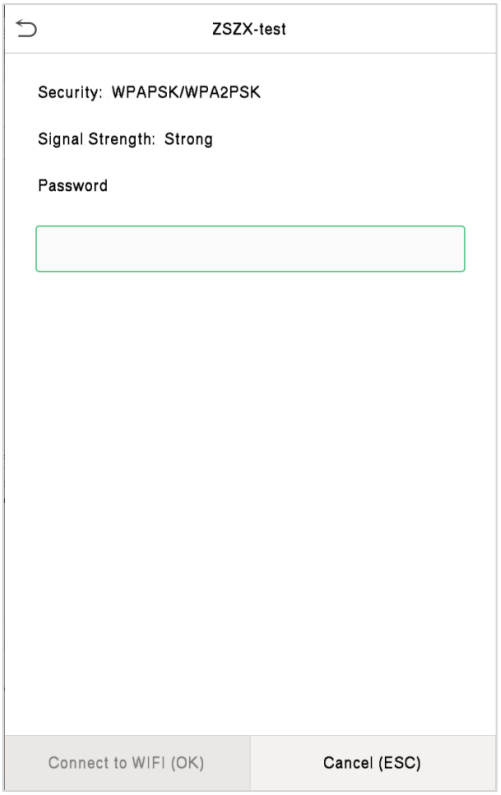
Tap **Wireless Network** on the **Comm.** Settings interface to configure the WiFi settings.



Search the WIFI Network

- WIFI is enabled in the Device by default. Toggle on button to enable or disable WIFI.
- Once the Wi-Fi is turned on, the device will search for the available WIFI within the network range.
- Tap on the appropriate WiFi name from the available list, and input the correct password in the password interface, and then tap **Connect to WIFI (OK)**.

WIFI Enabled: Tap on the required network from the searched network list.

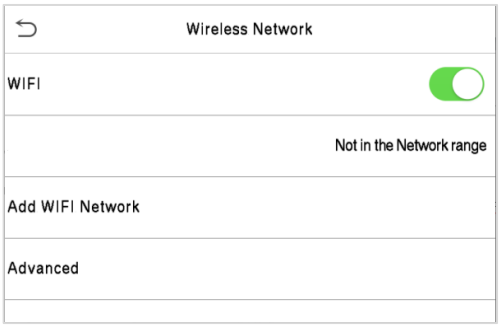


Tap on the password field to enter the password, and then tap on **Connect to WIFI (OK).**

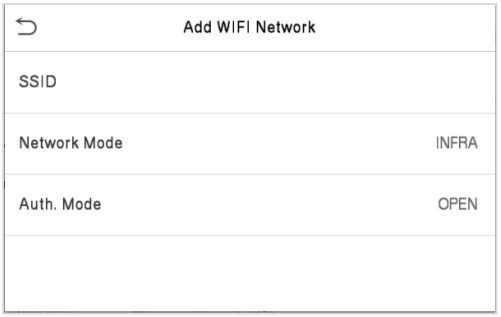
- When the WIFI is connected successfully, the initial interface will display the Wi-Fi logo.

Add WIFI Network Manually

The WIFI can also be added manually if the required WIFI is not displayed on the list.



Tap on **Add WIFI Network** to add the WIFI manually.

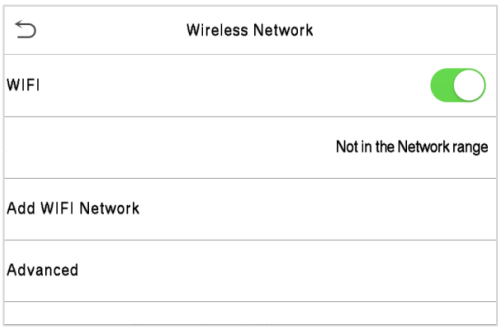


On this interface, enter the WIFI network parameters. (The added network must

NOTE: After successfully adding the WIFI manually, follow the same process to search for the added WIFI name. Click here to view the process to search the WIFI network.

Advanced Setting

On the **Wireless Network** interface , tap on **Advanced** to set the relevant parameters as required.

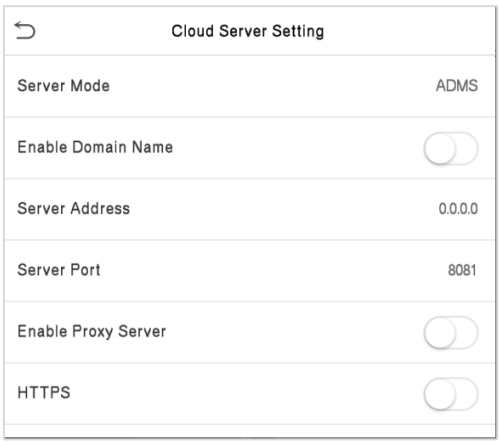


Function Description

Function Name	Description
DHCP	Dynamic Host Configuration Protocol (DHCP) dynamically allocates IP addresses to network clients. If the DHCP is enabled, then the IP cannot be set manually.
IP Address	IP address for the WIFI network, the default is 0.0.0.0. It can be modified according to the network availability.
Subnet Mask	The default Subnet Mask of the WIFI network is 255.255.255.0. It can be modified according to the network availability.
Gateway	The default Gateway address is 0.0.0.0. Can be modified according to the network availability.

7.5 Cloud Server Setting (Only avaiable model)

Tap **Cloud Server Setting** on the **Comm.** Settings interface to connect with the ADMS server.



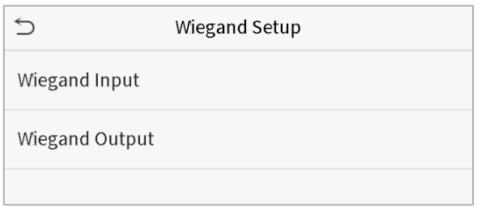
Function Description

Function Name		Description
Enable Domain Name	**Server Address**	Once this function is enabled, the domain name mode "http://..." will be used, such as http://www.XYZ.com, while "XYZ" denotes the domain name (when this mode is turned **ON**).
Disable Domain Name	**Server Address**	IP address of the ADMS server.
	Server Port	Port used by the ADMS server.
Enable Proxy Server		When you choose to enable the proxy, you need to set the IP address and port number of the proxy server.
HTTPS		Based on HTTP, transmission encryption and identity authentication ensure the security of the transmission process.

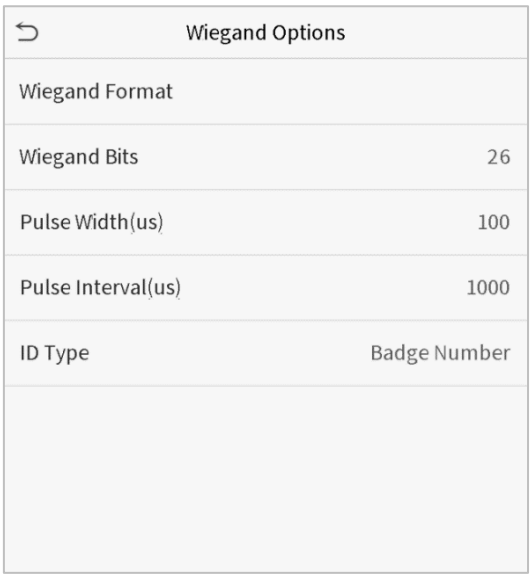
7.6 Wiegand Setup

To set the Wiegand input and output parameters.

Tap **Wiegand Setup** on the **Comm.** Settings interface to set the Wiegand input and output parameters.



7.6.1 Wiegand input



Function Description

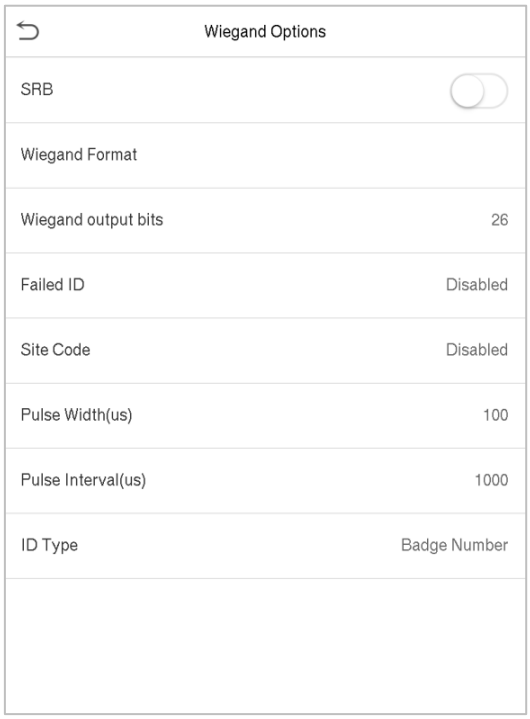
Function Name	Descriptions
Wiegand Format	Values range from 26 bits, 34 bits, 36 bits, 37 bits, and 50 bits.
Wiegand Bits	Number of bits of Wiegand data.
Pulse Width(us)	The value of the pulse width sent by Wiegand is 100 microseconds by default, which can be adjusted within the range of 20 to 100 microseconds.
Pulse Interval(us)	The default value is 1000 microseconds, which can be adjusted within the range of 200 to 20000 microseconds.
ID Type	Select between User ID and card number.

Various Common Wiegand Format Description:

Wiegand Format	Description
Wiegand26	ECCCCCCCCCCCCCCCCCCCCCCCO Consists of 26 bits of binary code. The 1st bit is the even parity bit of the 2nd to 13th bits, while the 26th bit is the odd parity bit of the 14th to 25th bits. The 2nd to 25th bits are the card numbers.
Wiegand26a	ESSSSSSSSCCCCCCCCCCCCCCCO Consists of 26 bits of binary code. The 1st bit is the even parity bit of the 2nd to 13th bits, while the 26th bit is the odd parity bit of the 14th to 25th bits. The 2nd to 9th bits are the site codes, while the 10th to 25th bits are the card numbers.
Wiegand34	ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO Consists of 34 bits of binary code. The 1st bit is the even parity bit of the 2nd to 17th bits, while the 34th bit is the odd parity bit of the 18th to 33rd bits. The 2nd to 25th bits are the card numbers.
Wiegand34a	ESSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCO Consists of 34 bits of binary code. The 1st bit is the even parity bit of the 2nd to 17th bits, while the 34th bit is the odd parity bit of the 18th to 33rd bits. The 2nd to 9th bits are the site codes, while the 10th to 25th bits are the card numbers.
Wiegand36	OFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCMME Consists of 36 bits of binary code. The 1st bit is the odd parity bit of the 2nd to 18th bits, while the 36th bit is the even parity bit of the 19th to 35th bits. The 2nd to

	17th bits are the device codes. The 18th to 33rd bits are the card numbers, and the 34th to 35th bits are the manufacturer codes.
Wiegand36a	EFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCO Consists of 36 bits of binary code. The 1st bit is the even parity bit of the 2nd to 18th bits, while the 36th bit is the odd parity bit of the 19th to 35th bits. The 2nd to 19th bits are the device codes, and the 20th to 35th bits are the card numbers.
Wiegand37	OMMMMSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCE Consists of 37 bits of binary code. The 1st bit is the odd parity bit of the 2nd to 18th bits, while the 37th bit is the even parity bit of the 19th to 36th bits. The 2nd to 4th bits are the manufacturer codes. The 5th to 16th bits are the site codes, and the 21st to 36th bits are the card numbers.
Wiegand37a	EMMMFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCCO Consists of 37 bits of binary code. The 1st bit is the even parity bit of the 2nd to 18th bits, while the 37th bit is the odd parity bit of the 19th to 36th bits. The 2nd to 4th bits are the manufacturer codes. The 5th to 14th bits are the device codes, and15th to 20th bits are the site codes, and the 21st to 36th bits are the card numbers.
Wiegand50	ESSSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO Consists of 50 bits of binary code. The 1st bit is the even parity bit of the 2nd to 25th bits, while the 50th bit is the odd parity bit of the 26th to 49th bits. The 2nd to 17th bits are the site codes, and the 18th to 49th bits are the card numbers.
"C" **denotes the card number;** "E" **denotes the even parity bit;** "O" **denotes the odd parity bit;** "F" **denotes the facility code;** "M" **denotes the manufacturer code;** "P" **denotes the parity bit; and** "S" **denotes the site code.**	

7.6.2 Wiegand output



Function Description

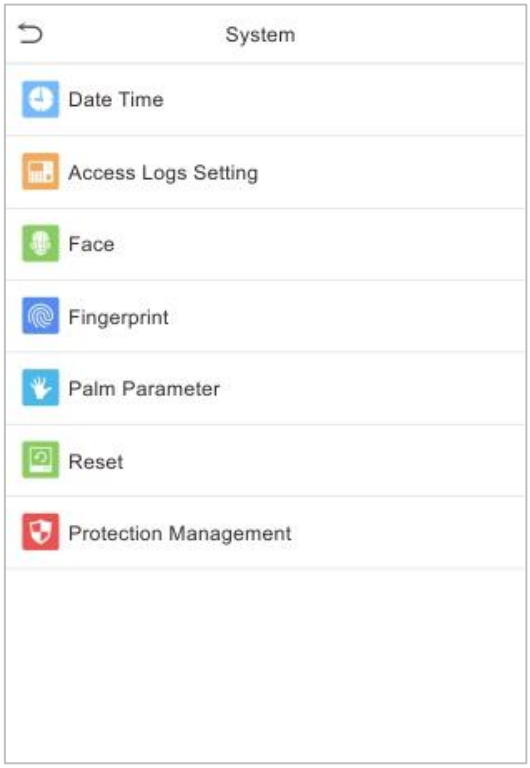
Function Name	Descriptions
SRB	When SRB is enabled, the lock is controlled by the SRB to prevent the lock from being opened due to device removal.
Wiegand Format	Values range from 26 bits, 34 bits, 36 bits, 37 bits, and 50 bits.
Wiegand output bits	After selecting the required Wiegand format, select the corresponding output bit digits of the Wiegand format.
Failed ID	If the verification is failed, the system will send the failed ID to the device and replace the card number or personnel ID with the new one.
Site Code	It is similar to the device ID. The difference is that a site code can be set manually, and is repeatable in a different device. The valid value ranges from 0 to 256 by default.

Pulse Width(us)	The time width represents the changes of the quantity of electric charge with regular high-frequency capacitance within a specified time.
Pulse Interval(us)	The time interval between pulses.
ID Type	Select the ID types as either User ID or card number.

8 System Settings

Set related system parameters to optimize the performance of the device.

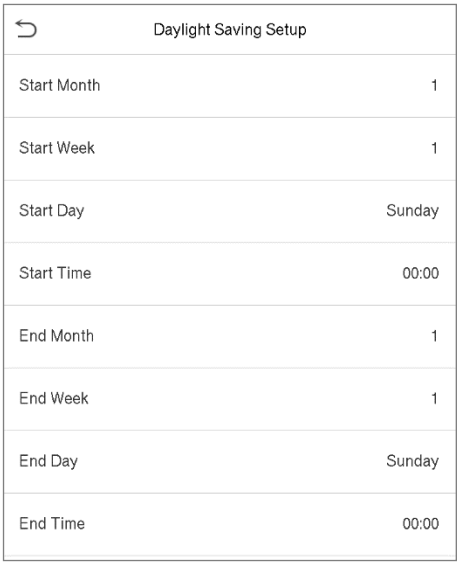
Tap **System** on the **Main Menu** interface to set the related system parameters so as to optimize the performance of the device.

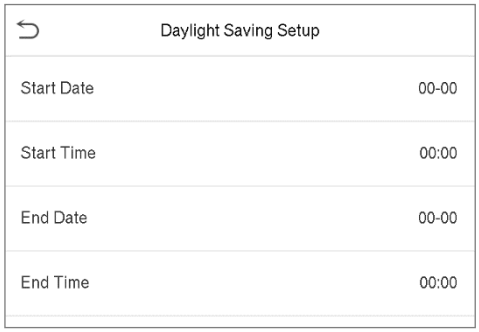


8.1 Date and Time

Tap **Date Time** on the **System** interface to set the date and time.

- Tap **Manual time setting** to manually set date and time and tap **Confirm** to save.
- Tap **24-Hour Time** to enable or disable this format. If enabled, then select the **Date Format** to set the date format.
- ★ Tap **Daylight Saving Time** to enable or disable the function. If enabled, tap **Daylight Saving Mode** to select a daylight-saving mode and then tap **Daylight Saving Setup** to set the switch time.





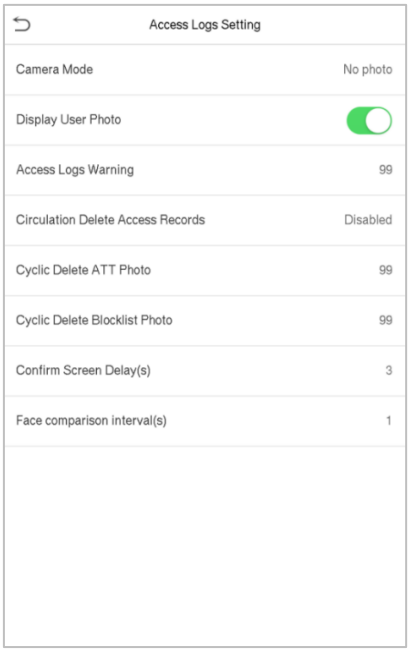
Week mode **Date mode**

- When restoring the factory settings, the time (24-hour) and date format (YYYY-MM-DD) can be restored, but the device date and time cannot be restored.

NOTE: For example, the user sets the time of the device (18:35 on March 15, 2019) to 18:30 on January 1, 2020. After restoring the factory settings, the time of the equipment will remain 18:30 on January 1, 2020.

8.2 Access Logs Setting

Click **Access Logs Setting** on the System interface.



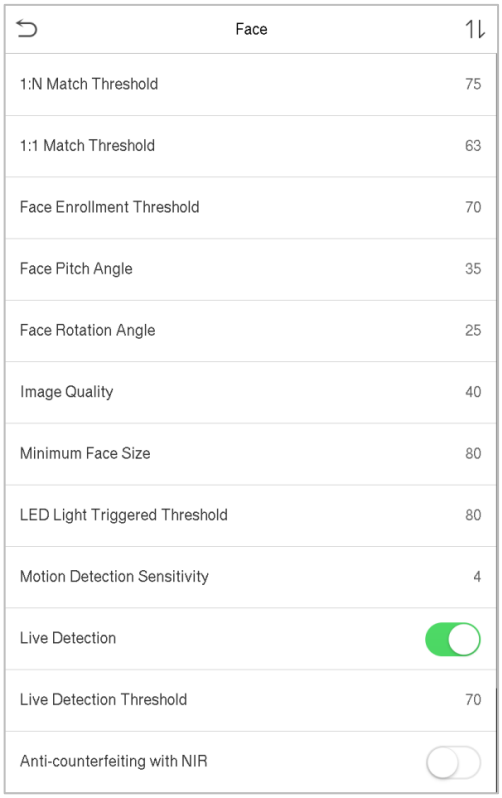
Function Description

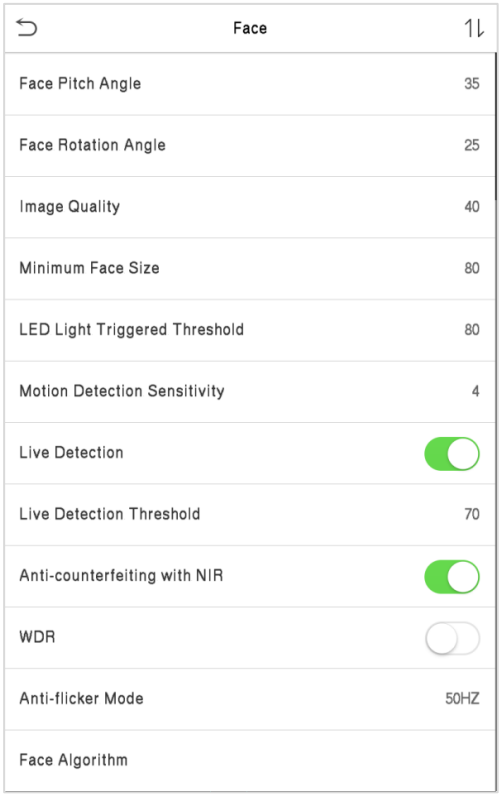
Function Name	Description
Camera Mode	Whether to capture and save the current snapshot image during verification. There are 5 modes: **No Photo:** No photo is taken during user verification. **Take photo, no save:** Photo is taken but is not saved during verification. **Take photo and save:** Photo is taken and saved during verification. **Save on successful verification:** Photo is taken and saved for each successful verification. **Save on failed verification:** Photo will be taken and saved only for each failed verification.
Display User Photo	Whether to display the user photo when the user passes the verification.
Access Logs Warning	When the record space of the attendance access reaches the maximum threshold value, the device will automatically display the memory space warning. Users may disable the function or set a valid value between 1 and 9999.
Circulation Delete Access Records	When access records have reached full capacity, the device will automatically delete a set of old access records. Users may disable the function or set a valid value between 1 and 999.
Cyclic Delete ATT Photo	When attendance photos have reached full capacity, the device will automatically delete a set of old attendance photos.

	Users may disable the function or set a valid value between 1 and 99.
Cyclic Delete Blocklist Photo	When block listed photos have reached full capacity, the device will automatically delete a set of old block listed photos. Users may disable the function or set a valid value between 1 and 99.
Confirm Screen Delay(s)	The time length of the message of successful verification displays. Valid value: 1~9 seconds.
Face comparison Interval (s)	To set the facial template matching time interval as required. Valid value: 0~9 seconds.

8.3 Face Parameters

Tap **Face** on the **System** interface to go to the face parameter settings.





FRR	FAR	Recommended Matching Thresholds	
		1:N	1:1
High	Low	85	80
Medium	Medium	82	75
Low	High	80	70

Function Description

Function Name	Description
1:N Match Threshold	Under 1:N verification mode, the verification will only be successful when the similarity between the acquired facial image and all registered facial templates is greater than the set value. The valid value ranges from 65 to 120. The higher the thresholds, the lower the misjudgement rate, the higher the rejection rate, and vice versa. It is recommended to set the default value of 75.
1:1 Match Threshold	Under 1:1 verification mode, the verification will only be successful when the similarity between the acquired facial image and the user's facial templates enrolled in the device is greater than the set value. The valid value ranges from 55 to 120. The higher the thresholds, the lower the misjudgement rate, the higher the rejection rate, and vice versa. It is recommended to set the default value of 63.
Face Enrollment Threshold	During face enrollment, 1:N comparison is used to determine whether the user has already registered before. When the similarity between the acquired facial image and all registered facial templates is greater than this threshold, it indicates that the face has already been registered.
Face Pitch Angle	The pitch angle tolerance of a face for facial registration and comparison. If a face's pitch angle exceeds this set value, it will be filtered by the algorithm, i.e. ignored by the terminal thus no registration and comparison interface will be triggered.
Face Rotation Angle	The rotation angle tolerance of a face for facial template registration and comparison. If a face's rotation angle exceeds this set value, it will be filtered by the algorithm, i.e. ignored by the terminal thus no registration and comparison interface will be triggered.
Image Quality	Image quality for facial registration and comparison. The higher the value, the clearer the image requires.
Minimum Face Size	Required for facial registration and comparison. If the minimum size of the captured figure is smaller than this set value, then it will be filtered off and not recognized as a face. This value can be understood as the face comparison distance. The farther the person is, the smaller the face is, and the smaller the face pixel will be obtained by the algorithm. Therefore, adjusting this parameter can adjust

	the furthest comparison distance of faces. When the value is 0, the face comparison distance is not limited.
LED Light Triggered Threshold	This value controls the on and off of the LED light. The larger the value, the more frequently the LED light will be turned on.
Motion Detection Sensitivity	It is to set the value for the amount of change in a camera's field of view, which is known as potential motion detection that wakes up the terminal from standby to the comparison interface. The larger the value, the more sensitive the system would be, i.e. if a larger value is set, the comparison interface is much easier and the motion detection frequently triggered.
Live Detection	Detecting the spoof attempt using visible light images to determine if the provided biometric source sample is really a person (a live human being) or false representation.
Live Detection Threshold	Facilitates to judge whether the captured visible image is really a person (a live human being). The larger the value, the better the anti-spoofing performance using visible light.
Anti-counterfeiting with NIR	Using near-infrared spectra imaging to identify and prevent fake photos and videos attack.
WDR	Wide Dynamic Range (WDR), which balances light and extends image visibility for surveillance videos under high contrast lighting scenes and improves object identification under bright and dark environment.
Anti-flicker Mode	It is used when WDR is turned off. This helps reduce flicker when the device's screen flashes at the same frequency as the light.
Face Algorithm	Facial algorithm related information and pause facial template update.
Notes	Improper adjustment of the exposure and quality parameters may severely affect the performance of the device. Please adjust the exposure parameter only under the guidance of the after-sales service personnel of our company.

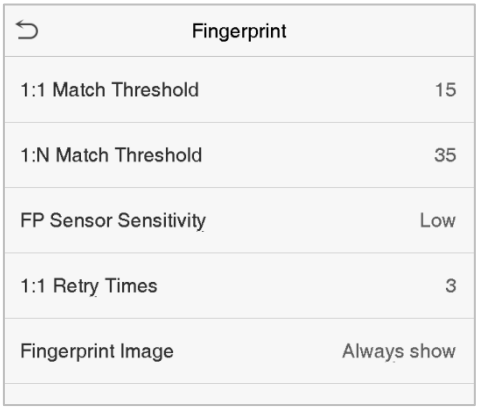
Process to modify the Face Recognition Accuracy

- On the **System** interface, tap on **Face** and then toggle to enable Anti-Spoofing using NIR to set the anti-spoofing.
- Then, on the **Main Menu**, tap **Auto-Test > Test Face** and perform the face test.
- Tap three times for the scores on the right upper corner of the screen, and the red rectangular box appears to start adjusting the mode.

- Keep one arm distance between the device and the face, and recommended not to move the face in wide range.

8.4 Fingerprint Parameters (Only avaiable model)

Tap **Fingerprint** on the **System** interface to configure the fingerprint settings.



FRR	FAR	Recommended Matching Thresholds	
		1:N	1:1
High	Low	45	25
Medium	Medium	35	15
Low	High	25	10

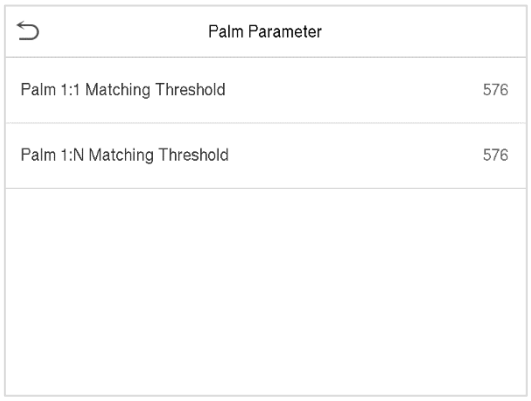
Function Description

Function Name	Descriptions
1:1 Match Threshold	Under 1:1 verification method, the verification will only be successful when the similarity between the acquired fingerprint data and the fingerprint template associated with the entered user ID that is enrolled in the device is greater than the set value.
1:N Match Threshold	Under 1:N verification method, the verification will only be successful when the similarity between the acquired fingerprint data and the fingerprint templates enrolled in the device is greater than the set value.

FP Sensor Sensitivity	To set the sensibility of fingerprint acquisition. It is recommended to use the default level "**Medium"**. When the environment is dry, resulting in slow fingerprint detection, you can set the level to "**High"** to raise the sensibility; when the environment is humid, making it hard to identify the fingerprint, you can set the level to "**Low**".
1:1 Retry Times	Users might forget the registered fingerprint or press the finger improperly. 1:1 Verification allows to set the retry authentication attempts for the users in order to reduce the process of re-entering user ID and increase the security.
Fingerprint Image	To set whether to display the fingerprint image on the screen during fingerprint enrollment or verification. Four choices are available: • **Show for enroll**: to display the fingerprint image on the screen only during enrollment. • **Show for match**: to display the fingerprint image on the screen only during verification. • **Always show**: to display the fingerprint image on screen during enrollment and verification. • **None**: not to display the fingerprint image.

8.5 Palm Parameters

Tap **Palm** on the **System** interface to configure the palm settings.



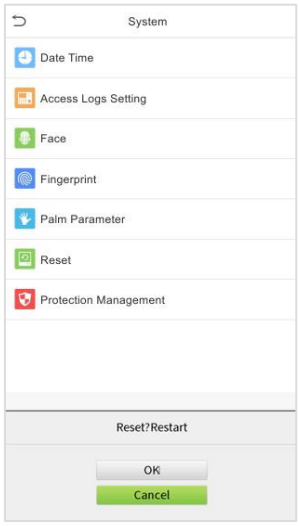
Function Description

Function Name	Description
Palm 1:1 Matching Threshold	Only when the similarity between the verifying palm and the user's registered palm is greater than this value can the verification succeed.
Palm 1:N Matching Threshold	Under 1:N Verification Method, only when the similarity between the verifying palm and all registered palm is greater than this value can the verification succeed.

8.6 Factory Reset

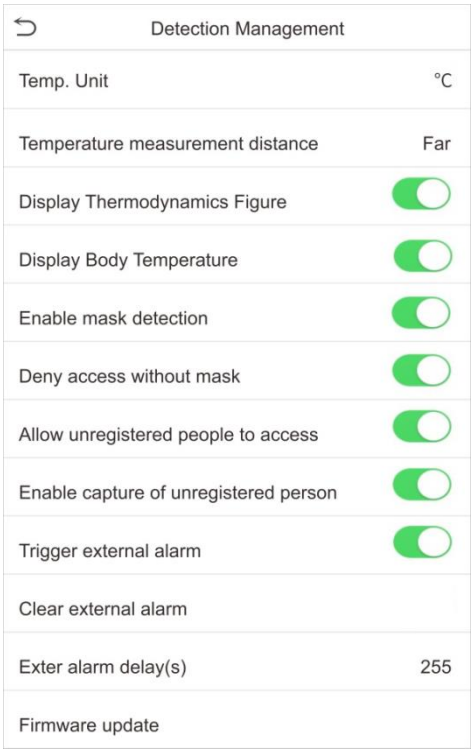
The Factory Reset function restores the device settings such as communication settings and system settings, to the default factory settings (This function does not clear registered user data).

Tap **Reset** on the **System** interface and then tap **OK** to restore the default factory settings.



8.7 Detection Management

Click **Detection Management** on the **System** interface to configure the Detection Management settings.



Function Description

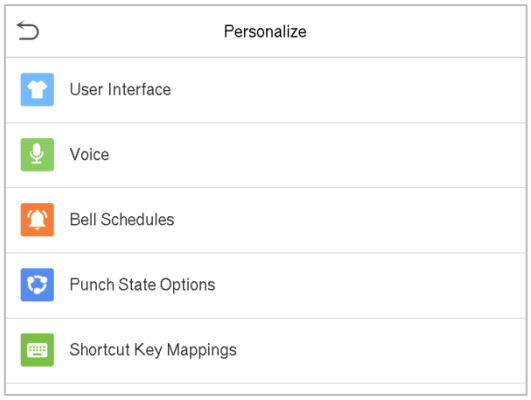
Function Name	Description
Enable temperature screening with infrared	To enable or disable the infrared temperature measurement. When this function is enabled, users must pass the temperature screening in addition to identity verification before the access is granted. To measure body temperature, user's faces must be aligned with the temperature measurement area.
High temperature alarm threshold	To set the value of the alarm threshold for high body temperature. When the temperature measured during verification is higher than the set value, the device will give a prompt and audio alarm. The default alarm threshold is 37.30°C.
Temperature over the range; access denied	When enabled, if the user's body temperature measured is above (or below) the alarm threshold, the user will not be granted access even if his/her identity is verified. When disabled, access is granted to the user if his/her identity is verified, regardless of his/her body temperature.

Temperature deviation correction	As the temperature measurement module reads a small range of variation of an observed value under unusual environments (humidity, extreme room temperature and such), the users may set the deviation value here to reflect the true temperature of the person.
Temp. Unit	The unit of body temperature can be toggled between Celsius (°C) and Fahrenheit (°F).
Temperature measurement distance	There are three modes while measuring temperature during the verification process, they are: **Near, Close** and **Far**.
Display Thermodynamics Figure	To enable or disable the display of the thermal image of a person. When enabled, the thermal image of the person is be displayed in the upper left corner of the device during the detection process.
Display Body Temperature	To enable or disable the display of body temperature. When enabled, the device will display the user's body temperature value during the verification process.
Enable mask detection	To enable or disable the mask detection function. When enabled, the device will identify whether the user is wearing a mask or not during verification.
Deny access without mask	To enable or disable the access of a person without mask. When enabled, the device will deny access of a person, if not wearing a mask.
Allow unregistered people to access	To enable or disable the access of unregistered person. When enabled, the device allows the person to enter without registration, as long as the person who passes the detection.
Enable capture of unregistered person	To enable or disable the capture photo of unregistered person. When enabled, the device will automatically capture the photo of the unregistered person, enabling this feature requires to enable **Allow unregistered people to access**.
Trigger external alarm	When enabled, if the user's temperature is higher than the set threshold value or the mask detection is enabled, but the mask is not worn by the person, it will trigger an alarm.
Clear external alarm	It clears the triggered alarm records of the device.
External alarm delay(s)	The delay (s) time for triggering an external alarm. It can be set in seconds. Users may disable the function or set a value between 1 to 255.

Firmware update	Choose whether to update the thermal imaging temperature detection module software version.

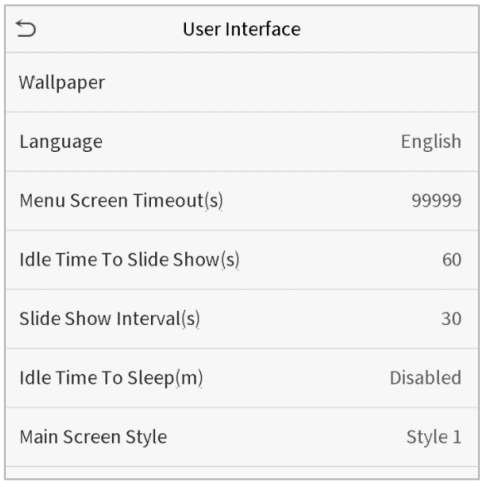
9 Personalize Settings

Tap **Personalize** on the **Main Menu** interface to customize interface settings, voice, bell, punch state options and shortcut key mappings.



9.1 Interface Settings

Tap **User Interface** on the **Personalize** interface to customize the display style of the main interface.



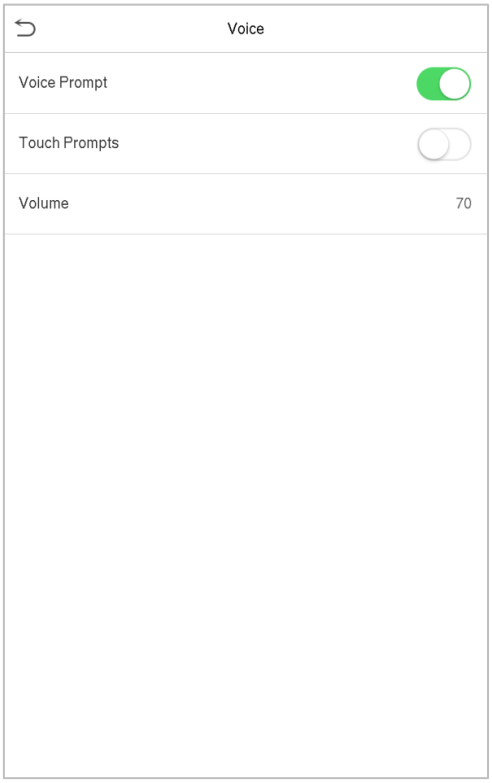
Function Description

Function Name	Description
Wallpaper	The main screen wallpaper can be selected according to the user preference.
Language	Select the language of the device.
Menu Screen Timeout (s)	When there is no operation, and the time exceeds the set value, the device will automatically go back to the initial interface.

	The function either can be disabled or set the required value between 60 and 99999 seconds.
Idle Time To Slide Show (s)	When there is no operation, and the time exceeds the set value, a slide show will be played. The function can be disabled, or you may set the value between 3 and 999 seconds.
Slide Show Interval (s)	It is the time interval in switching between different slide show pictures. The function can be disabled, or you may set the interval between 3 and 999 seconds.
Idle Time to Sleep (m)	If the sleep mode is activated, and when there is no operation in the device, then the device will enter standby mode. Press any key or finger to resume normal working mode. This function can be disabled or set a value within 1-999 minutes.
Main Screen Style	The main screen style can be selected according to the user preference.

9.2 Voice Settings

Tap **Voice** on the **Personalize** interface to configure the voice settings.



Function Description

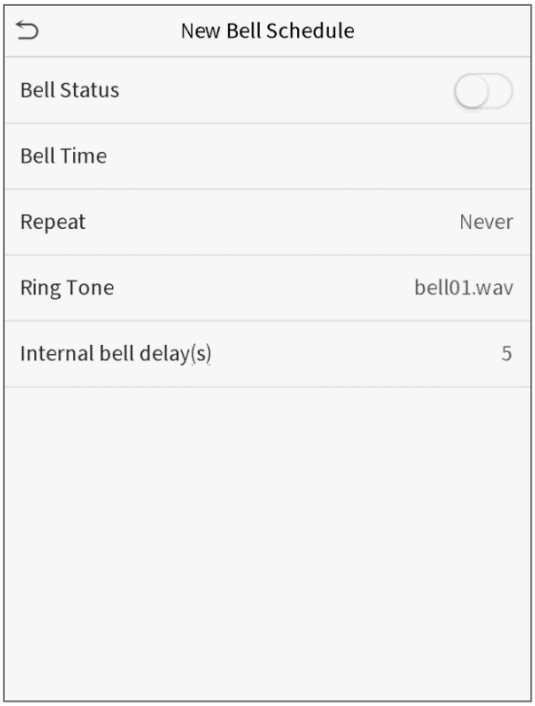
Function Name	Description
Voice Prompt	Toggle to enable or disable the voice prompts during function operations.
Touch Prompt	Toggle to enable or disable the keypad sounds.
Volume	Adjust the volume of the device which can be set between : 0-100.

9.3 Bell Schedules

Tap **Bell Schedules** on the **Personalize** interface to configure the Bell settings.

New Bell Schedule

Tap **New Bell Schedule** on the **Bell Schedule** interface to add a new bell schedule.



Function Description

Function Name	Description
Bell Status	Toggle to enable or disable the bell status.
Bell Time	Once the required time is set, the device will automatically trigger to ring the bell during that time.
Repeat	Set the required number of counts to repeat the scheduled bell.
Ring Tone	Select a ring tone.
Internal bell delay(s)	Set the replay time of the internal bell. Valid values range from 1 to 999 seconds.

All Bell Schedules

Once the bell is scheduled, on the **Bell Schedules** interface, tap **All Bell Schedules** to view the newly scheduled bell.

Edit the scheduled bell

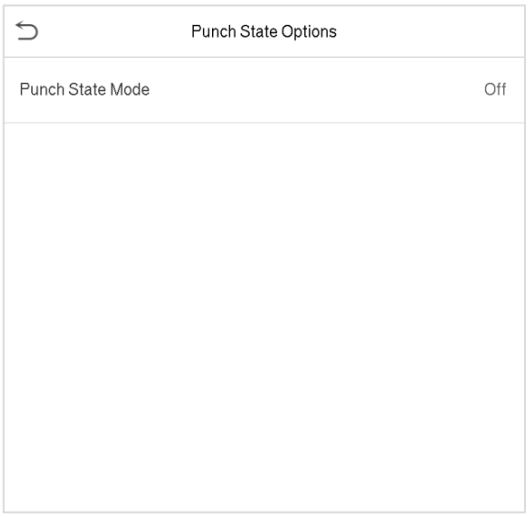
On the **All Bell Schedules** interface, tap on the required bell schedule, and tap **Edit** to edit the selected bell schedule. The editing method is the same as the operations of adding a new bell schedule.

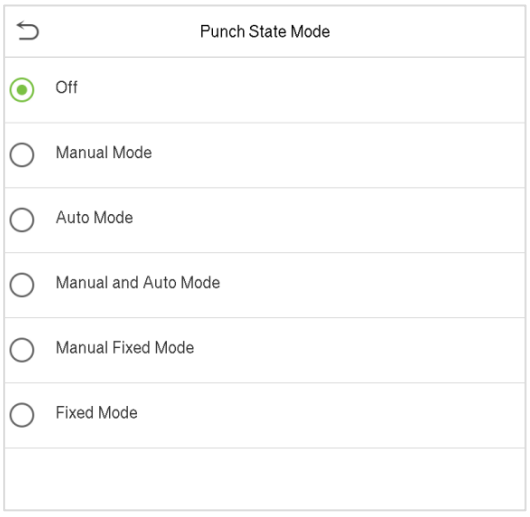
Delete a bell

On the **All Bell Schedules** interface, tap the required bell schedule, and tap **Delete**, and then tap **Yes** to delete the selected bell.

9.4 Punch States Options

Tap **Punch States Options** on the **Personalize** interface to configure the punch state settings.





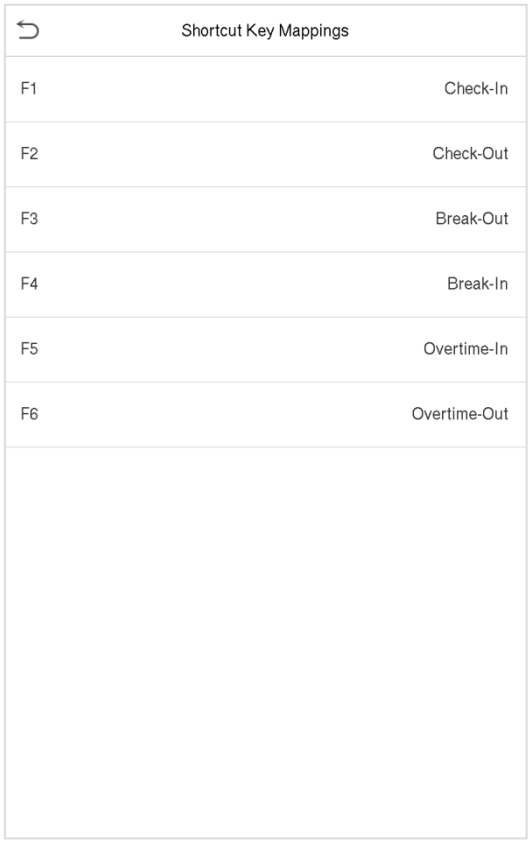
Function Description

Function Name	Description
Punch State Mode	**Off:** Disable the punch state function. Therefore, the punch state key set under **Shortcut Key Mappings** menu will become invalid. **Manual Mode:** Switch the punch state key manually, and the punch state key will disappear after **Punch State Timeout**. **Auto Mode:** The punch state key will automatically switch to a specific punch status according to the predefined time schedule which can be set in the Shortcut Key Mappings. **Manual and Auto Mode:** The main interface will display the auto-switch punch state key. However, the users will still be able to select alternative that is the manual attendance status. After timeout, the manual switching punch state key will become auto-switch punch state key. **Manual Fixed Mode:** After the punch state key is set manually to a particular punch status, the function will remain unchanged until being manually switched again. **Fixed Mode:** Only the manually fixed punch state key will be shown. Users cannot change the status by pressing any other keys.

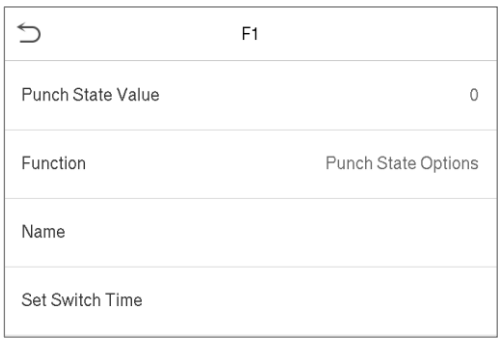
9.5 Shortcut Key Mappings

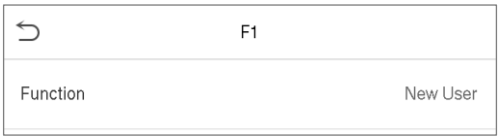
Users may define shortcut keys for attendance status and for functional keys which will be defined on the main interface. So, on the main interface, when the shortcut keys are pressed, the corresponding attendance status or the function interface will be displayed directly.

Tap **Shortcut Key Mappings** on the **Personalize** interface to set the required shortcut keys.



- On the **Shortcut Key Mappings** interface, tap on the required shortcut key to configure the shortcut key settings.
- On the **Shortcut Key (**that is "F1"**)** interface, tap **function** to set the functional process of the shortcut key either as punch state key or function key.
- If the Shortcut key is defined as a function key (such as New user, All users, etc.), the configuration is completed as shown in the image below.

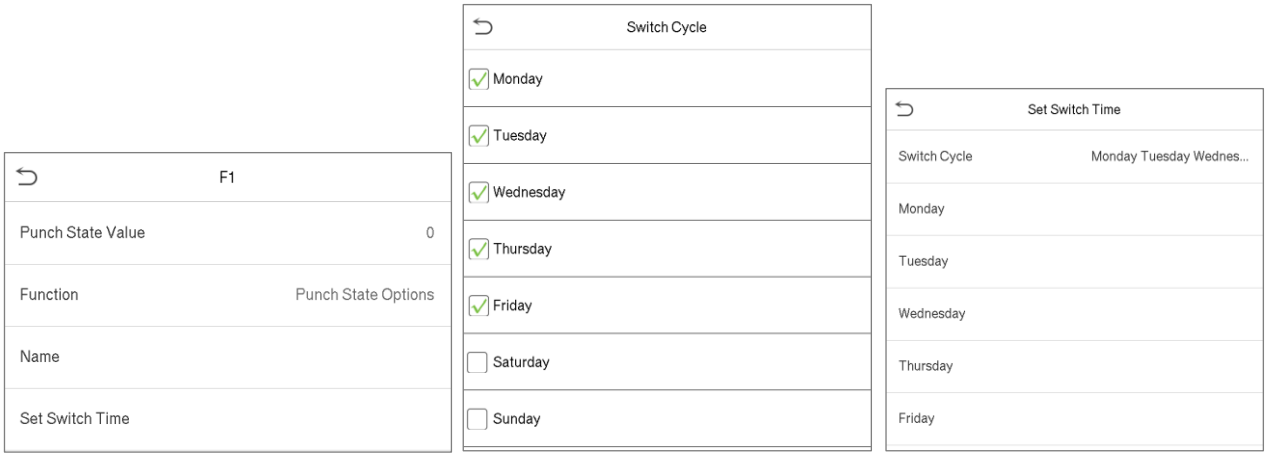




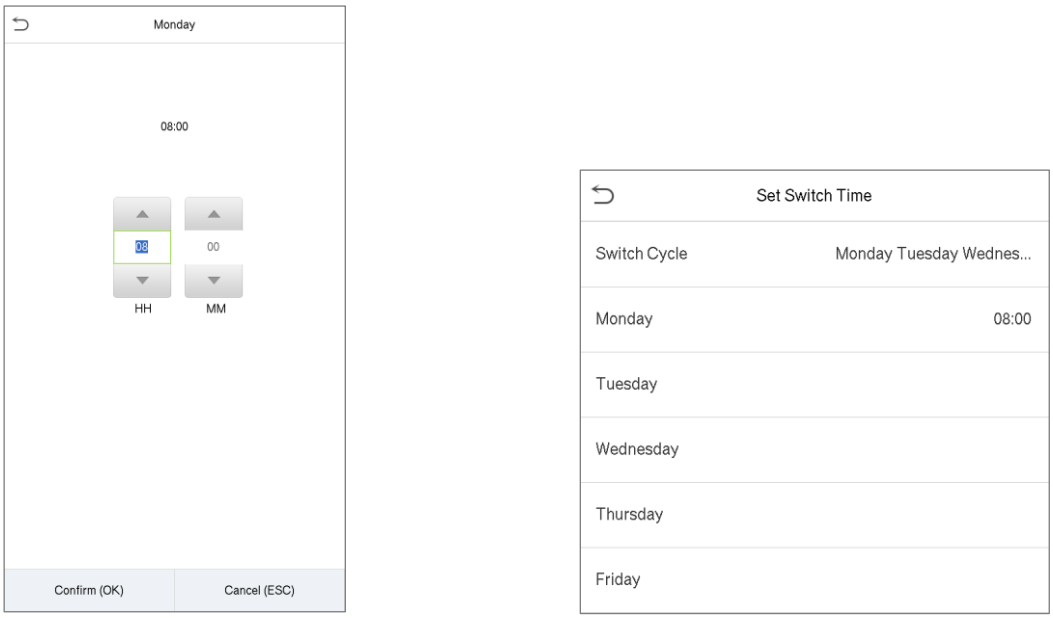
- If the Shortcut key is set as a punch state key (such as check in, check out, etc.), then it is required to set the punch state value (valid value 0~250), name and switch time.

Set the switch time

- The switch time is set in accordance with the punch state options.
- When the **punch state mode** is set to **auto mode**, the switch time should be set.
- On the **Shortcut Key** interface, tap **Set Switch Time** to set the switch time.
- On the **Switch Cycle** interface, select the switch cycle (Monday, Tuesday etc.) as shown in the image below.



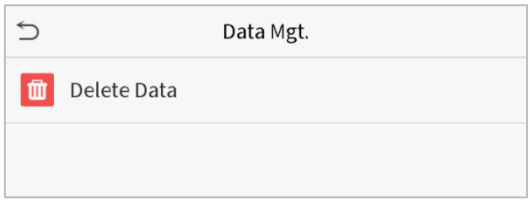
- Once the Switch cycle is selected, set the switch time for each day and tap **OK** to confirm, as shown in the image below.



Note: When the function is set to Undefined, the device will not enable the punch state key.

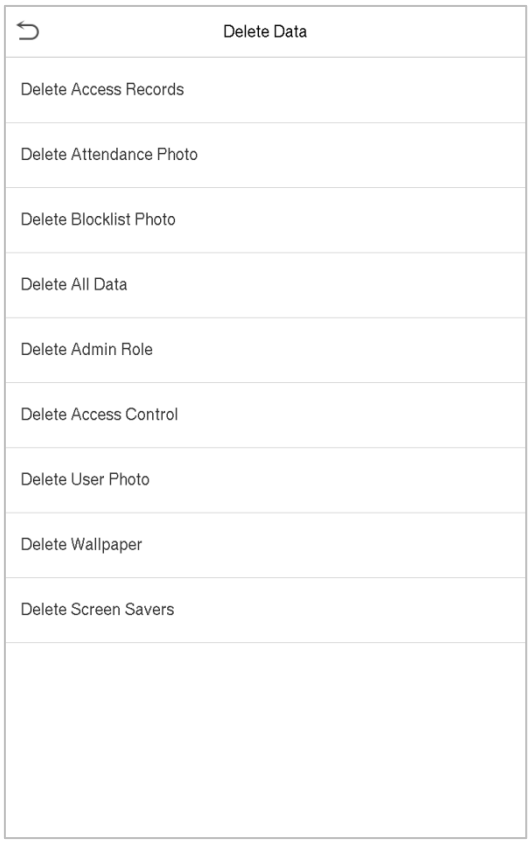
10 Data Management

On the **Main Menu**, tap **Data Mgt.** to delete the relevant data in the device.



10.1 Delete Data

Tap **Delete Data** on the **Data Mgt.** interface to delete the required data.

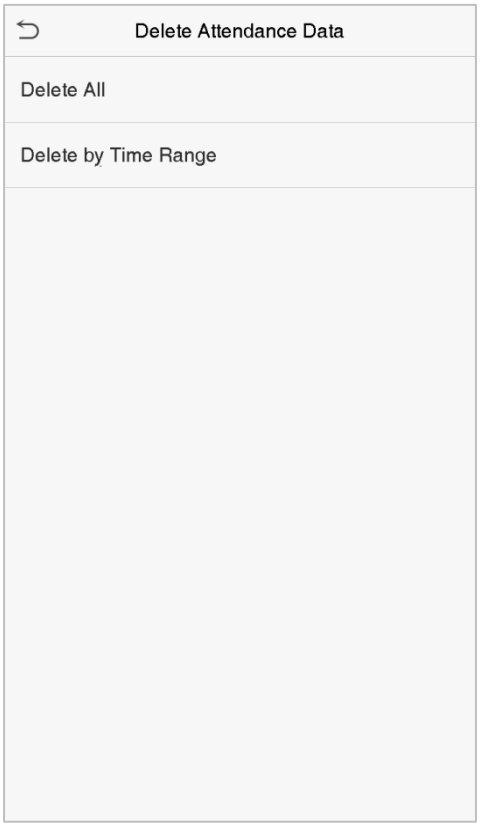


Function Description

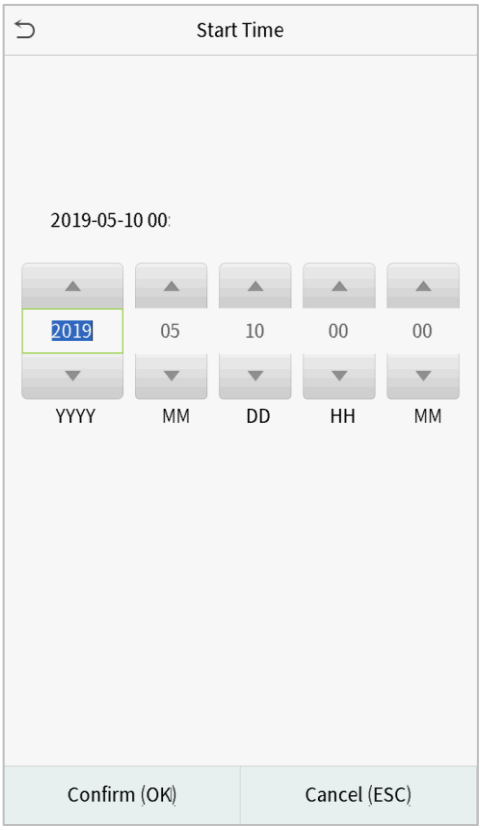
Function Name	Description
Delete Access Records	To delete attendance data/access records conditionally.
Delete Attendance Photo	To delete attendance photos of designated personnel.
Delete Blocklist Photo	To delete the photos taken during failed verifications.

Delete All Data	To delete information and attendance logs/access records of all registered users.
Delete Admin Role	To remove all administrator privileges.
Delete Access Control	To delete all access data.
Delete User Photo	To delete all user photos in the device.
Delete Wallpaper	To delete all wallpapers in the device.
Delete Screen Savers	To delete the screen savers in the device.

The user may select Delete All or Delete by Time Range when deleting the access records, attendance photos or block listed photos. Selecting Delete by Time Range, you need to set a specific time range to delete all data within a specific period.



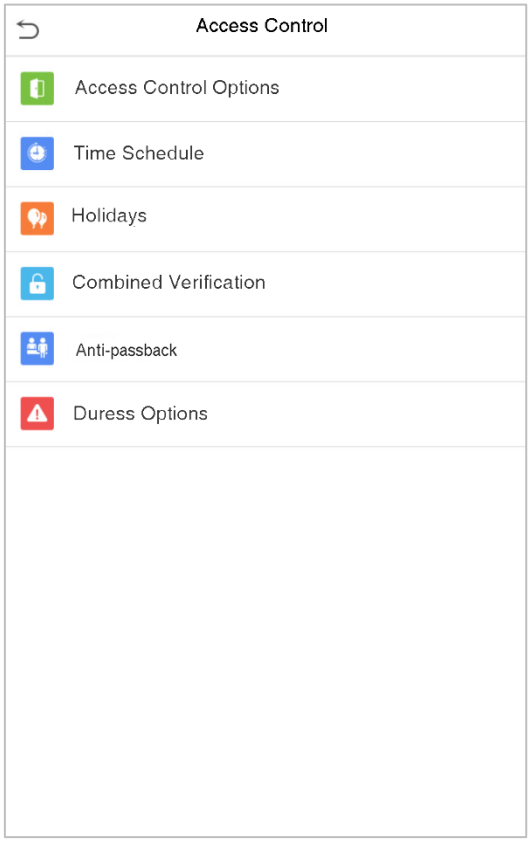
Select Delete by Time Range.



Set the time range and click **OK**.

11 Access Control

On the **Main Menu**, tap **Access Control** to set the schedule of door opening, locks control and to configure other parameters settings related to access control.

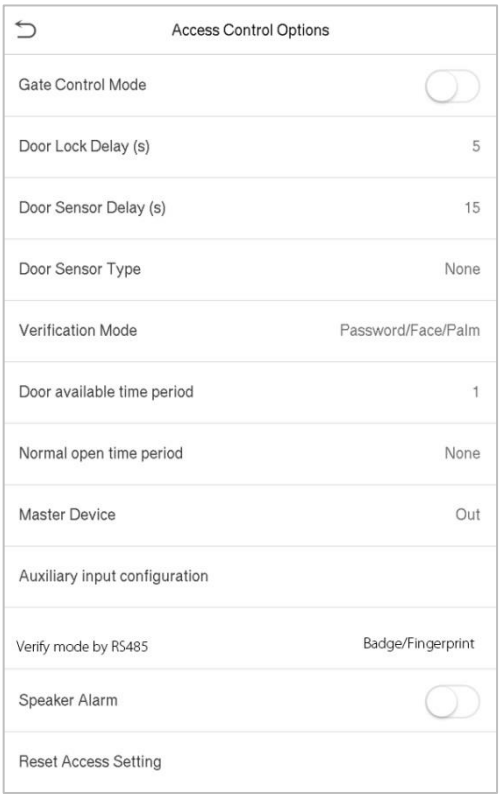


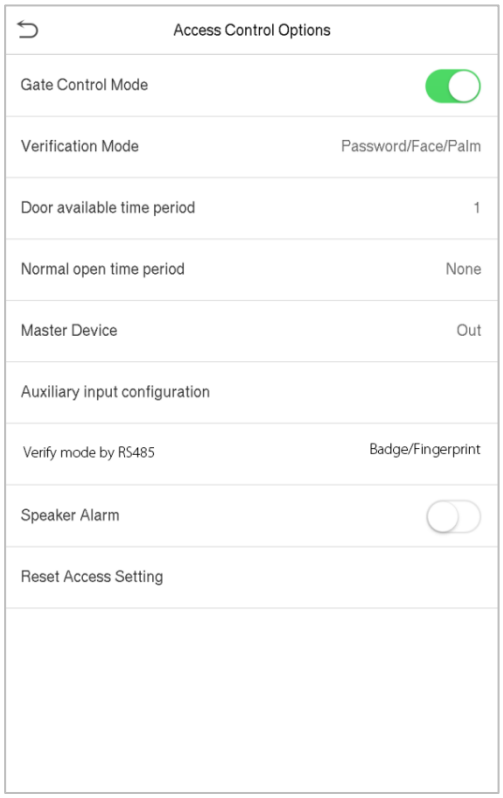
To gain access, the registered user must meet the following conditions:

- The relevant door's current unlock time should be within any valid time zone of the user time period.
- The corresponding user's group must be already set in the door unlock combination (and if there are other groups, being set in the same access combo, then the verification of those group's members are also required to unlock the door).
- In default settings, new users are allocated into the first group with the default group time zone, where the access combo is "1" and is set in unlock state by default.

11.1 Access Control Options

Tap **Access Control Options** on the **Access Control** interface to set the parameters of the control lock of the terminal and related equipment.





Function Description

Function Name	Description
Gate Control Mode	Toggle between ON or OFF switch to get into gate control mode or not. When set to **ON**, on this interface will remove Door lock relay, Door sensor relay and Door sensor type options.
Door Lock Delay (s)	The length of time that the device controls the electric lock to be in unlock state. Valid value: 1~10 seconds; 0 second represents disabling the function.
Door Sensor Delay (s)	If the door is not locked and is being left open for a certain duration (Door Sensor Delay), an alarm will be triggered. The valid value of Door Sensor Delay ranges from 1 to 255 seconds.
Door Sensor Type	There are three Sensor types: **None, Normal Open** and **Normal Closed**. **None:** It means door sensor is not in use.

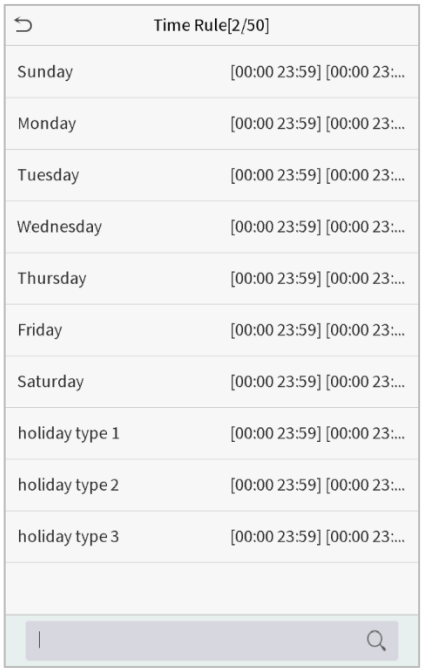
	Normal Open: It means the door is always left opened when electric power is on. **Normal Closed:** It means the door is always left closed when electric power is on.
Verification Mode	The supported verification mode includes Password/Face, User ID only, Password, Face only, and Face + Password.
Door available time period	To set time period for door, so that the door is available only during that period.
Normal open time Period	Scheduled time period for "Normal Open" mode, so that the door is always left open during this period.
Master Device	When setting up the master and slave, the status of the master can be set to exit on enter. **Exit:** The record verified on the host is the exit record. **Enter:** The record verified on the host is the entry record.
Auxiliary input configuration	Sets the door unlock time period and auxiliary output type of the auxiliary terminal device. Auxiliary output types include None, Trigger door open, Trigger Alarm, Trigger door open and Alarm.
Verify mode by RS485	The verification mode is used when the device is used either as a host or slave. The supported verification mode includes Card/Fingerprint, Fingerprint only, Card only, Fingerprint + Password, Card + Password, Card + Fingerprint, and Card + Fingerprint + Password.
Speaker Alarm	Transmits a sound alarm or disassembly alarm from the local. When the door is closed or the verification is successful, the system will cancel the alarm from the local.
Reset Access Setting	The access control reset parameters include door lock delay, door sensor delay, door sensor type, verification mode, door available time period, normal open time period, master device, and alarm. However, erased access control data in Data Mgt. is excluded.

11.2 Time Schedule

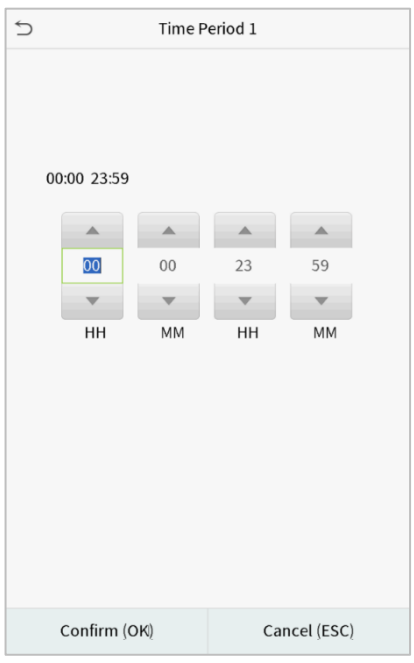
Tap **Time Rule Setting** on the Access Control interface to configure the time settings.

- The entire system can define up to 50 Time Periods.
- Each Time Period represents **10** Time Zones, i.e. **1** week and **3** holidays, and each time zone is a standard 24 hour period per day and the user can only verify within the valid time period.
- One can set a maximum of 3 time periods for every time zone. The relationship among these time periods is "**OR**". Thus when the verification time falls in any one of these time periods, the verification is valid.
- The Time Zone format of each Time Period: HH MM-HH MM, which is accurate to minutes according to the 24-hour clock.

Tap the grey box to search the required Time Zone and specify the required Time Zone number (maximum: up to 50 zones).



On the selected Time Zone number interface, tap on the required day (that is Monday, Tuesday etc.) to set the time.



Specify the start and the end time, and then tap **OK**.

NOTE:

1）When the End Time is earlier than the Start Time, (such as 23:57~23:56), it indicates that access is prohibited all day.

2）When the End Time is later than the Start Time, (such as 00:00~23:59), it indicates that the interval is valid.

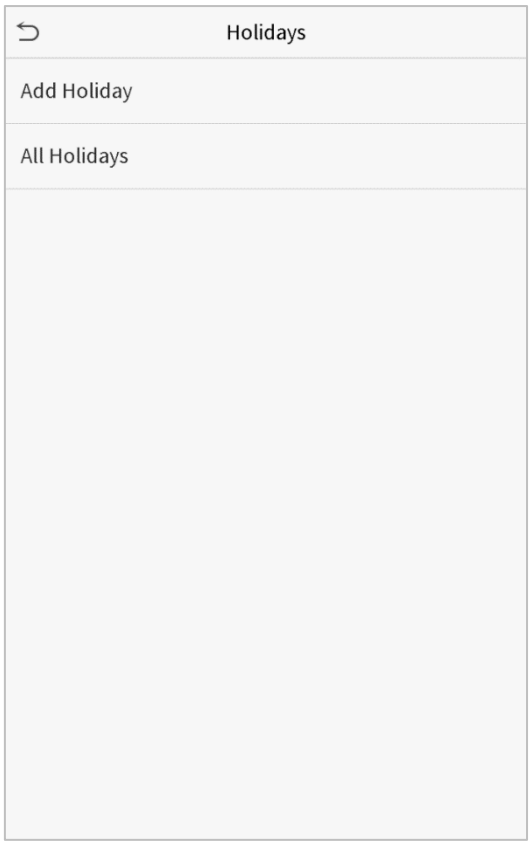
3）The effective Time Period to keep the Door Unlock or open all the day is (00:00~23:59) or also when the Ending Time is later than the Starting Time, (such as 08:00~23:59).

4）The default Time Zone 1 indicates that door is open all day long.

11.3 Holidays

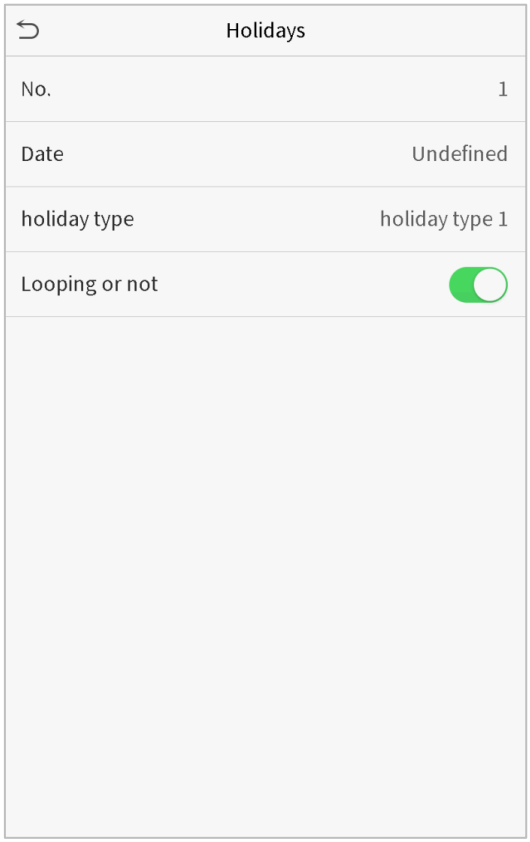
Whenever there is a holiday, you may need a special access time; but changing everyone's access time one by one is extremely cumbersome, so you can set a holiday access time which is applicable to all employees, and the user will be able to open the door during the holidays.

Tap **Holidays** on the **Access Control** interface to set the Holiday access.



- **Add a New Holiday**

Tap **Add Holiday** on the **Holidays** interface and set the holiday parameters.



- **Edit a Holiday**

On the **Holidays** interface, select a holiday item to be modified. Tap **Edit** to modify holiday parameters.

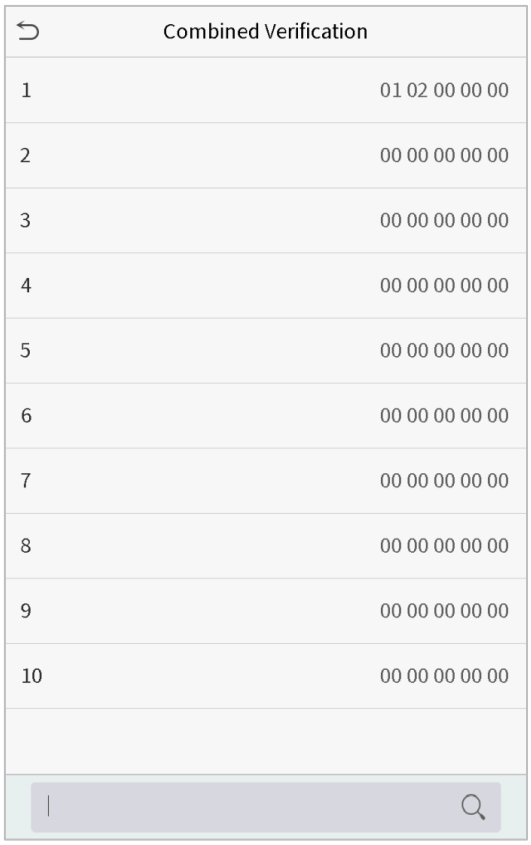
- **Delete a Holiday**

On the **Holidays** interface, select a holiday item to be deleted and tap **Delete**. Press **OK** to confirm deletion. After deletion, this holiday is no longer displayed on **All Holidays** interface.

11.4Combined Verification

Access groups are arranged into different door-unlocking combinations to achieve multiple verifications and strengthen the security. In a door-unlocking combination, the range of the combined number N is: $0 \leq N \leq 5$, and the number of members N may all belong to one access group or may belong to five different access groups.

Tap **Combined Verification on** the **Access Control** interface to configure the combined verification setting.



On the combined verification interface, tap the Door-unlock combination to be set, and tap the **up** and **down** arrows to input the combination number, and then press **OK**.

For Example:

- The **Door-unlock combination 1** is set as **(01 03 05 06 08)**, indicating that the unlock combination 1 consists of 5 people, and the 5 individuals are from 5 groups, namely, **Access Control Group** 1 (AC group 1), AC group 3, AC group 5, AC group 6, and AC group 8, respectively.
- The **Door-unlock combination 2** is set as **(02 02 04 04 07)**, indicating that the unlock combination 2 consists of 5 people; the first two are from AC group 2, the next two are from AC group 4, and the last person is from AC group 7.
- The **Door-unlock combination 3** is set as **(09 09 09 09 09)**, indicating that there are 5 people in this combination; all of which are from AC group 9.
- The **Door-unlock combination 4** is set as **(03 05 08 00 00)**, indicating that the unlock combination 4 consists of only three people. The first person is from AC group 3, the second person is from AC group 5, and the third person is from AC group 8.

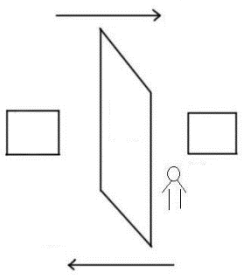
Delete a door-unlocking combination

Set all Door-unlock combinations to 0 if you want to delete door-unlock combinations.

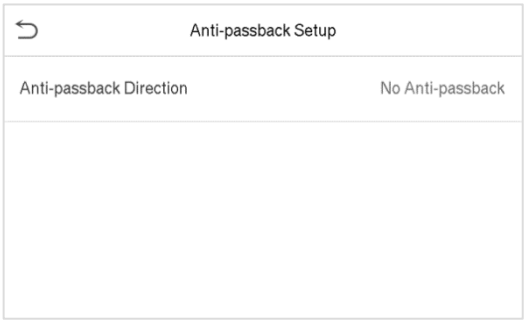
11.5 Anti-passback Setup

It is possible that users may be followed by some persons to enter the door without verification, resulting in a security breach. So, to avoid such a situation, the Anti-Passback option was developed. Once it is enabled, the check-in record must match with the check-out record so as to open the door.

This function requires two devices to work together: one is installed inside the door (master device), and the other one is installed outside the door (slave device). The two devices communicate via the Wiegand signal. The Wiegand format and Output type (User ID / Card Number) adopted by the master device and slave device must be consistent.



Tap **Anti-passback Setup** on the **Access Control** interface.



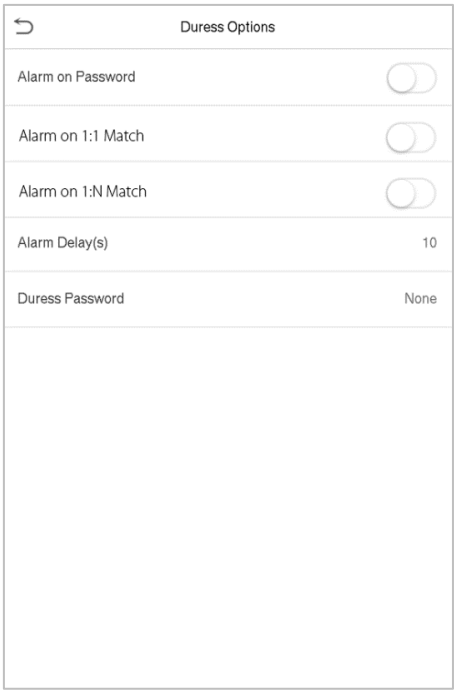
Function Description

Function Name	Description
Anti-passback direction	**No Anti-passback:** Anti-passback function is disabled, which means successful verification through either the master device or slave device can unlock the door. The attendance state is not saved in this option. **Out Anti-passback:** After a user checks out, only if the last record is a check-in record, the user can check-out again; otherwise, the alarm will be triggered. However, the user can check-in freely. **In Anti-passback:** After a user checks in, only if the last record is a check-out record, the user can check-in again; otherwise, the alarm will be triggered. However, the user can check-out freely. **In/Out Anti-passback:** After a user checks in/out, only if the last record is a check-out record, the user can check-in again; or if it is a check-in record, the user can check-out again; otherwise, the alarm will be triggered.

11.6 Duress Options

Once a user activates the duress verification function with specific authentication method(s), and when he/she is under coercion and authenticates using duress verification, the device will unlock the door as usual, but at the same time, a signal will be sent to trigger the alarm.

On **Access Control** interface, tap **Duress Options** to configure the duress settings.



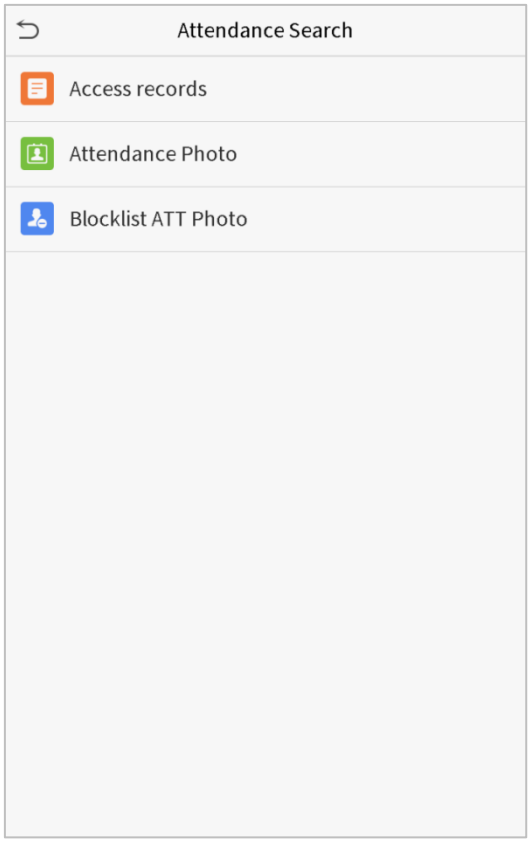
Function Description

Function Name	Description
Alarm on Password	When a user uses the password verification method, an alarm signal will be generated only when the password verification is successful, otherwise there will be no alarm signal.
Alarm on 1:1 Match	When a user uses any fingerprint to perform the 1:1 verification, an alarm signal will be generated only when the 1:1 verification is successful, otherwise there will be no alarm signal.
Alarm on 1:N Match	When a user uses any fingerprint to perform 1:N verification, an alarm signal will be generated only when the 1:N identification is successful, otherwise there will be no alarm signal.
Alarm Delay (s)	Alarm signal will not be transmitted until the alarm delay time is elapsed. The value ranges from 1 to 999 seconds.
Duress Password	Set the 6-digit duress password. When the user enters this duress password for verification, an alarm signal is be generated.

12 Attendance Search

Once the identity of a user is verified, the Access record will be saved in the device. This function enables users to check their access records.

Click **Attendance Search** on the **Main Menu** interface to search for the required Access/Attendance log.

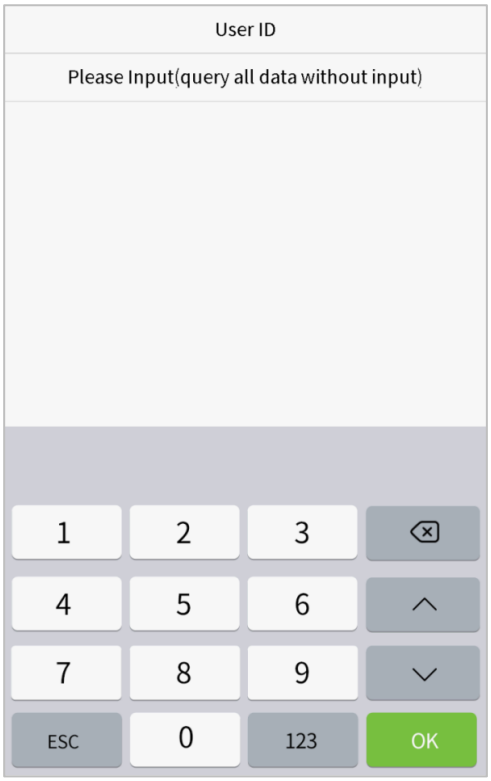


The process of searching for attendance and blocklist photos is similar to that of searching for access records. The following is an example of searching for access records.

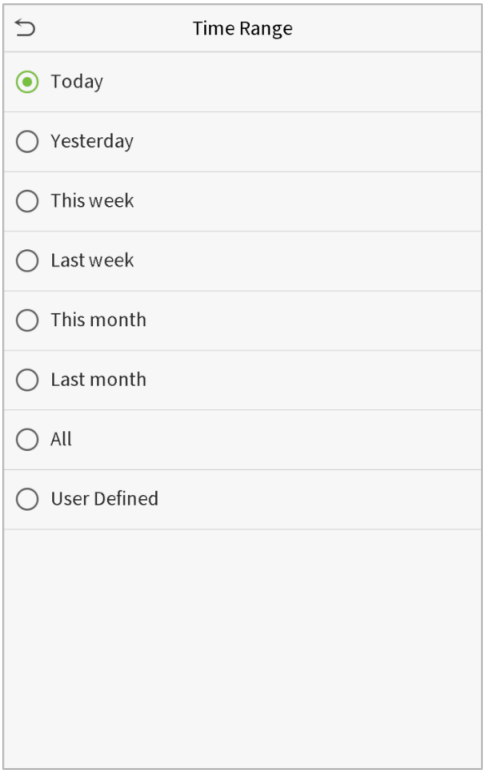
On the **Attendance Search** interface, tap **Access Record** to search for the required record.

1. Enter the user ID to be searched and click OK. If you want to search for records of all users, click OK without entering any user ID.

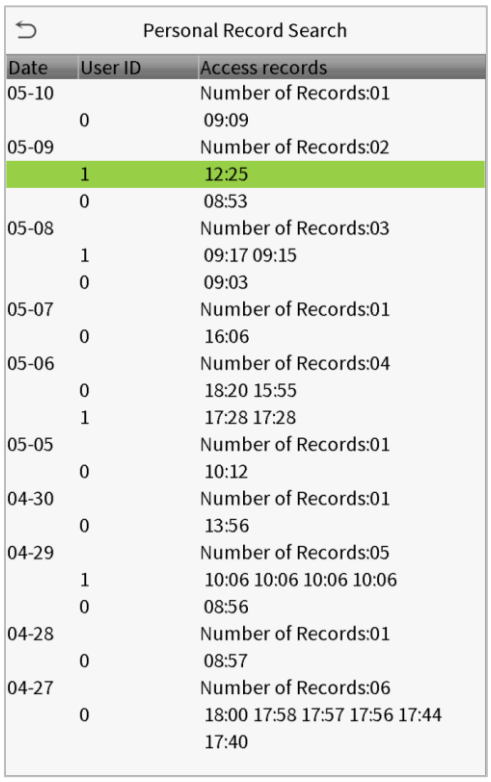
2. Select the time range in which the records need to be searched.

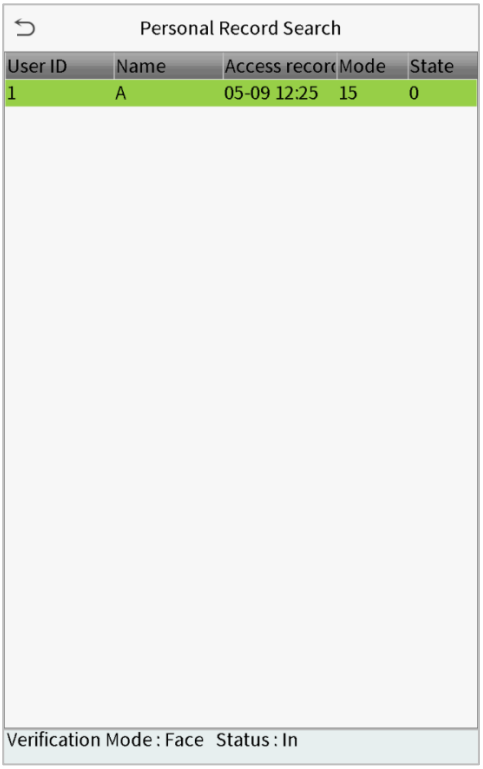


3. Once the record search succeeds. Tap the record in highlighted in green to view its details.



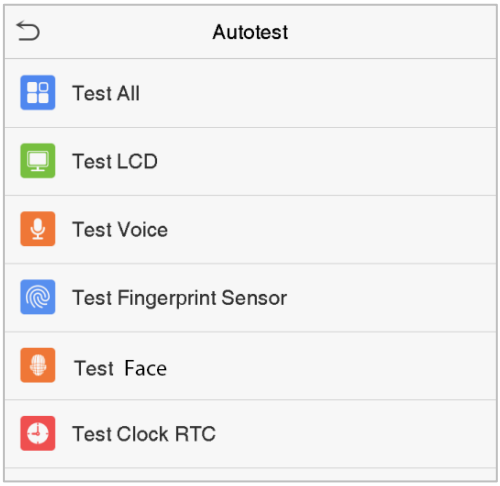
4. The below figure shows the details of the selected record.





13 Autotest

On the **Main Menu**, tap **Autotest** to automatically test whether all modules in the device function properly, which include the LCD, Voice, Fingerprint Sensor, Camera and Real-Time Clock (RTC).

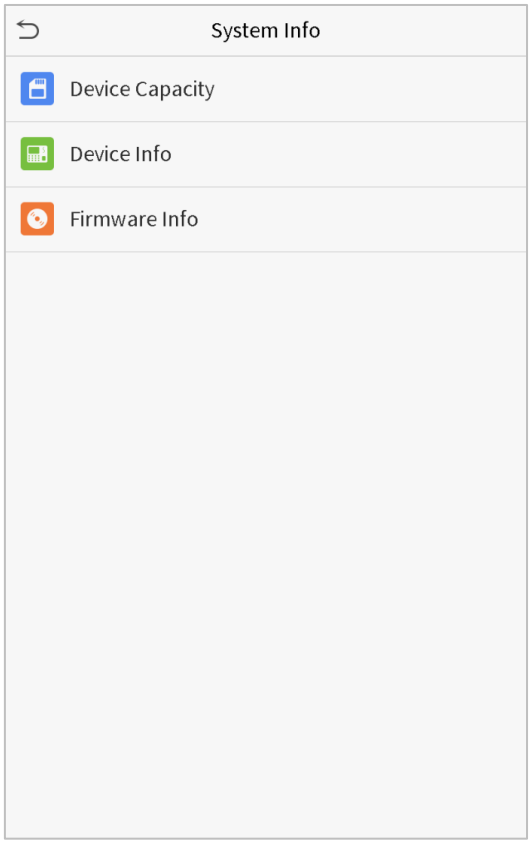


Function Description

Function Name	Description
Test All	To automatically test whether the LCD, Audio, Camera and RTC are normal.
Test LCD	To automatically test the display effect of LCD screen by displaying full-color, pure white, and pure black to check whether the screen displays colors normally.
Test Voice	To automatically test whether the audio files stored in the device are complete and the voice quality is good.
Test Fingerprint Sensor	To test the fingerprint sensor by pressing a finger on the scanner to check if the acquired fingerprint image is clear. When you are pressing a finger on the scanner, the fingerprint image will display on the screen.
Test Face	To test if the camera functions properly by checking the pictures taken to see if they are clear enough.
Test Clock RTC	To test the RTC. The device tests whether the clock works normally and accurately with a stopwatch. Tap the screen to start counting and press it again to stop counting.

14 System Information

On the **Main Menu**, tap **System Info** to view the storage status, the version information of the device, and firmware information.



Function Description

Function Name	Description
Device Capacity	Displays the current device's user storage, palm, fingerprint, password and face storage, administrators, access records, attendance and blocklist photos, and user photos.
Device Info	Displays the device's name, serial number, MAC address, palm, fingerprint and face algorithm, version information, platform information, and manufacturer and manufacture date.
Firmware Info	Displays the firmware version and other version information of the device.

Appendix 1

Requirements of Live Collection and Registration of Visible Light Face Images

1. It is recommended to perform registration in an indoor environment with an appropriate light source without underexposure or overexposure.
2. Do not place the device towards outdoor light sources like door or window or other harsh light sources.
3. Dark-color apparels, different from the background color is recommended for registration.
4. Please expose your face and forehead properly and do not cover your face and eyebrows with your hair.
5. It is recommended to show a plain facial expression. (A smile is acceptable, but do not close your eyes, or incline your head to any orientation).
6. Two images are required for a person with eyeglasses, one image with eyeglasses and the other without the eyeglasses.
7. Do not wear accessories like a scarf or mask that may cover your mouth or chin.
8. Please face right towards the capturing device, and locate your face in the image capturing area as shown in the image below.
9. Do not include more than one face in the capturing area.
10. A distance of 50cm to 80cm is recommended for capturing the image. (the distance is adjustable, subject to body height).

Requirements for Visible Light Digital Face Image Data

The digital photo should be straight-edged, colored, half-portrayed with only one person, and the person should be uncharted and in casuals. Persons who wear eyeglasses should remain to put on eyeglasses for getting photo captured.

- **Eye Distance**

200 pixels or above are recommended with no less than 115 pixels of distance.

- **Facial Expression**

Neutral face or smile with eyes naturally open are recommended.

- **Gesture and Angel**

Horizontal rotating angle should not exceed ±10°, elevation should not exceed ±10°, and depression angle should not exceed ±10°.

- **Accessories**

Masks or colored eyeglasses are not allowed. The frame of the eyeglasses should not cover eyes and should not reflect light. For persons with thick eyeglasses frame, it is recommended to capture two images, one with eyeglasses and the other one without the eyeglasses.

- **Face**

Complete face with clear contour, real scale, evenly distributed light, and no shadow.

- **Image Format**

Should be in BMP, JPG or JPEG.

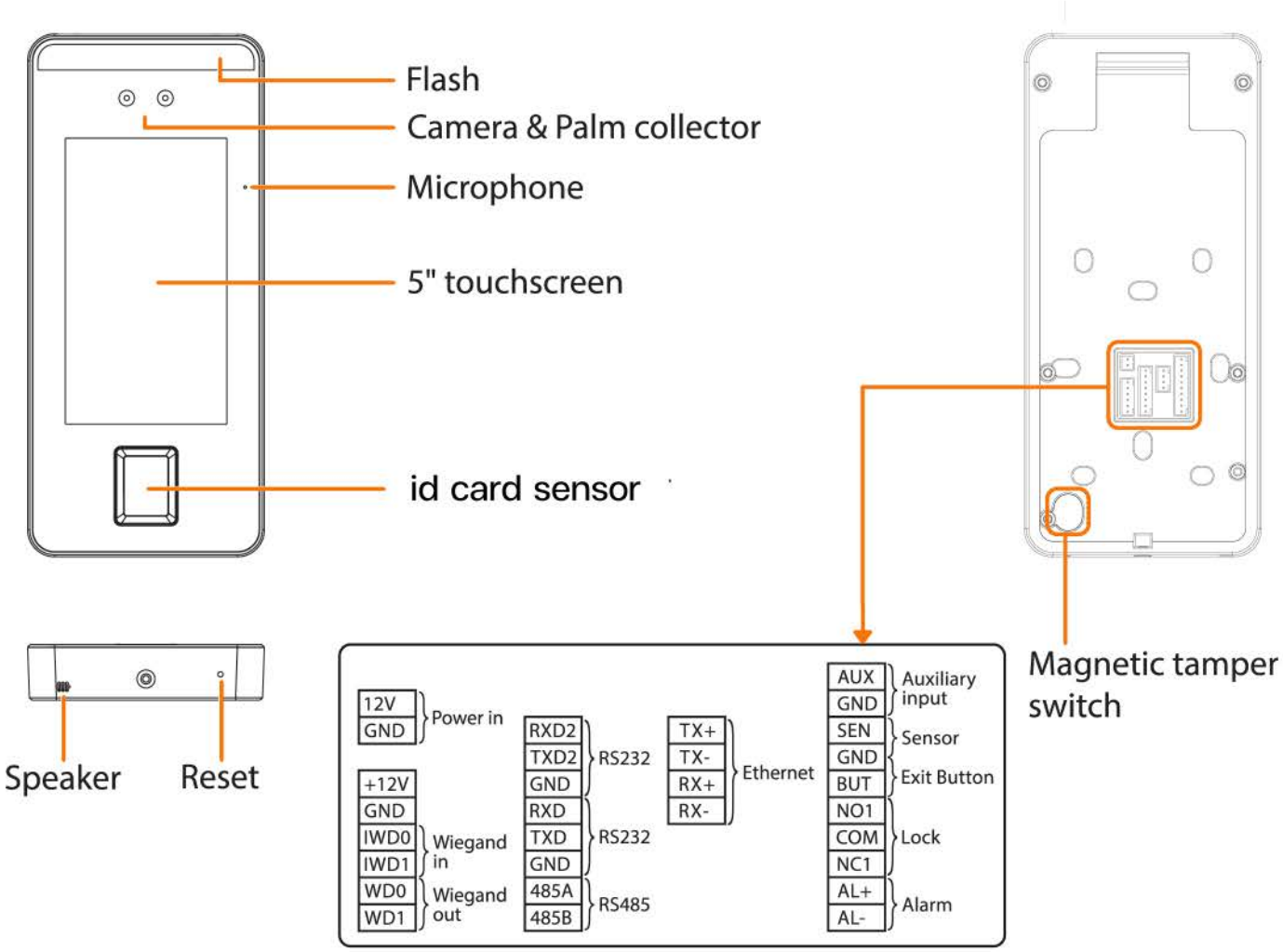
- **Data Requirement**

Should comply with the following requirements:

1. White background with dark-colored apparel.
2. 24bit true color mode.
3. JPG format compressed image with not more than 20kb size.
4. Resolution should be between 358 x 441 to 1080 x 1920.
5. The vertical scale of head and body should be in a ratio of 2:1.
6. The photo should include the captured person’s shoulders at the same horizontal level.
7. The captured person’s eyes should be open and with clearly seen iris.
8. Neutral face or smile is preferred, showing teeth is not preferred.
9. The captured person should be clearly visible, natural in color, no harsh shadow or light spot or reflection in face or background. The contrast and lightness level should be appropriat

Installation Guide

Overview



Note: Not all products have the function with , the real product shall prevail.

Installation Environment

Please refer to the following recommendations for installation.

INDOOR USE

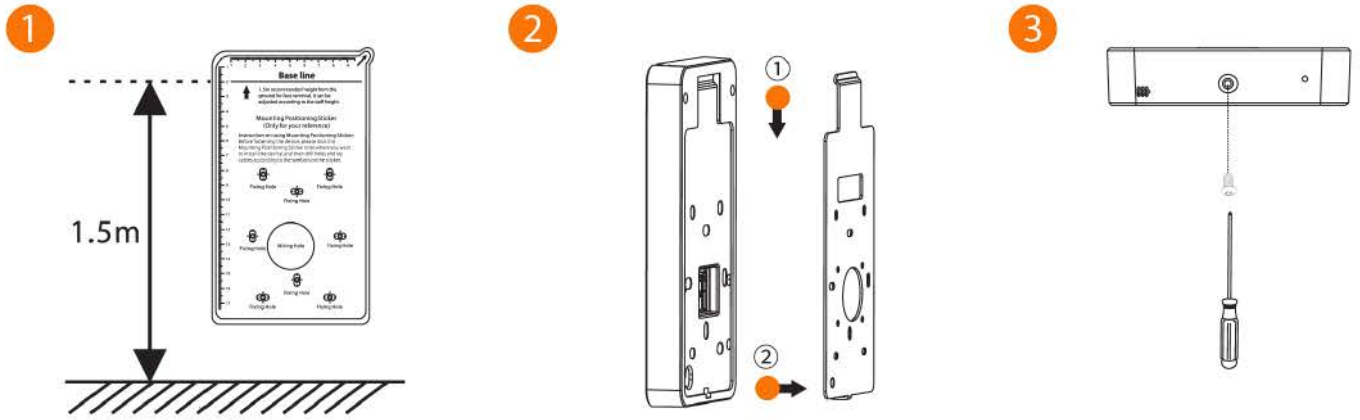
AVOID GLASS REFRACTION

AVOID DIRECT SUNLIGHT AND EXPOSURE

FAR AWAY HEAT SOURCE

KEEP EFFECTIVE DISTANCE 0.3-2m

Device Installation

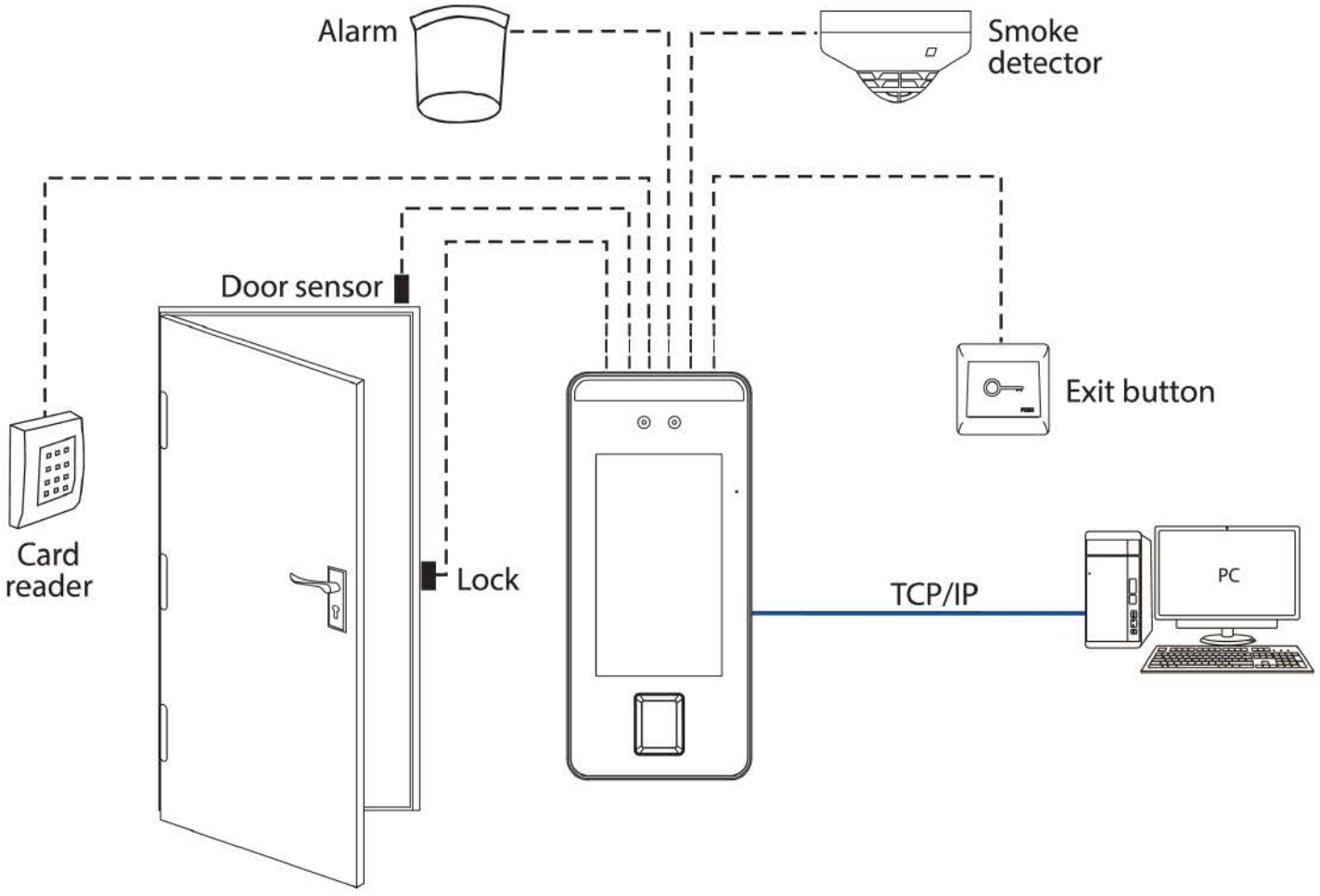


① Attach the mounting template sticker to the wall, and drill holes according to the mounting paper. Fix the back plate on the wall using wall mounting screws.

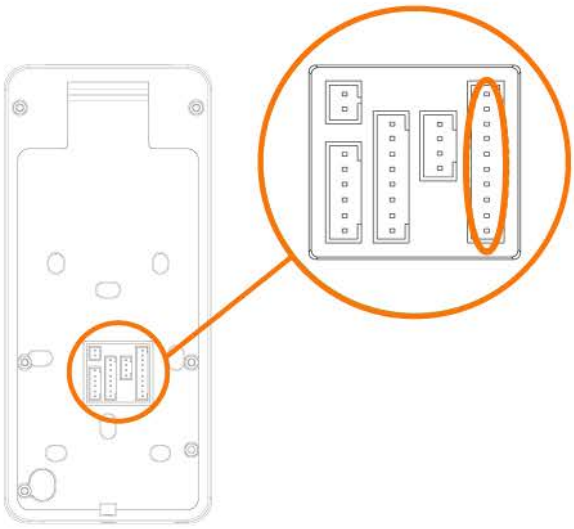
② Attach the device to the back plate.

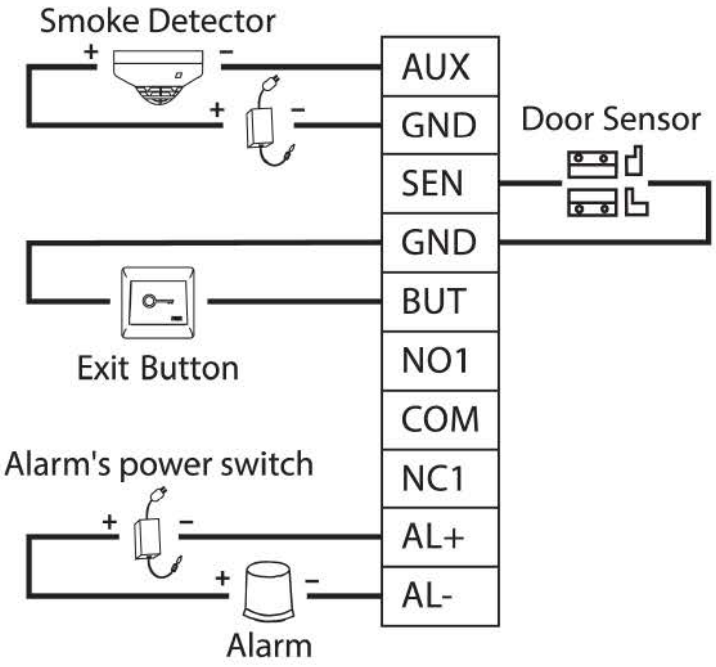
③ Fasten the device to the back plate with a security screw.

Standalone Installation



Door Sensor, Exit Button & Alarm Connection

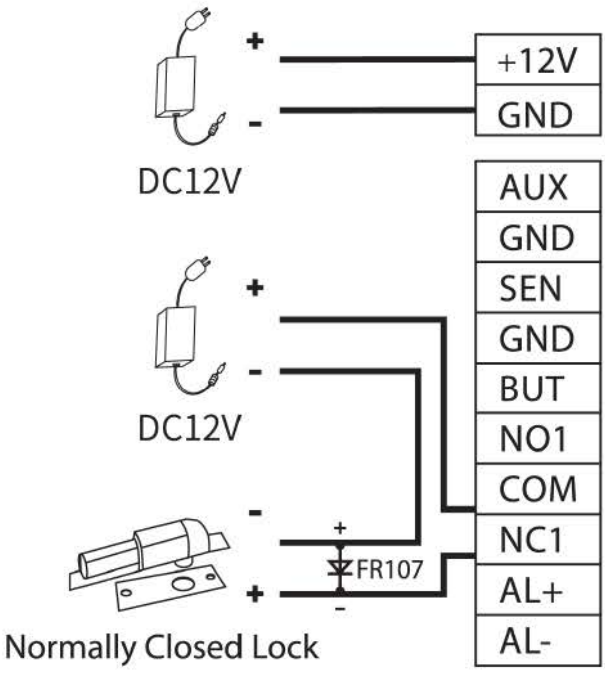




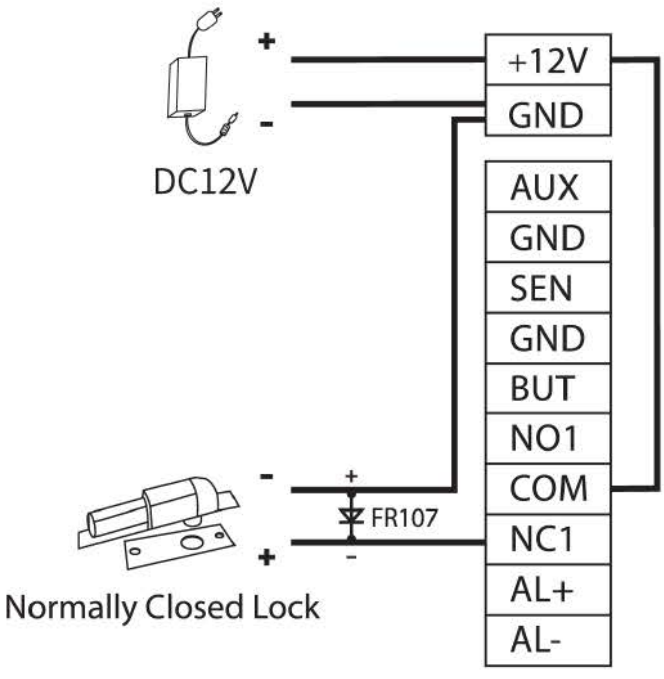
Lock Relay Connection

The system supports Normally Opened Lock and Normally Closed Lock.
The NO LOCK (normally opened at power on) is connected with 'NO1' and 'COM' terminals, and the NC LOCK (normally closed at power on) is connected with 'NC1' and 'COM' terminals. Take NC Lock as an example below:

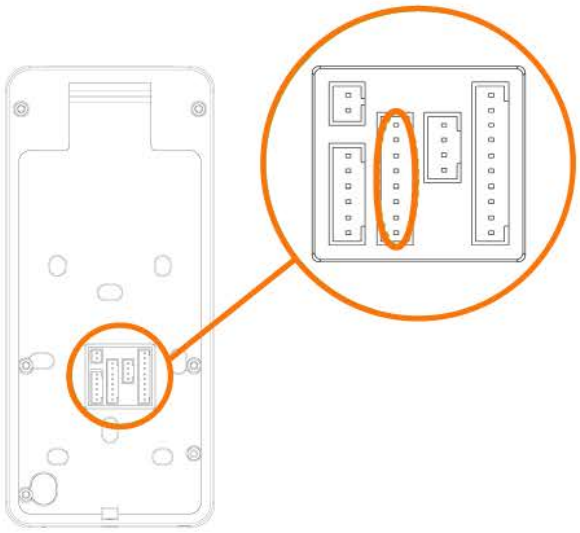
1) Device not sharing power with the lock

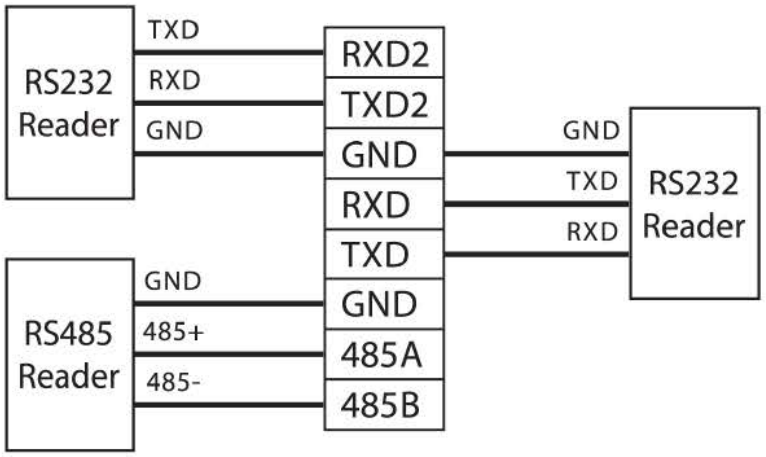


2) Device sharing power with the lock

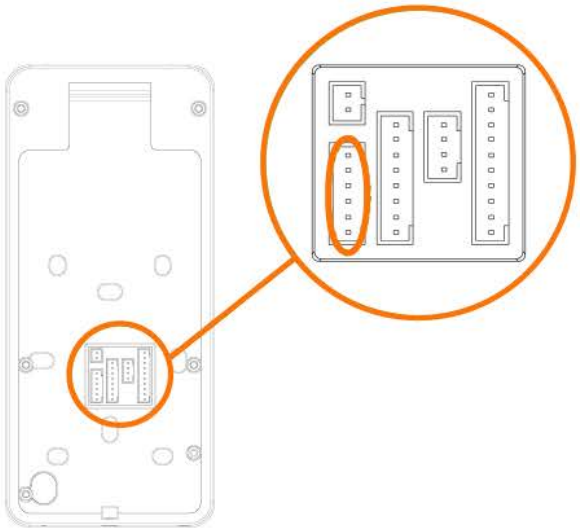


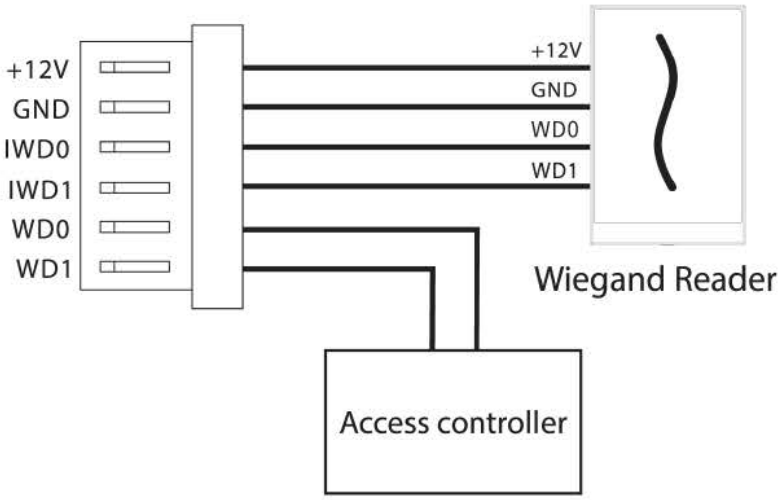
RS485 and RS232 Connection



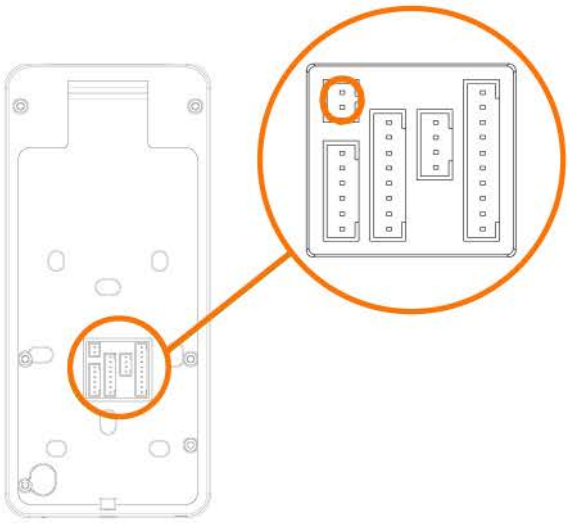


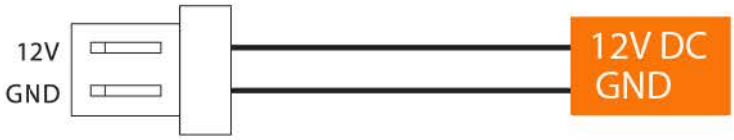
Wiegand Reader Connection





Power Connection

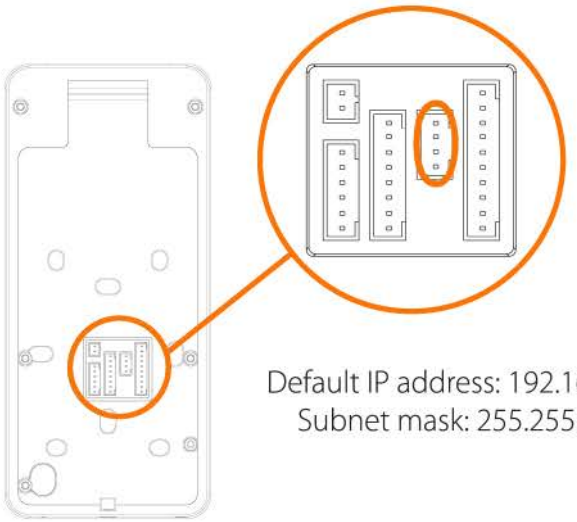




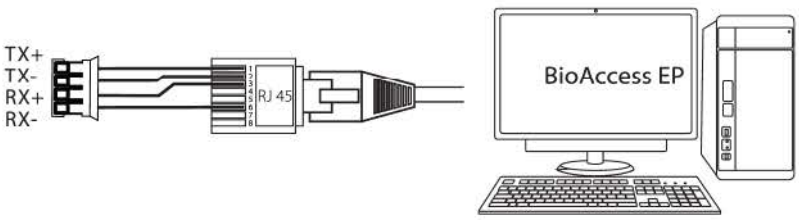
Recommended power supply

1) 12V ± 10%, at least 3000mA.
2) To share the power with other devices, use a power supply with higher current ratings.

Ethernet Connection



Default IP address: 192.168.1.201
Subnet mask: 255.255.255.0



IP address: 192.168.1.130
Subnet mask: 255.255.255.0

Click [**COMM.**] > [**Ethernet**] > [**IP Address**] , input the IP address and click [**OK**].

Note: In LAN, IP addresses of the server (PC) and the device must be in the same network segment when connecting to ZKBioAccess EP software.

Workplace Intelligence

2525 FYI Center, Building 1, 5th Floor,
Unit 1/506, Rama 4 Road, Klong Toei,
KlongToei, Bangkok 10110, Thailand

Tel : (+66) 2 784-5855