iomo

FCA-4000

The FCA-4000 is a touchless biometric facial recognition device with an ID card scanner designed to support the clocking of a large number of employees. With access control and built-in Wi-Fi and 4G Communication

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.
For Device	
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

	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

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).
   - 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.
- 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, odour, or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service centre.
- 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:

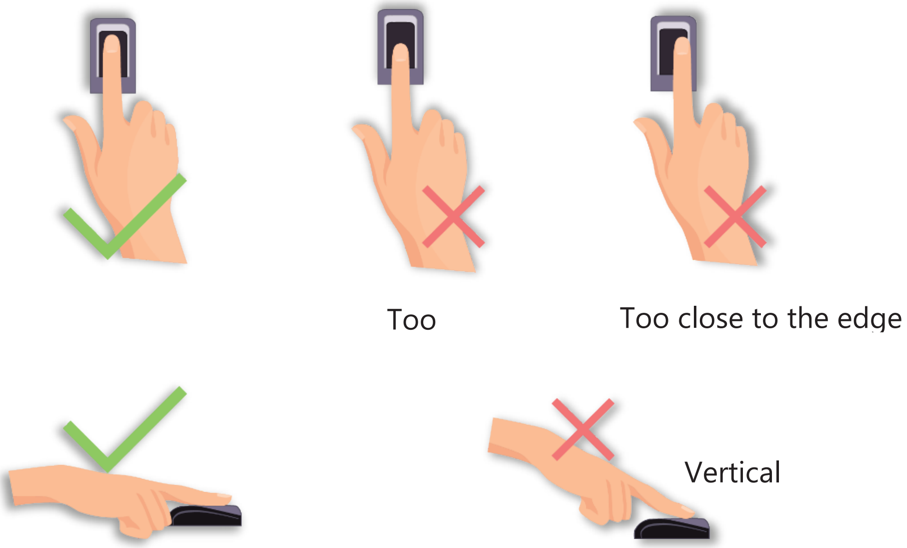
- Make sure whether the positive polarity and negative polarity of the DC 12V power supply is connected correctly. A reverse connection may damage the device. It is not advisable to connect the AC 24V power supply to the DC 12V input port.
- Make sure to connect the wires following the positive polarity 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.

1 Instruction for Use

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

1.1 Finger Positioning

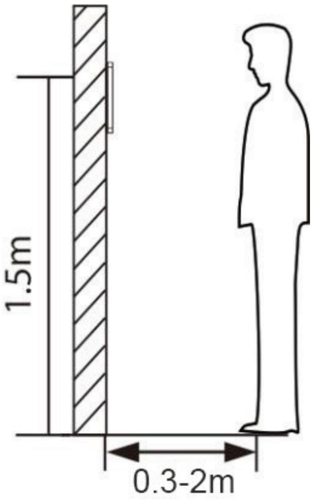
Recommended fingers: Index, middle, or ring fingers; avoid using the thumb or pinky, as they are difficult to accurately press onto the fingerprint reader.



NOTE: Please use the correct method when pressing your fingers onto the fingerprint reader for registration and identification. Our company will assume no liability for recognition issues that may result from incorrect usage of the product. We reserve the right of final interpretation and modification concerning this point.

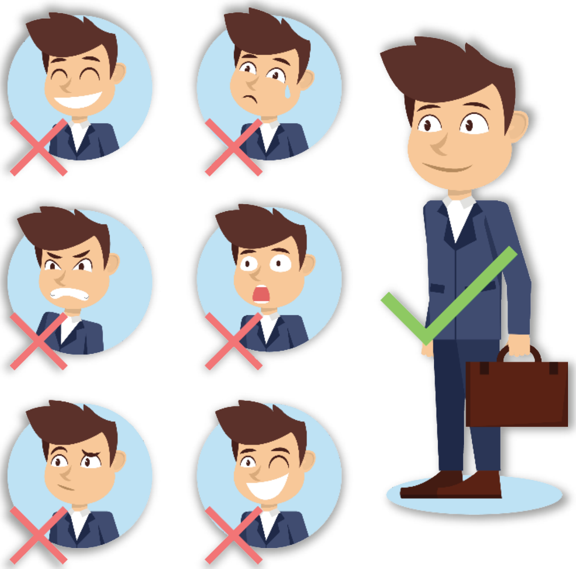
1.2 Standing Position, Facial Expression and Standing Posture

- **The recommended distance**

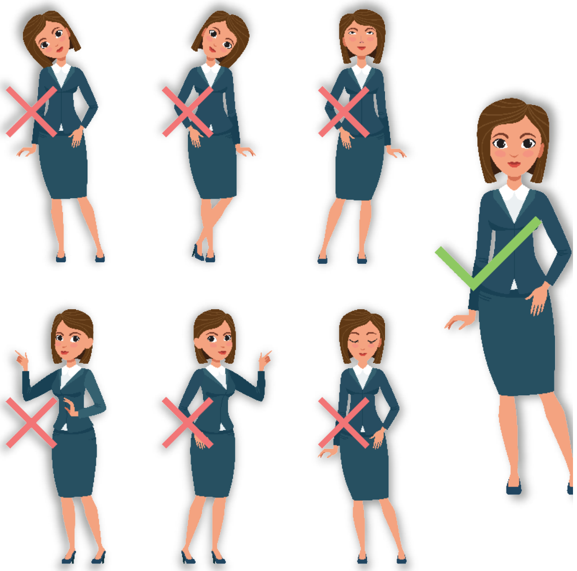


The distance between the device and a user whose height is in a range of 1.55m-1.85m is recommended to be 0.3-2.5m. Users may slightly move forward or backward to improve the character of facial images captured.

- **Recommended Standing Posture and Facial Expression**



Facial Expression

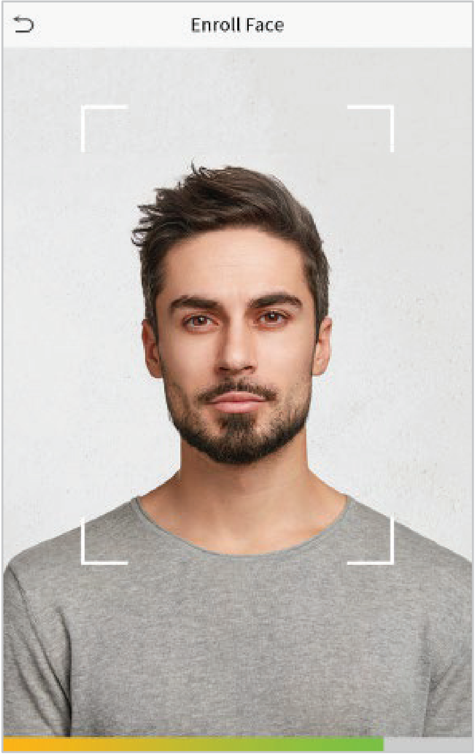


Standing Posture

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

1.3 Face Registration

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



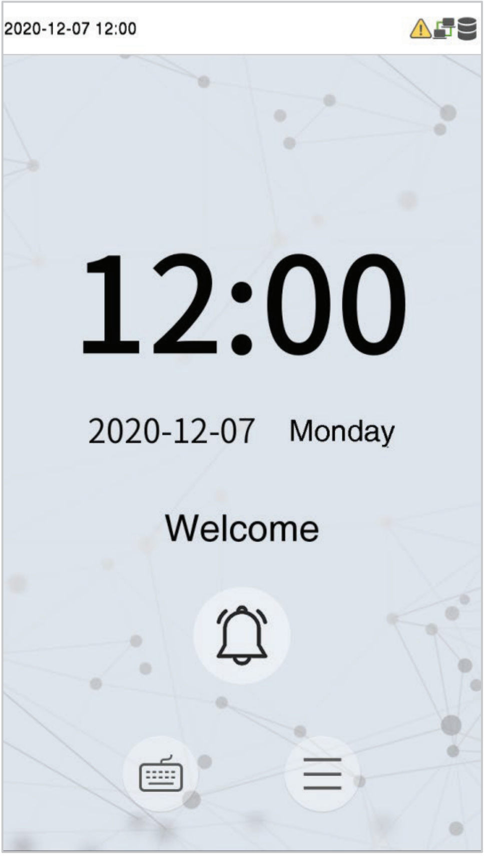
Correct face registration and authentication method

- **Recommendation for registering a face**
  - When registering a face, maintain a distance of 40cm to 80cm between the device and the face.
  - Be careful to keep your facial expression natural and not to change. (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.
  - Sometimes, authentication may fail due to the change in the wearing glasses then the one used while registration. In such a case, you may require authenticating your face with the previously worn glasses. If your face was registered without glasses, you should authenticate your face without glasses further.
  - 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.

1.4 Standby Interface

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



2020-12-07 12:00

12:00

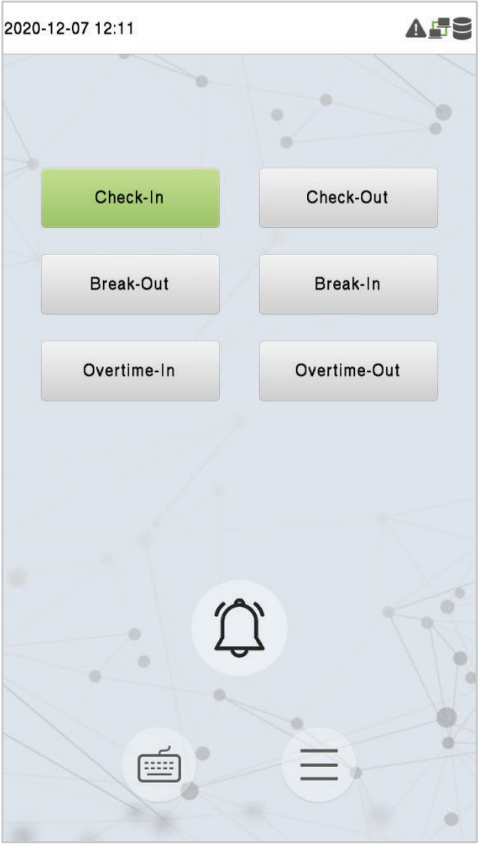
2020-12-07 Monday

Welcome

- Tap ⌨ to enter the User ID input interface.
- When there is no Super Administrator set in the device, t ☰ to go to the menu.
- After adding a Super Administrator on the device, it requires the Super Administrator's verification before opening the menu functions.

  NOTE: For the security of the device, it is recommended to register a super administrator the first time you use the device.

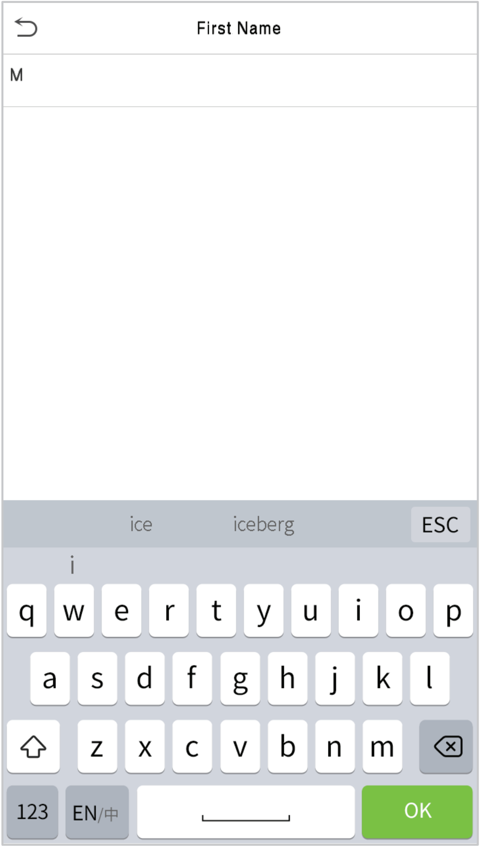
- The punch state options can also be displayed and used directly on the standby interface. Tap anywhere on the screen apart from the icons, and six shortcut keys appears on the screen, as shown in the figure below:



- Press the corresponding punch state key to select your current punch state, which is displayed in green. Please refer to Shortcut Key Mappings for the specific operation method.

NOTE: The punch state options are off by default and need to select other mode options in the Punch State Option to get the punch state options on the standby screen.

1.5 Virtual Keyboard



NOTE:

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

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

1.6 Verification Mode

1.6.1 Fingerprint Verification

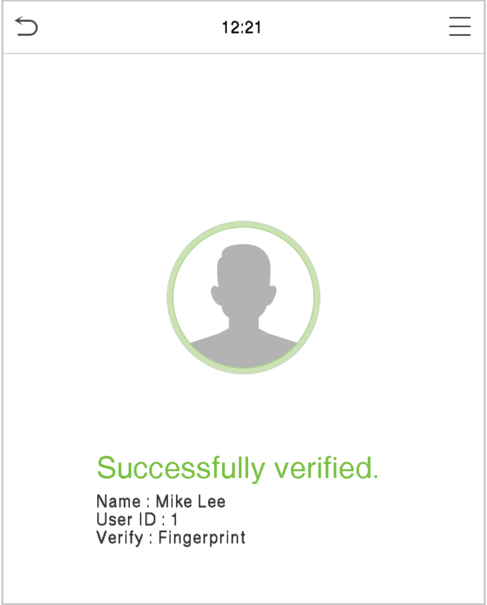
- **1: N fingerprint verification mode**

Compares the fingerprint that is being pressed onto the fingerprint reader with all of the fingerprint data that is stored in the device.

The device enters the fingerprint authentication mode when a user presses his/her finger onto the fingerprint scanner.

Please follow the correct way to place your finger onto the sensor. For details, please refer to section Finger Positioning.

Verification is successful.

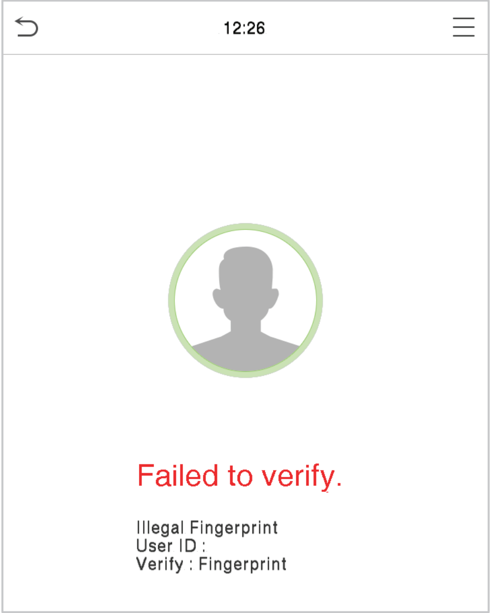


12:21

Successfully verified.

Name : Mike Lee
User ID : 1
Verify : Fingerprint

Verification is failed.



12:26

Failed to verify.

Illegal Fingerprint
User ID :
Verify : Fingerprint

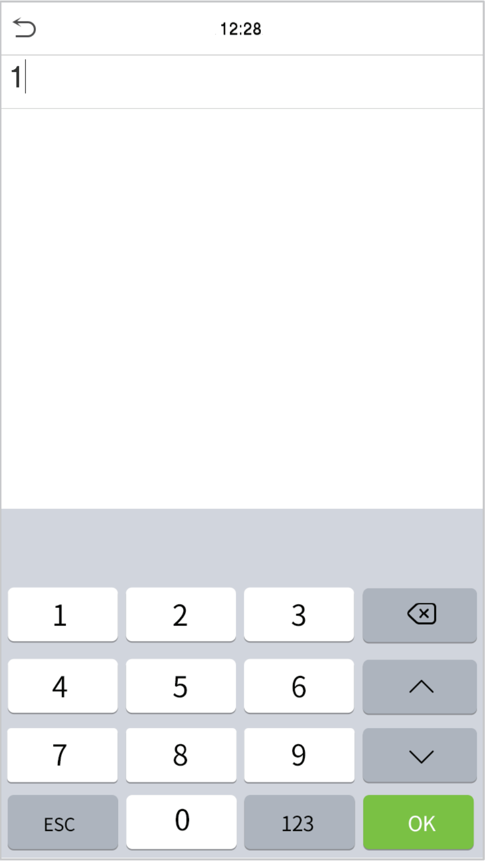
- **1: 1 fingerprint verification mode**

Compares the fingerprint that is being pressed onto the fingerprint reader with the fingerprints that are linked to User ID input via the virtual keyboard.

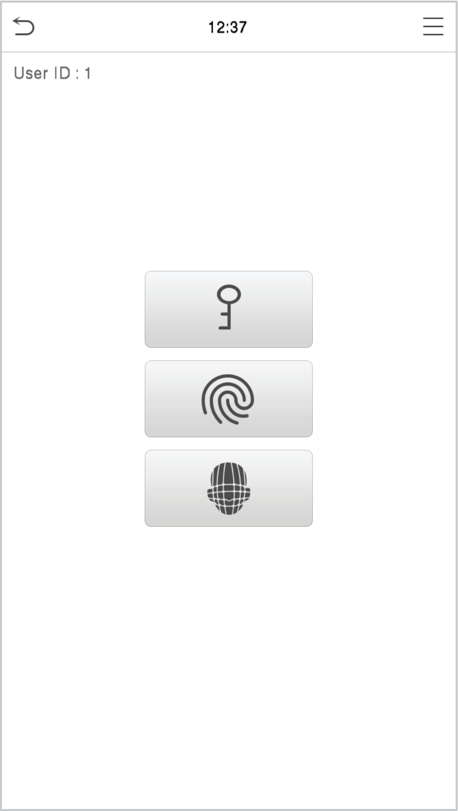
Users may verify their identities with 1:1 verification mode when they cannot gain access with 1: N authentication method.

Click the ⌨ button on the main screen to enter 1:1 fingerprint verification mode.

1. Input the user ID and press [OK].



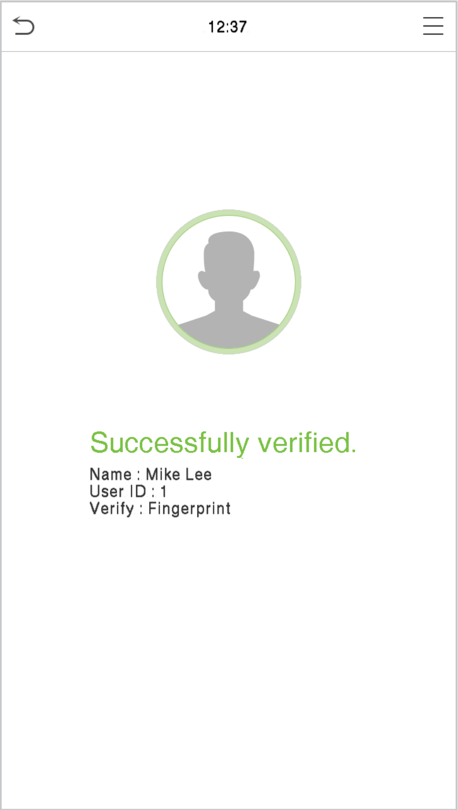
If the user has registered face and password in addition to his/her fingerprints and the verification method is set to Password/Fingerprint/Face verification, the following screen will appear. Select the ⦾gerprint icon to enter fingerprint verification mode.



User ID : 1

2. Press the fingerprint to verify.

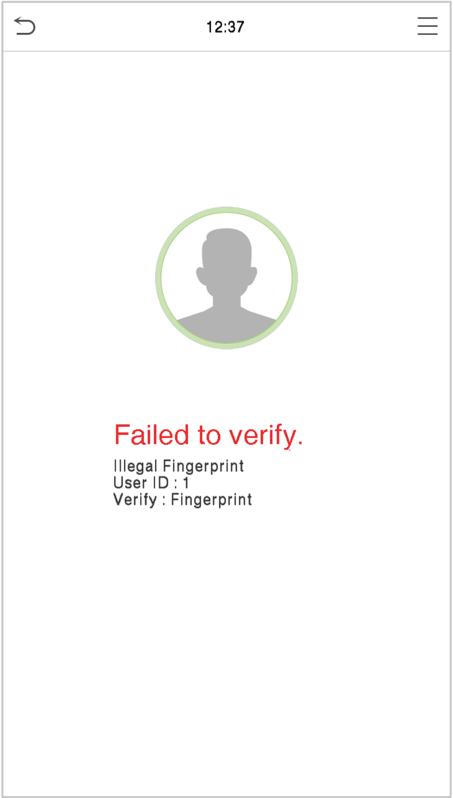
3. Verification is successful.



Successfully verified.

Name : Mike Lee
User ID : 1
Verify : Fingerprint

4. Verification is failed.



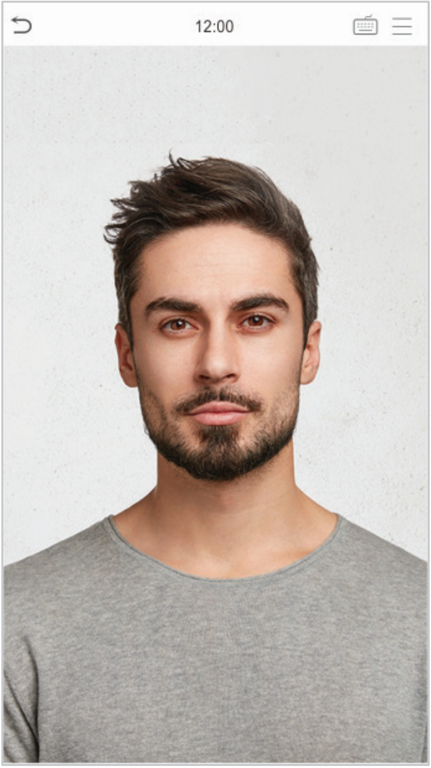
Failed to verify.

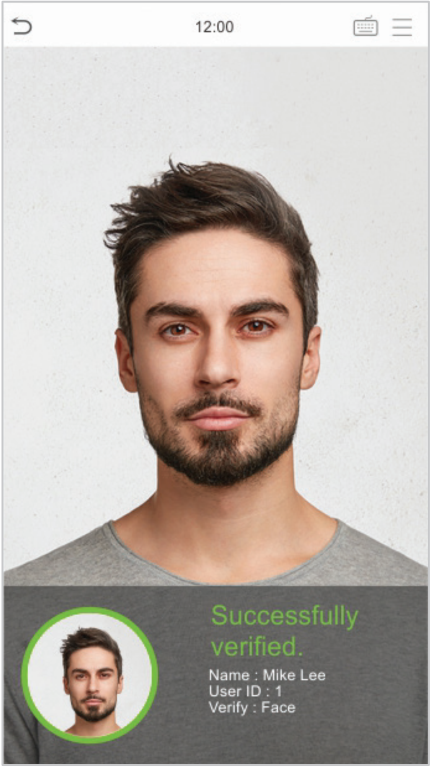
Illegal Fingerprint
User ID : 1
Verify : Fingerprint

16.2 Facial Verification

- **1:N Facial Verification**

It compares the acquired facial images with all face data registered in the device. The following is the pop-up prompt box of comparison results.





Successfully verified.

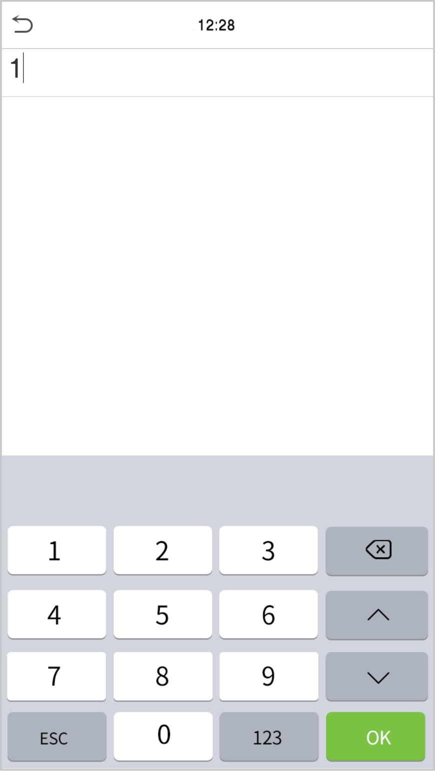
Name : Mike Lee
User ID : 1
Verify : Face

1:1 Facial Verification

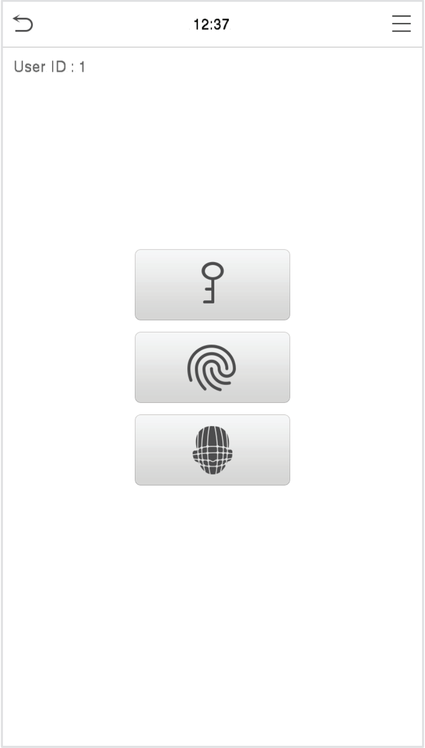
Compare the face captured by the camera with the facial template related to the entered user ID.

Press on the main interface and enter the 1:1 facial verification mode.

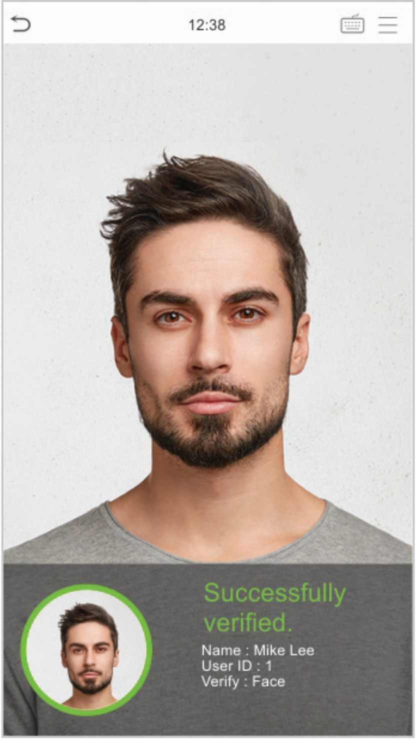
Enter the user ID and click [**OK**].



If an employee registers a fingerprint and password in addition to the face, the following screen will appear. Select the icon to enter face verification mode.


12:37
User ID : 1

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



12:38

Successfully verified.

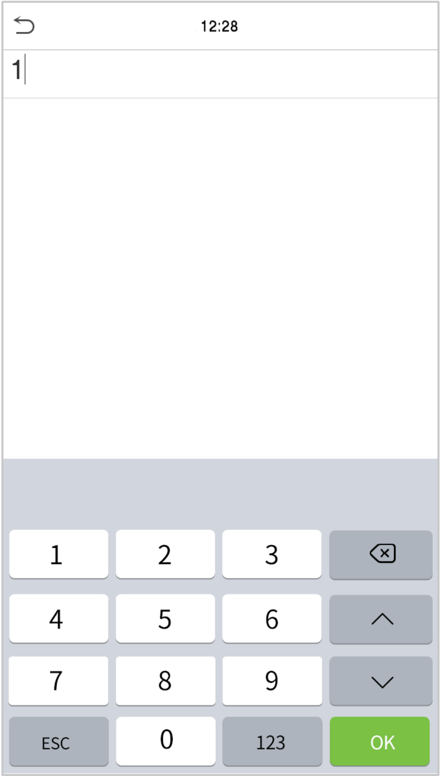
Name : Mike Lee
User ID : 1
Verify : Face

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

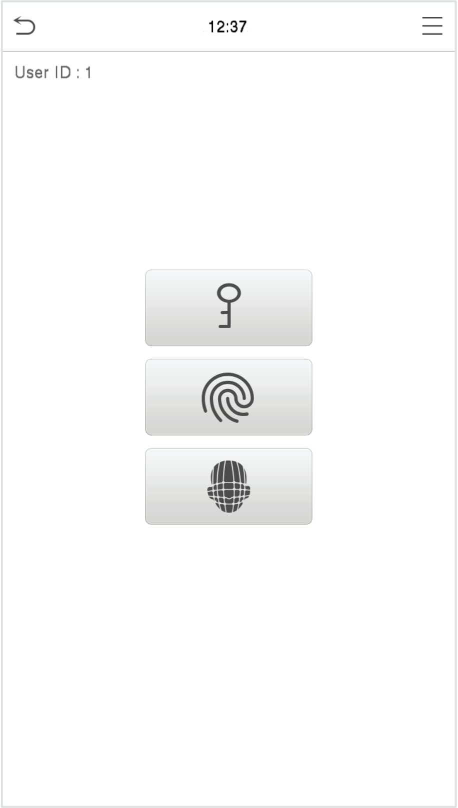
16.3 Password Verification

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

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

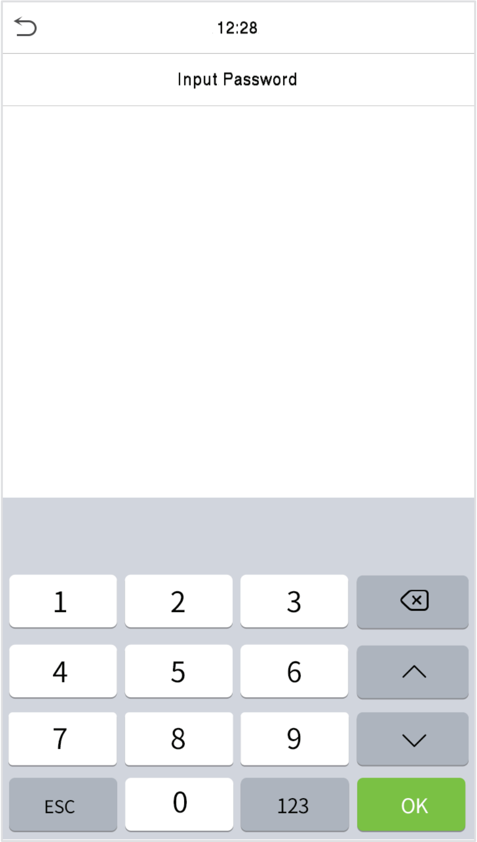


If an employee registers fingerprint and face in addition to password, the following screen will appear. Select the 🔑 icon to enter password verification mode.



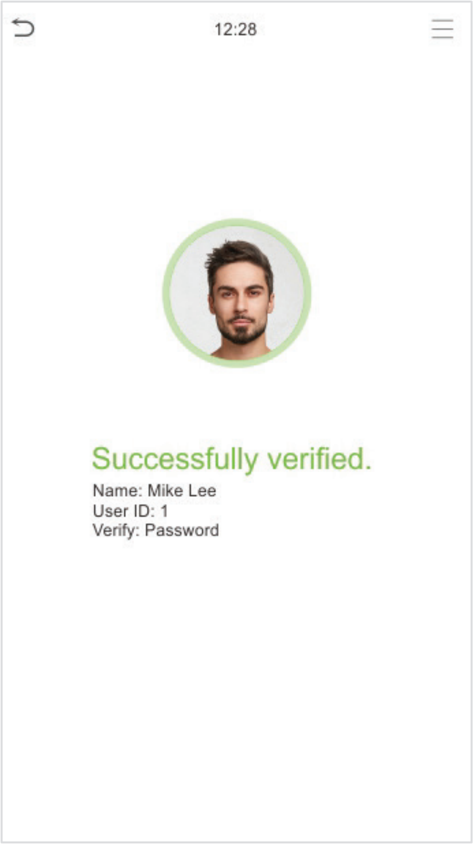
User ID : 1

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



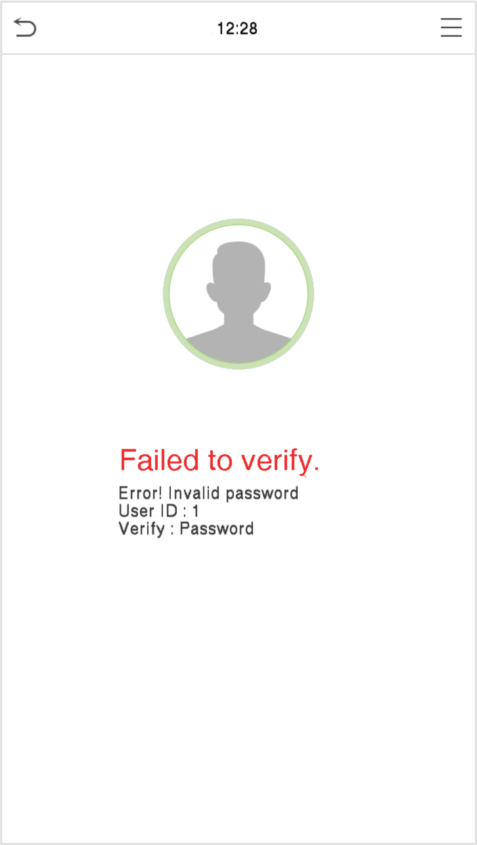
Following are the display screen after entering a correct password and a wrong password respectively.

Verification is successful: **Verification is failed:**



Successfully verified.

Name: Mike Lee
User ID: 1
Verify: Password

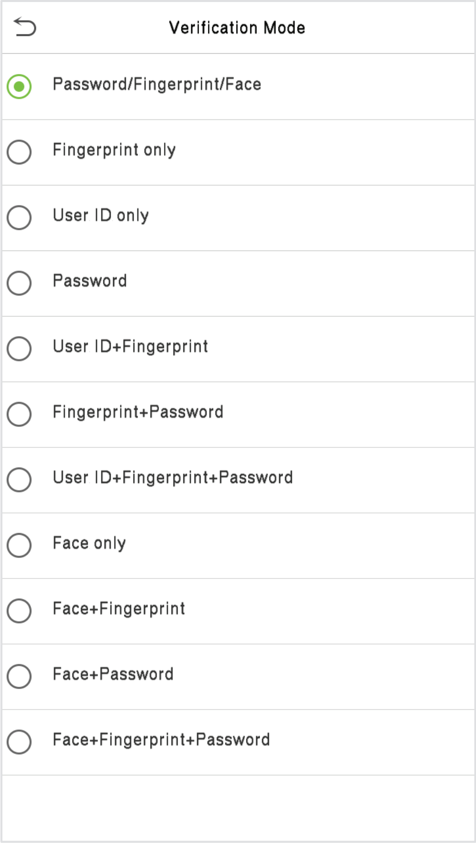


Failed to verify.

Error! Invalid password
User ID : 1
Verify : Password

16.4 Combined Verification

To increase security, this device offers the option of using multiple forms of verification methods.



Verification Mode

● Password/Fingerprint/Face

○ Fingerprint only

○ User ID only

○ Password

○ User ID+Fingerprint

○ Fingerprint+Password

○ User ID+Fingerprint+Password

○ Face only

○ Face+Fingerprint

○ Face+Password

○ Face+Fingerprint+Password

Procedure to set for Combined Verification Mode

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

But as the employee has registered only the Face but not the Password, the verification will not get completed and the Device displays "**Verification Failed**".

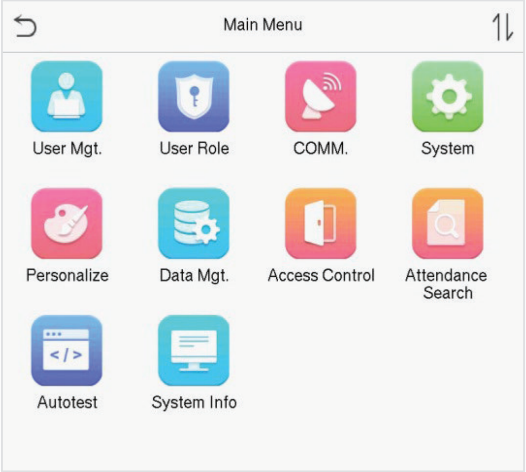
NOTE:

- "**/**" means "**or**", and "**+**" means "**and**".

- You must register the required verification information before using the combination verification mode, otherwise the verification may fail. For example, if a user uses Face Registration but the verification mode is Face + Password, this user will never pass verification.

2 Main Menu

Press ☰ on the initial interface to enter the main menu, as shown below:



Function Description

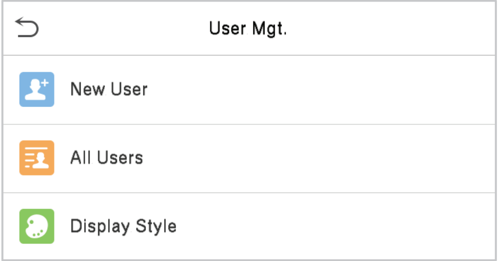
Menu	Descriptions
User Mgt.	To Add, Edit, View, and Delete information of a User.
User Role	To set the permission scope of the custom role and enroller for the users, that is, the rights to operate the system.
COMM.	To set the relevant parameters of Network, Serial Comm., PC Connection, Wireless Network, Cloud Server, Wiegand and Network Diagnosis.
System	To set parameters related to the system, including Date & Time, Access Logs Setting, Face & Fingerprint parameters, Video Intercom parameters, and resetting to factory settings.
Personalize	To customize settings of 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, Microphone, Fingerprint sensor, Camera, and Real-Time Clock.

System Info	To view Data Capacity and Device and Firmware information of the current device.

3 User Management

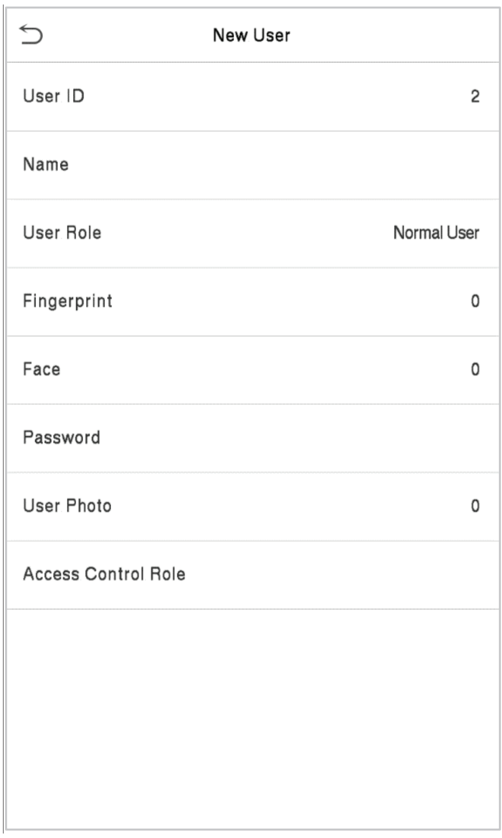
3.1 User Registration

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



- **Register a User ID and Name**

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



User ID 2

Name

User Role Normal User

Fingerprint 0

Face 0

Password

User Photo 0

Access Control Role

NOTE:

1） A name can take up to 17 characters.

2） The user ID may contain 1-9 digits by default.

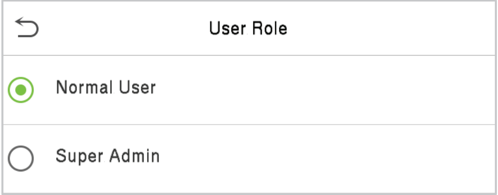
3） You can modify your ID during the initial registration but not after registration.

4) If a message "**Duplicated!**" pops up, you must choose another ID as the entered User ID already exists.

- **Setting the User Role**

There are two types of user accounts: the **normal user** and the **super admin**. If there is already a registered administrator, the normal users have no rights to manage the system and may only access authentication verifications. The administrator owns all management privileges. If a custom role is set, you can also select **user defined role** permissions for the user.

Click **User Role** to select Normal User or Super Admin.


User Role

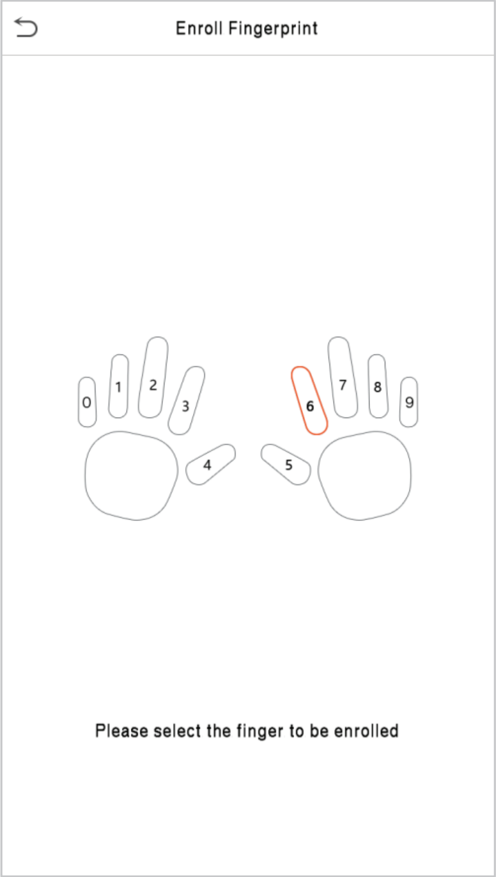
● Normal User

○ Super Admin

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 1.7 Verification Mode.

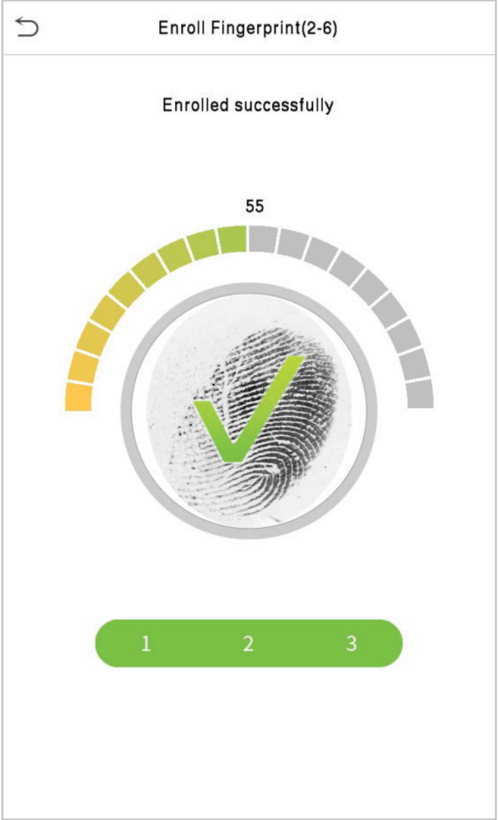
- **Register fingerprint**

Click **Fingerprint** to enter the fingerprint registration page. Select the finger to be enrolled.


Enroll Fingerprint

Please select the finger to be enrolled

Press the same finger on the fingerprint reader three times. Green indicates that the fingerprint was enrolled successfully.

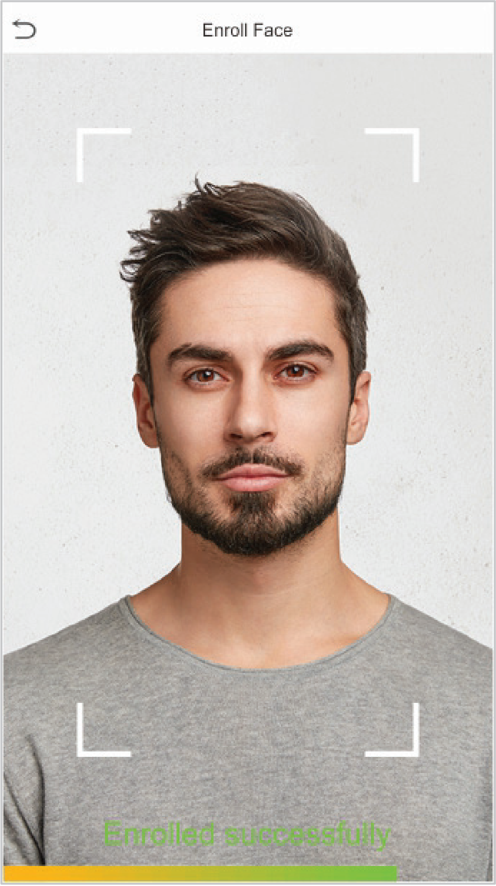


Enroll Fingerprint(2-6)

Enrolled successfully

- **Register face**

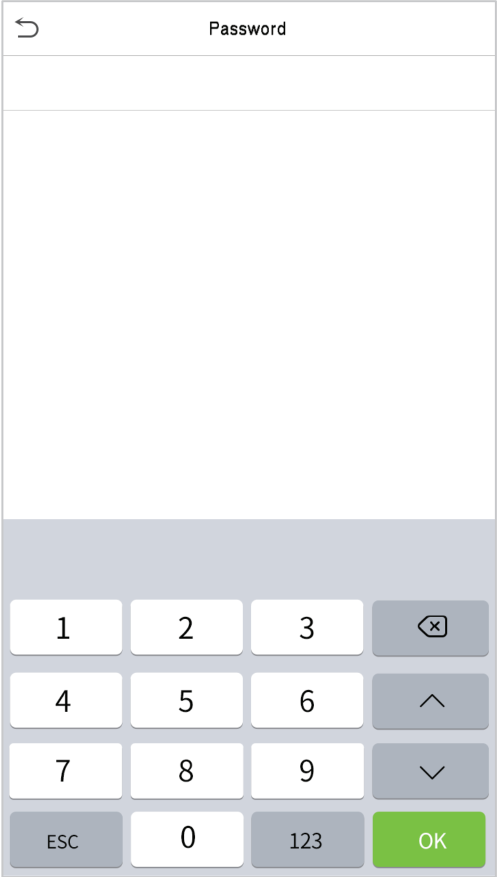
Click **Face** to enter the face registration page. Please face the camera and stay still during face registration. The registration interface is as follows:



Enrolled successfully

- **Register password**

Tap **Password** to enter the password registration page. Enter a password and re-enter it. Tap **OK**. If the two entered passwords are different, the prompt "**Password not match**!" will appear.



NOTE: The password may contain one to eight digits by default.

- **Register user photo**

When a user registered with a photo passes the authentication, the registered photo will be displayed.

Click **User Photo**, click the camera icon to take a photo. The system will return to the New User interface after taking a photo.

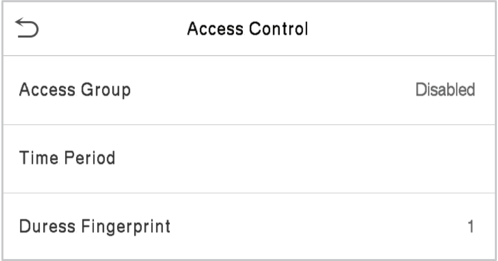
NOTE: While registering a face, the system will automatically capture a picture as the user photo. If you do not want to register a user photo, the system will automatically set the picture captured as the default photo.

- **Access Control Role**

User access control sets the door unlocking rights of each person, including the group and the time period that the user belongs to.

Click **Access Control Role** > **Access Group**, 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.

Click **Time Period**, select the time period to use.



Access Control

Access Group Disabled

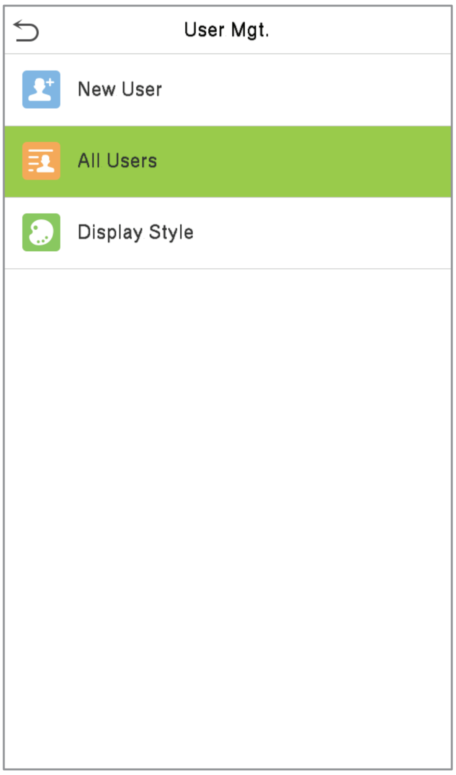
Time Period

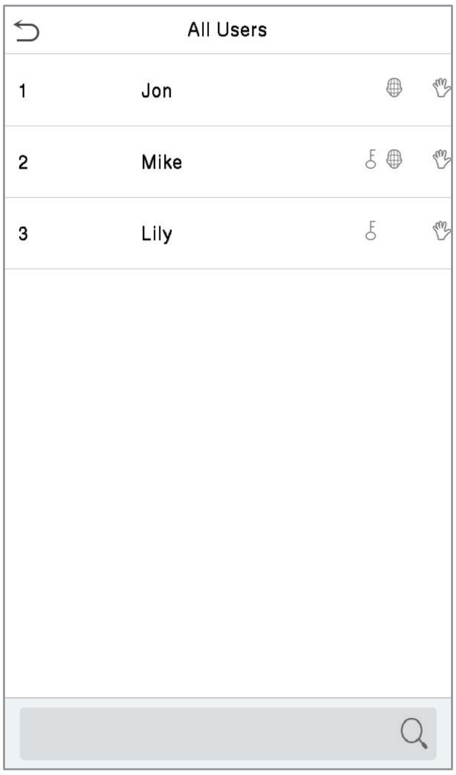
Duress Fingerprint 1

3.2 Search User

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





All Users

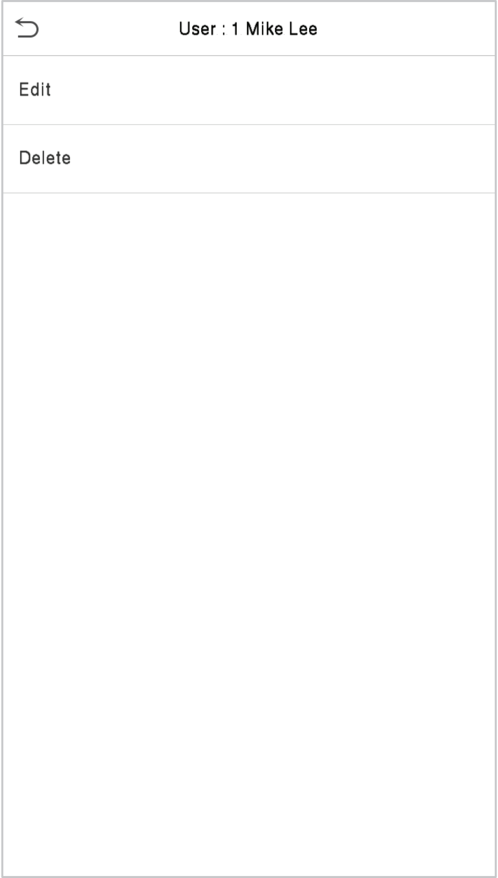
1 Jon

2 Mike

3 Lily

3.3 Edit User

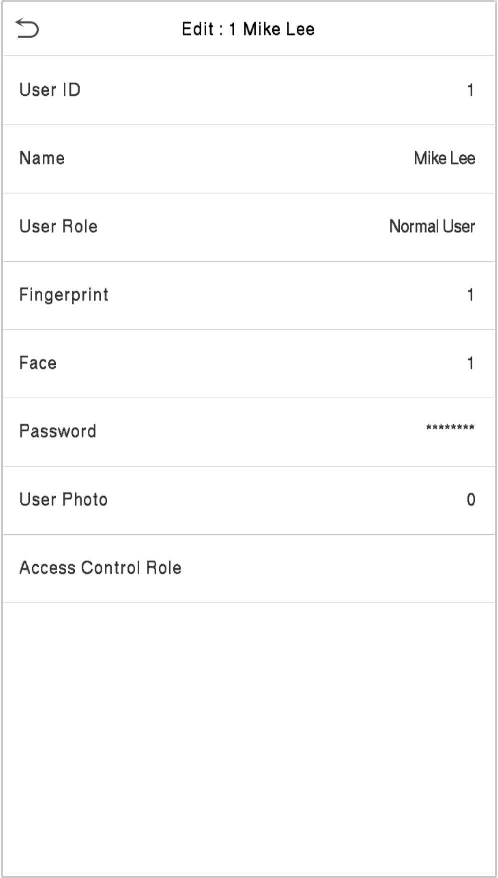
On the **All Users** interface, tap on the required user from the list and tap **Edit** to edit the user information.



User : 1 Mike Lee

Edit

Delete



Edit : 1 Mike Lee

User ID	1
Name	Mike Lee
User Role	Normal User
Fingerprint	1
Face	1
Password	********
User Photo	0
Access Control Role	

NOTE: The process of editing the user information is the same as adding a new user, except that the User ID cannot be modified when editing a user. The process in detail refers to "3.1 Adding users".

3.4 Deleting User

On the **All Users** interface, tap on the required user from the list and tap **Delete** to delete the user or 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 Face Only: Deletes the Face information of the selected user.

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

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

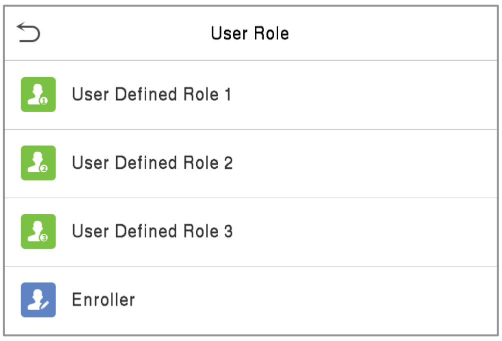
NOTE: If you select **Delete User**, all information of the user will be deleted.

4 User Role

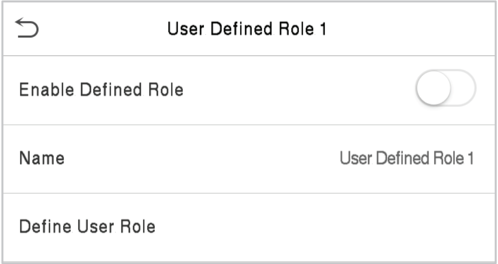
If you need to assign some specific permissions to certain users, you may edit the "User Defined Role" under the **User Role** menu.

You may set the permission scope of the custom role (up to 3 roles) and enroller, that is, the permission scope of the operation menu.

Click **User Role** on the main menu interface.

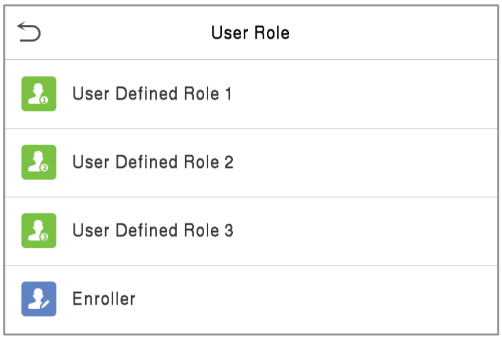


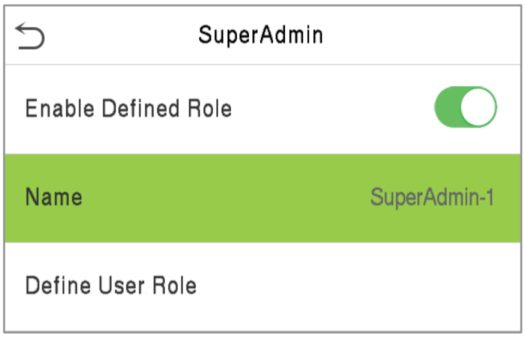
- On the **User Defined Role** interface, toggle **Enable Defined Role** to enable or disable the user-defined role.



Name User Defined Role 1

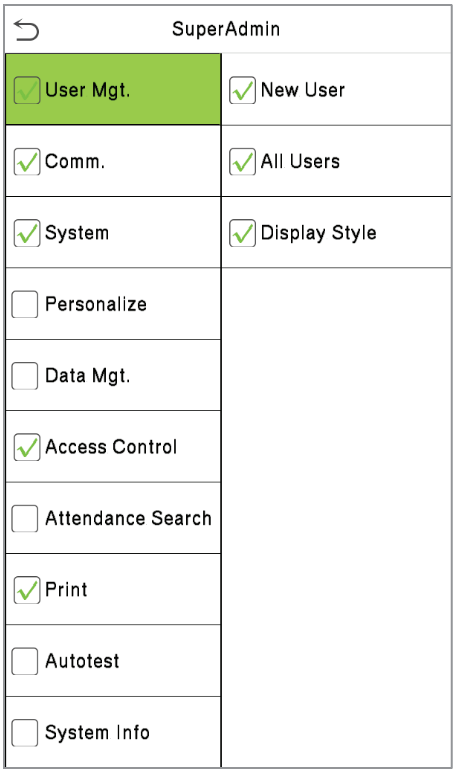
- Tap on **Name** and enter the custom name of the role.





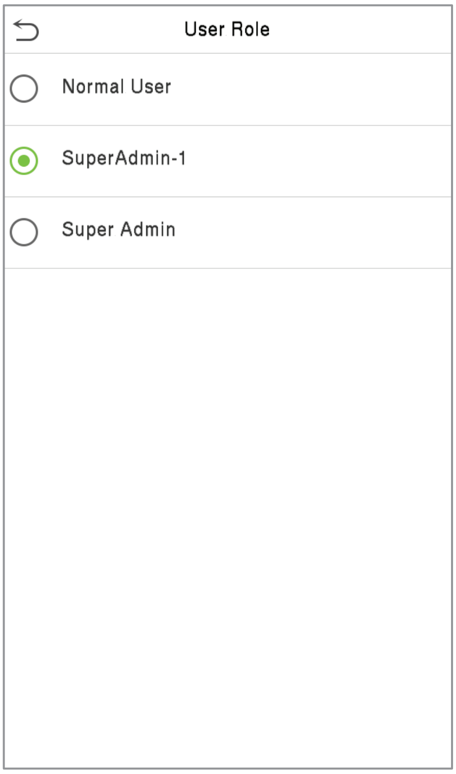
Name SuperAdmin-1

- 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** functions, and then select its required sub-menus from the list which the user can access.



SuperAdmin

☑ User Mgt.	☑ New User
☑ Comm.	☑ All Users
☑ System	☑ Display Style
□ Personalize	
□ Data Mgt.	
☑ Access Control	
□ Attendance Search	
☑ Print	
□ Autotest	
□ System Info	



User Role

○ Normal User

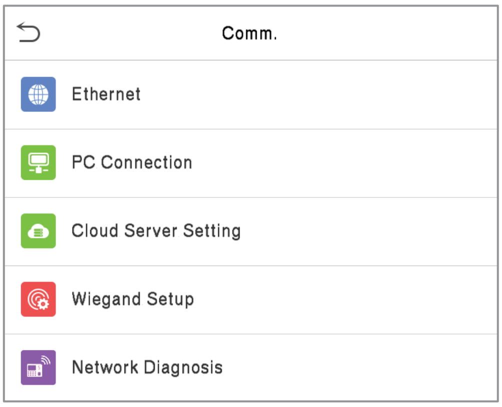
● SuperAdmin-1

○ Super Admin

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.

5 Communication Settings

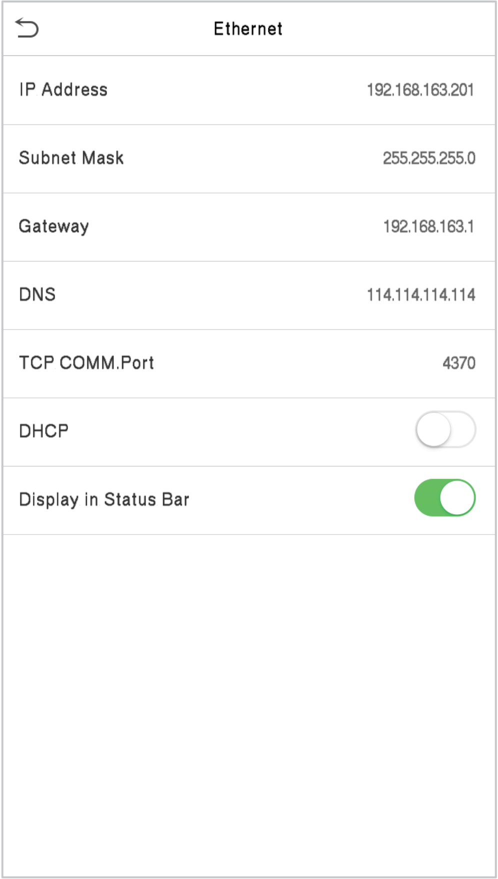
Tap **COMM.** on the **Main Menu** to set the Ethernet PC connection, Cloud Server setting and Wiegand.



5.1 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 connect to the same network segment.

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



Ethernet

IP Address	192.168.163.201
Subnet Mask	255.255.255.0
Gateway	192.168.163.1
DNS	114.114.114.114
TCP COMM.Port	4370
DHCP	○
Display in Status Bar	●

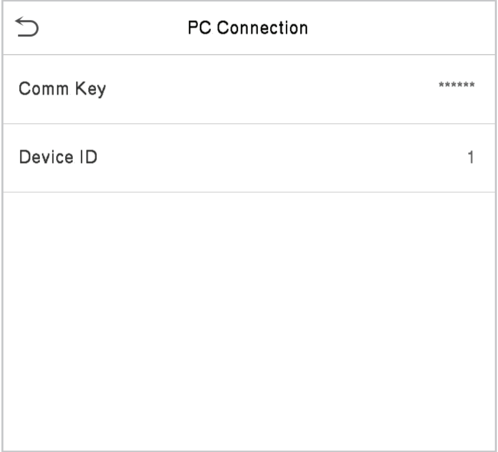
Function Description

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 dynamically allocates IP addresses for clients via server.
Display in Status Bar	Toggle to set whether to display the network icon on the status bar.

5.2 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, a password is required to connect the device to the PC software.

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



PC Connection

Comm Key ******

Device ID 1

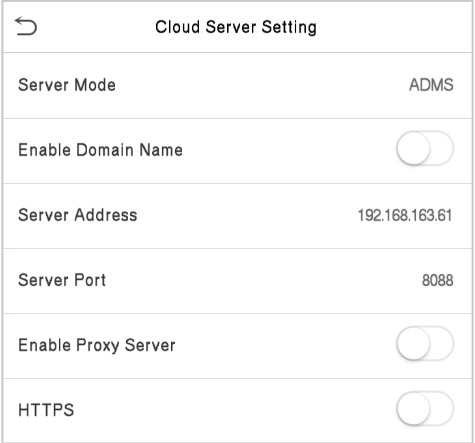
Function Description

Function Name	Descriptions
Comm Key	The default password is 0 and can be changed.

	The Comm Key can contain 1-6 digits.
Device ID	It is the identification 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.

5.3 Cloud Server Setting

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



Cloud Server Setting

Server Mode	ADMS
Enable Domain Name	
Server Address	192.168.163.61
Server Port	8088
Enable Proxy Server	
HTTPS	

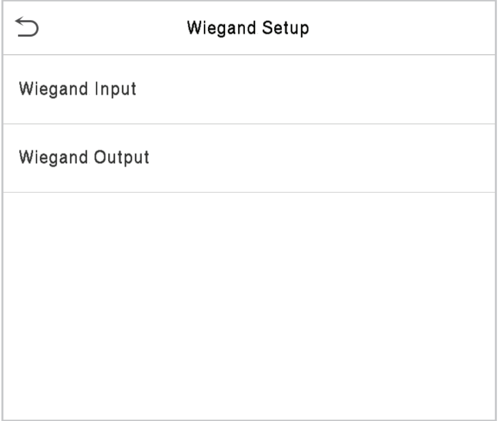
Function Description

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

5.4 Wiegand Setup

It is used to set the Wiegand input and output parameters.

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

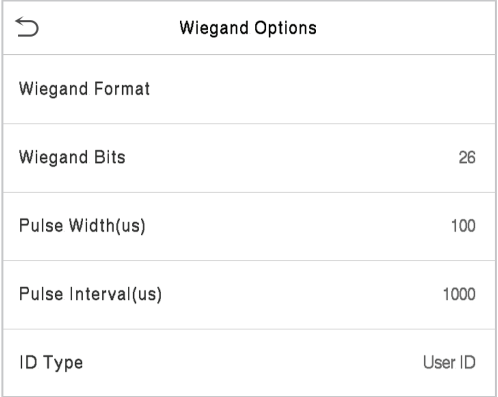


Wiegand Setup

Wiegand Input

Wiegand Output

5.4.1 Wiegand input



Wiegand Options

Wiegand Format

Wiegand Bits 26

Pulse Width(us) 100

Pulse Interval(us) 1000

ID Type User ID

Function Description

Function Name	Descriptions
Wiegand Format	Its value can be 26 bits, 34 bits, 36 bits, 37 bits, and 50 bits.
Wiegand Bits	The number of bits of the 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 and can be adjusted within the range of 200 to 20000 microseconds.
ID Type	Select between the User ID and card number.

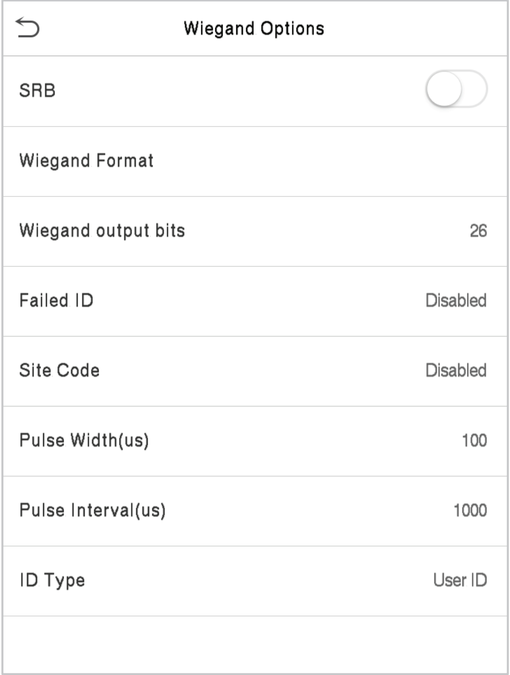
Various Common Wiegand Format Description:

Wiegand Format	Description

Wiegand26	ECCCCCCCCCCCCCCCCCCCCCCCCO It 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 is the card numbers.
Wiegand26a	ESSSSSSSSCCCCCCCCCCCCCCCCO It 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 is the site codes, while the 10th to 25th bits are the card numbers.
Wiegand34	ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO It 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 is the card numbers.
Wiegand34a	ESSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCO It 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 is the site codes, while the 10th to 25th bits are the card numbers.
Wiegand36	OFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCMME It 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 is the device codes. The 18th to 33rd bits is the card numbers, and the 34th to 35th bits are the manufacturer codes.
Wiegand36a	EFFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCO It 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 is the device codes, and the 20th to 35th bits are the card numbers.
Wiegand37	OMMMMSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCE It 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 is the manufacturer codes. The 5th to 16th bits is the site codes, and the 21st to 36th bits are the card numbers.
Wiegand37a	EMMMFFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCCO It 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 is the manufacturer codes. The 5th to 14th bits is the device codes, and15th to 20th bits are the site codes, and the 21st to 36th bits are the card numbers.
Wiegand50	ESSSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO It 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 is 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.

5.4.2 Wiegand output



Wiegand Options

SRB ○

Wiegand Format

Wiegand output bits 26

Failed ID Disabled

Site Code Disabled

Pulse Width(us) 100

Pulse Interval(us) 1000

ID Type User ID

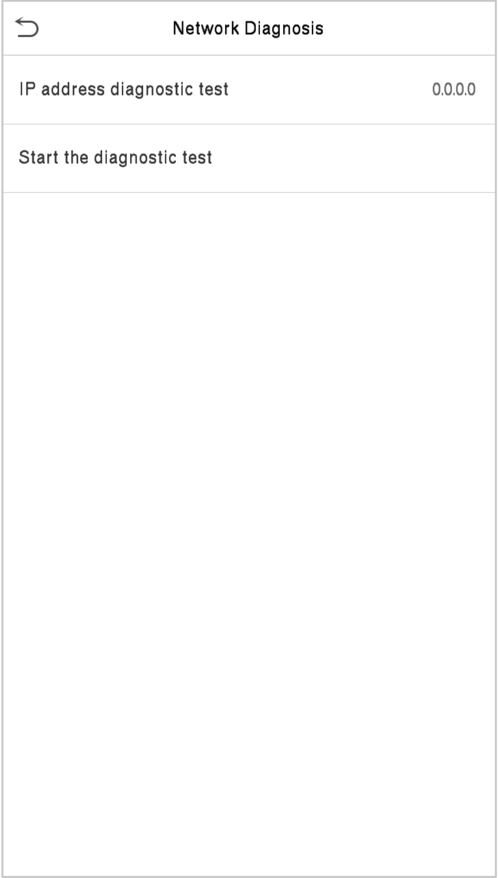
Function Description

Function Name	Descriptions
SRB	When SRB is enabled, the lock is controlled by the SRB to prevent the lock from opening due to device removal.
Wiegand Format	Its value can be 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 fails, 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 on a different device. The valid value ranges from 0 to 256 by default.
Pulse Width(**us**)	The time width represents the changes in 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.

Network Diagnosis

To set the network diagnosis parameters.

Click **Network Diagnosis** on the Comm. Settings interface. Enter the IP address that needs to be diagnosed, and click **Start the diagnostic test** to check whether the network can connect to the device.



Network Diagnosis

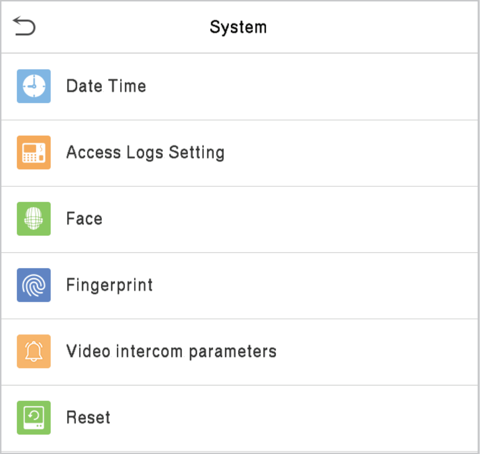
IP address diagnostic test 0.0.0.0

Start the diagnostic test

6 System Settings

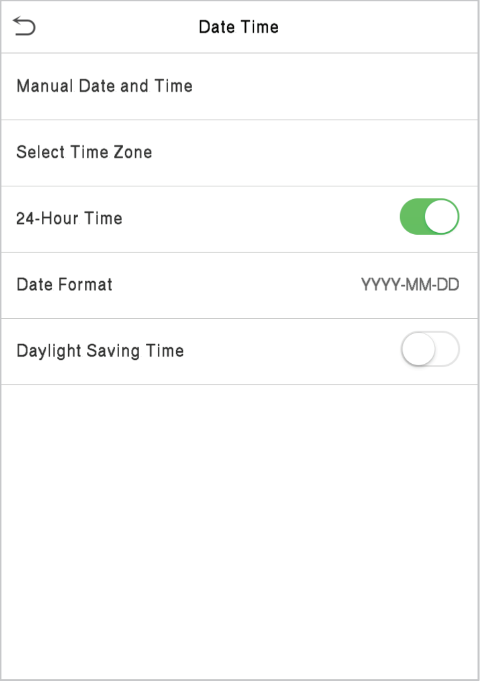
It helps to set related system parameters to optimize the accessibility of the device.

Tap **System** on the **Main Menu** interface to get into its menu options.



6.1 Date and Time

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



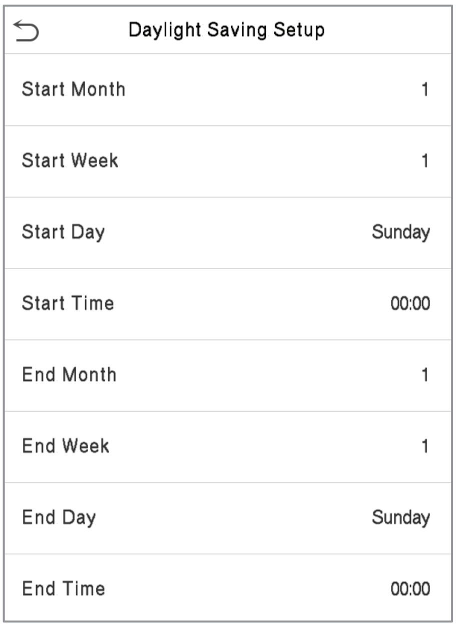
24-Hour Time: on

Date Format: YYYY-MM-DD

Daylight Saving Time: off

1. Tap **Manual Date and Time** to manually set date and time and tap **Confirm** to save.
2. Tap **Select Time Zone** to select a time zone then tap the return button to save and exit.
3. Tap **24-Hour Time** to enable or disable this format. If enabled, then select the **Date Format** to set the date format i.e., the way date should be displayed on the device.
4. ★ Tap **Daylight Saving Time** to enable or disable the function. If enabled, tap **Daylight**

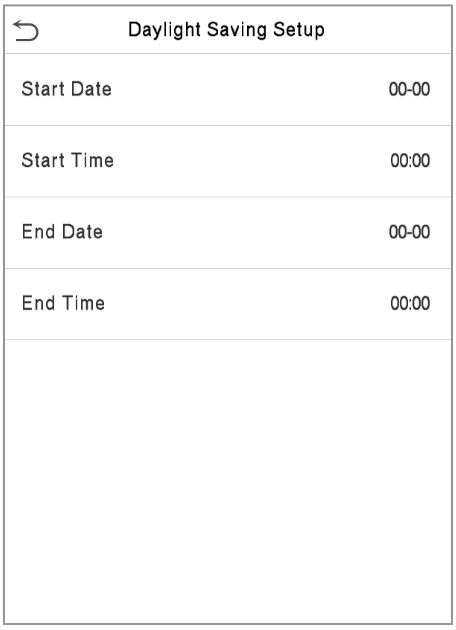
Saving Mode to select a daylight-saving mode and then tap **Daylight Saving Setup** to set the switch time.



Daylight Saving Setup

Start Month	1
Start Week	1
Start Day	Sunday
Start Time	00:00
End Month	1
End Week	1
End Day	Sunday
End Time	00:00

Week Mode



Daylight Saving Setup

Start Date	00-00
Start Time	00:00
End Date	00-00
End Time	00:00

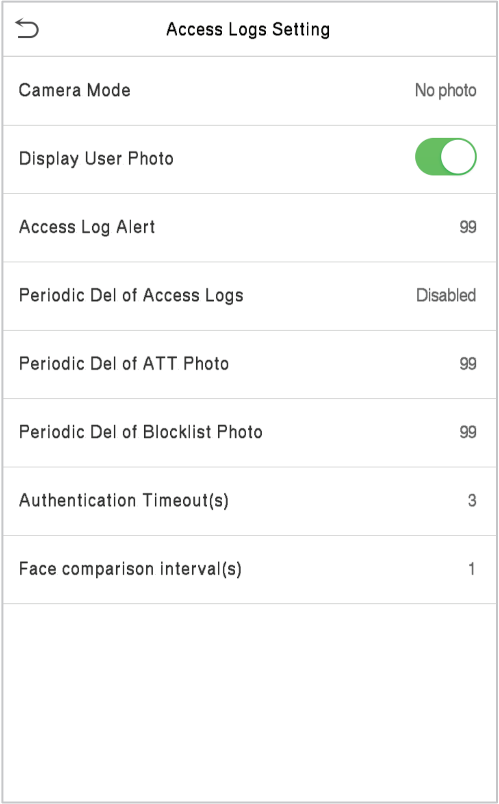
Date Mode

- 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, if a 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 device will remain at 18:30 on January 1, 2020.

6.2 Access Logs Setting

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



Access Logs Setting

Camera Mode	No photo
Display User Photo	●
Access Log Alert	99
Periodic Del of Access Logs	Disabled
Periodic Del of ATT Photo	99
Periodic Del of Blocklist Photo	99
Authentication Timeout(s)	3
Face comparison interval(s)	1

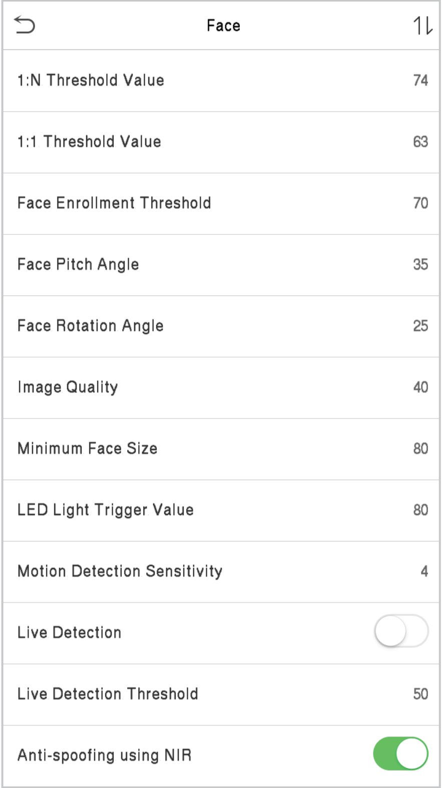
Function Description

Function Name	Description
Camera Mode	Choose 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 not saved during verification. **Take photo and save:** All the photos taken during verification is saved. **Save on successful verification:** Photo is taken and saved for each successful verification. **Save on failed verification:** Photo is taken and saved only for each failed verification.
Display User Photo	Choose whether to display the user photo when the user passes the verification.
Access Log Alert	When the record space of the attendance access reaches the maximum threshold value, the device automatically displays the memory space warning. Users may disable the function or set a valid value between 1 and 9999.
Periodic Del of Access Logs	When access logs reach its maximum capacity, the device automatically deletes a set of old access logs. Users may disable the function or set a valid value between 1 and 999.

Periodic Del of ATT Photo	When attendance photos reach its maximum capacity, the device automatically deletes a set of old attendance photos. Users may disable the function or set a valid value between 1 and 99.
Periodic Del of Blocklist Photo	When block listed photos reach its maximum capacity, the device automatically deletes a set of old block listed photos. Users may disable the function or set a valid value between 1 and 99.
Authentication Timeout(**s**)	The amount of time taken to display a successful verification message. Valid value: 1~9 seconds.
Face comparison Interval (**s**)	The amount of time required to compare facial templates. Valid value: 0~9 seconds.

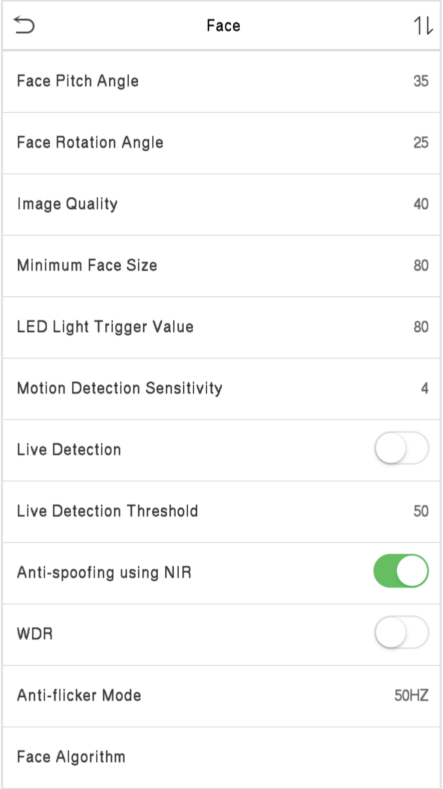
6.3 Face Parameters

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



Face

1:N Threshold Value	74
1:1 Threshold Value	63
Face Enrollment Threshold	70
Face Pitch Angle	35
Face Rotation Angle	25
Image Quality	40
Minimum Face Size	80
LED Light Trigger Value	80
Motion Detection Sensitivity	4
Live Detection	○
Live Detection Threshold	50
Anti-spoofing using NIR	●



Face

Face Pitch Angle	35
Face Rotation Angle	25
Image Quality	40
Minimum Face Size	80
LED Light Trigger Value	80
Motion Detection Sensitivity	4
Live Detection	○
Live Detection Threshold	50
Anti-spoofing using NIR	●
WDR	○
Anti-flicker Mode	50HZ
Face Algorithm	

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 and 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 and 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 the set threshold, it indicates that the face has already been registered.
Face Pitch Angle	It is the pitch angle tolerance of a face for facial template registration and comparison. If a face's pitch angle exceeds the 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	It is the rotation angle tolerance of a face for facial template registration and comparison. If a face's rotation angle exceeds the 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	It is the image quality for facial registration and comparison. The higher the value, the clearer image is required.
Minimum Face Size	It sets the minimum face size required for facial registration and comparison. If the minimum size of the captured image is smaller than the set value, then it will be filtered off and not recognized as a face. This value can also be interpreted as the face comparison distance. The farther the individual is, the smaller the face, and the smaller number of pixels of the face obtained by the algorithm. Therefore, adjusting this parameter can adjust the farthest comparison distance of faces. When the value is 0, the face comparison distance is not limited.
LED Light Trigger Threshold	This value controls the turning on and off of the LED light. The larger the value, the LED light will turn on or off more frequently.
Motion Detection Sensitivity	It sets the value for the amount of change in a camera's field of view 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 activates with much ease, and the motion detection is frequently triggered.
Live Detection	It detects the spoof attempt using visible light images to determine if the provided biometric source sample is of a real person (a live human being) or a false representation.
Live Detection Threshold	It facilitates judging whether the captured visible image is a real 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) balances light and extends image visibility for surveillance videos under high contrast lighting scenes and improves object identification under bright and dark environments.
Anti-flicker Mode	It is used when WDR is turned off. It helps to reduce flicker when the device's screen flashes at the same frequency as the light.
Face Algorithm	It has facial algorithm related information and pause facial template update.

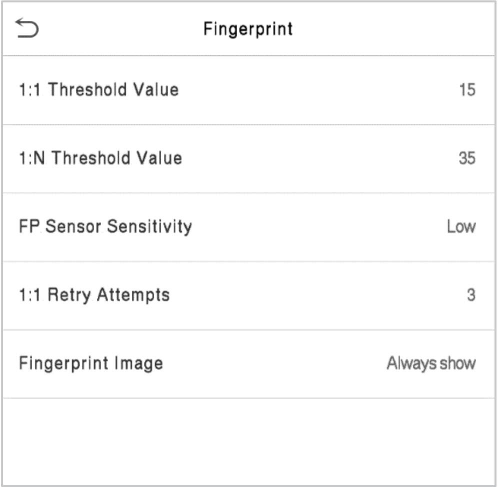
NOTE: Improper adjustment of the exposure and quality parameters may severely affect the performance of the device. Please adjust the exposure parameter only under the guidance of the after-sales service personnel of our company.

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. It is recommended not to move the face in a wide range.

6.4 Fingerprint Parameters

Click **Fingerprint** on the System interface.



Fingerprint

1:1 Threshold Value 15

1:N Threshold Value 35

FP Sensor Sensitivity Low

1:1 Retry Attempts 3

Fingerprint Image Always show

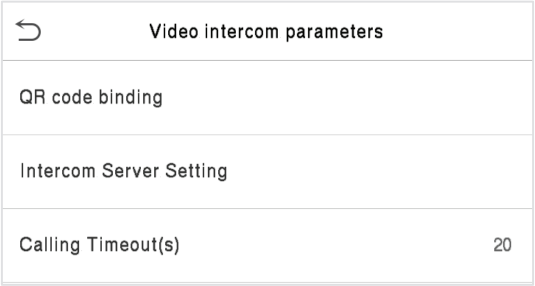
FRR	FAR	Recommended matching thresholds	
		1:N	1:1
High	Low	45	25
Medium	Medium	35	15
Low	High	25	10

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 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	In 1:1 Verification, users might forget the registered fingerprint, or press the finger improperly. To reduce the process of re-entering user ID, retry is allowed.
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.

6.5 Video intercom parameters

Click **Video intercom parameters** on the System interface.


Video intercom parameters

QR code binding

Intercom Server Setting

Calling Timeout(s) 20

Function Description

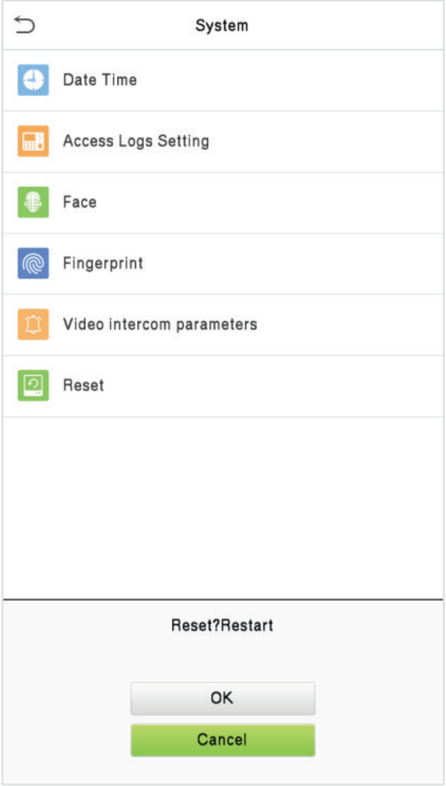
Function Name	Description

QR code binding	Use the APP client to scan the QR code to connect and bind the device.
Intercom Server Setting	Set the IP address and port number of the intercom server. **Server Address:** Enter the sever installation IP address. **Server Port:** It is the service port set during installation (not the ADMS port).
Calling Timeout(s)	If the call is not answered within a specified time, it exits to the main interface.

6.6 Factory Reset

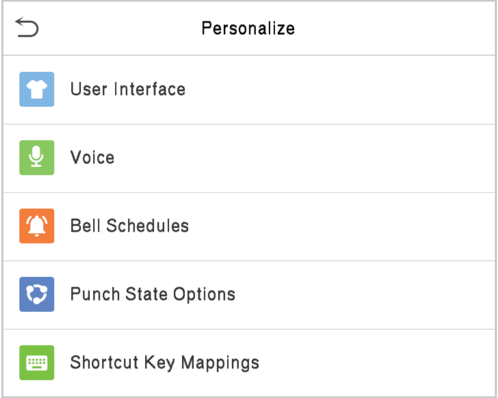
The Factory Reset function restores the device settings such as communication settings and system settings, to the default factory settings (this function does not clear registered user data).

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



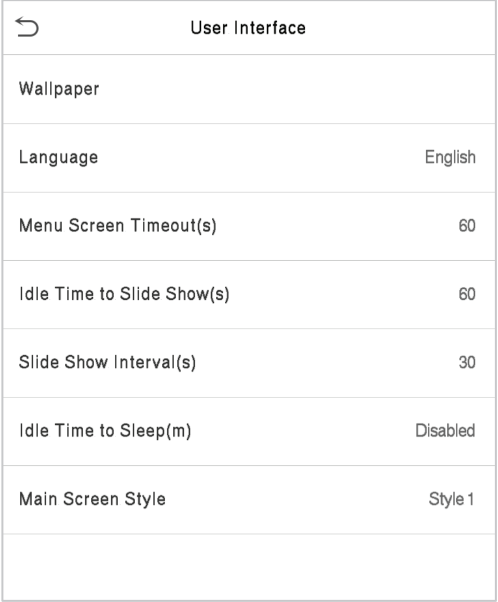
7 Personalize Settings

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



7.1 Interface Settings

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



User Interface

Wallpaper

Language English

Menu Screen Timeout(s) 60

Idle Time to Slide Show(s) 60

Slide Show Interval(s) 30

Idle Time to Sleep(m) Disabled

Main Screen Style Style 1

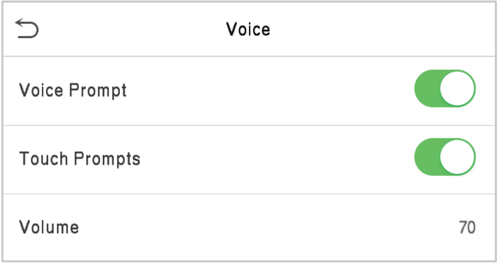
Function Description

Function Name	Description
Wallpaper	It helps to select the main screen wallpaper according to the user preference.
Language	It helps to select the language of the device.
Menu Screen Timeout (s)	When there is no operation, and the time exceeds the set value, the device automatically goes back to the initial interface.

	The function can either 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 is displayed. 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 style of the main screen can be selected according to the user preference.

7.2 Voice Settings

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



Voice

Voice Prompt

Touch Prompts

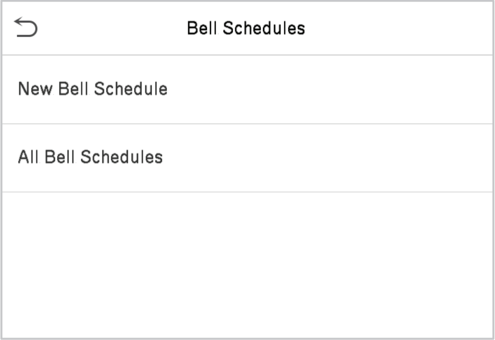
Volume 70

Function Description

Function Name	Description
Voice Prompt	Select whether to enable voice prompts during operating.
Touch Prompt	Select whether to enable keypad sounds.
Volume	Adjust the volume of the device; valid value: 0-100.

7.3 Bell Schedules

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



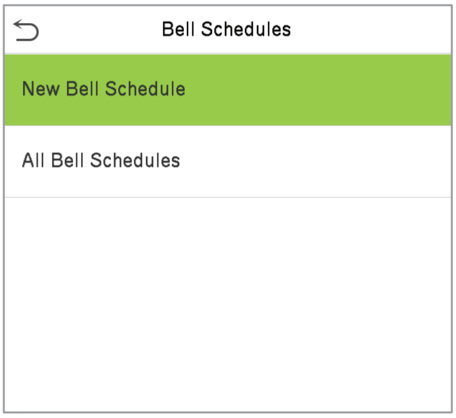
Bell Schedules

New Bell Schedule

All Bell Schedules

New Bell Schedule

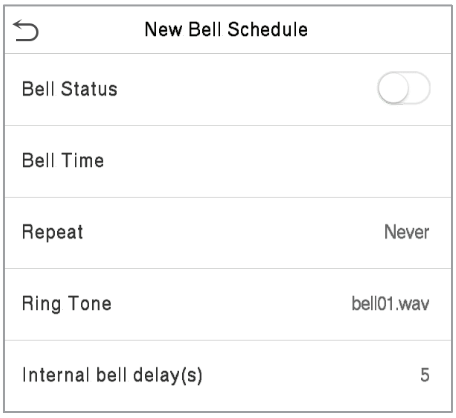
Tap **New Bell Schedule** on the **Bell Schedule** interface to add a new bell schedule.



Bell Schedules

New Bell Schedule

All Bell Schedules



New Bell Schedule

Bell Status

Bell Time

Repeat Never

Ring Tone bell01.wav

Internal bell delay(s) 5

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 automatically triggers to ring the bell during that time.
Repeat	Set the required number of counts to repeat the scheduled bell.
Ring Tone	Select a ringtone.
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

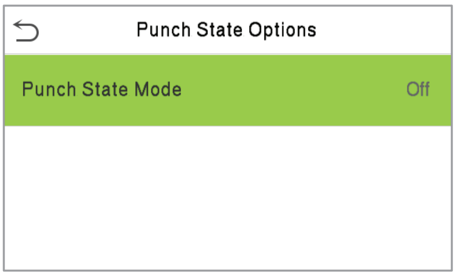
On the **All Bell Schedules** interface, tap on the required bell schedule, and tap **Edit** to edit the selected bell schedule. The editing method is the same as the operations of adding a new bell schedule.

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.

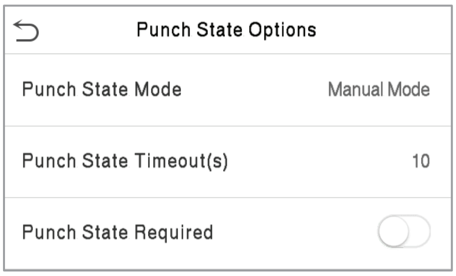
7.4 Punch States Options

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



Punch State Options

Punch State Mode Off



Punch State Options

Punch State Mode Manual Mode

Punch State Timeout(s) 10

Punch State Required ○

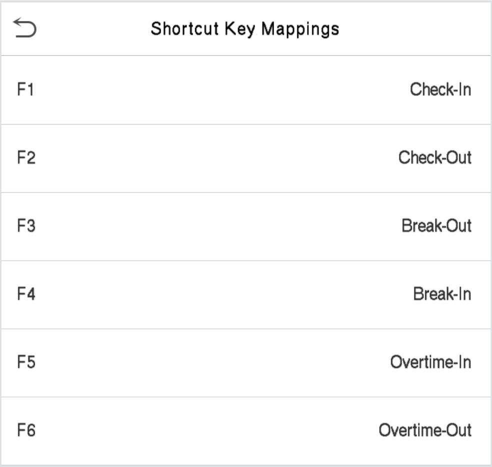
Function Description

Function Name	Description
Punch State Mode	Select a punch state mode, which can be: **Off:** It disables the punch state function. And the punch state key set under the **Shortcut Key Mappings** menu becomes 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 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 an alternative that is the manual attendance status. After the timeout, the manual switching punch state key will become an 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 manually switched again. **Fixed Mode:** Only the manually fixed punch state key is shown. Users cannot change the status by pressing any other keys.
Punch State Timeout(s)	It is the amount of time for which the punch state is displayed. The value ranges from 5~999 seconds.
Punch State Required	To choose whether an attendance state needs to be selected during verification.

7.5 Shortcut Keys Mappings

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

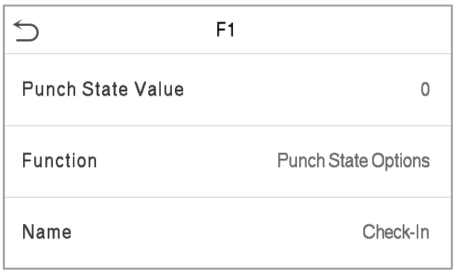
Tap **Shortcut Key Mappings** on the **Personalize** interface to set the required shortcut keys.



Shortcut Key Mappings

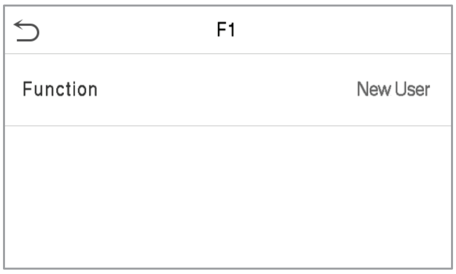
F1	Check-In
F2	Check-Out
F3	Break-Out
F4	Break-In
F5	Overtime-In
F6	Overtime-Out

- On the **Shortcut Key Mappings** interface, tap on the required shortcut key to configure the shortcut key settings.
- On the **Shortcut Key** ("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 done as shown in the image below.



F1

Punch State Value	0
Function	Punch State Options
Name	Check-In



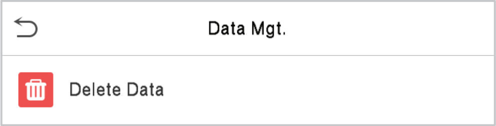
F1

Function	New User

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.

8 Data Management

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

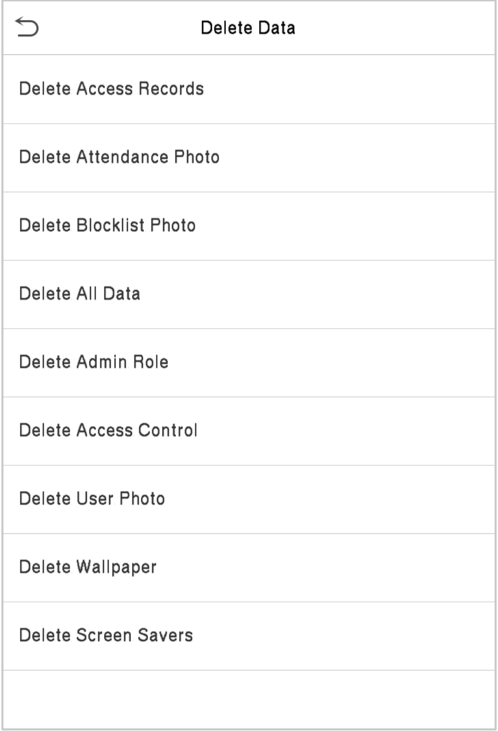


Data Mgt.

Delete Data

8.1 Delete Data

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



Delete Data

Delete Access Records

Delete Attendance Photo

Delete Blocklist Photo

Delete All Data

Delete Admin Role

Delete Access Control

Delete User Photo

Delete Wallpaper

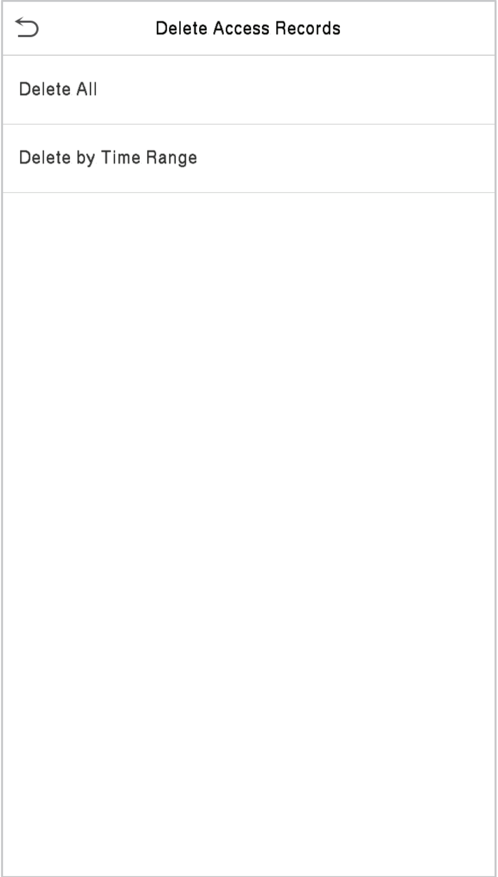
Delete Screen Savers

Function Description

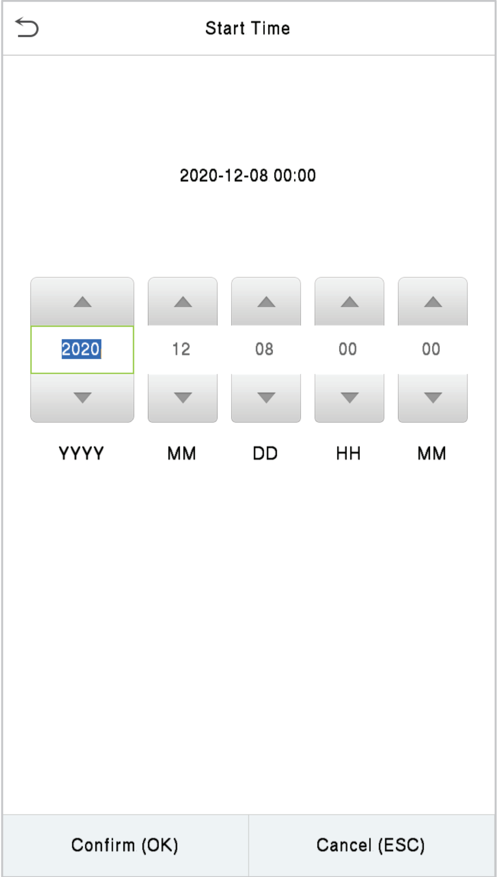
Function Name	Description
Delete Access Records	To delete attendance data/access records conditionally.
Delete Attendance Photo	To delete attendance photos of designated personnel.
Delete Blacklist Photo	To delete the photos taken during failed verifications.
Delete All Data	To delete information and attendance logs/access records of all registered users.
Delete Admin Role	To remove 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.



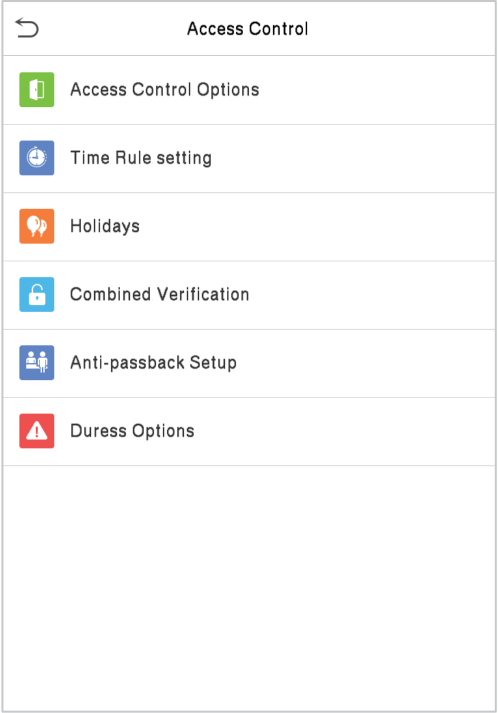
Select Delete by Time Range



Set the time range and click **OK**

9 Access Control

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

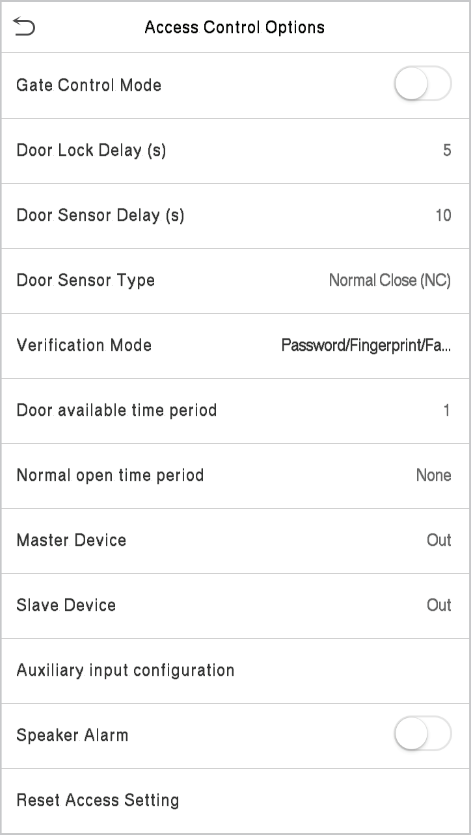


To gain access, the registered user must meet the following conditions:

1. The relevant door's current unlock time should be within any valid time zone of the user's time period.
2. 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 is also required to unlock the door).
3. 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.

9.1 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.



Access Control Options

Gate Control Mode ○

Door Lock Delay (s) 5

Door Sensor Delay (s) 10

Door Sensor Type Normal Close (NC)

Verification Mode Password/Fingerprint/Fa...

Door available time period 1

Normal open time period None

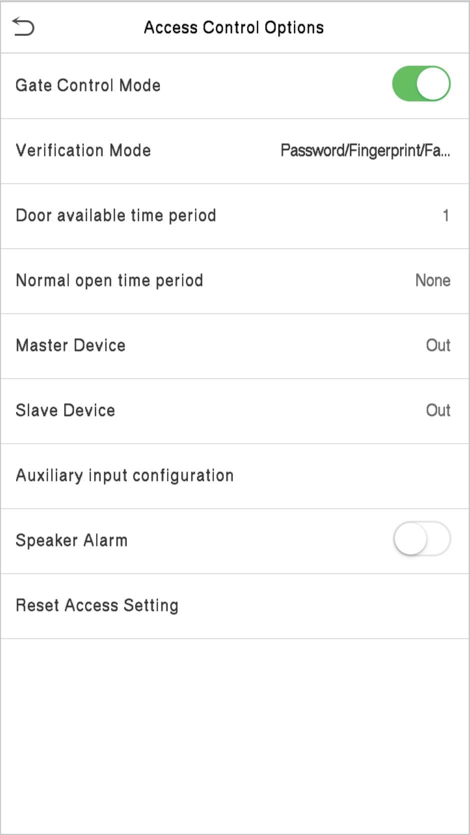
Master Device Out

Slave Device Out

Auxiliary input configuration

Speaker Alarm ○

Reset Access Setting



Access Control Options

Gate Control Mode ●

Verification Mode Password/Fingerprint/Fa...

Door available time period 1

Normal open time period None

Master Device Out

Slave Device Out

Auxiliary input configuration

Speaker Alarm ○

Reset Access Setting

Function Description

Function Name	Description
GateControl Mode	It toggles between **ON** or **OFF** switch to get into gate control mode or not. When set to **ON**, the interface removes the 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 seconds represents disabling the function.
Door Sensor Delay (s)	If the door is not locked and is 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 the door sensor is not in use. **Normally Open:** It means the door is always left open when electric power is on. **Normally Closed:** It means the door is always left closed when electric power is on.
Verification Mode	The supported verification mode includes Password/Face/Palm, User ID only, Password, Face only, Face + Password, Palm, and Palm + Face.
Door available time period	It sets the timing for the door so that the door is accessible only during that period.
Normal open time Period	It is the scheduled time-period for “Normal Open” mode so that the door is always open during this period.
Master Device	While configuring the master and slave devices, you may set the state of the master as **Out** or **In**. **Out**: A record of verification on the master device is a check-out record. **In**: A record of verification on the master device is a check-in record.
Slave Device	While configuring the master and slave devices, you may set the state of the slave as **Out** or **In**. **Out**: A record of verification on the slave device is a check-out record. **In**: A record of verification on the slave device is a check-in 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.
Speaker Alarm	It transmits a sound alarm or disassembly alarm from the local. When the door is closed or the verification is successful, the system cancels 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.

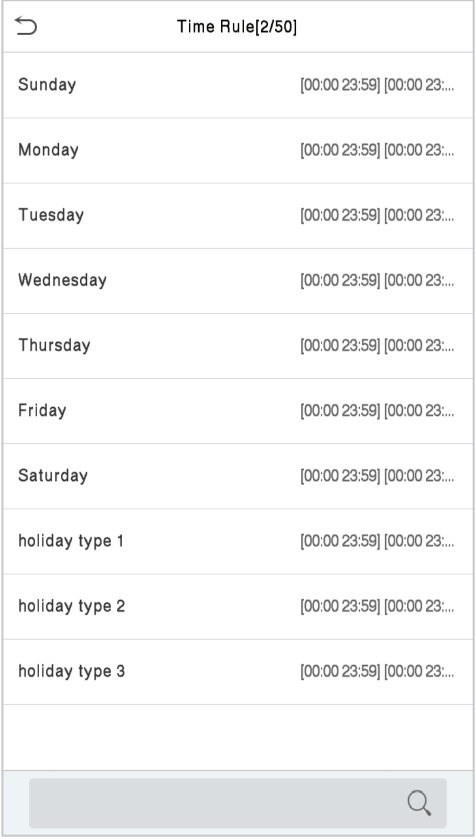
9.2 Time Schedule

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 is **HH MM-HH MM**, which is accurate to minutes according to the 24-hour clock.

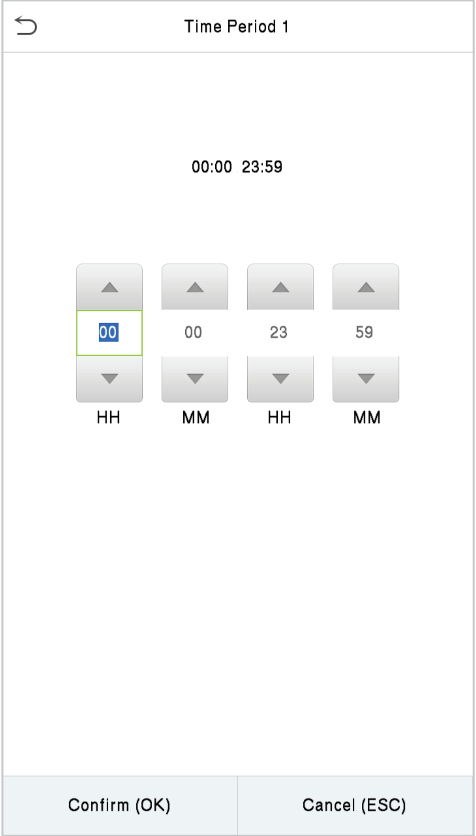
Tap the grey box to search the required Time Zone and specify the required Time Zone number (maximum up to 50 zones).



Time Rule[2/50]

Sunday	[00:00 23:59] [00:00 23:...
Monday	[00:00 23:59] [00:00 23:...
Tuesday	[00:00 23:59] [00:00 23:...
Wednesday	[00:00 23:59] [00:00 23:...
Thursday	[00:00 23:59] [00:00 23:...
Friday	[00:00 23:59] [00:00 23:...
Saturday	[00:00 23:59] [00:00 23:...
holiday type 1	[00:00 23:59] [00:00 23:...
holiday type 2	[00:00 23:59] [00:00 23:...
holiday type 3	[00:00 23:59] [00:00 23:...

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


Time Period 1

00:00 23:59

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

NOTE:

1) The door is inaccessible for the whole day when the End Time occurs before the Start Time (such as **23:57~23:56**).

2) It is the time interval for valid access when the End Time occurs after the Start Time (such as **08:00~23:59**).

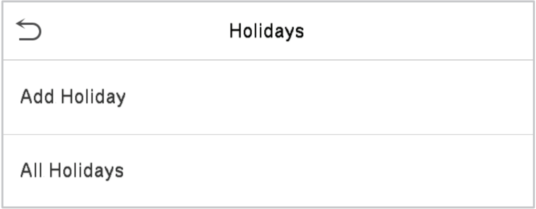
3) The door is accessible for the whole day when the End Time occurs after the Start Time (such that Start Time is **00:00** and End Time is **23:59**).

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

9.3 Holidays

Whenever there is a holiday, you may need a distinct access time; but changing everyone's access time one by one is extremely cumbersome, so a holiday access time can be set that applies 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.



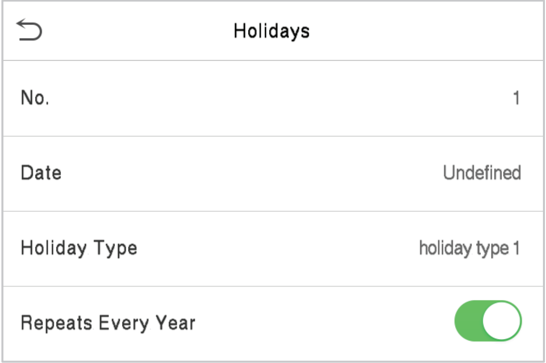
Holidays

Add Holiday

All Holidays

- **Add a New Holiday**

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



Holidays

No.	1
Date	Undefined
Holiday Type	holiday type 1
Repeats Every Year	●

- **Edit a Holiday**

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

- **Delete a Holiday**

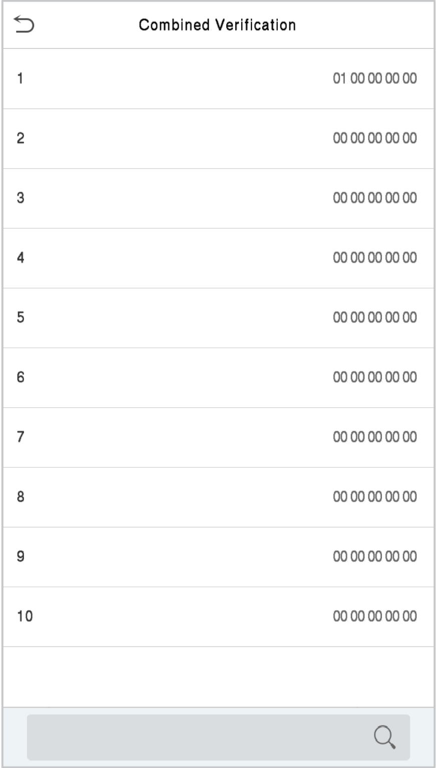
On the **Holidays** interface, select a holiday item to be deleted and tap **Delete**. Press **OK** to confirm the deletion. After deletion, this holiday does not display on the **All Holidays** interface.

9.4 Combined Verification

Access groups are arranged into different door-unlocking combinations to achieve multiple verifications and strengthen security.

In a door-unlocking combination, the range of the combined number N is **0 ≤ N ≤ 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.



Combined Verification

1	01 00 00 00 00
2	00 00 00 00 00
3	00 00 00 00 00
4	00 00 00 00 00
5	00 00 00 00 00
6	00 00 00 00 00
7	00 00 00 00 00
8	00 00 00 00 00
9	00 00 00 00 00
10	00 00 00 00 00

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:

- If the **Door-unlock combination 1** is set as (**01 03 05 06 08**). It indicates that the unlock combination 1 consists of 5 people and all the 5 individuals are from 5 groups, namely, AC Group 1, AC Group 3, AC Group 5, AC Group 6, and AC Group 8, respectively.
- If the **Door-unlock combination 2** is set as (**02 02 04 04 07**). It indicates 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.
- If the **Door-unlock combination 3** is set as (**09 09 09 09 09**). It indicates that there are 5 people in this combination; all of which are from AC Group 9.
- If the **Door-unlock combination 4** is set as (**03 05 08 00 00**). It indicates 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.

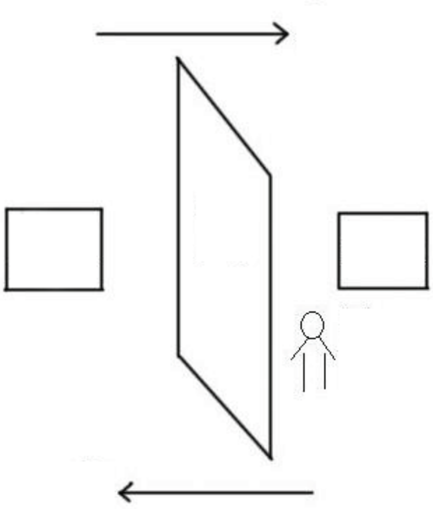
NOTE: To delete the door-unlock combination, set all Door-unlock combinations to 0.

9.5 Anti-passback Setup

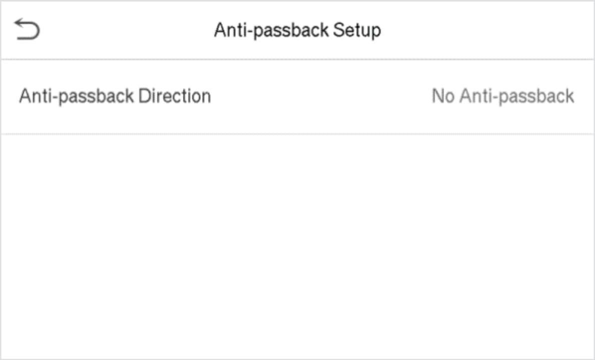
A user may be followed by some person(s) to enter the door without verification, resulting in a security breach. So, to avoid such situations, the Anti-Passback option was developed. Once it is enabled, the check-in and check-out record must occur alternatively to open the door to represent a consistent pattern.

This function requires two devices to work together:

One device is installed on the indoor side of the door (master device), and the other one is installed on the outdoor side of the door (the 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.

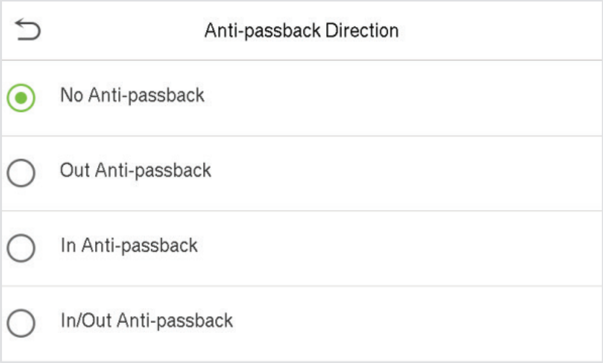


Tap **Anti-Passback Setup** on the **Access Control** interface.



Anti-passback Setup

Anti-passback Direction   No Anti-passback



Anti-passback Direction

● No Anti-passback

○ Out Anti-passback

○ In Anti-passback

○ In/Out Anti-passback

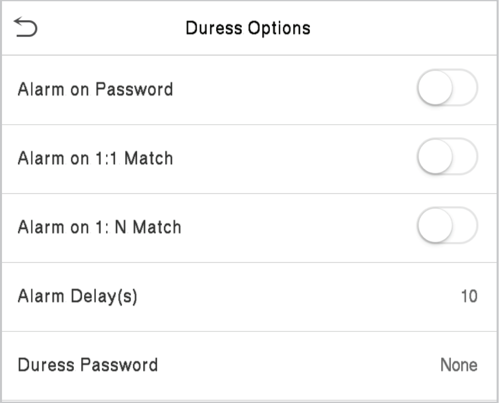
Function Description

Function Name	Description
Anti-passback direction	**No Anti-Passback:** The 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:** The user can check-out only if the last record is a check-in record otherwise an alarm is raised. However, the user can check-in freely. **In Anti-Passback:** The user can check-in again only if the last record is a check-out record otherwise an alarm is raised. However, the user can check-out freely. **In/Out Anti-Passback:** In this case, a user can check-in only if the last record is a check-out or the user can check-out only if the last record is a check-in otherwise the alarm is triggered.

9.6 Duress Options Settings

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

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



Duress Options

Alarm on Password ○

Alarm on 1:1 Match ○

Alarm on 1: N Match ○

Alarm Delay(s) 10

Duress Password None

Function Description

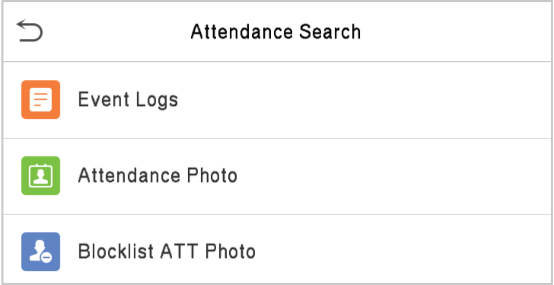
Function Name	Description
Alarm on Password	When a user uses the password verification method, an alarm signal will be generated, otherwise there will be no alarm signal.
Alarm on 1:1 Match	When a user uses the 1:1 verification method, an alarm signal will be generated, otherwise there will be no alarm signal.

Alarm on 1:N Match	When a user uses the 1:N verification method, an alarm signal will be generated, 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 will be generated.

10 Attendance Search

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

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

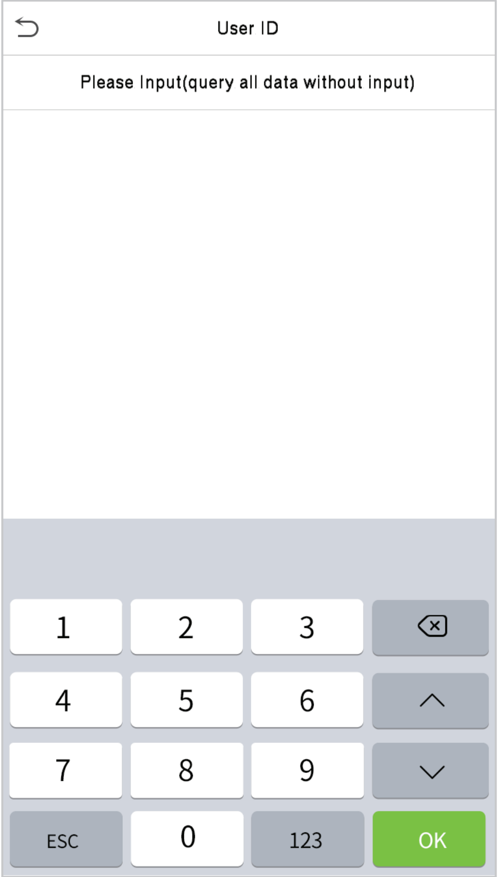


The process of searching for attendance and blocklist photos is similar to that of searching for access records. The following is an example of searching for access records.

On the **Attendance Search** interface, tap **Event Logs** to search for the required record.

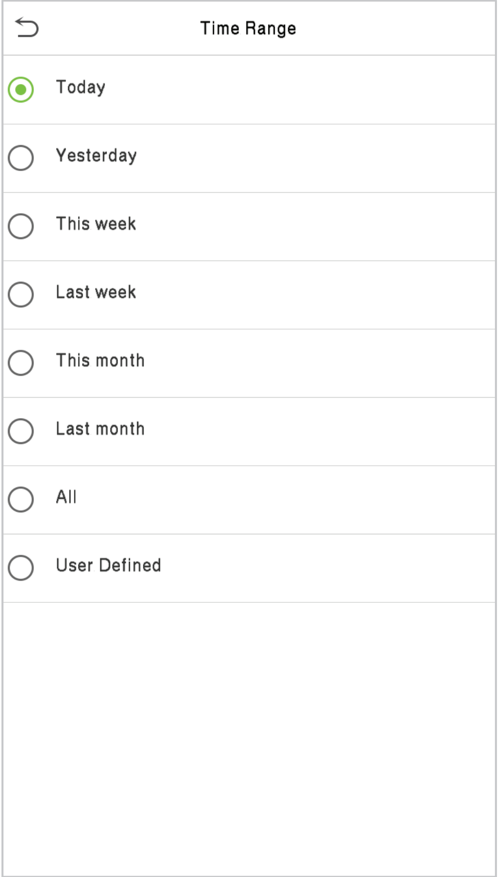
1. Enter the user ID to be searched and tap **OK**. If you want to search for records of all users, tap **OK** without entering any user ID.

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



User ID

Please Input(query all data without input)



Time Range

● Today

○ Yesterday

○ This week

○ Last week

○ This month

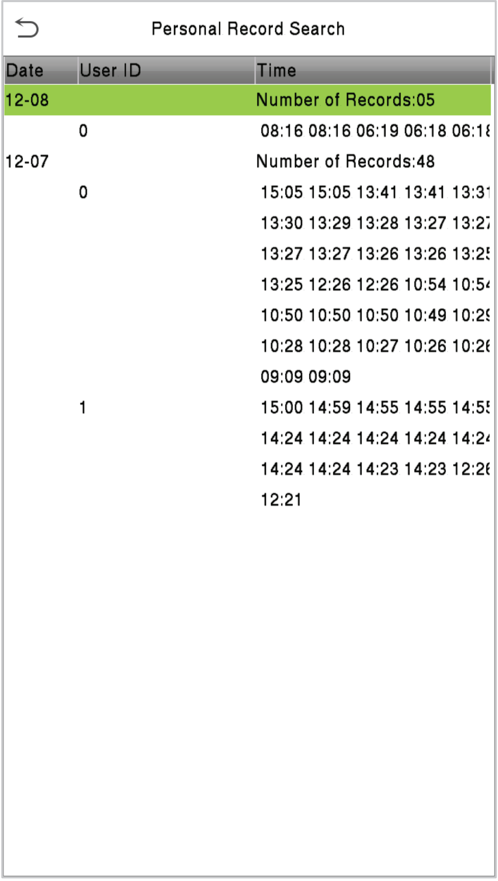
○ Last month

○ All

○ User Defined

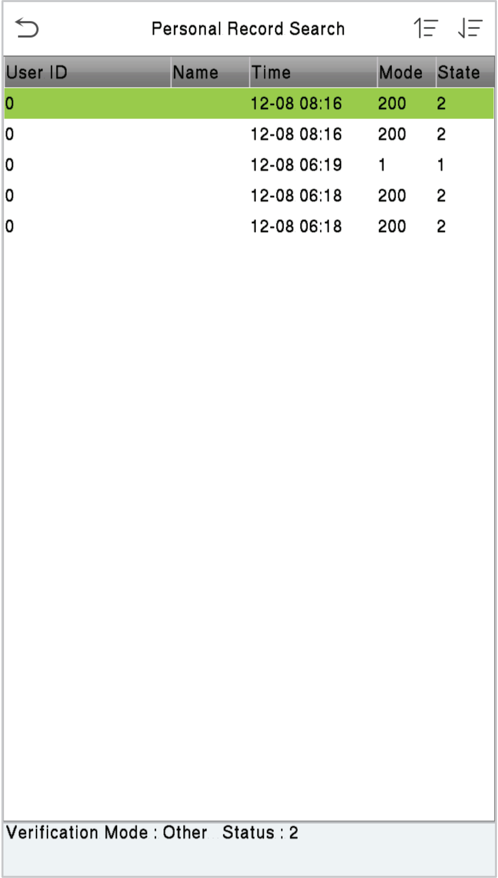
3. Once the record search completes. Tap the record highlighted in green to view its details.

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



Personal Record Search

Date	User ID	Time
12-08		Number of Records:05
	0	08:16 08:16 06:19 06:18 06:1
12-07		Number of Records:48
	0	15:05 15:05 13:41 13:41 13:3
		13:30 13:29 13:28 13:27 13:2
		13:27 13:27 13:26 13:26 13:2
		13:25 12:26 12:26 10:54 10:5
		10:50 10:50 10:50 10:49 10:2
		10:28 10:28 10:27 10:26 10:2
		09:09 09:09
	1	15:00 14:59 14:55 14:55 14:5
		14:24 14:24 14:24 14:24 14:2
		14:24 14:24 14:23 14:23 12:2
		12:21



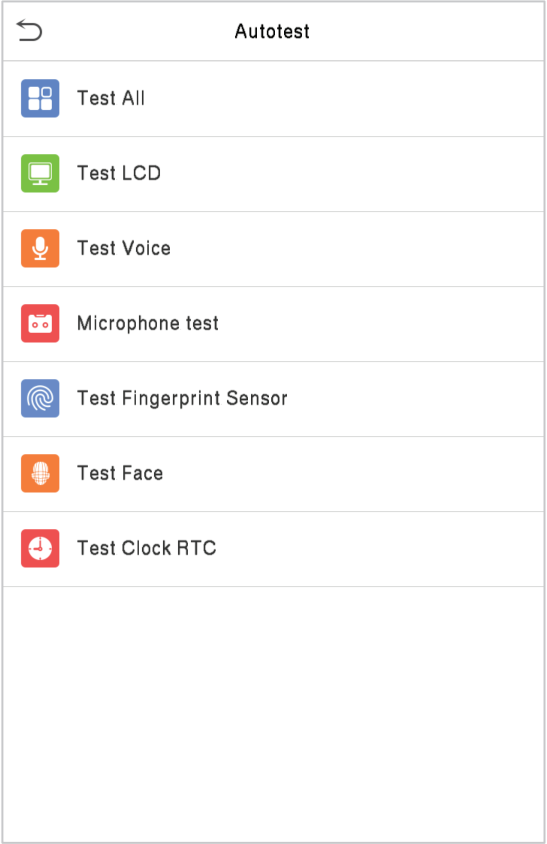
Personal Record Search

User ID	Name	Time	Mode	State
0		12-08 08:16	200	2
0		12-08 08:16	200	2
0		12-08 06:19	1	1
0		12-08 06:18	200	2
0		12-08 06:18	200	2

Verification Mode : Other   Status : 2

11 Autotest

Select **Main Menu**, tap **Autotest.** It enables the system to automatically test whether the functions of various modules are working normally, including the LCD, Voice, Camera, and Real-Time Clock (RTC).



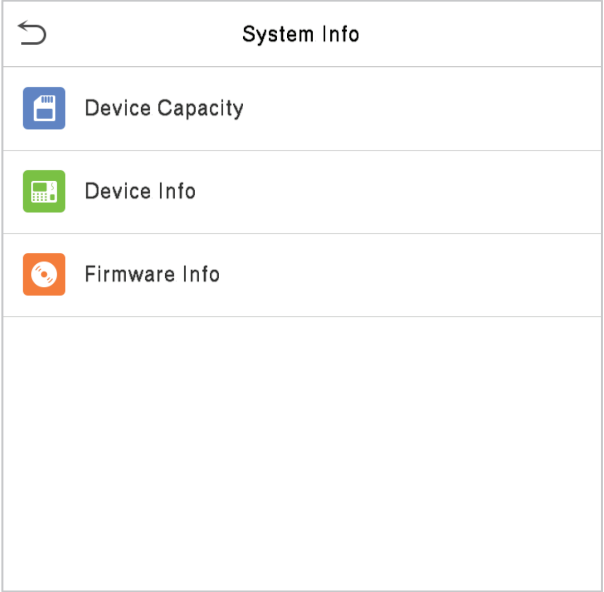
Function Description

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.
Microphone test	To test if the microphone is working properly by speaking into the microphone.
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. Touch the screen to start counting and press it again to stop counting.

12 System Information

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



System Info

Device Capacity

Device Info

Firmware Info

Function Description

Function Name	Description
Device Capacity	Displays the current device's user storage, palm, 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 and face algorithm, 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 on the face.

2） Do not place the device towards outdoor light sources like door or window or other harsh light sources.

3） Dark-color apparels other than the background color are recommended for registration.

4） Expose your face and forehead properly and do not cover your face and eyebrows with your hair.

5） It is recommended to show a normal facial expression. (A smile is acceptable, but do not close your eyes, or incline your head to any orientation).

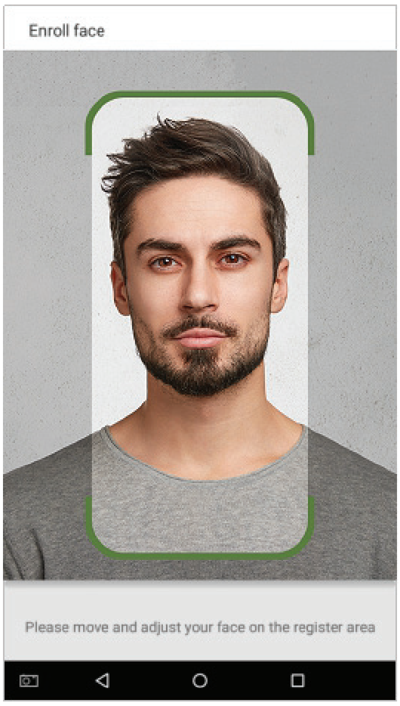
6） Two images are required for persons with eyeglasses, one image with eyeglasses and one other without them.

7） Do not wear accessories like 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, coloured, 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 photos captured.

- **Eye Distance**

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

- **Facial Expression**

A neutral face or smile with eyes naturally open are recommended.

- **Gesture and Angel**

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

- **Accessories**

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

- **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-coloured 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）A neutral face or smile is preferred, showing teeth is not preferred.

9）The captured person should be easily visible, natural in color, no harsh shadow or light spot or reflection in the face or background. The contrast and lightness level should be appropriate.

Eco-friendly Operation

The product's "eco-friendly operational period" refers to the time period during which this product will not discharge any toxic or hazardous substances when used in accordance with the prerequisites in this manual.

The eco-friendly operational period specified for this product does not include batteries or other components that are easily worn down and must be periodically replaced. The battery's eco-friendly operational period is 5 years.

Hazardous or Toxic substances and their quantities

Component Name	Hazardous/Toxic Substance/Element					
	Lead (Pb)	Mercury (Hg)	Cadmium (Cd)	Hexavalent chromium (Cr6+)	Polybrominated Biphenyls (PBB)	Polybrominated Diphenyl Ethers (PBDE)
Chip Resistor	×	○	○	○	○	○
Chip Capacitor	×	○	○	○	○	○
Chip Inductor	×	○	○	○	○	○
Diode	×	○	○	○	○	○
ESD component	×	○	○	○	○	○
Buzzer	×	○	○	○	○	○
Adapter	×	○	○	○	○	○
Screws	○	○	○	×	○	○

○ indicates that the total amount of toxic content in all the homogeneous materials is below the limit as specified in SJ/T 11363—2006.

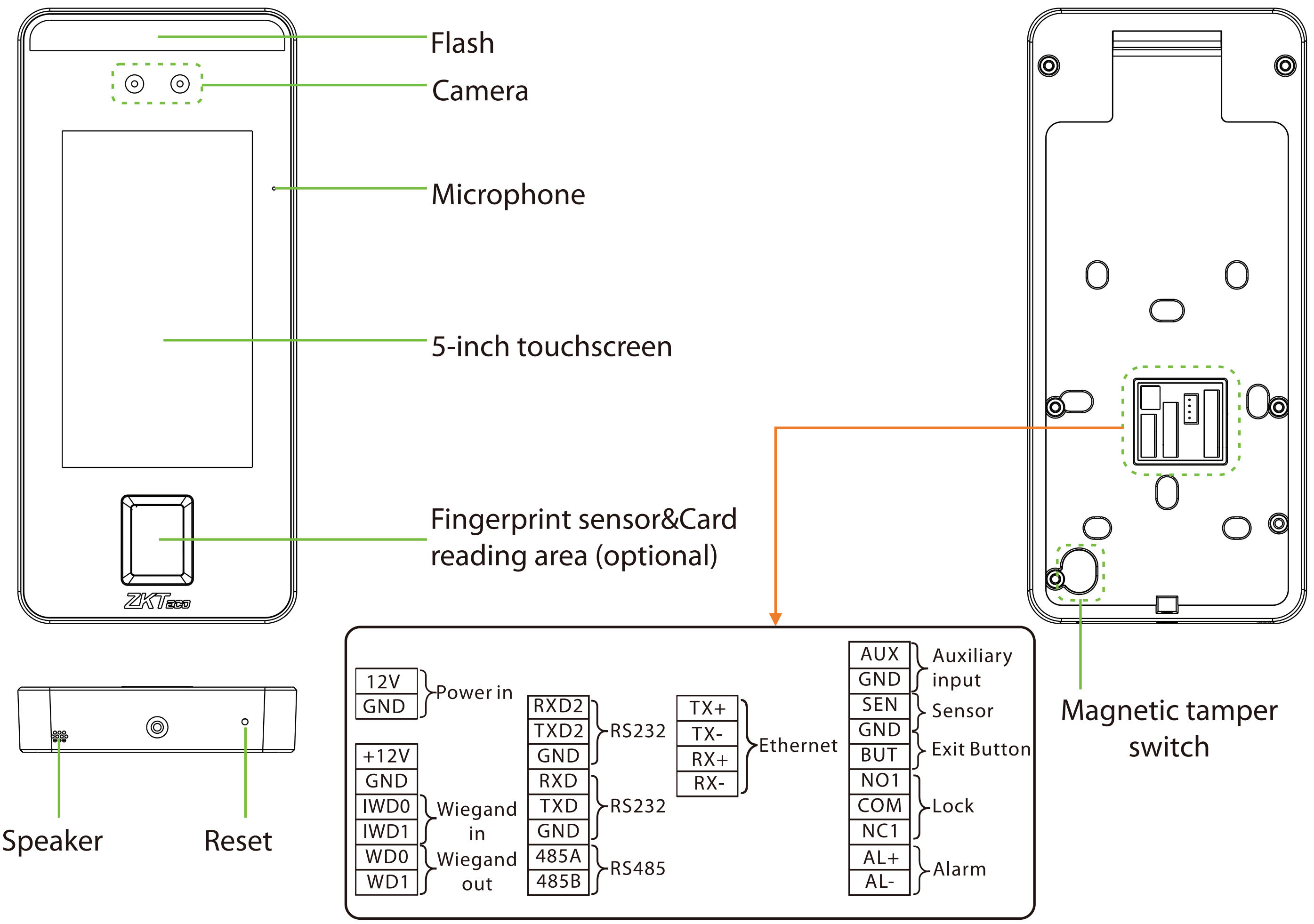
× indicates that the total amount of toxic content in all the homogeneous materials exceeds the limit as specified in SJ/T 11363—2006.

Note: 80% of this product’s components are manufactured using non-toxic and eco-friendly materials. The components which contain toxins or harmful elements are included due to the current economic or technical limitations which prevent their replacement with non-toxic materials or elements.

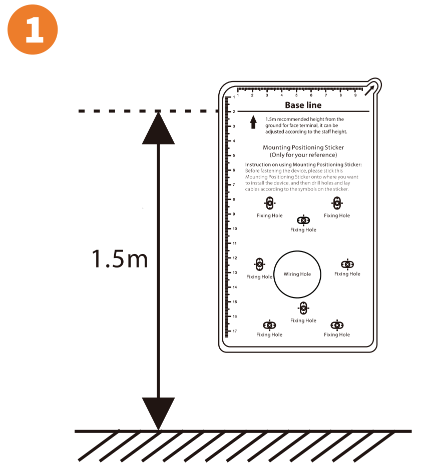
iomo

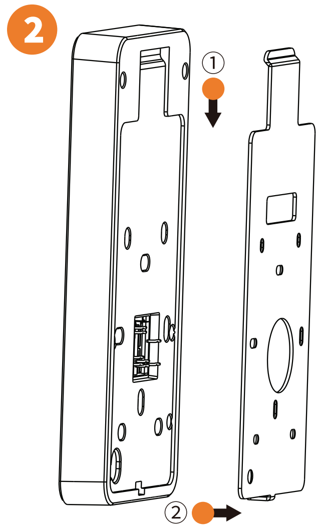
Installation Guide

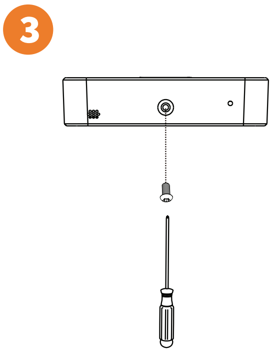
Overview



Device Installation





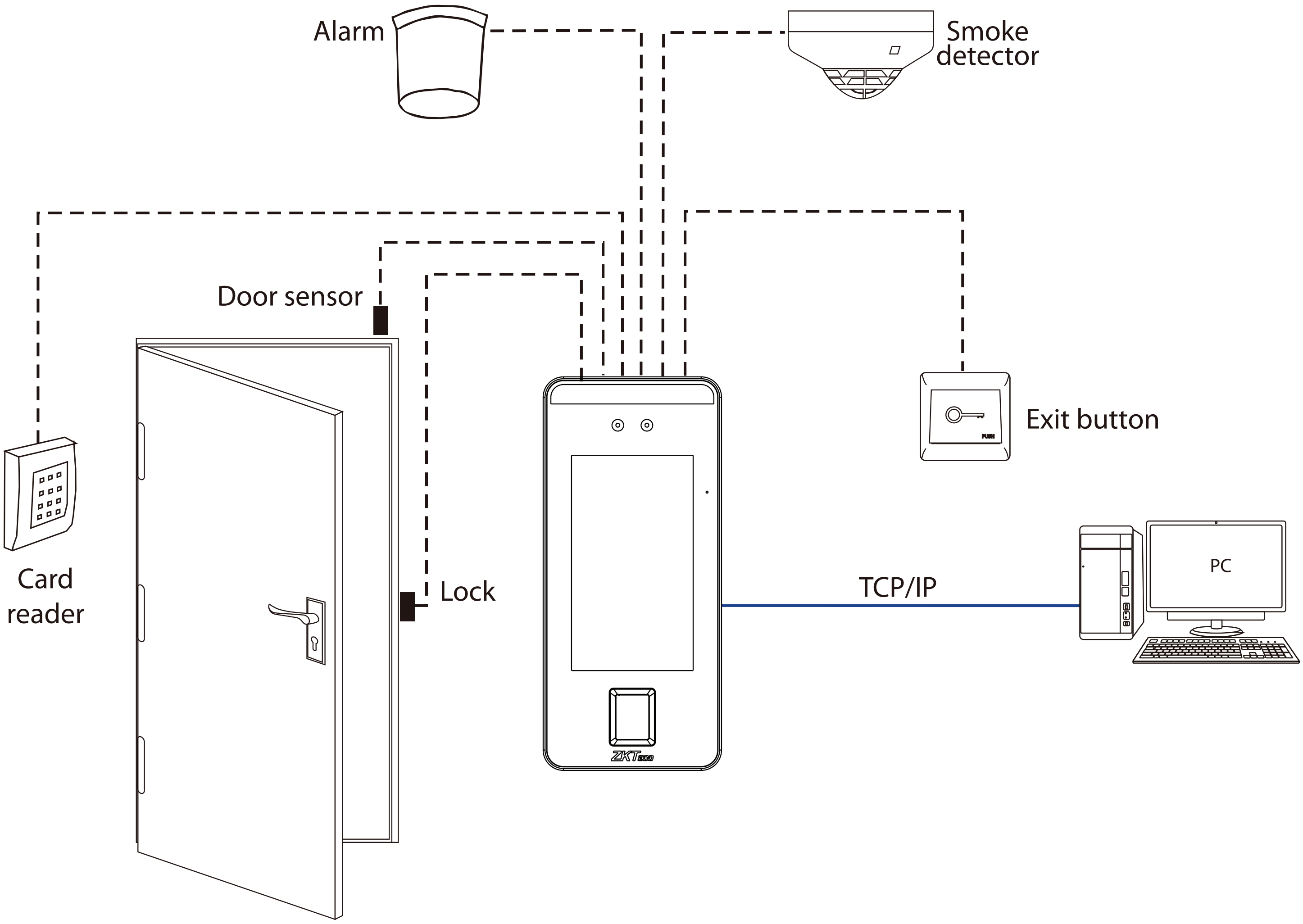


① Attach the mounting template sticker to the wall, and drill holes according to the mounting paper. Fix the back plate on the wall using wall mounting screws.

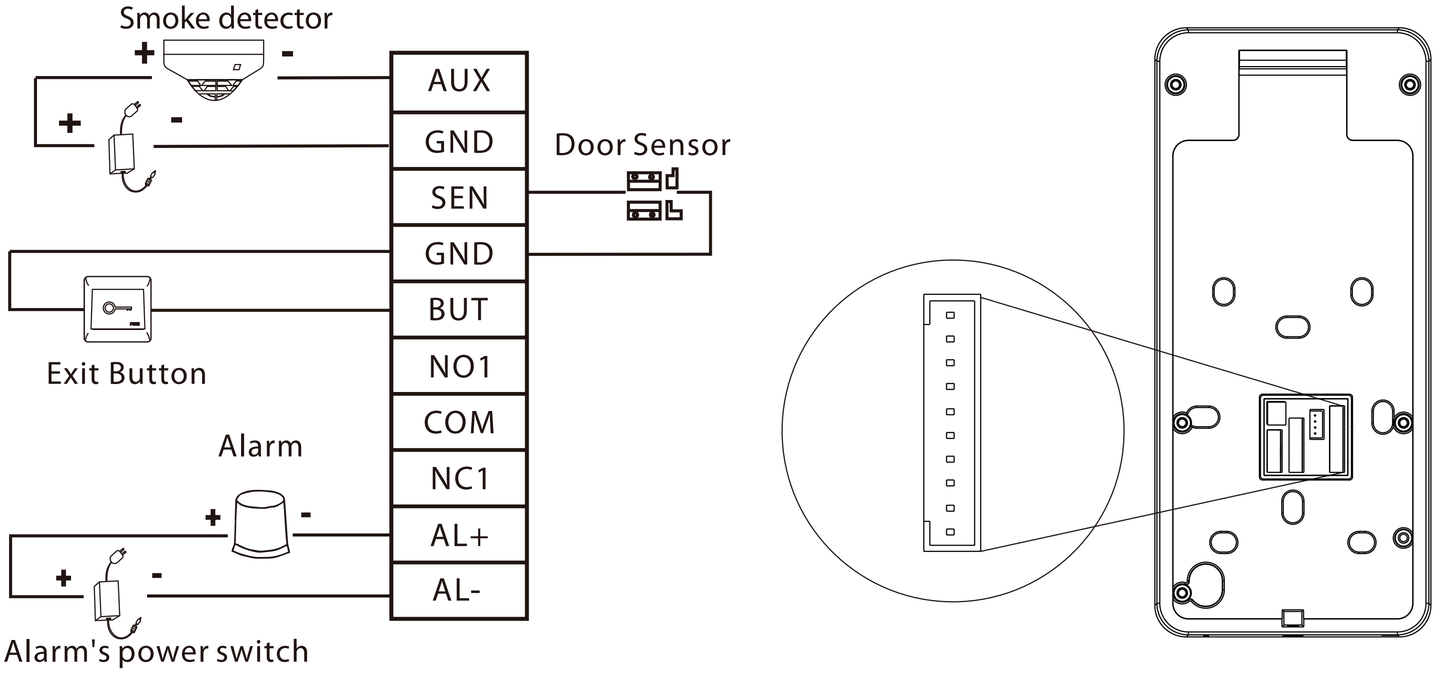
② Attach the device to the back plate.

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

Standalone Installation



Door Sensor, Exit Button & Alarm Connection

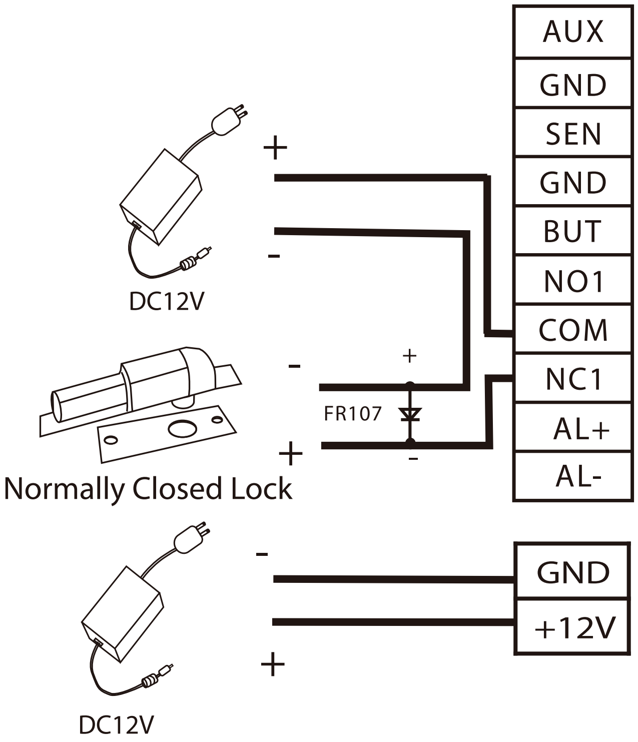


Lock Relay Connection

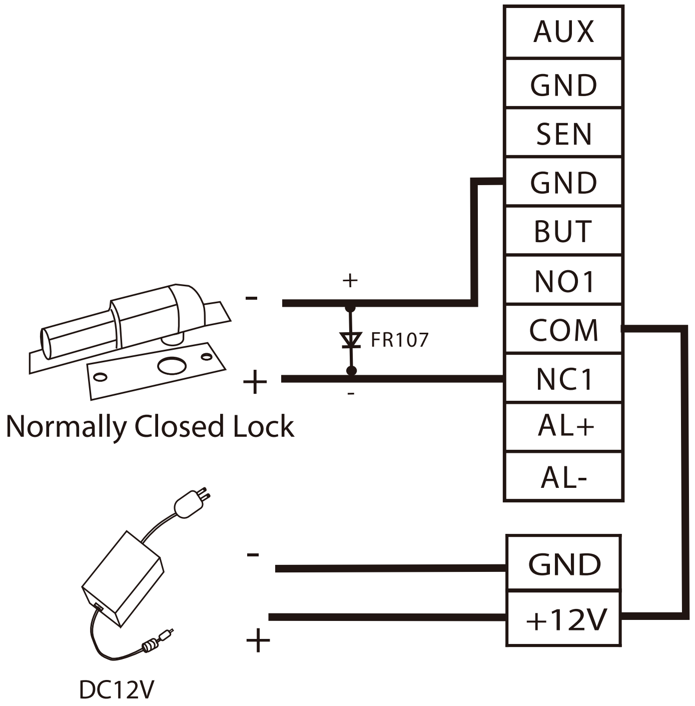
The system supports Normally Opened Lock and Normally Closed Lock.

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:

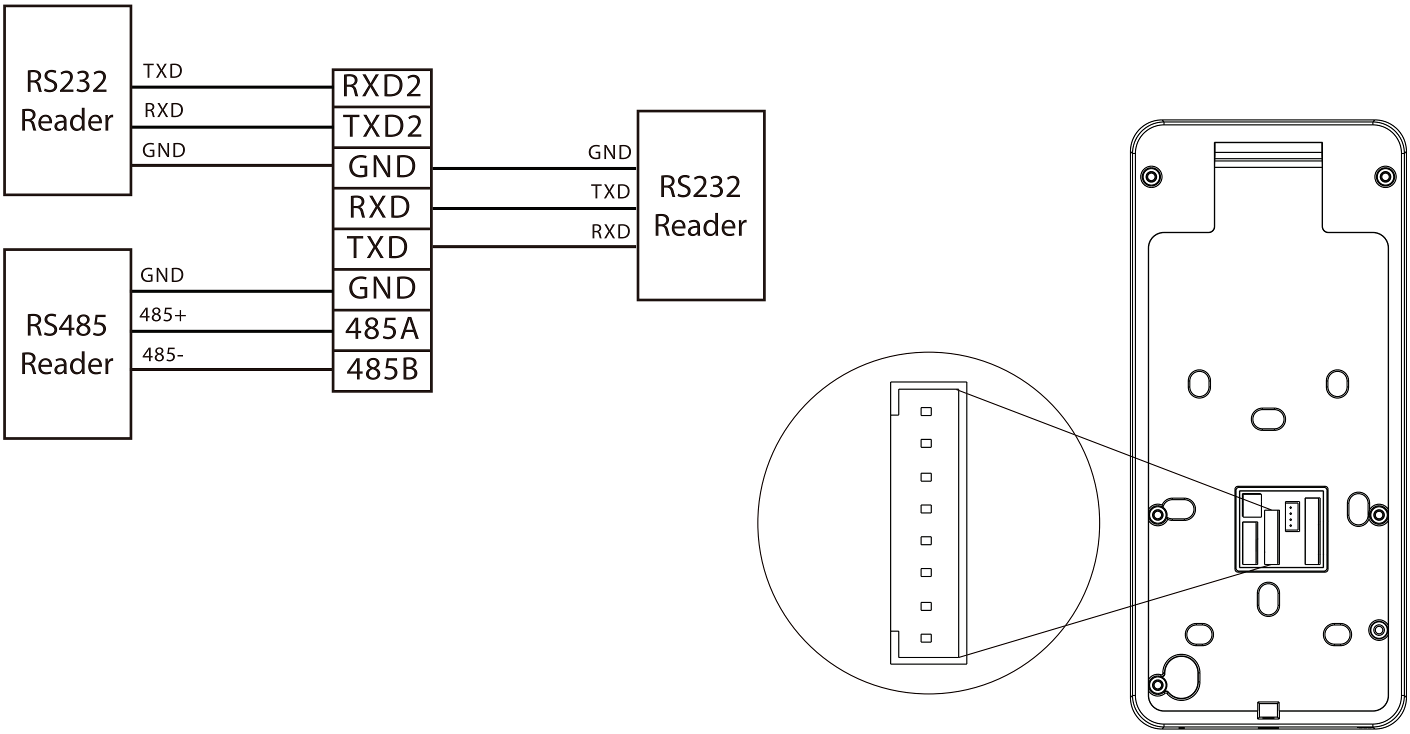
1) Device not sharing power with the lock



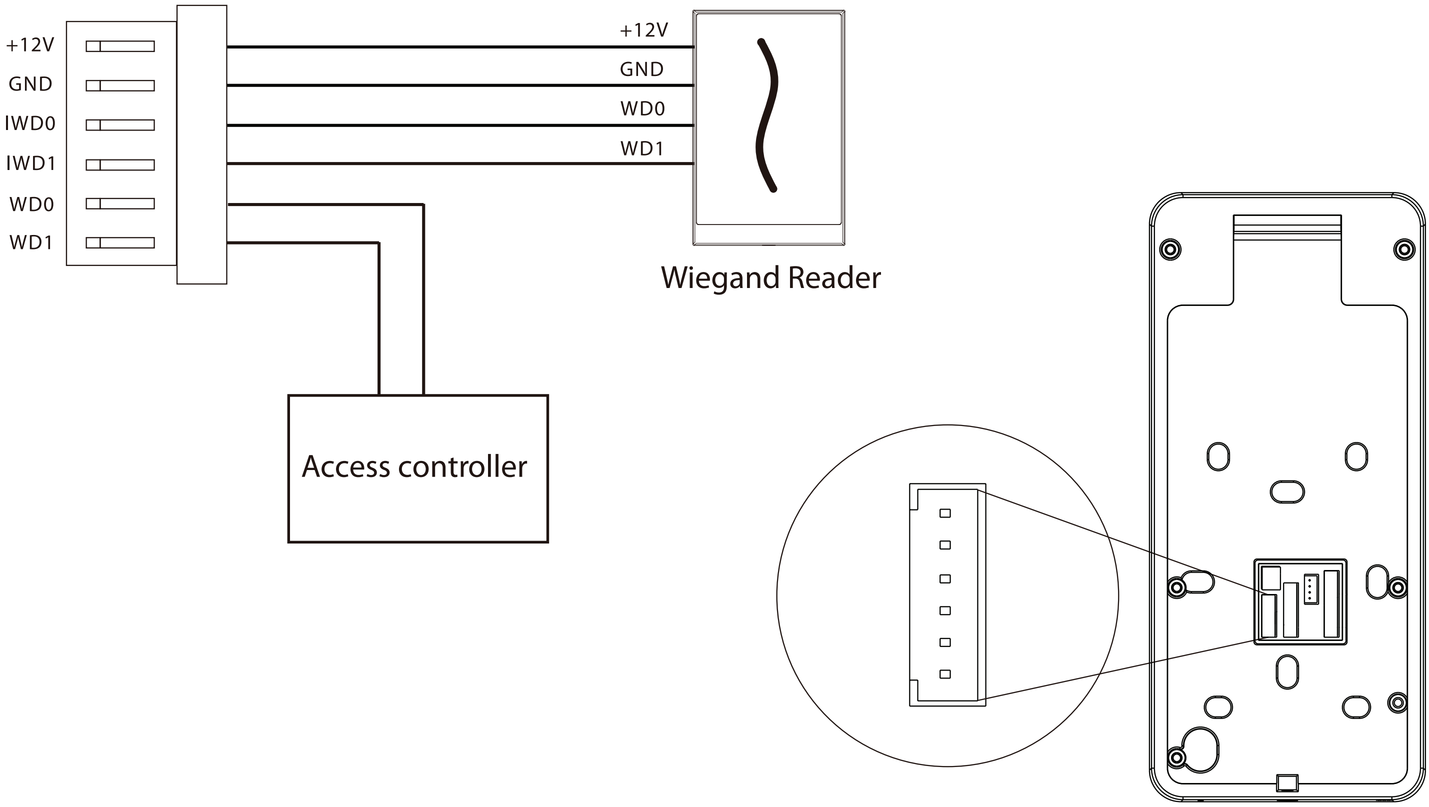
2) Device sharing power with the lock



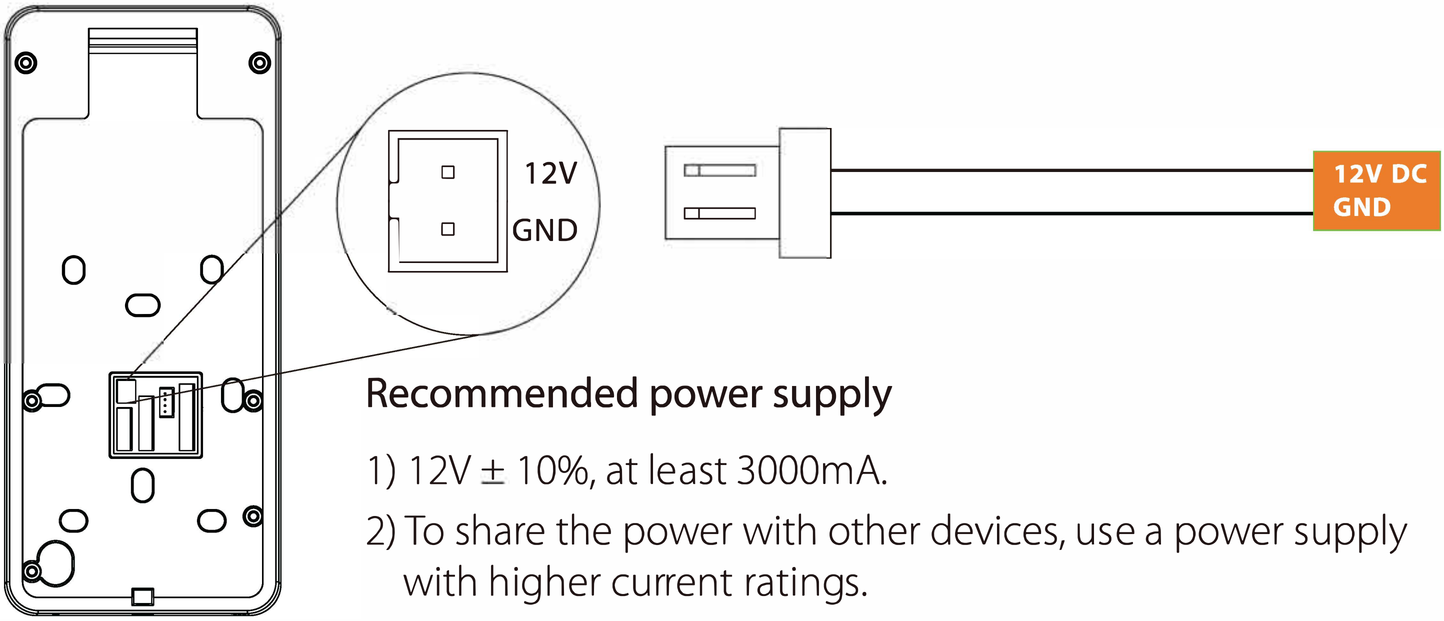
RS485 and RS232 Connection



Wiegand Reader Connection



Power Connection

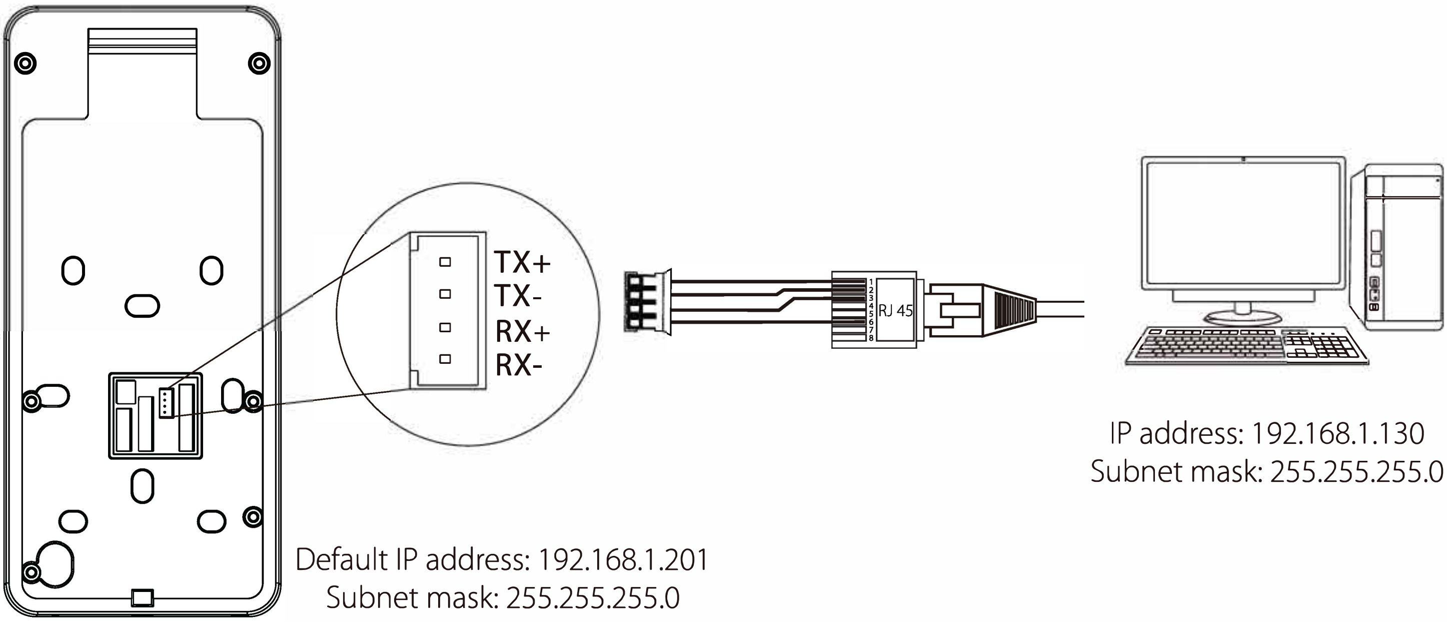


Recommended power supply

1) 12V ± 10%, at least 3000mA.

2) To share the power with other devices, use a power supply with higher current ratings.

Ethernet Connection


TX+
TX-
RX+
RX-
RJ 45
IP address: 192.168.1.130
Subnet mask: 255.255.255.0
Default IP address: 192.168.1.201
Subnet mask: 255.255.255.0

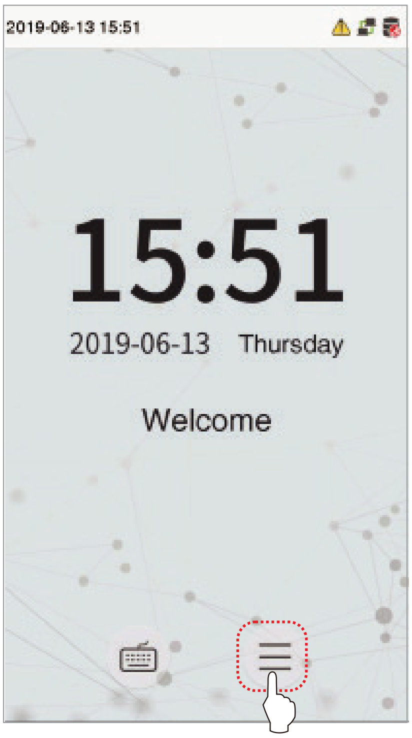
Click [COMM.] > [Ethernet] > [IP Address] , input the IP address and click [OK].

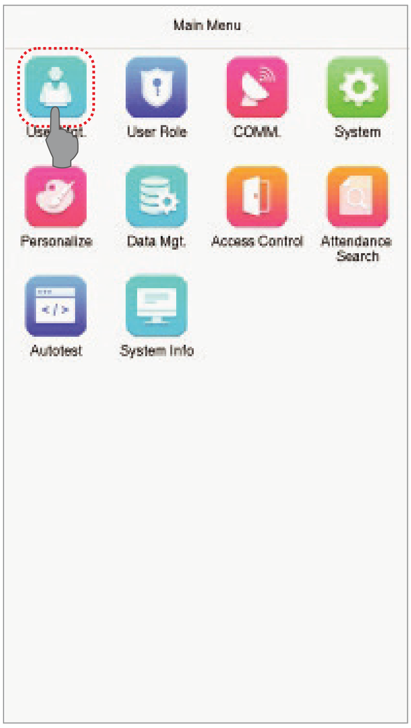
User Registration

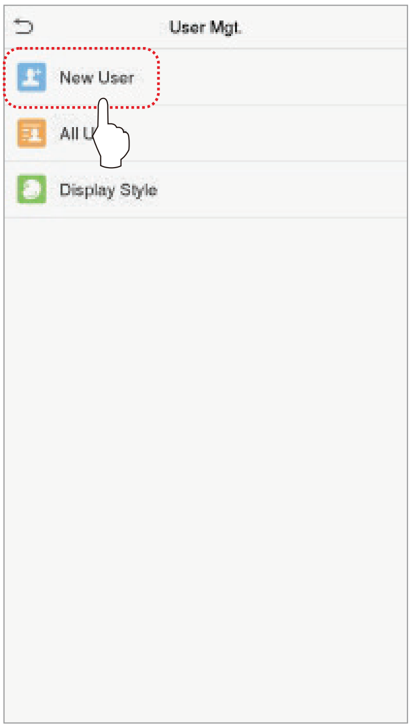
When there is no super administrator set in the device, click on ≡ to enter the menu. After setting the super administrator, the system will request for the administrator's verification before entering the menu. For the security purpose, it is recommended to register a super administrator at the first time you use the device.

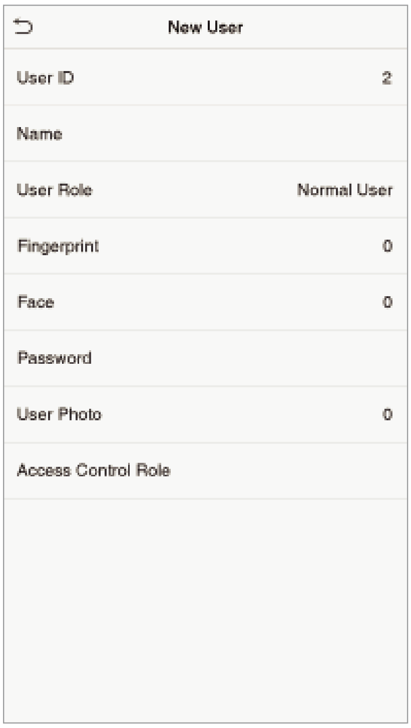
Method1: Register on the device

Click on ≡ > [User Mgt.] > [New User] to register a new user. Settings include entering user ID and name, registering a fingerprint, face, password, badge (optional) and user photo, setting user role and access control role.



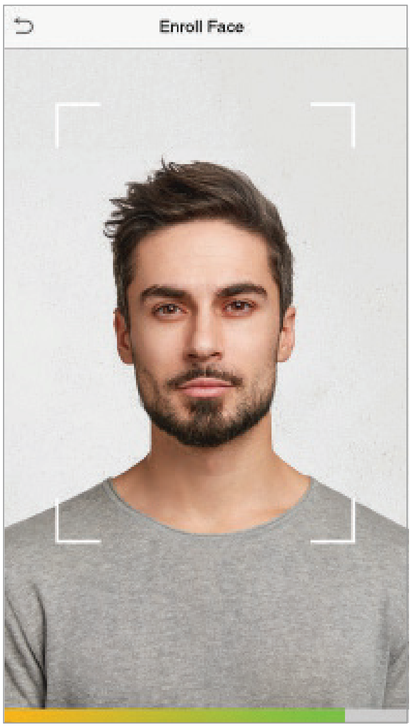






New User

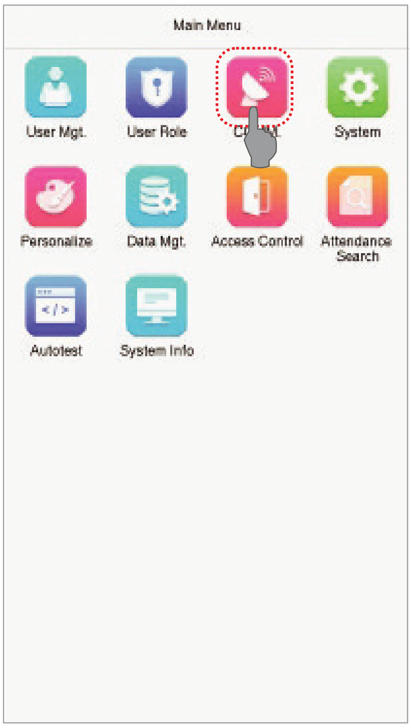
User ID	2
Name	
User Role	Normal User
Fingerprint	0
Face	0
Password	
User Photo	0
Access Control Role	

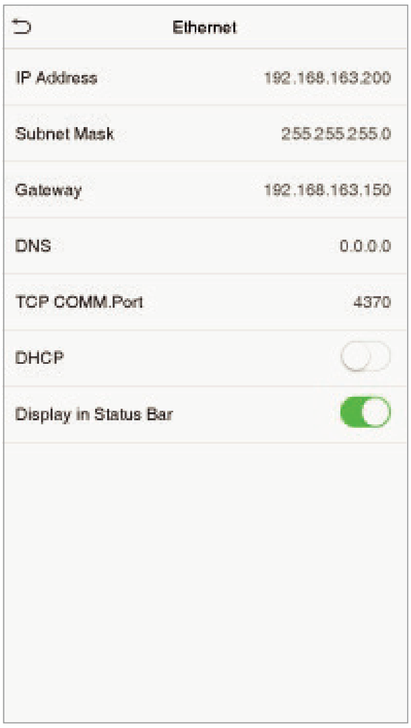


Ethernet and Cloud Server Settings

Click on ≡ > [COMM.] > [Ethernet] to set the network parameters. If the TCP/IP communication of the device is successful, the icon 🖧 will be displayed in the upper right corner of the standby interface.

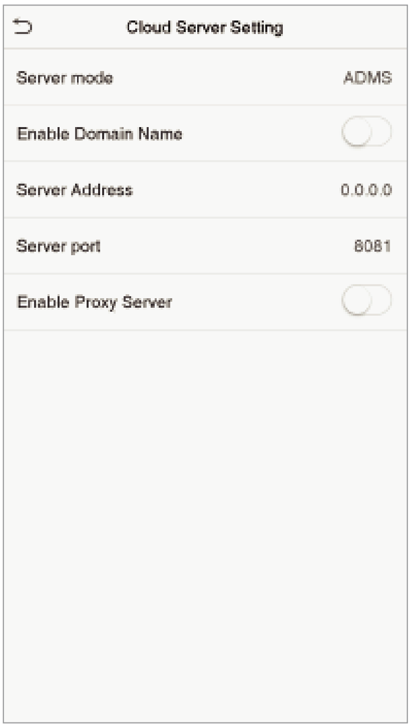
Click on ≡ > [COMM.] > [Cloud Server Setting] to set the server address and server port, that is, the IP address and port number of the server after the software is installed. If the device communicates with the server successfully, the icon 🗄 will be displayed in the upper right corner of the standby interface.





Ethernet

IP Address	192.168.163.200
Subnet Mask	255.255.255.0
Gateway	192.168.163.150
DNS	0.0.0.0
TCP COMM.Port	4370
DHCP	○
Display in Status Bar	●

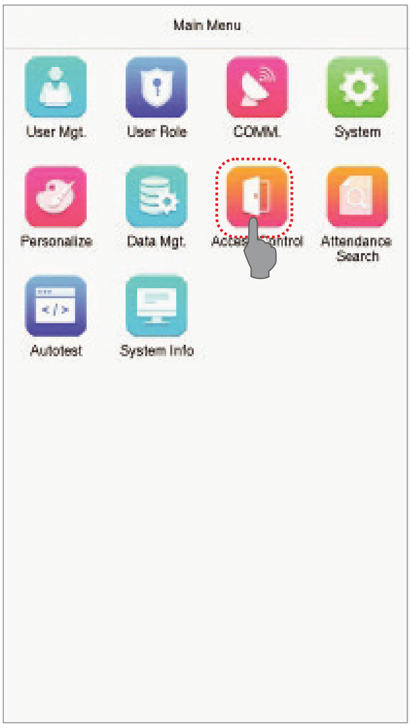


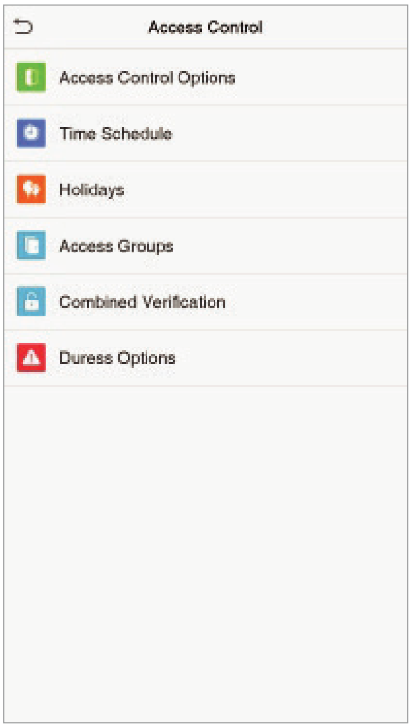
Cloud Server Setting

Server mode	ADMS
Enable Domain Name	○
Server Address	0.0.0.0
Server port	8081
Enable Proxy Server	○

Access Control Settings

Click on ≡ > [Access Control] to enter the access control management interface and set relevant parameters of access control.

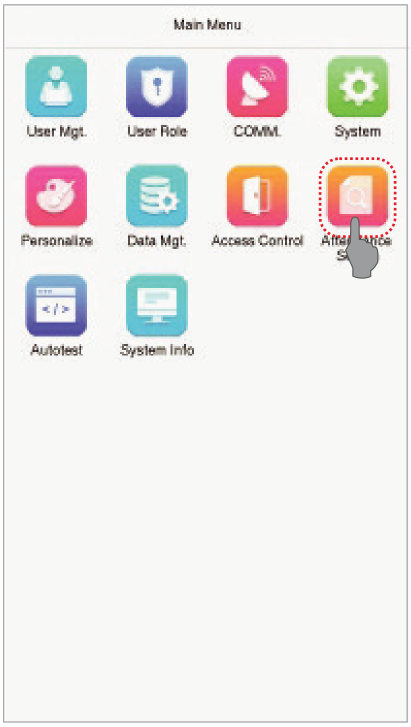


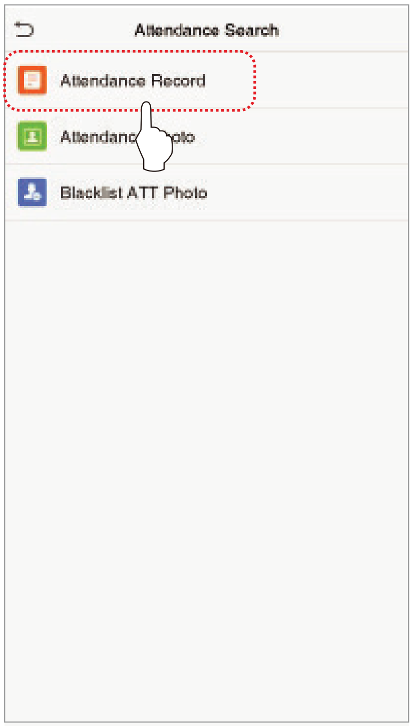


Records Query

Click on ☰ > [Attendance Search] > [Attendance Record] to enter the records query interface, input the user ID and select the time range, the corresponding attendance logs will be displayed.

.





iomo

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