User Manual

ProFace X Series

Date: May 2022

Doc Version: 1.0

English

Thank you for choosing our product. Please read the instructions carefully before operation. Follow these instructions to ensure that the product is functioning properly. The images shown in this manual are for illustrative purposes only.

For further details, please visit our Company's website www.zkteco.com.

Trademark

ZKTeco is a registered trademark of ZKTeco. Other trademarks involved in this manual are owned by their respective owners.

Disclaimer

This manual contains information on the operation and maintenance of the ZKTeco equipment. The copyright in all the documents, drawings, etc. in relation to the ZKTeco supplied equipment vests in and is the property of ZKTeco. The contents hereof should not be used or shared by the receiver with any third party without express written permission of ZKTeco.

The contents of this manual must be read as a whole before starting the operation and maintenance of the supplied equipment. If any of the content(s) of the manual seems unclear or incomplete, please contact ZKTeco before starting the operation and maintenance of the said equipment.

It is an essential pre-requisite for the satisfactory operation and maintenance that the operating and maintenance personnel are fully familiar with the design and that the said personnel have received thorough training in operating and maintaining the machine/unit/equipment. It is further essential for the safe operation of the machine/unit/equipment that personnel has read, understood and followed the safety instructions contained in the manual.

In case of any conflict between terms and conditions of this manual and the contract specifications, drawings, instruction sheets or any other contract-related documents, the contract conditions/documents shall prevail. The contract specific conditions/documents shall apply in priority.

ZKTeco offers no warranty, guarantee or representation regarding the completeness of any information contained in this manual or any of the amendments made thereto. ZKTeco does not extend the warranty of any kind, including, without limitation, any warranty of design, merchantability or fitness for a particular purpose.

ZKTeco does not assume responsibility for any errors or omissions in the information or documents which are referenced by or linked to this manual. The entire risk as to the results and performance obtained from using the information is assumed by the user.

ZKTeco in no event shall be liable to the user or any third party for any incidental, consequential, indirect, special, or exemplary damages, including, without limitation, loss of business, loss of profits, business interruption, loss of business information or any pecuniary loss, arising out of, in connection with, or relating to the use of the information contained in or referenced by this manual, even if ZKTeco has been advised of the possibility of such damages.

This manual and the information contained therein may include technical, other inaccuracies or typographical errors. ZKTeco periodically changes the information herein which will be incorporated into

new additions/amendments to the manual. ZKTeco reserves the right to add, delete, amend or modify the information contained in the manual from time to time in the form of circulars, letters, notes, etc. for better operation and safety of the machine/unit/equipment. The said additions or amendments are meant for improvement /better operations of the machine/unit/equipment and such amendments shall not give any right to claim any compensation or damages under any circumstances.

ZKTeco shall in no way be responsible (i) in case the machine/unit/equipment malfunctions due to any non-compliance of the instructions contained in this manual (ii) in case of operation of the machine/unit/equipment beyond the rate limits (iii) in case of operation of the machine and equipment in conditions different from the prescribed conditions of the manual.

The product will be updated from time to time without prior notice. The latest operation procedures and relevant documents are available on http://www.zkteco.com.

If there is any issue related to the product, please contact us.

ZKTeco Headquarters

Address ZKTeco Industrial Park, No. 32, Industrial Road,
Tangxia Town, Dongguan, China.
Phone +86 769 - 82109991
Fax +86 755 - 89602394

For business related queries, please write to us at: sales@zkteco.com.

To know more about our global branches, visit www.zkteco.com.

About the Company

ZKTeco is one of the world's largest manufacturer of RFID and Biometric (Fingerprint, Facial, Finger-vein) readers. Product offerings include Access Control readers and panels, Near & Far-range Facial Recognition Cameras, Elevator/floor access controllers, Turnstiles, License Plate Recognition (LPR) gate controllers and Consumer products including battery-operated fingerprint and face-reader Door Locks. Our security solutions are multi-lingual and localized in over 18 different languages. At the ZKTeco state-of-the-art 700,000 square foot ISO9001-certified manufacturing facility, we control manufacturing, product design, component assembly, and logistics/shipping, all under one roof.

The founders of ZKTeco have been determined for independent research and development of biometric verification procedures and the productization of biometric verification SDK, which was initially widely applied in PC security and identity authentication fields. With the continuous enhancement of the development and plenty of market applications, the team has gradually constructed an identity authentication ecosystem and smart security ecosystem, which are based on biometric verification techniques. With years of experience in the industrialization of biometric verifications, ZKTeco was officially established in 2007 and now has been one of the globally leading enterprises in the biometric verification industry owning various patents and being selected as the National High-tech Enterprise for 6 consecutive years. Its products are protected by intellectual property rights.

About the Manual

This manual introduces the operations of **ProFace X / ProFace X [TI] / ProFace X [TD]**.

All figures displayed are for illustration purposes only. Figures in this manual may not be exactly consistent with the actual products.

Features and parameters with ★ are not available in all devices.

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

Convention	Description
	This represents a note that needs to pay more attention to.
	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

Data Security Statement

ZKTeco, as a smart product supplier, may also need to know and collect some of your personal information in order to better assist you in using ZKTeco's goods and services, and will treat your privacy carefully by developing a Privacy Policy.

Please read and understand completely all the privacy protection policy regulations and key points that appear on the device before using ZKTeco products.

As a product user, you must comply with applicable laws and regulations related to personal data protection when collecting, storing, and using personal data, including but not limited to taking protective measures for personal data, such as performing reasonable rights management for devices, strengthening the physical security of device application scenarios, and so on.

Safety Measures

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

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

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

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

   And do not connect multiple devices to one power adapter as adapter overload can cause over-heat or fire hazard.

7. **Replacement parts** - When replacement parts are needed, service technicians must only use replacement parts provided by the supplier. Unauthorized substitutes can result in a burn, shock, or other hazards.
8. **Safety check** - On completion of service or repair work on the unit, ask the service technician to perform safety checks to ensure proper operation of the device.
9. **Power sources** - Operate the system only from the label's power source form. If the sort of power supply to use is unclear, call your dealer.
10. **Lightning** - Can install external lightning conductors to protect against electrical storms. It stops power-ups from destroying the system.

    Recommended installing the devices in areas with limited access.

Electrical Safety

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

Operation Safety

- If smoke, 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.

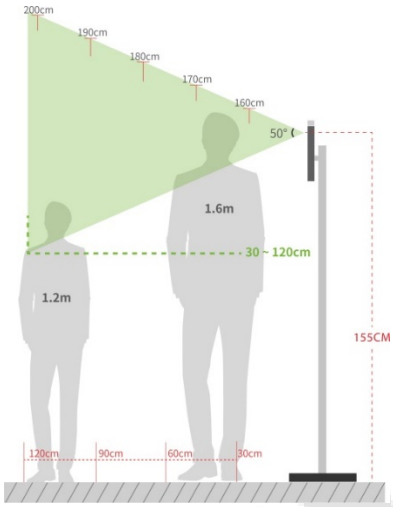
1 Overview

This document describes the operating procedure of **ProFace X Series** device. The operating modules of the device include User management, User role assignment, Device communication, Temperature detection, Access control, and so on. The device supports hassle-free access of users into the premises without compromising any security aspect thus ensuring protection.

2 Instructions to Use

2.1 Standing Position, Facial Expression and Standing Posture

- **Recommended Distance**



The distance between the device and a user whose height is within 1.55m to 1.85m is recommended to be 0.3 to 2.5m. Users may slightly move forwards and backwards to improve the quality of the facial images captured.

- **Facial Expression and Standing Posture**

Facial Expression

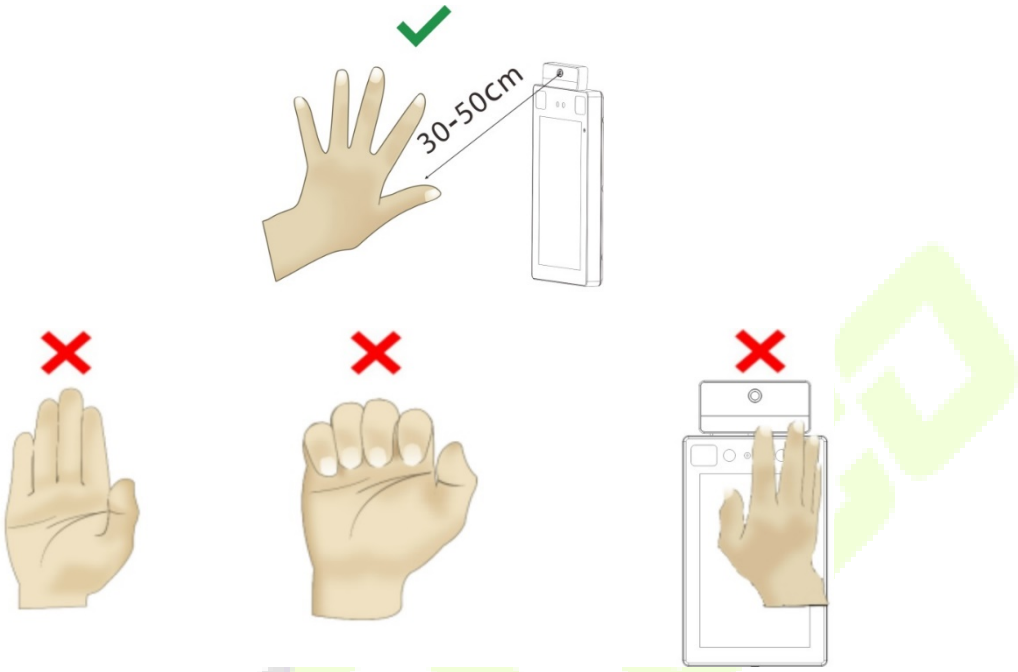
Standing Posture

Note: During enrollment and verification, please keep natural facial expression and standing posture.

2.2 Palm Registration

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

Make sure to keep space between your fingers.



2.3 Face Registration

Try to keep your face in the center of the screen during registration. Please face the camera and stay still during face registration. The page looks like shown below:

- **Face Registration and Authentication Methods**

Instructions to register a face:

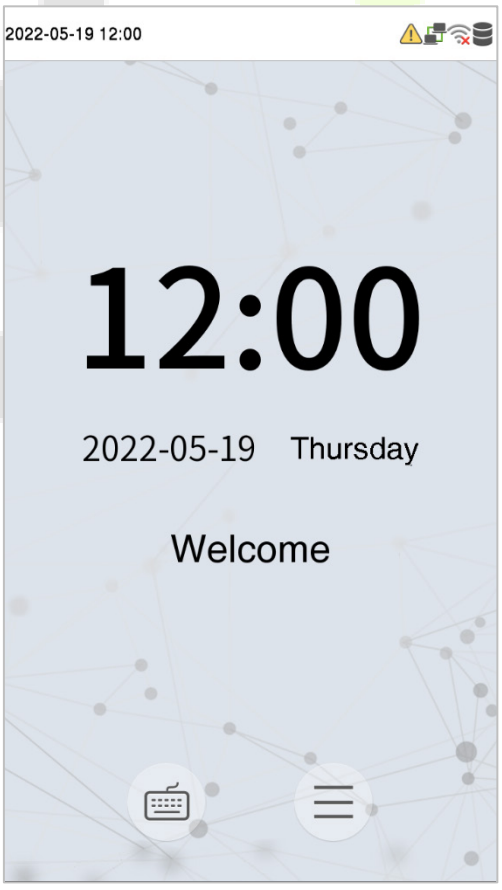
- When registering a face, maintain a distance of 40cm to 80cm between the device and the face.
- Be careful not to change the facial expression. (smiling face, drawn face, wink, etc.)
- If you do not follow the instructions on the screen, the face registration may take a longer time or may fail.
- Be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

Instructions to authenticate a face:

- Ensure that the face appears inside the detection area displayed on the device screen.
- If eyeglasses have been changed, authentication may fail. If the face without glasses has been registered, authenticate the face without glasses. If only the face with glasses has been registered, authenticate the face with the previously worn glasses again.
- 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.

2.4 Standby Interface

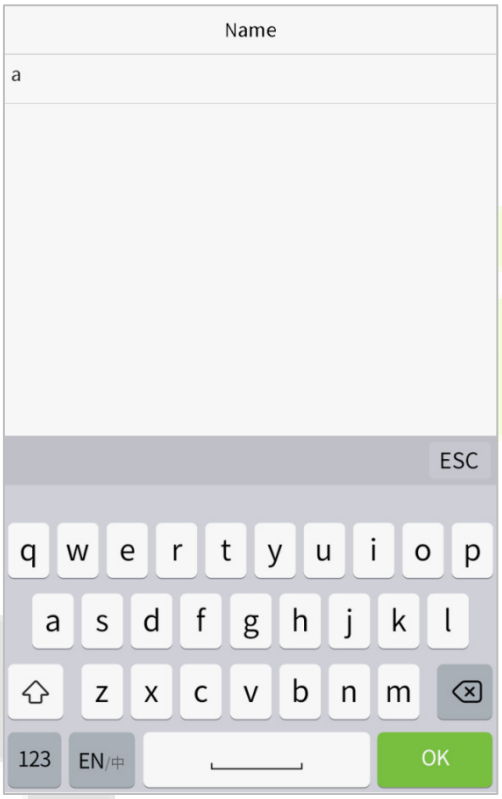
After connecting the power supply, the home screen appears as shown below:



Note:

- Click  to open the interface to enter the User ID.
- When there is no Super Administrator set in the device, click  to enter the menu. After setting the Super Administrator, it requires the Super Administrator's verification before entering the menu operation. For ensured security of the device, it is recommended to register a Super Administrator the first time you use the device.

2.5 Virtual Keyboard



Note: The device supports the input of Chinese and English characters, numbers, and symbols. Click **En** to switch to the English keyboard. Press **123** to switch to the numeric and special character keyboard, and click **ABC** to return to the alphabetic keyboard. Click the input box, and virtual keyboard appears. Click **ESC** to delete the entered characters.

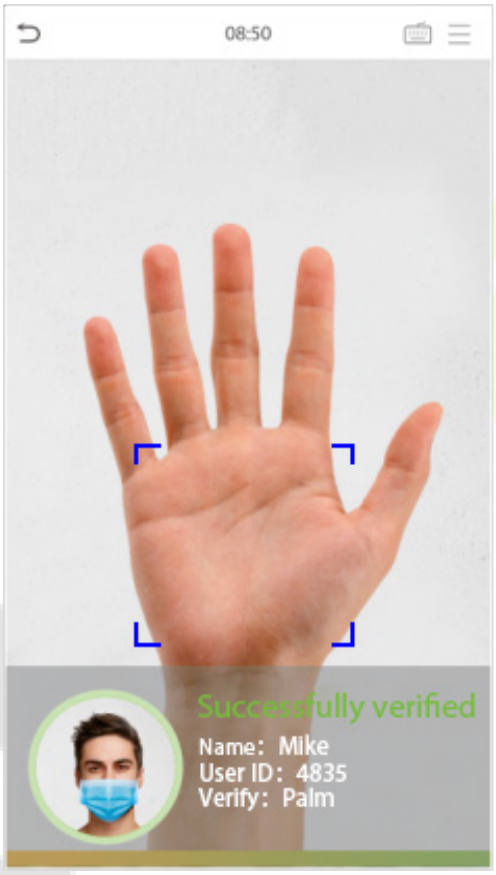
2.6 Verification Mode

2.6.1 Palm Verification

- **1:N (One to Many) Palm Verification Mode**

This verification mode compares the palm image collected by the palm module with all the palm data template in the device.

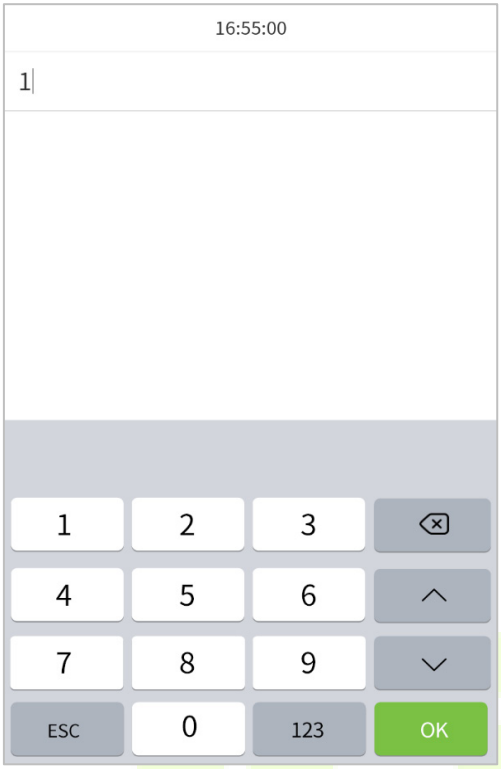
The device will automatically distinguish between the palm and face verification mode. Place the palm in the area that can be collected by the palm module, so that the device will automatically switch to palm verification mode.



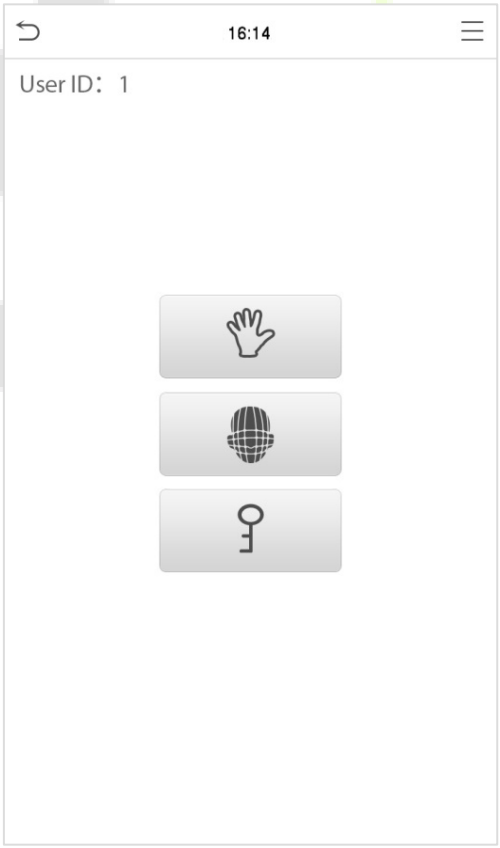
- **1:1 (One to One) Palm Verification Mode**

Click the button on the main screen to open the 1:1 (One to One) palm verification mode.

1. Input the user ID and press OK.



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

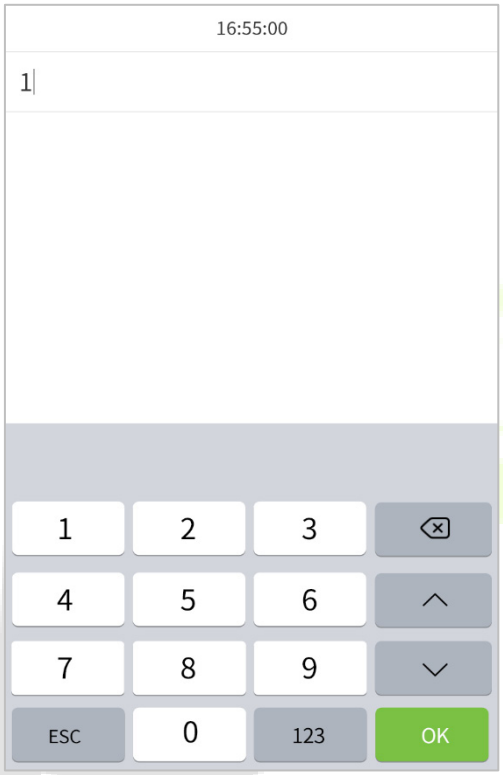


2.6.2 Password Verification

The Password Verification mode compares the entered password with the registered User ID and Password.

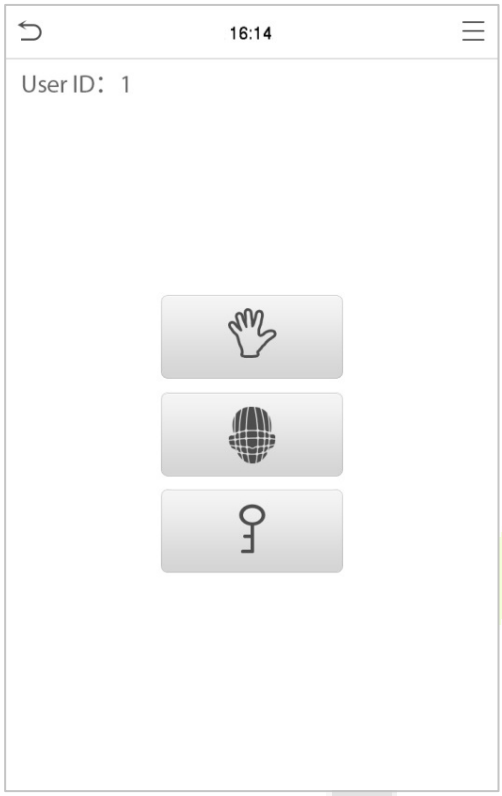
Click the button on the main screen to open the 1:1 (One to One) password verification mode.

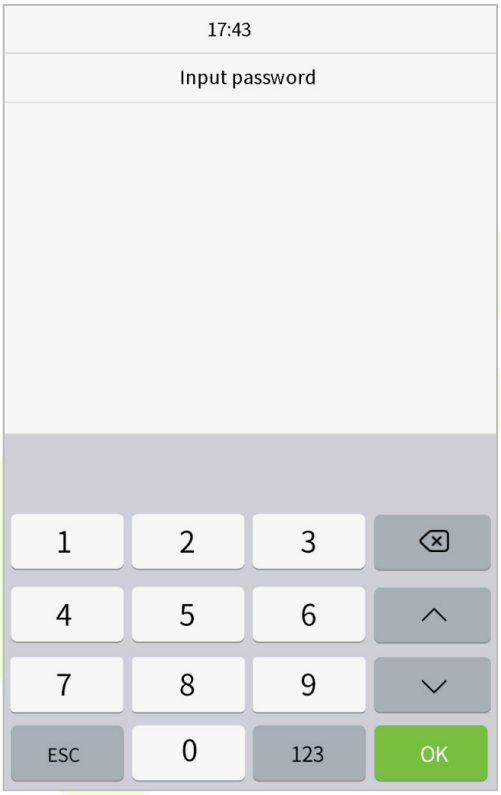
1. Input the user ID and press OK.



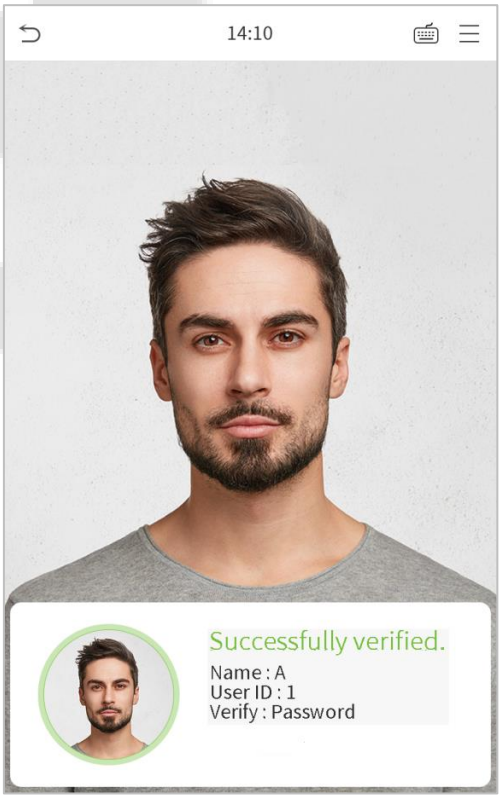
2. If an employee registers palm and face in addition to password, the following screen will appear. Select the  icon to enter the password verification mode.

3. Input the password and press OK.

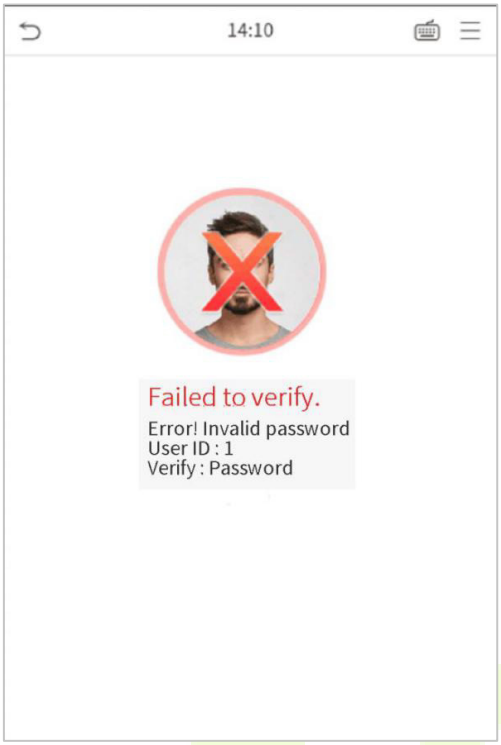




Successful Verification:



Failed Verification:



2.6.3 Facial Verification

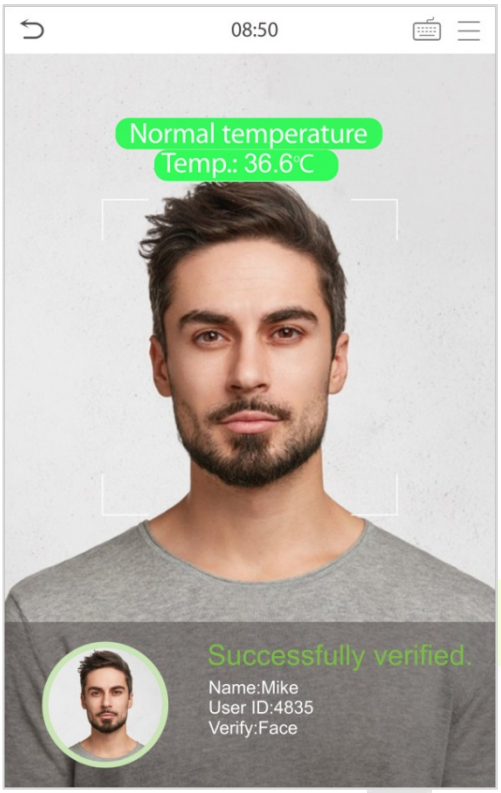
- **1:N (One to Many) Facial Verification Mode**

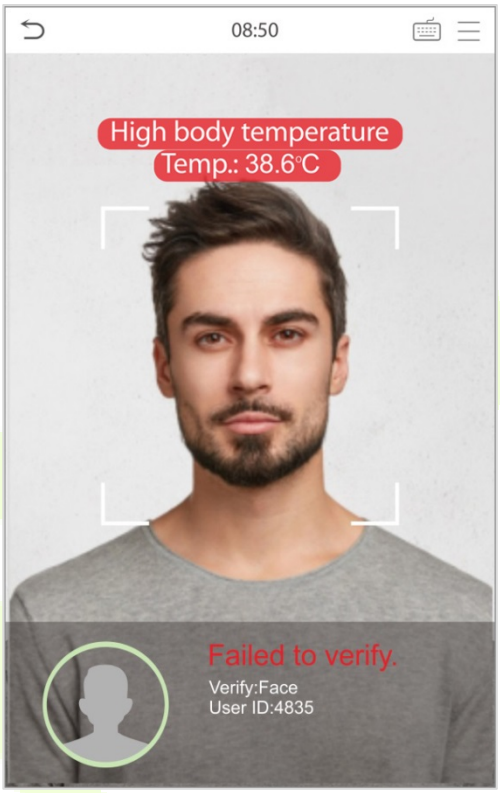
1. Conventional verification

   The conventional method compares the acquired facial images with all the face data templates registered in the device. The following is the pop-up prompt box of comparison result.

2. Temperature screening with infrared

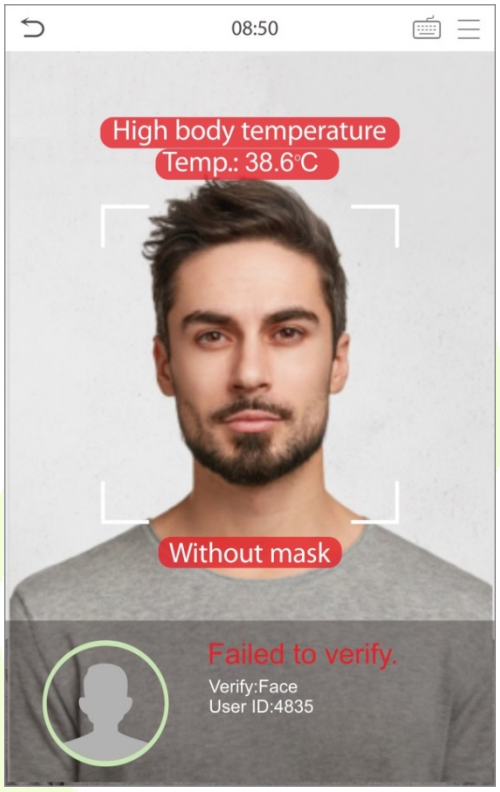
When the user enabled temperature screening with infrared function, during user verification, in addition to the conventional verification method, the user's face must be aligned with the temperature detection area to detect the body temperature before the conventional verification is conducted. The following is the verification interface.





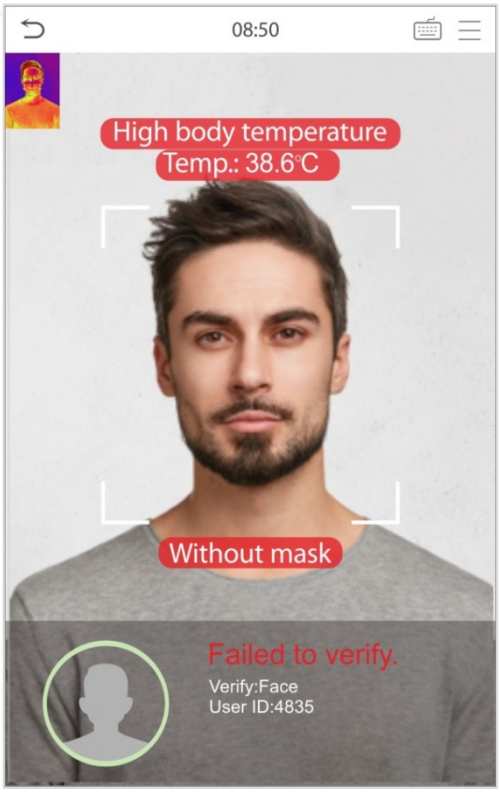
3. Mask detection

When the user enabled the **Mask detection** function, the device will identify whether the user is wearing a mask or not. The following is the verification interface.



4. Display Thermodynamics Figure

When the user enabled the **Display Thermodynamics Figure** function, during the detection process, the thermal image of the person will be displayed in the top left corner of the device.

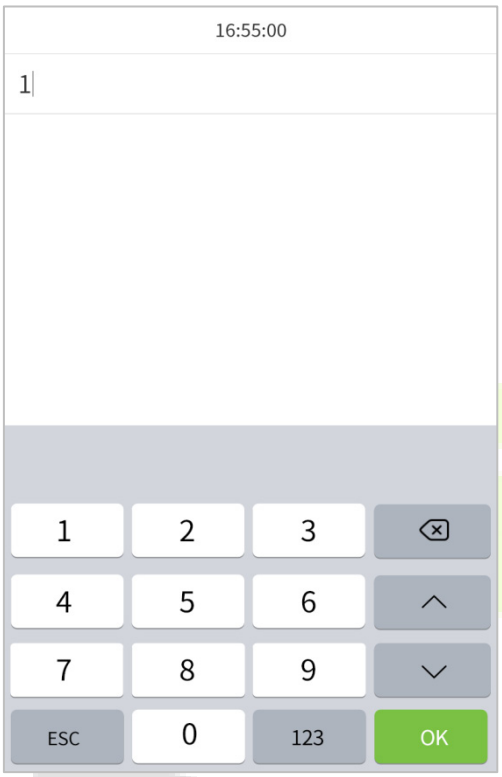


- **1:1 (One to One) Facial Verification Mode**

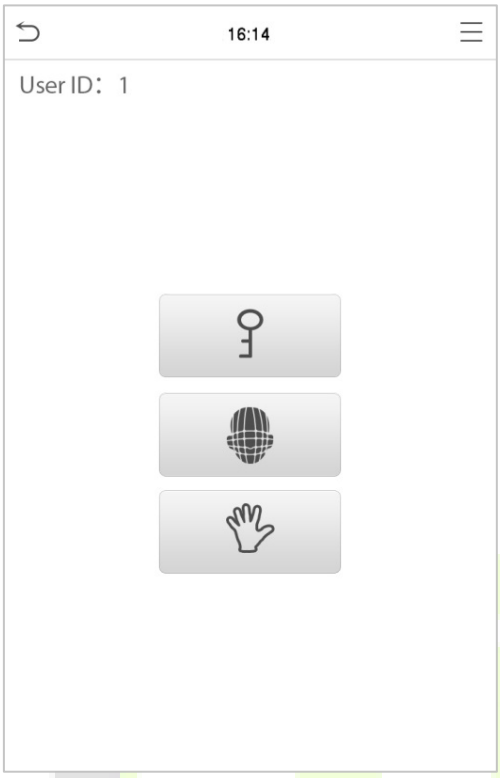
This verification method compares the face captured by the camera with the facial template related to the entered user ID.

Press  on the main interface to open the 1:1 facial verification mode.

1. Enter the User ID and click OK.



2. If an employee registered palm and password in addition to face, the following screen will appear. Select the  icon to open the face verification mode.

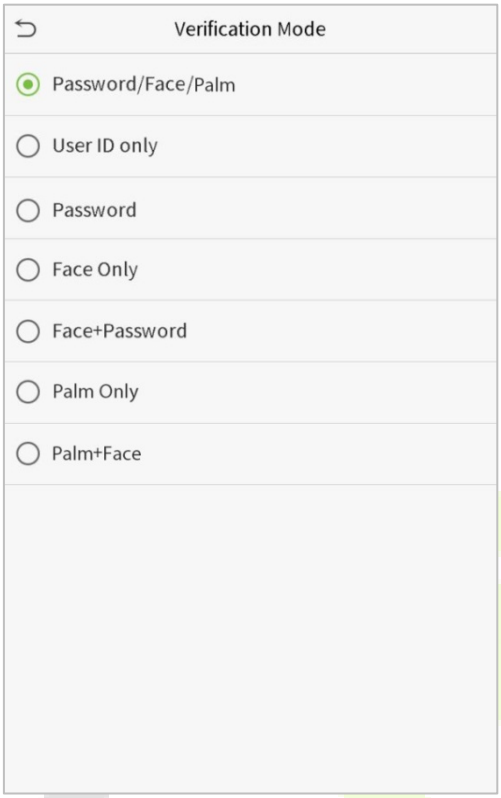


After successful verification, the prompt "Successfully verified" will appear.

If the verification is failed, it will prompt "**Please adjust your position!**".

2.6.4 Combined Verification

To ensure security, this device offers multiple verification methods. A total of 7 different verification combinations can be used, as shown below:

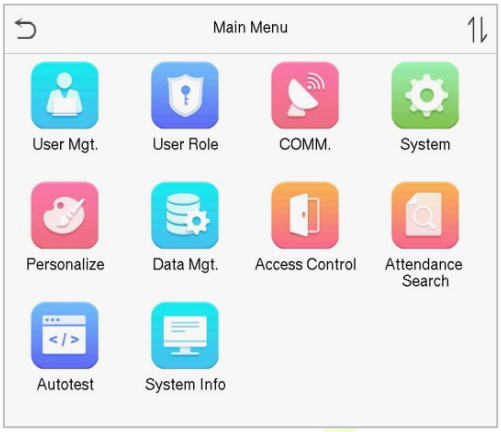


Note:

- "/" 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 the verification.

3 Main Menu

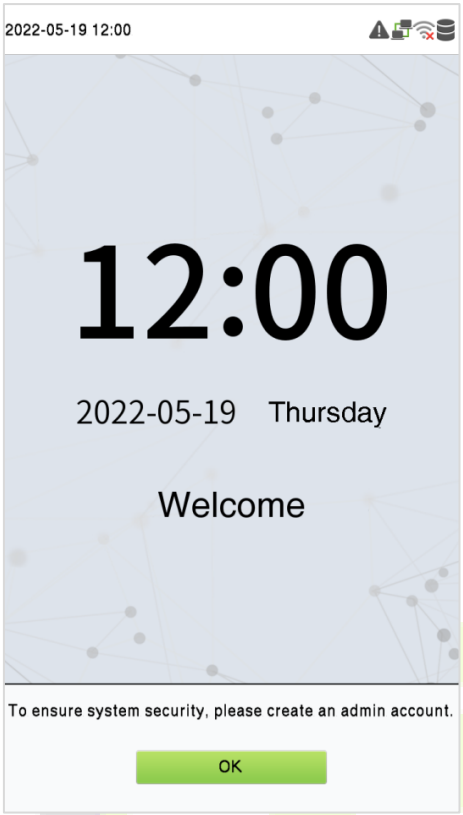
Press on the initial interface to enter the main menu, as shown below:



Menu	Description
User Mgt.	To add, edit, view, and delete basic information about a user.
User Role	To set the permission scope of the custom role and enroller, that is, the rights to operate the system.
COMM.	To set the relevant parameters of the network, PC connection, wireless network, cloud server and Wiegand.
System	To set the parameters related to the system, including date & time, access records, facial templates, palm templates, security setting, resetting to factory settings, temperature management and detection management.
Personalize	This includes user Interface, voice, bell, punch state options and shortcut key mappings settings.
Data Mgt.	To delete all the relevant data in the device.
Access Control	To set the parameters of the lock and access control device.
Attendance Search	To query the specified access record, check attendance photos and blocklist photos.
Autotest	To automatically test whether each module functions properly, including the screen, audio, camera, and real-time clock.
System Info	To view the data capacity, device, firmware information and privacy policy of the current device.

Note: When users use the product for the first time, they should operate it after setting administrator privileges. Tap **User Mgt.** to add an administrator or edit user permissions as a super administrator. If the

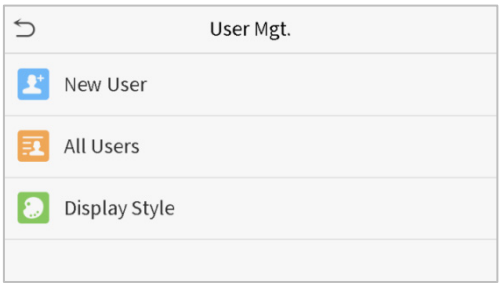
product does not have an administrator setting, the system will show an administrator setting command prompt every time you enter the device menu.



4 User Management

4.1 Adding Users

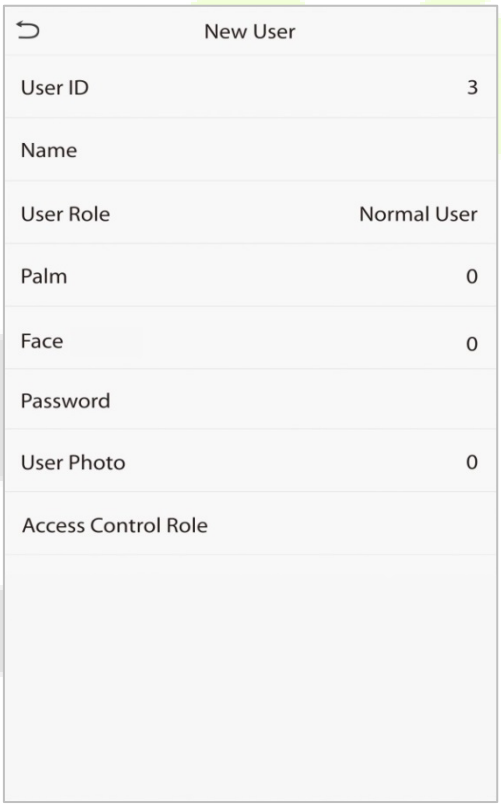
Click **User Mgt.** on the main menu.



Click **New User.**

- **Register a User ID and Name**

Enter the User ID and Name.



Note:

- A User Name may contain 17 characters.
- The User ID may contain 1 to 9 digits by default.
- During the initial registration, you can modify your ID, which cannot be modified after registration.
- If a message "Duplicated ID" pops up, you must choose another ID.

- **Setting the User Role**

There are two types of user accounts namely **Normal User** and **Super Admin**. If there is already a registered administrator, the normal users have no rights to manage the system and may only access the verification module. The administrator owns all the management privileges. If a custom role is set, you can also select **user defined role** permissions for the user.

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

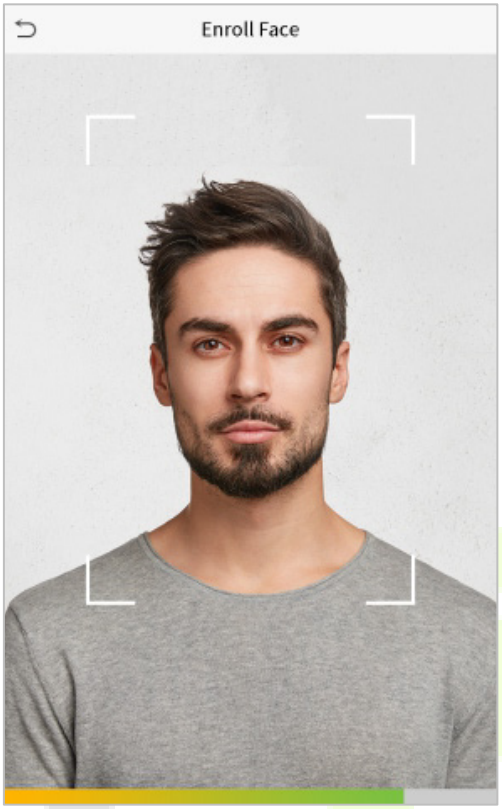
Note: If the selected user role is Super Admin, the user must pass the identity authentication to access the main menu. The authentication is based on the authentication method(s) that the super administrator has registered. Please refer "2.6 Verification Mode".

- **Register Palm**

Click **Palm** to open the palm registration page. Select the palm to be enrolled.

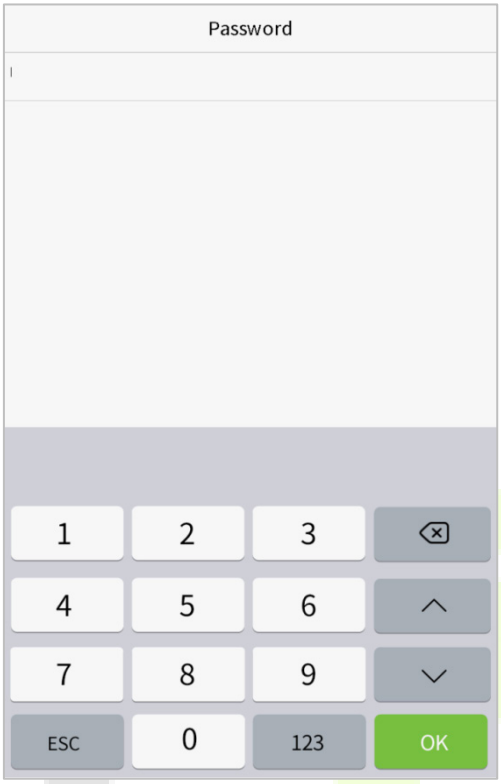
- **Register Face**

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



- **Register Password**

Click **Password** to open the password registration page. Enter a password and re-enter it for confirmation. Click **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 is verified successfully, 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.

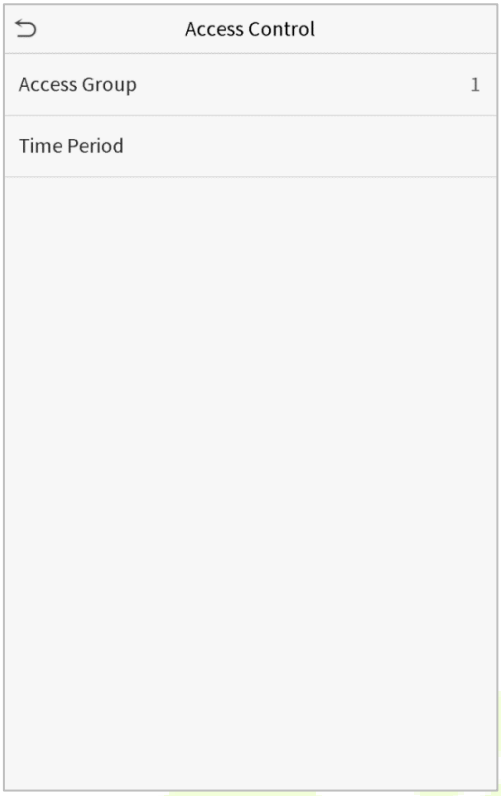
Note: While registering a face, the system will automatically capture a picture as the user photo. If you do not want to register a user photo, the system will automatically set the picture captured as the default photo.

- **Access Control Role**

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

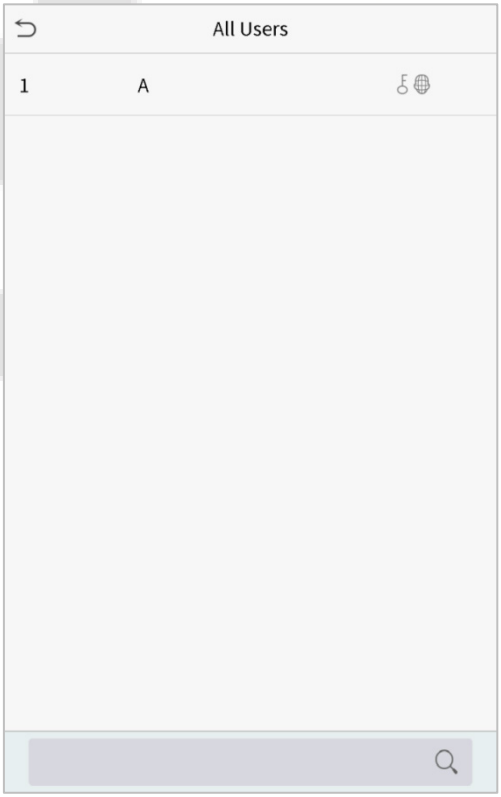
Click **Access Control Role** > **Access Group**, assign the registered users to different groups for better management. New users belong to Group 1 by default, and can be reassigned to other groups. The device supports up to 99 access control groups.

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



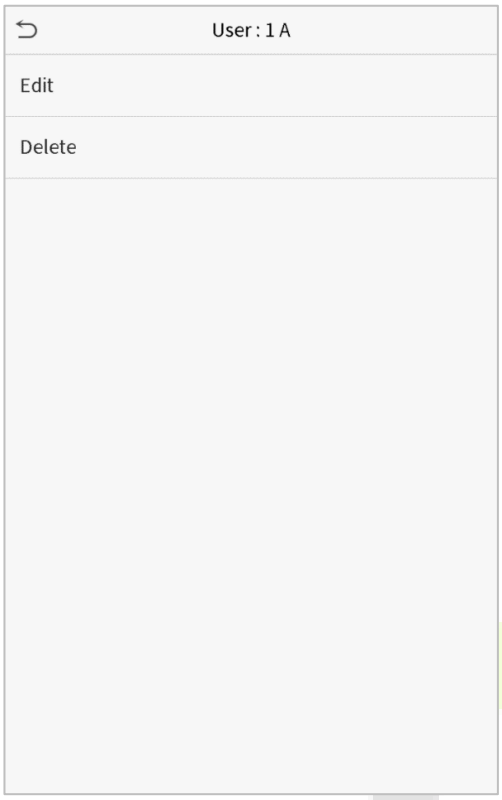
4.2 Search for Users

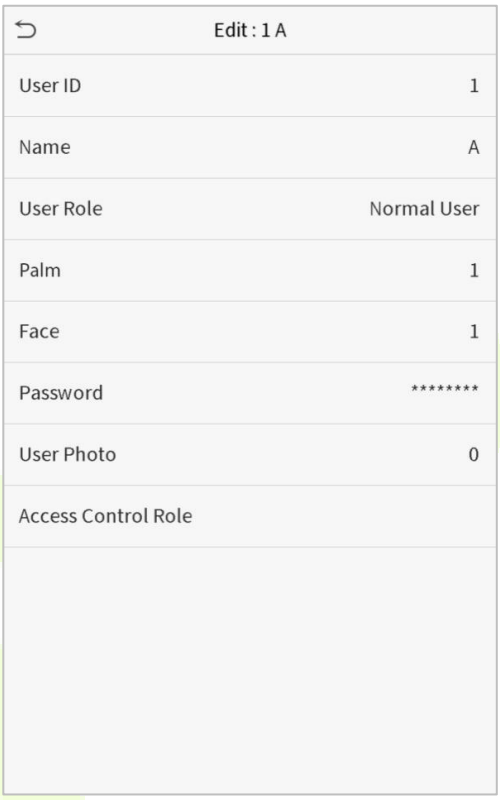
Click the search bar on the user list and enter the retrieval keyword (The keyword may be an ID, surname, or full name). The system will search for the users related to the information.



4.3 Edit Users

Choose a user from the list and click **Edit** to open the edit user interface:





Note: The operation of editing a user is the same as that of adding a user, except that the user ID cannot be modified when editing a user. Operation method refers to "4.1 Adding Users".

4.4 Deleting Users

Choose a user from the list and click **Delete** to enter the delete user interface. Select the user information to be deleted and click **OK**.

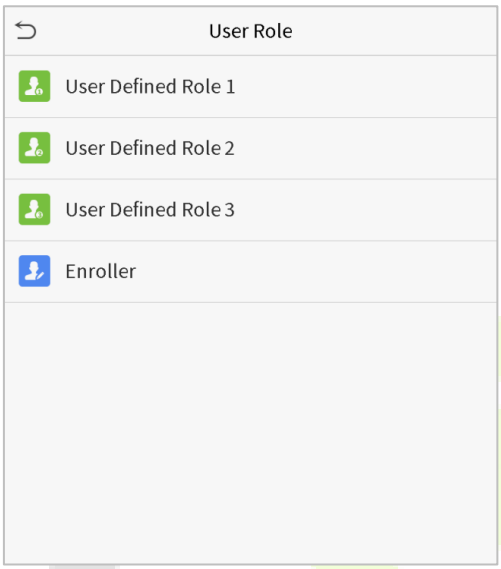
Note: If you select **Delete User**, all the information of the user will be deleted.

5 User Role

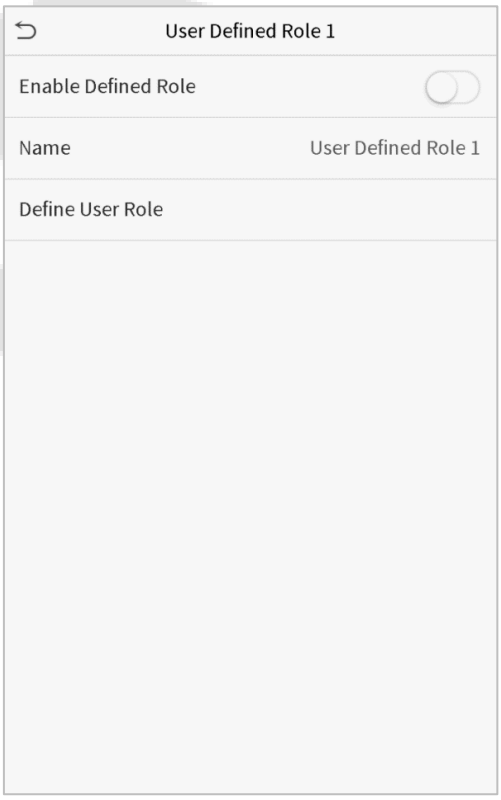
If you need to assign some specific permissions to certain users, you may edit the "User Defined Role" under the **User Role** menu.

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.

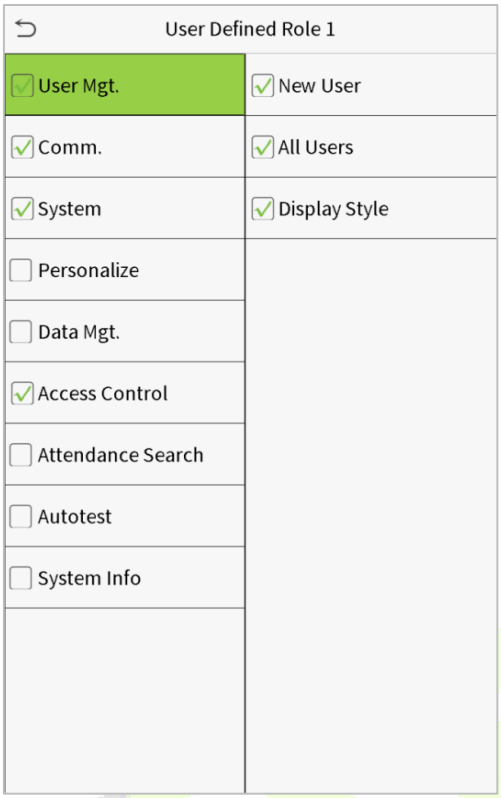
Click **User Role** on the main menu interface.



1. Click any role to set a defined role. Toggle the **Enable Defined Role** button to enable this defined role. Click **Name** and enter the name of the role.



2. Click **Define User Role** to assign the privileges to the role. Click **Return** after assigning privileges.



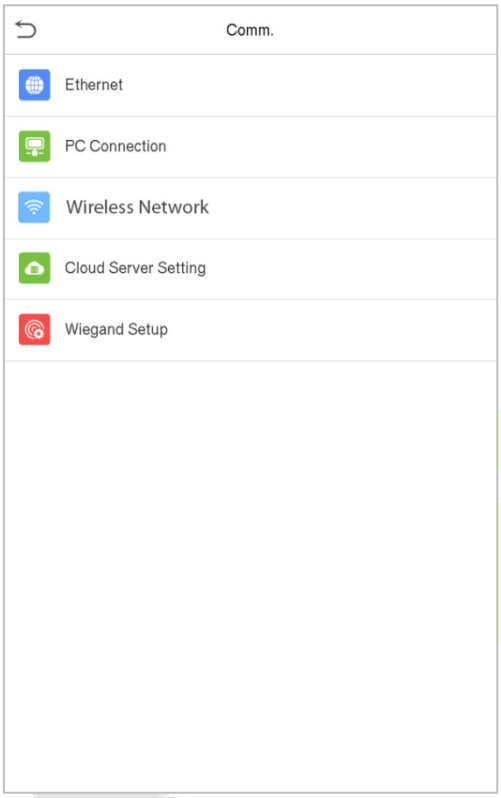
Note: During privilege assignment, the main menu is on the left and its sub-menus are on the right. You only need to select the features in sub-menus. If the device has a role enabled, you may assign the roles you set to users by clicking User Mgt. > New User > User Role.

If no super administrator is registered, the device will prompt "**Please register super administrator user first!**" after clicking the enable bar.

6 Communication Settings

The Communication Settings are used to set the parameters of the Network, PC connection, Wireless network, Cloud server and Wiegand.

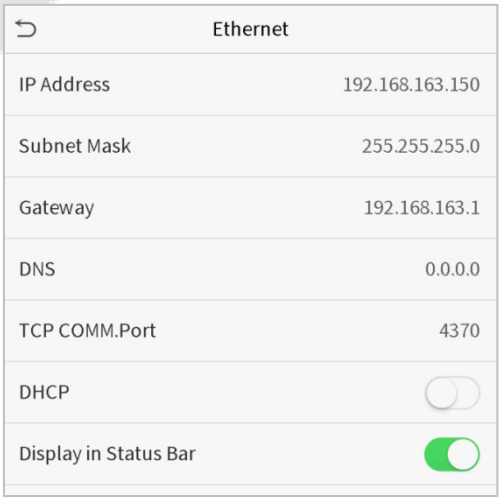
Tap **COMM.** on the main menu.



6.1 Network Settings

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

Click **Ethernet** on the Comm. Settings interface.



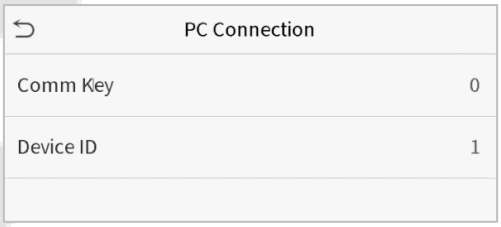
Menu Name	Description
IP Address	The factory default value is 192.168.1.201. Please set the value according to the actual network situation.
Subnet Mask	The factory default value is 255.255.255.0. Please set the value according to the actual network situation.
Gateway	The factory default address is 0.0.0.0. Please set the value according to the actual network situation.
DNS	The factory default address is 0.0.0.0. Please set the value according to the actual network situation.
TCP COMM. Port	The factory default value is 4370. Please set the value according to the actual network situation.
DHCP	Dynamic Host Configuration Protocol, which is to dynamically allocate IP addresses for clients via server.
Display in Status Bar	To set whether to display the network icon on the status bar.

6.2 PC Connection

To improve the security of data, please set a Comm Key for communication between the device and the PC.

If a Comm Key is set, this connection password must be entered before the device can be connected to the PC software.

Click **PC Connection** on the Comm. Settings interface.



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

6.3 Wireless Network

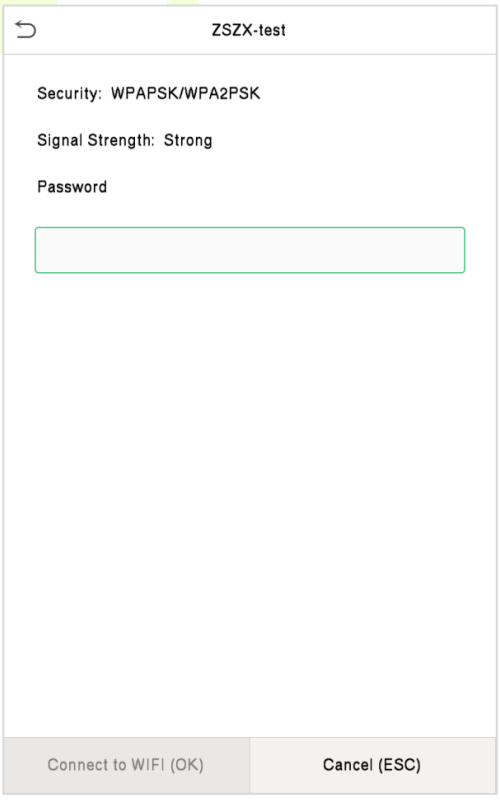
It is used for network connection, wireless data transmission and communication.

Click **Wireless Network** on the Comm. Settings interface.

Wi-Fi is enabled in the Device by default. Toggle on button to enable or disable Wi-Fi.

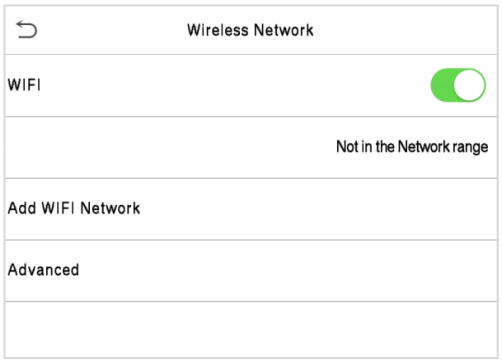
When Wi-Fi is enabled, tap on the required network from the searched network list.

Wi-Fi Enabled: Tap on the required network from the searched network list.

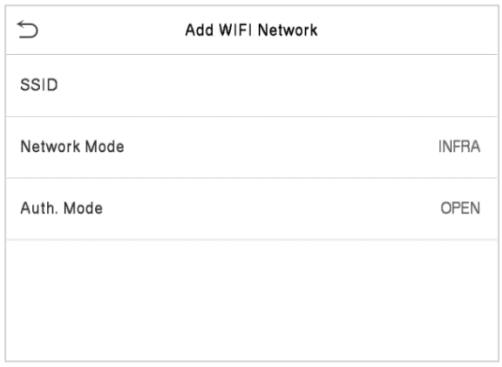


Tap on the password field to enter the password, and then tap on **Connect to Wi-Fi (OK).**

- **Add Wi-Fi Network Manually**



Tap on **Add Wi-Fi Network** to add the Wi-Fi manually.

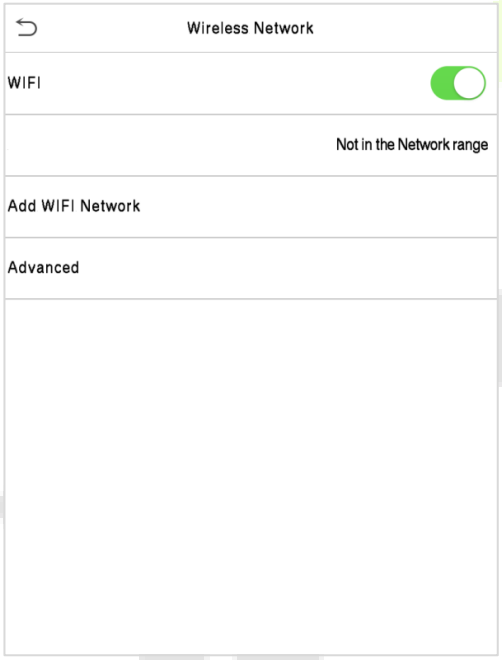


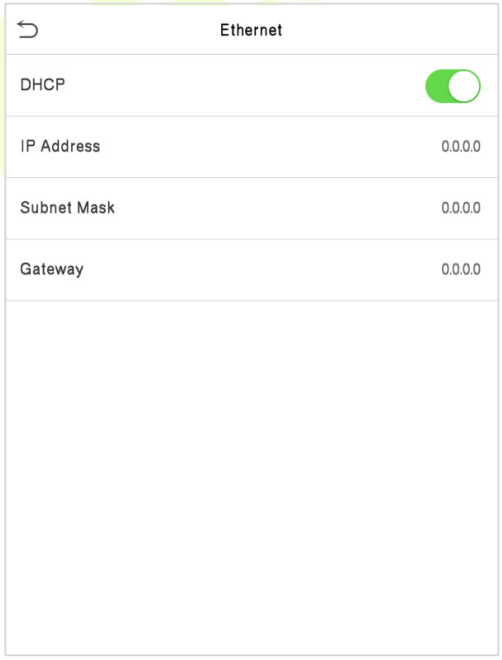
On this interface, enter the Wi-Fi network parameters. (The added network must exist.)

Once added, find the added Wi-Fi network in the list and connect to the network by following the same procedure.

- **Advanced Options**

This interface is used to set the network parameters.



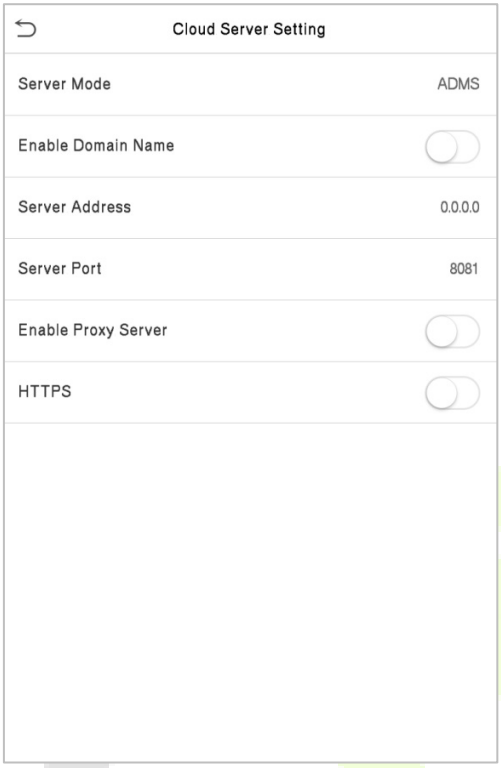


Menu Name	Description
DHCP	Dynamic Host Configuration Protocol, which involves allocating dynamic IP addresses to network clients.
IP Address	IP address of the Wi-Fi network.
Subnet Mask	Subnet mask of the Wi-Fi network.
Gateway	Gateway address of the Wi-Fi network.

6.4 Cloud Server Setting

This represents settings used for connecting the ADMS server.

Click **Cloud Server Setting** on the Comm. Settings interface.

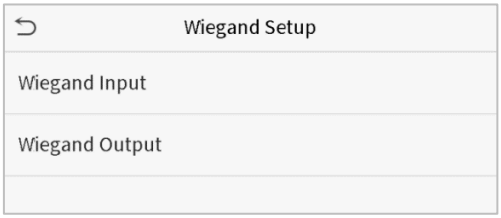


Menu		Description
Enable Domain Name	**Server Address**	When this function is enabled, the domain name mode "http://..." will be used, such as http://www.XYZ.com, while "XYZ" denotes the domain name when this mode is turned ON.
Disable Domain Name	**Server Address**	IP address of the ADMS server.
	Server Port	Port used by the ADMS server.
Enable Proxy Server		When you choose to enable the proxy, you need to set the IP address and port number of the proxy server.
HTTPS		To increase the security of browser access, users can enable the HTTPS protocol to create a secure and encrypted network transmission and assure the security of sent data through identity authentication and encrypted communication. This function is enabled by default. This function can be enabled or disabled through the menu interface, and when changing the HTTPS status, the device will pop up a security prompt, and restart after confirmation.

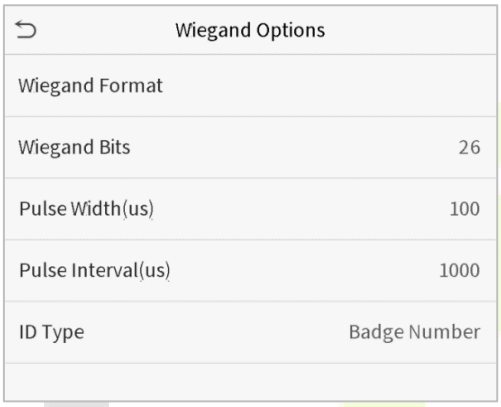
6.5 Wiegand Setup

The Wiegand Setup menu is used to set the Wiegand input and output parameters.

Click **Wiegand Setup** on the Comm. Settings interface.



6.5.1 Wiegand Input



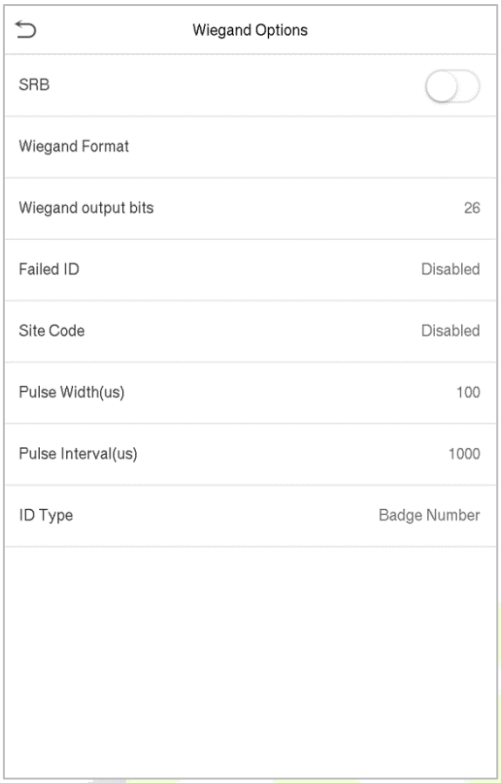
Menu Name	Description
Wiegand Format	Values range from 26 bits, 34 bits, 36 bits, 37 bits, and 50 bits.
Wiegand Bits	Number of bits of Wiegand data.
Pulse Width(us)	The value of the pulse width sent by Wiegand is 100 microseconds by default, which can be adjusted within the range of 20 to 100 microseconds.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

Definitions of various common Wiegand formats:

Wiegand Format	Definitions
Wiegand26	ECCCCCCCCCCCCCCCCCCCCCCCCO Consists of 26 bits of binary code. The 1st bit is the even parity bit of the 2nd to 13th bits, while the 26th bit is the odd parity bit of the 14th to 25th bits. The 2nd to 25th bits are the card numbers.

Wiegand26a	ESSSSSSSSCCCCCCCCCCCCCCCO Consists of 26 bits of binary code. The 1st bit is the even parity bit of the 2nd to 13th bits, while the 26th bit is the odd parity bit of the 14th to 25th bits. The 2nd to 9th bits are the site codes, while the 10th to 25th bits are the card numbers.
Wiegand34	ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO Consists of 34 bits of binary code. The 1st bit is the even parity bit of the 2nd to 17th bits, while the 34th bit is the odd parity bit of the 18th to 33rd bits. The 2nd to 25th bits are the card numbers.
Wiegand34a	ESSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCO Consists of 34 bits of binary code. The 1st bit is the even parity bit of the 2nd to 17th bits, while the 34th bit is the odd parity bit of the 18th to 33rd bits. The 2nd to 9th bits are the site codes, while the 10th to 25th bits are the card numbers.
Wiegand36	OFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCMME Consists of 36 bits of binary code. The 1st bit is the odd parity bit of the 2nd to 18th bits, while the 36th bit is the even parity bit of the 19th to 35th bits. The 2nd to 17th bits are the device codes. The 18th to 33rd bits are the card numbers, and the 34th to 35th bits are the manufacturer codes.
Wiegand36a	EFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCO Consists of 36 bits of binary code. The 1st bit is the even parity bit of the 2nd to 18th bits, while the 36th bit is the odd parity bit of the 19th to 35th bits. The 2nd to 19th bits are the device codes, and the 20th to 35th bits are the card numbers.
Wiegand37	OMMMMSSSSSSSSSSSCCCCCCCCCCCCCCCCCCE Consists of 37 bits of binary code. The 1st bit is the odd parity bit of the 2nd to 18th bits, while the 37th bit is the even parity bit of the 19th to 36th bits. The 2nd to 4th bits are the manufacturer codes. The 5th to 16th bits are the site codes, and the 21st to 36th bits are the card numbers.
Wiegand37a	EMMMFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCCO Consists of 37 bits of binary code. The 1st bit is the even parity bit of the 2nd to 18th bits, while the 37th bit is the odd parity bit of the 19th to 36th bits. The 2nd to 4th bits are the manufacturer codes. The 5th to 14th bits are the device codes, and15th to 20th bits are the site codes, and the 21st to 36th bits are the card numbers.
Wiegand50	ESSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO Consists of 50 bits of binary code. The 1st bit is the even parity bit of the 2nd to 25th bits, while the 50th bit is the odd parity bit of the 26th to 49th bits. The 2nd to 17th bits are the site codes, and the 18th to 49th bits are the card numbers.
"C" denotes the card number; **"E"** denotes the even parity bit; **"O"** denotes the odd parity bit; **"F"** denotes the facility code; **"M"** denotes the manufacturer code; **"P"** denotes the parity bit; and **"S"** denotes the site code.	

6.5.2 Wiegand Output

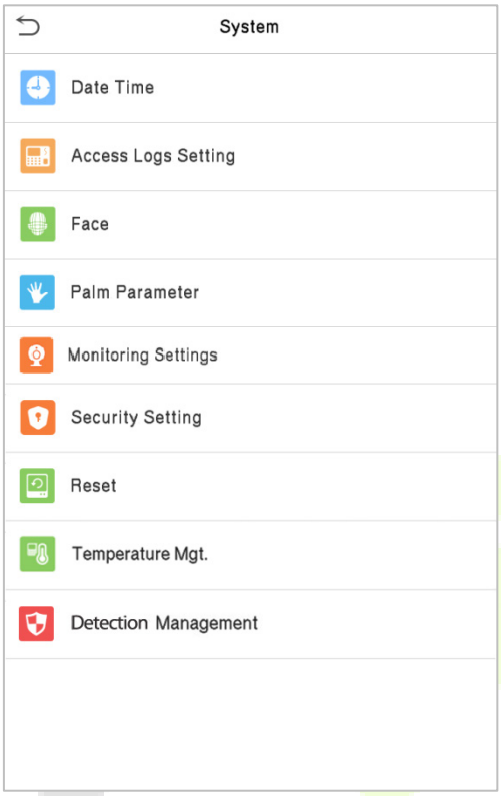


Menu Name	Description
SRB(Security Relay Box)	When SRB is enabled, the lock is controlled by the SRB to prevent the lock from being opened due to device removal.
Wiegand Format	Values range from 26 bits, 34 bits, 36 bits, 37 bits, and 50 bits.
Wiegand Output Bits	After choosing the Wiegand format, you can select one of the corresponding output digits in the Wiegand format
Failed ID	If the verification is failed, the system will send the failed ID to the device and replace the card number or Personnel ID with the new ones.
Site Code	It is similar to the device ID. The difference is that a site code can be set manually, and is repeatable in a different device. The valid value ranges from 0 to 256 by default.
Pulse Width(us)	The time width represents the changes of the quantity of electric charge with high-frequency capacitance regularly within a specified time.
Pulse Interval(us)	The time interval between pulses.
ID Type	Select between User ID and Access Card.

7 System Settings

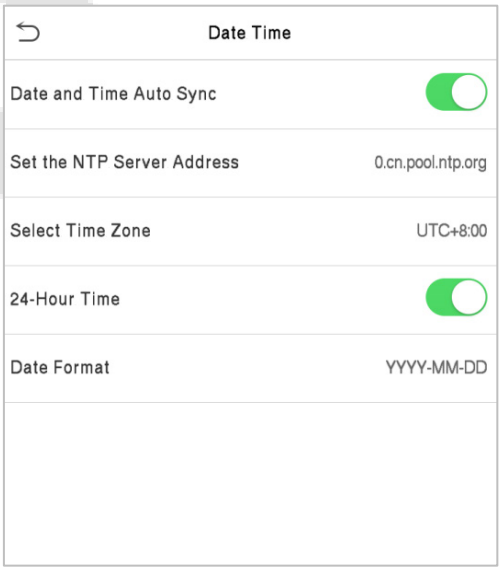
Here, you can set the related system parameters to optimize the performance of the device.

Click **System** on the main menu interface.



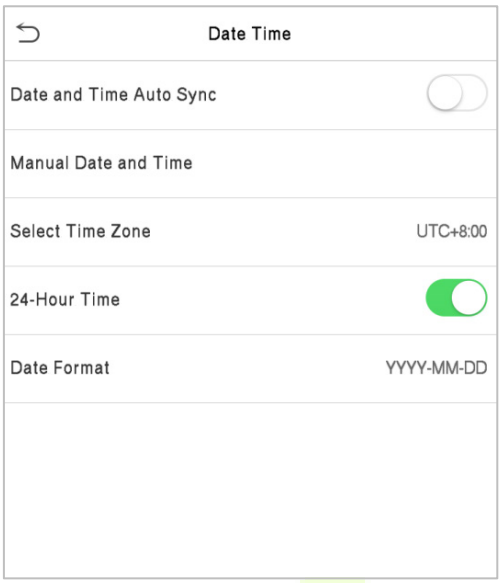
7.1 Date and Time

Click **Date Time** on the System interface.



1. The product supports the NTP synchronization time system by default. This function takes effect after **Date and Time Auto Sync** is enabled and the corresponding NTP server address link is set.

2. If users need to set date and time manually, disable **Date and Time Auto Sync** first, and then tap **Manual Time Setting** to set date and time and tap Confirm to save.



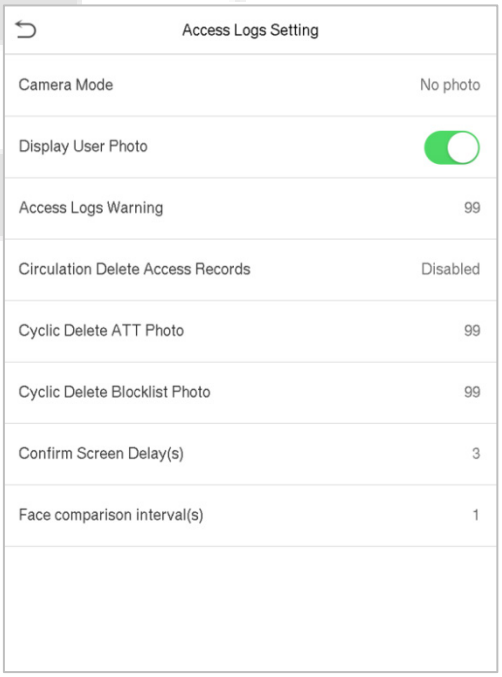
3. Toggle the button to enable or disable the 24-Hour time format and select the date format.

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

Note: For example, the user sets the time of the device (18:35 on March 15, 2020) to 18:30 on January 1, 2021. After restoring the factory settings, the time of the equipment will change to 18:30 on January 1, 2021.

7.2 Access Logs Setting

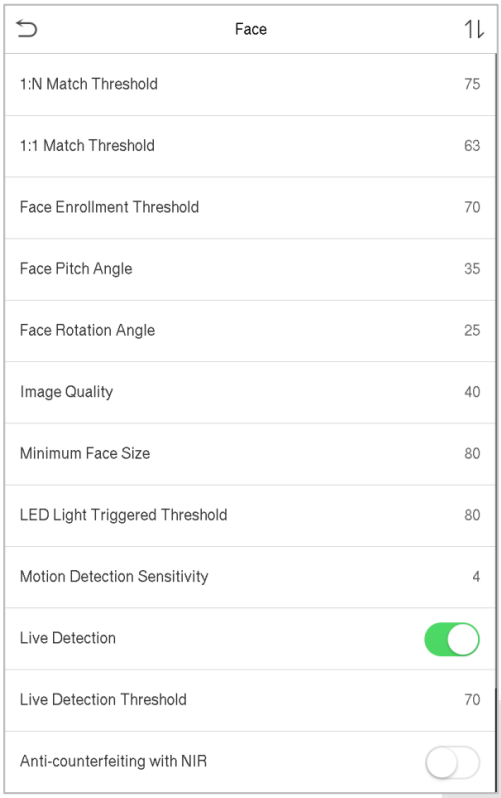
Click **Access Logs Setting** on the System interface.



Menu Name	Description
Camera Mode	This function is disabled by default. When enabled, a security prompt will pop-up and the sound of shutter in the camera will turn on mandatorily. There are 5 modes: **No photo:** No photo is taken during user verification. **Take photo, no save:** Photo is taken but is not saved during verification. **Take photo and save:** Photo is taken and saved during verification. **Save on successful verification:** Photo is taken and saved for each successful verification. **Save on failed verification:** Photo is taken and saved during each failed verification.
Display User Photo	This function is disabled by default. When enabled, there will be a security prompt.
Access Logs Warning	When the record space reaches a set value, the device will automatically display an alert. Users may disable the function or set a valid value between 1 and 9999.
Circulation Delete Access Records	When the access records have reached full capacity, the device will automatically delete a set value of old access records. Users may disable the function or set a valid value between 1 and 999.
Cyclic Delete ATT Photo	When the attendance photos have reached full capacity, the device will automatically delete a set value of old attendance photos. Users may disable the function or set a valid value between 1 and 99.
Cyclic Delete Blocklist Photo	When the blocklisted photos have reached full capacity, the device will automatically delete a set value of old blocklisted photos. Users may disable the function or set a valid value between 1 and 99.
Confirm Screen Delay(s)	The time duration to display the success verification message. The valid value is 1 to 9 seconds.
Face Comparison Interval (s)	To set the facial template matching time interval as needed. The valid value is 0 to 9 seconds.

7.3 Face Parameters

Click **Face** on the System interface.



FRR	FAR	Recommended matching thresholds	
		1:N	1:1
High	Low	85	80
Medium	Medium	82	75
Low	High	80	70

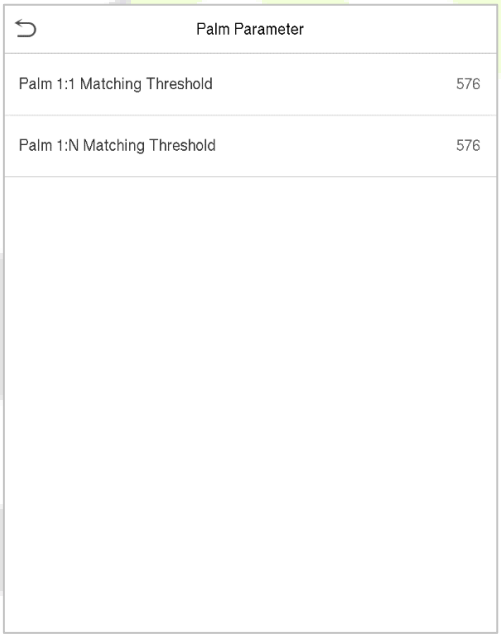
Menu Name	Description
1:N Match Threshold	In 1:N verification mode, the verification will only be successful when the similarity between the acquired facial image and all the registered facial templates is greater than the set value. The valid value ranges from 0 to 100. The higher the thresholds, the lower the misjudgement rate, the higher the rejection rate, and vice versa. The default value of 75 is recommended.
1:1 Match Threshold	In 1:1 verification mode, the verification will only be successful when the similarity between the acquired facial image and the facial templates enrolled in the device is greater than the set value. The valid value ranges from 0 to 100. The higher the thresholds, the lower the misjudgement rate, the higher the rejection rate, and vice versa. The default value of 63 is recommended.
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 the registered facial templates is greater than this threshold, it indicates that the face has already been registered.

Face Pitch Angle	The pitch angle tolerance of a face for facial registration and comparison. If a face's pitch angle exceeds this set value, it will be filtered by the algorithm, i.e. ignored by the terminal thus no registration and comparison interface will be triggered.
Face Rotation Angle	The rotation angle tolerance of a face for facial template registration and comparison. If a face's rotation angle exceeds this set value, it will be filtered by the algorithm, i.e. ignored by the terminal thus no registration and comparison interface will be triggered.
Image Quality	Image quality for facial registration and comparison. The higher the value, the clearer the image.
Minimum Face Size	Required for facial registration and comparison. If an object's size is smaller than this set value, the object will be filtered and not recognized as a face. This value can be taken as the face comparison distance. The farther the person is, the smaller the face is, and the smaller the face pixel will be obtained by the algorithm. Therefore, adjusting this parameter can adjust the furthest comparison distance of faces. When the value is 0, the face comparison distance is not limited.
LED Light Triggered Threshold	This value controls to turn on and off the LED light. The larger the value, the more frequently the LED light will be turned on.
Motion Detection Sensitivity	A measurement of the amount of change in a camera's field of view that qualifies as potential motion detection that wakes up the terminal from standby to the comparison interface. The larger the value, the more sensitive the system would be, i.e. if a larger value is set, the comparison interface is much easier and frequently triggered.
Live Detection	Detecting a spoof attempt by determining whether the source of a biometric sample is a live human being or a fake representation using visible light images.
Live Detection Threshold	Judges whether the visible image comes from an alive body. The larger the value, the better the visible light anti-spoofing performance.
Anti-counterfeiting with NIR	Using near-infrared spectra imaging to identify and prevent fake photos and videos attack.
Binocular Live Detection Threshold	It is convenient to judge whether the near-infrared spectral imaging is fake photo and video. The larger the value, the better the anti-spoofing performance of near-infrared spectral imaging.

WDR	Wide Dynamic Range (WDR), which balances light and extends image visibility for surveillance videos under high contrast lighting scenes and improves object identification under bright and dark environment.
Anti-flicker Mode	Used when WDR is turned off. This helps reduce flicker when the device's screen flashes at the same frequency as the light.
Face Algorithm	Facial algorithm related information and pause the facial template update.
Save Photo as Template	This function is enabled by default, and the menu interface supports enabling or disabling this function, and there is a security prompt when switching. When this function is disabled, it will indicate that there is a risk reminder: "**Face re-registration is required after an algorithm upgrade.**"
Notes	Improper adjustment of the exposure and quality parameters may severely affect the performance of the device. Please adjust the exposure parameter only under the guidance of the after-sales service personnel of our company.

7.4 Palm Parameters

Click **Palm** on the System interface.

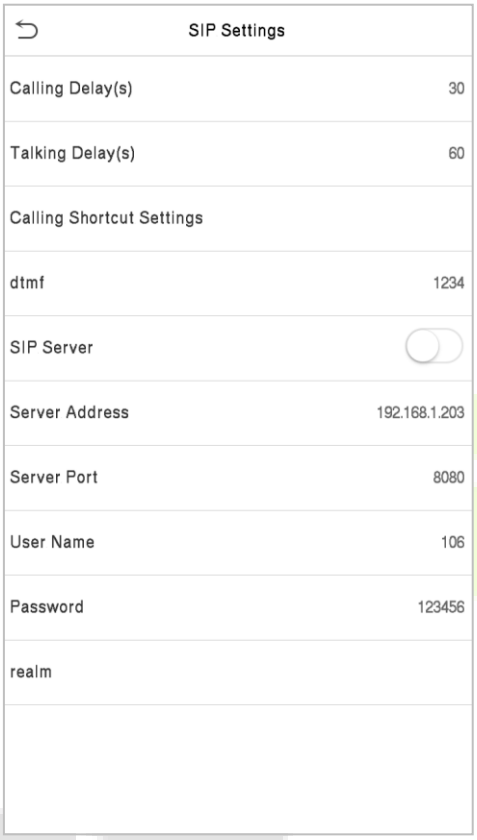


Menu Name	Description
Palm 1:1 Matching Threshold	In 1:1 Verification Method, only when the similarity between the verifying palm and the user's registered palm is greater than this value can the verification succeed.
Palm 1:N Matching Threshold	In 1:N Verification Method, only when the similarity between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

7.5 Monitoring Settings★

Tap **Monitoring Settings** on the **System** interface to go to the monitoring parameter settings.

Note: This function needs to be used with the indoor station Vpad A2. Please refer to 18 Connecting to SIP.



Function Description

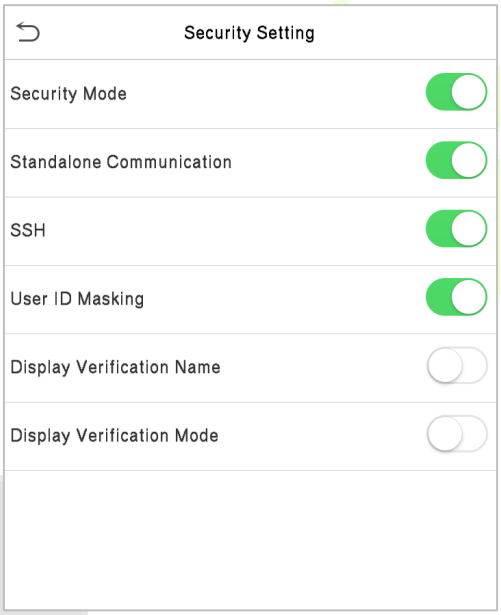
Function Name	Description
Calling Delay(s)	Set the time of call, valid value 30 to 60 seconds.
Talking Delay(s)	Set the time of intercom, valid value 60 to 120 seconds.
Calling Shortcut Settings	You can set a shortcut key to call the indoor station quickly without entering the IP address of the indoor unit each time.
dtmf	The value of WebServer is the same as the value of DMTF in the device in order to unlock it.
SIP Server	Select whether to enable the server address. Once you have connected to the server, you can call it by entering the username of the indoor station.

Server Address	Enter the server address.
Server Port	Enter the server port.
User Name	Enter the Username of server.
Password	Enter the password of server.
realm	Enter the realm of server.

The ProFace X and the indoor station to achieve video intercom there are two modes, respectively, the LAN and SIP server.

7.6 Security Setting

Click **Security Setting** on the System interface.



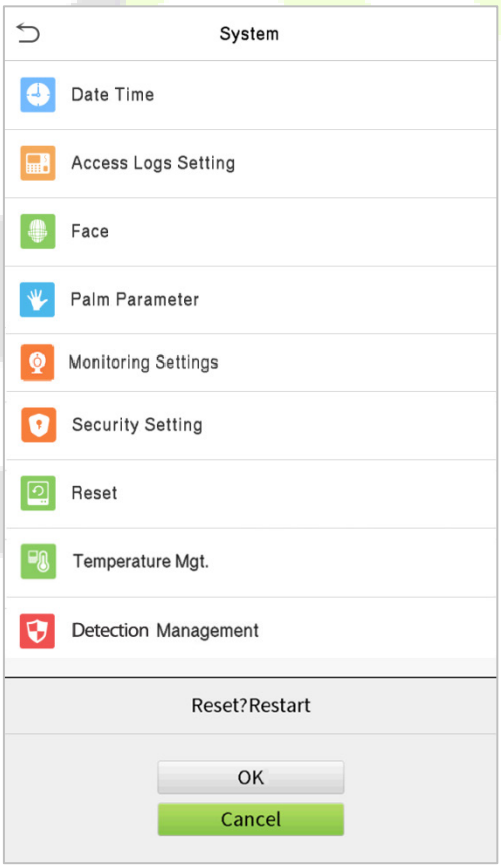
Menu Name	Description
Security Mode	When enabled, user information verification has a high level of security. This function can be enabled or disabled via the menu interface. When switching on and off, there are security prompts. All data will be deleted and the device will be restarted after confirmation. **Note:** After turning on the security mode, the product will forcibly enable the function of returning to the standby interface when the menu times out by default (default 60s). It does not support disabling in security mode, but it does support disabling in non-security mode. To configure, go to **Personalize** > **User Interface** > **Menu Screen Timeout(s)**.
Standalone Communication	By default, this function is disabled. This function can be enabled or disabled via the menu interface. When it is switched on, a security prompt appears, and the device will restart after you confirm.

SSH	The device does not support the Telnet feature, hence SSH is typically used for remote debugging. By default, SSH is enabled. The menu interface allows you to enable and disable SSH. When enabled, there will be a security prompt, but the device will not need to be restarted after confirmation.
User ID Masking	After enabled, the User ID will be partially displayed after the personnel verification result (only the User ID with more than 2 digits supports the masking display), and it is enabled by default.
Display Verification Name	After enabled, the user's name will be displayed in the personnel verification result. The verification result will not show the name after disabling it.
Display Verification Mode	After enabled, the personnel verification result will show the user's verification mode. The verification result will not show the verification mode after you disable it.

7.7 Factory Reset

The Factory reset module restores the device, such as communication settings and system settings, to factory settings (does not clear the registered user data).

Click **Reset** on the System interface.

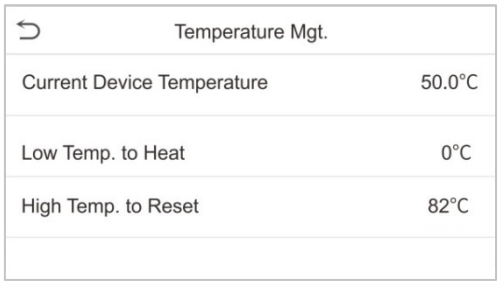


Click **OK** to reset.

7.8 Temperature Management

The device has a built-in temperature sensor, and when the environment temperature is too low or too high, it will trigger self-heating or shut down.

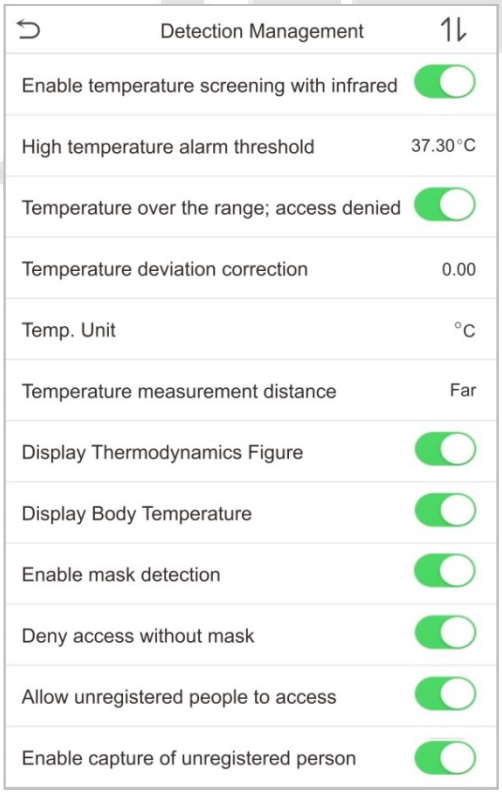
Click **Temperature Mgt.** on the System interface.

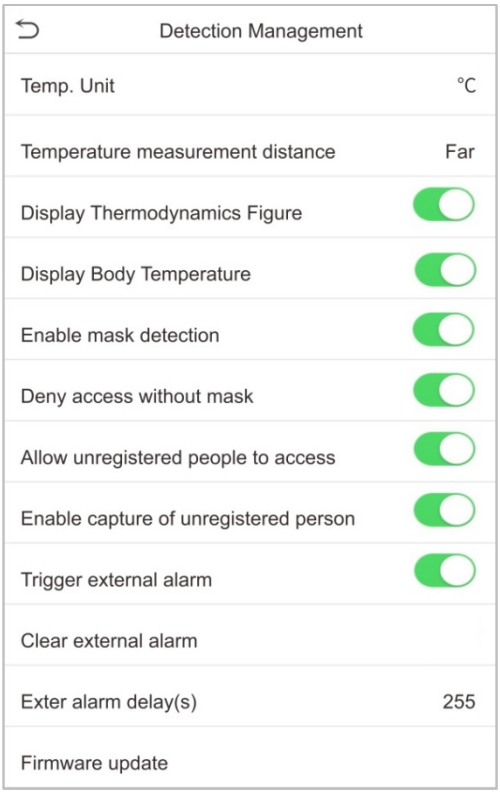


Menu Name	Description
Current Device Temperature	This column shows the real- time temperature of the device.
Low Temp. to Heat	Once the device temperature is lower than the set value, the device will start self-heating, the range is 0 to 10(℃).
High Temp. to Reset	When the device temperature is lower than the set value, it will shut down automatically to protect the hardware, the range is 60 to 80 (℃).

7.9 Detection Management★

Click **Detection Management** on the System interface.





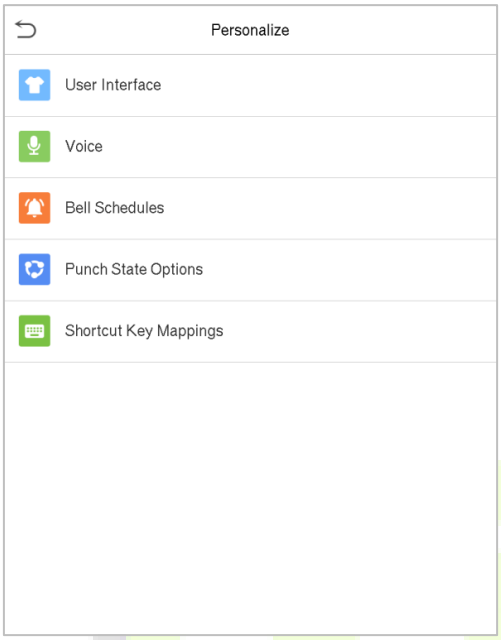
Function Name	Description
Enable Temperature Screening with Infrared	To enable or disable the infrared temperature measurement function. When this function is enabled, before the access is granted, users must pass the temperature screening in addition to identity verification. To measure body temperature, users' faces must be aligned with the temperature measurement area.
High Temperature Alarm Threshold	To set the value of the alarm threshold of high body temperature. When the temperature measured during verification is higher than the set value, the device will give a prompt and audio alarm. The default alarm threshold is 37.30°C.
Temperature Over the Range; Access Denied	When this function is enabled, if the user's body temperature measured is above (or below) the alarm threshold, the user will not be granted access even if his/her identity is verified. If this function is disabled, the user is allowed to access the restricted area when his/her identity is verified, regardless of his/her body temperature.
Temperature Deviation Correction	As the temperature measurement module allows a small range of errors (disturbance) of an observed value under different environments (humidity, room temperature and such), users may set the deviation value here.
Temp. Unit	The unit of body temperature can be switched between Celsius (°C) and Fahrenheit (°F).
Temperature Measurement Distance	When measuring temperature during the verification process, there are three modes: Near, Close and Far.
Display Thermodynamics Figure★	To enable or disable the display of the thermal image of a person. When enabled, the thermal image of the person is be displayed in the upper left corner of the device during the detection process.
Enable Palm Temp. Detection★	To enable or disable the palm temperature detection function. When enabled, the device will display the user's palm temperature during the verification process. **Note:** This function is not enabled by default, and can be upgraded to support.
Temperature Calibration★	Calibrate the temperature by comparing the current temperature value with the surface temperature value of the device.
Enable Mask Detection	To enable or disable the mask detection function. When it's enabled, the device will identify whether the user is wearing a mask or not during verification.

Display Body Temperature	To enable or disable the display body temperature function. When enabled, the device will display the user's specific temperature value during the verification process.
Enable Mask Detection	To enable or disable the mask detection function. When it's enabled, the device will identify whether the user is wearing a mask or not during verification.
Deny Access without Mask	To enable or disable the deny access without mask function. When it's enabled, even if the body temperature is normal, the person who does not wear a mask will not allow the person to enter.
Allow Unregistered People to Access	To enable or disable the unregistered people to access function. When enabled, as long as the person who passes the detection, the device allows the personnel to enter without registration.
Enable Capture of Unregistered Person	To enable or disable the capture of unregistered person function. When enabled, the device will automatically capture the photo of the unregistered person, enabling this feature requires to enable **Allow Unregistered People to Access**.
Trigger External Alarm★	When enabled, if the user's temperature is higher than the set threshold value or the mask detection is enabled, but the mask is not worn by the person, it will trigger an alarm.
Clear External Alarm★	It clears the triggered alarm records of the device.
External Alarm Delay(s)★	The delay (s) time for triggering an external alarm. It can be set in seconds. Users may disable the function or set a value between 1 to 255.
Firmware Update ★	Choose whether to update the thermal imaging temperature detection module software version.

8 Personalize Settings

You may customize the interface settings, audio and bell.

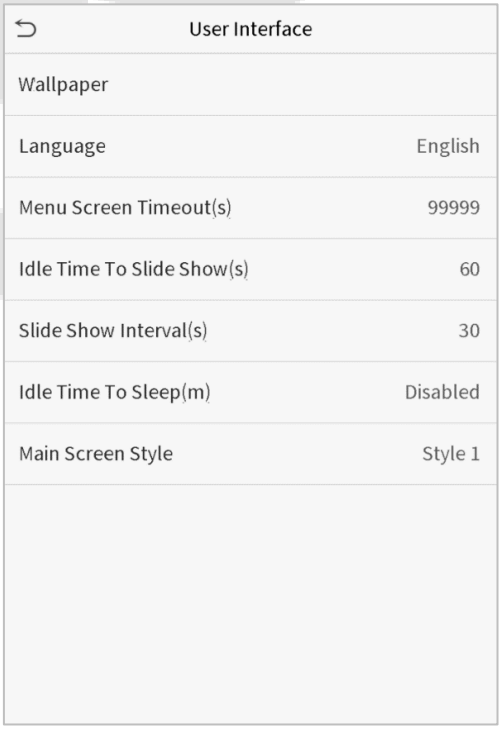
Click **Personalize** on the main menu interface.



8.1 Interface Settings

You can customize the display style of the main interface.

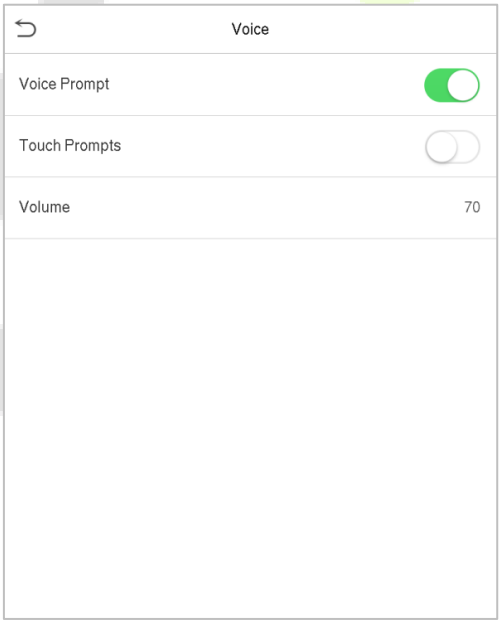
Click **User Interface** on the Personalize interface.



Menu Name	Description
Wallpaper	To select the main screen wallpaper according to your personal preference.
Language	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 will automatically go back to the initial interface. You can disable the function or set the value between 60 and 99999 seconds.
Idle Time to Slide Show (s)	When there is no operation, and the time exceeds the set value, a slide show will be played. It can be disabled, or you may set the value between 3 and 999 seconds.
Slide Show Interval (s)	This refers to the time interval switching 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 you have activated the sleep mode, when there is no operation, the device will enter standby mode. You can disable this function or set a value within 1 to 999 minutes.
Main Screen Style	To select the main screen style according to your personal preference.

8.2 Voice Settings

Click **Voice** on the Personalize interface.



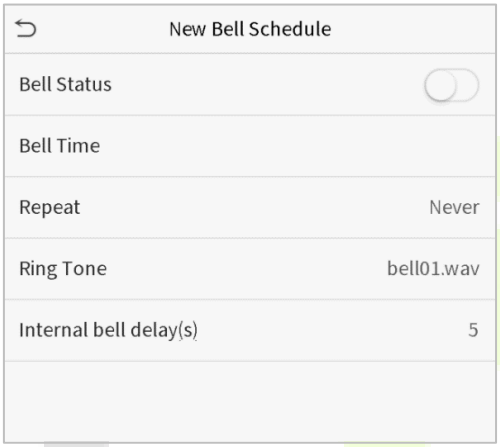
Menu Name	Description
Voice Prompt	Select whether to enable voice prompts during operating.
Touch Prompt	Select whether to enable keypad sounds.
Volume	Adjust the volume of the device and the valid value is 0 to 100.

8.3 Bell Schedules

Click **Bell Schedules** on the Personalize interface.

- **Add a Bell**

1. Click **New Bell Schedule** to enter the adding interface:



Function Name	Description
Bell Status	Set whether to enable the bell status.
Bell Time	At this time of day, the device automatically rings the bell.
Repeat	Set the repetition cycle of the bell.
Ring Tone	Select a ring tone.
Internal Bell Delay(s)	Set the duration of the internal bell. Valid values range from 1 to 999 seconds.

2. Back to the Bell Schedules interface; click **All Bell Schedules** to view the newly added bell.

- **Edit a Bell**

On the All Bell Schedules interface, tap the bell to be edited.

Click **Edit**, the editing method is the same as the operations of adding a bell.

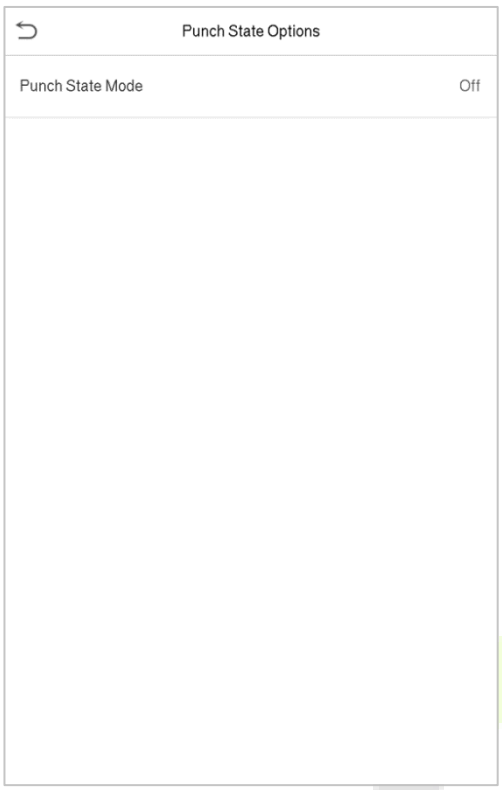
- **Delete a Bell**

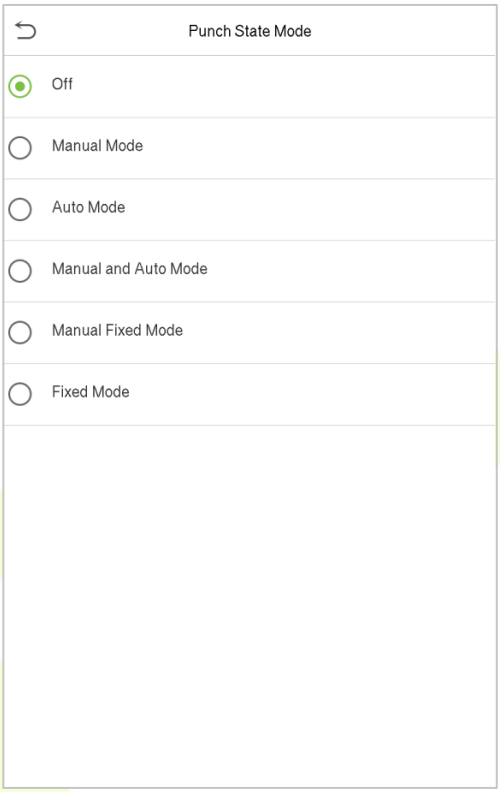
On the All Bell Schedules interface, tap the bell to be deleted.

Tap **Delete** and select **Yes** to delete the bell.

8.4 Punch States Options

Click **Punch State Options** on the Personalize interface.



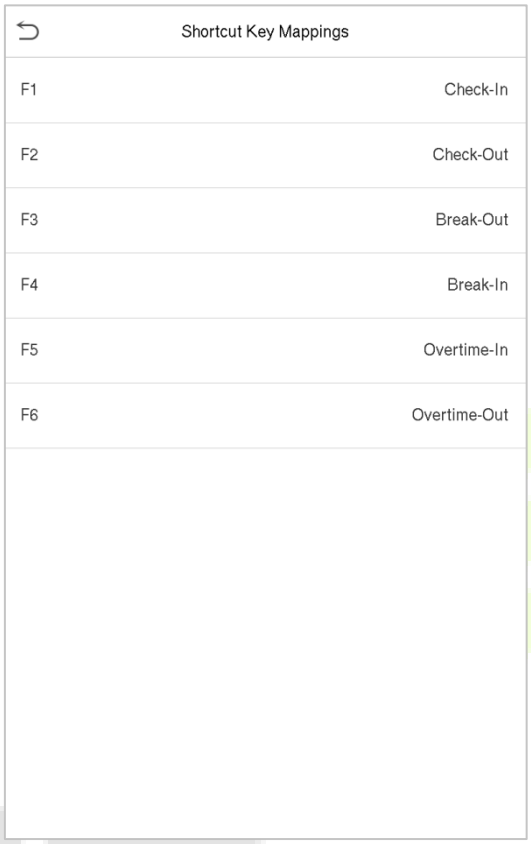


Function Name	Description
Punch State Mode	Select a punch state mode, which can be: **Off:** To disable the punch state key function. The punch state key set under **Shortcut Key Mappings** menu will become invalid. **Manual Mode:** To switch the punch state key manually, and the punch state key will disappear after **Punch State Timeout**. **Auto Mode:** After this mode is chosen, set **the** switching time of punch state key in **Shortcut Key Mappings**; when the switching time is reached, the set punch state key will be switched automatically. **Manual and Auto Mode:** Under this mode, the main interface will display the auto-switching punch state key, meanwhile supports manually switching punch state key. After the timeout, the manually switching punch state key will become an auto-switching punch state key. **Manual Fixed Mode:** After the punch state key is manually switched, the punch state key will remain unchanged until being manually switched next time. **Fixed Mode:** Only the fixed punch state key will be shown, and it cannot be switched.

8.5 Shortcut Keys Mappings

Users may define shortcuts as attendance status or functional keys. On the main interface, when the shortcut keys are pressed, the corresponding attendance status or function interface will quickly display.

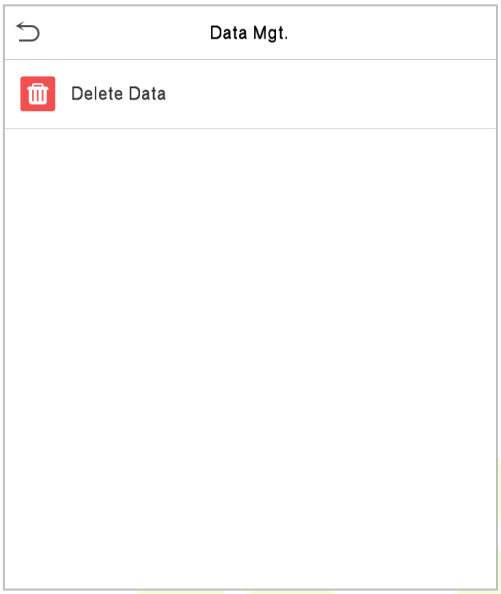
Click **Shortcut Key Mappings** on the Personalize interface.



9 Data Management

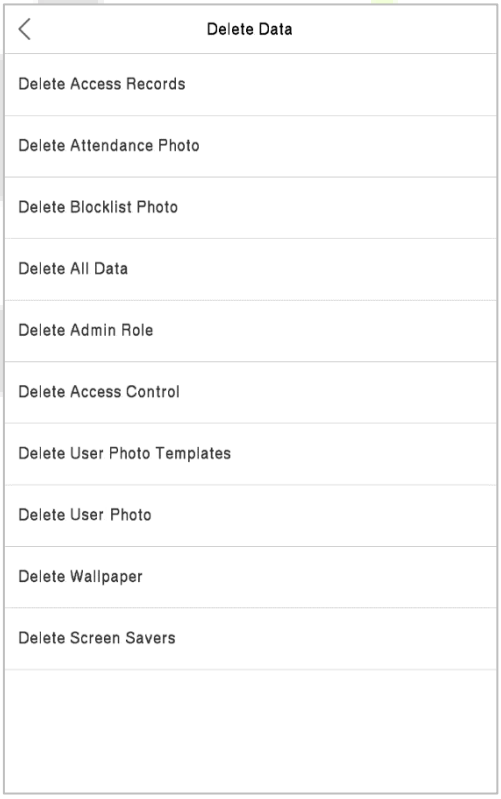
The Data Management interface is used to delete the relevant data in the device.

Click **Data Mgt.** on the main menu interface.



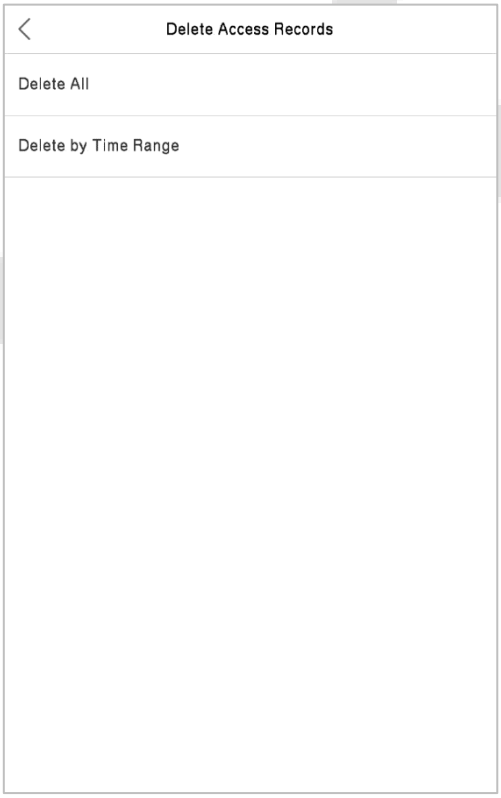
9.1 Delete Data

Click **Delete Data** on the Data Mgt. interface.

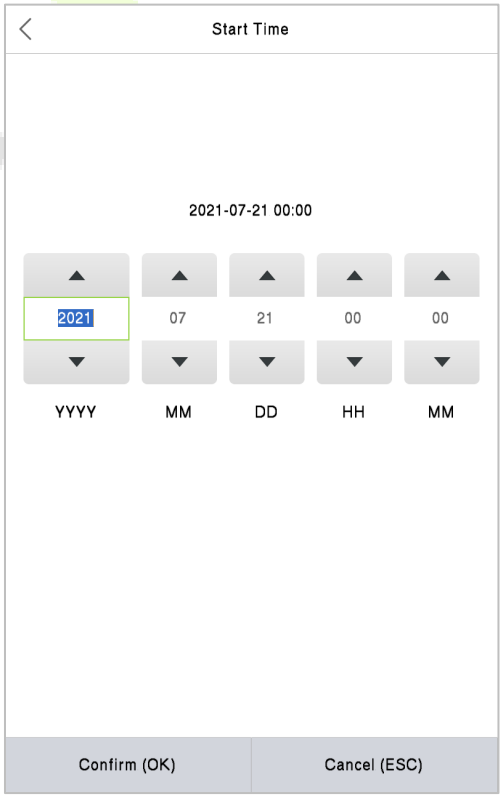


Menu Name	Description
Delete Access Records	To delete the access records conditionally.
Delete Attendance Photo	To delete the attendance photos of the designated personnel.
Delete Blocklist Photo	To delete the photos taken during verifications those failed.
Delete All Data	To delete information and access records of all registered users.
Delete Admin Role	To remove the administrator privileges.
Delete Access Control	To delete all the access data.
Delete User Photo Templates	When deleting template photos, there is a risk reminder: "**Face re-registration is required after an algorithm upgrade.**"
Delete User Photo	To delete all the user photos in the device.
Delete Wallpaper	To delete all the wallpapers in the device.
Delete Screen Savers	To delete the screen savers in the device.

Note: When deleting the access records, attendance photos or blocklisted photos, you may select Delete All or Delete by Time Range. Selecting Delete by Time Range, you need to set a specific time range to delete all data with the period.



Select Delete by Time Range.

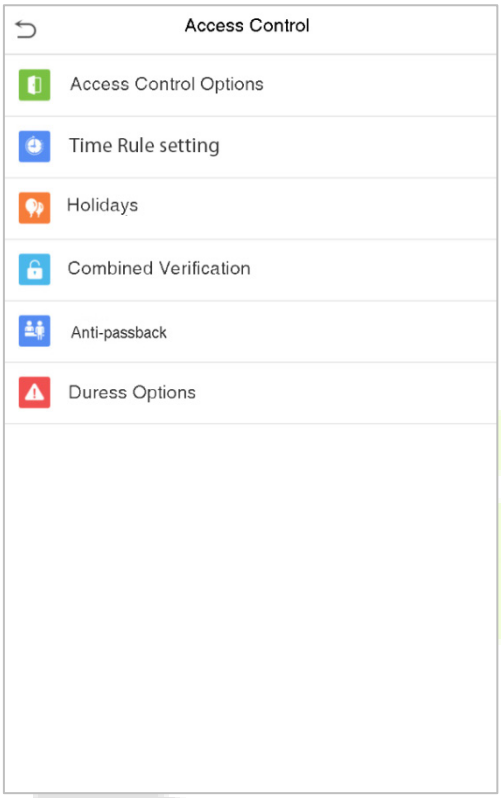


Set the time range and click OK.

10 Access Control

Access Control is used to set the schedule of door opening, lock control and other parameters settings related to access control.

Click **Access Control** on the main menu interface.



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

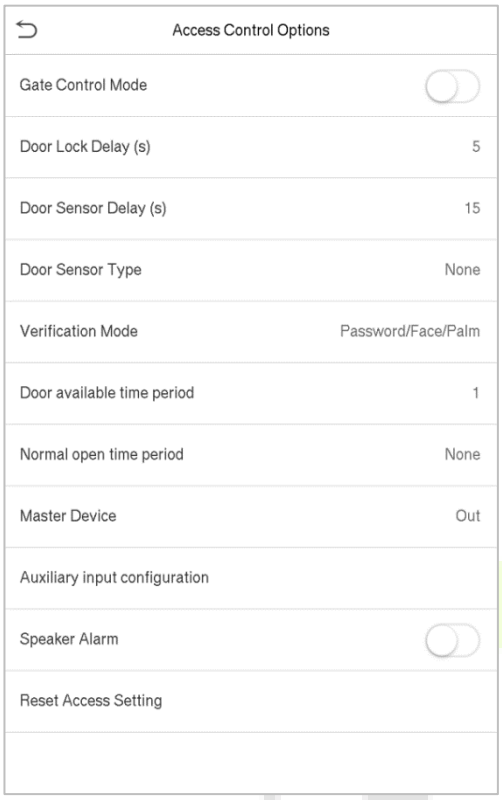
1. The current door unlock time should be within any valid time zone of the user time period.
2. The user's group must be in the door unlock combination (when there are other groups in the same access combo, verification of members of those groups are also required to unlock the door).

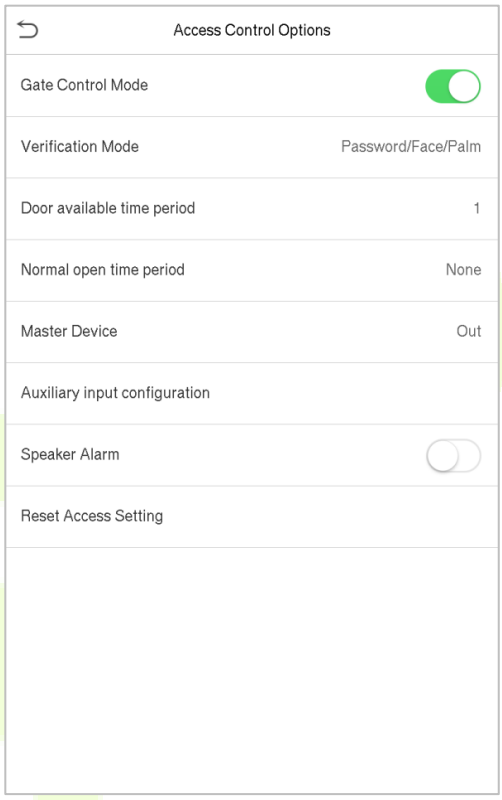
In default settings, new users are allocated into the first group with the default group time zone and access combo as "1" and set in unlocking state.

10.1 Access Control Options

To set the parameters of the control lock of the terminal and related devices.

Click **Access Control Options** on the Access Control interface.





Menu Name	Description
Gate Control Mode	Whether to turn on the gate control mode or not, when set to ON, this interface will remove Door lock relay, Door sensor relay and Door sensor type function.
Door Lock Delay (s)	The time duration that the device controls the electric lock to be unlocked. The valid range is 1 to 10 seconds; 0 second represents disabling the function.
Door Sensor Delay (s)	If the door is not closed and locked after opening 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 types: None, Normal Open, and Normal Closed. None means door sensor is not in use; Normal Open means the door is always opened when electricity is on; Normal Closed means the door is always closed when electricity is on.
Verification Mode	The supported verification mode includes Password/Face, User ID only, Password, Face only, and Face + Password.

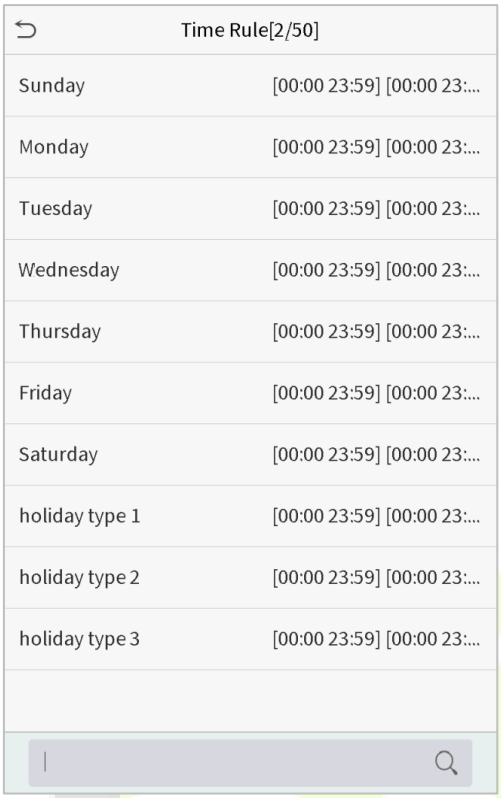
Door Available Time Period	To set time period for door, so that the door is accessible only during this time period.
Normal Open Time Period	Scheduled time period for "Normal Open" mode, so that the door is always unlocked during this period.
Master Device	When setting up the master and slave, the status of the master can be set to exit on enter. **Exit:** The record verified on the host is the exit record. **Enter:** The record verified on the host is the entry record.
Auxiliary Input Configuration	Set 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	To transmit a sound alarm or disable the alarm from the local. When the door is closed or the verification is successful, the system will cancel the alarm from the local.
Reset Access Setting	The restored access control 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, the erased access control data in Data Mgt. is excluded.

10.2 Time Rule setting

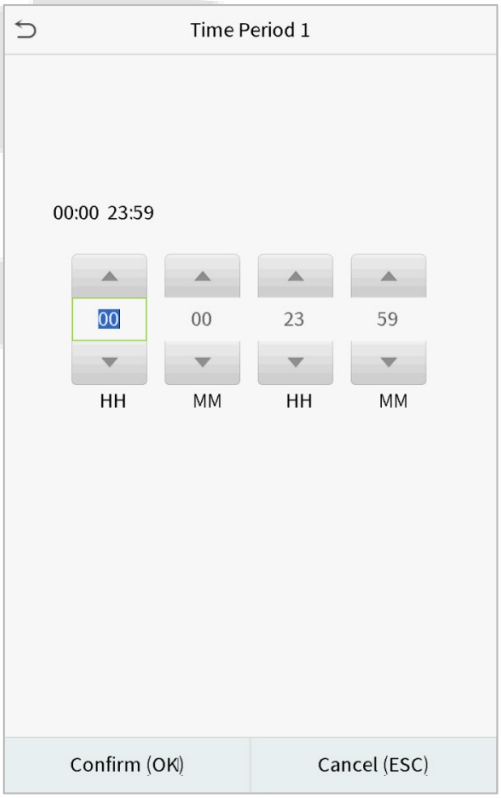
The entire system can define up to 50 time rules. Each time rule represents ten time zones, i.e. one week and 3 holidays, and each time zone is a valid time period within 24 hours per day. You may set a maximum of 3 time periods for every time zone. The relationship among these time periods is "or". When the verification time falls in any one of these time periods, the verification is valid. Each time period format of the time zone: HH MM-HH MM, which is accurate to minutes according to the 24-hour clock.

Click **Time Rule Setting** on the Access Control interface.

1. Click the grey box to input a time zone to search. Enter the number of time zone (maximum: 50 zones).



2. Click the date on which time zone settings is required. Enter the starting and ending time, and then press OK.



Note:

- When the ending time is earlier than the starting time, such as 23:57~23:56, it indicates that access is prohibited all day; when the ending time is later than the starting time, such as 00:00~23:59, it indicates that the interval is valid.
- The effective time period to unlock the door: open all day (00:00~23:59) or when the ending time is later than the starting time, such as 08:00~23:59.
- The default time zone 1 indicates that door is open all day long.

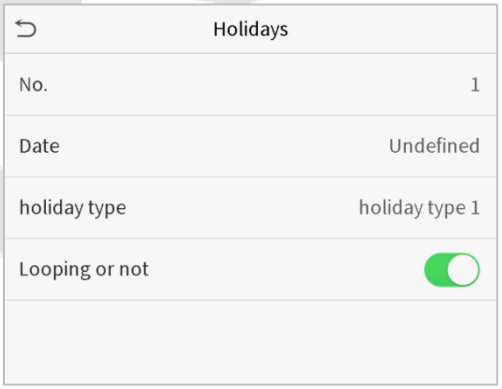
10.3 Holiday Settings

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

Click **Holidays** on the Access Control interface.

- **Add a New Holiday**

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



- **Edit a Holiday**

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

- **Delete a Holiday**

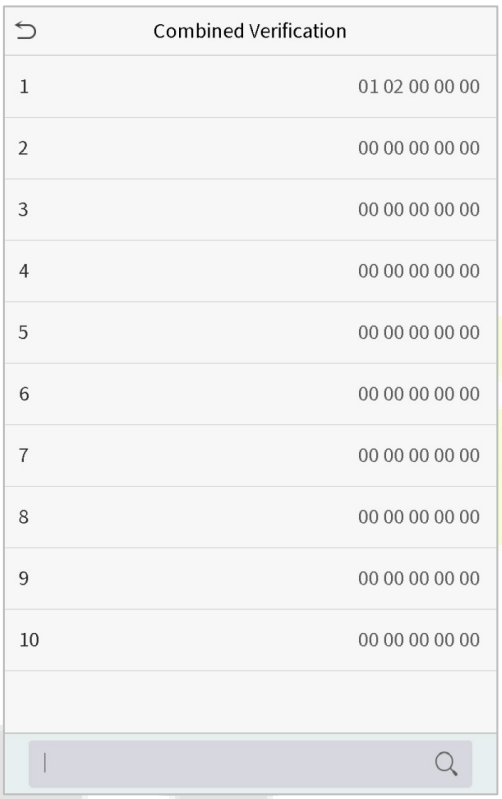
On the Holidays interface, select a holiday item to be deleted and click **Delete**. Click **OK** to confirm the deletion. After deletion, this holiday is no longer displayed on All Holidays interface.

10.4 Combined Verification Settings

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 $0 \leq N \leq 5$, and the number of members N may all belong to one access group or may belong to five different access groups.

Click **Combined Verification** on the Access Control interface.



Click the door-unlocking combination to be set. Click the up and down arrows to input the combination number, then press OK.

Examples:

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

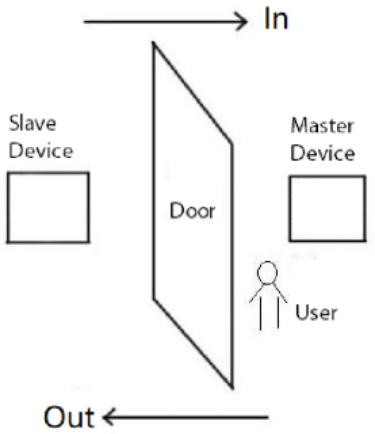
- **Delete a door-unlocking combination**

Set all the group numbers as 0 if you want to delete door-unlocking combinations.

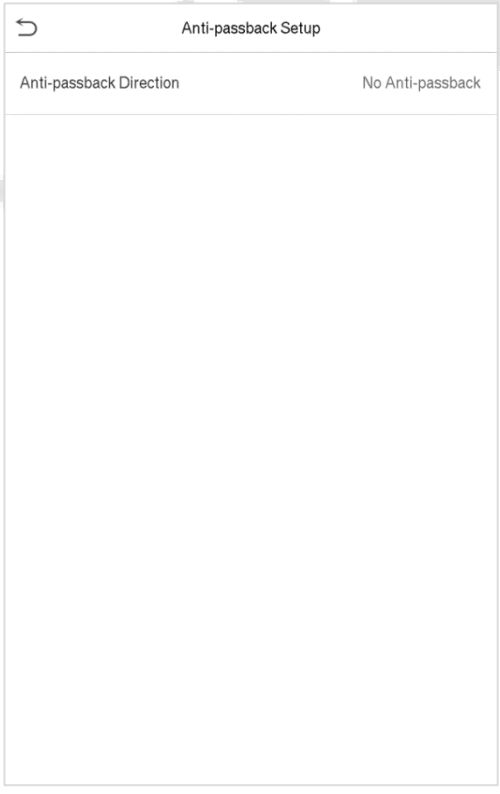
10.5 Anti-Passback Setup

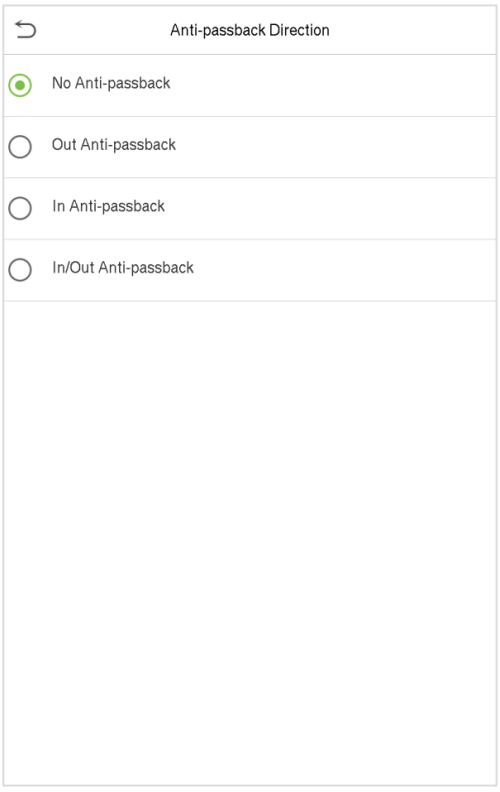
It is possible that users may be followed by some persons to enter the door without verification, resulting in security problem. So, to avoid this situation, Anti-Passback option is developed. Once it is enabled, the check-in record must match with check- out record so as to open the door.

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



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



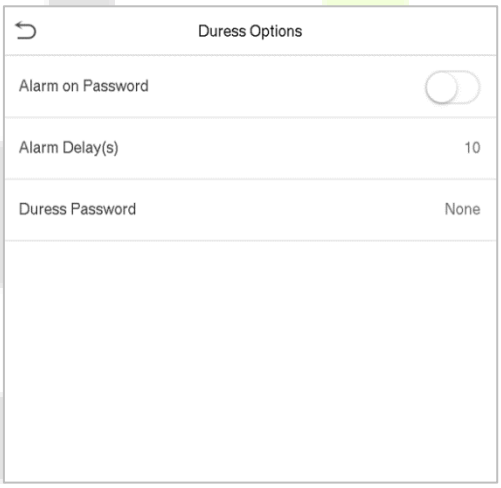


Menu Name	Description
Anti-passback Direction	**No Anti-passback:** Anti-passback function is disabled, which means successful verification through either master device or slave device can unlock the door. Attendance state is not saved. **Out Anti-passback:** After a user checks out, only if the last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

10.6 Duress Options Settings

If a user activated the duress verification function with specific authentication method(s), when he/she is in emergency during authentication with such method, the device will unlock the door as usual, but at the same time a signal will be sent to trigger the alarm.

Click **Duress Options** on the Access Control interface.

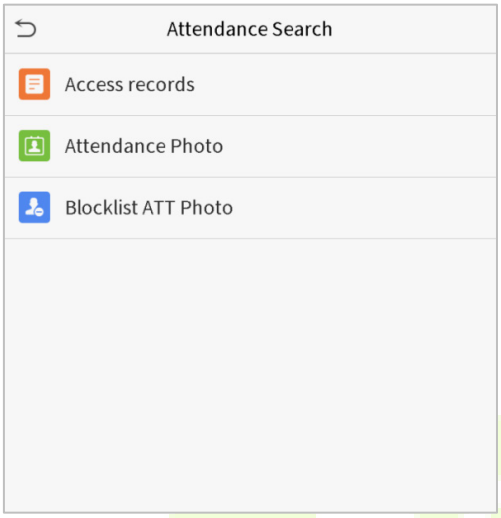


Menu Name	Description
Alarm on Password	When a user uses the password verification method, an alarm signal will be generated; otherwise there will be no alarm signal.
Alarm Delay (s)	Alarm signal will not be transmitted until the alarm delay time is elapsed. The value ranges from 1 to 999 seconds.
Duress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

11 Attendance Search

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

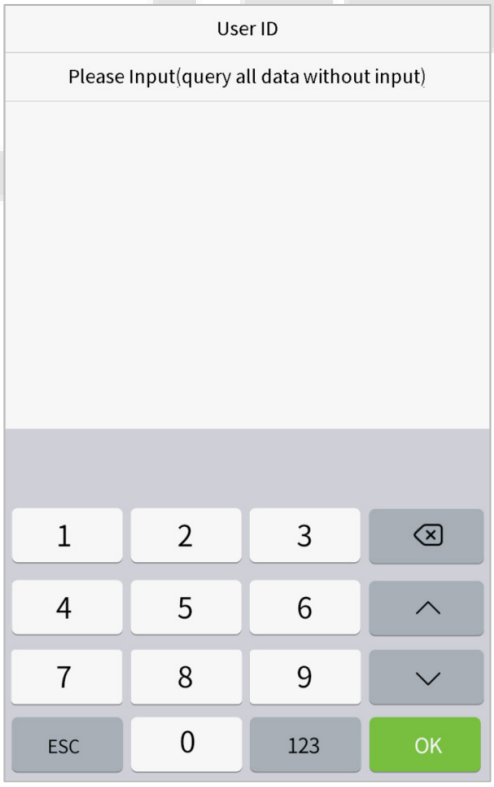
Click **Attendance Search** on the main menu interface.



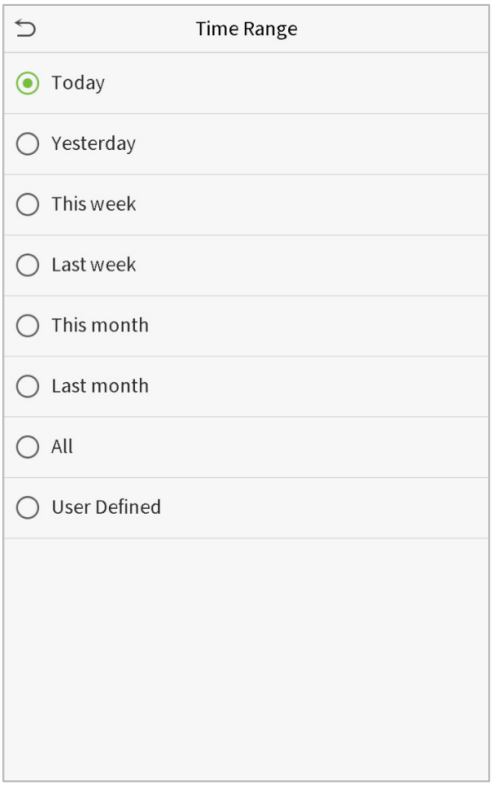
The process of searching for attendance and blocklist photos is similar to that of searching for access records. The following is an example of searching for access records.

On the Attendance Search interface, click **Access Records**.

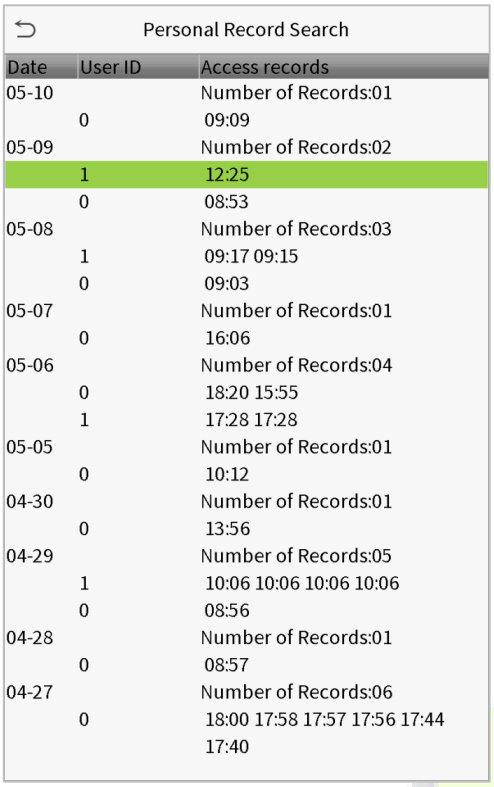
1. Enter the user ID to be searched and click OK. If you want to search for records of all users, click OK without entering any user ID.



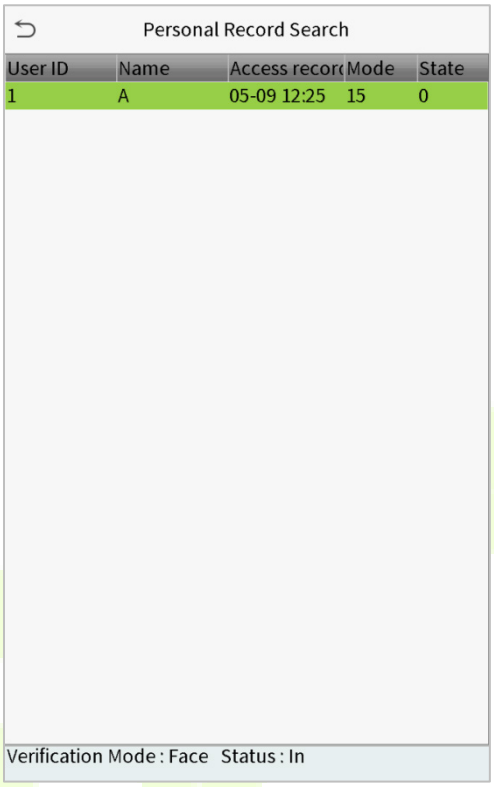
2. Select the time range in which the records you want to search for.



3. The record search succeeds. Click the record in green to view its details.



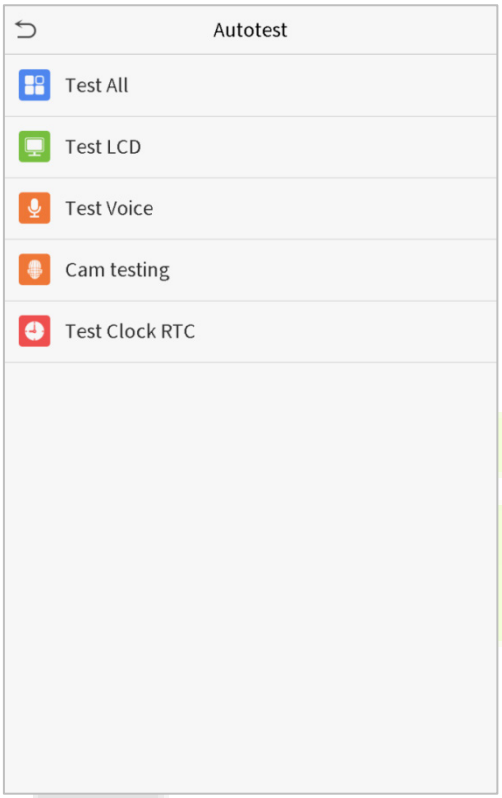
4. The below figure shows the details of the selected record.



12 Autotest

This function automatically tests whether all the modules in the device function properly, which include the LCD, audio, camera and real-time clock (RTC).

Click **Autotest** on the main menu interface.

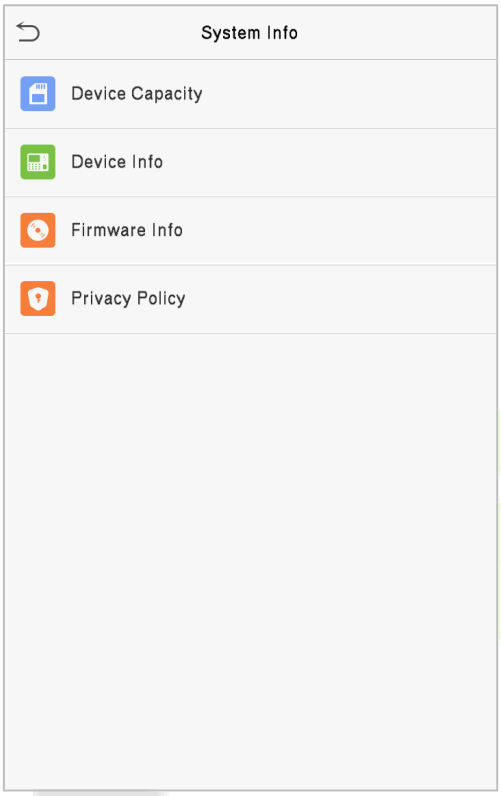


Menu Name	Description
Test All	To automatically test whether the LCD, audio, camera and RTC are normal.
Test LCD	To automatically test the display effect of LCD screen by displaying full-color, pure white, and pure black to check whether the screen displays the colors normally.
Test Voice	To automatically test whether the audio files stored in the device are complete and the voice quality is good.
Camera Testing	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.

13 System Information

With the system information option, you can view the storage status, the version information of the device, and so on.

Click **System Info** on the main menu interface.



Menu 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, Face algorithm version information, Platform information, and Manufacturer details.
Firmware Info	Displays the firmware version and other version information of the device.
Privacy Policy	The privacy policy control will appear when the gadget turns on for the first time. After clicking "**I have read it**," the customer can use the product regularly. Click **System Info** -> **Privacy Policy** to view the content of the privacy policy. The privacy policy's content does not allow for U disc export. **Note:** The current privacy policy's text is only available in Simplified Chinese/English. However, translation of other multi-language content is underway, with more iterations.

14 Connecting to ZKBioSecurity MTD Software★

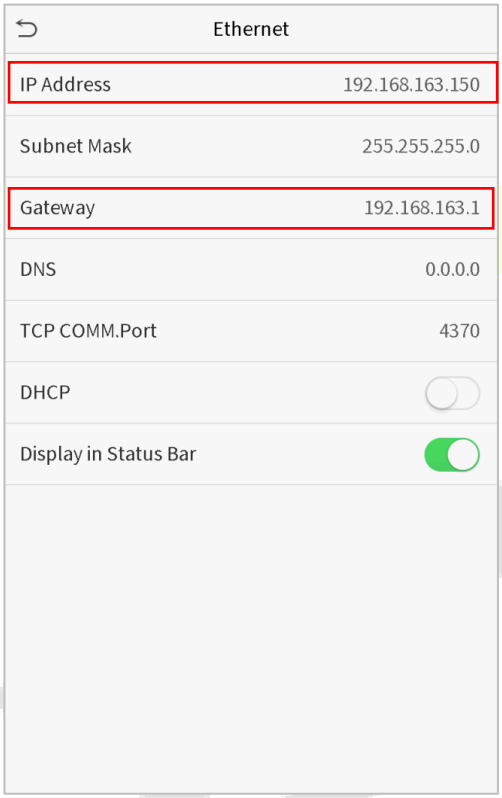
14.1 Set the Communication Address

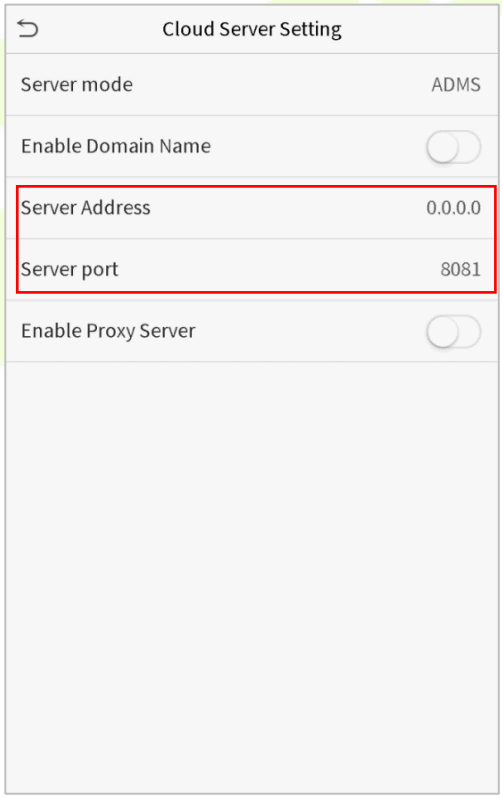
- **Device Side**

1. Click **COMM.** > **Ethernet** in the main menu to set IP address and gateway of the device. (**Note:** The IP address should be able to communicate with the ZKBioSecurity MTD server, preferably in the same network segment with the server address).
2. In the main menu, click **COMM.** > **Cloud Server Setting** to set the server address and server port.

   Server address: Set as the IP address of ZKBioSecurity MTD server.

   Server port: Set as the service port of ZKBioSecurity MTD (The default is 8088).





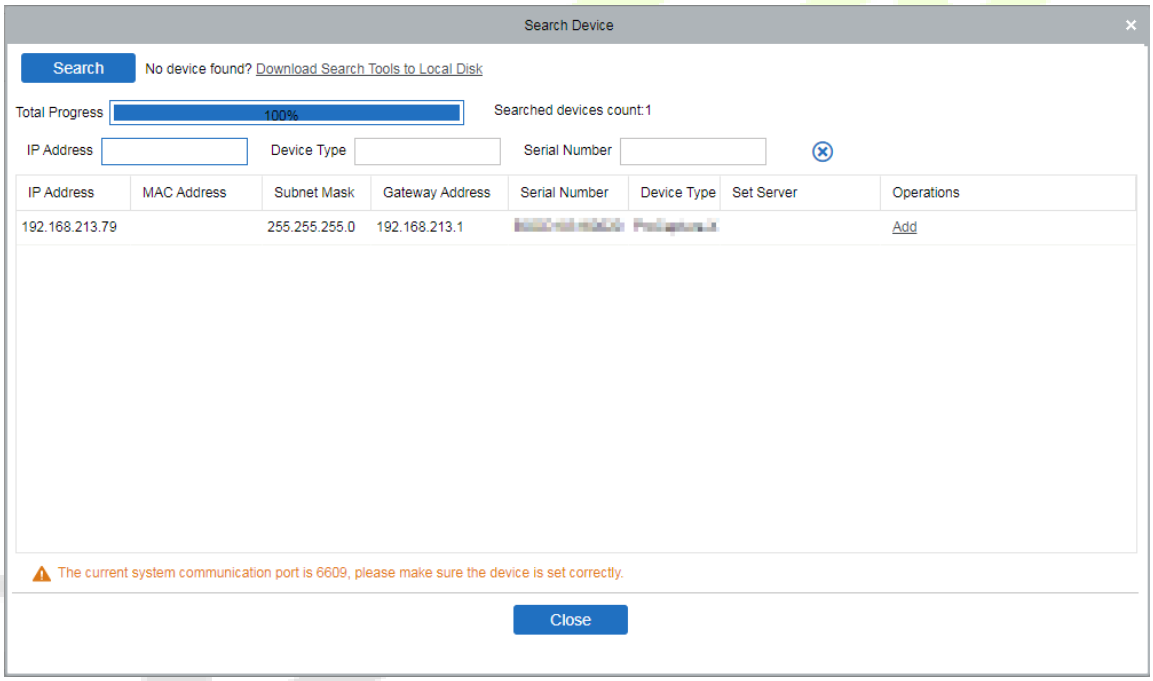
- **Software Side**

Login to ZKBioSecurity MTD software, click **System** > **Communication** > **Communication Device** to set the ADMS service port, as shown in the figure below:

14.2 Add Device on the Software

You can add a device by searching. The process is as follows:

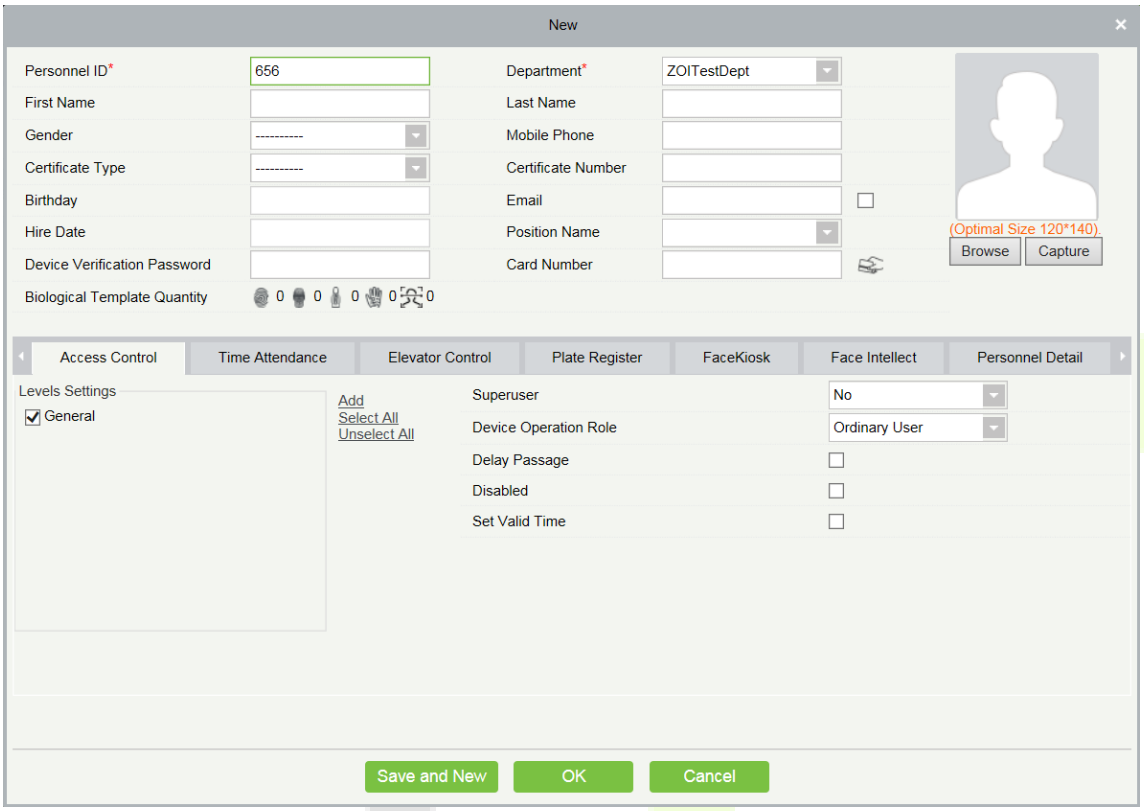
1. Click **Access Control** > **Device** > **Search Device**, to open the Search interface.
2. Click **Search**, and it will prompt "**Searching**……."
3. After searching, the list and total number of access controllers will be displayed.



4. Click **Add** after the device to complete adding.

14.3 Add Personnel on the Software

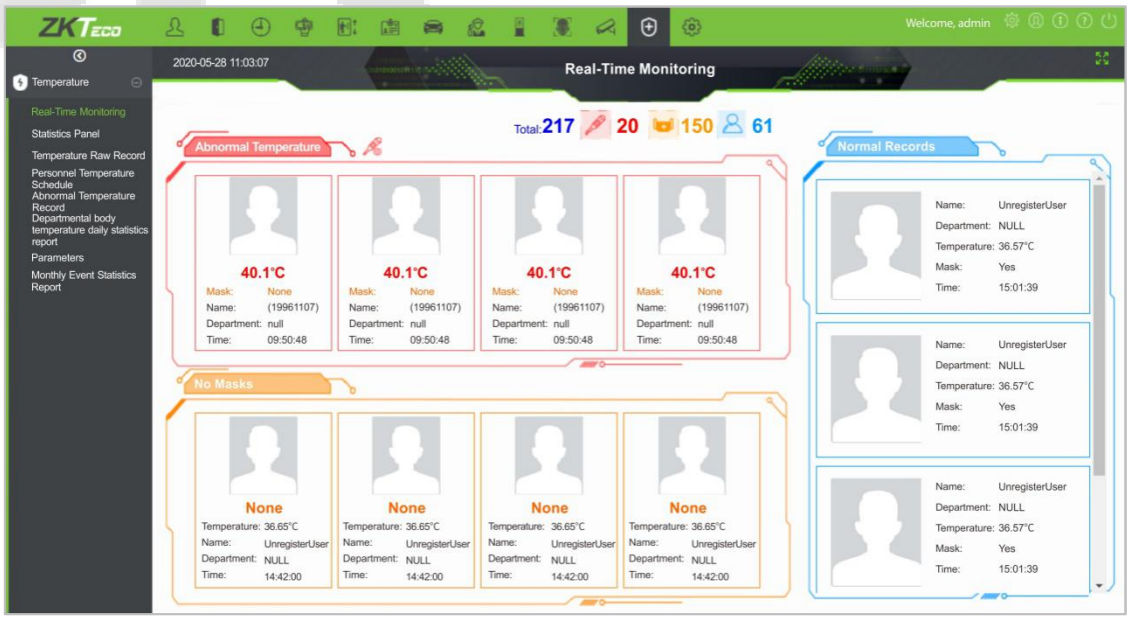
1. Click **Personnel** > **Person** > **New**.



2. After setting all the parameters, click **OK**.

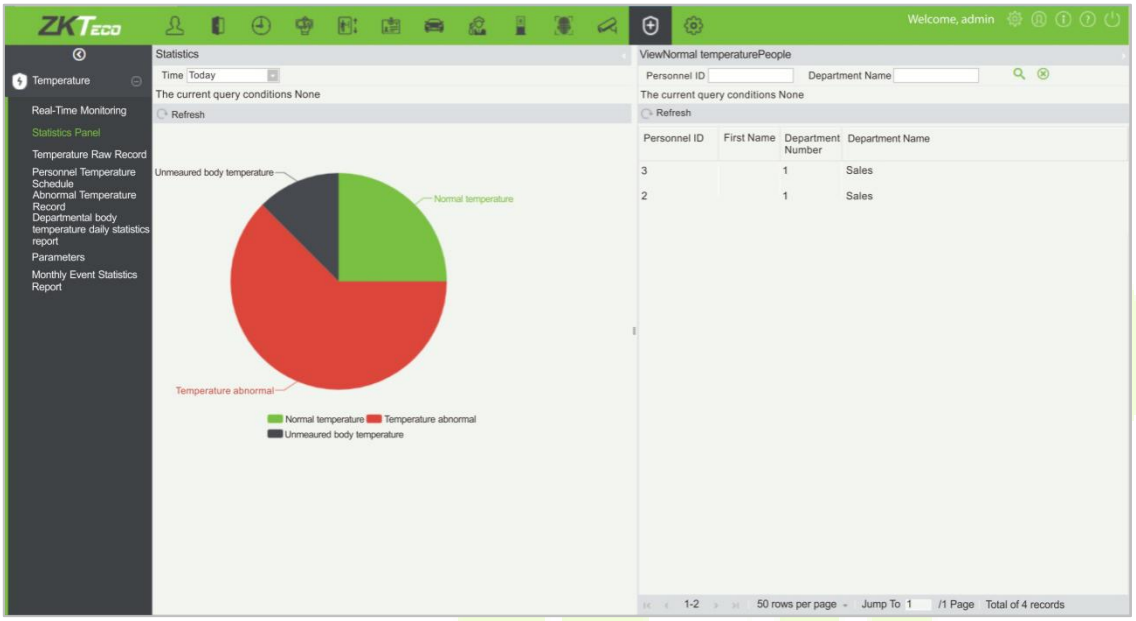
14.4 Real-time monitoring on the Software

1. Click **Prevention** > **Epidemic** > **Real-time monitoring** to view all the events include the user whose temperature is over the range:



When the **Alarm temperature setting** has set, the abnormal body temperature will be marked red automatically.

2. Click **Epidemic > Statistics panel** to view the analysis of statistical data and view the personnels with normal temperature.



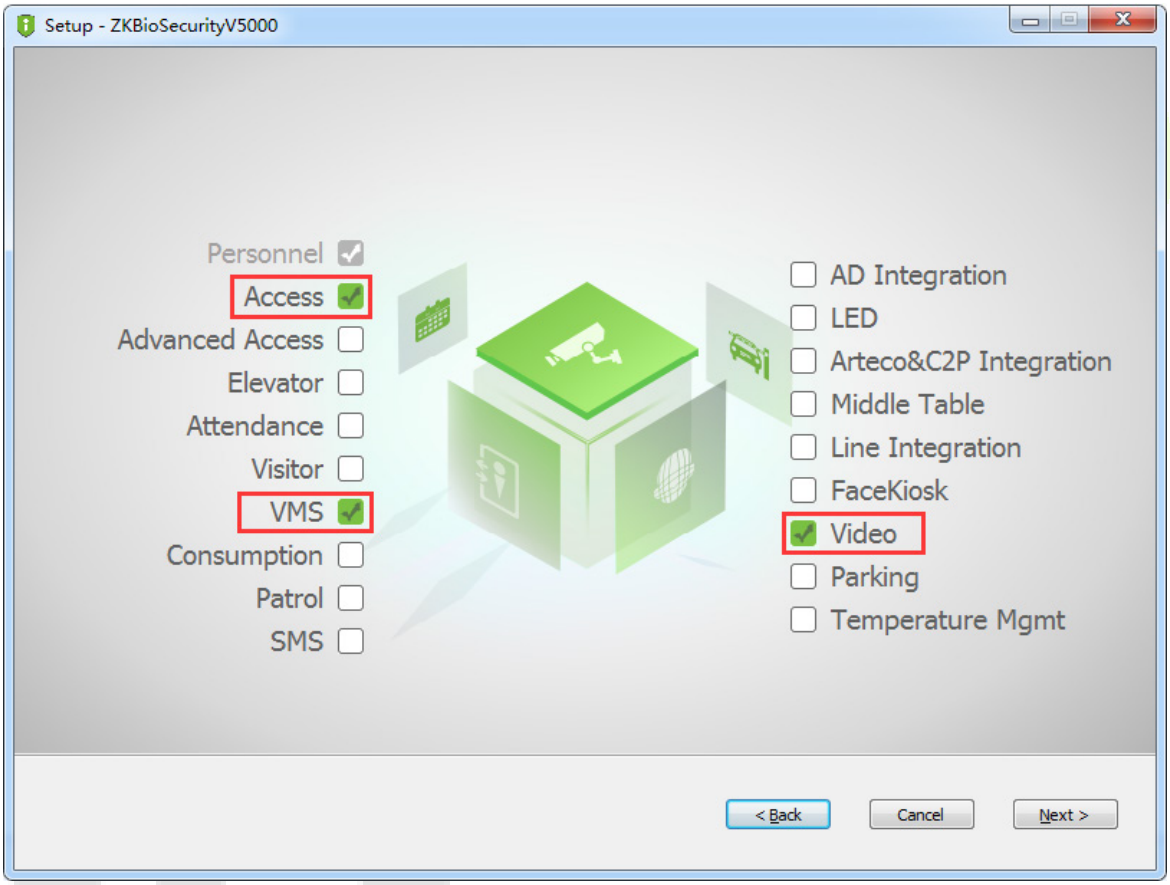
Note: For other specific operations, please refer ZKBioSecurity MTD User Manual.

15 LAN Video Intercom Function Settings★

15.1 Installing ZKBio VMS Plugin in the ZKBioSecurity Software

- **Install the ZKBioSecurity Software**

While installing, select the "VMS" module of the ZKBioSecurity software to install, as shown in the following installation interface.



Note: The Video module and the VMS module cannot be selected at the same time.

- **Installing the ZKBio VMS Plugin**

Double-click on the provided **ZKBioVMSPlugin_sqlite.exe** file to install the ZKBio VMS Plugin.

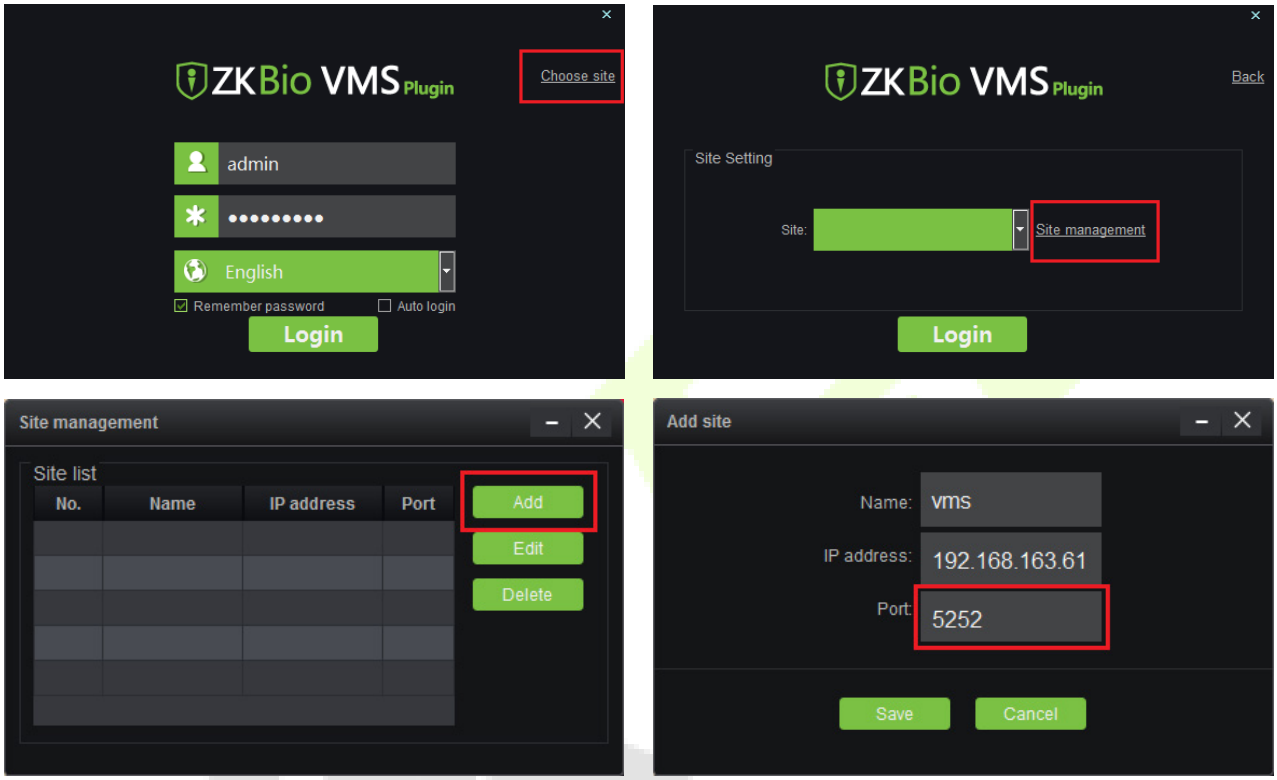
Note: The ZKBioSecurity software and ZKBio VMS Plugin need to be opened simultaneously to recognize the intercom function.

15.2 Configuration Parameters

Set the required parameters correctly to ensure a connection between the device and the software.

1. **Add site on the Video-VMS plugin**

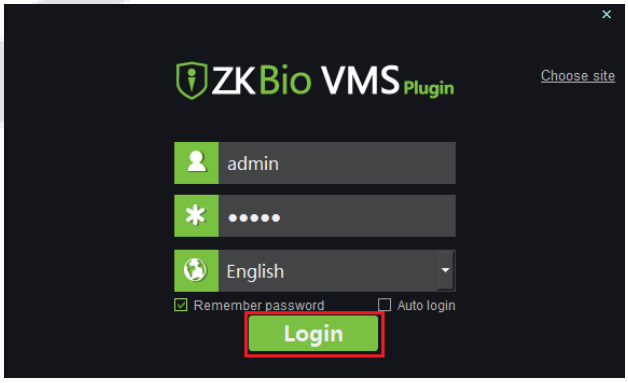
a. Double click the icon to open the Video-VMS Plugin. Click ***Choose site** > **Site management** > **Add** on the login interface. Then, enter the Name, IP address, and Port to add a site, as shown in the following figure.



IP address: Enter the local IP address.

Port: The default port is **5252**.

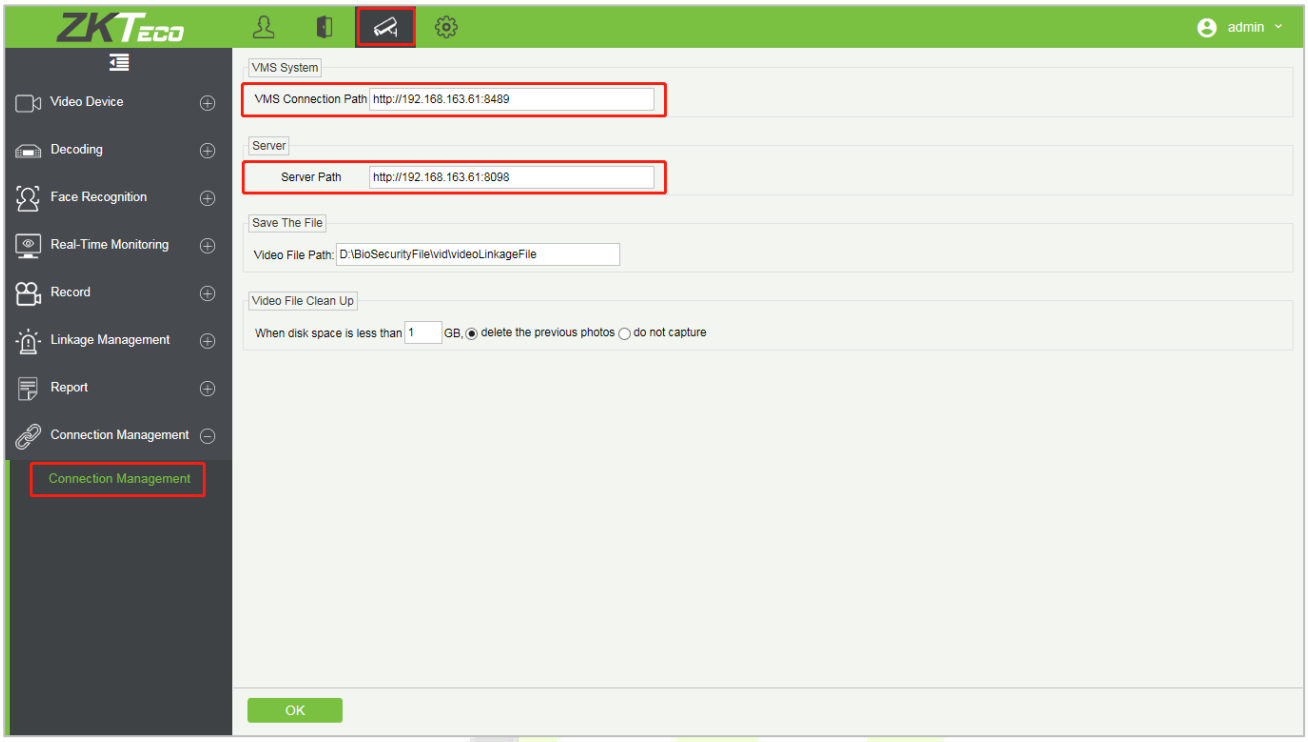
b. Enter the username and the password after adding the site and click **Login** to login the Video-VMS plugin. The username and the initial password are both **admin**.



Note: When the Video-VMS plugin is connected successfully to the ZKBioSecurity, the password changes synchronously to the admin user password of the ZKBioSecurity.

2. Configure the connection path of the ZKBioSecurity and VMS plugin

Click **Video** > **Connection** > **Connection Management** on the ZKBioSecurity software to change the path, as shown in the following image:



VMS Connection Path

- **URL:** "http://local IP address: port"
- **Port:** It is **8489** by default (e.g., http://192.168.163.61:8489).

Server Path

- **URL:** "http://server IP address: port"
- **Port:** The port is the service port set during installation (e.g., http://192.168.163.61:8098) (not the ADMS port).

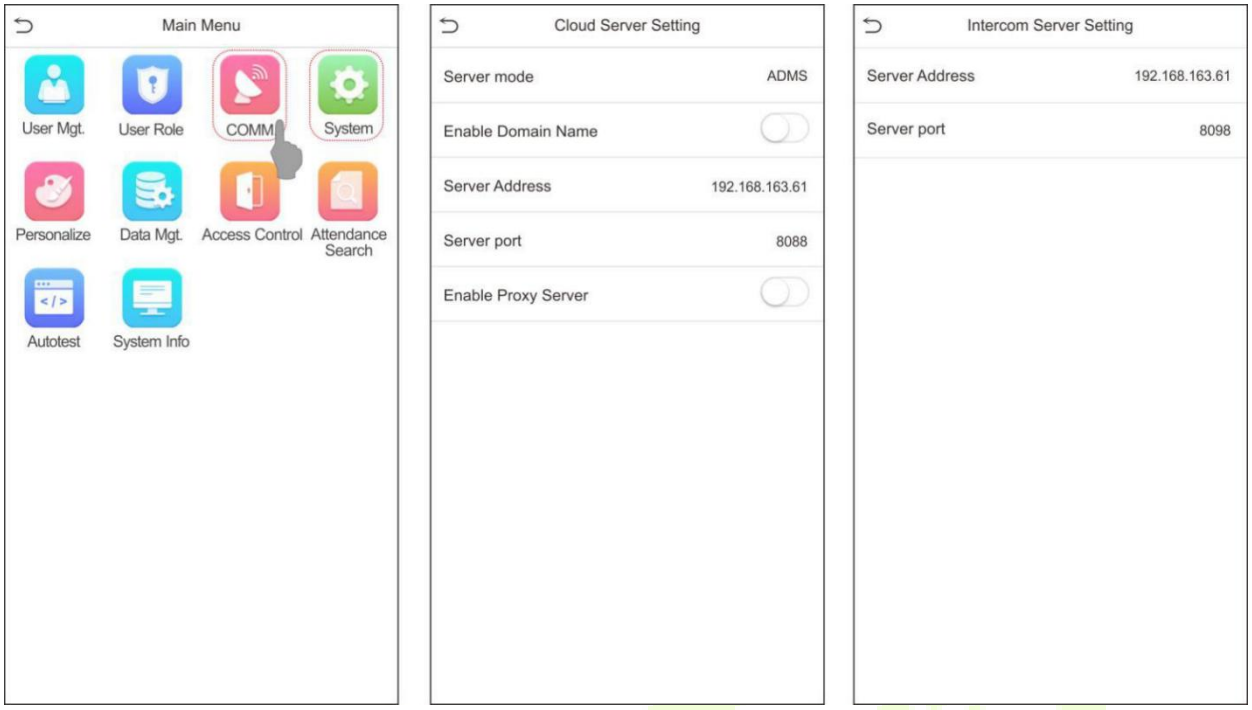
3. Configure the parameters on the device

a. Click on ☰ > **COMM.** > **Cloud Server Setting** on device to set the server address and server port, i.e., the IP address and port number of the server after the software is installed. If the device communicates with the server successfully, the icon is displayed in the upper right corner of the standby interface.

b. Click on ☰ > **System** > **Video Intercom Parameters** > **Intercom Server Setting** to set the server address and server port.

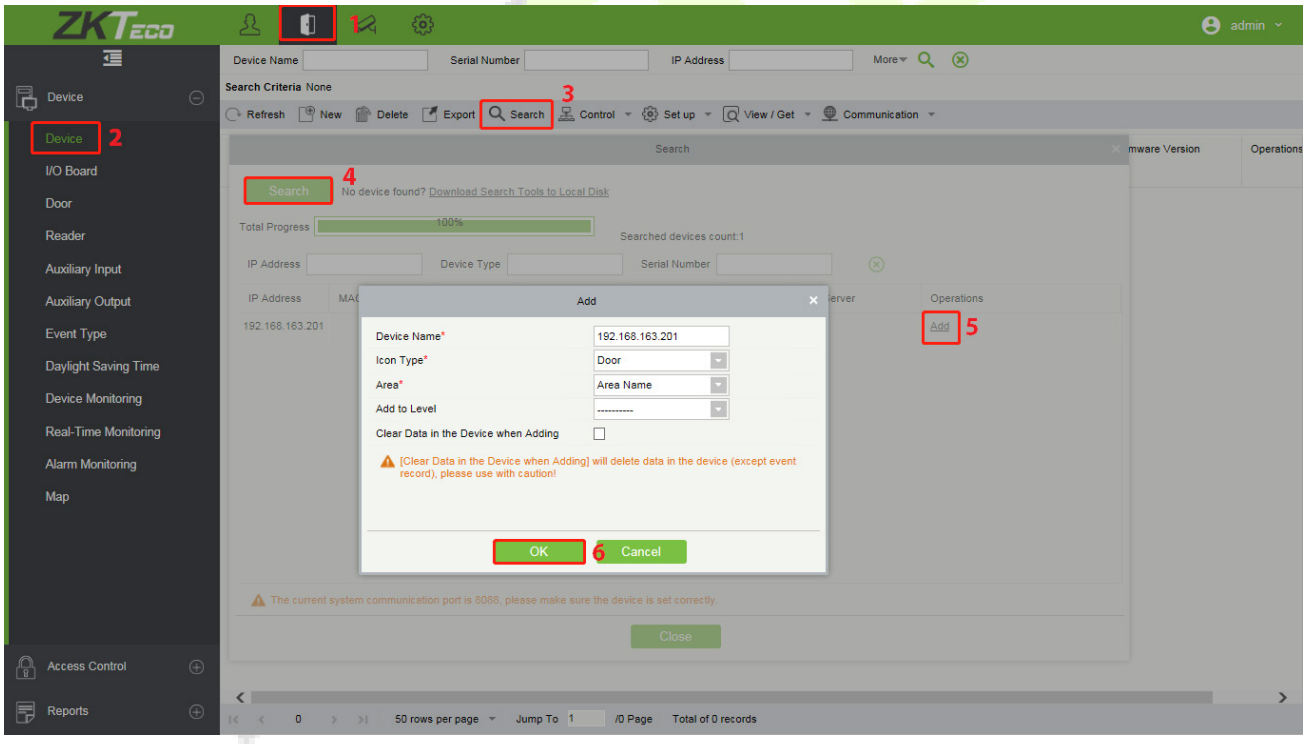
Server Address: Enter the ZKBioSecurity installation IP address.

Server Port: The port is the service port set during installation (not the ADMS port).

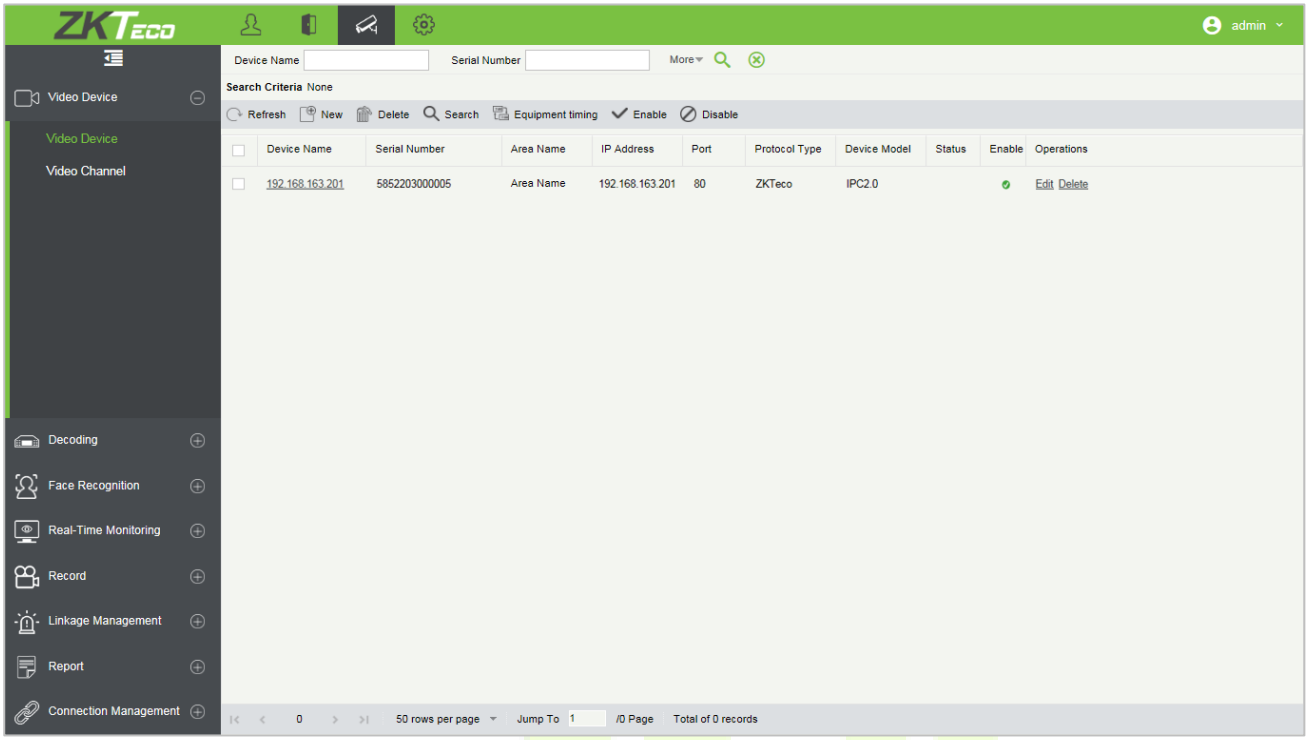


4. Adding device on the ZKBioSecurity software

a. Click **Access** > **Device** > **Device** > **Search** to add the device on the ZKBioSecurity software.



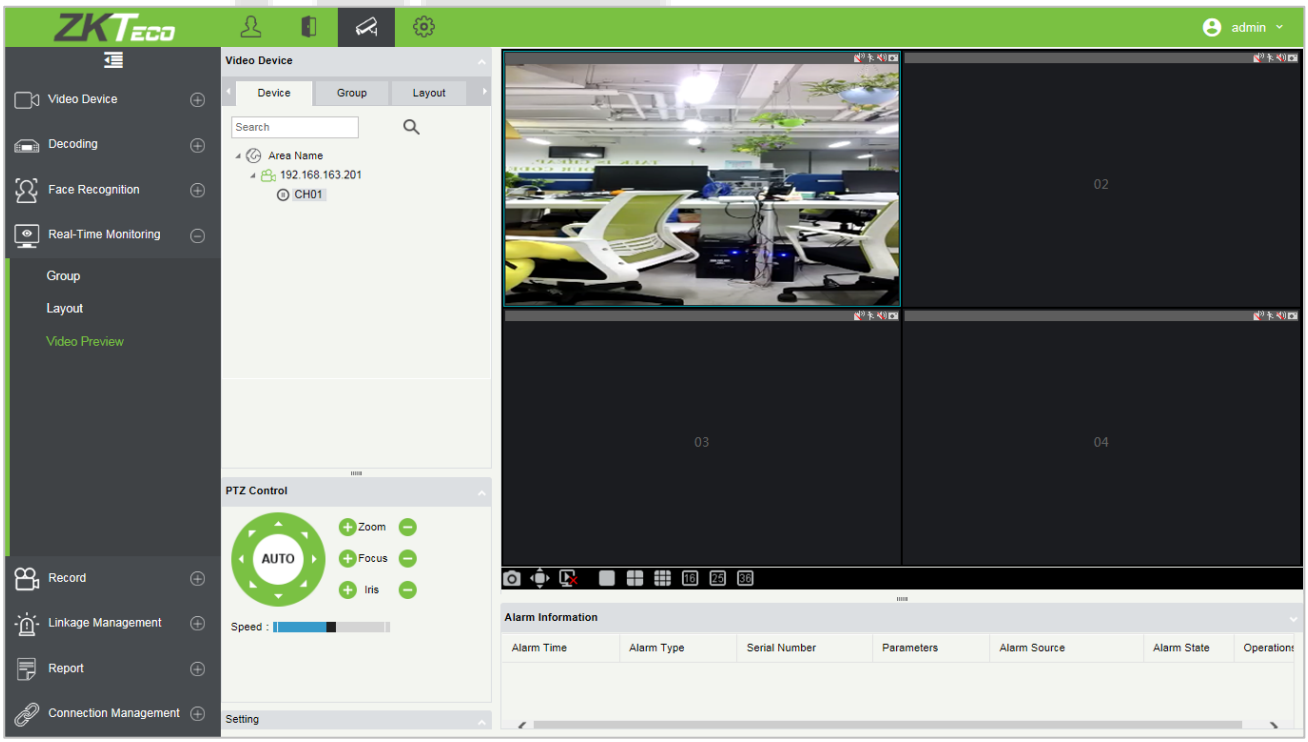
b. After the device is added successfully to the access module, it automatically adds to the video module. User can click **Video** > **Video Device** > **Search** to view.



Note: If the device is not added to the Video module, please check whether the parameter settings are correct.

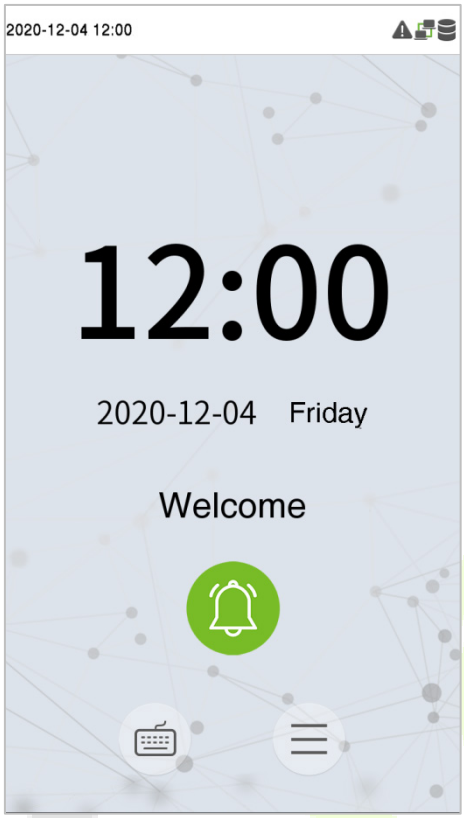
15.3 Video Preview on the ZKBioSecurity Software

Click **Video** > **Real-Time Monitoring** > **Video Preview** to enter the preview interface of the device.

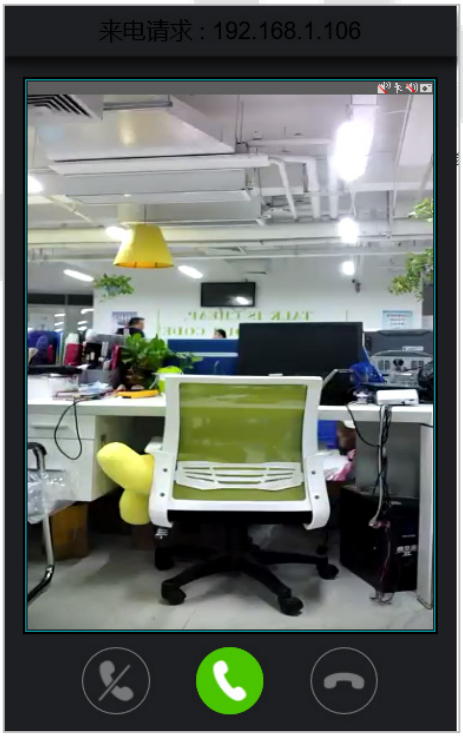


15.4 Make a Call on the Device

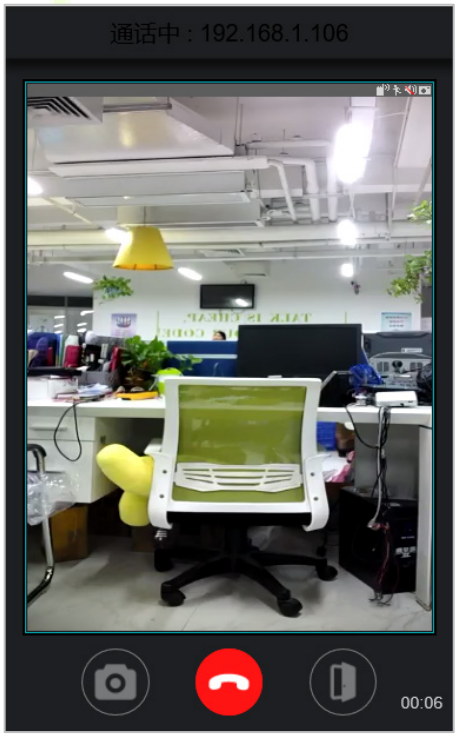
1. Click on icon on the welcome screen of the device to make a call.



2. The server page pops up the call window by default, as shown in the following figure.

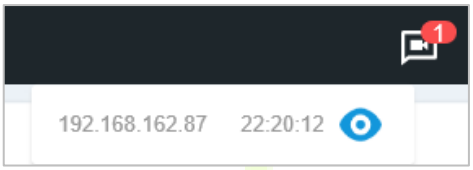


Call Interface



In-call Interface

Function Description

	It is the Answer key, the user can click to answer the current call. After answering, enter the window during the call, and turn on audio and video by default.
	It is the Hang up key. After hanging up, immediately end the current call.
	It is the Ignore key, used to ignore the current call. Click it to close the call window, and the icon  in the upper right corner will display the number of pending calls, like this  The user can click the  icon in the drop-down menu to open the call window of the current device again and choose to answer, as shown following figure. 
	It is the Hang up key, used to hang up the current call.
	It is the Snapshot key, used to take a snapshot.
	It is the Remote Open key, used to open the door remotely. The default lock drive time is 5 seconds.

Note: If the device preview interface is opened on the ZKBioSecurity software, the call interface will no longer be displayed in this call window.

16 Connecting to ZKBio Talk Software★

Download and install the ZKBio Talk software. Then, keep the parameter settings of ZKBioSecurity software unchanged for the relevant settings.

Following are the steps to connect ZKBio Talk to the ZKBioSecurity software:

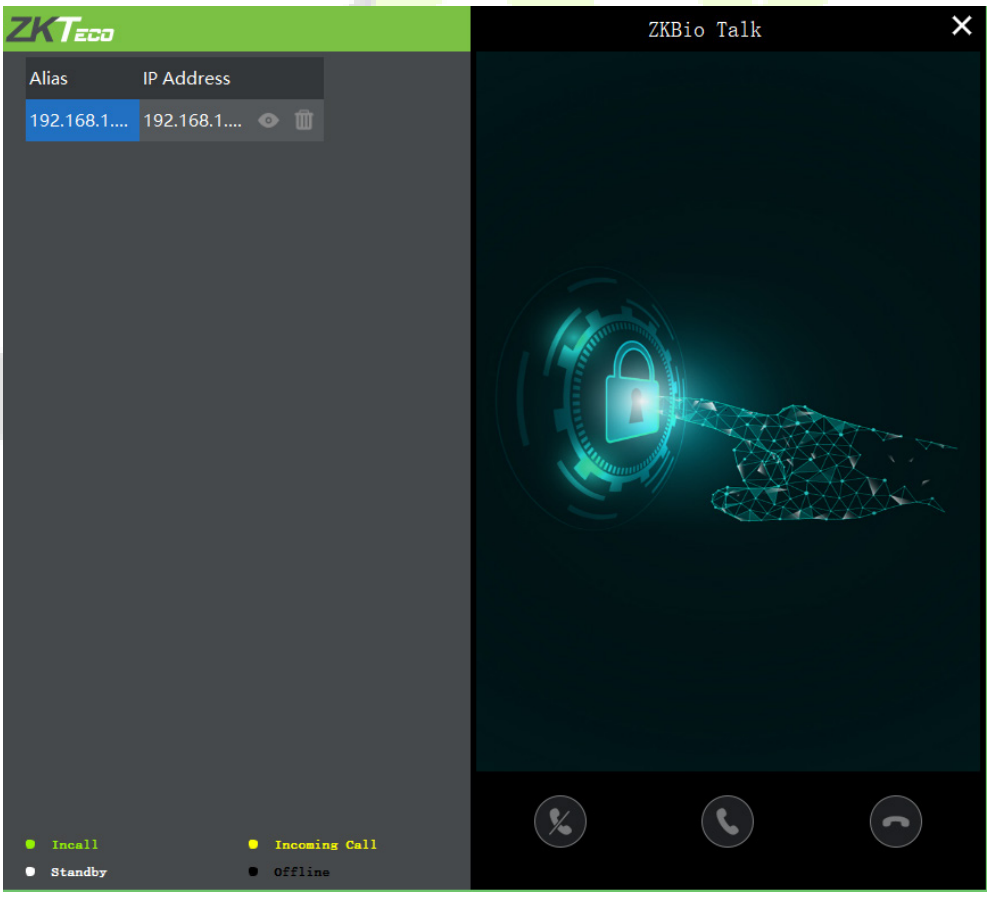
1. Firstly, change the parameter on the device:

   Tap on ☰ > **System** > **Video intercom parameters** > **Intercom Server Setting** on the device to change the server address and server port, as shown in the following figure.

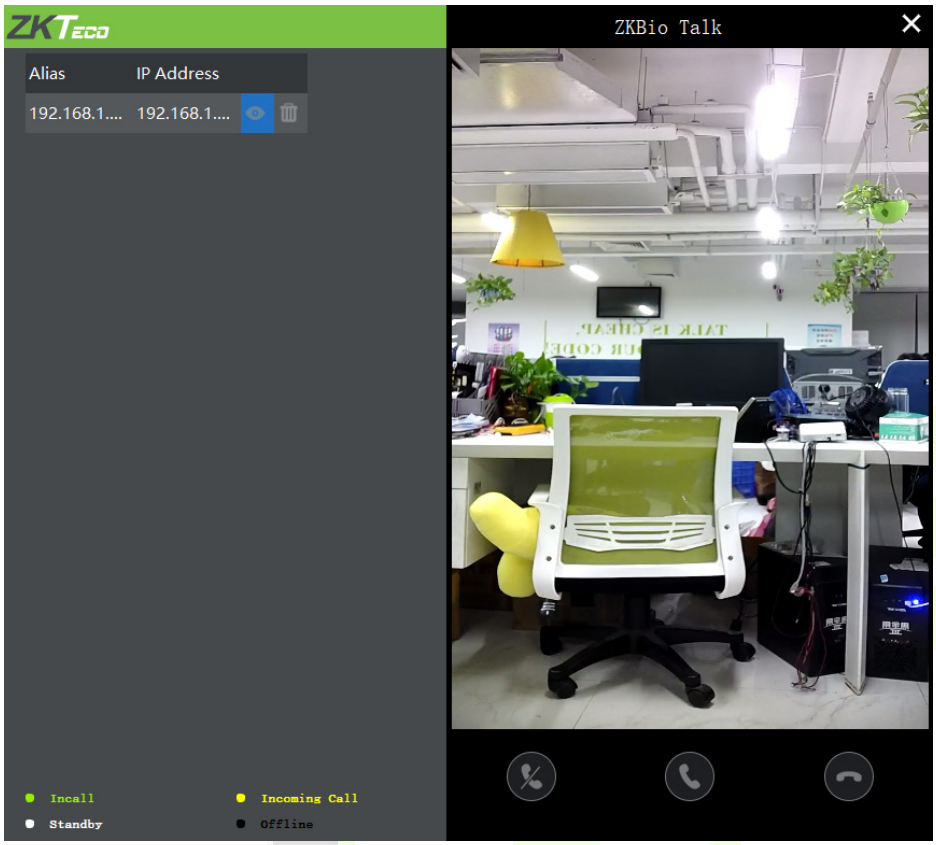
   Server Address: Enter the current server installation IP address.

   Server Port: The default server port is **25550**.

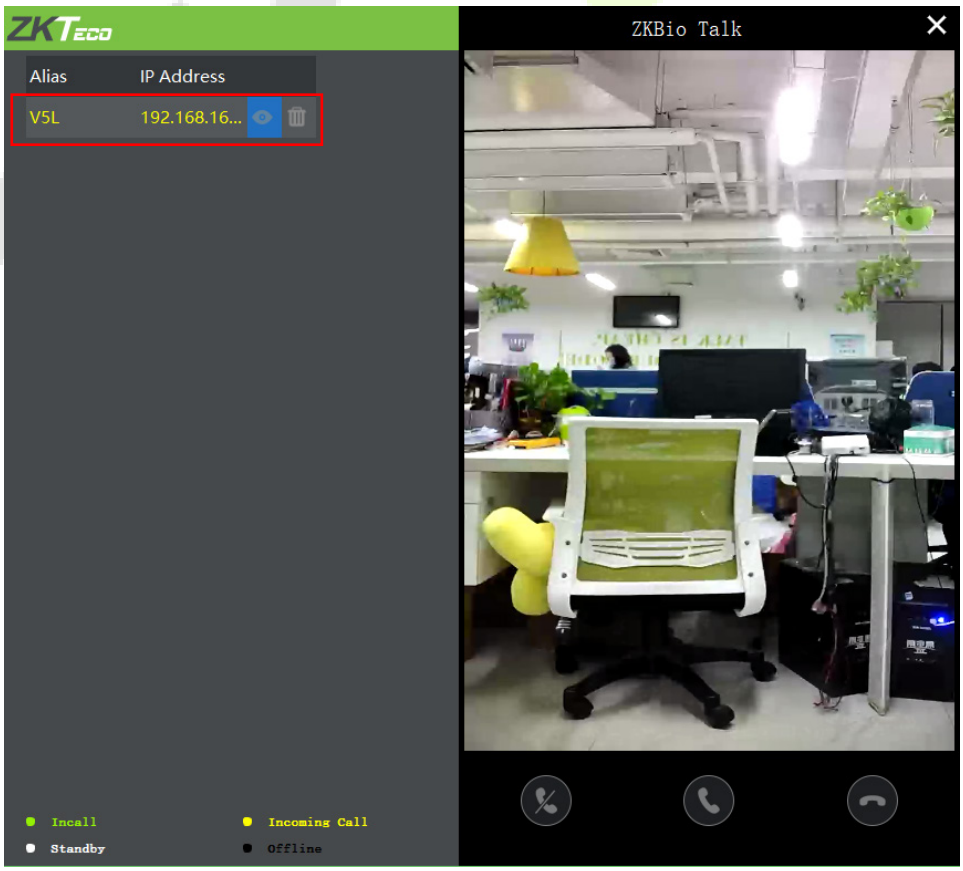
2. Double click the icon to open the ZKBio Talk software. When the device-side video intercom parameters are set correctly, the device automatically pushes the device list on the left, as shown in following figure.



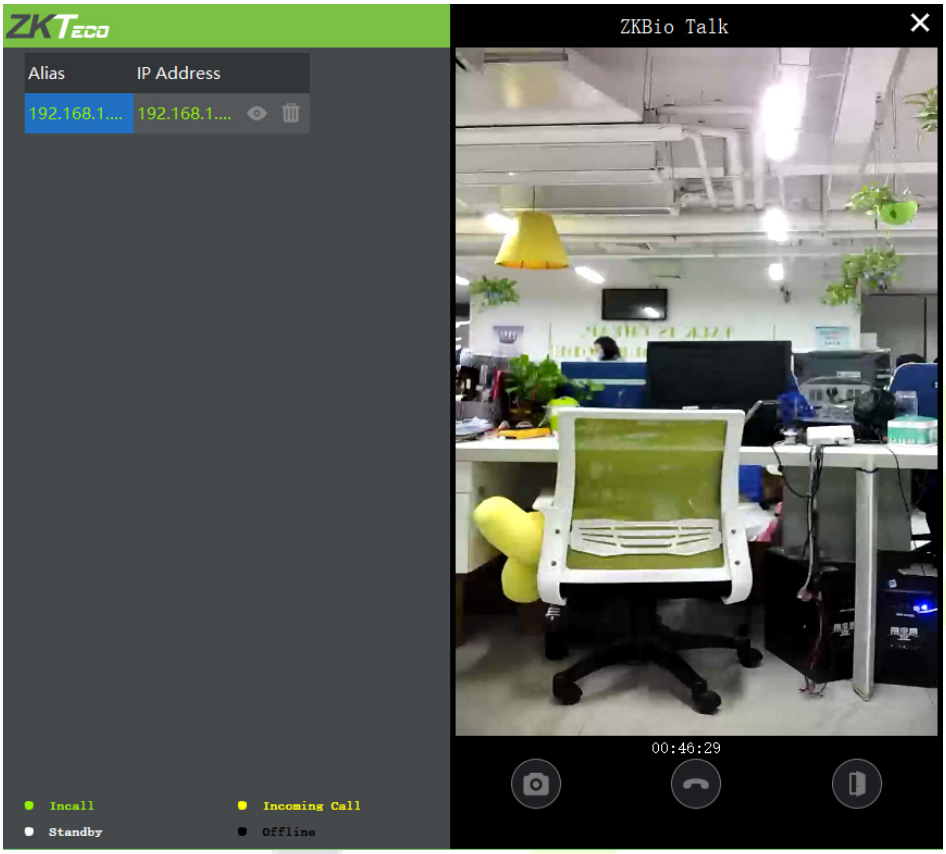
3. A user can click on to preview the video on the right. On clicking or icon, a user can close the preview screen. No action is taken when is clicked.



4. When a user clicks icon on the main interface of the device to make a call, the software interface displays the IP address of the calling device in yellow.



5. When the user clicks the  icon to answer the call, the IP address is displayed in green while on the call. The call duration is also displayed just above the icon.



Function Description:

	This is the Snapshot key, used to take a snapshot
	This is the Remote open key, used to open the door remotely. The default lock drive time is 5 seconds

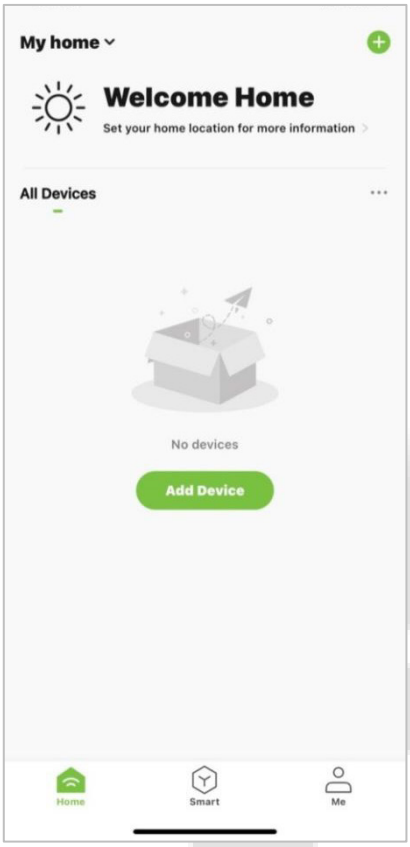
Note: Only the offline devices can be removed.

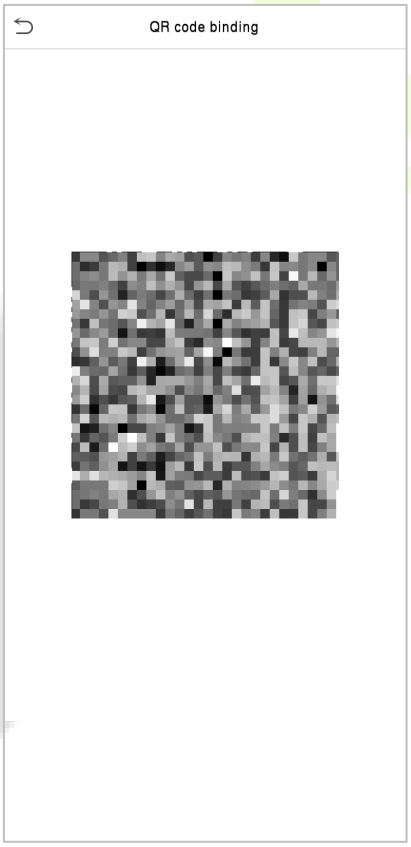
17 Connecting to ZSmart APP★

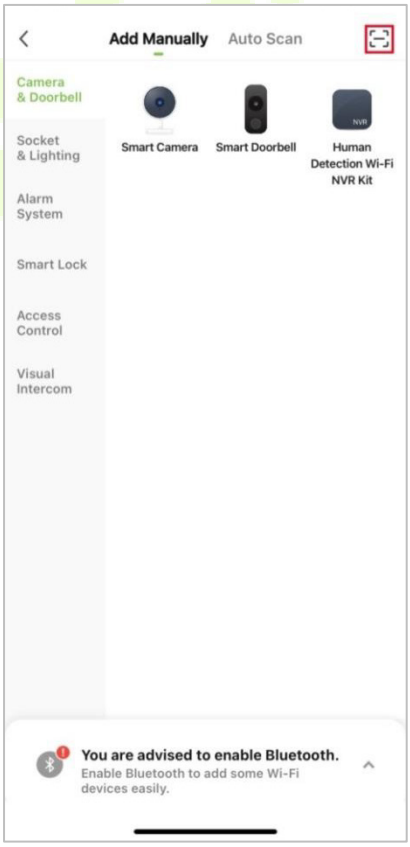
17.1 Adding Device on the ZSmart APP

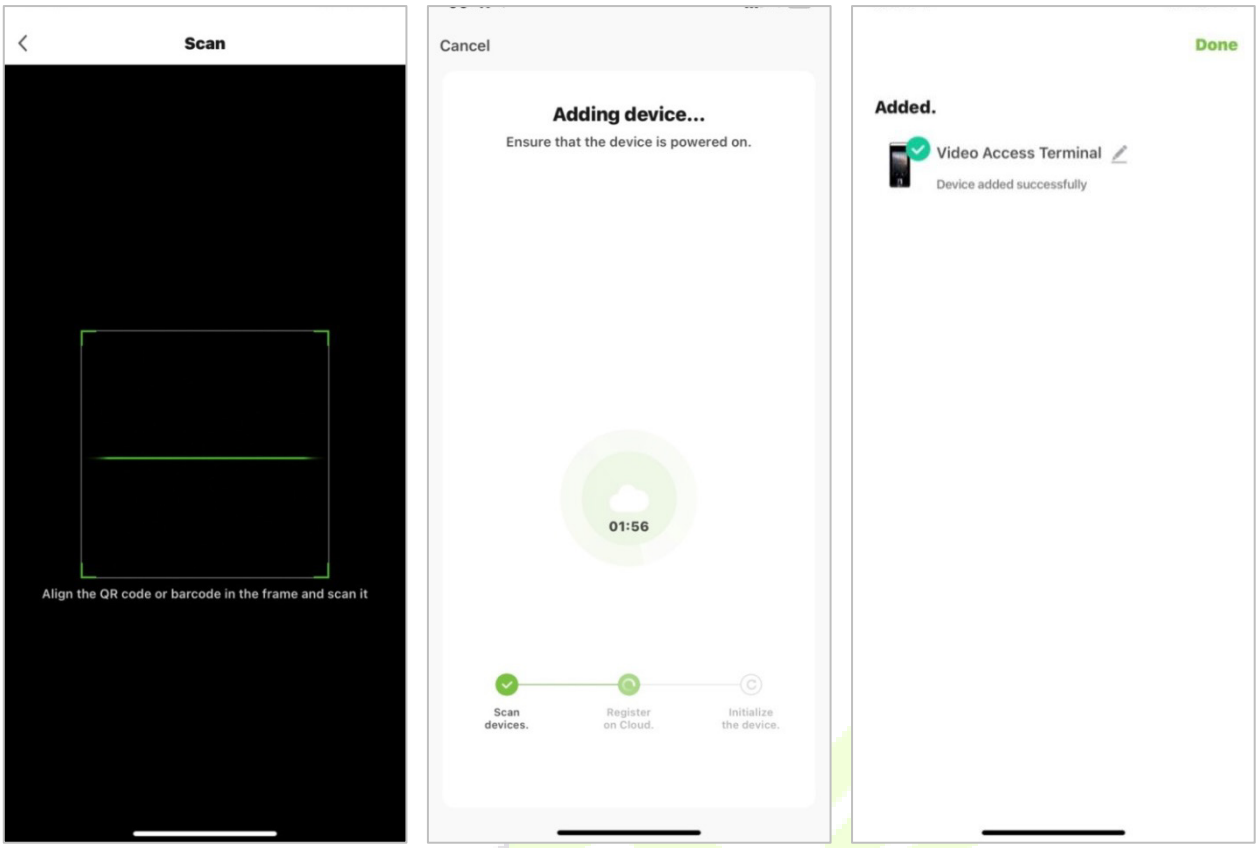
After downloading and installing the ZSmart APP on your phone, create a User account initially with your Email ID. After creating the User account, log in to the App, and click Add Device or + icon on the top right corner of the screen to add a device. The process is as follows:

1. Click **Add Device** on the Home page.
2. Tap on **System** > **Video Intercom Parameters** > **QR Code Binding** to show the QR code of the device.
3. Click the icon in the upper right corner.



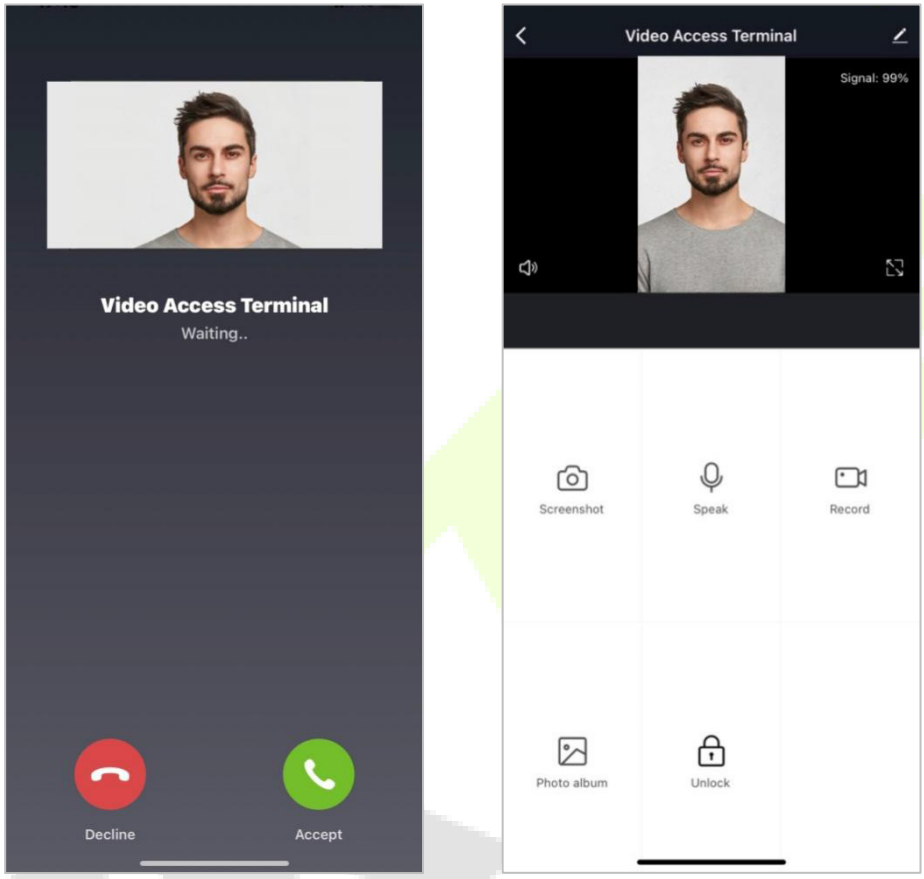






17.2 Video Phone Connection

Visitors press the button on the device to make a call and the phone will ring. The user can accept or decline the call. After the user accepts the call, it will open the video door phone interface. Enter the password to unlock the door.



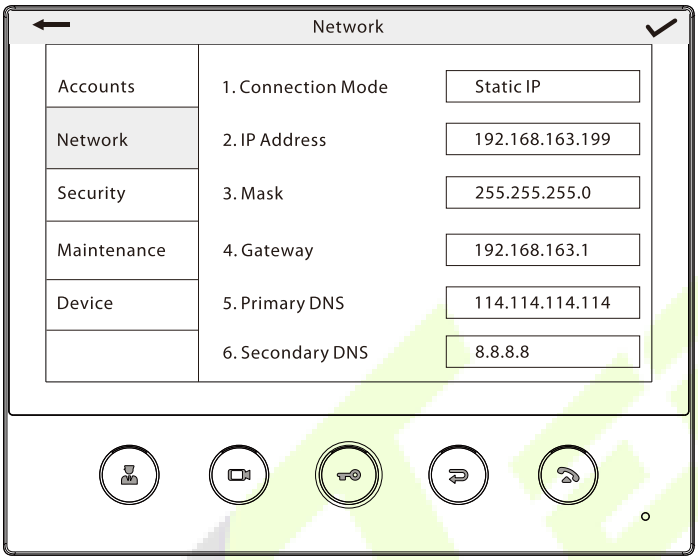
Parameter	Description
Screenshot	Click to take a screenshot.
Speak	The icon becomes blue when click it, and you can talk to the device at this time.
Record	Click to make a record video.
Photo album	View and delete screenshots and recorded videos.
Unlock	Click to open the door remotely. The unlocking record is saved in **Me** > **Message Center**.

Note: For other specific operations, please refer to the *ZSmartAPP User Manual*.

18 Connecting to SIP★

18.1 Local Area Network Use

Set the IP address on the indoor station, Tap **[Menu]** > **[Advanced]** > **[Network]** > **[1. Network]** > **[1. IPv4]**.



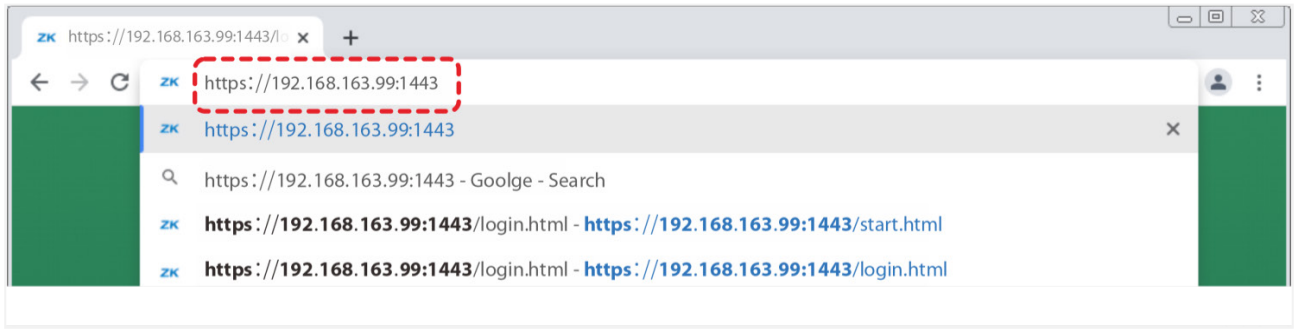
Note: In LAN, the IP addresses of the indoor station and the ProFace X must be in the same network segment.

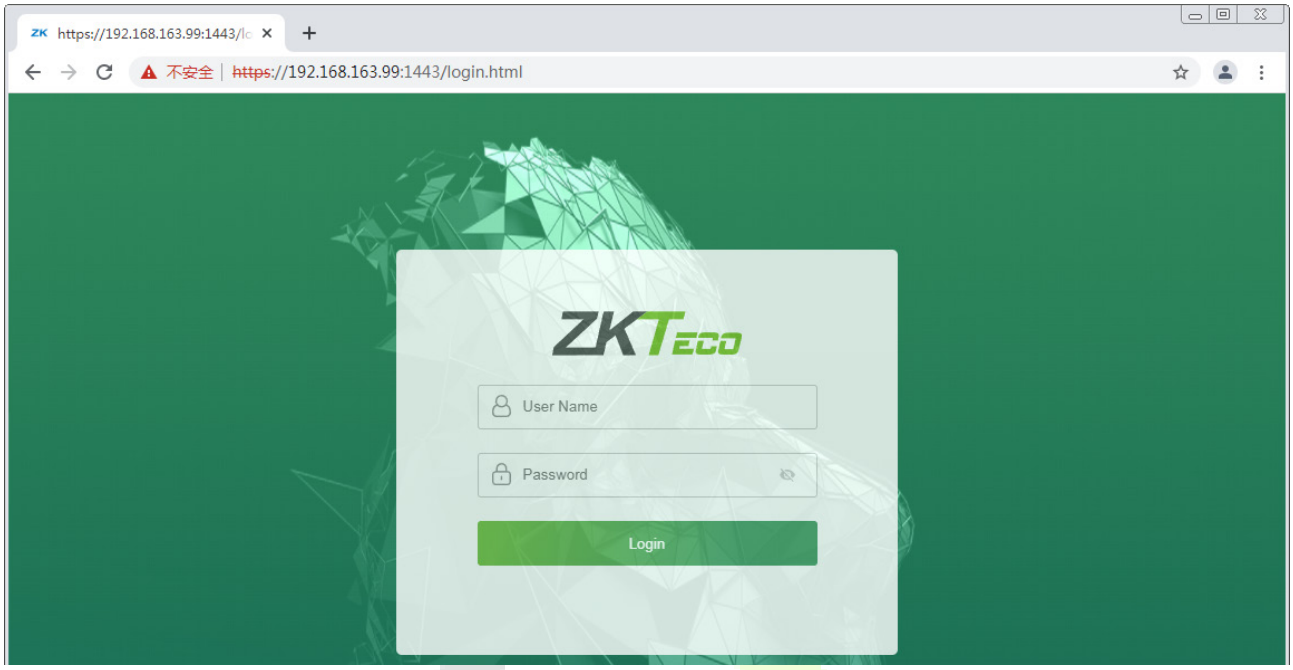
- **Directly Enter the IP Address of the Indoor Station**

Once the indoor station is configured with the network, the video intercom function can be realized by tap the icon on the ProFace X screen and entering the IP address of the indoor station in the jumping interface.

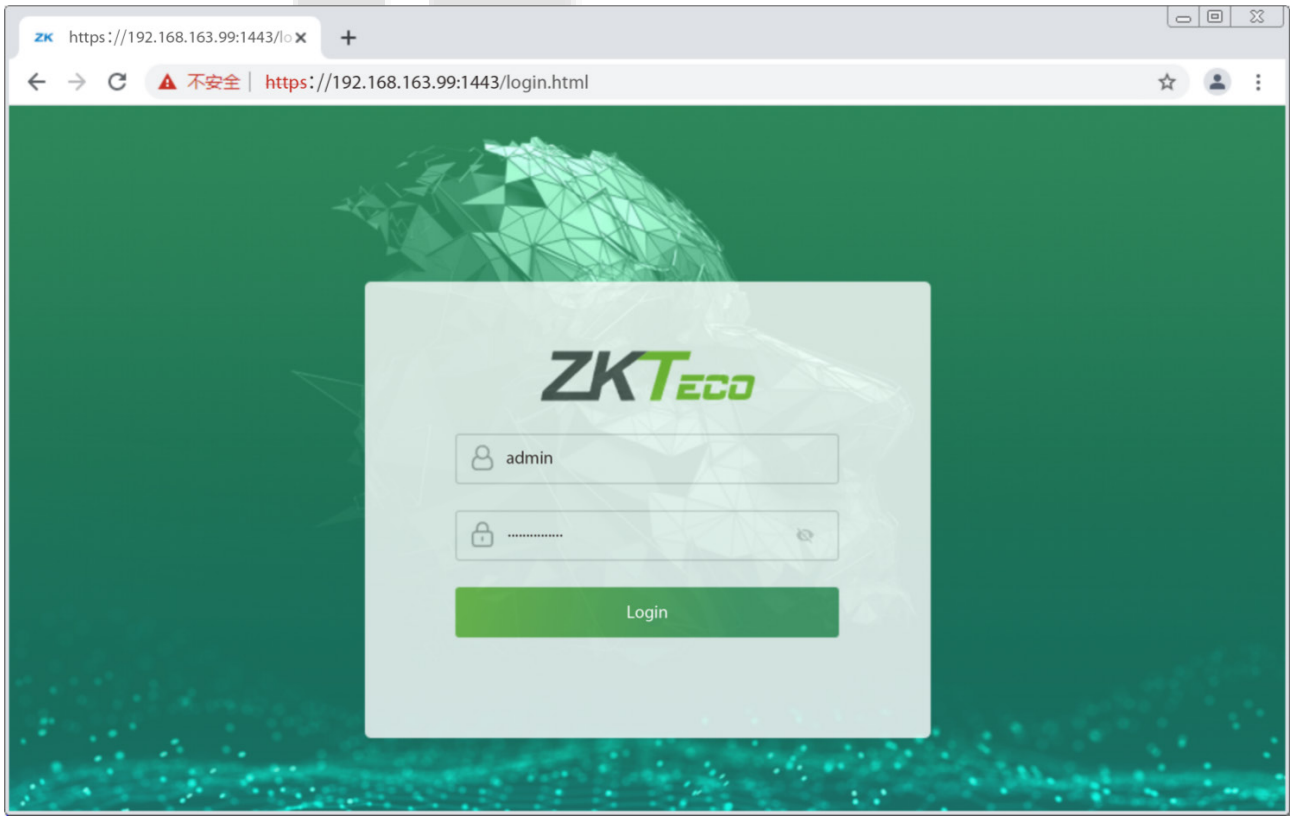
- **Custom the Punch Status Options**

1. Use your browser to enter the address to log into WebSever, the address is the **Serial IP Address:1443**, for example: https: //192.168.163.99:1443.

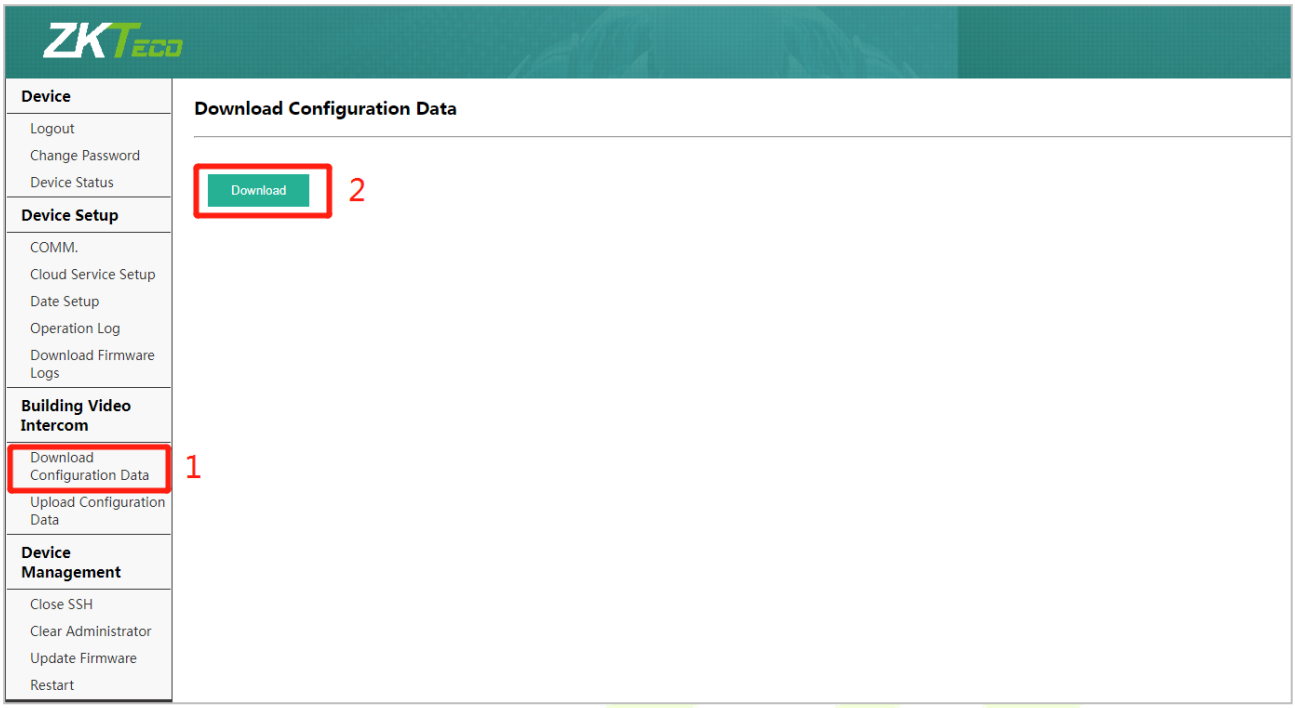




2. Enter the WebSever account and password, the initial account is: **admin**, password: **admin@123**.



3. Download configuration data.



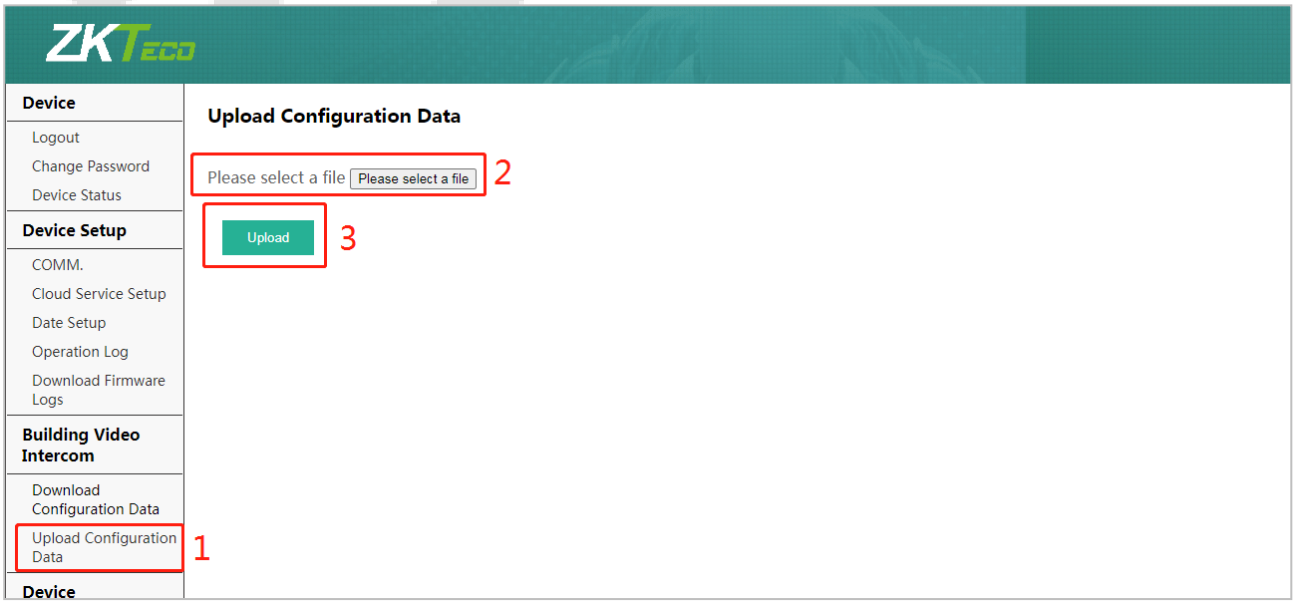
4. Enter the indoor station's communication address and device number in the downloadable form.

	A	B	C	D	E
1	IP Address	Subnet Mask	Gateway	Dialing Number	
2	192.168.163.199	255.255.255.0	192.168.163.1	9	
3	192.168.163.205	255.255.255.0	192.168.163.1	3	
4	192.168.163.103	255.255.255.0	192.168.163.1	4	
5	192.168.163.104	255.255.255.0	192.168.163.1	5	
6	192.168.163.105	255.255.255.0	192.168.163.1	6	
7					

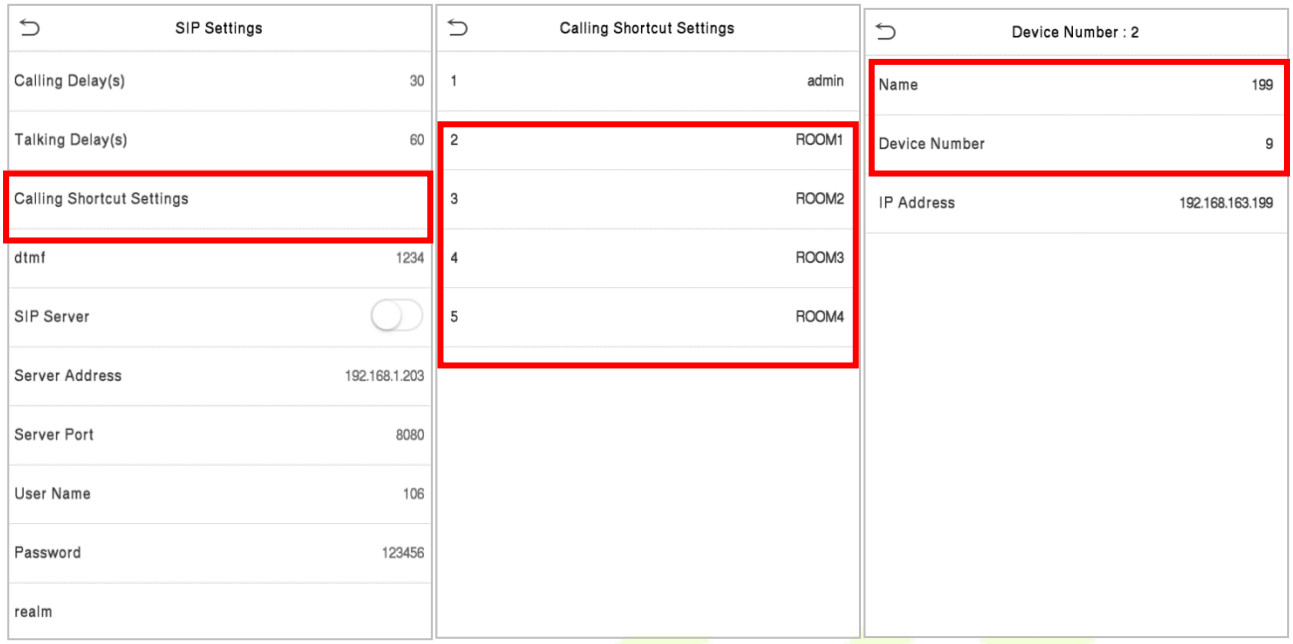
IP Address/Subnet Mask/Gateway: Must be the same as the indoor station to be connected.

Dialing Number: Customize the number of the indoor station, you can enter the value on ProFace X to call the indoor station quickly for video intercom.

5. Once the form is set up and saved, upload the configuration form in WebSever.



6. On ProFace X, tap **[Calling Shortcut Settings]**, select any item except admin, and enter the form information you just uploaded.

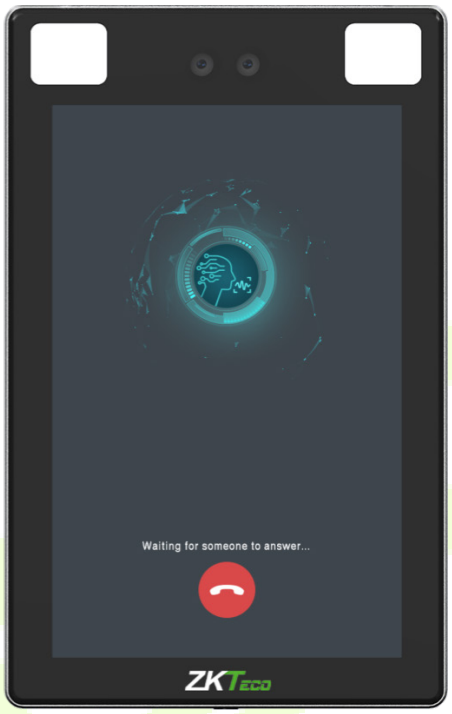


Function Description

Function Name	Description
Name	You can customize any character (support Chinese, English, numbers, symbols, etc.) that will be displayed on the call page.
Device Number	It is the dialing number in the configuration data, you can enter the value on ProFace X to call the indoor station quickly for video intercom.
IP Address	After entering the dialing number, the corresponding IP address in the configuration data will be automatically paired.

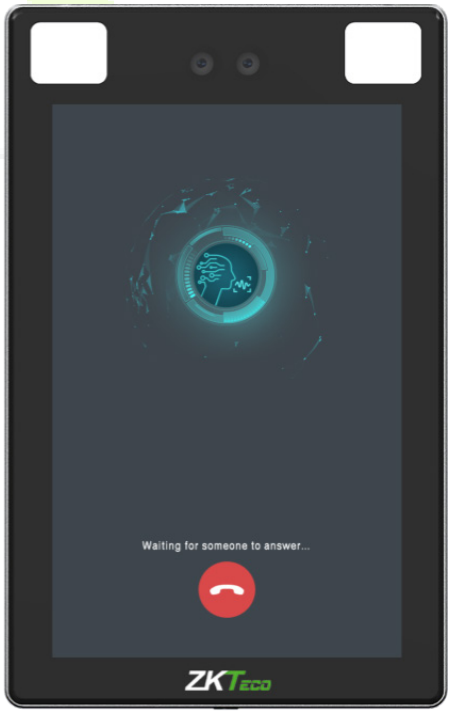
- **Name**

You can then tap **[199]** on the punch status options to directly implement the video intercom.



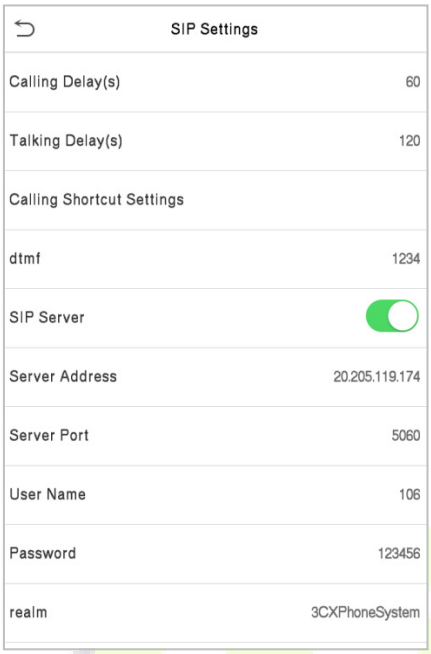
- **Device Number**

Enter the device number in the call screen.

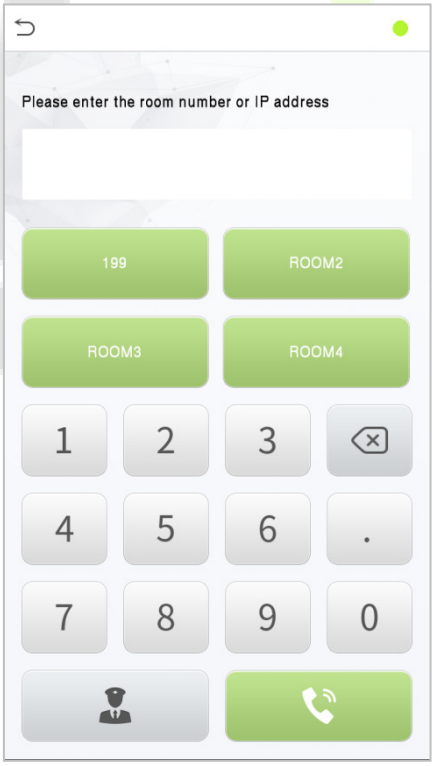


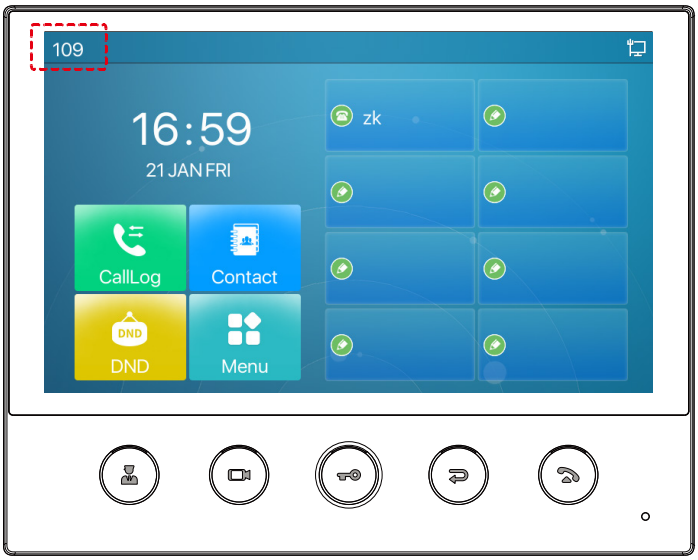
18.2 SIP Server

On ProFace X, tap [**SIP Server**], after the device is rebooted, enter the server-related parameters, as shown below:



Once the SIP is set up correctly, a green dot will appear in the upper right corner of the call page to indicate that the ProFace X is connected to the server. You can call the account name of the indoor station.



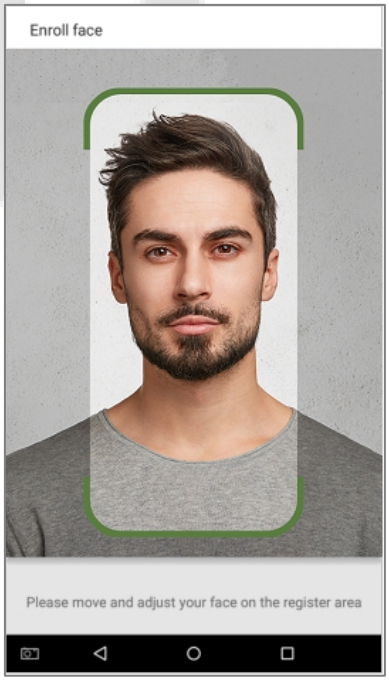


For details on the operation and use of the indoor station, please refer to the *indoor station user manual*.

Appendix 1

Requirements for Live Collection and Registration of Visible Light Face Images

1) It is recommended to perform the 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 a person with eyeglasses, one image with eyeglasses and the other without eyeglasses.
7) Do not wear accessories like a scarf or mask that may cover your mouth or chin.
8) Please face right towards the capturing device and locate your face in the image capturing area as shown in the image below.
9) Do not include more than one face in the capturing area.
10) A distance of 50cm to 80cm is recommended for capturing the image (the distance is adjustable, subject to body height).



Requirements for Visible Light Digital Face Image Data

The digital photo should be straight-edged, 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 plain face or smile with eyes naturally open is 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 eyeglasses.

Face

The image must have 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 the 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 have open and with clearly seen iris.
8) A plain 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.

Appendix 2

Privacy Policy

Notice:

To help you better use the products and services of ZKTeco (hereinafter referred as "we", "our", or "us") a smart service provider, we consistently collect your personal information. Since we understand the importance of your personal information, we took your privacy sincerely and we have formulated this privacy policy to protect your personal information. We have listed the privacy policies below to precisely understand the data and privacy protection measures related to our smart products and services.

Before using our products and services, please read carefully and understand all the rules and provisions of this Privacy Policy. If you do not agree to the relevant agreement or any of its terms, you must stop using our products and services.

I. Collected Information

To ensure the normal product operation and help the service improvement, we will collect the information voluntarily provided by you or provided as authorized by you during registration and use or generated as a result of your use of services.

1. **User Registration Information:** At your first registration, the feature template (**Fingerprint template/Face template/Palm template**) will be saved on the device according to the device type you have selected to verify the unique similarity between you and the User ID you have registered. You can optionally enter your Name and Code. The above information is necessary for you to use our products. If you do not provide such information, you cannot use some features of the product regularly.

2. **Product information:** According to the product model and your granted permission when you install and use our services, the related information of the product on which our services are used will be collected when the product is connected to the software, including the Product Model, Firmware Version Number, Product Serial Number, and Product Capacity Information. **When you connect your product to the software, please carefully read the privacy policy for the specific software.**

II. Product Security and Management

1. When you use our products for the first time, you shall set the Administrator privilege before performing specific operations. Otherwise, you will be frequently reminded to set the Administrator privilege when you enter the main menu interface. **If you still do not set the Administrator privilege after receiving the system prompt, you should be aware of the possible security risk (for example, the data may be manually modified).**
2. All the functions of displaying the biometric information are disabled in our products by default. You can choose Menu > System Settings to set whether to display the biometric

information. If you enable these functions, we assume that you are aware of the personal privacy security risks specified in the privacy policy.

3. Only your user ID is displayed by default. You can set whether to display other user verification information (such as Name, Department, Photo, etc.) under the Administrator privilege. **If you choose to display such information, we assume that you are aware of the potential security risks (for example, your photo will be displayed on the device interface).**

4. The camera function is disabled in our products by default. If you want to enable this function to take pictures of yourself for attendance recording or take pictures of strangers for access control, the product will enable the prompt tone of the camera. **Once you enable this function, we assume that you are aware of the potential security risks.**

5. All the data collected by our products is encrypted using the AES 256 algorithm. All the data uploaded by the Administrator to our products are automatically encrypted using the AES 256 algorithm and stored securely. If the Administrator downloads data from our products, we assume that you need to process the data and you have known the potential security risk. In such a case, you shall take the responsibility for storing the data. You shall know that some data cannot be downloaded for sake of data security.

6. All the personal information in our products can be queried, modified, or deleted. If you no longer use our products, please clear your personal data.

III. How we handle personal information of minors

Our products, website and services are mainly designed for adults. Without consent of parents or guardians, minors shall not create their own account. If you are a minor, it is recommended that you ask your parents or guardian to read this Policy carefully, and only use our services or information provided by us with consent of your parents or guardian.

We will only use or disclose personal information of minors collected with their parents' or guardians' consent if and to the extent that such use or disclosure is permitted by law or we have obtained their parents' or guardians' explicit consent, and such use or disclosure is for the purpose of protecting minors.

Upon noticing that we have collected personal information of minors without the prior consent from verifiable parents, we will delete such information as soon as possible.

IV. Others

You can visit https://www.zkteco.com/cn/index/Index/privacy_protection.html to learn more about how we collect, use, and securely store your personal information. To keep pace with the rapid development of technology, adjustment of business operations, and to cope with customer needs, we will constantly deliberate and optimize our privacy protection measures and policies. Welcome to visit our official website at any time to learn our latest privacy policy.

Eco-friendly Use

The product's "eco-friendly operational period" refers to the time 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.

ZKTeco Industrial Park, No. 32, Industrial Road,

Tangxia Town, Dongguan, China.

Phone : +86 769 - 82109991

Fax : +86 755 - 89602394

www.zkteco.com