User Manual

SF1008-T+

Date: June 2020

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.zktecousa.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 USA Headquarters

Address 1600 Union Hill Road

Phone (862) 505 2101

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

To know more about our global branches, visit www.zktecousa.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 SF1008-T+ Product.

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

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

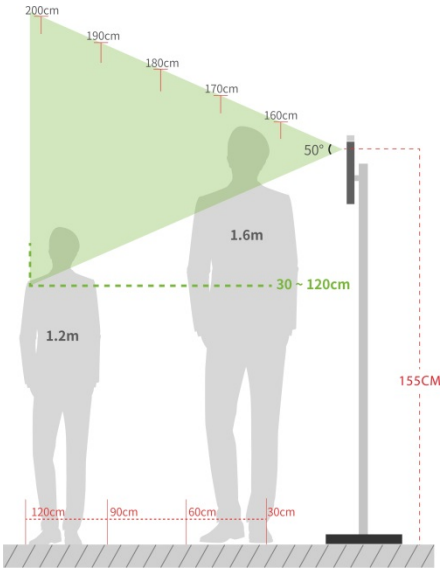
Convention	Description
	This implies about the notice or pays attention to, in the manual
	The general information which helps in performing the operations faster
	The information which is significant
	Care taken to avoid danger or mistakes
	The statement or event that warns of something or that serves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

Table of Contents

1 Notice for Use

1.1 Standing Position, Facial Expression and Standing Posture

- **The recommended distance**



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

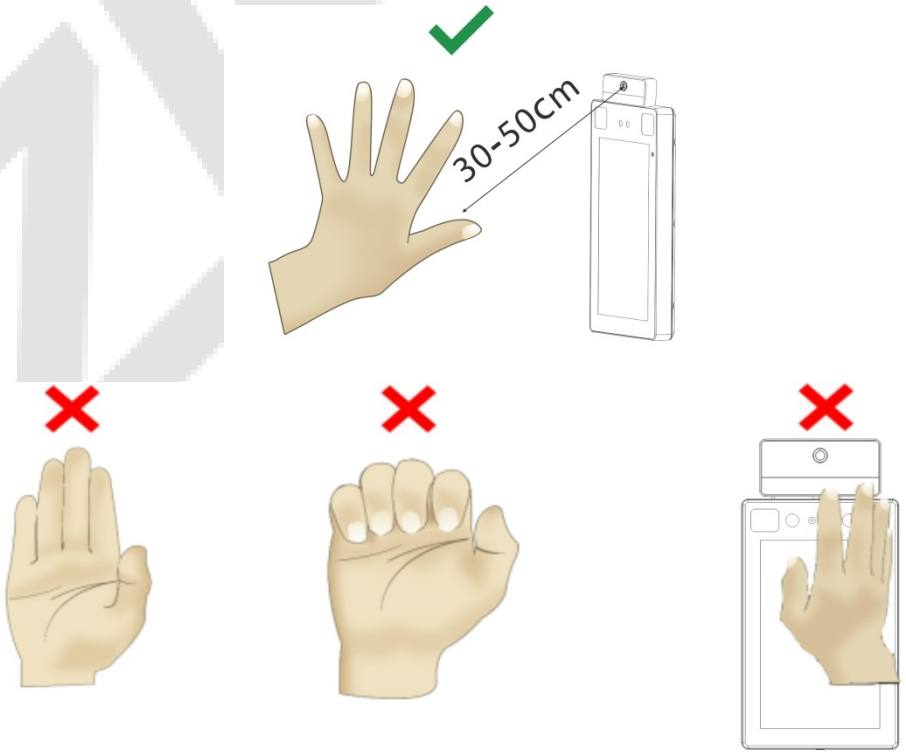
- **Facial expression and standing posture**

Note: During enrolment and verification, please remain natural facial expression and standing posture.

1.2 Palm Registration

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

Make sure to keep space between your fingers.



1.3 Face Registration

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

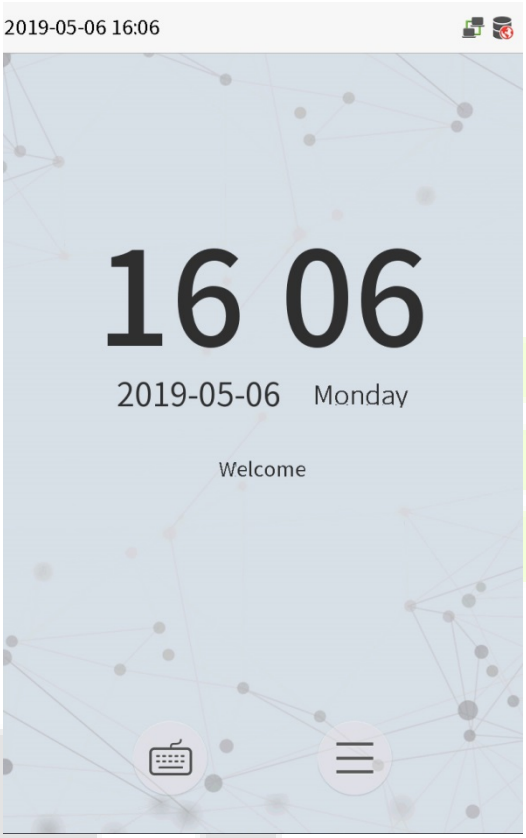
Correct face registration and authentication method

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

1.4 Standby Interface

After connecting the power supply, enter the following standby interface:

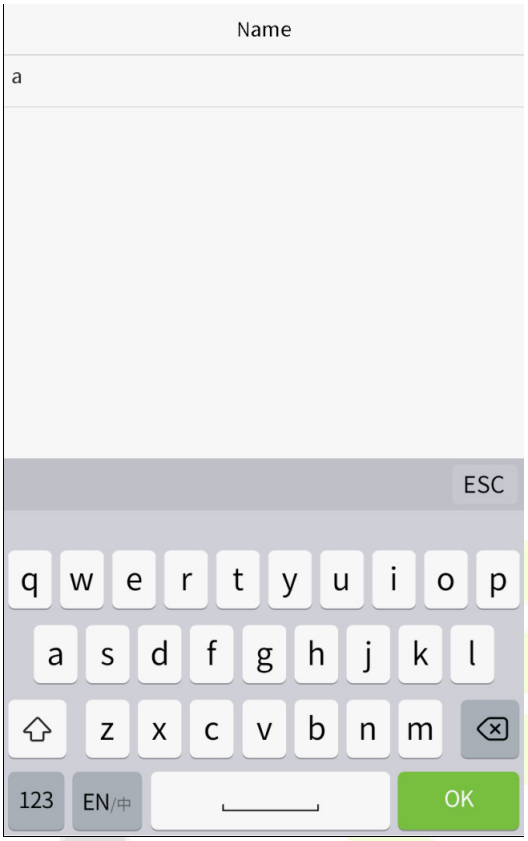


Notes:

1) Click to enter the User ID input interface.

2) 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 the security of the device, it is recommended to register super administrator the first time you use the device.

1.5 Virtual Keyboard



Note: The device supports the input of Chinese, English, numbers and symbols. Click [**En**] to switch to English keyboard. Press [**123**] to switch to the numeric and symbolic keyboard, and click [**ABC**] to return to the alphabetic keyboard. Click the input box, virtual keyboard appears. Click [**ESC**] to exit the input.

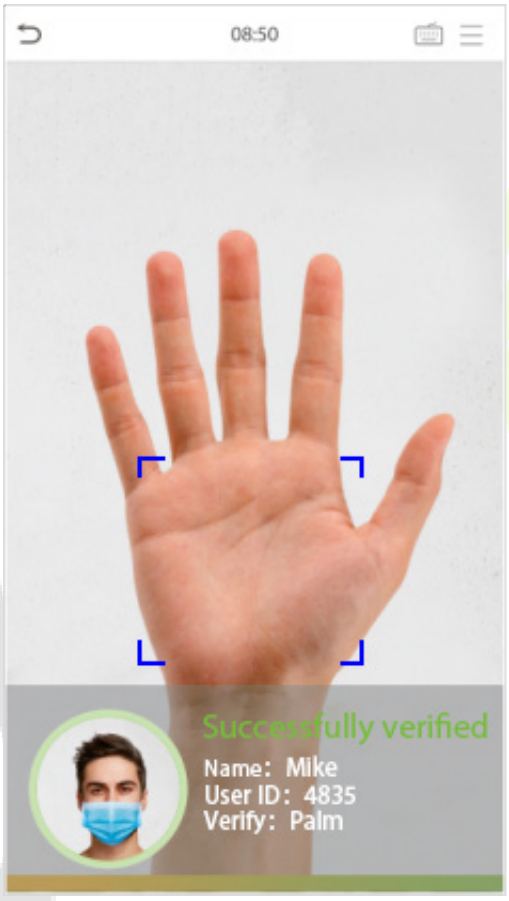
1.6 Verification Mode

1.6.1 Palm Verification

- **1: N Palm Verification mode**

Compare the palm image collected by the palm collector with all the palm data in the device.

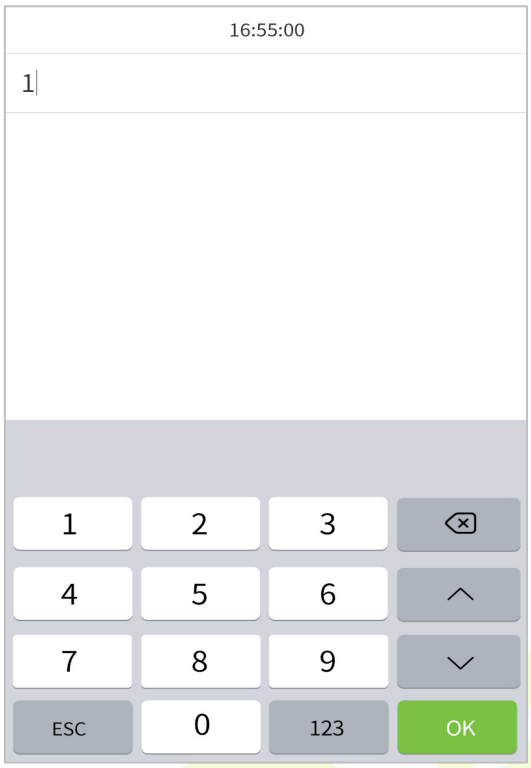
The device will automatically distinguish between the palm and the face verification mode, and place the palm in the area that can be collected by the palm collector, and the device will automatically detect the palm verification mode.



- **1: 1 Palm Verification mode**

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

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



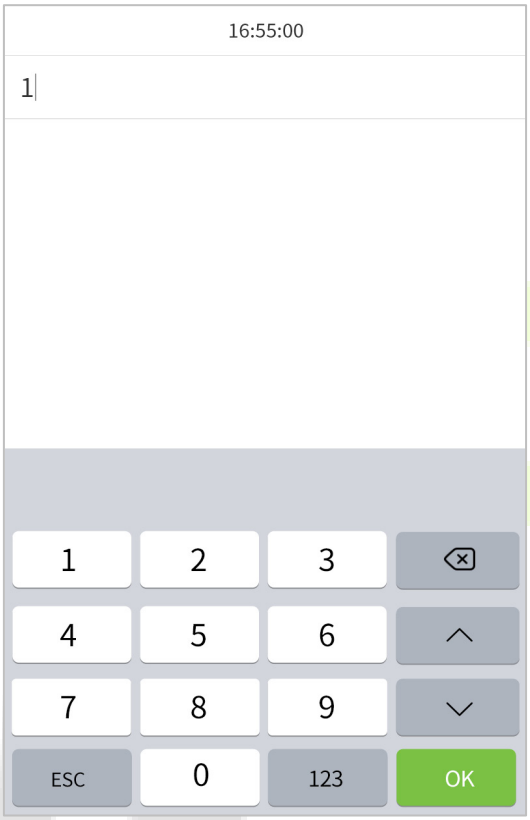
If the user has registered the face and password in addition to his/her palm, and the verification method is set to palm/face/password verification, the following screen will appear. Select the palm icon to enter palm verification mode.

1.6.2 Password Verification

Compare the entered password with the registered User ID and password.

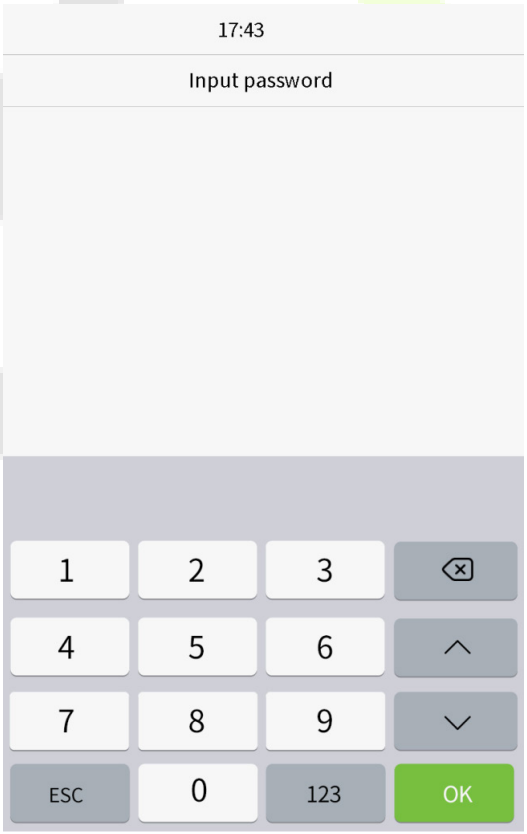
Click the  button on the main screen to enter the 1:1 password verification mode.

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

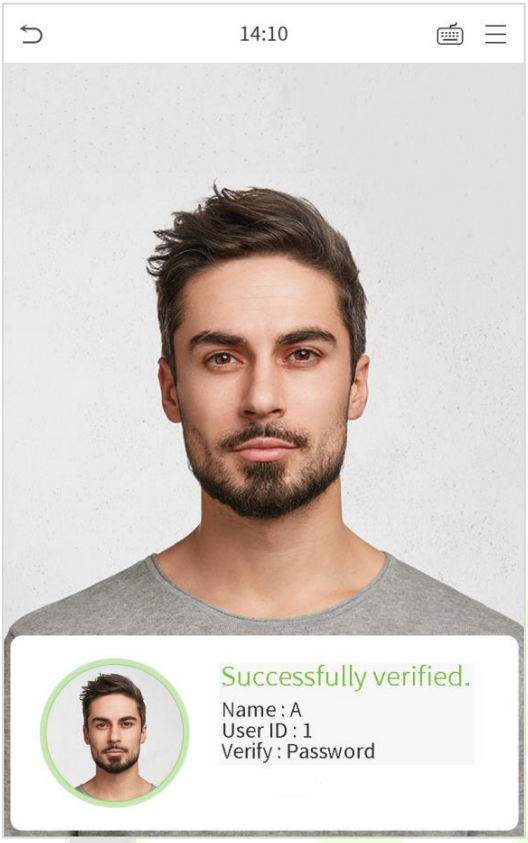


If an employee registers palm and face in addition to password, the following screen will appear. Select the  icon to enter password verification mode.

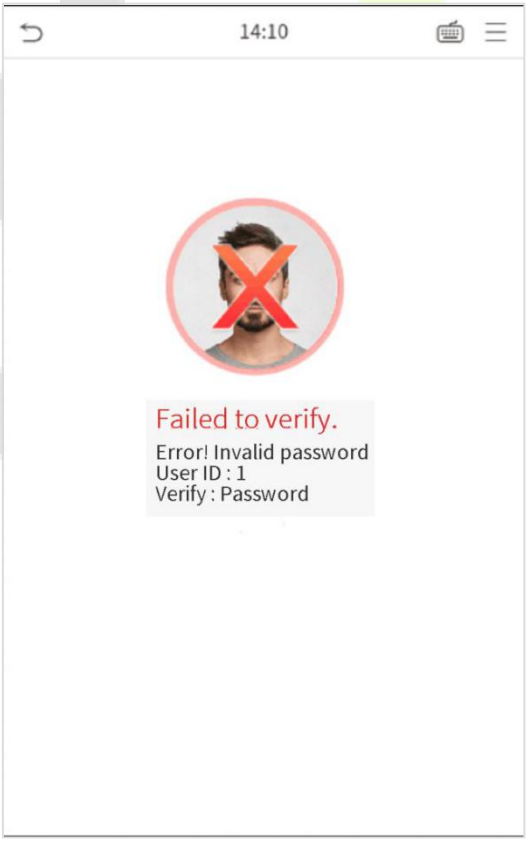
2. Input the password and press [OK].



Verification is successful:



Verification is failed:



1.6.3 Facial Verification

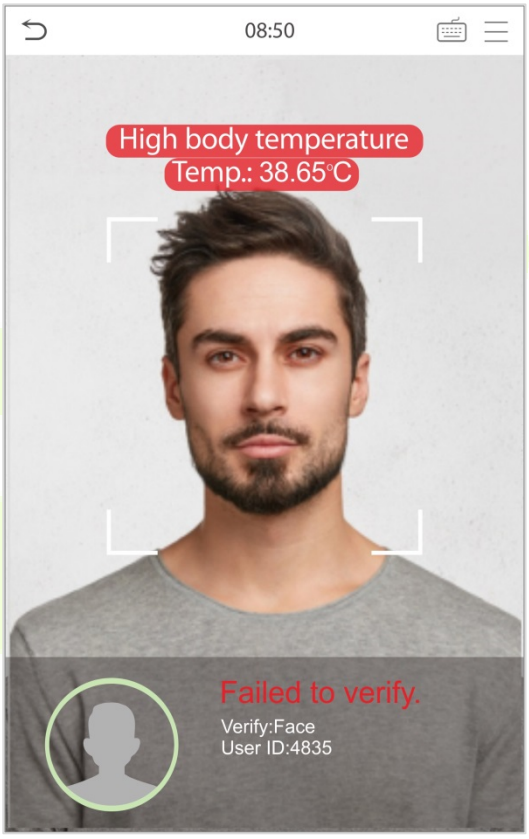
- **1:N Facial Verification**

  1. **Conventional verification**

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

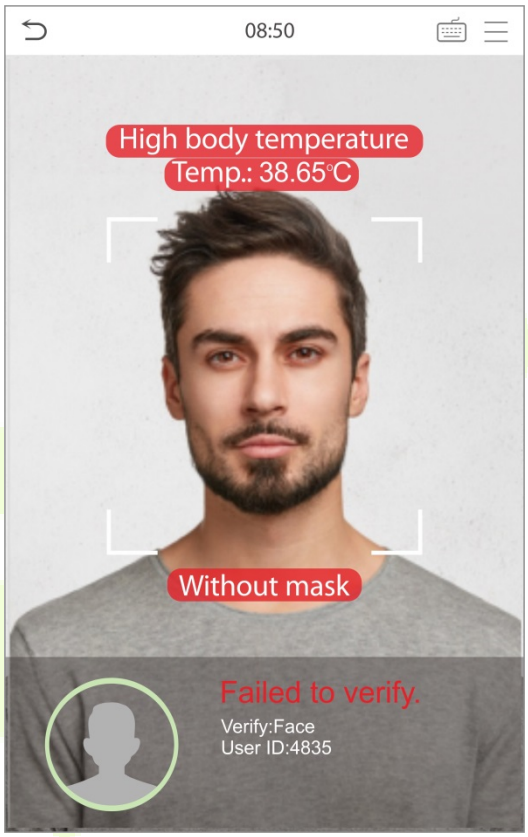
2. Enable temperature screening with infrared

When the user enabled the Enable 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 measurement area to measure the body temperature before the verification can be conducted. The following is a popup of the comparison result prompt interface.



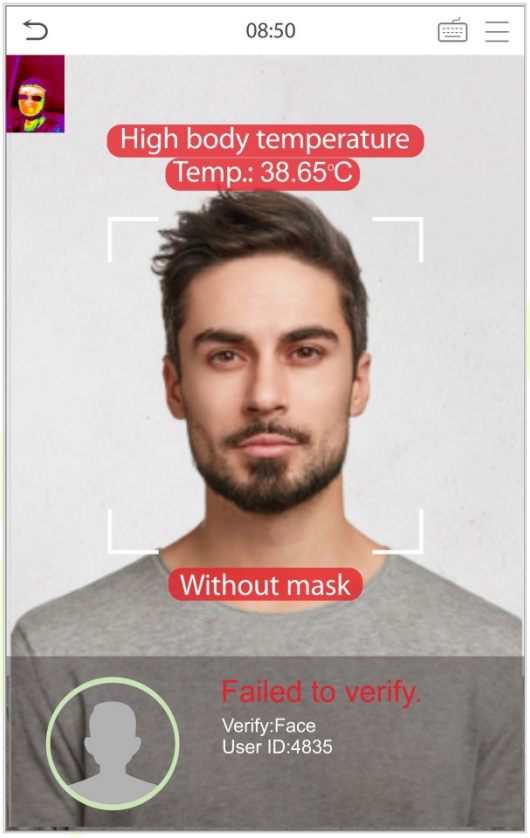
3. Enable mask detection

When the user enabled the **Enable mask detection** function, the device will identify whether the user is wearing a mask or not. The following is a popup of the comparison result prompt 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 upper left corner of the device.

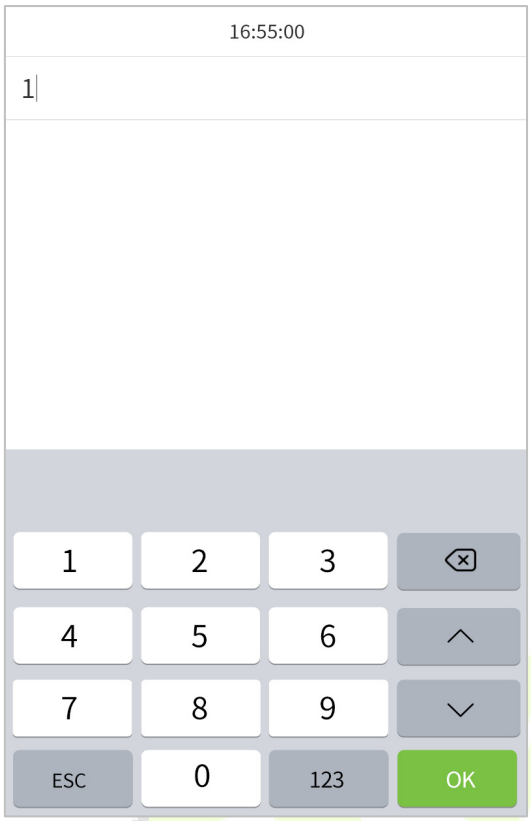


- **1:1 Facial Verification**

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

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

Enter the user ID and click [OK].



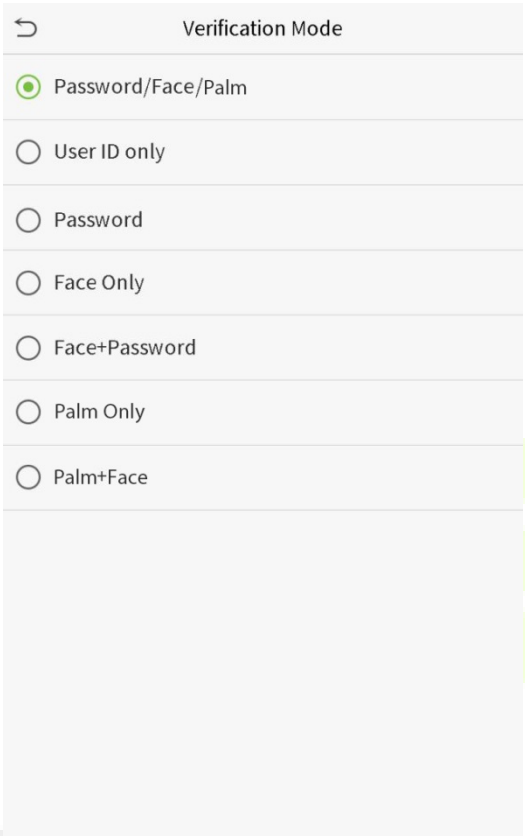
If an employee registers palm and password in addition to face, the following screen will appear. Select the  icon to enter face verification mode.

After successful verification, the prompt box "successfully verified" will appear.

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

1.6.4 Combined Verification

To increase security, this device offers the option of using multiple forms of verification methods. A total of 7 different verification combinations can be used, as shown below:



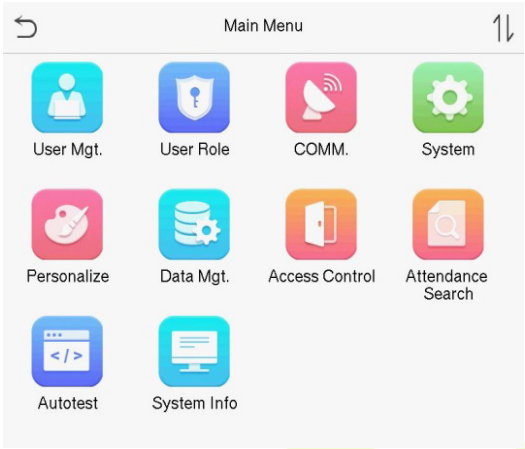
Notes:

1）"/" means “or”, and "+" means “and”.

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

2 Main Menu

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

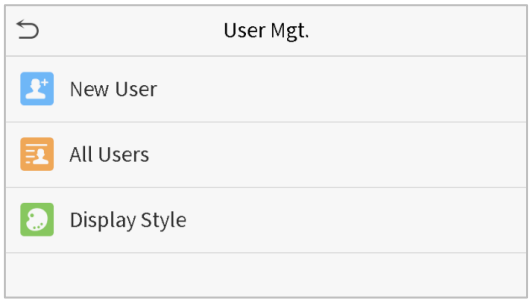


Items	Descriptions
User Mgt.	To add, edit, view, and delete basic information about a user.
User Role	To set the permission scope of the custom role and enroller, that is, the rights to operate the system.
COMM.	To set the relevant parameters of the network, PC connection, wireless network, cloud server and wiegand.
System	To set parameters related to the system, including date & time, access records, facial templates, palm templates, 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 relevant data in the device.
Access Control	To set the parameters of the lock and the relevant access control device.
Attendance Search	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 data capacity, device and firmware information of the current device.

3 User Management

3.1 Adding Users

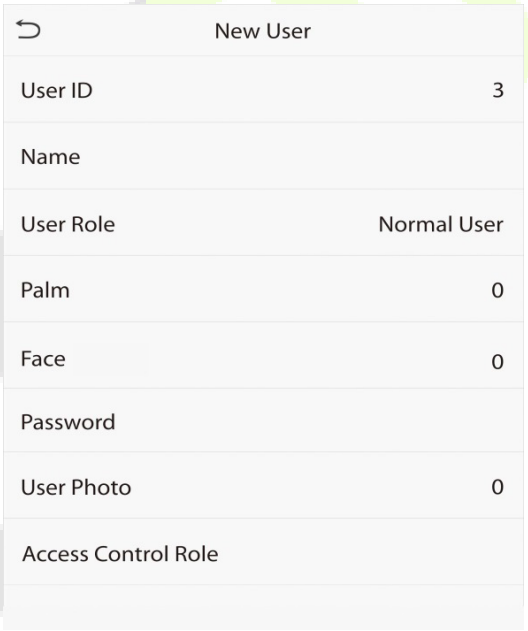
Click **User Mgt.** on the main menu.



Click **New User.**

- **Register a User ID and Name**

Enter the user ID and name.



Notes:

1）A user name may contain 17 characters.

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

3）During the initial registration, you can modify your ID, which cannot be modified after registration.

4）If a message "Duplicated ID" pops up, you must choose another ID.

- **Setting the User Role**

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

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

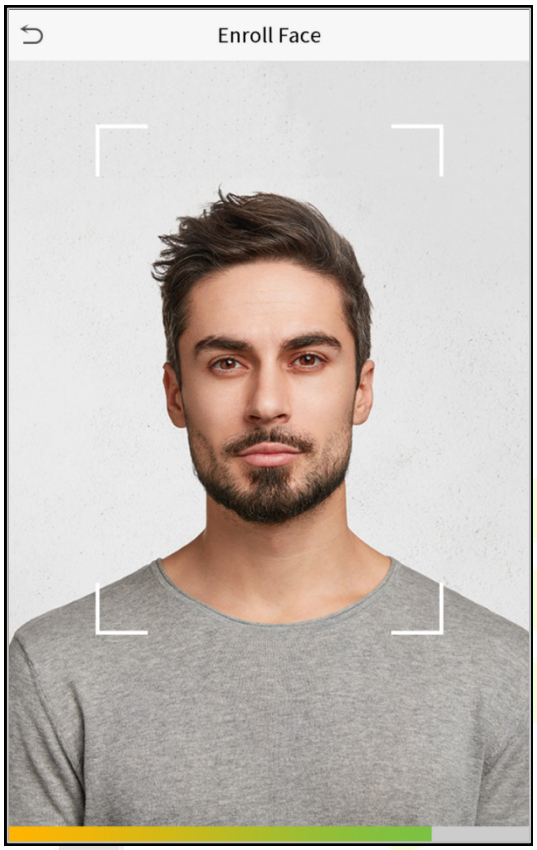
Note: If the selected user role is the Super Admin, the user must pass the identity authentication to access the main menu. The authentication is based on the authentication method(s) that the super administrator has registered. Please refer to 1.6 Verification Method.

- **Register palm**

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

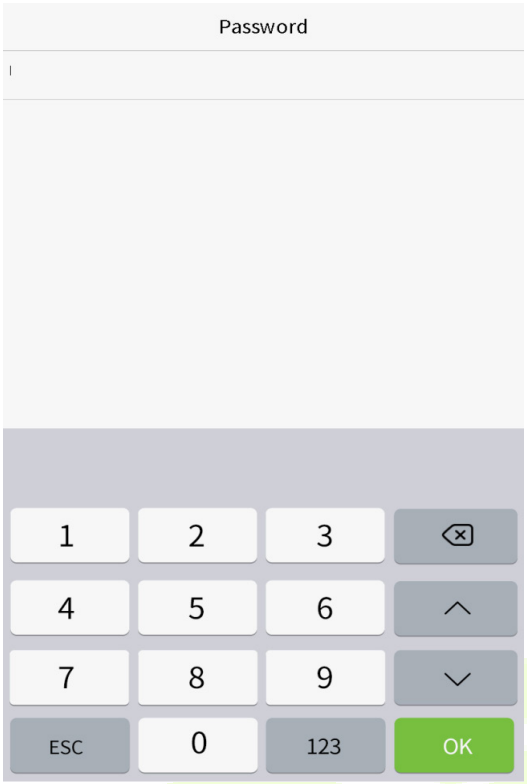
- **Register face**

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



- **Register password**

Click **Password** to enter the password registration page. Enter a password and re-enter it. 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 passes the authentication, the registered photo will be displayed.

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

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

- **Access Control Role**

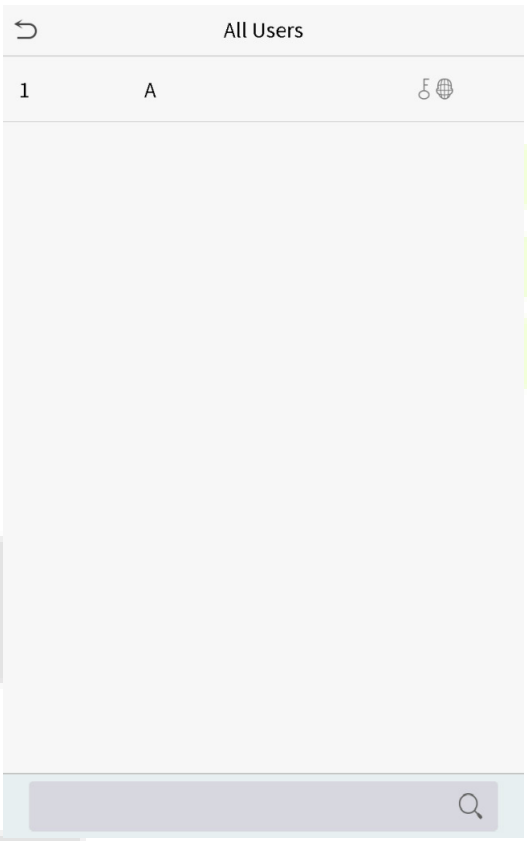
User access control sets the door unlocking rights of each person, including the group and the time period that the user belongs to.

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

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

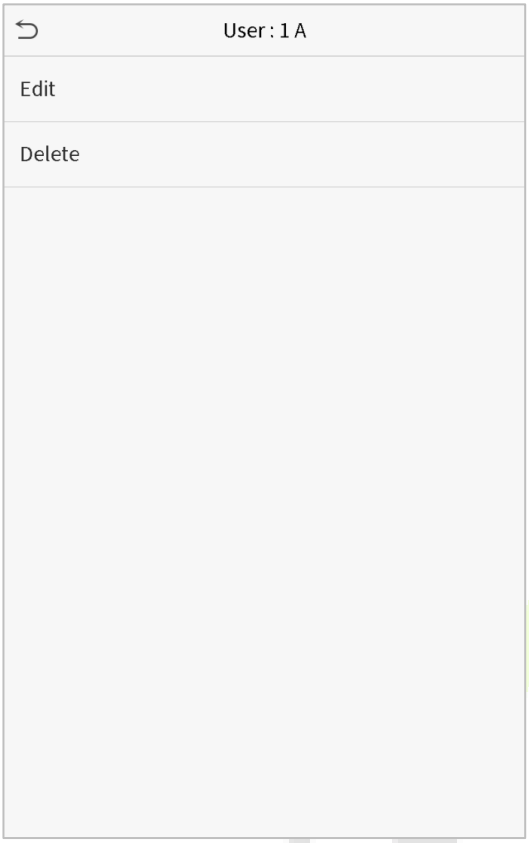
3.2 Search for Users

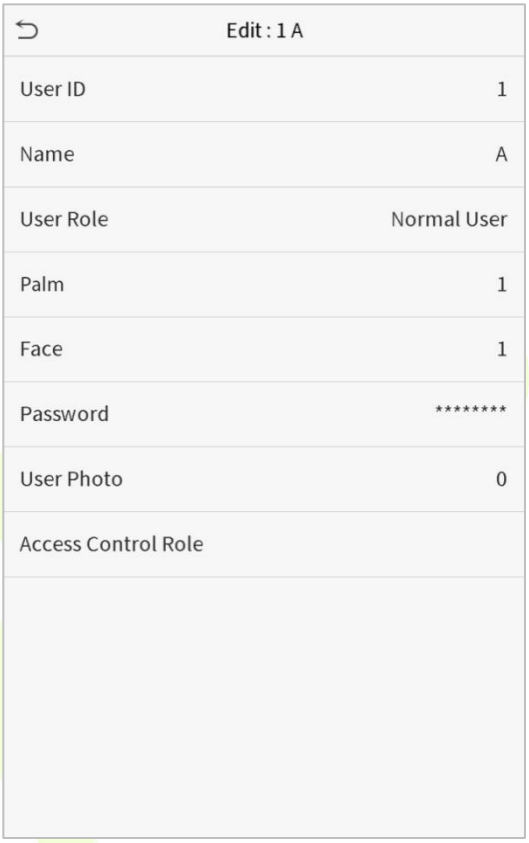
Click the search bar on the user list and enter the retrieval keyword (The keyword may be an ID, surname or full name.). The system will search for the users related to the information.



3.3 Edit Users

Choose a user from the list and click **Edit** to enter 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 "3.1 Adding users".

3.4 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**.

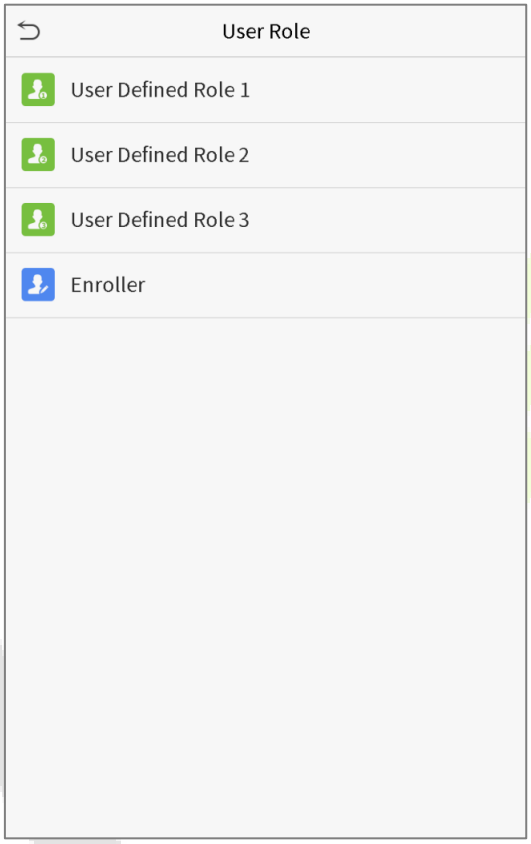
Note: If you select **Delete User**, all information of the user will be deleted.

4 User Role

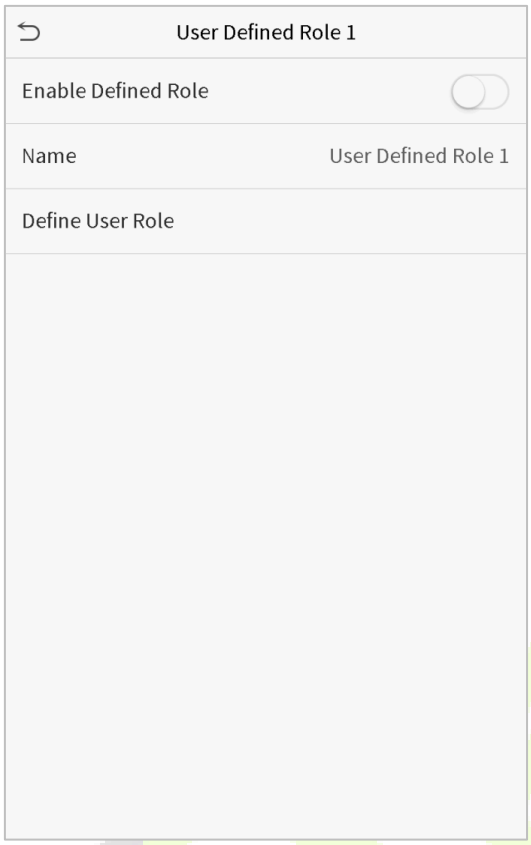
If you need to assign some specific permissions to certain users, you may edit the "User Defined Role" under the **User Role** menu.

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

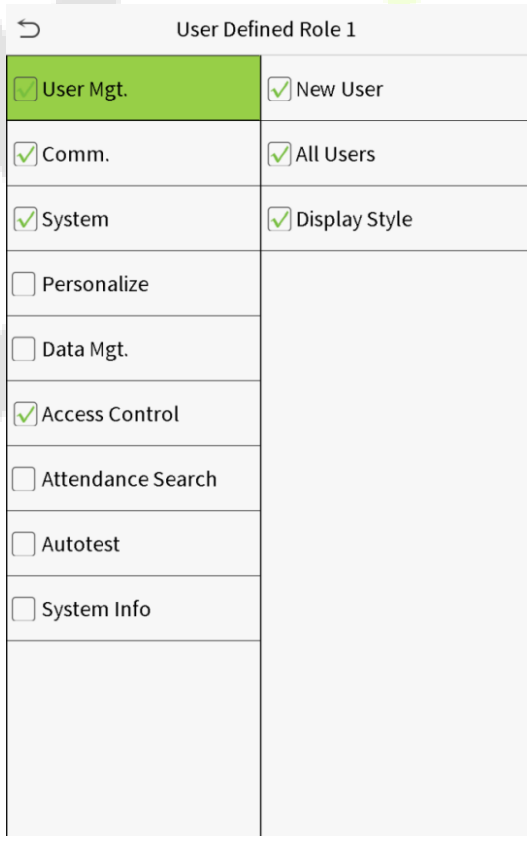
Click **User Role** on the main menu interface.



1. Click any item to set a defined role. Click the row of **Enable Defined Role** 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. The privilege assignment is completed. Click Return.



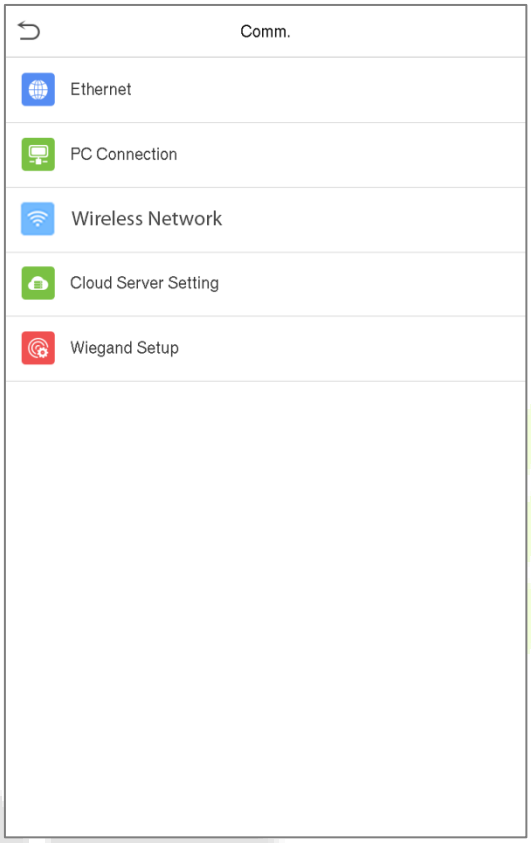
Note: During privilege assignment, the main menu is on the left and its sub-menus are on the right. You only need to select the features in sub-menus. If the device has a role enabled, you may assign the roles you set to users by clicking User Mgt. > New User > User Role.

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

5 Communication Settings

Set parameters of the network, PC connection, wireless network , cloud server and Wiegand.

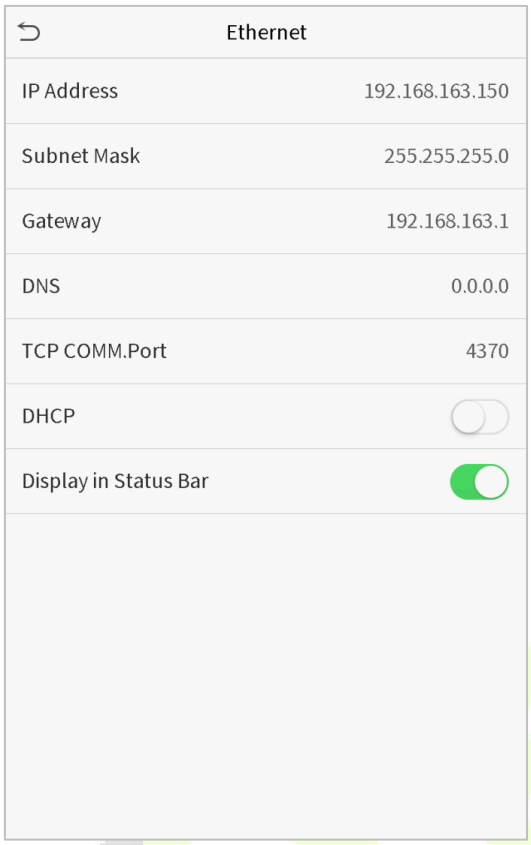
Tap **COMM.** on the main menu.



5.1 Network Settings

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

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



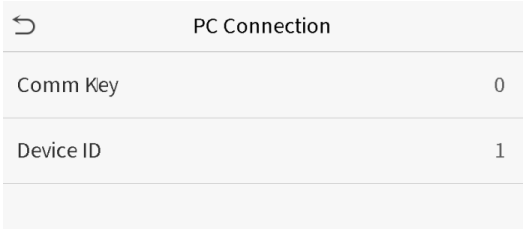
Item	Descriptions
IP Address	The factory default value is 192.168.1.201. Please adjust them according to the actual network situation.
Subnet Mask	The factory default value is 255.255.255.0. Please adjust them according to the actual network situation.
Gateway	The factory default address is 0.0.0.0. Please adjust them according to the actual network situation.
DNS	The factory default address is 0.0.0.0. Please adjust them according to the actual network situation.
TCP COMM. Port	The factory default value is 4370. Please adjust them 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.

5.2 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.

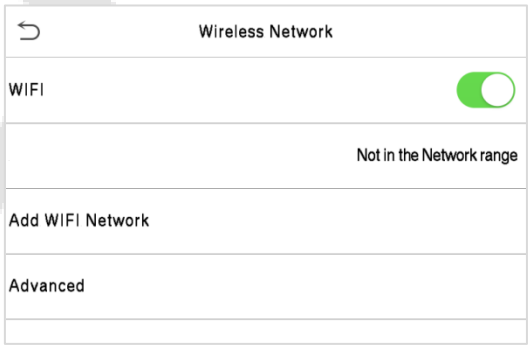


Item	Descriptions
Comm Key	Comm Key: The default password is 0, which can changed. The Comm Key may contain1-6 digits.
Device ID	Identity number of the device, which ranges between 1 and 254. If the communication method is RS232/RS485, you need to input this device ID in the software communication interface.

5.3 Wireless Network

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

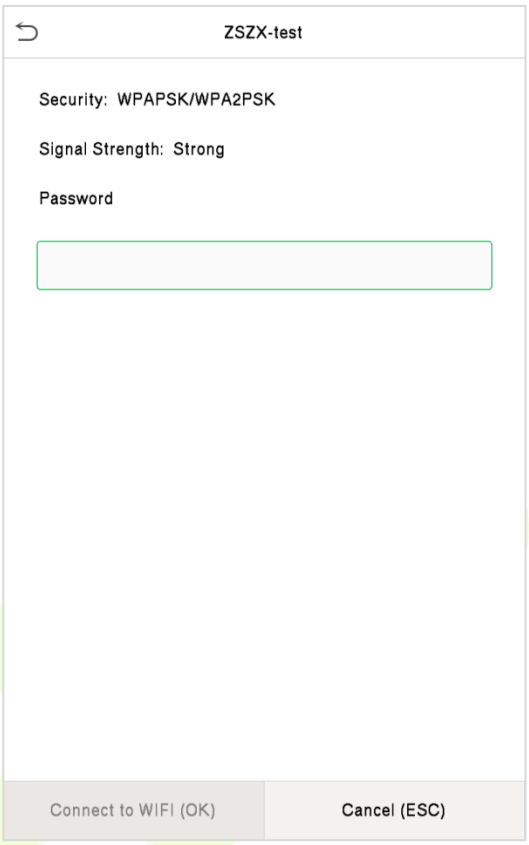
Click **Wireless Network** on the Comm. Settings interface.



WIFI is enabled in the Device by default. Toggle on button to enable or disable WIFI.

When WIFI is enabled, tap on the required network from the searched network list.

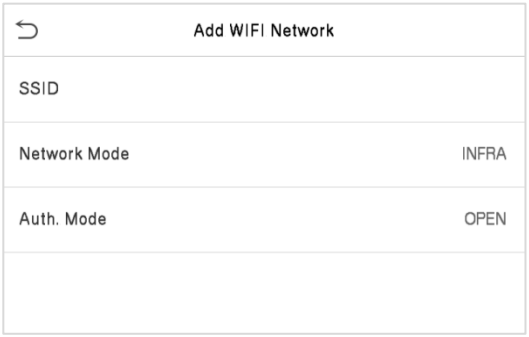
WIFI Enabled: Tap on the required network from the searched network list.



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

Add WIFI Network Manually

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

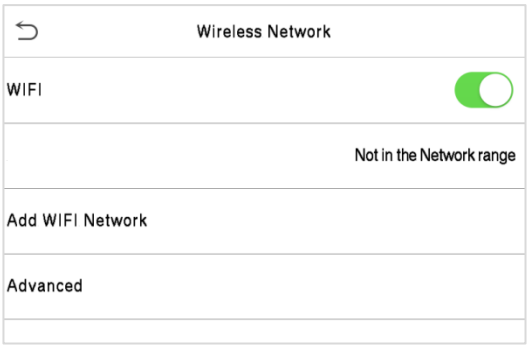


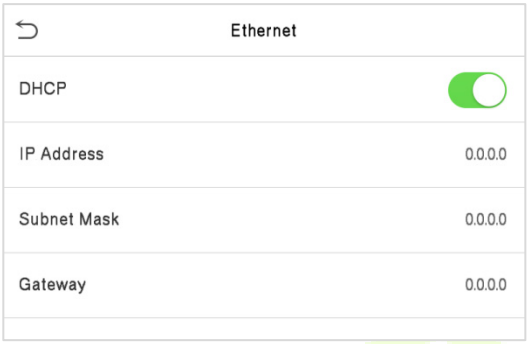
On this interface, enter the WIFI network parameters. (The added network must exist.)

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

Advanced Options

This interface is to set the WIFI network parameters.





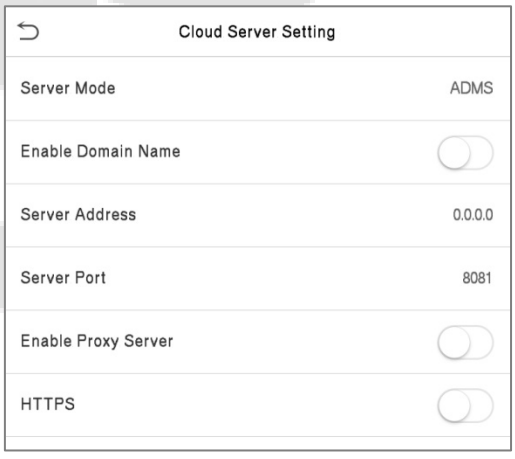
Function Description

Menu Item	Description
DHCP	Short for Dynamic Host Configuration Protocol, which involves allocating dynamic IP addresses to network clients.
IP Address	IP address of the WIFI network.
Subnet Mask	Subnet mask of the WIFI network.
Gateway	Gateway address of the WIFI network.

5.4 Cloud Server Setting

This represents settings used for connecting with the ADMS server.

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



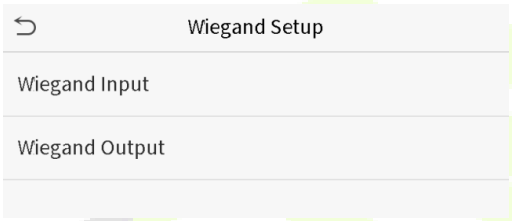
Item		Description
Enable Domain Name	**Server Address**	When this function is enabled, the domain name mode "http://..." will be used, such as http://www.XYZ.com, while "XYZ" denotes the domain name when this mode is turned ON.

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		It is an HTTP channel with security as its goal. Based on HTTP, transmission encryption and identity authentication ensure the security of the transmission process.

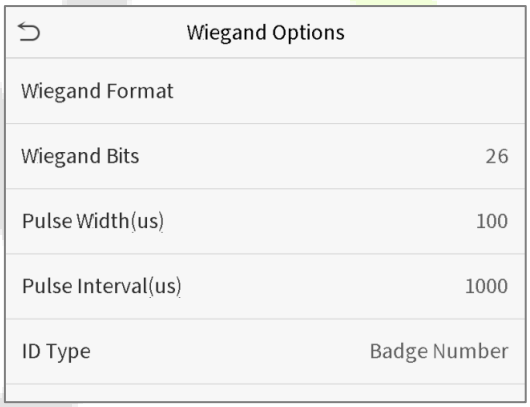
5.5 Wiegand Setup

To set the Wiegand input and output parameters.

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



- **Wiegand input**



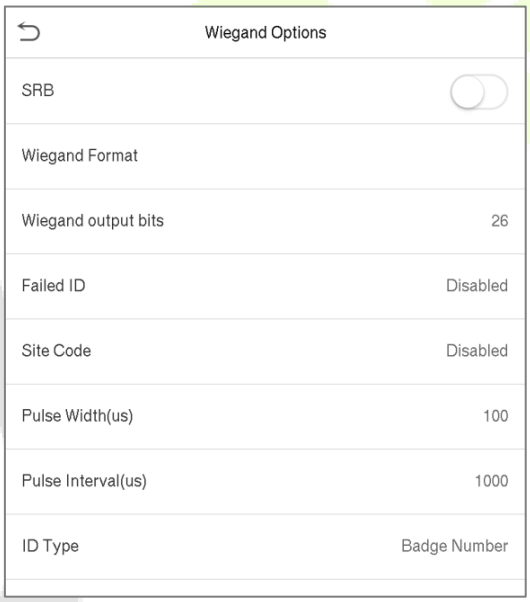
Item	Descriptions
Wiegand Format	Values range from 26 bits, 34 bits, 36 bits, 37 bits, and 50 bits.
Wiegand Bits	Number of bits of Wiegand data.
Pulse Width(us)	The value of the pulse width sent by Wiegand is 100 microseconds by default, which can be adjusted within the range of 20 to 100 microseconds.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

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	ESSSSSSSSCCCCCCCCCCCCCCCCO Consists of 26 bits of binary code. The 1st bit is the even parity bit of the 2nd to 13th bits, while the 26th bit is the odd parity bit of the 14th to 25th bits. The 2nd to 9th bits are the site codes, while the 10th to 25th bits are the card numbers.
Wiegand34	ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO Consists of 34 bits of binary code. The 1st bit is the even parity bit of the 2nd to 17th bits, while the 34th bit is the odd parity bit of the 18th to 33rd bits. The 2nd to 25th bits are the card numbers.
Wiegand34a	ESSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCO Consists of 34 bits of binary code. The 1st bit is the even parity bit of the 2nd to 17th bits, while the 34th bit is the odd parity bit of the 18th to 33rd bits. The 2nd to 9th bits are the site codes, while the 10th to 25th bits are the card numbers.
Wiegand36	OFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCMME Consists of 36 bits of binary code. The 1st bit is the odd parity bit of the 2nd to 18th bits, while the 36th bit is the even parity bit of the 19th to 35th bits. The 2nd to 17th bits are the device codes. The 18th to 33rd bits are the card numbers, and the 34th to 35th bits are the manufacturer codes.
Wiegand36a	EFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCO Consists of 36 bits of binary code. The 1st bit is the even parity bit of the 2nd to 18th bits, while the 36th bit is the odd parity bit of the 19th to 35th bits. The 2nd to 19th bits are the device codes, and the 20th to 35th bits are the card numbers.
Wiegand37	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	EMMMFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCO 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	ESSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO 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.	

- **Wiegand output**



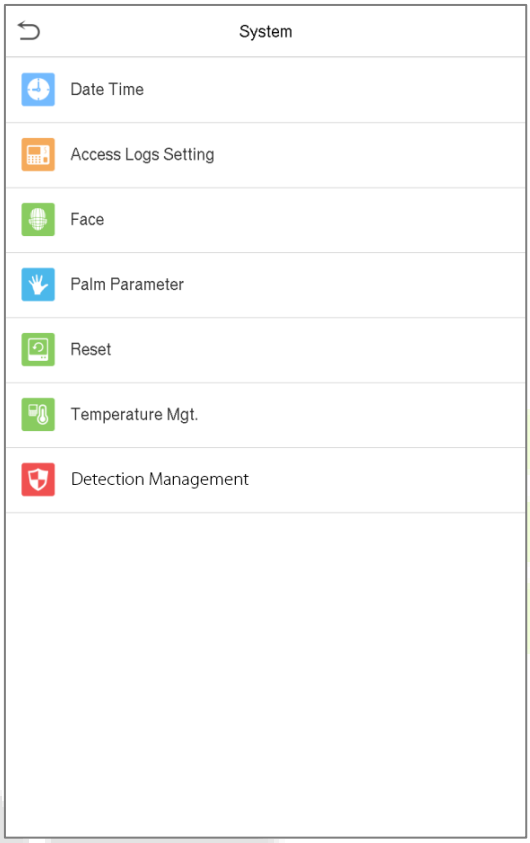
Item	Descriptions
SRB	When SRB is enabled, the lock is controlled by the SRB to prevent the lock from being opened due to device removal.
Wiegand Format	Values range from 26 bits, 34 bits, 36 bits, 37 bits, and 50 bits.
Wiegand output bits	After choosing the Wiegand format, you can select one of the 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 badge number.

6 System Settings

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

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



6.1 Date and Time

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

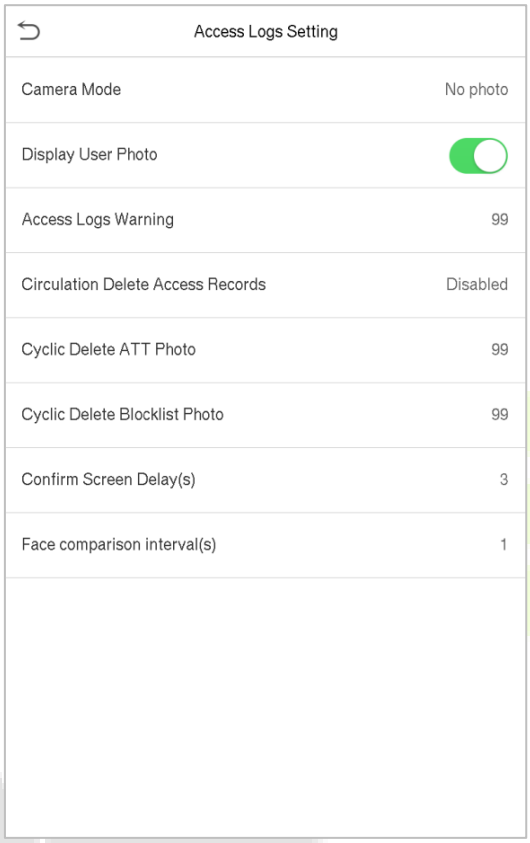
1. You can manually set date and time and click Confirm to save.
2. Click 24-Hour Time to enable or disable this format and select the date format.

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, 2019) to 18:30 on January 1, 2020. After restoring the factory settings, the time of the equipment will remain 18:30 on January 1, 2020.

6.2 Access Logs Setting

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

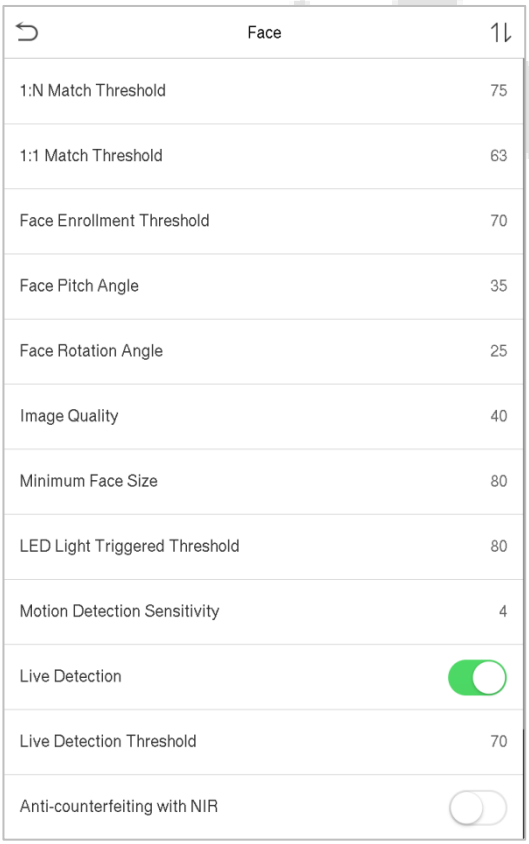


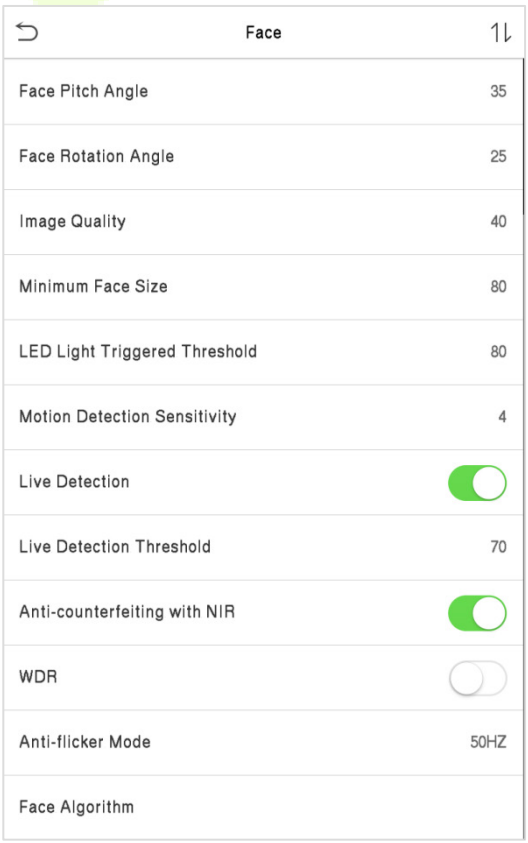
Item	Description
Camera Mode	Whether to capture and save the current snapshot image during verification. There are 5 modes: **No Photo:** No photo is taken during user verification. **Take photo, no save:** Photo is taken but is not saved during verification. **Take photo and save:** Photo is taken and saved during verification. **Save on successful verification:** Photo is taken and saved for each successful verification. **Save on failed verification:** Photo is taken and saved during each failed verification.
Display User Photo	Whether to display the user photo when the user passes verification.

Access Logs Warning	When remaining record space reaches a set value, the device will automatically display a remaining record memory warning. Users may disable the function or set a valid value between 1 and 9999.
Circulation Delete Access Records	When access records have reached full capacity, the device will automatically delete a set value of old access records. Users may disable the function or set a valid value between 1 and 999.
Cyclic Delete ATT Photo	When attendance photos have reached full capacity, the device will automatically delete a set value of old attendance photos. Users may disable the function or set a valid value between 1 and 99.
Cyclic Delete Blocklist Photo	When 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 length of time that the message of successful verification displays. Valid value: 1~9 seconds.
Face comparison Interval (s)	To set the facial template matching time interval as needed. Valid value: 0~9 seconds.

6.3 Face Parameters

Click **Face** on the System interface.





Item	Description
1:N Match Threshold	Under 1:N verification mode, the verification will only be successful when the similarity between the acquired facial image and all registered facial templates is greater than the set value. The valid value ranges from 65 to 120. The higher the thresholds, the lower the misjudgment rate, the higher the rejection rate, and vice versa. The default value of 75 is recommended.
1:1 Match Threshold	Under 1:1 verification mode, the verification will only be successful when the similarity between the acquired facial image and the facial templates enrolled in the device is greater than the set value. The valid value ranges from 55 to 120. The higher the thresholds, the lower the misjudgment 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 registered facial templates is greater than this threshold, it indicates that the face has already been registered.
Face Pitch Angle	The pitch angle tolerance of a face for facial registration and comparison. If a face's pitch angle exceeds this set value, it will be filtered by the algorithm, i.e. ignored by the terminal thus no registration and comparison interface will be triggered.
Face Rotation Angle	The rotation angle tolerance of a face for facial template registration and comparison. If a face's rotation angle exceeds this set value, it will be filtered by the algorithm, i.e. ignored by the terminal thus no registration and comparison interface will be triggered.
Image Quality	Image quality for facial registration and comparison. The higher the value, the clearer the image requires.

Minimum Face Size	Required for facial registration and comparison. If 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 understood as the face comparison distance. The farther the person is, the smaller the face is, and the smaller the face pixel will be obtained by the algorithm. Therefore, adjusting this parameter can adjust the furthest comparison distance of faces. When the value is 0, the face comparison distance is not limited.
LED Light Triggered Threshold	This value controls the on and off of the LED light. The larger the value, the more frequently the LED light will be turned on.
Motion Detection Sensitivity	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	Helping to judge 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.
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 facial template update.
Notes	Improper adjustment of the exposure and quality parameters may severely affect the performance of the device. Please adjust the exposure parameter only under the guidance of the after-sales service personnel of our company.

6.4 Palm Parameters

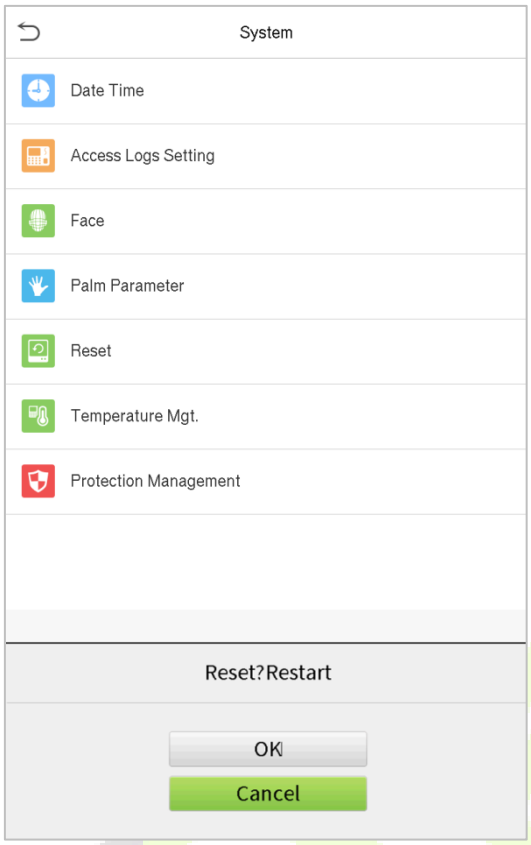
Click **Palm** on the System interface.

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

6.5 Factory Reset

Restore the device, such as communication settings and system settings, to factory settings (Do not clear registered user data).

Click **Reset** on the System interface.

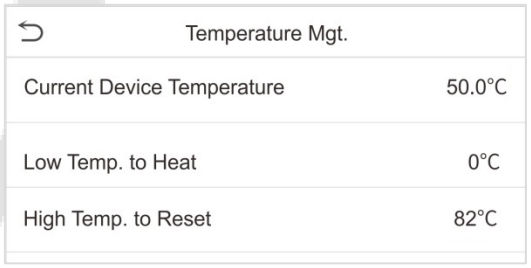


Click **OK** to reset.

6.6 Temperature Management

Terminal has built-in temperature sensor, when the temperature is too low or too high, it will trigger self-heating or shut down.

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

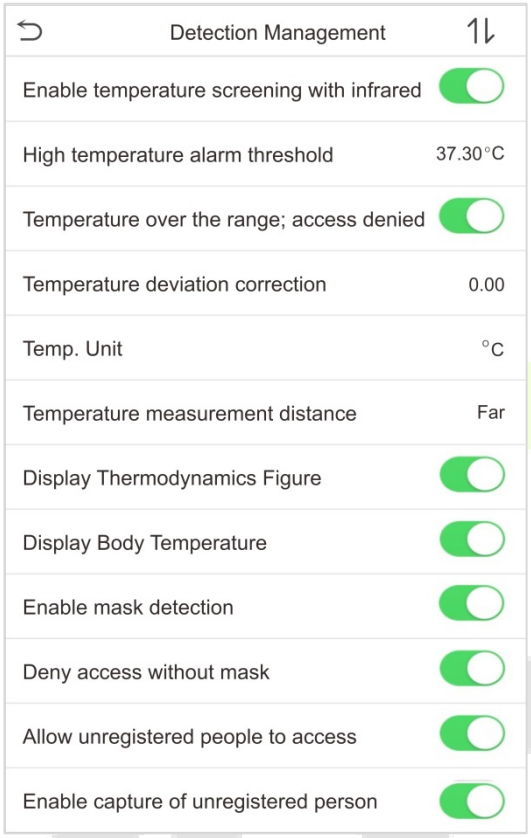


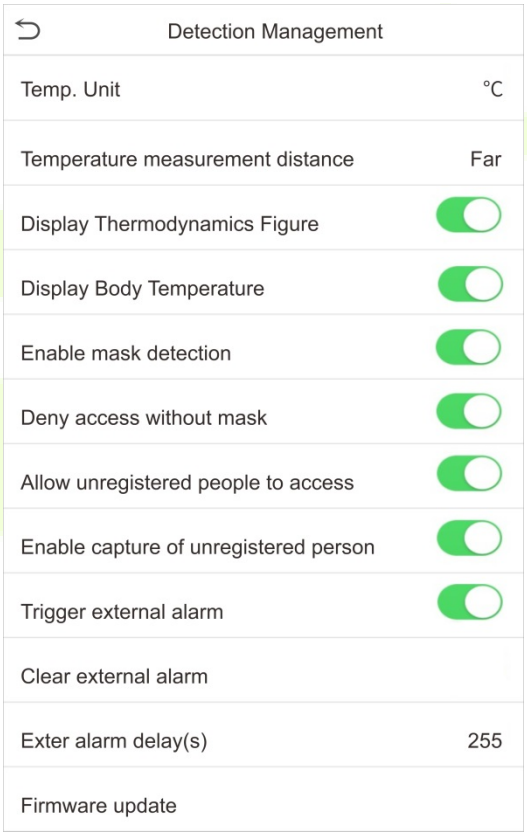
Item	Description
Current Device Temperature	This column shows real time inner temperature of the terminal.
Low Temp. to Heat	Once terminal temperature is lower than set value, terminal will start self-heating, the set range is 0~10(°C).

High Temp. to Reset	When the terminal temperature is high than set value, it will shut down automatically to protect hardware, the set range is 60~80 (℃).

6.7 Detection Management

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





Item	Description
Enable temperature screening with infrared	To enable or disable the infrared temperature measurement function. When this function is enabled, before access 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.

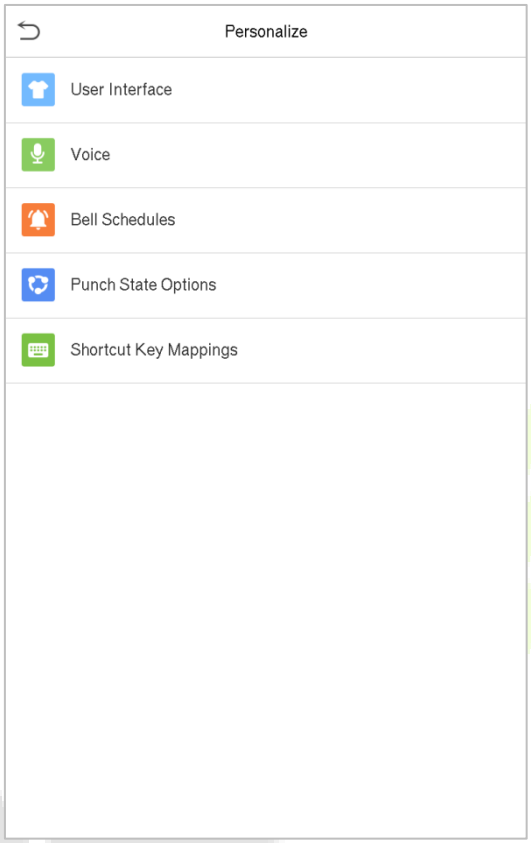
High temperature alarm threshold	To set the value of the alarm threshold of high body temperature. When the temperature measured during verification is higher than the set value, the device will give a prompt and audio alarm. The default alarm threshold is 37.30°C.
Temperature over the range; access denied	When this's 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's 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 Temperature Figure	To enable or disable the display temperature figure function. When enabled, during the detection process, the thermal image of the person will be displayed in the upper left corner of the device.
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.
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 value or the mask detection is enabled, but the mask is not worn, it will trigger an alarm.
Clear external alarm	Clear the triggered alarm records of the device.
External alarm delay(s)	The delay (s) time for triggering an external alarm can be set in seconds, users may disable the function or set a valid value between 1 to 255.
Firmware update	Choose whether to update the thermal imaging temperature detection module software version.

7 Personalize Settings

You may customize interface settings, audio and bell.

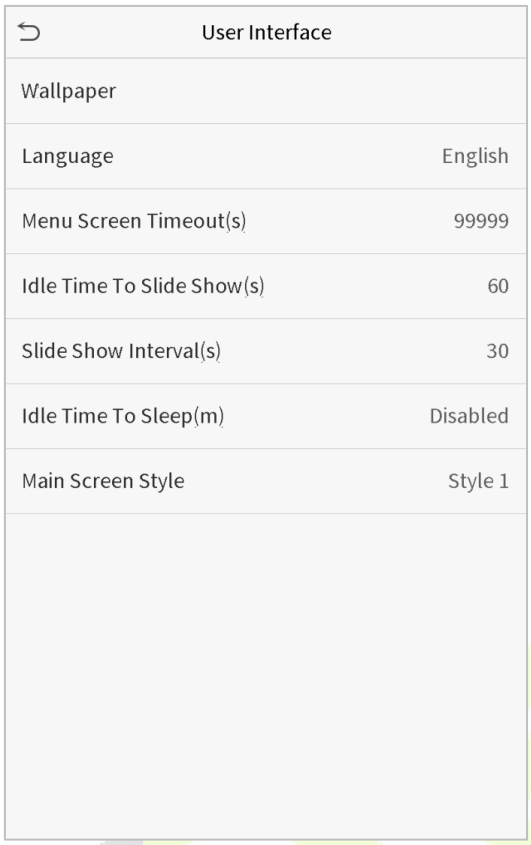
Click **Personalize** on the main menu interface.



7.1 Interface Settings

You can customize the display style of the main interface.

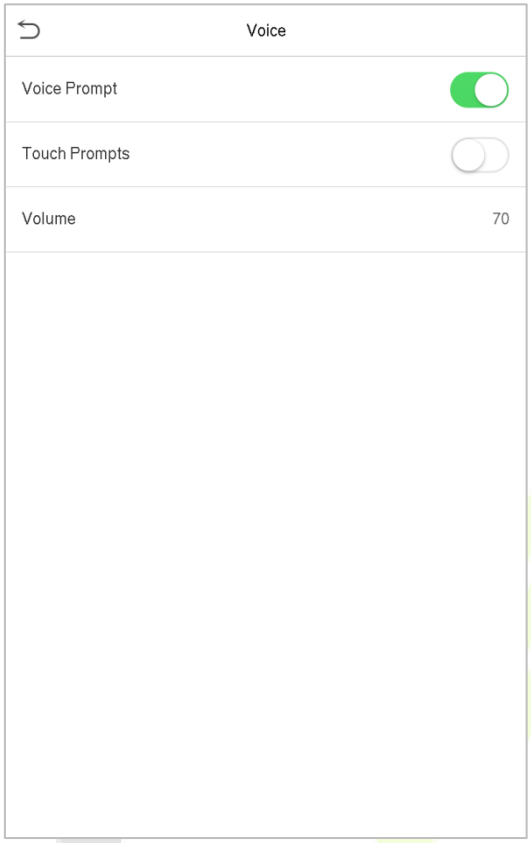
Click **User Interface** on the Personalize interface.



Item	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. Press any key or finger to resume normal working mode. You can disable this function or set a value within 1-999 minutes.
Main Screen Style	To select the main screen style according to your personal preference.

7.2 Voice Settings

Click **Voice** on the Personalize interface.



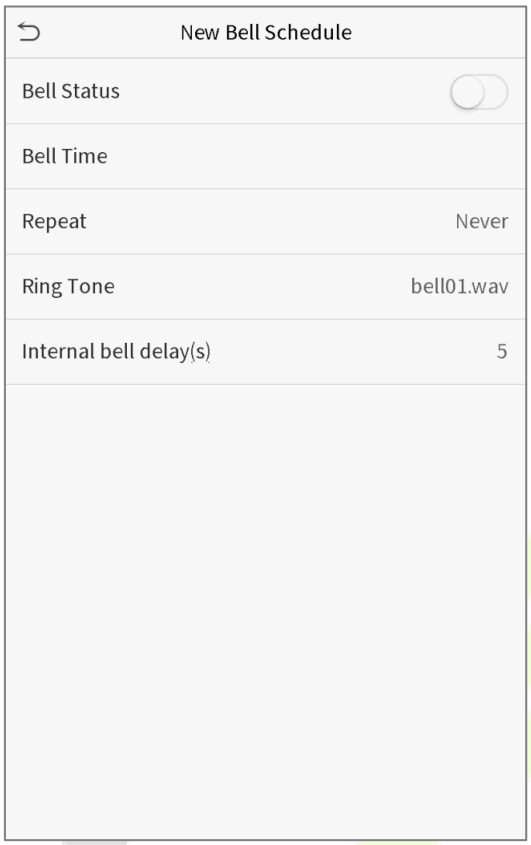
Item	Description
Voice Prompt	Select whether to enable voice prompts during operating.
Touch Prompt	Select whether to enable keypad sounds.
Volume	Adjust the volume of the device; valid value: 0-100.

7.3 Bell Schedules

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

- **Add a bell**

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



Item	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.

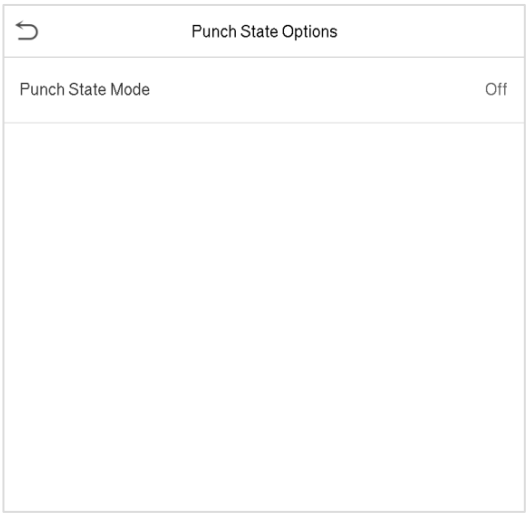
- **Delete a bell**

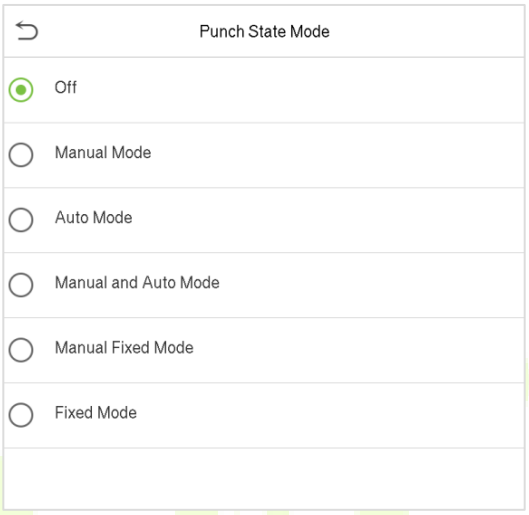
On the All Bell Schedules interface, tap the bell to be deleted.

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

7.4 Punch States Options

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



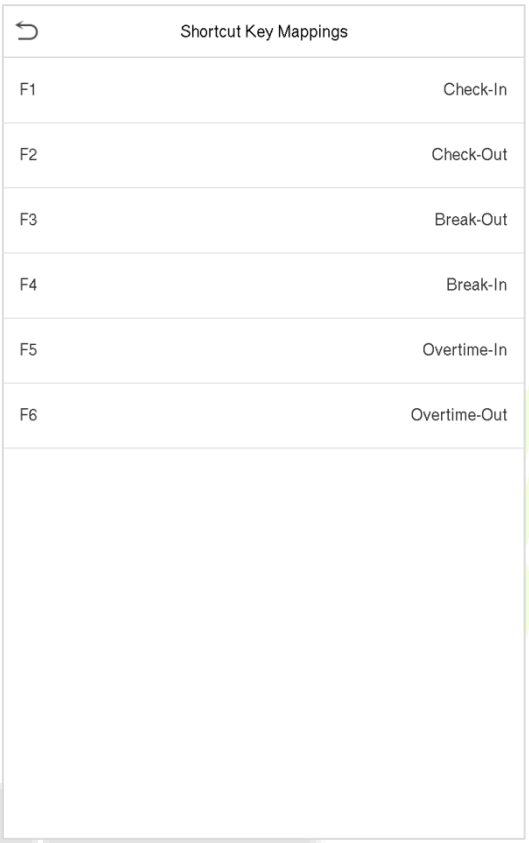


Item	Description
Punch State Mode	Select a punch state mode, which can be: **Off:** To disable the punch state key function. The punch state key set under **Shortcut Key Mappings** menu will become invalid. **Manual Mode:** To switch the punch state key manually, and the punch state key will disappear 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. **Manal 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 timeout, the manually switching punch state key will become auto-switching punch state key. **Manual Fixed Mode:** After 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.

7.5 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.

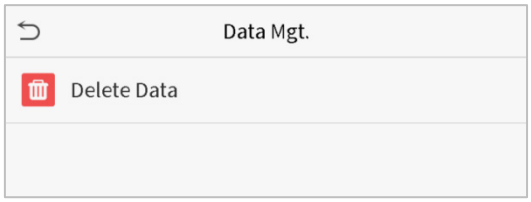
Click **Shortcut Key Mappings** on the Personalize interface.



8 Data Management

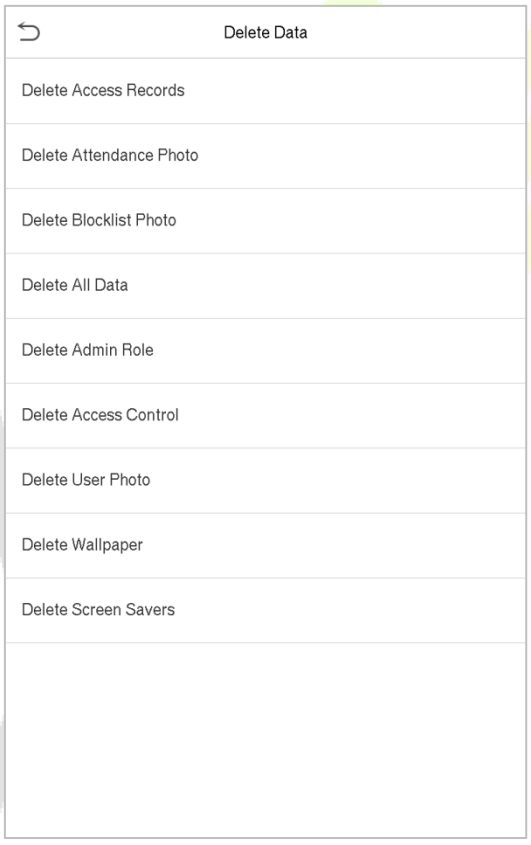
To delete the relevant data in the device.

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



8.1 Delete Data

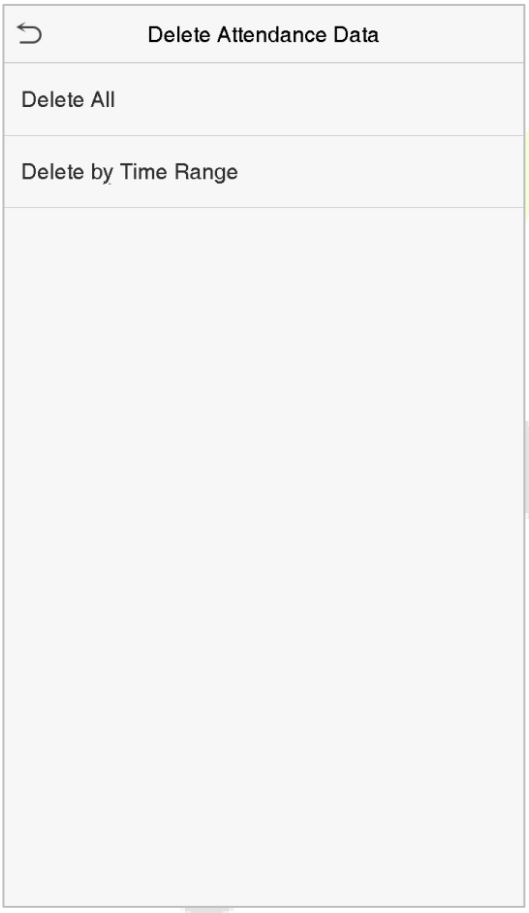
Click **Delete Data** on the Data Mgt. interface.



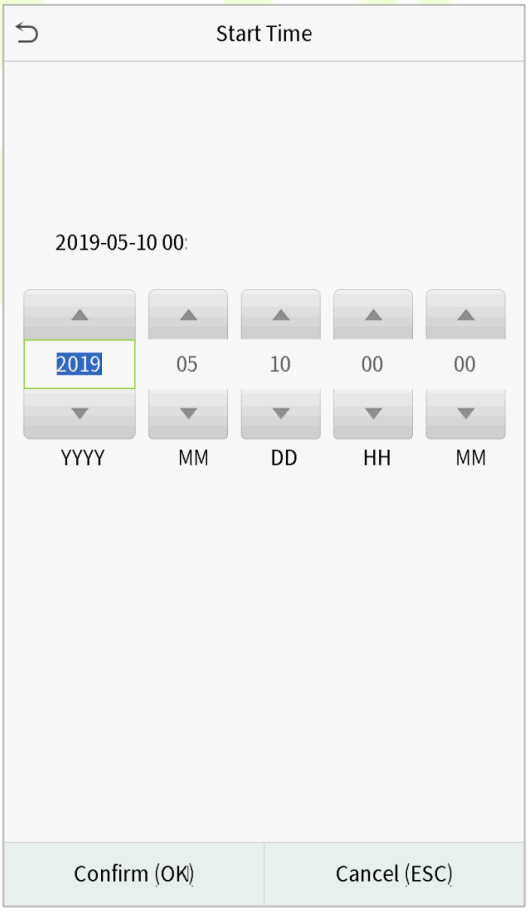
Item	Description
Delete Access Records	To delete attendance data/access records conditionally.
Delete Attendance Photo	To delete attendance photos of designated personnel.
Delete Blocklist Photo	To delete the photos taken during verifications which are failed.

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

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.

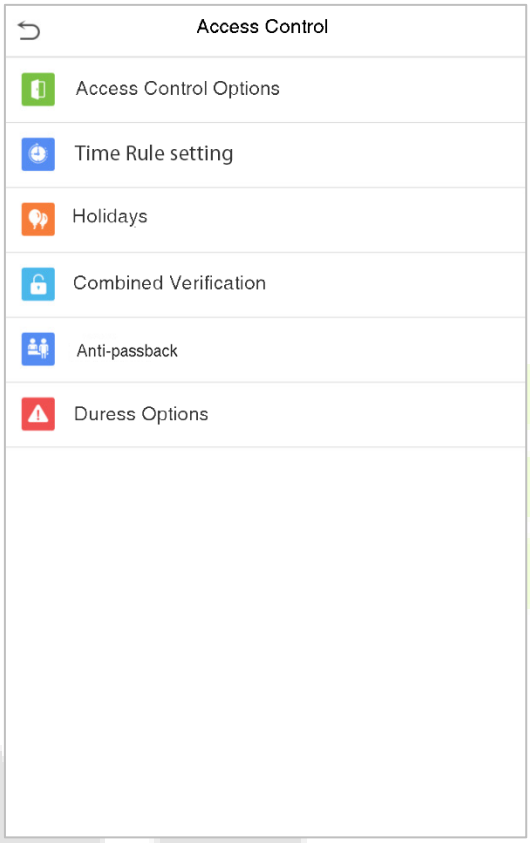


Set the time range and click OK.

9 Access Control

Access Control is used to set the schedule of door opening, locks 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:

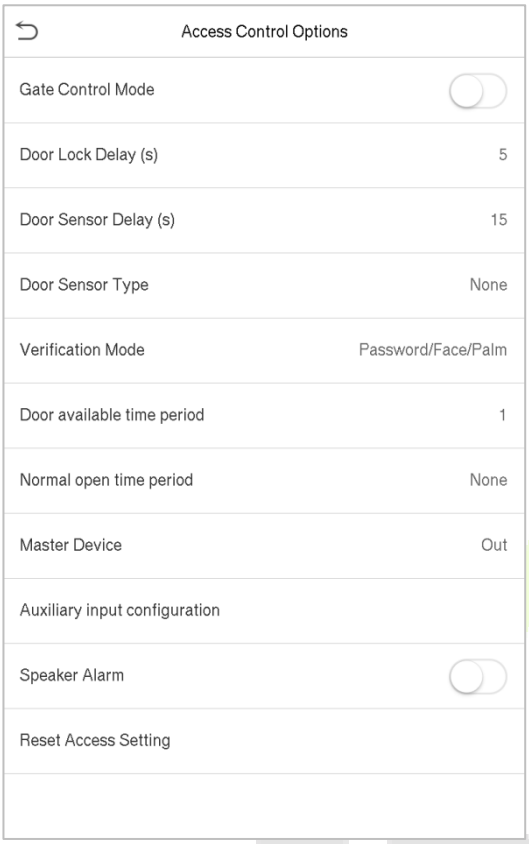
1. The current door unlock time should be within any valid time zone of the user time period.
2. The user's group must be in the door unlock combination (when there are other groups in the same access combo, verification of members of those groups are also required to unlock the door).

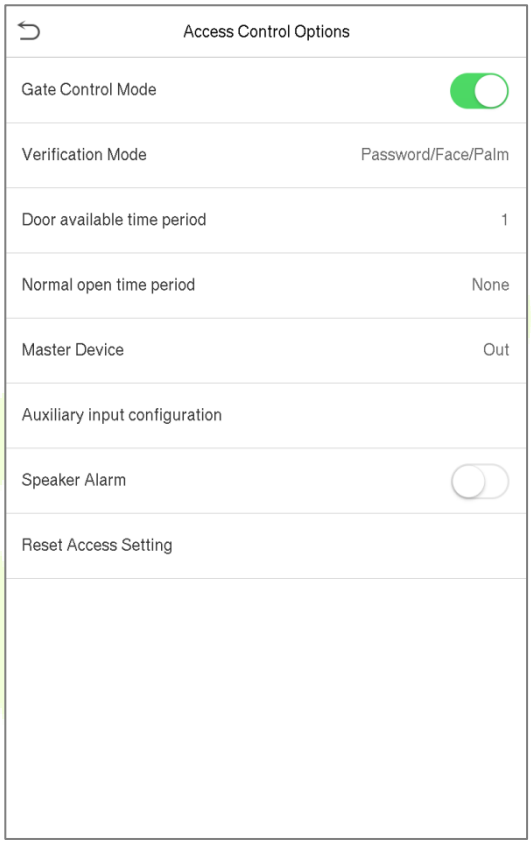
In default settings, new users are allocated into the first group with the default group time zone and access combo as "1" and set in unlocking state.

9.1 Access Control Options

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

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





Item	Description
GateControl Mode	Whether to turn on the gate control mode or not, when set to ON, on this interface will remove Door lock relay, Door sensor relay and Door sensor type function.
Door Lock Delay (s)	The length of time that the device controls the electric lock to be unlock. Valid value: 1~10 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.

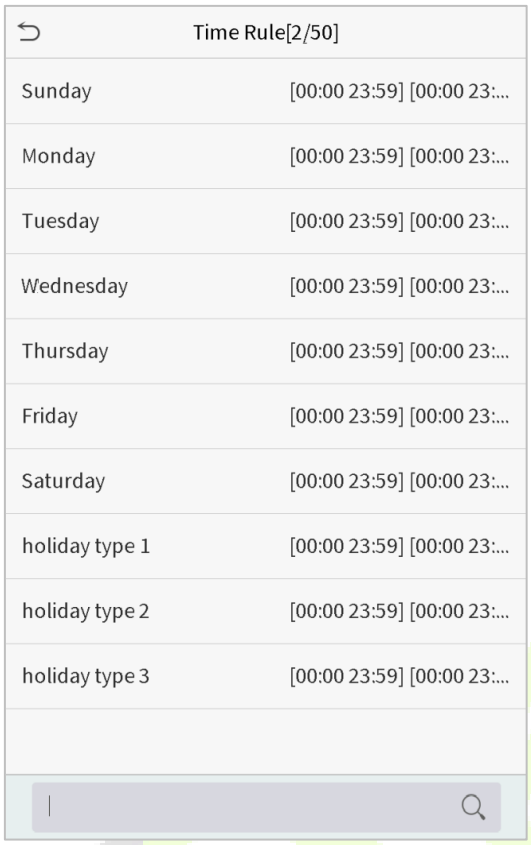
Verification Mode	The supported verification mode includes password/face, User ID only, password, face only, and face + password.
Door available time period	To set time period for door, so that the door is available only during this.
Normal open time Period	Scheduled time period for "Normal Open" mode, 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 disassembly alarm from the local. When the door is closed or the verification is successful, the system will cancel the alarm from the local.
Reset Access Setting	The 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, erased access control data in Data Mgt. is excluded.

9.2 Time Rule setting

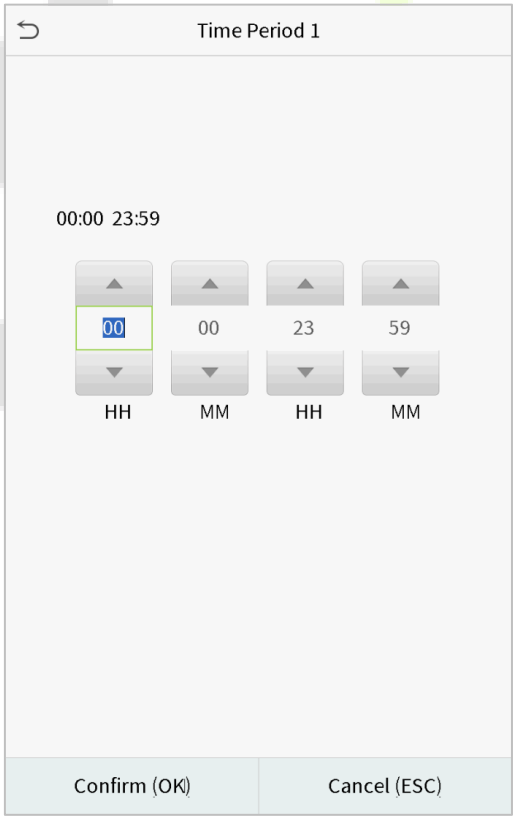
The entire system can define up to 50 time rules. Each time rule represents ten time zones, i.e. one week and 3 holidays, and each time zone is a valid time period within 24 hours per day. You may set a maximum of 3 time periods for every time zone. The relationship among these time periods is "or". 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.



Notes:

1）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.

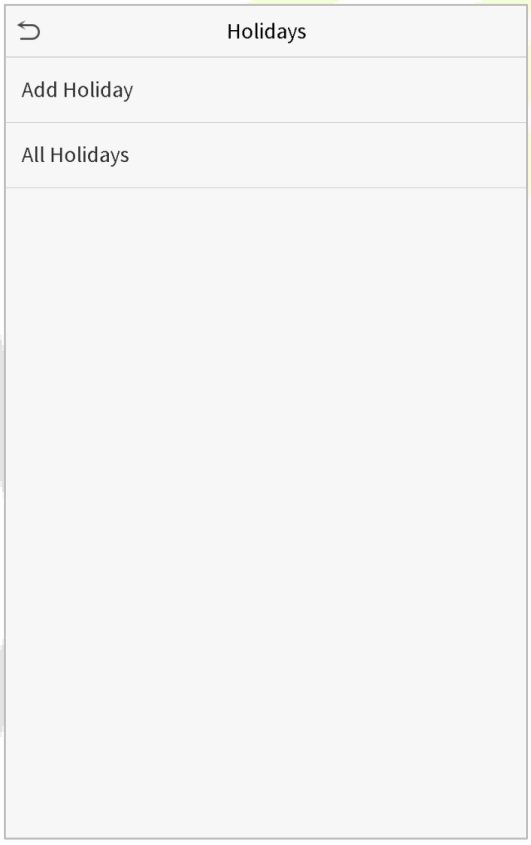
2）The effective time period to unlock the door: open all day (00:00~23:59) or when the ending time is later than the starting time, such as 08:00~23:59.

3）The default time zone 1 indicates that door is open all day long.

9.3 Holiday Settings

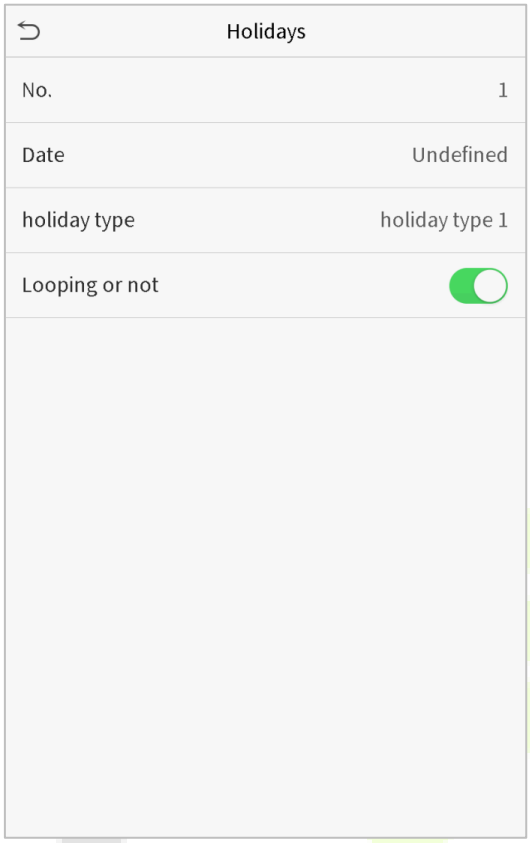
Whenever there is a holiday, you may need a special access time; but changing everyone's access time one by one is extremely cumbersome, so you can set a holiday access time which is applicable to all employees, and the user will be able to open the door during the holidays.

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**

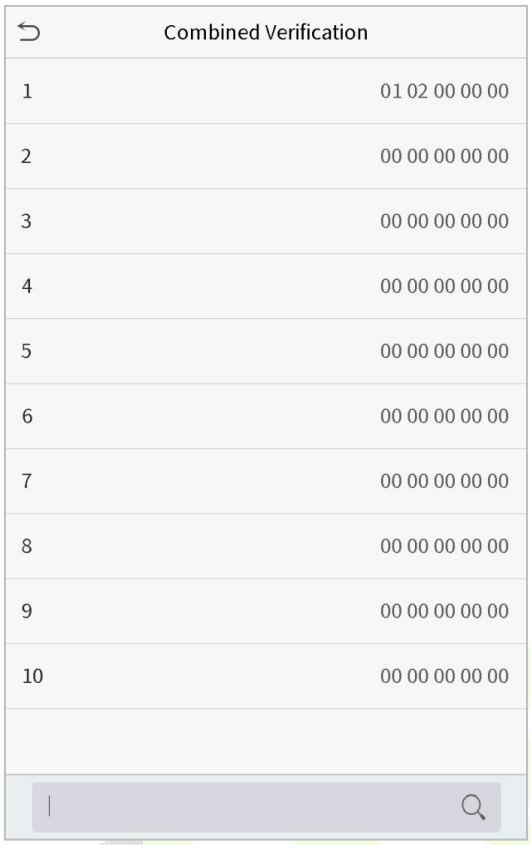
On the Holidays interface, select a holiday item to be deleted and click Delete. Click OK to confirm deletion. After deletion, this holiday is no longer displayed on All Holidays interface.

9.4 Combined Verification Settings

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

In a door-unlocking combination, the range of the combined number N is: $0 \leq N \leq 5$, and the number of members N may all belong to one access group or may belong to five different access groups.

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.

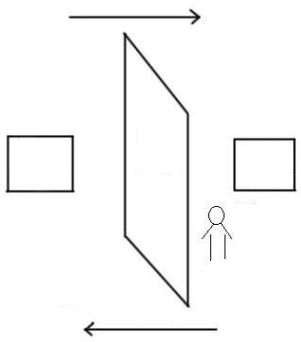
Delete a door-unlocking combination

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

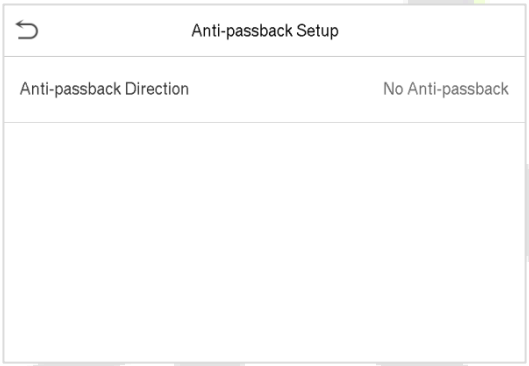
9.5 Anti-passback Setup

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.



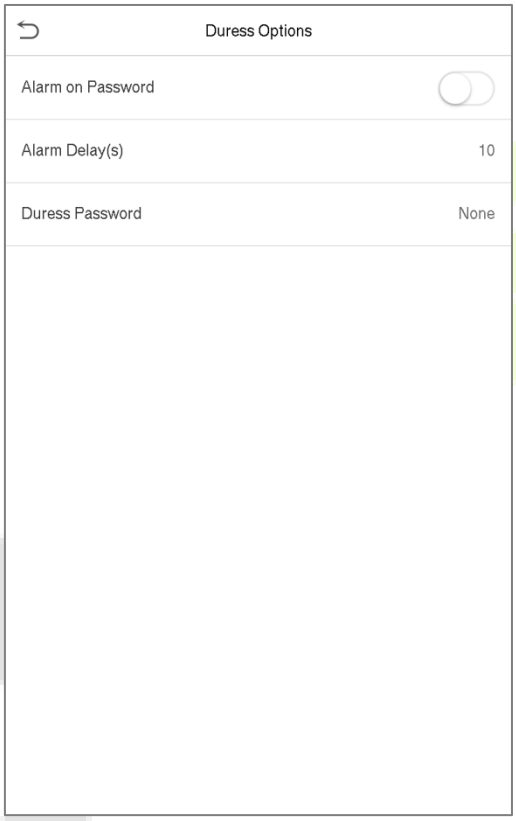
Item	Description
Anti-passback direction	**No Anti-passback:** Anti-passback function is disabled, which means successful verification through either master device or slave device can unlock the door. Attendance state is not saved. **Out Anti-passback:** After a user checks out, only if the last record 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.

9.6 Duress Options Settings

If a user activated the duress verification function with specific authentication method(s), when he/she is under coercion 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.

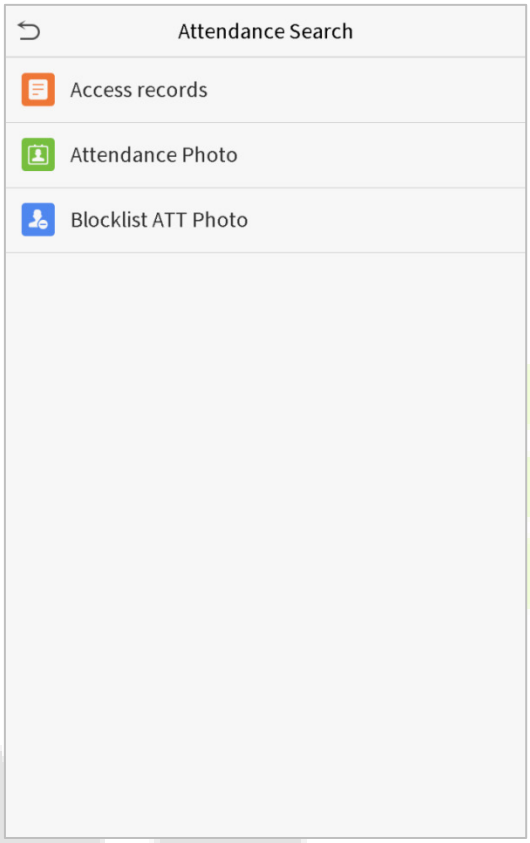


Item	Description
Alarm on Password	When a user uses the password verification method, an alarm signal will be generated, otherwise there will be no alarm signal.
Alarm Delay (s)	Alarm signal will not be transmitted until the alarm delay time is elapsed. The value ranges from 1 to 999 seconds.
Duress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

10 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.

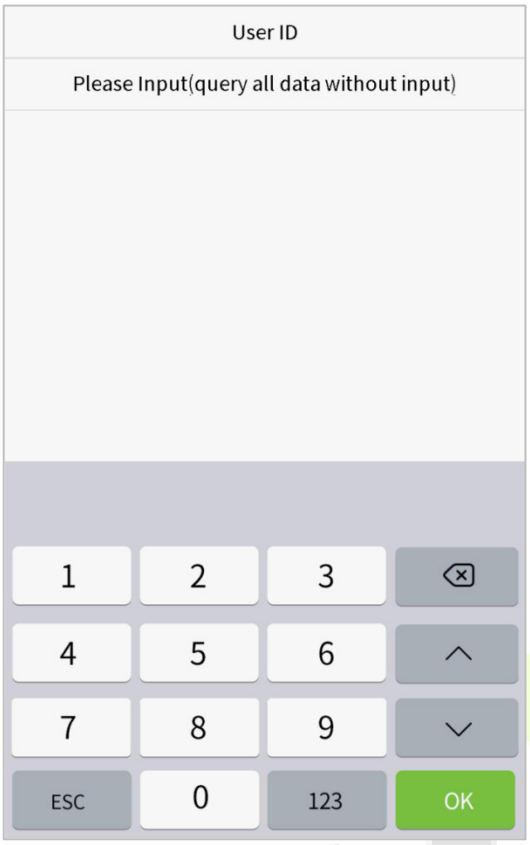
Click **Attendance Search** on the main menu interface.



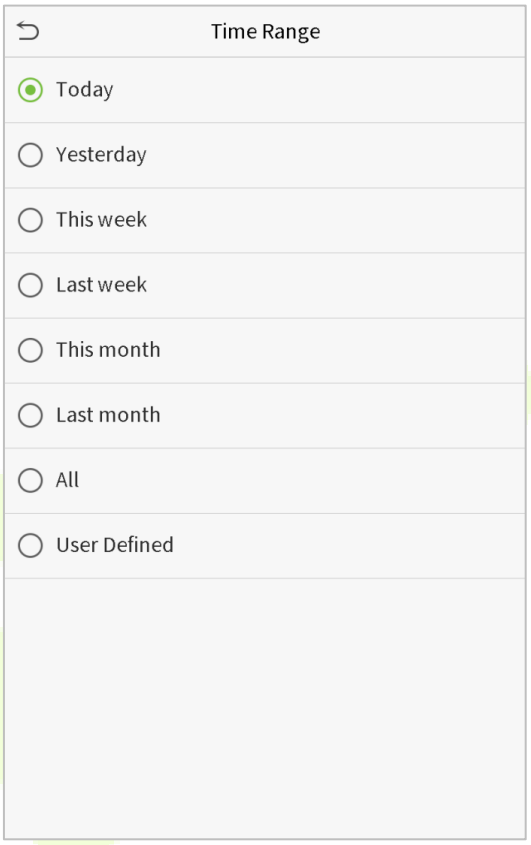
The process of searching for attendance and blocklist photos is similar to that of searching for access records. The following is an example of searching for access records.

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

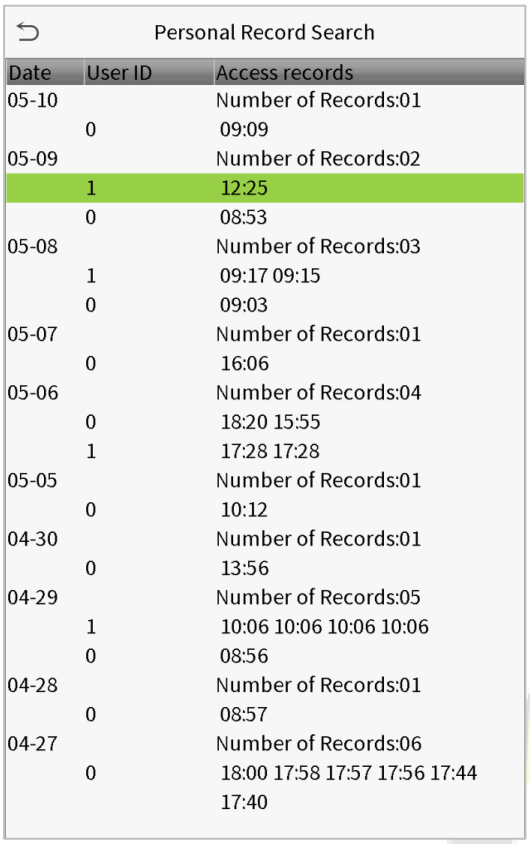
1. Enter the user ID to be searched and click OK. If you want to search for records of all users, click OK without entering any user ID.



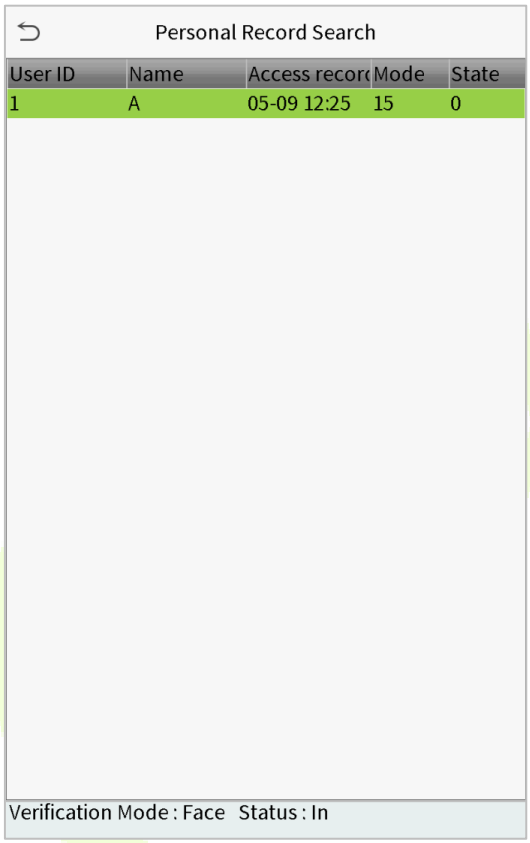
2. Select the time range in which the records you want to search for.



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



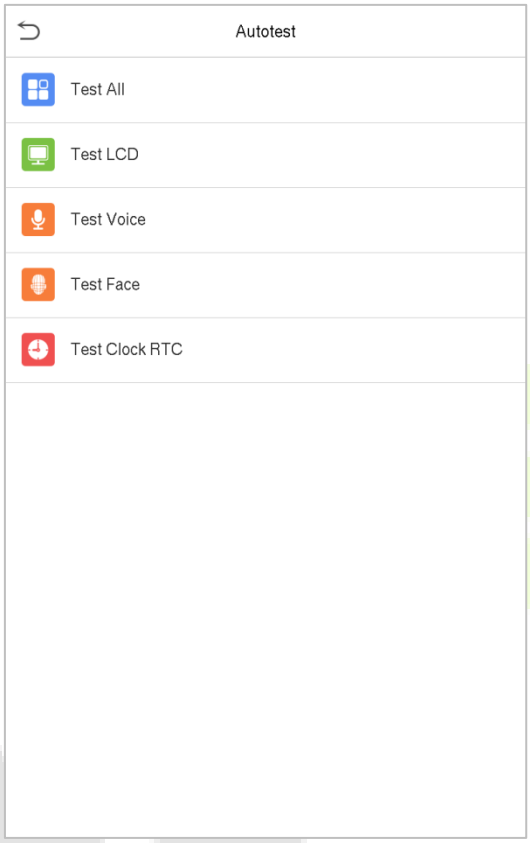
4. The below figure shows the details of the selected record.



11 Autotest

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

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

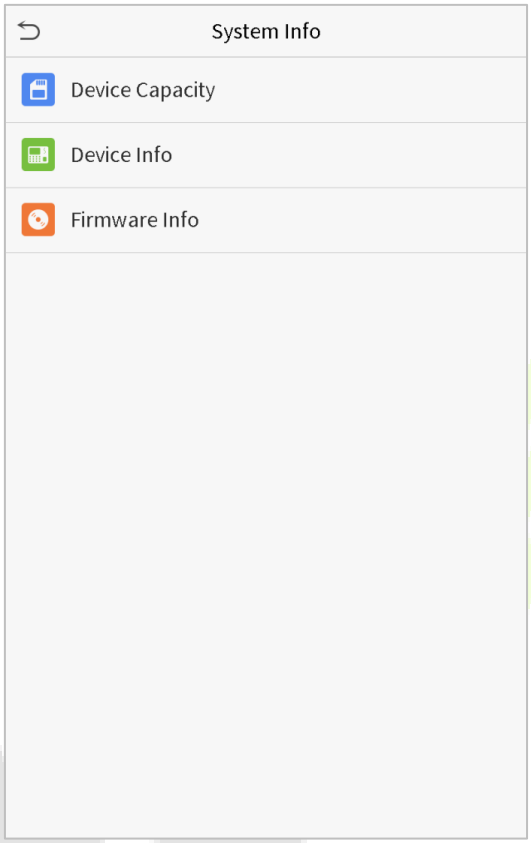


Item	Description
Test All	To automatically test whether the LCD, audio, camera and RTC are normal.
Test LCD	To automatically test the display effect of LCD screen by displaying full-color, pure white, and pure black to check whether the screen displays colors normally.
Test Voice	To automatically test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

12 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.



Item	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.
Firmware Info	Displays the firmware version and other version information of the device.

13 Connect to ZKBioSecurity MTD Software

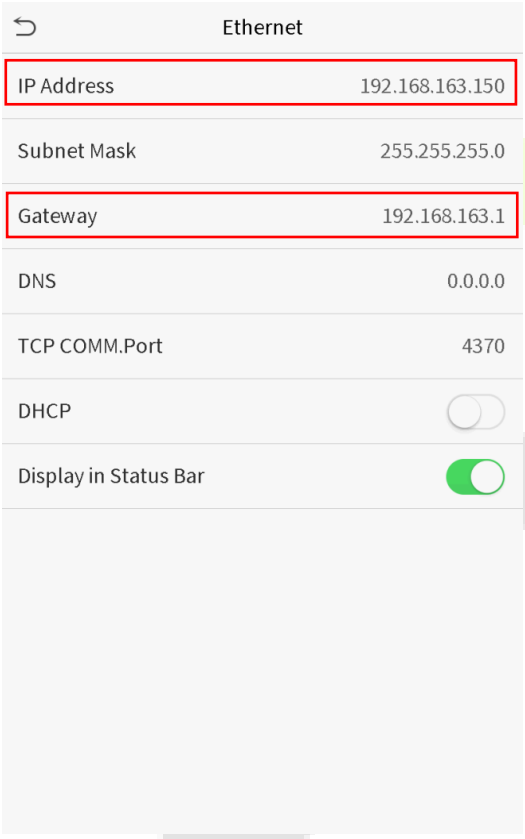
13.1 Set the Communication Address

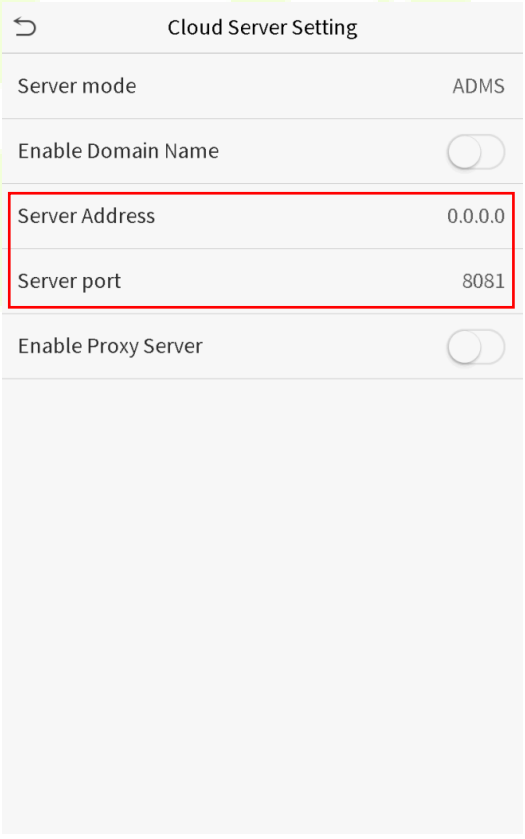
- **Device side**

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.

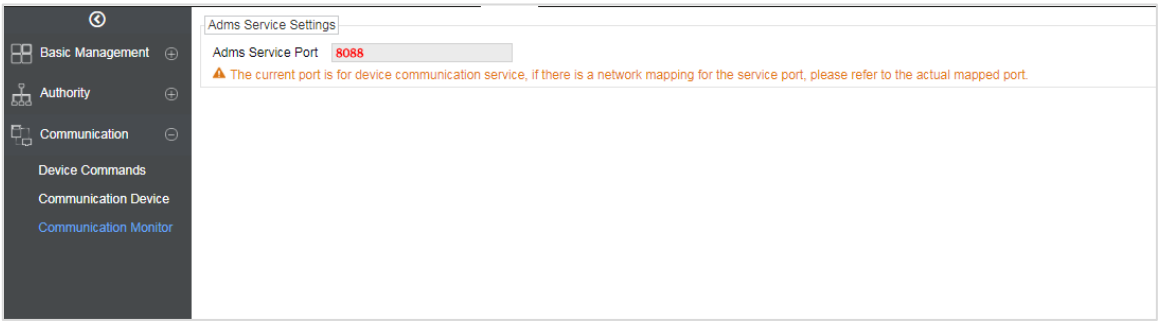
Server port: Set as the service port of ZKBioSecurity MTD (The default is 8088).





- **Software side**

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



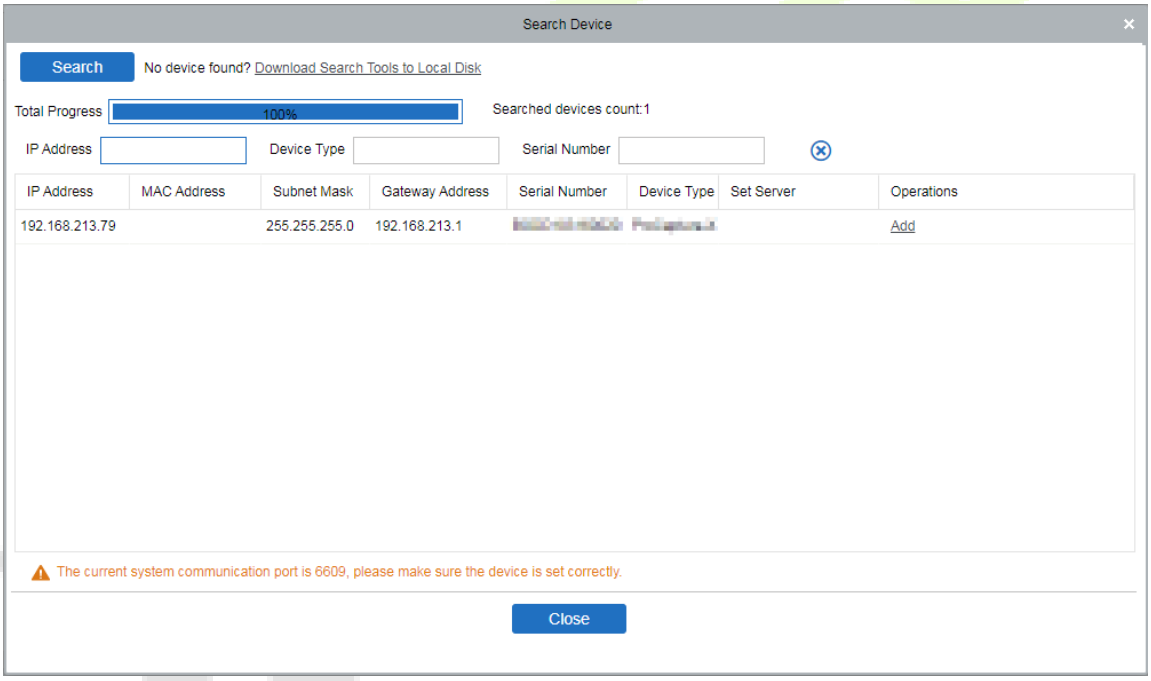
13.2 Add Device on the Software

Add 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**……].

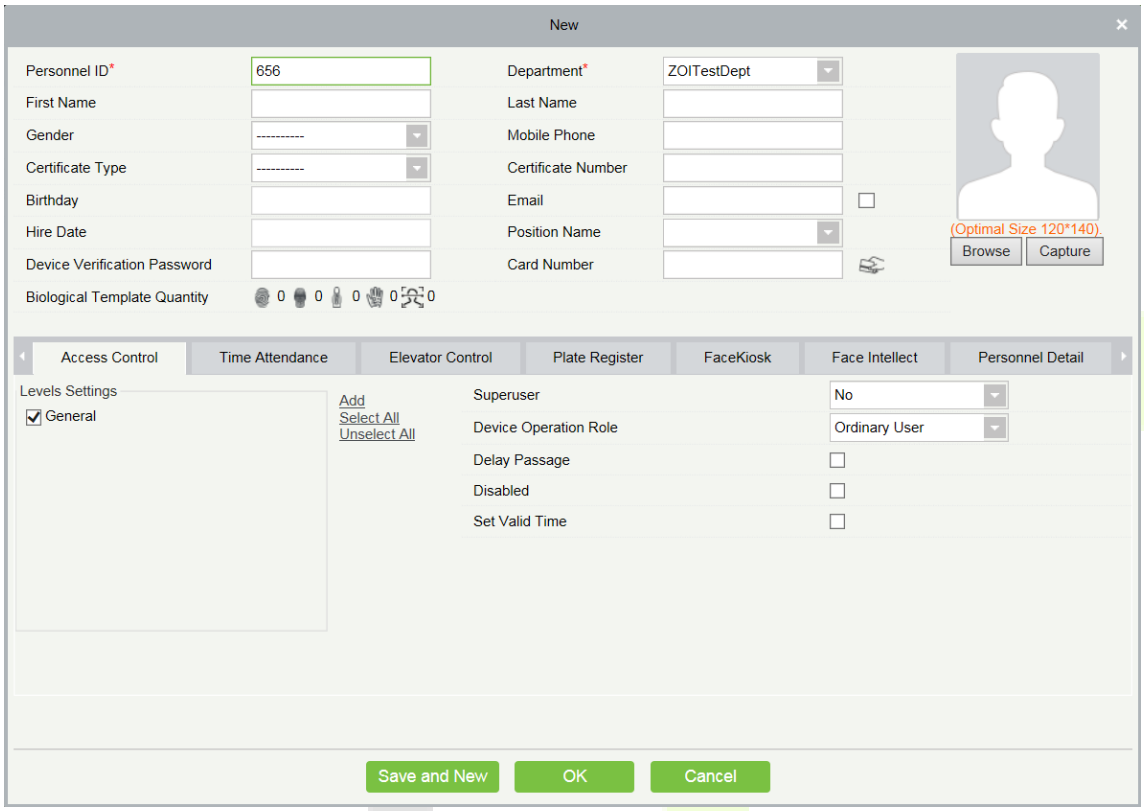
3) After searching, the list and total number of access controllers will be displayed.



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

13.3 Add Personnel on the Software

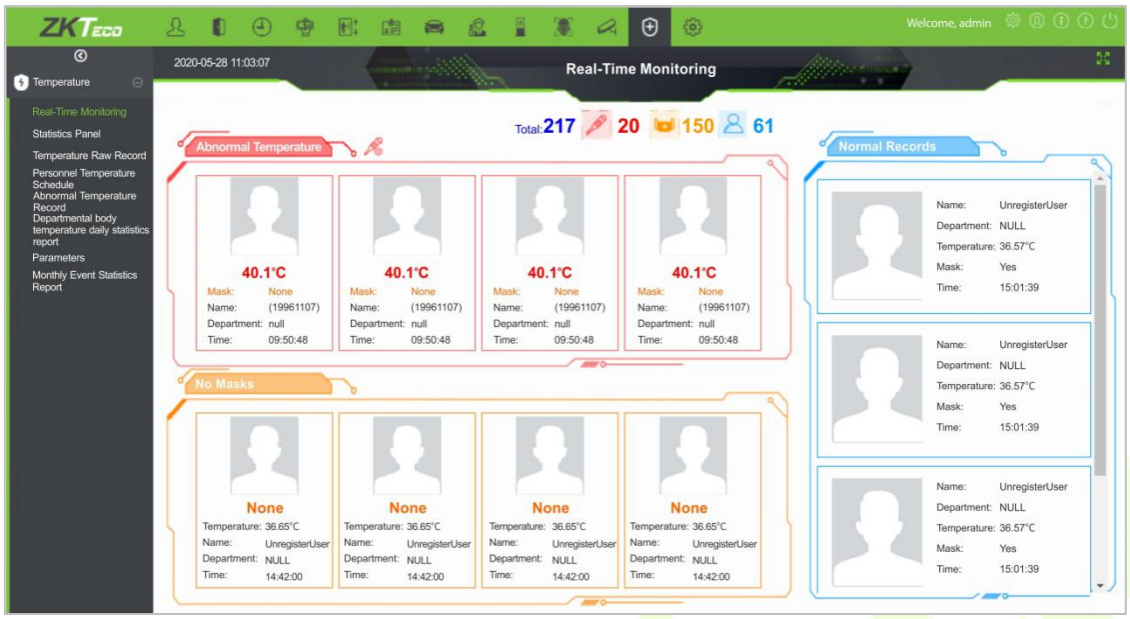
1. Click **Personnel** > **Person** > **New**:



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

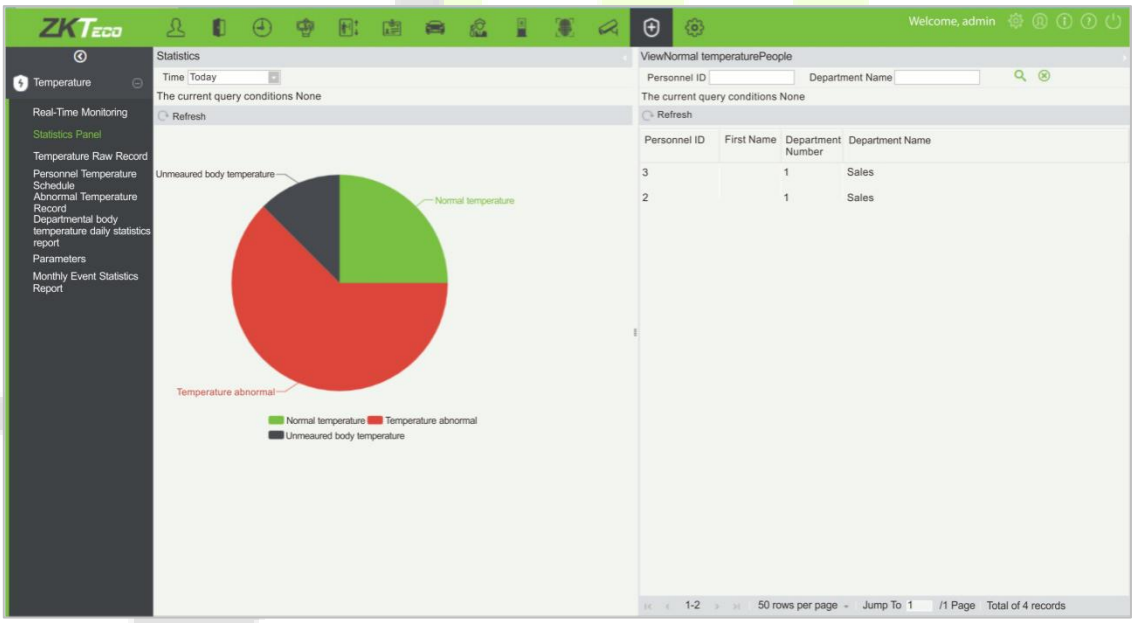
13.4 Real-time monitoring on the Software

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 to *ZKBioSecurity MTD User Manual*.

Appendix 1

Requirements of Live Collection and Registration of Visible Light Face Images

1) It is recommended to perform registration in an indoor environment with an appropriate light source without underexposure or overexposure.

2) Do not shoot towards outdoor light sources like door or window or other strong light sources.

3) Dark-color apparels which are different from the background color are recommended for registration.

4) Please show your face and forehead, and do not cover your face and eyebrows with your hair.

5) It is recommended to show a plain facial expression. Smile is acceptable, but do not close your eyes, or incline your head to any orientation. Two images are required for persons with eyeglasses, one image with eyeglasses and one other without.

6) Do not wear accessories like scarf or mask that may cover your mouth or chin.

7) Please face right towards the capturing device, and locate your face in the image capturing area as shown in Image 1.

8) Do not include more than one face in the capturing area.

9) 50cm - 80cm is recommended for capturing distance adjustable subject to body height.

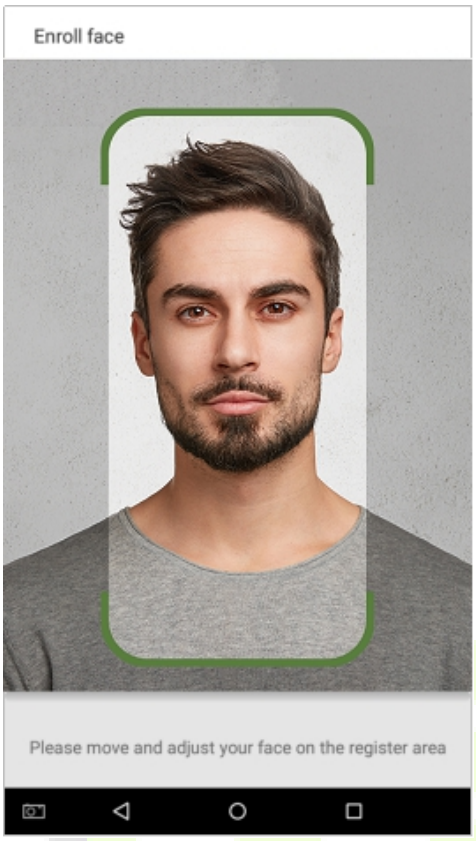


Image1 Face Capture Area

Requirements for Visible Light Digital Face Image Data

Digital photo should be straightly edged, colored, half-portrayed with only one person, and the person should be uncharted and not in uniform. Persons who wear eyeglasses should remain to put on eyeglasses for photo capturing.

- **Eye Distance**

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

- **Facial Expression**

Plain face or smile with eyes naturally open are recommended.

- **Gesture and Angel**

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

- **Accessories**

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

- **Face**

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

- **Image Format**

Should be in BMP, JPG or JPEG.

- **Data Requirement**

Should comply with the following requirements:

1) White background with dark-colored apparel.

2) 24bit true color mode.

3) JPG format compressed image with not more than 20kb size.

4) Definition rate between 358 x 441 to 1080 x 1920.

5) The vertical scale of head and body should be 2:1.

6) The photo should include the captured person's shoulders at the same horizontal level.

7) The captured person should be eyes-open and with clearly seen iris.

8) Plain face or smile is preferred, showing teeth is not preferred.

9) The captured person should be clearly seen, natural in color, and without image obvious twist, no shadow, light spot or reflection in face or background, and appropriate contrast and lightness level.

Appendix 2

Statement on the Right to Privacy

Dear Customers:

Thank you for choosing this hybrid biometric recognition product, which was designed and manufactured by ZKTeco. As a world-renowned provider of core biometric recognition technologies, we are constantly developing and researching new products, and strive to follow the privacy laws of each country in which our products are sold.

We Declare That:

1. All of our civilian fingerprint recognition devices capture only characteristics, not fingerprint images, and do not involve privacy protection.
2. None of the fingerprint characteristics that we capture can be used to reconstruct an image of the original fingerprint, and do not involve privacy protection.
3. As the provider of this device, we will assume no direct or indirect responsibility for any consequences that may result from your use of this device.
4. If you would like to dispute human rights or privacy issues concerning your use of our product, please directly contact your dealer.

Our other law-enforcement fingerprint devices or development tools can capture the original images of citizen's fingerprints. As to whether or not this constitutes an infringement of your rights, please contact your Government or the final supplier of the device. As the manufacturer of the device, we will assume no legal liability.

Note:

The Chineselaw includes the following provisions on the personal freedom of its citizens:

1. There shall be no illegal arrest, detention, search, or infringement of persons;
2. Personal dignity is related to personal freedom and shall not be infringed upon;
3. A citizen's house may not be infringed upon;
4. A citizen's right to communication and the confidentiality of that communication is protected by the law.

As a final point, we would like to further emphasize that biometric recognition is an advanced technology that will be certainly used in E-commerce, banking, insurance, judicial, and other sectors in the future. Every year the world is subjected to major losses due to the insecure nature of passwords. The Biometric products serve to protect your identity in high-security environments.

Eco-friendly Operation

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

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

Hazardous or Toxic substances and their quantities

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

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

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

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

1600 Union Hill Rd. Alpharetta GA, 30005

Phone : 862 505 2101

info@zktecousa.com

www.zktecousa.com