

# User Manual

## Elite Series[TI]

Date: May 2021

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](http://www.zkteco.com).

## Copyright © 2021 ZKTECO CO., LTD. All rights reserved.

Without the prior written consent of ZKTeco, no portion of this manual can be copied or forwarded in any way or form. All parts of this manual belong to ZKTeco and its subsidiaries (hereinafter the "Company" or "ZKTeco").

## 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 product. The copyright in all the documents, drawings, etc. in relation to the ZKTeco supplied product 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 product. 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 product.

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/product. It is further essential for the safe operation of the machine/unit/product 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/product. The said additions or amendments are meant for improvement /better operations of the machine/unit/product 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/product malfunctions due to any non-compliance of the instructions contained in this manual (ii) in case of operation of the machine/unit/product beyond the rate limits (iii) in case of operation of the machine and production 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. 26, 188 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](mailto:sales@zkteco.com).

To know more about our global branches, visit [www.zkteco.com](http://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 Elite Series[TI] 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 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

<b>1</b>	<b>OVERVIEW.....</b>	<b>8</b>
<b>2</b>	<b>FEATURES .....</b>	<b>8</b>
<b>3</b>	<b>TECHNICAL SPECIFICATIONS.....</b>	<b>9</b>
<b>4</b>	<b>COMPONENTS AND CONNECTION.....</b>	<b>11</b>
<b>5</b>	<b>INSTALLATION REQUIREMENTS.....</b>	<b>12</b>
5.1	STANDING POSITION, FACIAL EXPRESSION AND STANDING POSTURE .....	12
<b>6</b>	<b>FACE REGISTRATION.....</b>	<b>14</b>
<b>7</b>	<b>HOME SCREEN .....</b>	<b>15</b>
7.1	VIRTUAL KEYBOARD.....	16
<b>8</b>	<b>VERIFICATION MODES .....</b>	<b>17</b>
8.1	PASSWORD VERIFICATION.....	17
8.2	FACIAL VERIFICATION.....	21
8.2.1	COMBINED VERIFICATION.....	26
<b>9</b>	<b>MAIN MENU .....</b>	<b>27</b>
<b>10</b>	<b>USER MANAGEMENT .....</b>	<b>28</b>
10.1	ADD USERS.....	28
10.2	SEARCH USERS.....	33
10.3	EDIT USERS.....	34
10.4	DELETE USERS .....	34
<b>11</b>	<b>USER ROLE .....</b>	<b>34</b>
<b>12</b>	<b>COMMUNICATION SETTINGS.....</b>	<b>37</b>
12.1	NETWORK SETTINGS.....	37
12.2	PC CONNECTION.....	38
12.3	CLOUD SERVER SETTINGS.....	39
12.4	WIEGAND SETUP.....	40
<b>13</b>	<b>SYSTEM SETTINGS .....</b>	<b>43</b>
13.1	DATE AND TIME .....	44
13.2	ACCESS LOGS SETTING.....	45
13.3	FACE PARAMETERS.....	46
13.4	FACTORY RESET .....	49

13.5	TEMPERATURE MANAGEMENT .....	49
13.6	DETECTION MANAGEMENT.....	51
14	<b>PERSONALIZE SETTINGS.....</b>	<b>49</b>
14.1	INTERFACE SETTINGS.....	49
14.2	VOICE SETTINGS.....	50
14.3	BELL SCHEDULES.....	51
14.4	PUNCH STATES OPTIONS.....	52
14.5	SHORTCUT KEYS MAPPINGS .....	53
15	<b>DATA MANAGEMENT .....</b>	<b>54</b>
15.1	DELETE DATA .....	54
16	<b>ACCESS CONTROL.....</b>	<b>56</b>
16.1	ACCESS CONTROL OPTIONS .....	57
16.2	TIME RULE SETTINGS .....	58
16.3	HOLIDAY SETTINGS .....	60
16.4	COMBINED VERIFICATION SETTINGS .....	61
16.5	ANTI-PASSBACK SETUP .....	63
16.6	DURESS OPTIONS SETTINGS .....	65
17	<b>ATTENDANCE SEARCH .....</b>	<b>65</b>
18	<b>AUTOTEST.....</b>	<b>67</b>
19	<b>SYSTEM INFORMATION.....</b>	<b>68</b>
20	<b>CONNECT TO ZKBIOSECURITY MTD SOFTWARE .....</b>	<b>69</b>
20.1	SET THE COMMUNICATION ADDRESS.....	69
20.2	ADD DEVICE TO THE SOFTWARE .....	70
20.3	ADD PERSONNEL ON THE SOFTWARE.....	71
20.4	REAL-TIME MONITORING ON THE SOFTWARE.....	71
APPENDIX 1	.....	73
	REQUIREMENTS OF LIVE DETECTION AND REGISTRATION OF VISIBLE LIGHT FACE IMAGES.....	73
	REQUIREMENTS FOR VISIBLE LIGHT DIGITAL FACE IMAGE DATA.....	74
APPENDIX 2	.....	75
	STATEMENT ON THE RIGHT TO PRIVACY .....	75
	ECO-FRIENDLY OPERATION.....	76

## 1 Overview

Elite Series [TI] is a fully upgraded version of the Elite Series Visible Light facial recognition terminals using intelligent facial recognition algorithms and the latest computer vision technology. It is a high-level facial recognition and Thermal Imaging Temperature Detection terminal supported with ZKTeco's customized powerful CPU and ultra-large capacity of facial templates, a maximum of 50,000 facial templates for 1:N recognition.

Elite Series [TI] adopts the latest touchless recognition technology for temperature detection and masked individual identification, which eliminates hygiene concerns effectively. It is also equipped with an ultimate anti-spoofing algorithm for facial recognition against almost all types of fake photos and videos attack. The device with temperature and mask detection will be a perfect choice to help reduce the risk of infection and germs spreading during the recent global public health issue as well.

Elite Series [TI] enables fast and accurate body temperature measurement and masked individual identification during face verification at all access points, especially in hospitals, factories, schools, commercial buildings, airports, stations, and other public areas.

## 2 Features

- **Large Capacity:** For 1:N facial authentication, the device supports  
Standard: 30,000 templates  
Optional: 50,000 templates
- Incomparable facial recognition speed of 0.3 seconds per face.
- Integrated 125kHz Proximity Card Reader (Optional MiFare).
- 2MP starlight CMOS sensor camera with WDR function, which enables the device to recognize faces in complex lighting environments (0.5 lux to 50,000 lux).
- Anti-spoofing algorithm against print attack (Laser, color and B/W photos), videos attack, and 3D mask attack.
- Smart energy-saving design; an RF detector will wake up the device when it precisely detects the distance between the user and the device is 300cm (9.84ft) or less.
- 8-inch touchscreen with 400 lux, which offers high visibility under strong and direct light.
- Secondary lighting feature with adjustable brightness.
- High-speed temperature detection of 0.1s at a distance of 30cm to 120cm.
- Temperature Measurement Accuracy:  $\pm 0.3^{\circ}\text{C}$  ( $\pm 0.54^{\circ}\text{F}$ ), tested in 80cm (2.63ft) under  $25^{\circ}\text{C}$  ( $77^{\circ}\text{F}$ ) environment.
- Detects and limits access for people not wearing a mask.
- Facial verification with wearing a mask.
- Denied access for personnel with elevated body temperature.

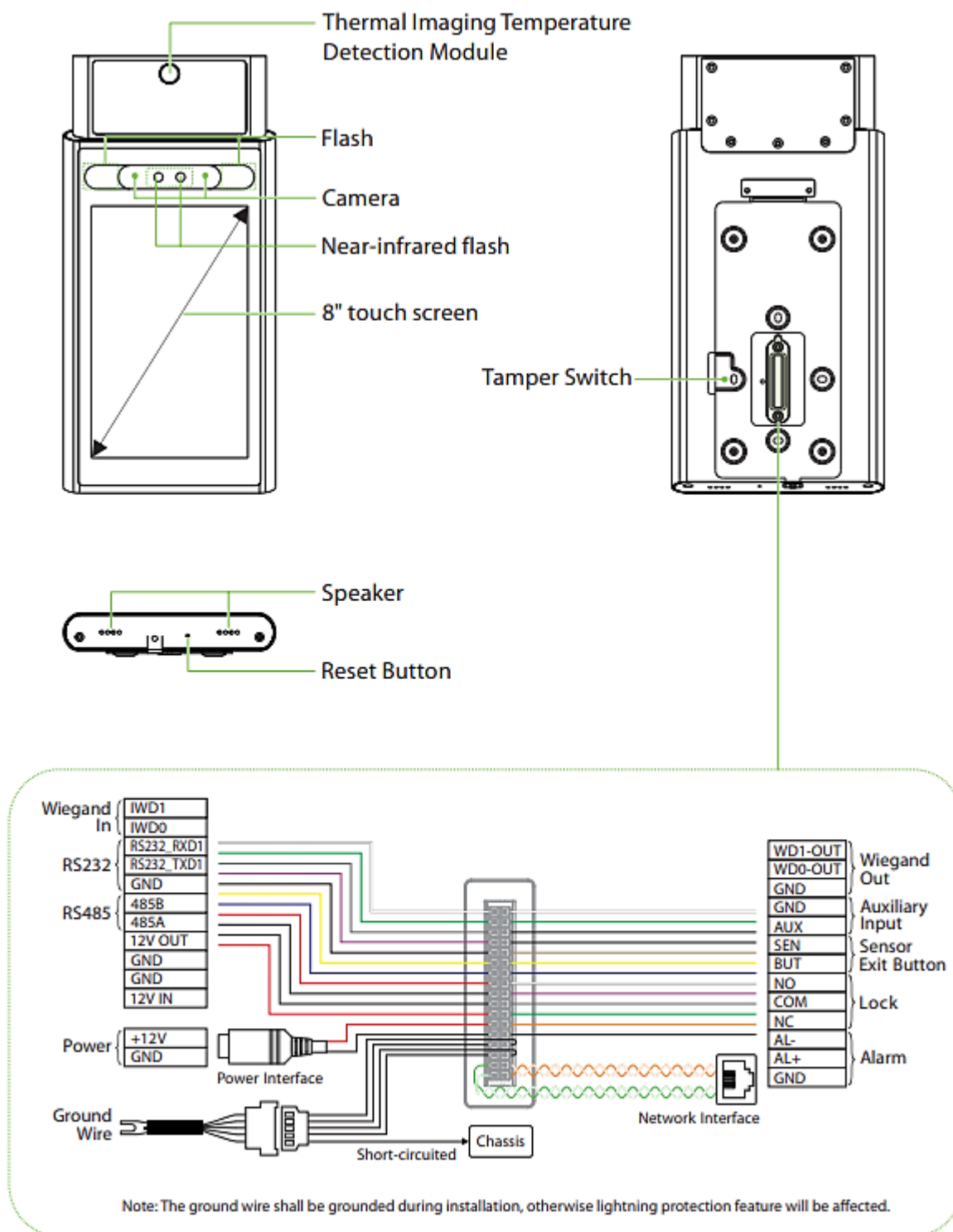
**Note:** The Temperature detection data is only for reference and not for any medical purpose.

### 3 Technical Specifications

Type	Parameter	Description
<b>Capacity</b>	Face Template	30,000(Standard) 50,000(Optional)
	Transactions	1,000,000
	User Photos	20,000
	Event Photos	10,000
<b>Verification</b>	Biometrics	Face
	Access Cards	MiFare Card (13.56 MHz) 125KHz EM FeliCa
<b>General</b>	Processor	900MHz Dual Core Customized CPU
	Memory	8GB Flash and 512MB RAM
	Proximity Sensor	RF Sensor
	LCD Type	8" High Brightness IPS Touch LCD
<b>Environment</b>	Operating Temperature	20°C to 35°C (60°F to 95°F)
	Operating Humidity	≤93%
	Storage Temperature	-40°C to 65°C (-40°F to 149°F)
	Storage Humidity	≤93%
<b>Camera</b>	Camera Type	2MP starlight CMOS sensor camera with WDR
	Camera Resolution	1600 x 1200 pixels
<b>Power</b>	Operating Voltage	12V DC
	Operating Current	<2000mA
<b>Interface</b>	Access Control Interface	1 Lock Relay Output
		Alarm Output / Auxiliary Input
		1 Exit Button / Door Sensor

<b>Functionalities</b>	Standard	Access Levels Groups Holidays Daylight Saving Time (DST) Duress Mode Anti-Passback Record Query Custom Wallpaper & Screen Saver Tamper Switch Alarm
	Significant	High-Speed Facial Recognition (0.3s) Liveness Detection HTTPS Encryption (optional) Event Snapshot
<b>Data Transmission</b>	Communication	TCP / IP RS485 / RS232 ( 1 Host or 1 Slave) 1 Wiegand Input, 1 Wiegand Output Wi-Fi (optional)
<b>Algorithm</b>	Face Algorithm	ZKLiveFace 5.8
<b>Supported Software</b>	ZKBioSecurity	
<b>Certificates</b>	CE, FCC, RoHS	
<b>Detection</b>	Mask Detection	Enabled
	Temperature Detection	Temperature Detection Accuracy: $\pm 0.3^{\circ}\text{C}$ ( $\pm 0.54^{\circ}\text{F}$ ) Temperature Detection Range: $20^{\circ}\text{C}$ to $50^{\circ}\text{C}$ ( $68^{\circ}\text{F}$ to $122^{\circ}\text{F}$ )
<b>Others</b>	Net Weight	Elite Access[TI]: 1.42kg Elite Pass[TI]: 1.83kg
	Dimensions	Elite Access[TI]: 144mm×296.4mm×28.7mm Elite Pass[TI]: 144mm×296.4mm×25.5mm

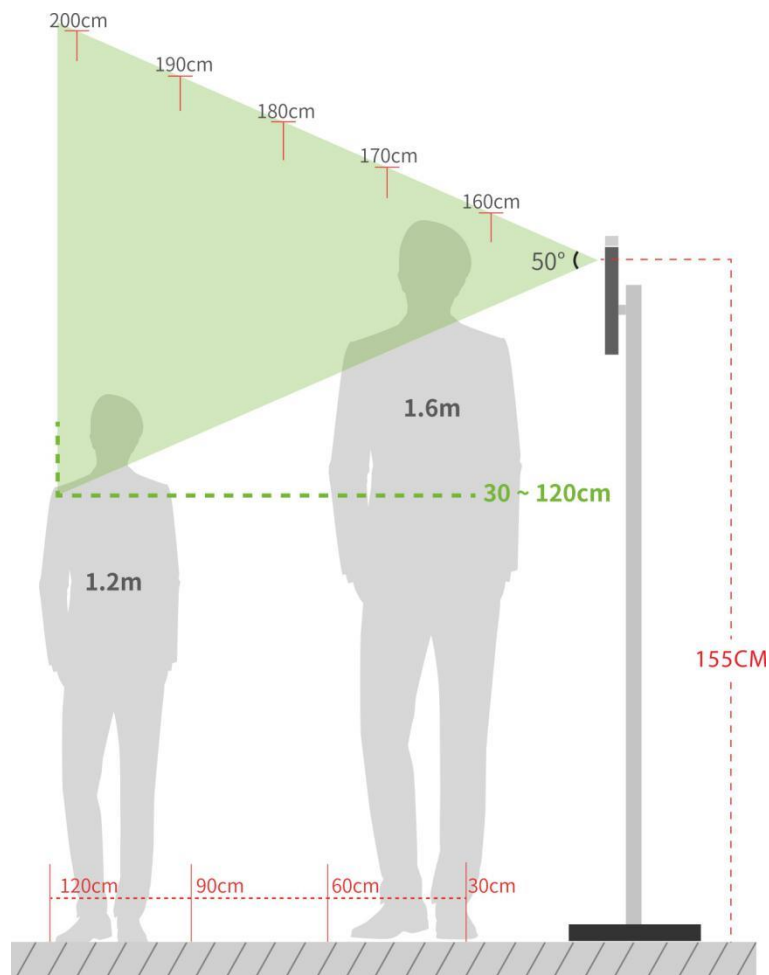
## 4 Components and Connection



## 5 Installation Requirements

### 5.1 Standing Position, Facial Expression and Standing Posture

#### Recommended Distance

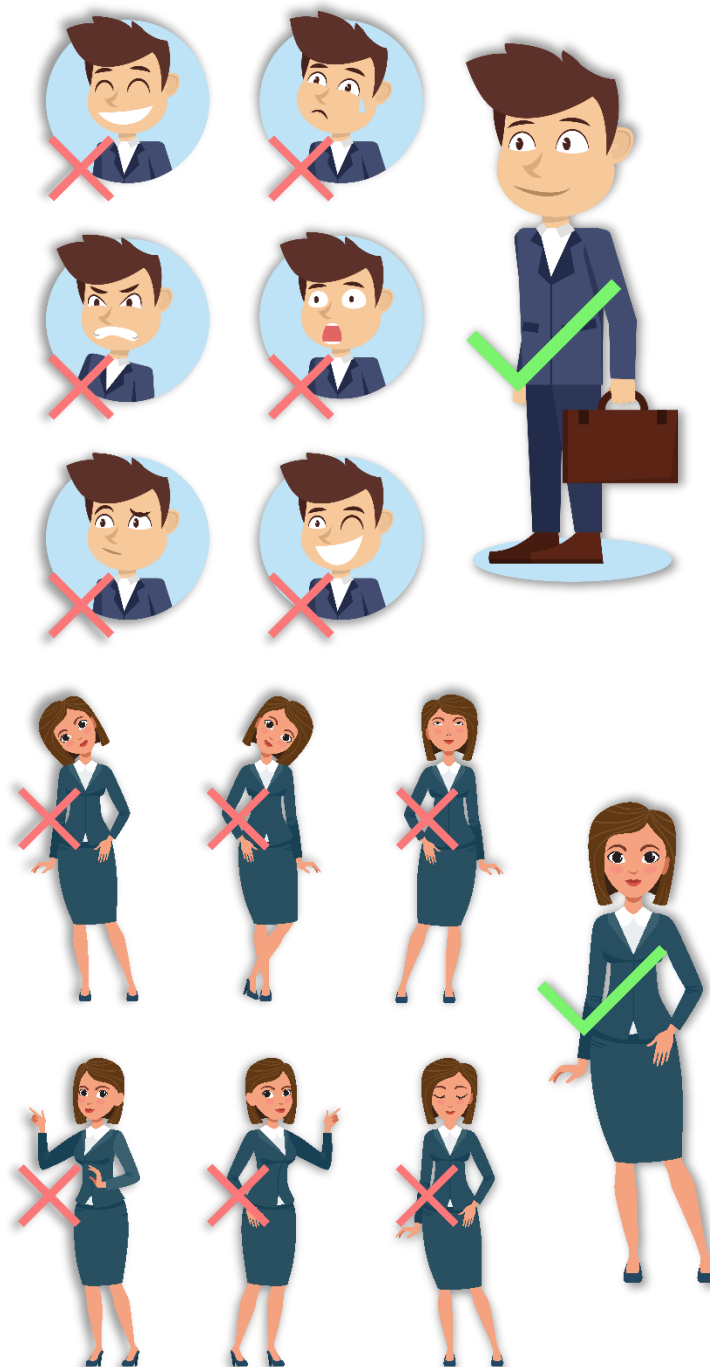


The distance between the device and a user whose height is within 1.55m to 1.85m is recommended to be 0.3 to 2.5m. Users may slightly move forward and backward to improve the quality of the facial images captured.

#### **Recommended Installation Guidelines:**

- Installation Height: 1.55m
- FOV (field of view) of the thermal imaging device: 50°
- Height of the face adapted for detection: 1.2m to 2m
- Temperature Measurement Distance for Elite Access[TI] and Elite Pass[TI]: 0.3m to 1.2m



**Facial expression and standing posture**

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

## 6 Face Registration

Keep your face in the center of the screen during registration. Please face the camera and stay still during face registration. The screen appears as shown below:



### Face registration and authentication methods

#### Instructions to register a face

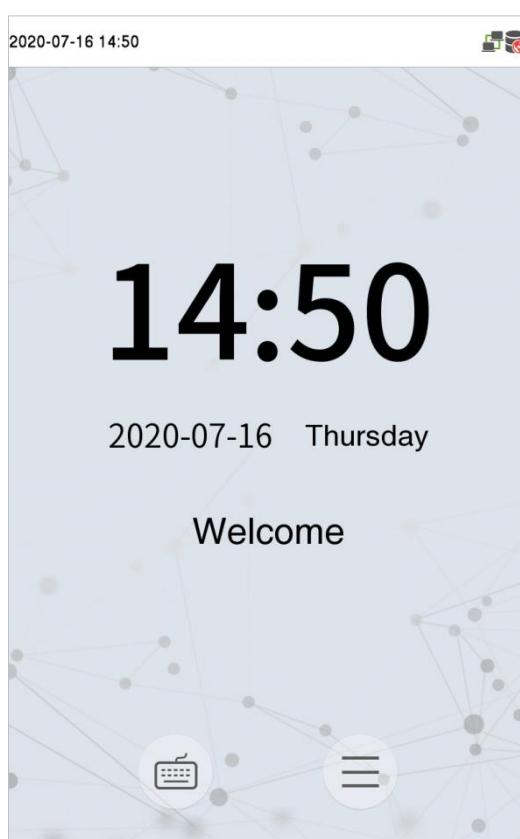
- When registering the face, maintain a distance of 40cm to 80cm between the device and the face.
- Please make sure not to change the facial expression. (smiling, wink, etc.)
- If you do not follow the instructions on the screen, the face registration may take a longer time or may fail.
- Make sure not to 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 wearing 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.

## **7 Home Screen**

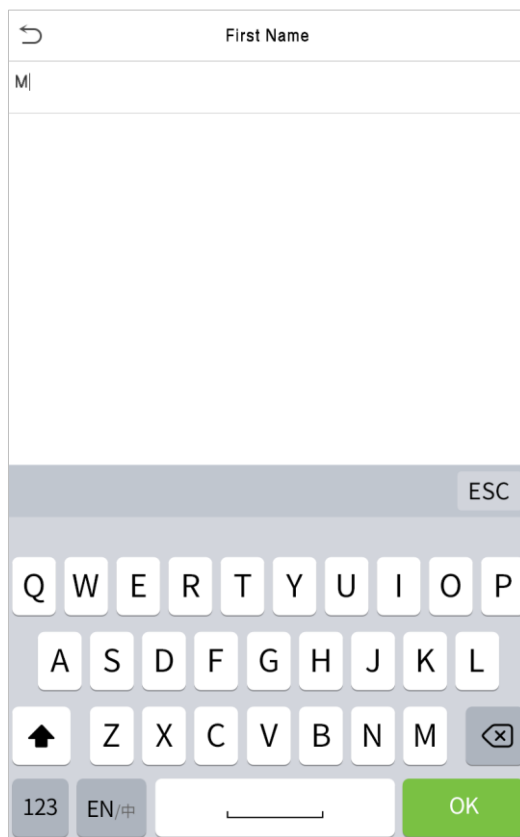
After connecting the power supply, the home screen appears as shown below:



### **Note:**

1. Click  to open the virtual keyboard.
2. When there is no Super Administrator registered in the device, click  to open 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 for the first time you use the device.

## 7.1 Virtual Keyboard




**Note:** Click the Virtual Keyboard on the Home screen. 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 characters keyboard and click **[ABC]** to return to the alphabetic keyboard. Click **[ESC]** to delete the entered characters.

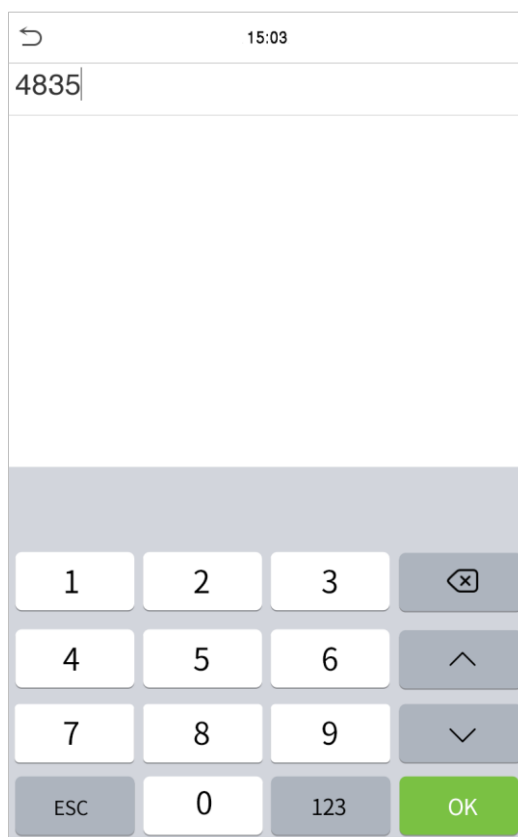
## 8 Verification Modes

### 8.1 Password Verification


The Password verification method compares the entered password with the registered User ID and password.

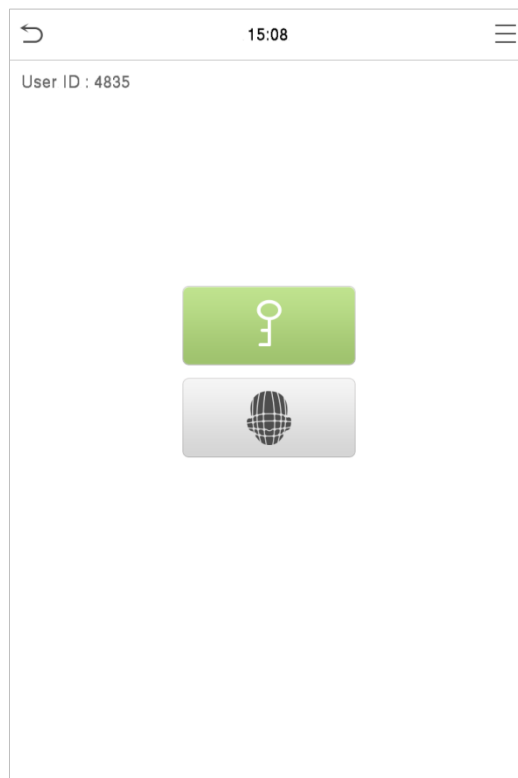
Click the  button on the main screen to open the 1:1 password verification mode.

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

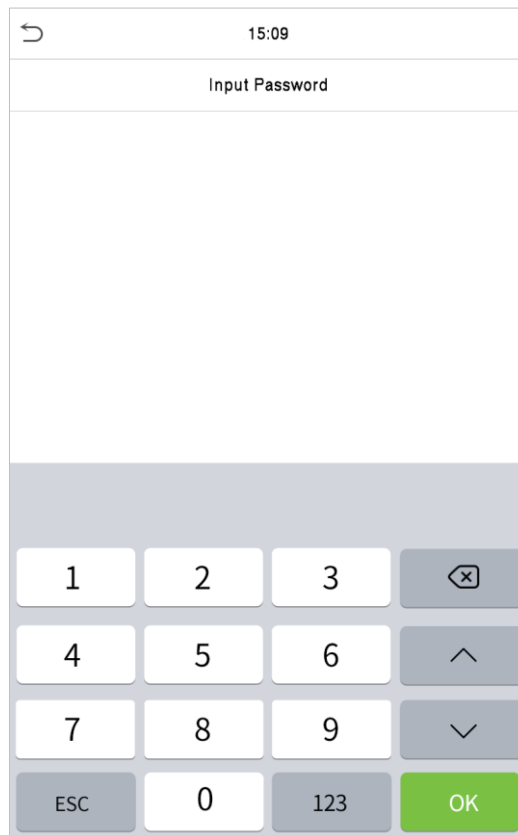


←		15:03	
4835			
1	2	3	ⓧ
4	5	6	^
7	8	9	∨
ESC	0	123	OK

If an employee registered the face in addition to a password, the following screen would appear. Select the  icon to open the password verification mode.

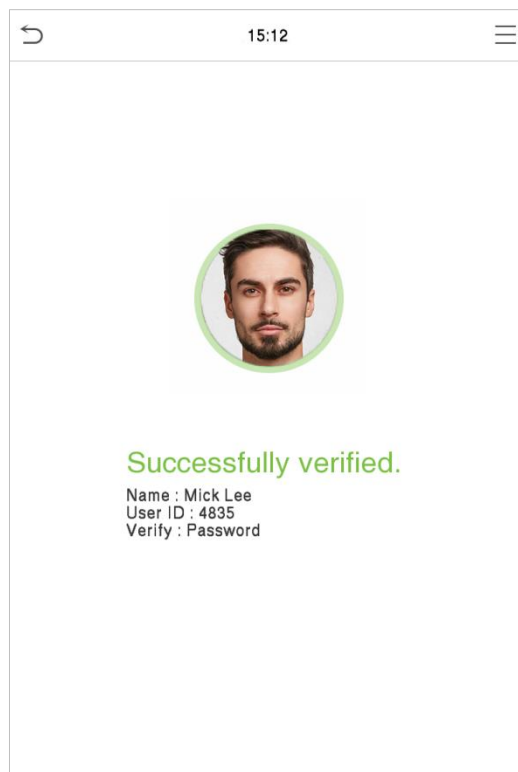


2. Input the password and press [OK].

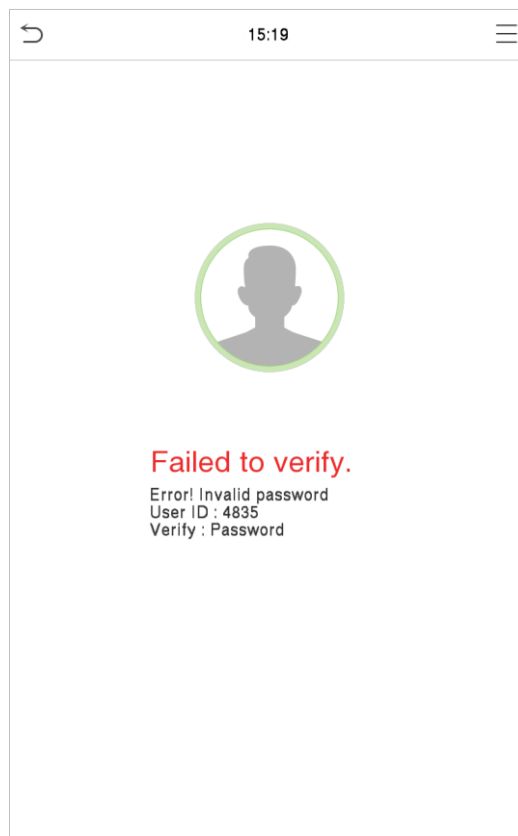


The screenshot shows a mobile application interface for password input. At the top, there is a status bar with a back arrow, the time 15:09, and the title 'Input Password'. Below the title is a large empty rectangular area for password entry. At the bottom, there is a numeric keypad with buttons for digits 1 through 9, 0, and function keys: ESC, 123, and a green OK button. The OK button is highlighted in green.

### **Successful Verification**



The screenshot shows a mobile application interface for successful verification. At the top, there is a status bar with a back arrow, the time 15:12, and a menu icon. Below the status bar is a large empty rectangular area. In the center, there is a circular profile picture of a man. Below the profile picture, the text 'Successfully verified.' is displayed in green. Underneath, the user details are listed: Name : Mick Lee, User ID : 4835, and Verify : Password.

**Failed Verification**

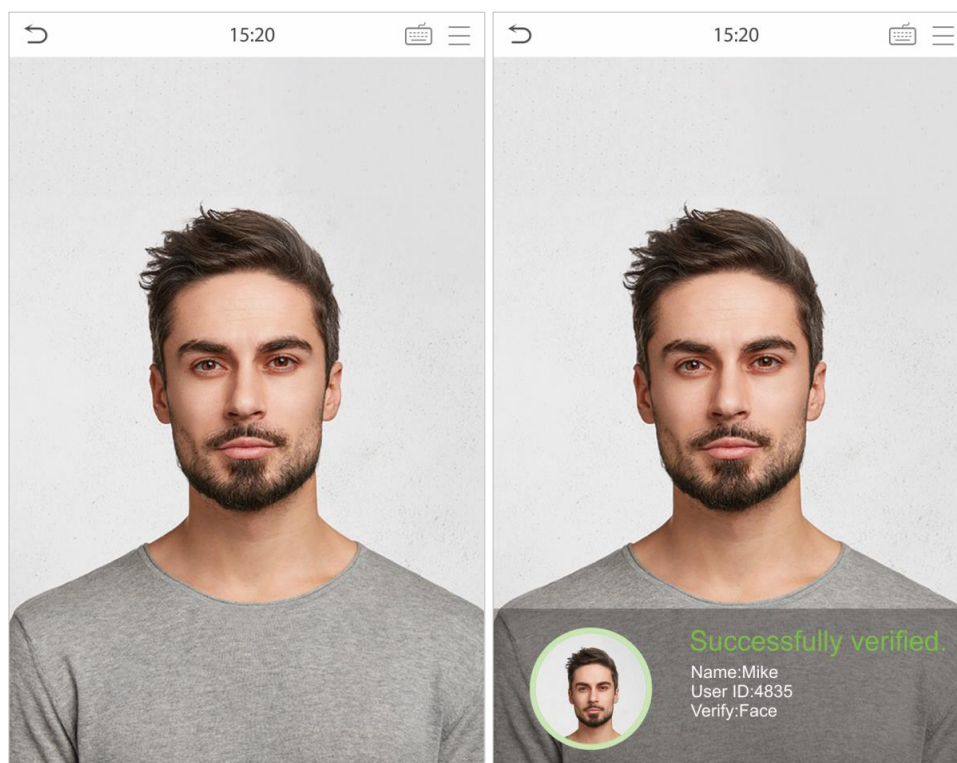


## 8.2 Facial Verification

### 1:N (One-to-Many) Facial Verification

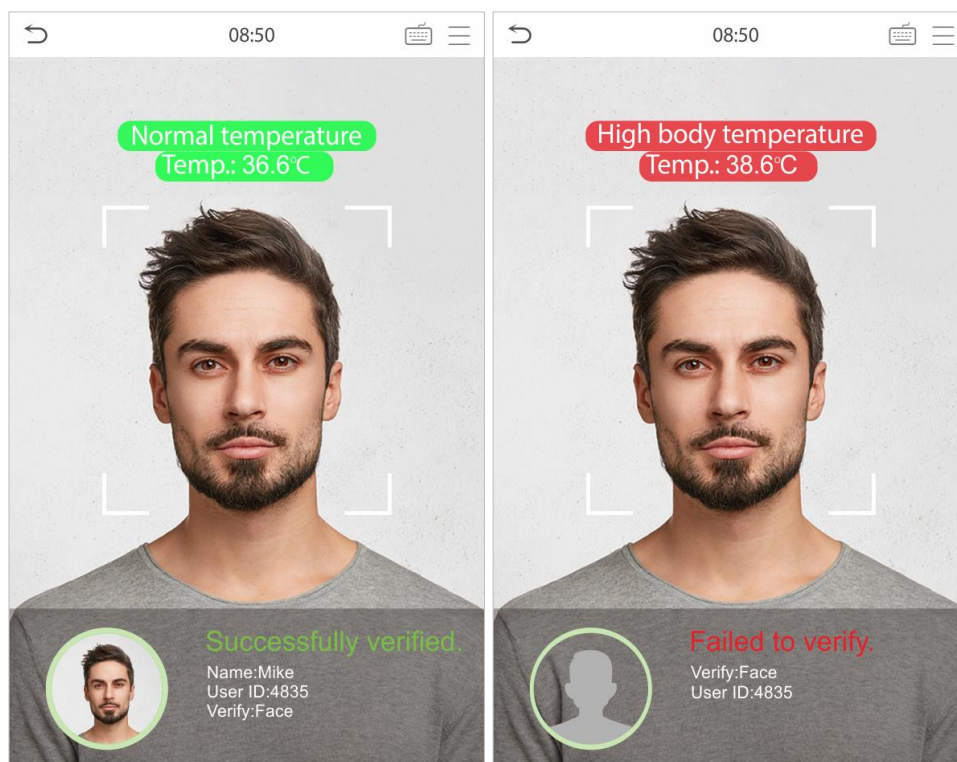
#### 1. Conventional verification

The conventional method compares the acquired facial images with all the facial data templates registered in the device. The following pop-up appears when the user is successfully verified.



#### 2. Infrared Temperature Screening

When the user enabled infrared temperature screening during user verification, the body temperature of the user is also detected. To achieve this, the user face must be aligned with the temperature detection area before the conventional user verification is performed. The verification screen appears as shown below:



### 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 verification screen appears as shown below:




#### 4. Display Thermodynamics Figure

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

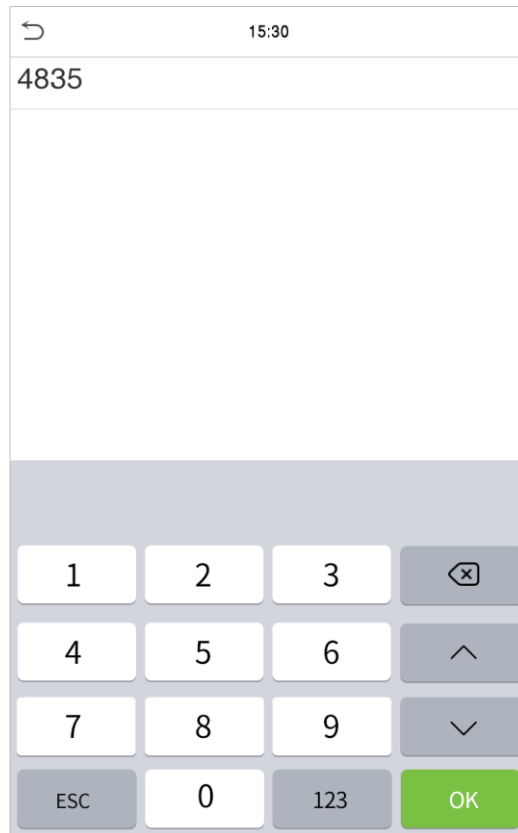


#### **1:1 (One-to-One) Facial Verification**

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.

Enter the User ID and click [OK].



← 15:30


4835

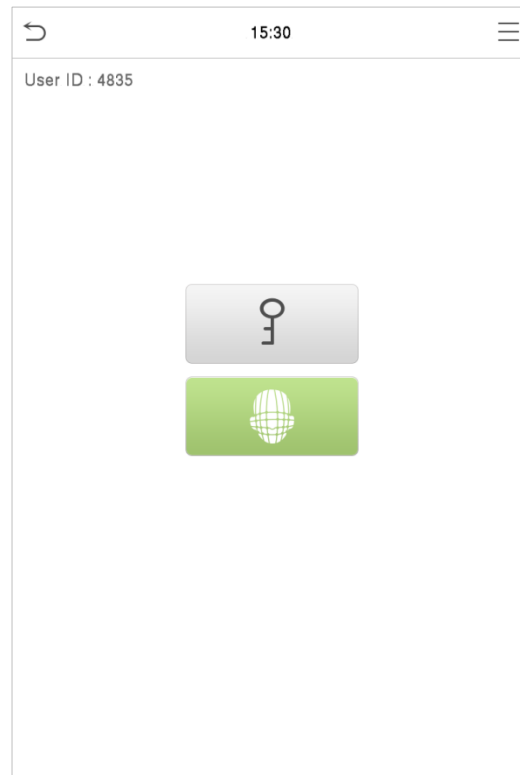
1 2 3

4 5 6

7 8 9

ESC 0 123 OK

If an employee registered a password in addition to the 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!".

### 8.2.1 Combined Verification

To ensure security, this device offers multiple verification methods. A total of 5 different verification combinations can be used, as shown below:


	Verification Mode
<input checked="" type="radio"/>	Password/Face
<input type="radio"/>	User ID only
<input type="radio"/>	Password
<input type="radio"/>	Face only
<input type="radio"/>	Face+Password

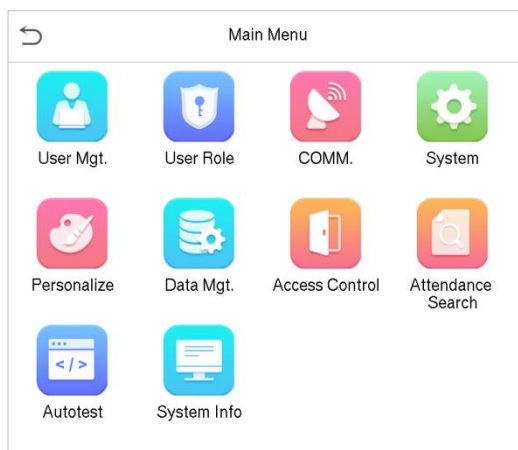
#### Note:

1. "/" 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.

## 9 Main Menu

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



Menu	Description
<b>User Mgt.</b>	Add, edit, view, and delete basic information about a user.
<b>User Role</b>	Set the permission scope of the custom role and enroller, that is, the rights to operate the system.
<b>COMM.</b>	Set the relevant parameters of the Network, PC connection, Wireless network, Cloud server, and Wiegand.
<b>System</b>	Set the parameters related to the system, including date & time, access records, facial templates, resetting to factory settings, temperature management, and detection
<b>Personalize</b>	Includes User Interface, voice, bell, check-in/check-out options, and shortcut key mappings settings.
<b>Data Mgt.</b>	Delete all the relevant data in the device.
<b>Access Control</b>	Set the parameters of the lock and access control device
<b>Attendance Search</b>	Query the specified access record, check attendance photos, and blocklist photos.
<b>Autotest</b>	Automatically tests whether each module functions properly, including the screen, audio, camera, and real-time clock.

**System Info**

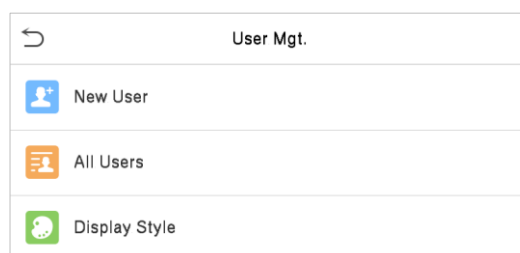
View data capacity, device, and firmware information of the current device.

## 10 User Management

The User Management module is used to add basic user details, privileges, permissions, and roles to define security policies and grant access to users.

### 10.1 Add Users

Click **User Mgt.** on the main menu and click **New User**.



#### **Register User ID and Name**

Enter the User ID and Name.

 A screenshot of a "New User" registration form. It has a back arrow icon in the top left corner. The form contains several input fields with labels and values: "User ID" with value "1", "Name" with value "Mike Lee", "User Role" with value "Normal User", "Face" with value "0", "Password" (empty), "User Photo" with value "0", and "Access Control Role" (empty). There is a large empty rectangular area at the bottom of the form.
**Note:**

1. A Username may contain 17 characters.
2. The User ID may contain 1 to 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 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 interface. The Administrator owns all the management privileges. If a custom role is set, you can also select **user-defined role** permissions for the user.

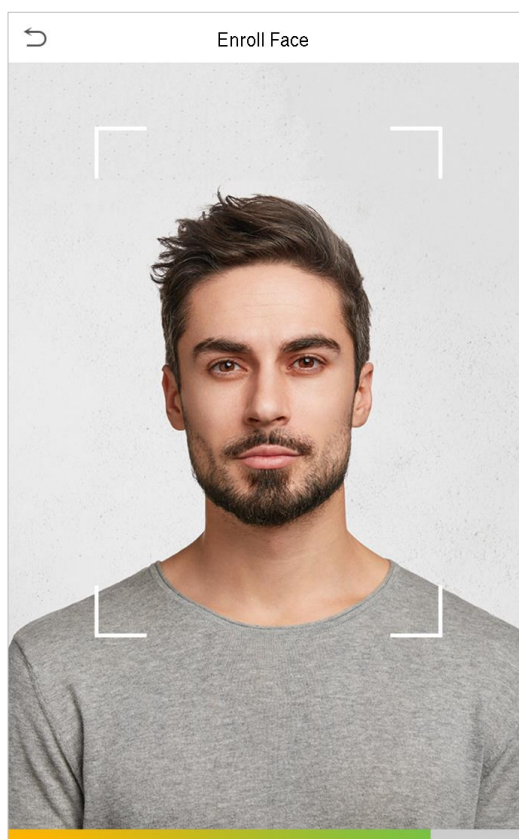
Click **User Role** to select a Normal User or Super Admin.

User Role	
<input checked="" type="radio"/>	Normal User
<input type="radio"/>	Super Admin

**Note:** If the selected user role is Super Admin, the Admin must validate the identity to access the main menu. The authentication is based on the authentication method(s) that the super administrator has registered. Please refer [Verification Modes](#).

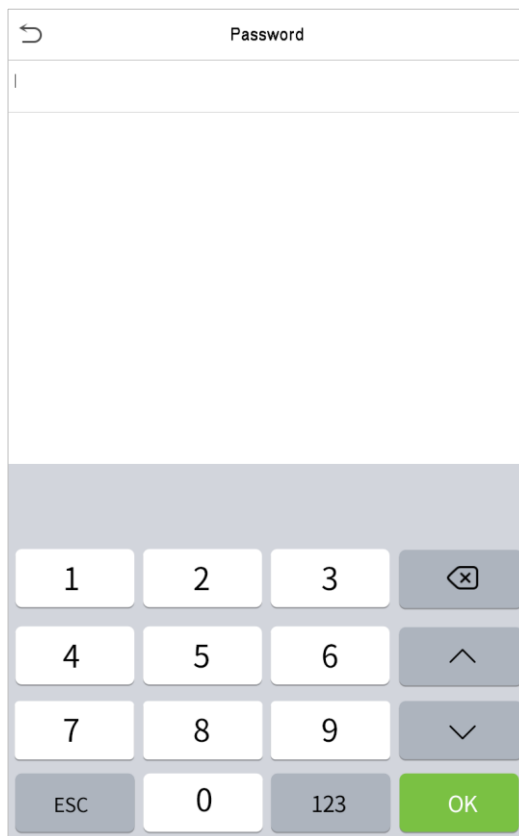
## **Register Face**

Click **Face** to open the face registration page. Please face the camera and stay still during face registration. The registration screen appears as shown below:



### **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.

The image shows a mobile application interface for password registration. At the top, there is a title bar with a back arrow icon on the left and the word "Password" in the center. Below the title bar is a large, empty rectangular input field for entering a password. At the bottom of the screen is a numeric keypad. The keypad consists of a 3x4 grid of buttons. The first three columns contain digits 1 through 9, and the fourth column contains a delete button (represented by a square with an 'x' and a left arrow). The second row of the keypad contains digits 4, 5, 6, and an up arrow button. The third row contains digits 7, 8, 9, and a down arrow button. The bottom row of the keypad contains an "ESC" button, a "0" button, a "123" button, and a green "OK" button.

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

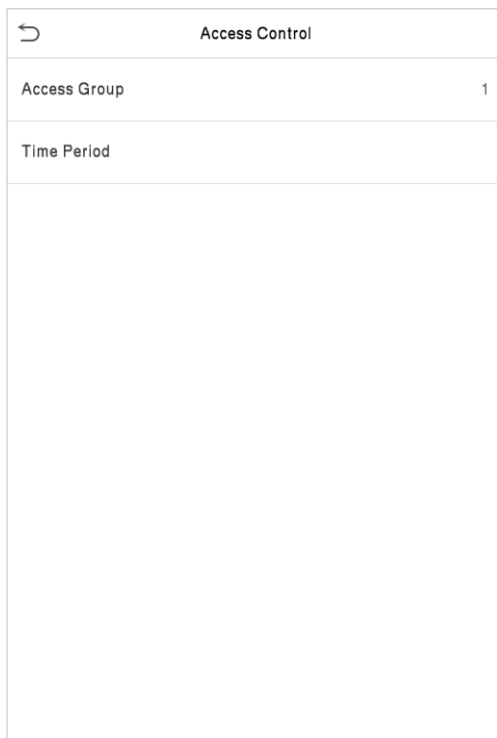
**Note:** While registering a face, the system will automatically capture a picture as the user photo. If you do not want to register a user photo, the system will automatically set the captured picture as the default photo.

### **Access Control Role**

The Access Control feature 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 streamlined user management. The 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** to set the time duration during which the specified user can access the area.



Access Control	
Access Group	1
Time Period	

## 10.2 Search 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 and display the information related to the entered keyword.

## 10.3 Edit Users

Select a user from the list and click **Edit** to modify the existing user details.

<div> <div>↶</div> <div>User : 1 Tom Lee</div> </div> <div> <div>Edit</div> <div>Delete</div> </div>	<div> <div>↶</div> <div>Edit : 1 Tom Lee</div> </div> <div> <div>User ID</div> <div>1</div> </div> <div> <div>Name</div> <div>Tom Lee</div> </div> <div> <div>User Role</div> <div>Normal User</div> </div> <div> <div>Face</div> <div>0</div> </div> <div> <div>Password</div> <div>*****</div> </div> <div> <div>User Photo</div> <div>1</div> </div> <div> <div>Access Control Role</div> </div>
--	---

**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 user details. For further operations, see [Add Users](#).

## 10.4 Delete Users

Select the desired user from the list and click **Delete**. Select the user information to be deleted and click **OK**.

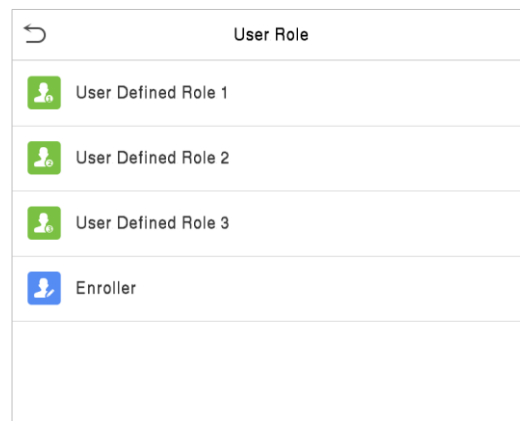
**Note:** If you select **Delete User**, all the information of the user will be deleted.

## 11 User Role

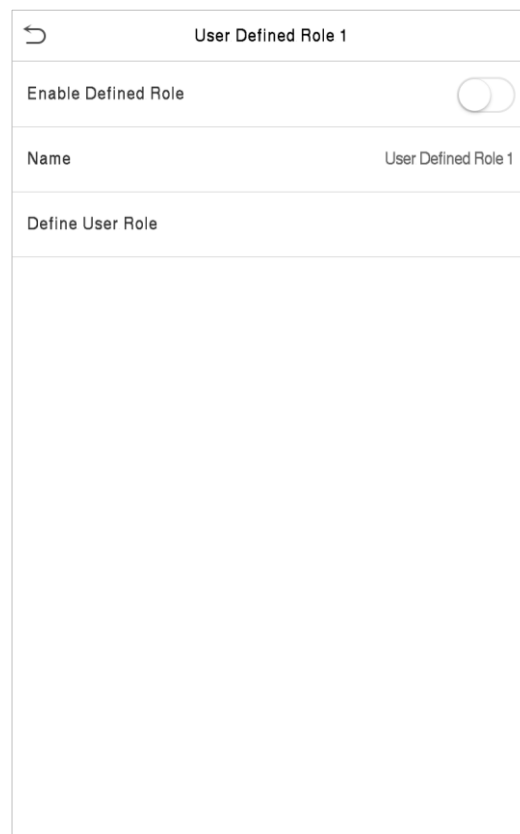
Roles are collections of permissions that can be associated with or granted to users. Roles provide a convenient way to package all the permissions required to perform a specific task. If you need to assign some specific permissions to certain users, you may configure the "User Defined Role" under the **User Role** menu.

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

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



1. Click any role to configure a new 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 privileges to the role.

User Defined Role 1	
<input checked="" type="checkbox"/> User Mgt.	<input checked="" type="checkbox"/> New User
<input checked="" type="checkbox"/> Comm.	<input checked="" type="checkbox"/> All Users
<input checked="" type="checkbox"/> System	<input checked="" type="checkbox"/> Display Style
<input type="checkbox"/> Personalize	
<input type="checkbox"/> Data Mgt.	
<input checked="" type="checkbox"/> Access Control	
<input type="checkbox"/> Attendance Search	
<input type="checkbox"/> Autotest	
<input type="checkbox"/> System Info	

**Note:** During the 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**.

User Role	
<input checked="" type="radio"/>	Normal User
<input type="radio"/>	Enroller
<input type="radio"/>	User Defined Role 1
<input type="radio"/>	Super Admin

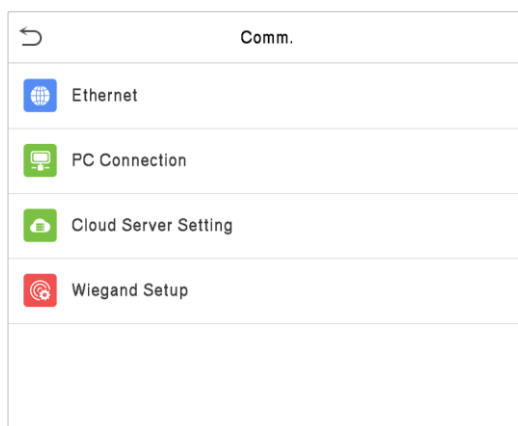
If no super administrator is registered, the device will prompt "Please register a Super Administrator user first!" after clicking the enable bar.



## 12 Communication Settings

The Communication Settings define the protocol and methodologies of data transfer between the device and PC/Server. The parameters include Network Connectivity, PC Connection, Wireless Network, Cloud Server, and Wiegand settings.

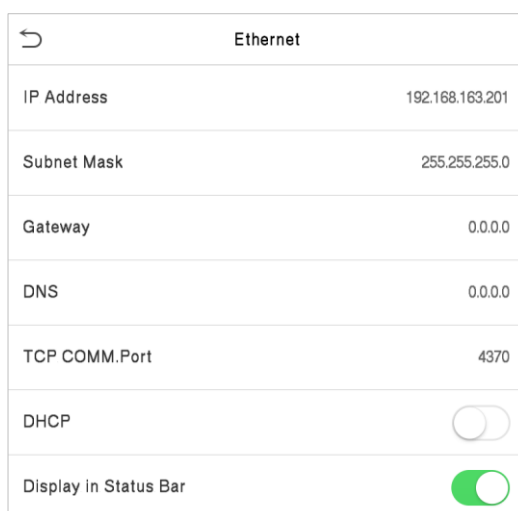
Tap **COMM.** on the main menu.



### 12.1 Network Settings

When the device needs to communicate with a PC over the Ethernet, you need to configure the 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	Description
<b>IP Address</b>	The factory default value is 192.168.1.201. Please set the value according to the requirements
<b>Subnet Mask</b>	The factory default value is 255.255.255.0. Please set the value according to the requirements
<b>Gateway</b>	The factory default address is 0.0.0.0. Please set the value according to the requirements
<b>DNS</b>	The factory default address is 0.0.0.0. Please set the value according to the requirements
<b>TCP COMM. Port</b>	The factory default value is 4370. Please set the value according to the requirements
<b>DHCP</b>	Dynamic Host Configuration Protocol, which is to dynamically allocate IP addresses for clients via the server
<b>Display in Status Bar</b>	To set whether to display the network icon on the status bar

## 12.2 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.

PC Connection	
Comm Key	0
Device ID	1

Menu	Description
<b>Comm Key</b>	The default password is 0, which can be changed. The Comm Key may contain 1 to 6 digits.
<b>Device ID</b>	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.

## 12.3 Cloud Server Settings

This represents settings used for connecting the ADMS server.

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

Cloud Server Setting	
Server Mode	ADMS
Enable Domain Name	<input type="checkbox"/>
Server Address	0.0.0.0
Server Port	8081
Enable Proxy Server	<input type="checkbox"/>
HTTPS	<input type="checkbox"/>

Menu	Description
<b>Enable Domain Name</b>	<b>Server Address</b> 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.
<b>Disable Domain Name</b>	<b>Server Address</b> IP address of the ADMS server.
	<b>Server Port</b> Port used by the ADMS server.
<b>Enable Proxy Server</b>	When you choose to enable the proxy, you need to set the IP address and port number of the proxy server.
<b>HTTPS</b>	It is an HTTP channel with security as its goal. Based on HTTP, transmission encryption and identity authentication ensure the security of the data transmission process.

## 12.4 Wiegand Setup

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

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

Wiegand Setup	
Wiegand Input	
Wiegand Output	

### Wiegand input

Wiegand Options	
Wiegand Format	
Wiegand Bits	26
Pulse Width(us)	100
Pulse Interval(us)	1000
ID Type	User ID


Menu	Description
<b>Wiegand Format</b>	Values range from 26 bits, 34 bits, 36 bits, 37 bits, and 50 bits.
<b>Wiegand Bits</b>	Number of Wiegand data bits.
<b>Pulse Width(μs)</b>	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.
<b>Pulse Interval(μs)</b>	The default value is 1000 microseconds, which can be adjusted within the range of 200 to 20000 microseconds.
<b>ID Type</b>	Select between the User ID and Access Card.

**Definitions of various common Wiegand formats:**

Wiegand Format	Definitions
Wiegand26	<p>EEEEEEEEEEEEEEEEEEEEEEEEEEEECO</p> <p>Consists of 26 bits of binary code. The 1<sup>st</sup> bit is the even parity bit of the 2<sup>nd</sup> to 13<sup>th</sup> bits, while the 26<sup>th</sup> bit is the odd parity bit of the 14<sup>th</sup> to 25<sup>th</sup> bits. The 2<sup>nd</sup> to 25<sup>th</sup> bits are the card numbers.</p>
Wiegand26a	<p>ESSSSSSSSSSSSSSSSSSSSSSSSSSCO</p> <p>Consists of 26 bits of binary code. The 1<sup>st</sup> bit is the even parity bit of the 2<sup>nd</sup> to 13<sup>th</sup> bits, while the 26<sup>th</sup> bit is the odd parity bit of the 14<sup>th</sup> to 25<sup>th</sup> bits. The 2<sup>nd</sup> to 9<sup>th</sup> bits are the site codes, while the 10<sup>th</sup> to 25<sup>th</sup> bits are the card numbers.</p>
Wiegand34	<p>EEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEECO</p> <p>Consists of 34 bits of binary code. The 1<sup>st</sup> bit is the even parity bit of the 2<sup>nd</sup> to 17<sup>th</sup> bits, while the 34<sup>th</sup> bit is the odd parity bit of the 18<sup>th</sup> to 33<sup>rd</sup> bits. The 2<sup>nd</sup> to 25<sup>th</sup> bits are the card numbers.</p>
Wiegand34a	<p>ESSSSSSSSSSSSSSSSSSSSSSSSSSSSSSCO</p> <p>Consists of 34 bits of binary code. The 1<sup>st</sup> bit is the even parity bit of the 2<sup>nd</sup> to 17<sup>th</sup> bits, while the 34<sup>th</sup> bit is the odd parity bit of the 18<sup>th</sup> to 33<sup>rd</sup> bits. The 2<sup>nd</sup> to 9<sup>th</sup> bits are the site codes, while the 10<sup>th</sup> to 25<sup>th</sup> bits are the card numbers.</p>
Wiegand36	<p>OFFFFFFFFFFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCMME</p> <p>Consists of 36 bits of binary code. The 1<sup>st</sup> bit is the odd parity bit of the 2<sup>nd</sup> to 18<sup>th</sup> bits, while the 36<sup>th</sup> bit is the even parity bit of the 19<sup>th</sup> to 35<sup>th</sup> bits. The 2<sup>nd</sup> to 17<sup>th</sup> bits are the device codes. The 18<sup>th</sup> to 33<sup>rd</sup> bits are the card numbers, and the 34<sup>th</sup> to 35<sup>th</sup> bits are the manufacturer codes.</p>
Wiegand36a	<p>EEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEECO</p> <p>Consists of 36 bits of binary code. The 1<sup>st</sup> bit is the even parity bit of the 2<sup>nd</sup> to 18<sup>th</sup> bits, while the 36<sup>th</sup> bit is the odd parity bit of the 19<sup>th</sup> to 35<sup>th</sup> bits. The 2<sup>nd</sup> to 19<sup>th</sup> bits are the device codes, and the 20<sup>th</sup> to 35<sup>th</sup> bits are the card numbers.</p>
Wiegand37	<p>OMMMMSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSCO</p> <p>Consists of 37 bits of binary code. The 1<sup>st</sup> bit is the odd parity bit of the 2<sup>nd</sup> to 18<sup>th</sup> bits, while the 37<sup>th</sup> bit is the even parity bit of the 19<sup>th</sup> to 36<sup>th</sup> bits. The 2<sup>nd</sup> to 4<sup>th</sup> bits are the manufacturer codes. The 5<sup>th</sup> to 16<sup>th</sup> bits are the site codes, and the 21<sup>st</sup> to 36<sup>th</sup> bits are the card numbers.</p>

Wiegand37a	<p>EMMMFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCCCO</p> <p>Consists of 37 bits of binary code. The 1<sup>st</sup> bit is the even parity bit of the 2<sup>nd</sup> to 18<sup>th</sup> bits, while the 37<sup>th</sup> bit is the odd parity bit of the 19<sup>th</sup> to 36<sup>th</sup> bits. The 2<sup>nd</sup> to 4<sup>th</sup> bits are the manufacturer codes. The 5<sup>th</sup> to 14<sup>th</sup> bits are the device codes, and 15<sup>th</sup> to 20<sup>th</sup> bits are the site codes, and the 21<sup>st</sup> to 36<sup>th</sup> bits are the card numbers.</p>
Wiegand50	<p>ESSSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO</p> <p>Consists of 50 bits of binary code. The 1<sup>st</sup> bit is the even parity bit of the 2<sup>nd</sup> to 25<sup>th</sup> bits, while the 50<sup>th</sup> bit is the odd parity bit of the 26<sup>th</sup> to 49<sup>th</sup> bits. The 2<sup>nd</sup> to 17<sup>th</sup> bits are the site codes, and the 18<sup>th</sup> to 49<sup>th</sup> bits are the card numbers.</p>
<p><b>“C”</b> denotes the card number; <b>“E”</b> denotes the even parity bit; <b>“O”</b> denotes the odd parity bit; <b>“F”</b> denotes the facility code; <b>“M”</b> denotes the manufacturer code; <b>“P”</b> denotes the parity bit; and <b>“S”</b> denotes the site code.</p>	

### Wiegand output


Wiegand Options

SRB

☐

Wiegand Format

Wiegand output bits

26

Failed ID

Disabled

Site Code

Disabled

Pulse Width(us)

100

Pulse Interval(us)

1000

ID Type

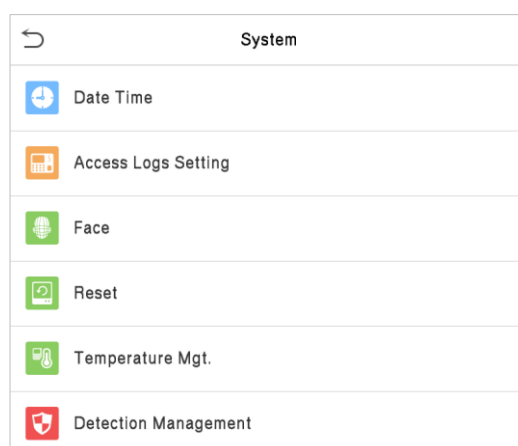
User ID

Menu	Description
<b>SRB (Security Relay Box)</b>	When SRB is enabled, the lock is controlled by the SRB to prevent the lock from being opened due to device removal.
<b>Wiegand Format</b>	Values range from 26 bits, 34 bits, 36 bits, 37 bits, and 50 bits.
<b>Wiegand output bits</b>	After choosing the Wiegand format, you can select one of the corresponding output digits in the Wiegand format
<b>Failed ID</b>	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.
<b>Site Code</b>	It is similar to the device ID. The difference is that a site code can be set manually and can be repeatable in a different device. The valid value ranges from 0 to 256 by default
<b>Pulse Width(μs)</b>	The time width represents the change of electric charge with high-frequency capacitance regularly within a specified time.
<b>Pulse Interval(μs)</b>	The time interval between two pulses
<b>ID Type</b>	Select between User ID and Access Card

## 13 System Settings

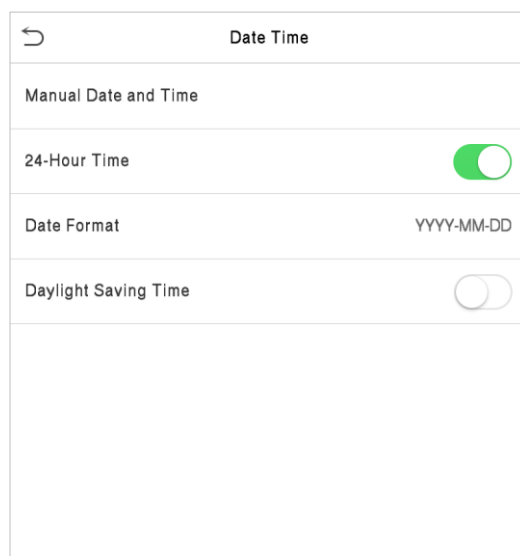
Here, you can set the related system parameters to optimize the performance of the device.

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



## 13.1 Date and Time

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



The screenshot shows a settings screen titled "Date Time" with a back arrow in the top left corner. The screen contains the following settings:

- Manual Date and Time**: A text input field.
- 24-Hour Time**: A toggle switch that is currently turned on (green).
- Date Format**: A text input field showing "YYYY-MM-DD".
- Daylight Saving Time**: A toggle switch that is currently turned off (grey).

Below these settings is a large empty rectangular area.

1. You can manually set the date and time and click **Confirm** to save.
2. 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, 2019) to 18:30 on January 1, 2020. After restoring the factory settings, the time of the device will change to 18:30 on January 1, 2020.



## 13.2 Access Logs Setting

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

Access Logs Setting	
Camera Mode	No photo
Display User Photo	<input checked="" type="checkbox"/>
Access Logs Warning	99
Circulation Delete Access Records	Disabled
Cyclic Delete ATT Photo	99
Cyclic Delete Blocklist Photo	99
Confirm Screen Delay(s)	3
Face comparison interval(s)	1

Menu	Description
<b>Camera Mode</b>	<p>It decides whether to capture and save the current snapshot image during verification. There are 5 modes:</p> <p><b>No Photo:</b> No photo is taken during user verification.</p> <p><b>Take photo, no save:</b> Photo is taken but is not saved during verification.</p> <p><b>Take photo and save:</b> Photo is taken and saved during verification.</p> <p><b>Save on successful verification:</b> Photo is taken and saved for each successful verification.</p> <p><b>Save on failed verification:</b> Photo is taken and saved during each failed verification.</p>
<b>Display User Photo</b>	Whether to display the user photo when the user verification is successful.
<b>Access Logs Warning</b>	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.

<b>Circulation Delete Access Records</b>	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.
<b>Cyclic Delete ATT Photo</b>	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.
<b>Cyclic Delete Blocklist Photo</b>	When the block-listed photos have reached full capacity, the device will automatically delete a set value of old block-listed photos. Users may disable the function or set a valid value between 1 and 99.
<b>Confirm Screen Delay(s)</b>	The time duration to display the success verification message. The valid value is 1 to 9 seconds.
<b>Face comparison Interval (s)</b>	To set the facial template matching time interval as needed. The valid value is 0 to 9 seconds.

### 13.3 Face Parameters

Click **Face** on the System interface.

↶	Face	1↓	↶	Face	1↓
	1:N Match Threshold	75		Face Pitch Angle	35
	1:1 Match Threshold	63		Face Rotation Angle	25
	Face Enrollment Threshold	70		Image Quality	40
	Face Pitch Angle	35		Minimum Face Size	80
	Face Rotation Angle	25		LED Light Triggered Threshold	80
	Image Quality	40		Motion Detection Sensitivity	4
	Minimum Face Size	80		Live Detection	<input checked="" type="checkbox"/>
	LED Light Triggered Threshold	80		Live Detection Threshold	70
	Motion Detection Sensitivity	4		Anti-counterfeiting with NIR	<input checked="" type="checkbox"/>
	Live Detection	<input checked="" type="checkbox"/>		WDR	<input type="checkbox"/>
	Live Detection Threshold	70		Anti-flicker Mode	50HZ
	Anti-counterfeiting with NIR	<input type="checkbox"/>		Face Algorithm	

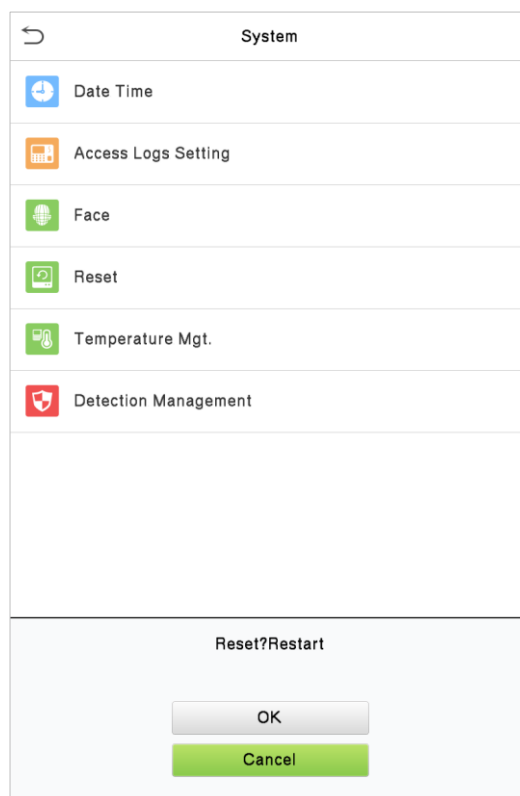
Menu	Description
<b>1:N Match Threshold</b>	<p>In 1:N verification mode, the verification will only be successful when the similarity between the acquired facial image template and all the registered facial templates is greater than the set value.</p> <p>The valid value ranges from 65 to 120. The higher the thresholds, the lower the misjudgement rate, the higher the rejection rate, and vice versa. The default value of 75 is recommended.</p>
<b>1:1 Match Threshold</b>	<p>In 1:1 verification mode, the verification will only be successful when the similarity between the acquired facial image template and the facial templates enrolled in the device is greater than the set value.</p> <p>The valid value ranges from 55 to 120. The higher the thresholds, the lower the misjudgement rate, the higher the rejection rate, and vice versa. The default value of 63 is recommended.</p>
<b>Face Enrollment Threshold</b>	<p>During face enrollment, 1:N comparison is used to determine whether the user has already registered before.</p> <p>When the similarity between the acquired facial image template and all the registered facial templates is greater than this threshold, it indicates that the face has already been registered.</p>
<b>Face Pitch Angle</b>	<p>The pitch angle tolerance of a face for facial registration and comparison.</p> <p>If a face's pitch angle exceeds this set value, it will be filtered by the algorithm, i.e. ignored by the device thus no registration and comparison interface will be shown.</p>
<b>Face Rotation Angle</b>	<p>The rotation angle tolerance of a face for facial template registration and comparison.</p> <p>If a face's rotation angle exceeds this set value, it will be filtered by the algorithm, i.e. ignored by the device thus no registration and comparison interface will be shown.</p>
<b>Image Quality</b>	<p>Image quality for facial registration and comparison. The higher the value, the clearer the image.</p>

<b>Minimum Face Size</b>	<p>Required for facial registration and comparison.</p> <p>If an object's size is smaller than this set value, the object will be filtered and not recognized as a face.</p> <p>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.</p>
<b>LED Light Triggered Threshold</b>	<p>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.</p>
<b>Motion Detection Sensitivity</b>	<p>A measurement of the amount of change in a camera's field of view that qualifies as potential motion detection that turn on the device 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.</p>
<b>Live Detection</b>	<p>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.</p>
<b>Live Detection Threshold</b>	<p>Judges whether the visible image comes from an alive body. The larger the value, the better the visible light anti-spoofing performance.</p>
<b>Anti-counterfeiting with NIR</b>	<p>Using near-infrared spectra imaging to identify and prevent fake photos and videos attack.</p>
<b>WDR</b>	<p>Wide Dynamic Range (WDR), which balances the light and extends image visibility for surveillance videos under high contrast lighting scenes and improves object identification under bright and dark environments.</p>
<b>Anti-flicker Mode</b>	<p>Used when WDR is turned off. This helps reduce flicker when the device's screen flashes at the same frequency as the light.</p>
<b>Face Algorithm</b>	<p>Facial algorithm related information and pause the facial template update.</p>
<b>Notes</b>	<p>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.</p>

## 13.4 Factory Reset

The Factory reset module restores the device parameters, 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.

## 13.5 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 process.
















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

Temperature Mgt.	
Current Device Temperature	37.5°C
Low Temp. to Heat	0°C
High Temp. to Reset	82°C

Menu	Description
<b>Current Device Temperature</b>	This column shows the actual temperature of the device.
<b>Low Temp. to Heat</b>	Once the device temperature is lower than the set value, the device will start self-heating process, the range is 0 to 10(°C).
<b>High Temp. to Reset</b>	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 (°C).

## 13.6 Detection Management

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

↶ Detection Management 1↓	↶ Detection Management 1↓
Enable temperature screening with infrared 	Temp. Unit °C
High temperature alarm threshold 37.30 °C	Temperature measurement distance Far
Temperature over the range; access denied 	Display Thermodynamics Figure 
Temperature deviation correction 0.00	Display Body Temperature 
Temp. Unit °C	Enable mask detection 
Temperature measurement distance Far	Deny access without mask 
Display Thermodynamics Figure 	Allow unregistered people to access 
Display Body Temperature 	Enable capture of unregistered person 
Enable mask detection 	Trigger external alarm 
Deny access without mask 	Clear external alarm
Allow unregistered people to access 	External alarm delay(s) 255
Enable capture of unregistered person 	Firmware update

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

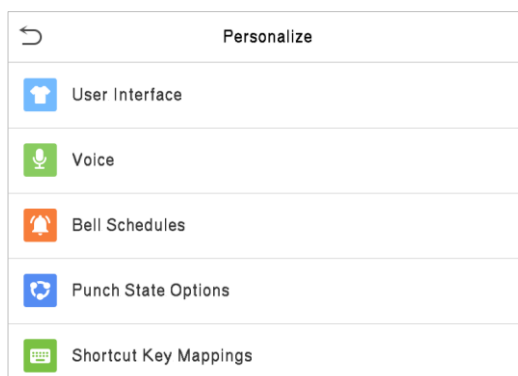
<b>Temperature deviation correction</b>	As the temperature measurement module allows a small range of errors (disturbance) of an observed value under different environments (humidity, room temperature, etc), users may set the deviation value here.
<b>Temp. Unit</b>	The unit of body temperature can be switched between Celsius (°C) and Fahrenheit (°F).
<b>Temperature measurement distance</b>	The distance modes during temperature verification are given as Near, Close and Far.
<b>Display Thermodynamics Figure</b>	To enable or disable the display of thermal screening image When this feature is enabled, the thermal screening image of the person will be displayed in the upper left corner of the device.
<b>Display Body Temperature</b>	To enable or disable the display body temperature during verification When enabled, the device will display the user's detected temperature value during the verification process.
<b>Enable mask detection</b>	To enable or disable the mask detection function. When it is enabled, the device will identify whether the user is wearing a mask or not during verification.
<b>Allow unregistered people to access</b>	To enable or disable the unregistered people to access function. When enabled, the device allows the person to enter without registration by only detecting the temperature.
<b>Enable capture of unregistered person</b>	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 <b>Allow unregistered people to access</b> .
<b>Trigger external alarm</b>	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.
<b>Clear external alarm</b>	Clear the triggered alarm records of the device.
<b>External alarm delay(s)</b>	The delay time(s) for triggering an external alarm can be set in seconds, users may disable the function or set a valid value between 1 to 255.
<b>Firmware Update</b>	Choose whether to update the thermal imaging temperature detection module software version.



## 14 Personalize Settings

**Personalization** allows users to make selections and set preferences in a system, with the intent of giving users more control over the user experience. You may customize the interface settings, audio, and bell.

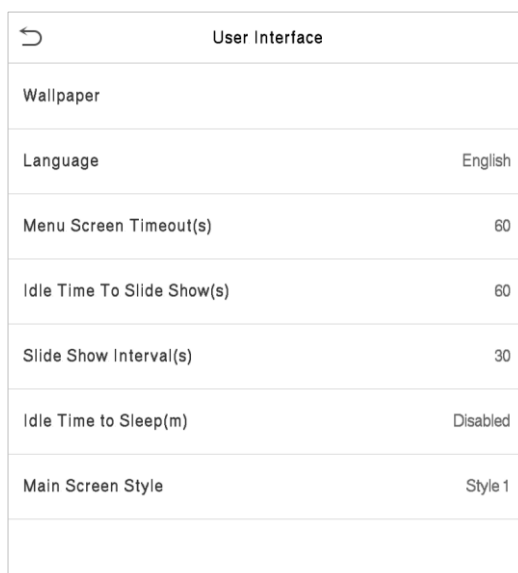
Click **Personalize** on the main menu interface.



### 14.1 Interface Settings

Here, you can customize the display style of the main interface.

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

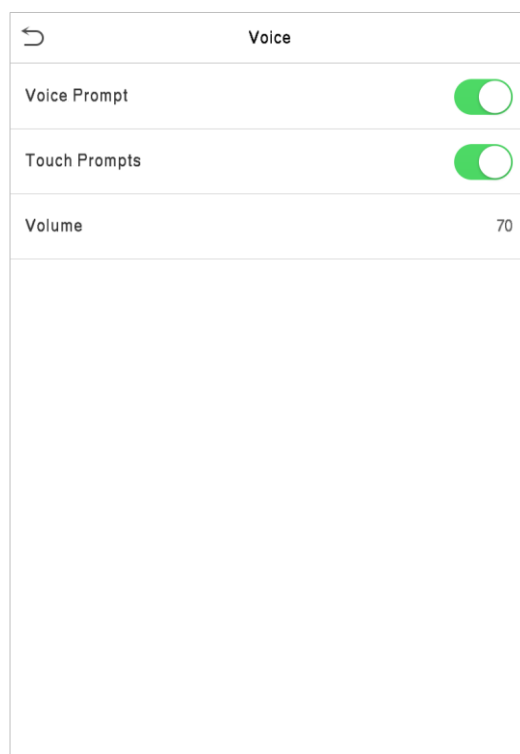


Menu	Description
<b>Wallpaper</b>	To select the main screen wallpaper according to your personal preference.
<b>Language</b>	To select the language of the device.
<b>Menu Screen</b>	When there is no operation, and the time exceeds the set value, the device will

<b>Timeout (s)</b>	automatically go back to the initial interface. You can disable the function or set the value between 60 and 99999 seconds.
<b>Idle Time To Slide Show (s)</b>	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.
<b>Slide Show Interval (s)</b>	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.
<b>Idle Time to Sleep (m)</b>	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 to 999 minutes.
<b>Main Screen Style</b>	To select the main screen style according to your personal preference.

## 14.2 Voice Settings

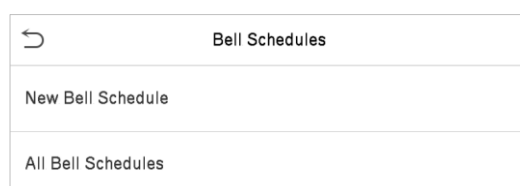
Click **Voice** on the **Personalize** interface.



Menu	Description
<b>Voice Prompt</b>	Select whether to enable voice prompts during operation
<b>Touch Prompt</b>	Select whether to enable keypad sounds
<b>Volume</b>	Adjust the volume of the device and the valid value is 0 to 100.

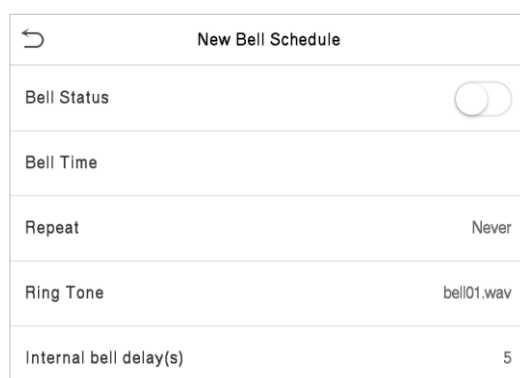
## 14.3 Bell Schedules

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



### Add a bell

1. Click **New Bell Schedule** to open the interface.



Menu	Description
<b>Bell Status</b>	Set whether to enable the bell status.
<b>Bell Time</b>	At this time of day, the device automatically rings the bell.
<b>Repeat</b>	Set the repetition cycle of the bell.
<b>Ring Tone</b>	Select a ring tone.
<b>Internal bell delay(s)</b>	Set the duration of the internal bell. The valid value ranges from 1 to 999 seconds.

2. Go 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.

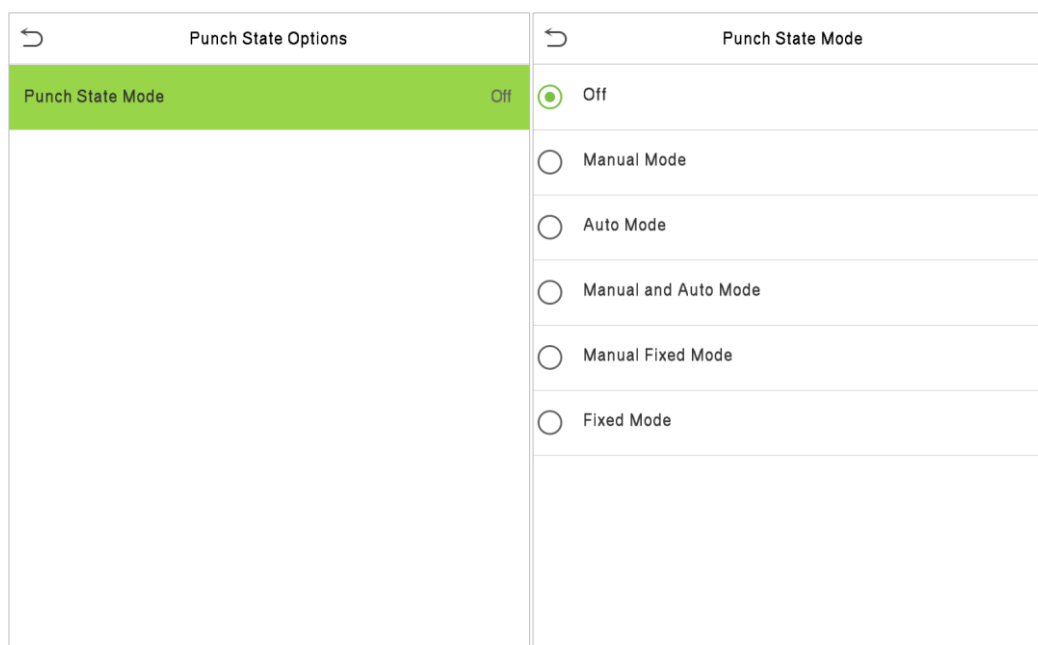
### Delete a bell

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

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

## 14.4 Punch States Options

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



Menu	Description
<b>Punch State Mode</b>	<p>Select a punch state mode, which can be:</p> <p><b>Off:</b> Disables the punch state key function. The punch state key set under the <b>Shortcut Key Mappings</b> menu will become invalid.</p> <p><b>Manual Mode:</b> To switch the punch state key manually, and the punch state key will disappear after <b>Punch State Timeout</b>.</p> <p><b>Auto Mode:</b> After this mode is chosen, set the switching time of punch state key in <b>Shortcut Key Mappings</b>; when the switching time is reached, the set punch state key will be switched automatically.</p> <p><b>Manual and Auto Mode:</b> In this mode, the main interface will display the auto-</p>

switching punch state key by default. Meanwhile, it also supports manual switching punch state key. After timeout, the manual switching punch state key will become the default 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 changed.

## 14.5 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 be displayed quickly.

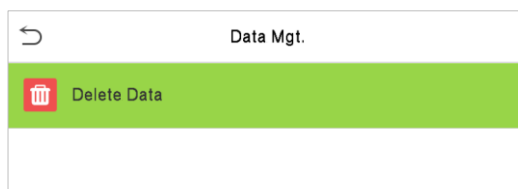
Click **Shortcut Key Mappings** on the Personalize interface.

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

## 15 Data Management

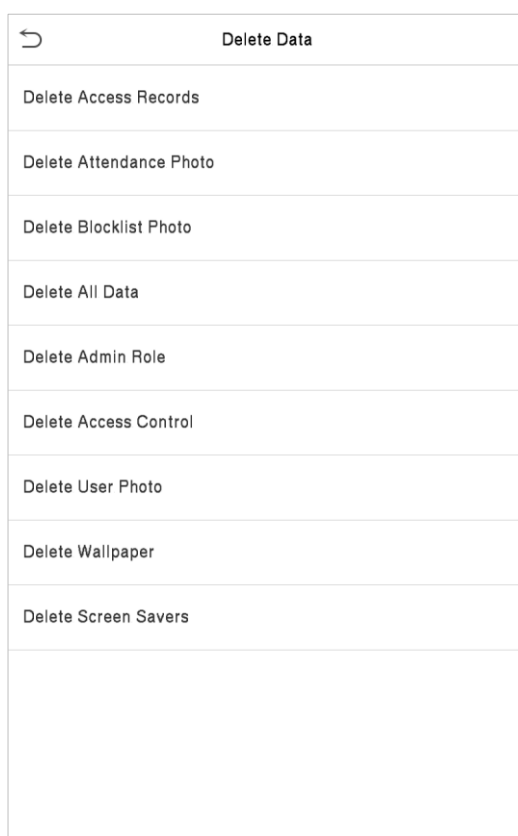
The Data Management interface is used to delete the relevant data in the device.

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



### 15.1 Delete Data

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



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

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

**Note:** When deleting the access records, attendance photos or block-listed photos, you may select Delete All or Delete by Time Range. When selecting Delete by Time Range, you need to set a specific time range to delete all the data within the period.

←

Delete Access Records

Delete All

Delete by Time Range

←

Start Time

2020-07-16 00:00

▲

2020

▼

YYYY

▲

07

▼

MM

▲

16

▼

DD

▲

00

▼

HH

▲

00

▼

MM

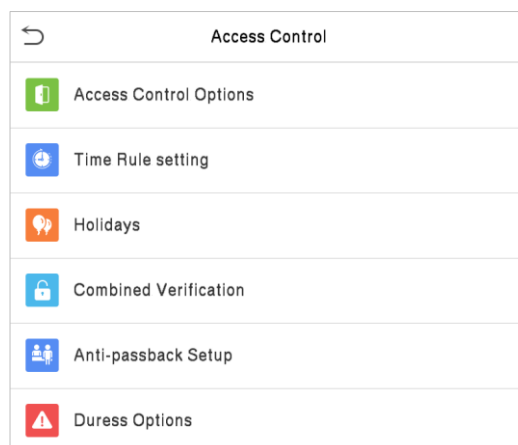
Confirm (OK)

Cancel (ESC)

## 16 Access Control

Access Control is used to set the schedule of the door opening, lock control, and other parameter 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 combination as "1" and set in unlocking state.



## 16.1 Access Control Options

The Access Control options are used to set the parameters of the control lock of the device.

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

Access Control Options	Access Control Options
Gate Control Mode 	Gate Control Mode 
Door Lock Delay (s) 5	Verification Mode Password/Face
Door Sensor Delay (s) 10	Door available time period 1
Door Sensor Type None	Normal open time period None
Verification Mode Password/Face	Master Device In
Door available time period 1	Auxiliary input configuration
Normal open time period None	Speaker Alarm 
Master Device In	Reset Access Setting
Auxiliary input configuration	
Speaker Alarm 	
Reset Access Setting	

Menu	Description
<b>Gate Control Mode</b>	Whether to turn on the gate control mode or not. When set to ON, this interface will remove the Door lock relay, Door sensor relay and Door sensor type function.
<b>Door Lock Delay (s)</b>	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.
<b>Door Sensor Delay (s)</b>	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.
<b>Door Sensor Type</b>	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.

<b>Verification Mode</b>	The supported verification mode includes Password/Face, User ID only, Password, Face only, and Face + Password.
<b>Door available time period</b>	To set time period for door, so that the door is accessible only during this time period.
<b>Normal open time Period</b>	Scheduled time period for "Normal Open" mode, so that the door is always unlocked during this period.
<b>Master Device</b>	<p>When setting up the master and slave, the status of the master can be set to exit on enter.</p> <p><b>Exit:</b> The record verified on the host is the exit record.</p> <p><b>Enter:</b> The record verified on the host is the entry record.</p>
<b>Auxiliary input configuration</b>	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.
<b>Speaker Alarm</b>	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.
<b>Reset Access Setting</b>	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 deleted access control data in Data Mgt. is excluded.

## 16.2 Time Rule settings

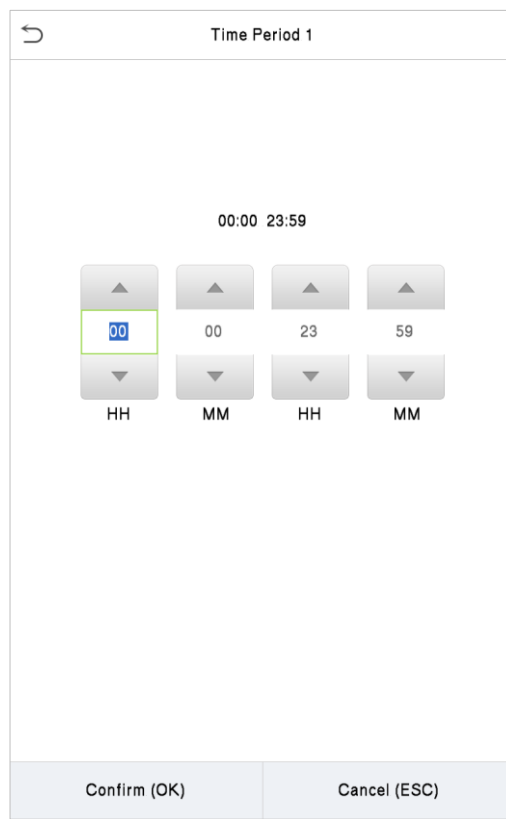
The entire system can define up to 50-time rules. Each time rule represents ten time zones, i.e. one week and 3 holidays, and each time zone is a valid time period within 24 hours per day. You may set a maximum of 3 time periods for every time zone. The relationship among these time periods is "or".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

Time Rule[2/50]	
Sunday	[00:00 23:59] [00:00 23:59...
Monday	[00:00 23:59] [00:00 23:59...
Tuesday	[00:00 23:59] [00:00 23:59...
Wednesday	[00:00 23:59] [00:00 23:59...
Thursday	[00:00 23:59] [00:00 23:59...
Friday	[00:00 23:59] [00:00 23:59...
Saturday	[00:00 23:59] [00:00 23:59...
holiday type 1	[00:00 23:59] [00:00 23:59...
holiday type 2	[00:00 23:59] [00:00 23:59...
holiday type 3	[00:00 23:59] [00:00 23:59...
<div></div>	

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



Time Period 1

00:00 23:59

00 00 23 59

HH MM HH MM

Confirm (OK) Cancel (ESC)

**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.

## 16.3 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.

Holidays	
Add Holiday	
All Holidays	

### **Add a New Holiday**

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

Holidays	
No.	1
Date	Undefined
Holiday Type	holiday type 1
Looping or not	<input checked="" type="checkbox"/>

### **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.

## 16.4 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.

Combined Verification	
1	01 00 00 00 00
2	00 00 00 00 00
3	00 00 00 00 00
4	00 00 00 00 00
5	00 00 00 00 00
6	00 00 00 00 00
7	00 00 00 00 00
8	00 00 00 00 00
9	00 00 00 00 00
10	00 00 00 00 00
<input type="text"/>	

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.

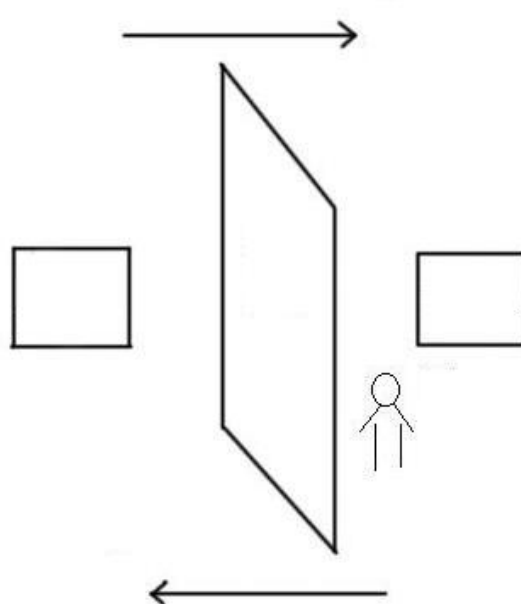
### **Delete a door-unlocking combination**

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

## 16.5 Anti-Passback Setup

It is possible that users may be followed by some unauthorized 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 access area (master device), the other one is installed outside the access area (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.

Anti-passback Setup		Anti-passback Direction	
Anti-passback Direction	No Anti-passback	<input checked="" type="radio"/> No Anti-passback	
		<input type="radio"/> Out Anti-passback	
		<input type="radio"/> In Anti-passback	
		<input type="radio"/> In/Out Anti-passback	

Menu	Description
<b>Anti-Passback direction</b>	<p><b>No Anti-Passback:</b> Anti-Passback function is disabled, which means successful verification through either master device or slave device can unlock the door. The attendance state is not saved.</p> <p><b>Out Anti-Passback:</b> 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.</p> <p><b>In Anti-Passback:</b> 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.</p> <p><b>In/Out Anti-Passback:</b> 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.</p>



## 16.6 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.

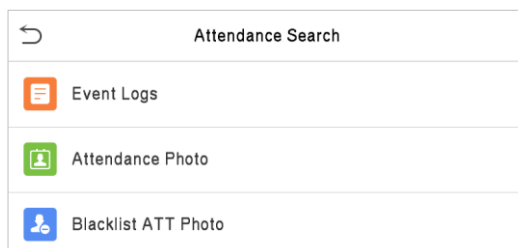
Duress Options	
Alarm on Password	<input type="checkbox"/>
Alarm Delay(s)	10
Duress Password	None

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

## 17 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 blacklist 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**.

User ID	Time Range
Please Input(query all data without input)	<input checked="" type="radio"/> Today
	<input type="radio"/> Yesterday
	<input type="radio"/> This week
	<input type="radio"/> Last week
	<input type="radio"/> This month
	<input type="radio"/> Last month
	<input type="radio"/> All
	<input type="radio"/> User Defined
<div> <div>1</div> <div>2</div> <div>3</div> <div>⌫</div> </div> <div> <div>4</div> <div>5</div> <div>6</div> <div>⤴</div> </div> <div> <div>7</div> <div>8</div> <div>9</div> <div>⤵</div> </div> <div> <div>ESC</div> <div>0</div> <div>123</div> <div>OK</div> </div>	

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

Personal Record Search					Personal Record Search		
User ID	Name	Time	Mode	State	Date	User ID	Time
4835	Mick Lee	07-16 15:31	15	0	07-16	Number of Records:49	
4835	Mick Lee	07-16 15:31	15	0	0		17:01 14:47 14:40 14:35
4835	Mick Lee	07-16 15:31	15	0	4835		15:31 15:31 15:31 15:31 15:20
4835	Mick Lee	07-16 15:31	15	0			15:20 15:20 15:20 15:20 15:12
4835	Mick Lee	07-16 15:20	15	0			15:12 15:12 15:11 15:11 15:11
4835	Mick Lee	07-16 15:20	15	0			15:11 15:11 15:10 15:10 15:10
4835	Mick Lee	07-16 15:20	15	0			15:10 15:10 15:10 15:10 15:10
4835	Mick Lee	07-16 15:20	15	0			15:09 15:09 15:09
4835	Mick Lee	07-16 15:20	15	0	1		14:38 14:38 14:38 14:38 14:38
4835	Mick Lee	07-16 15:12	3	0			14:38 14:38 14:38 14:38 14:38
4835	Mick Lee	07-16 15:12	15	0			14:38 14:37 14:37 14:37 14:37
4835	Mick Lee	07-16 15:12	15	0			14:37 14:37
4835	Mick Lee	07-16 15:11	15	0	07-15	Number of Records:03	
4835	Mick Lee	07-16 15:11	15	0	0		10:19 10:17 10:15
4835	Mick Lee	07-16 15:11	15	0	07-09	Number of Records:01	
4835	Mick Lee	07-16 15:11	15	0	0		10:33
4835	Mick Lee	07-16 15:11	15	0			
4835	Mick Lee	07-16 15:10	3	0			
4835	Mick Lee	07-16 15:10	15	0			
4835	Mick Lee	07-16 15:10	15	0			
4835	Mick Lee	07-16 15:10	15	0			
4835	Mick Lee	07-16 15:10	15	0			
4835	Mick Lee	07-16 15:10	15	0			
4835	Mick Lee	07-16 15:10	15	0			
4835	Mick Lee	07-16 15:10	15	0			
Verification Mode : Face Status : In							

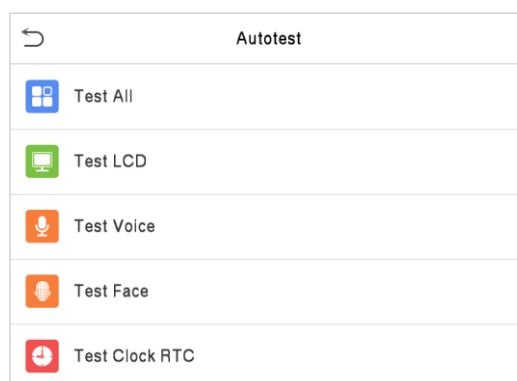
3. The record search succeeds. Click the record to view its details

4. The record details will be displayed as shown above.

## 18 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.

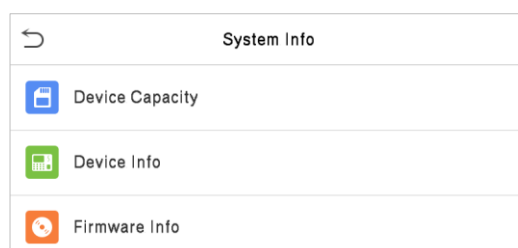


Menu	Description
<b>Test All</b>	To automatically test whether the LCD, audio, camera and RTC are normal.
<b>Test LCD</b>	To automatically test the display effect of LCD screen by displaying full-color, pure white, and pure black to check whether the screen displays colors normally.
<b>Test Voice</b>	To automatically test whether the audio files stored in the device are complete and the voice quality is good.
<b>Camera Testing</b>	To test if the camera functions properly by checking the pictures taken to see if they are clear enough.
<b>Test Clock RTC</b>	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.

## 19 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	Description
<b>Device Capacity</b>	Displays the current device's user storage, password and face storage, administrators, access records, attendance and blocklist photos, and user photos.
<b>Device Info</b>	Displays the Device's name, Serial number, MAC address, Face algorithm version information, Platform information, and Manufacturer details.
<b>Firmware Info</b>	Displays the Firmware version and other version information of the device.

## 20 Connect to ZKBioSecurity MTD Software

### 20.1 Set the Communication Address

#### **Device side**

1. Click **COMM. > Ethernet** in the main menu to set the 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.

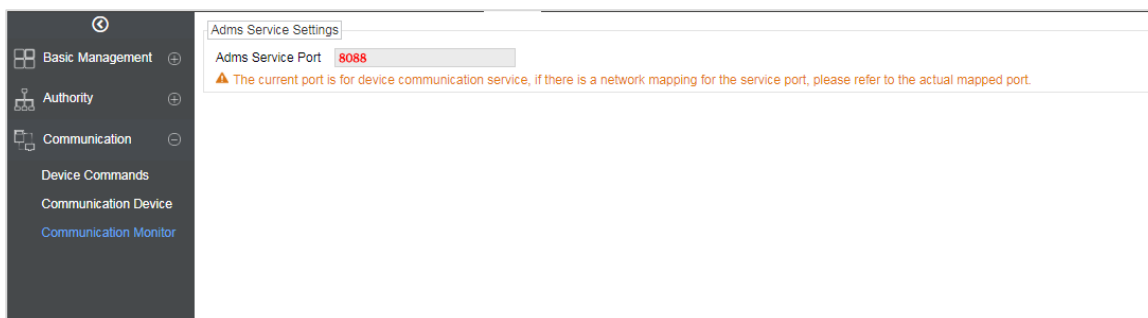
**Server address:** Set as the IP address of ZKBioSecurity MTD server.

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

Ethernet	Cloud Server Setting
IP Address 192.168.163.201	Server Mode ADMS
Subnet Mask 255.255.255.0	Enable Domain Name <input type="checkbox"/>
Gateway 0.0.0.0	Server Address 0.0.0.0
DNS 0.0.0.0	Server Port 8081
TCP COMM.Port 4370	Enable Proxy Server <input type="checkbox"/>
DHCP <input type="checkbox"/>	HTTPS <input type="checkbox"/>
Display in Status Bar <input checked="" type="checkbox"/>	

## Software Side

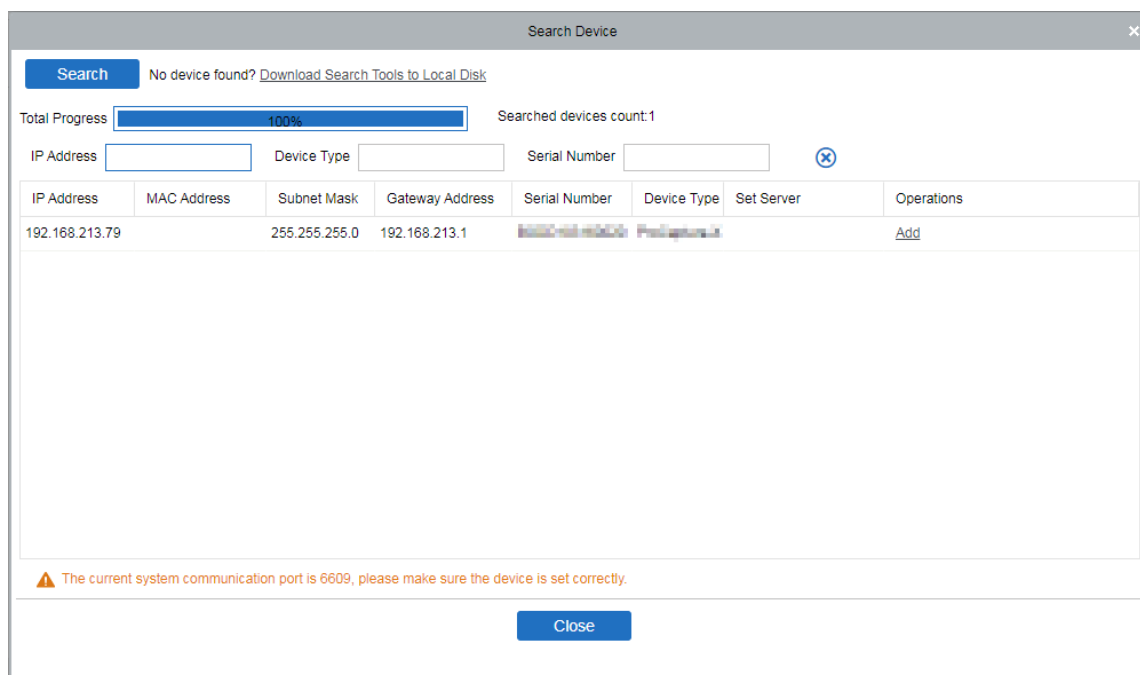
Login to ZKBioSecurity MTD software, click **System > Communication > Communication Device** to set the ADMS service port, as shown in the figure below:



## 20.2 Add Device to the Software

You can add a device by searching it. 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.

## 20.3 Add Personnel on the Software

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

**New**

Personnel ID\* 656 Department\* ZOITestDept

First Name Last Name

Gender Mobile Phone

Certificate Type Certificate Number

Birthday Email

Hire Date Position Name

Device Verification Password Card Number

Biological Template Quantity

Access Control Time Attendance Elevator Control Plate Register FaceKiosk Face Intellect Personnel Detail

Levels Settings

☒ General

Add Select All Unselect All

Superuser No

Device Operation Role Ordinary User

Delay Passage ☐

Disabled ☐

Set Valid Time ☐

Save and New OK Cancel

2. Enter the required details and click **OK**.

## 20.4 Real-time monitoring on the Software

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

**ZKTECO** Welcome, admin

2020-05-28 11:03:07

**Real-Time Monitoring**

Total: 217 20 150 61

**Abnormal Temperature**

40.1°C

Mask: None

Name: (19961107)

Department: null

Time: 09:50:48

**No Masks**

None

Temperature: 36.65°C

Name: UnregisterUser

Department: NULL

Time: 14:42:00

**Normal Records**

36.57°C

Name: UnregisterUser

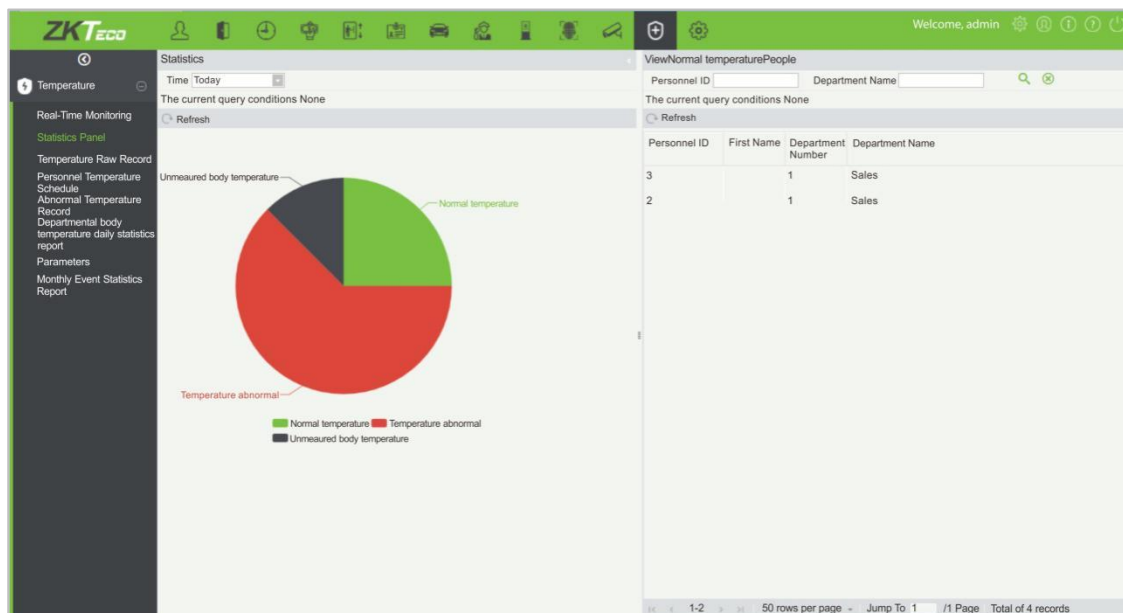
Department: NULL

Mask: Yes

Time: 15:01:39

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

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



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



## **Appendix 1**

### **Requirements of Live Detection 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 focus on 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 tilt your head. Two images are required for persons with eyeglasses, one image with eyeglasses and one other without eyeglasses.
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 show more than one face in the capturing area.
9. The recommended capturing distance is 50cm - 80cm adjustable subject to body height.



Image1-Face Capture Area

## Requirements for Visible Light Digital Face Image Data

The digital photo should be straight edged, colored, half-portrayed with only one person. Persons who wear eyeglasses should put on their eyeglasses for photo capturing.

### **Eye Distance**

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

### **Facial Expression**

A plain face or smile with opened eyed is recommended.

### **Gesture and Angle**

The horizontal rotating angle should not exceed  $\pm 10^\circ$ , elevation should not exceed  $\pm 10^\circ$ , and the depression angle should not exceed  $\pm 10^\circ$ .

### **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**

The image format should be in BMP, JPG or JPEG.

### **Requirements**

The image data 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 iris should be clearly visible.
8. Normal face or smile is preferred. Grin is not recommended.
9. The captured person should be clearly seen, natural in color, and without image twist, 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 Chinese law 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.

ZKTeco Industrial Park, No. 26, 188 Industrial Road,  
Tangxia Town, Dongguan, China.

Phone : +86 769 - 82109991

Fax : +86 755 - 89602394

[www.zkteco.com](http://www.zkteco.com)

