

User Manual

Elite Series

Applicable models: Elite Pass, Elite Access

Version: 1.1

Date: February 2020

Copyright © 2020 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 equipment. The copyright in all the documents, drawings, etc. in relation to the ZKTeco supplied equipment vests in and is the property of ZKTeco. The contents hereof should not be used or shared by the receiver with any third party without express written permission of ZKTeco.

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

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

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

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

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

ZKTeco in no event shall be liable to the user or any third party for any incidental, consequential, indirect, special, or exemplary damages, including, without limitation, loss of business, loss of profits, business interruption, loss of business information or any pecuniary loss, arising out of, in connection with, or

relating to the use of the information contained in or referenced by this manual, even if ZKTeco has been advised of the possibility of such damages.

This manual and the information contained therein may include technical, other inaccuracies or typographical errors. ZKTeco periodically changes the information herein which will be incorporated into new additions/amendments to the manual. ZKTeco reserves the right to add, delete, amend or modify the information contained in the manual from time to time in the form of circulars, letters, notes, etc. for better operation and safety of the machine/unit/equipment. The said additions or amendments are meant for improvement /better operations of the machine/unit/equipment and such amendments shall not give any right to claim any compensation or damages under any circumstances.

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

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

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

ZKTeco Headquarters

Address ZKTeco Industrial Park, No. 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.

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

About the Company

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

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

About the Manual

This manual introduces the operations of Elite Series product.

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

Table of Contents

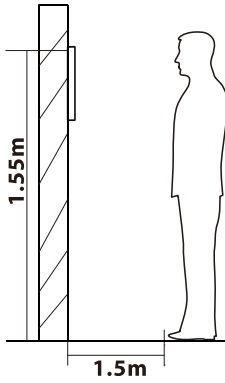
1	Notice for Use	1
1.1	Standing Position, Facial Expression and Standing Posture.....	1
1.2	Face Registration.....	2
1.3	Standby Interface.....	3
1.4	Virtual Keyboard.....	4
1.5	Verification Mode.....	5
1.5.1	Password Verification.....	5
1.5.2	Facial Verification.....	9
1.5.3	Combined Verification.....	12
2	Main Menu	13
3	User Management	14
3.1	Add Users	14
3.2	Search for Users.....	18
3.3	Edit Users.....	19
3.4	Delete Users.....	19
4	User Roles.....	20
5	Communication Settings.....	22
5.1	Network Settings.....	22
5.2	PC Connection.....	24
5.3	Cloud Server Settings.....	25
5.4	Wiegand Setup.....	26
6	System Settings.....	29
6.1	Date and Time.....	29
6.2	Access Logs Settings.....	30
6.3	Face Parameters.....	31
6.4	Factory Reset.....	33
6.5	Temperature Management.....	34
7.	Personalize Settings	35
7.1	Interface Settings.....	35
7.2	Voice Settings.....	36
7.3	Bell Schedules.....	37
8.	Data Management.....	38
8.1	Delete Data	38
9.	Access Control	40
9.1	Access Control Options.....	40
9.2	Time Rules.....	42
9.3	Holiday Settings.....	44

9.4	Combined Verification Settings.....	45
9.5	Anti-passback Setup	46
9.6	Duress Options.....	47
10.	Search for Logs.....	48
11.	Autotest.....	50
12.	System Information.....	51
13.	Connection to ZKBioSecurity Software.....	52
13.1	Set the Communication Address.....	52
13.2	Add a Device on the Software.....	53
13.3	Add Personnel on the Software.....	53
	Statement on the Right to Privacy.....	54
	Eco-friendly Use.....	55

1 Notice for Use

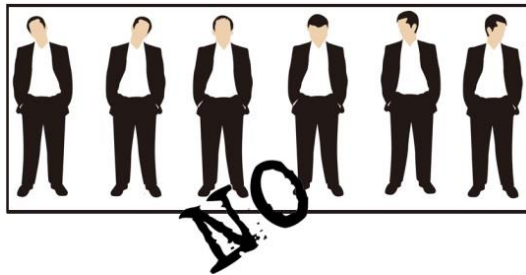
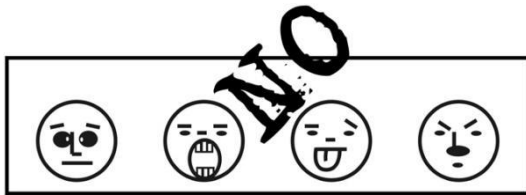
1.1 Standing Position, Facial Expression and Standing Posture

- The recommended distance



The distance between the device and a user whose height is within 1.55m-1.85m is recommended to be 1.5m. Users may slightly move forwards and backwards to improve the quality of facial images captured.

- Facial expression and standing posture



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

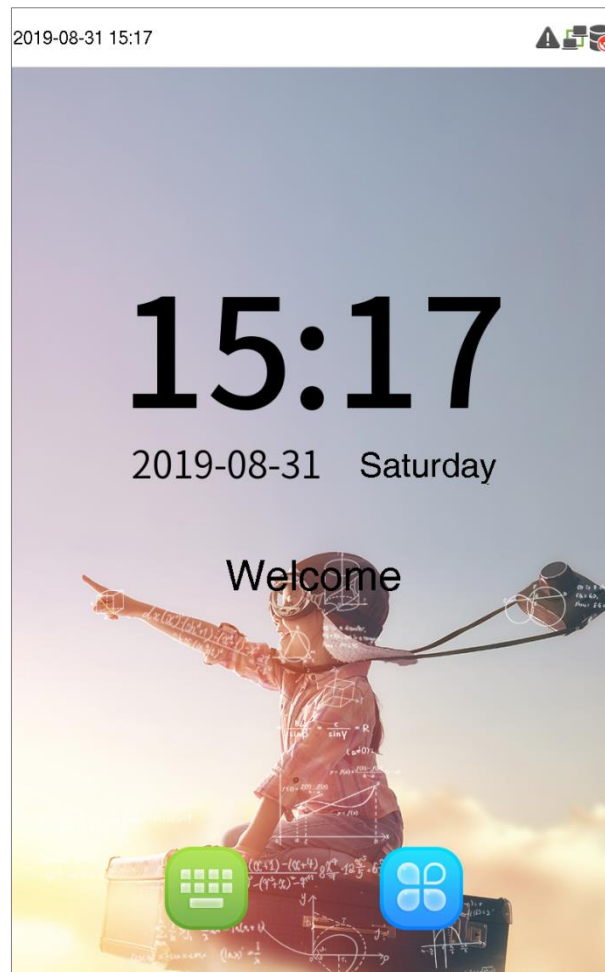
1.2 Face Registration

Try keeping the face at the center of the screen during registration. Please look straight at the camera and stay still during face registration as shown below.





1.3 Standby Interface

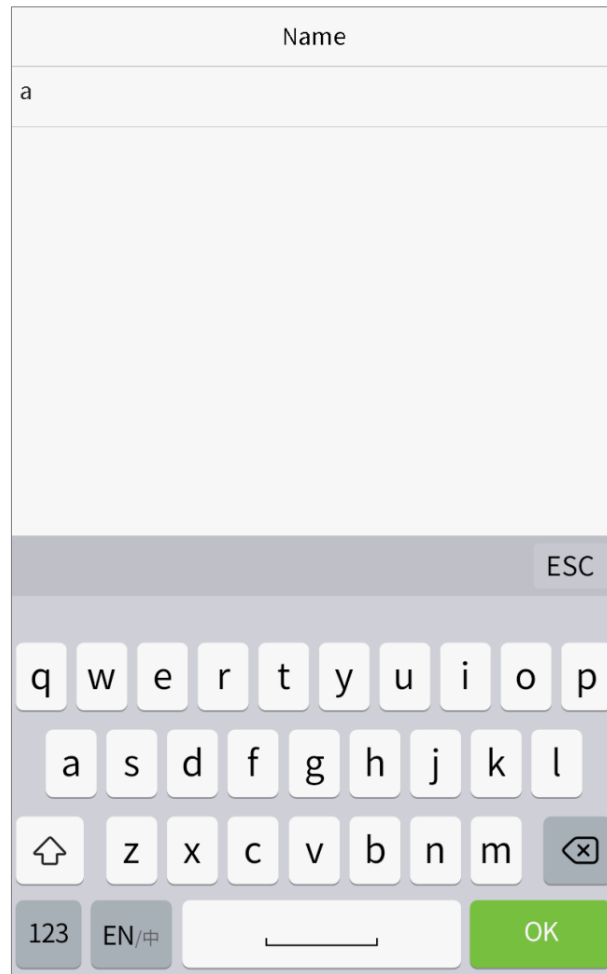
After connecting to the power supply, you will access the following standby interface:



Notes:

1. Click  to enter the User ID input interface.
2. When there is no super administrator set in the device, click  to enter the menu and set one. After setting the super administrator account, the user must verify his/her super administrator's identity before entering the menu. For the security purpose, it is recommended to register for a super administrator account for the first time using the device.

1.4 Virtual Keyboard




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

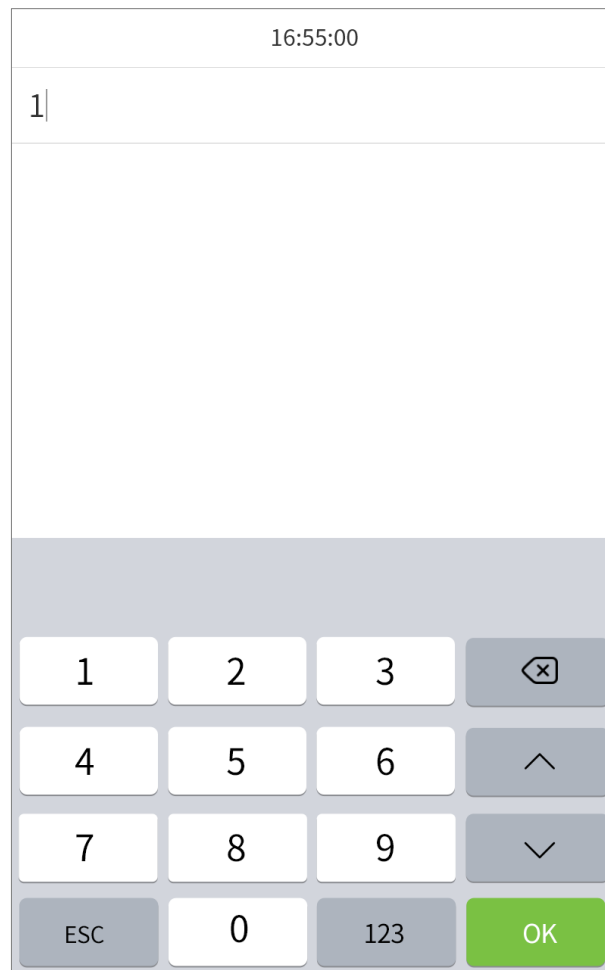
1.5 Verification Mode

1.5.1 Password Verification


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

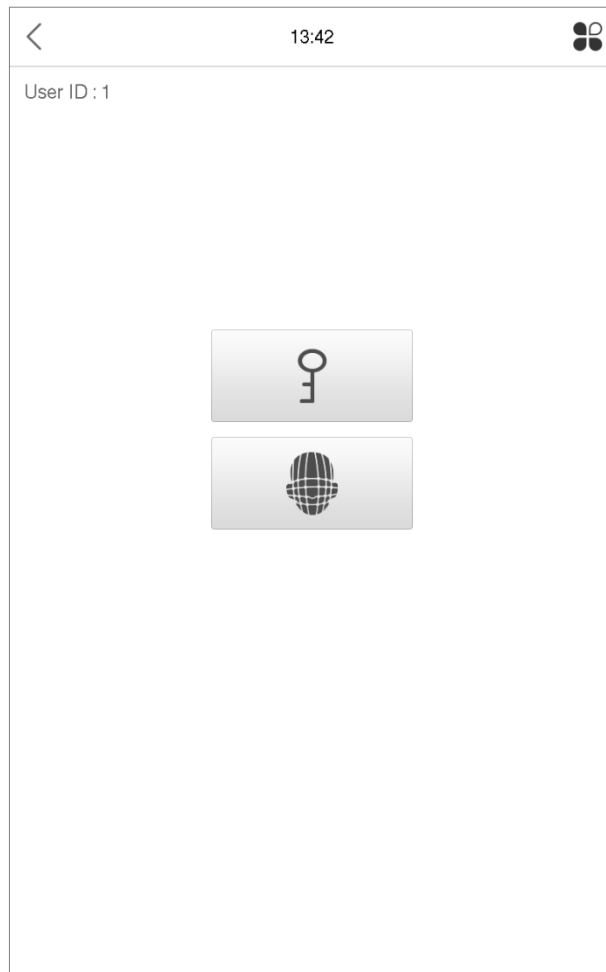
Click the  button on the main screen to enter the 1:1 password verification mode.

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

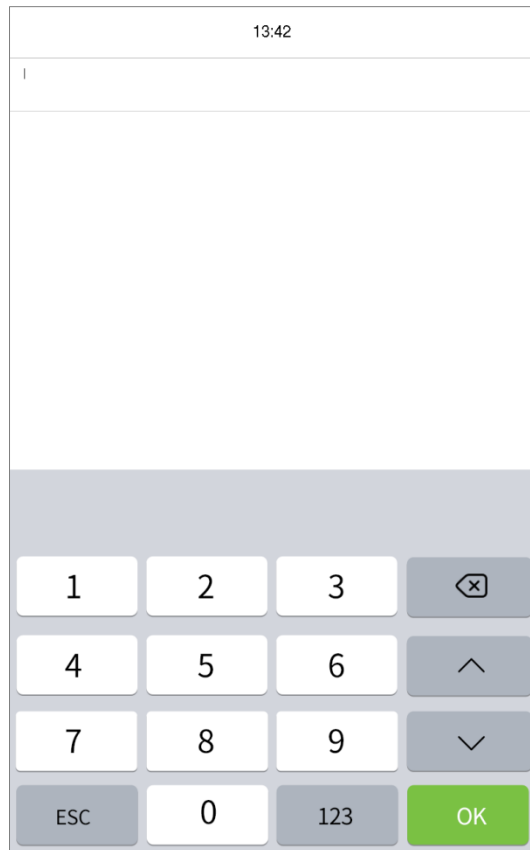


The screenshot shows a mobile application interface for password verification. At the top, the time is 16:55:00. Below the time is a text input field containing the digit '1'. The bottom half of the screen features a numeric keypad with buttons for digits 1-9, 0, and function keys: ESC, 123, a backspace key (X), an up arrow key (^), and a down arrow key (v). The OK button is highlighted in green.

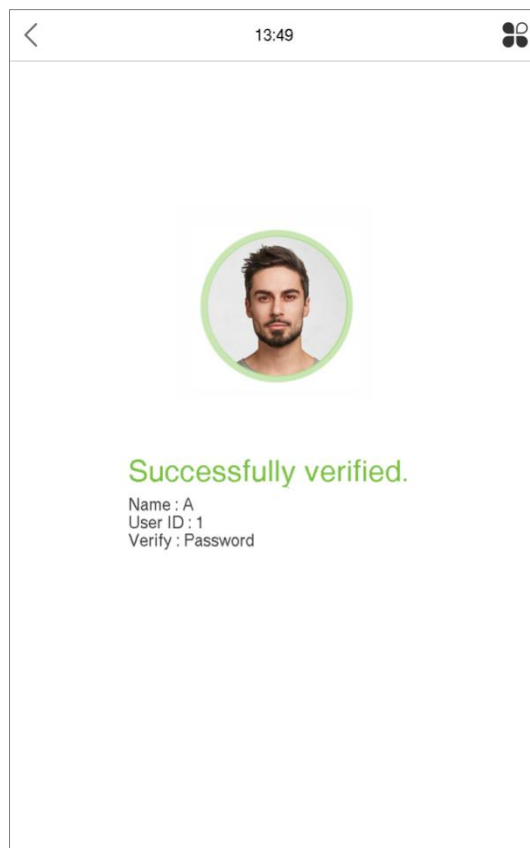
If the user has enrolled a facial template and set a password for verification, the following screen will appear. Select the  icon to enter password verification mode.



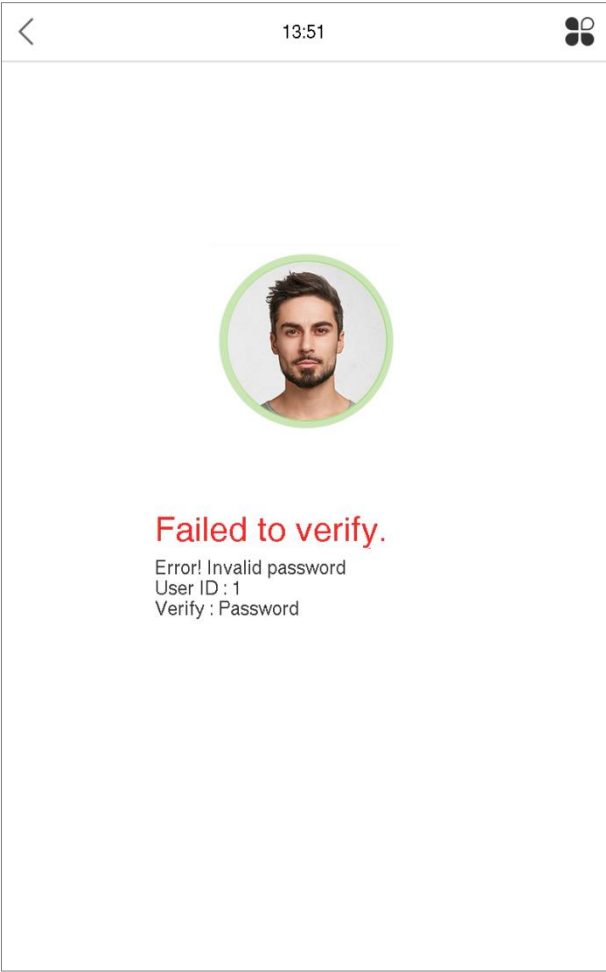
2. Input the password and press [OK].



Verification is successful.



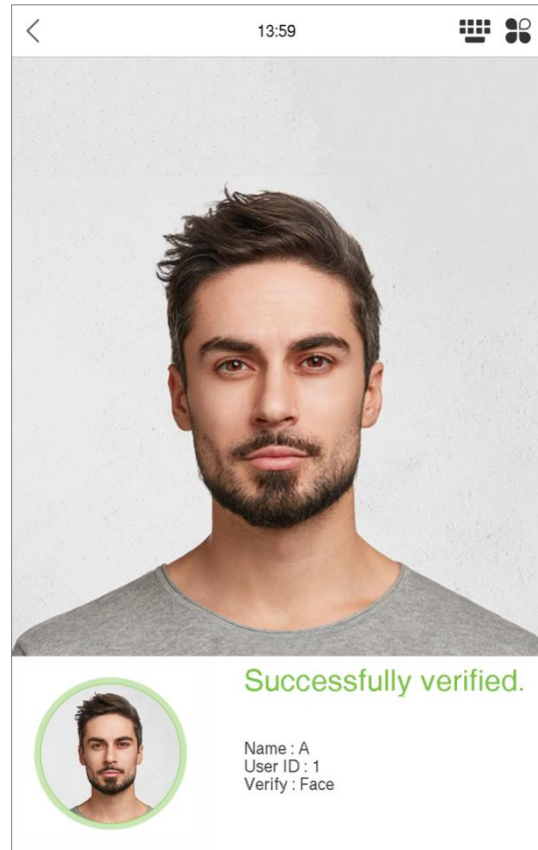
Verification is failed.



1.5.2 Facial Verification

- **1:N facial verification**

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

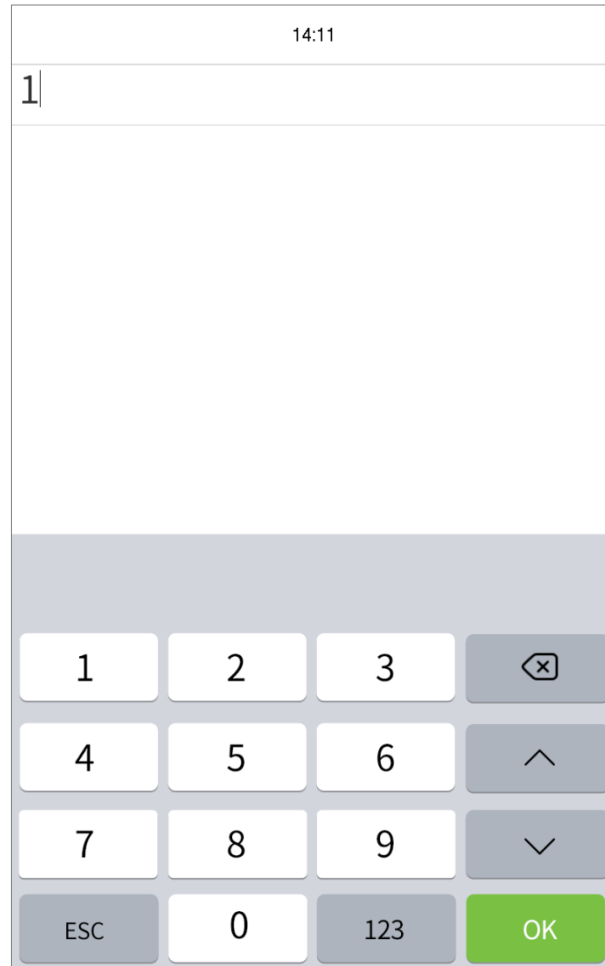


- **1:1 facial verification**

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

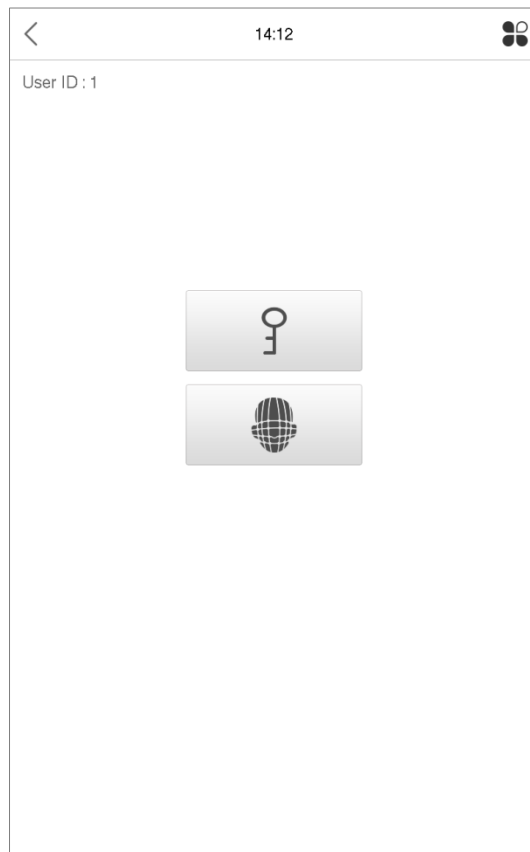
Press  on the main interface and enter the 1:1 facial verification mode.

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

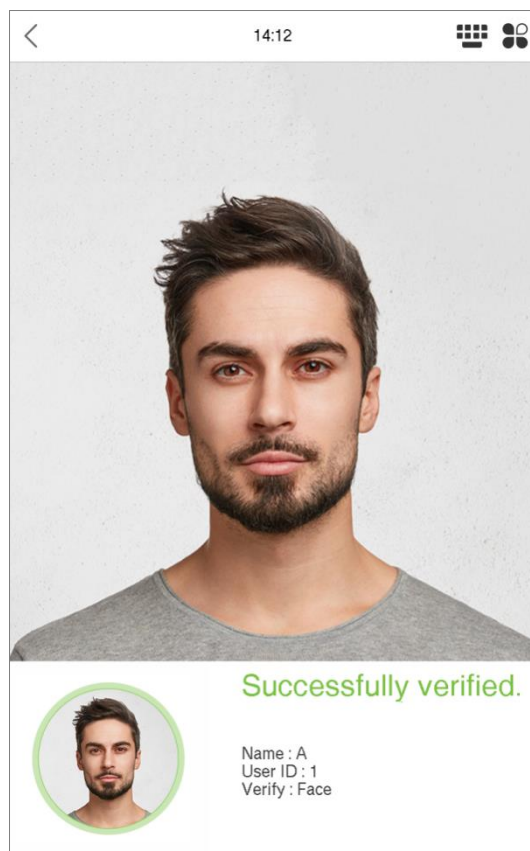


If the user has set a password and enrolled a facial template for verification, the following screen will appear. Select

the  icon to enter the facial verification mode.



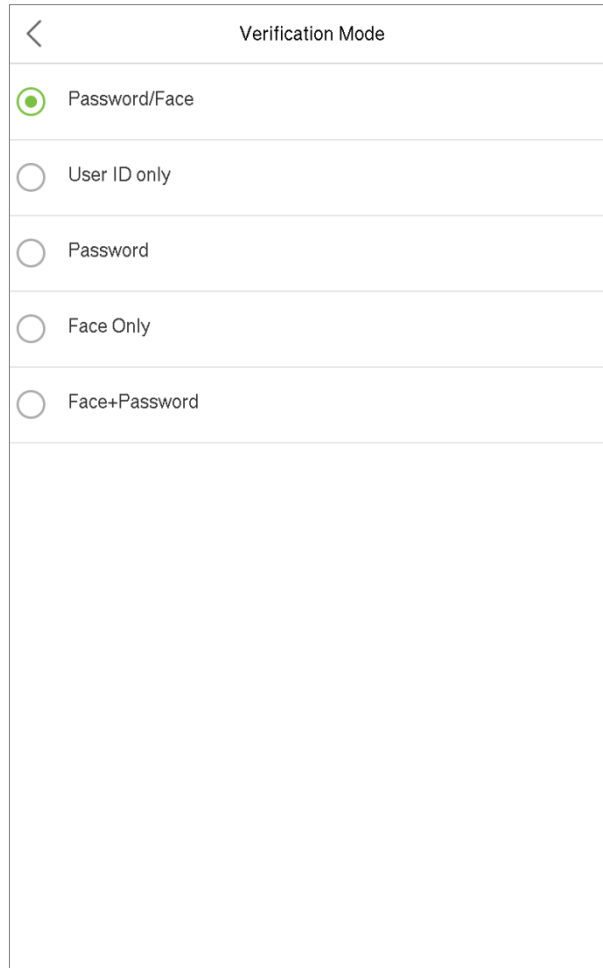
After successful verification, the system will prompt as below.



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

1.5.3 Combined Verification

To increase the level of security, this device offers options of multiple forms of verification methods. A total of 5 different verification combinations can be used, as shown below:



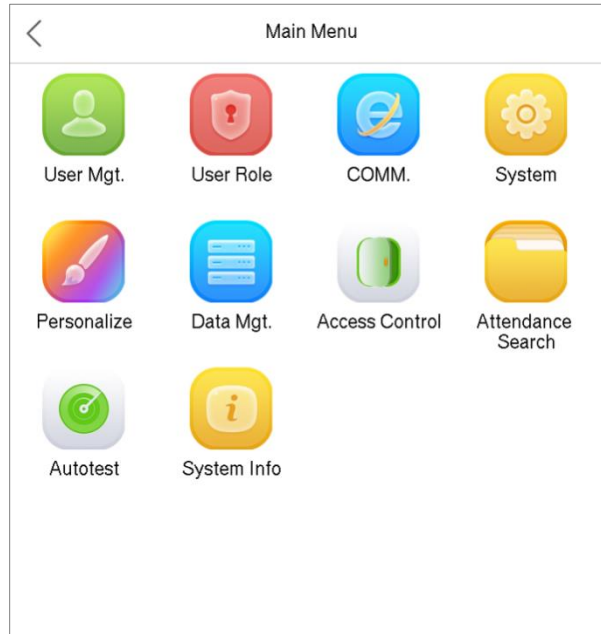
The screenshot shows a mobile application interface titled "Verification Mode". It features a list of five radio button options for selecting a verification method. The first option, "Password/Face", is selected, indicated by a green dot inside the radio button. The other options are "User ID only", "Password", "Face Only", and "Face+Password", each with an unselected white radio button. The interface has a simple, clean design with a white background and grey text.

Notes:

- 1) "/" means "or", and "+" means "and".
- 2) You must register for the required verification information before using verification combination, otherwise the verification may fail. For example, if a user who only registered with a facial template chooses "Face + Password" as the verification mode, this user will never pass verification.

2 Main Menu

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

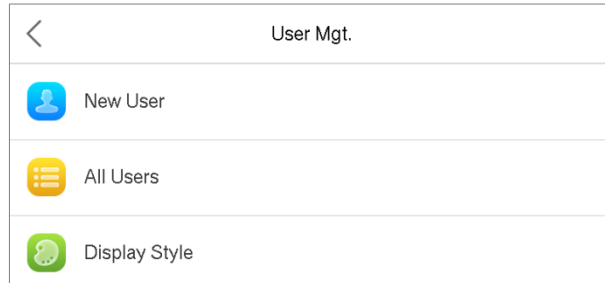


Item	Descriptions
User Mgt.	To add, edit, view, and delete basic information about a user.
User Role	To set the permission scope of the custom role and enroller, that is, the rights to operate the system.
COMM.	To set the relevant parameters of network, PC connection, cloud server and Wiegand.
System	To set parameters related to the system, including date & time, access records, facial templates, resetting to factory settings and temperature management.
Personalize	To customize settings of interface display, audio and bell.
Data Mgt.	To delete all relevant data in the device.
Access Control	To set the parameters of the lock and the relevant access control device.
Attendance Search	Query the specified access record, check attendance photos and blacklist photos.
Autotest	To automatically test whether each module functions properly, including the screen, audio, camera and real-time clock.
System Info	To view data capacity, device and firmware information of the current device.

3 User Management

3.1 Add Users

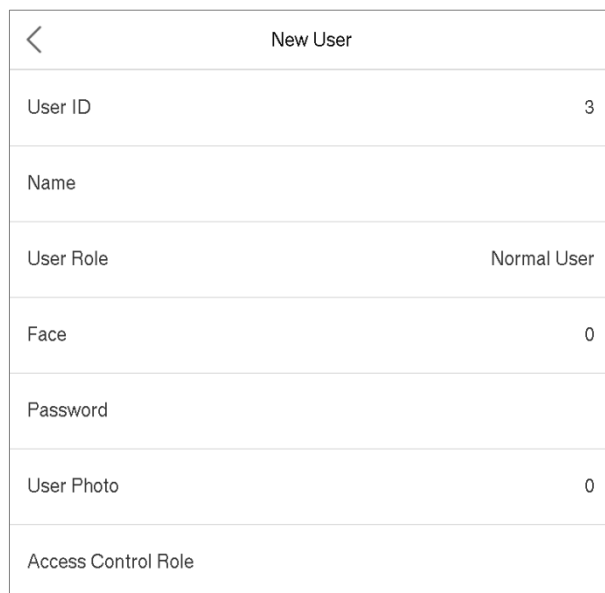
Click **User Mgt.** on the main menu.



Click **New User**.

- **Register with a User ID and Name**

Enter the user ID and name.



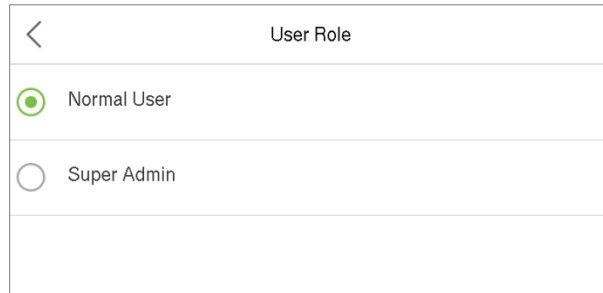
Notes:

- 1) A user name may contain 17 characters.
- 2) The user ID may contain 1-9 digits by default.
- 3) During the initial registration, you can modify your ID, which cannot be modified after registration.
- 4) If a message "The ID is already existed" pops up, you must choose another ID.

- **Setting the User Role**

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

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



Note: If the selected user role is the Super Admin, the user must pass the identity authentication to access the main menu. The authentication is based on the authentication method(s) that the super administrator has registered. Please refer to *1.5 Verification Mode*.

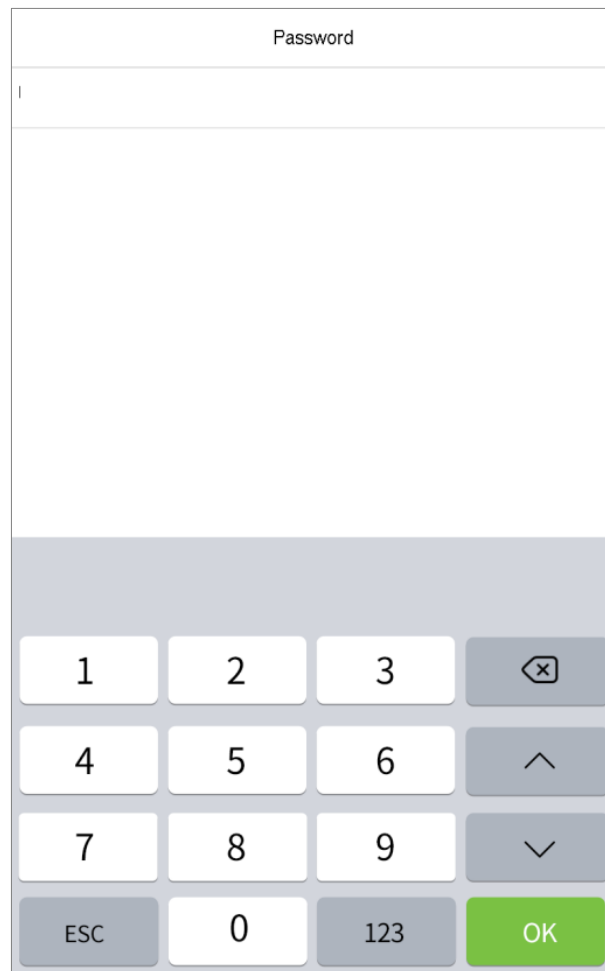
- **Register with a face**

Click **Face** to enter the facial registration interface. Please look straight at the camera and stay still during facial registration. The registration interface is as follows:



- **Register with a password**

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



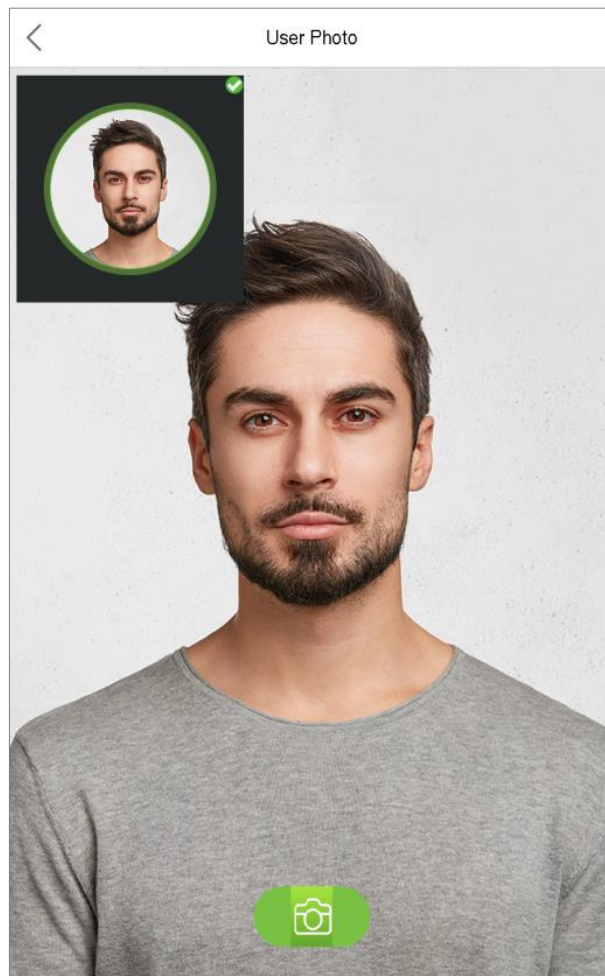
The image shows a password registration interface. At the top, the word "Password" is centered. Below it is a large, empty text input field. At the bottom of the screen is a numeric keypad with the following layout:

1	2	3	⌫
4	5	6	⤴
7	8	9	⤵
ESC	0	123	OK

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

- **Register with a user photo**

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



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

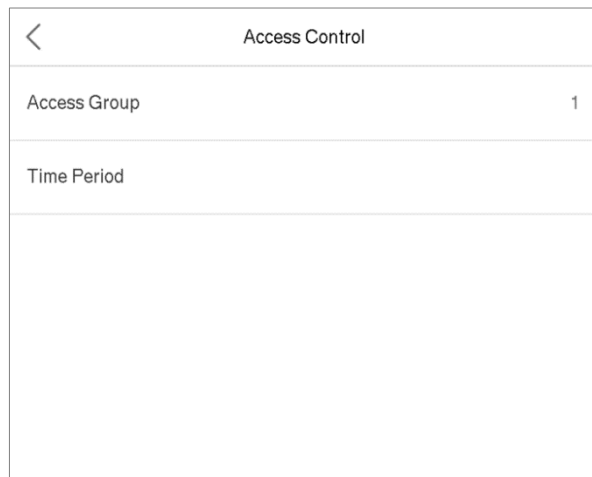
Note: While registering a face, the system will automatically capture a picture as the user photo. If you do not want to register for a user photo, the system will automatically set the picture captured as the default photo.

- **Access Control Role**

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

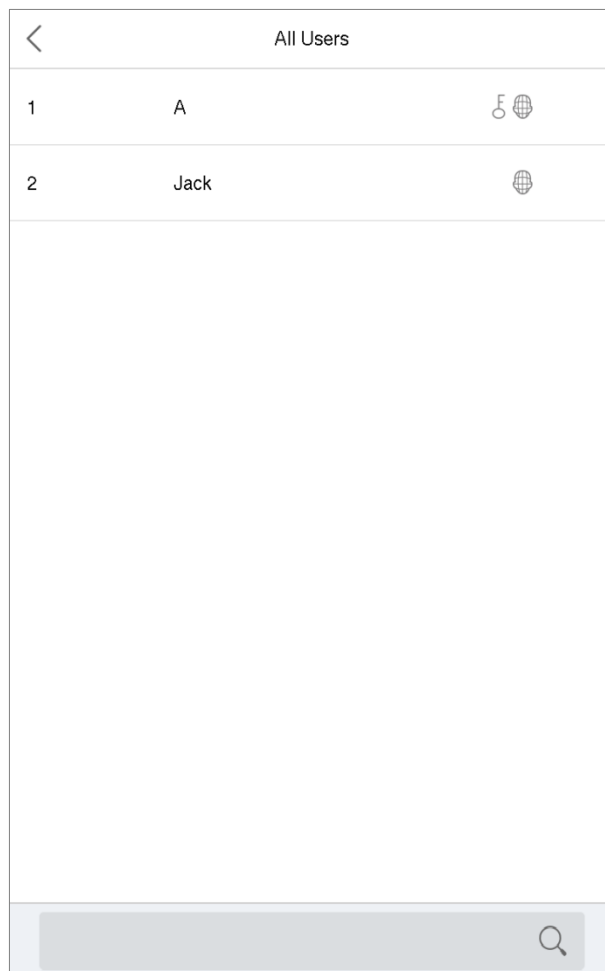
Click **Access Control Role > Access Group**, assign the registered users to different groups for better management. New users belong to Group 1 by default, and can be reassigned to other groups. The device supports up to 99 access control groups.

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



3.2 Search for Users

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



3.3 Edit Users

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

User : 1 A	
Edit	
Delete	

Edit : 1 A	
User ID	1
Name	A
User Role	Normal User
Face	1
Password	*****
User Photo	1
Access Control Role	

Note: The operation of editing a user is the same as that of adding a user, except that the user ID cannot be modified when editing a user. Operation method refers to "[3.1 new users](#)".

3.4 Delete Users

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

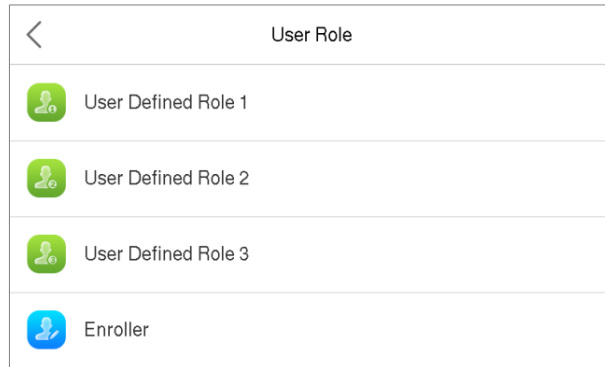
Note: If you select **Delete User**, all information of the user will be deleted.

4 User Roles

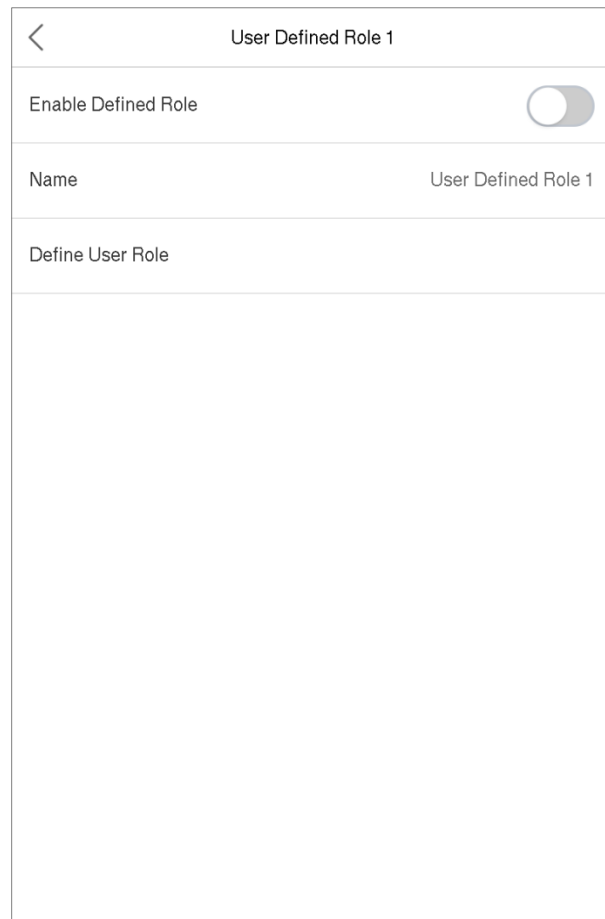
If you need to assign some specific permissions to certain users, you may edit the “User Defined Role” under the **User Role** menu.

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

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



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



2. Click **Define User Role** to assign the privileges to the role. When the privilege assignment is completed, click **Return**.

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 privilege assignment, the main menu is on the left and its sub-menus are on the right. You only need to select features shown in the 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.

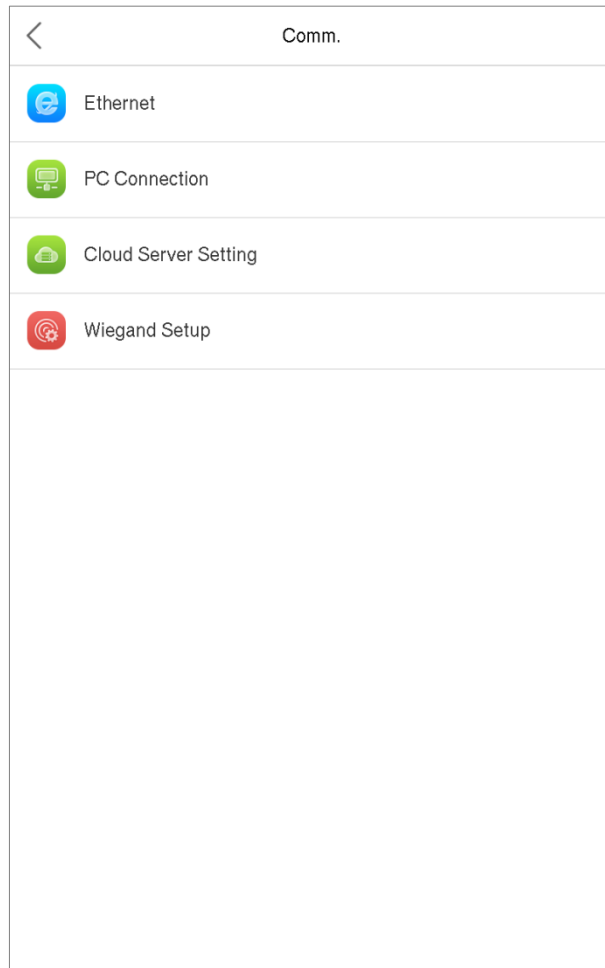
User Role	
<input checked="" type="radio"/>	Normal User
<input type="radio"/>	Enroller
<input type="radio"/>	User Defined Role 1
<input type="radio"/>	Super Admin

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

5 Communication Settings

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

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



5.1 Network Settings

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

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

Ethernet	
IP Address	192.168.163.200
Subnet Mask	255.255.255.0
Gateway	0.0.0.0
DNS	0.0.0.0
TCP COMM.Port	4370
DHCP	<input type="checkbox"/>
Display in Status Bar	<input checked="" type="checkbox"/>

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

5.2 PC Connection

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

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

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

PC Connection	
Comm Key	0
Device ID	1

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

5.3 Cloud Server Settings

This represents settings used for connecting with the ADMS server.

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

The screenshot shows a mobile application interface titled "Cloud Server Setting". It features a list of settings:

- Server Mode:** Set to "ADMS".
- Enable Domain Name:** A toggle switch that is currently turned off.
- Server Address:** Set to "0.0.0.0".
- Server Port:** Set to "8081".
- Enable Proxy Server:** A toggle switch that is currently turned off.

Item	Descriptions
Enable Domain Name	When this function is enabled, the domain name mode "http://..." will be used, such as http://www.XYZ.com, while "XYZ" denotes the domain name when this mode is turned ON.
Disable Domain Name	IP address of the ADMS server.
Server Address	Port used by the ADMS server.
Server Port	When you choose to enable the proxy, you need to set the IP address and port number of the proxy server.
Enable Proxy Server	

5.4 Wiegand Setup

To set the Wiegand input and output parameters.

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

<	Wiegand Setup
Wiegand Input	
Wiegand Output	

➤ Wiegand input

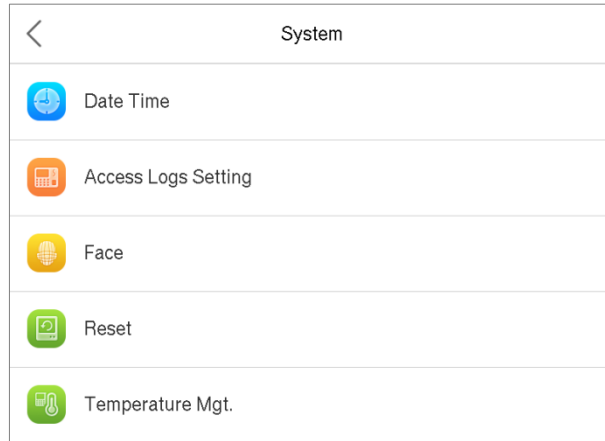
<	Wiegand Options
Wiegand Format	
Wiegand Bits	26
Pulse Width(us)	100
Pulse Interval(us)	1000
ID Type	Badge Number

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

6 System Settings

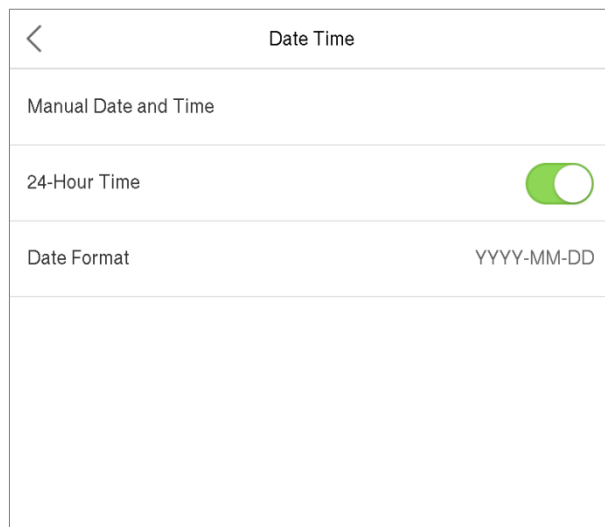
Set related system parameters to optimize the performance of the device.

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



6.1 Date and Time

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




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

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

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

6.2 Access Logs Settings

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

Access Logs Setting	
Camera Mode	No photo
Display User Photo	
Access Logs Warning	99
Circulation Delete Access Records	Disabled
Cyclic Delete ATT Photo	99
Cyclic Delete Blacklist Photo	99
Confirm Screen Delay(s)	3
Face comparison interval(s)	1

Item	Descriptions
Camera Mode	<p>Whether to capture and save the current snapshot image during verification. There are 5 modes:</p> <p>No Photo: No photo is taken during user verification.</p> <p>Take photo, no save: Photo is taken but is not saved during verification.</p> <p>Take photo and save: Photo is taken and saved during verification.</p> <p>Save on successful verification: Photo is taken and saved for each successful verification.</p> <p>Save on failed verification: Photo is taken and saved during each failed verification.</p>
Display User Photo	Whether to display the user photo when the user passes verification.
Access Logs Warning	When the remaining record space reaches a set value, the device will automatically display a remaining record memory warning. Users may disable the function or set a valid value between 1 and 9999.
Circulation Delete Access Records	When access records have reached full capacity, the device will automatically delete a set value of old access records. Users may disable the function or set a valid value between 1 and 999.
Cyclic Delete ATT Photo	When attendance photos have reached full capacity, the device will automatically delete a set value of old attendance photos. Users may disable the function or set a valid value between 1 and 99.

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

6.3 Face Parameters

Click **Face** on the System interface.

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

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

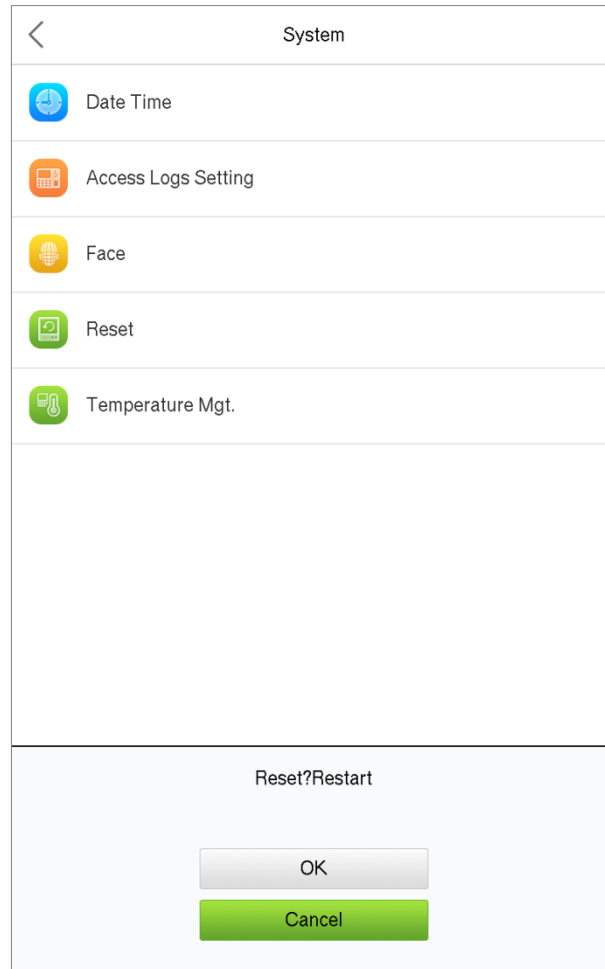
Item	Descriptions
1:N Match Threshold	Under 1:N verification mode, the verification will only be successful when the similarity between the acquired facial image and all registered facial templates is greater than the set value. The valid value ranges from 65 to 120. The higher the thresholds set, the lower the misjudgment rate, the higher the rejection rate, and vice versa.

1:1 Match Threshold	Under 1:1 verification mode, the verification will only be successful when the similarity between the acquired facial image and the facial templates enrolled in the device is greater than the set value. The valid value ranges from 55 to 120. The higher the thresholds set, the lower the misjudgment rate, the higher the rejection rate, and vice versa.
Face Enrollment Threshold	During face enrollment, 1:N verification is used to determine whether the user has been registered. The current face is registered when the similarity between the acquired facial image and all registered facial templates is greater than the set value.
Face Pitch Angle	To limit the pitch angle of face in face recognition, the recommended threshold is 20.
Face Rotation Angle	To limit the rotation angle of face in face recognition, the recommended threshold is 20.
Image Quality	To get the quality threshold of facial images. When the value of image quality is greater than the set value, the device will accept the facial images and start the algorithm processing, otherwise, the device will filter the facial images out.
Minimum Face Size	To limit the face detection pixel of face in face recognition, the recommended threshold is 80.
LED Light Triggered Threshold	Detect ambient light intensity. When the ambient brightness is less than the threshold, the fill light is turned on; When ambient brightness is greater than this threshold, the fill light does not turn on. The default value is 80.
Motion Detection Sensitivity	During face verification, the moving facial images collected in time are compared with all the facial images in the device by the corresponding algorithm. If the value is greater than or equal to the set value, it means that the verification passes; otherwise, it means that the verification fails.
Live Detection	If enabled, it will automatically detect whether there is a moving person in front of the device.
Live Detection Threshold	Detect whether there is a moving person in front of the device to determine whether face recognition is enabled. The default value is 100. The valid value ranges from 0 to 100.
Anti-counterfeiting with NIR	If enabled, the image will be taken from the black and white camera to determine whether the face is a real person.
WDR	Wide Dynamic
Anti-flicker Mode	To set up to prevent screen flicker.
Notes	Improper adjustment of the exposure and quality parameters may severely affect the performance of the device. Please adjust the exposure parameter only under the guidance of the after-sales service personnel of our company.

6.4 Factory Reset

Restore the device, such as communication settings and system settings, to factory settings without clearing registered user data.

Click **Reset** on the System interface.

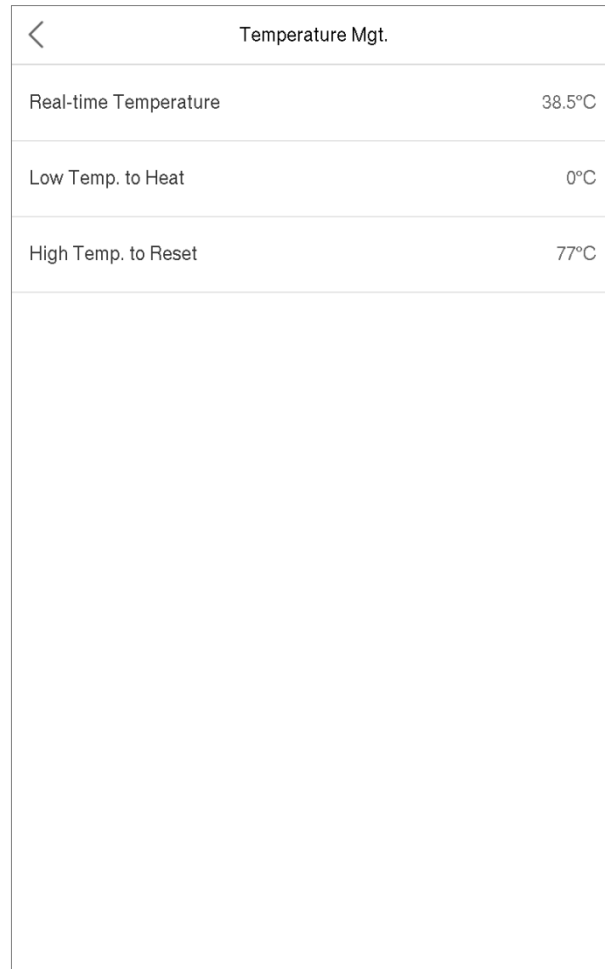


Click **OK** to reset.

6.5 Temperature Management

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

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



The screenshot shows a mobile interface titled "Temperature Mgt." with a back arrow on the left. It displays three rows of data: "Real-time Temperature" at 38.5°C, "Low Temp. to Heat" at 0°C, and "High Temp. to Reset" at 77°C. Below these rows is a large empty white space.

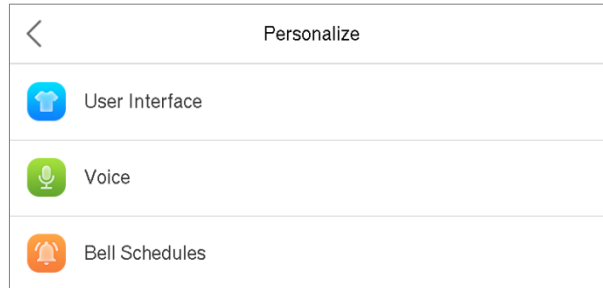
Temperature Mgt.	
Real-time Temperature	38.5°C
Low Temp. to Heat	0°C
High Temp. to Reset	77°C

Item	Descriptions
Real-time Temperature	This column shows real-time inner temperature of terminal.
Low temp. to Heat	When the terminal's temperature is lower than the set value, it will start self-heating, the set range is 0~10°C.
High Temp. to Reset	When the terminal's temperature is high than the set value, it will shut down automatically to protect the hardware; the set range is 60~80°C.

7. Personalize Settings

You may customize interface settings, audio and bell.

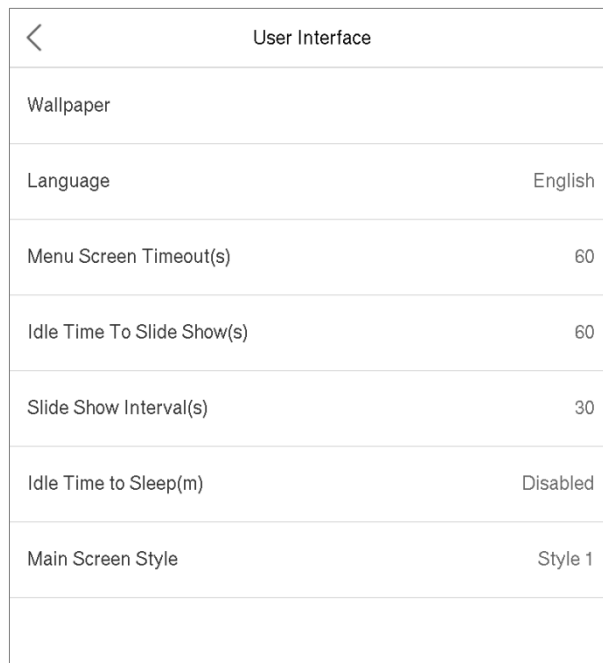
Click **Personalize** on the main menu.



7.1 Interface Settings

You can customize the display style of the main interface.

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

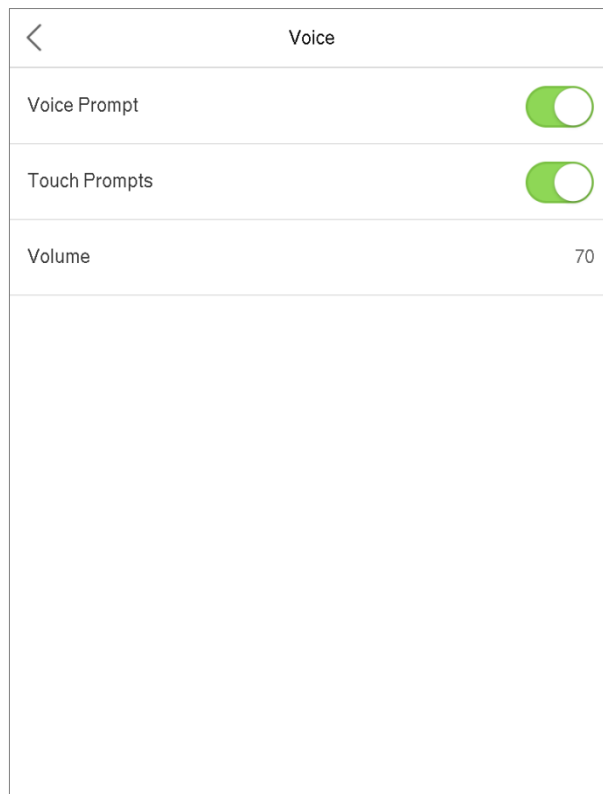


Item	Descriptions
Wallpaper	To select the main screen wallpaper according to your personal preference.
Language	To select the language of the device.
Menu Screen Timeout (s)	When there is no operation, and the time exceeds the set value, the device will automatically go back to the initial interface. You can disable the function or set the value between 60 and 99999 seconds.

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

7.2 Voice Settings

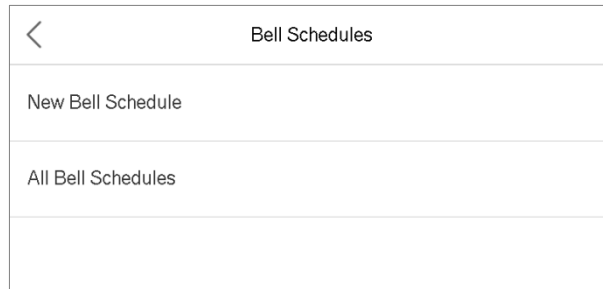
Click **Voice** on the Personalize interface.



Item	Descriptions
Voice Prompt	Select whether to enable voice prompts during operations.
Touch Sound	Select whether to enable keypad sound.
Volume	Adjust the volume of the device; valid value: 0-100.

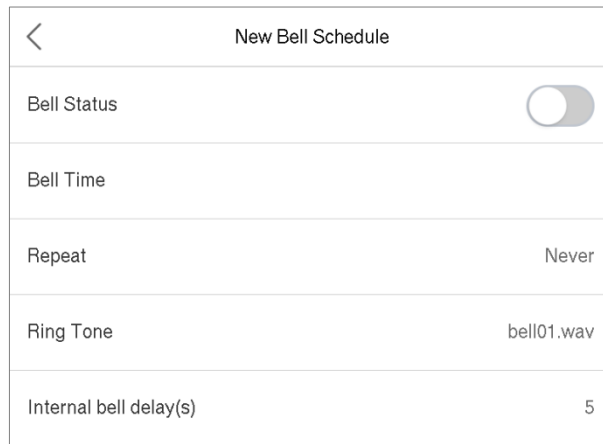
7.3 Bell Schedules

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



- **Add a bell**

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



Item	Descriptions
Bell Status	Show the bell status.
Bell Time	Set the time activating the bell.
Repeat	Set the repetition cycle of the bell.
Ring Tone	Select a ring tone.
Internal bell delay(s)	Duration of an internal bell. Valid value ranges from 1 to 999 seconds.

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

- **Edit a bell**

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

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

- **Delete a bell**

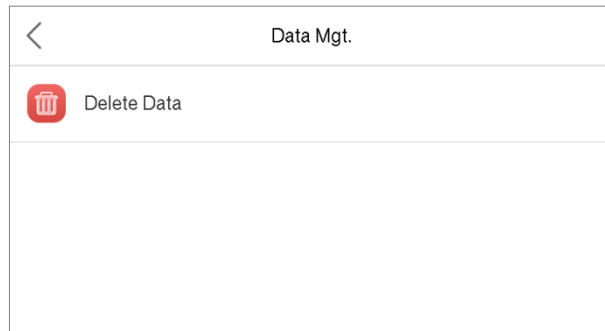
On the All Bell Schedules interface, tap the bell to be deleted.

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

8. Data Management

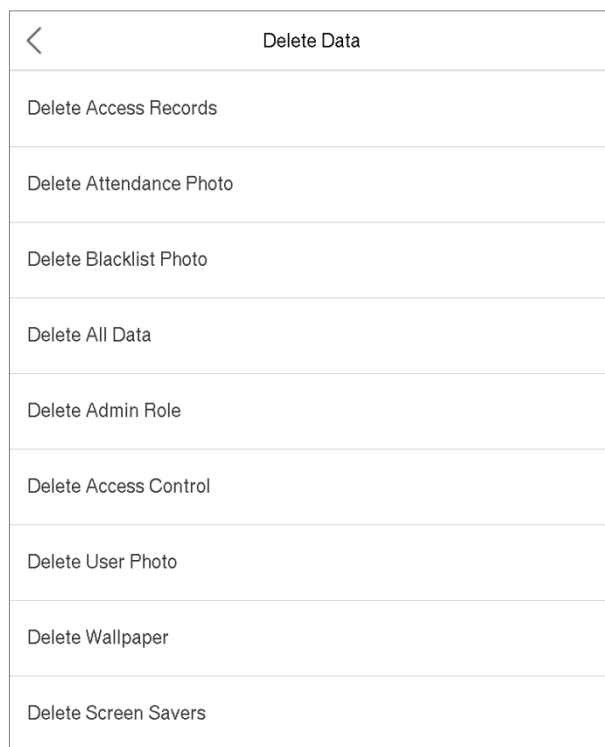
To delete the relevant data in the device.

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



8.1 Delete Data

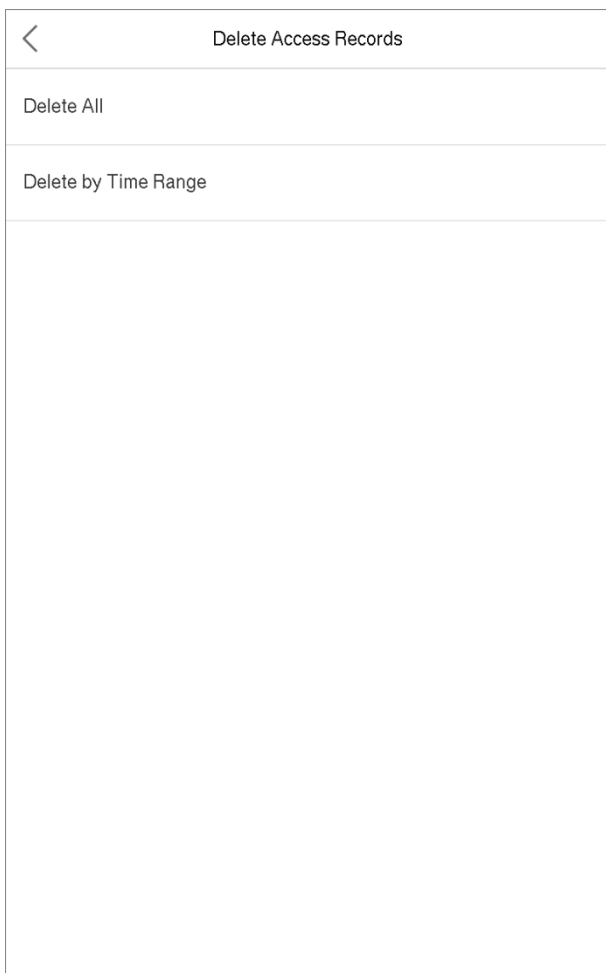
Click **Delete Data** on the Data Mgt. interface.



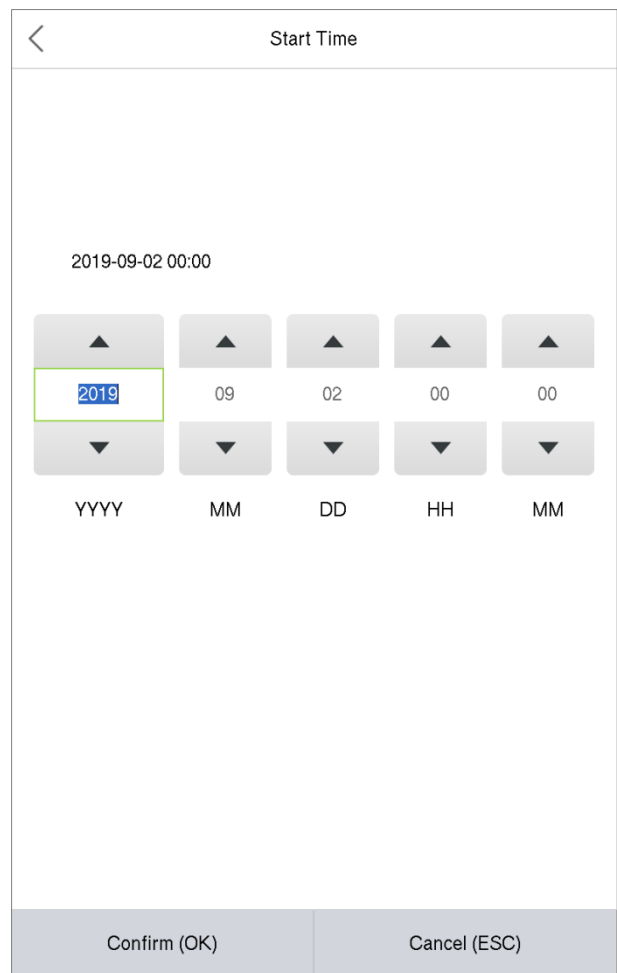
Item	Descriptions
Delete Access Records	To delete access records conditionally.
Delete Attendance Photo	To delete attendance photos of designated personnel.
Delete Blacklist Photo	To delete the photos taken during failed verifications.

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

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



Select Delete by Time Range.

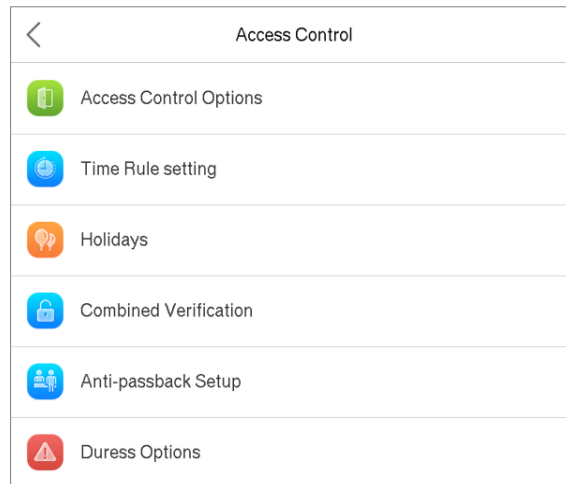


Set the time range and click OK.

9. Access Control

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

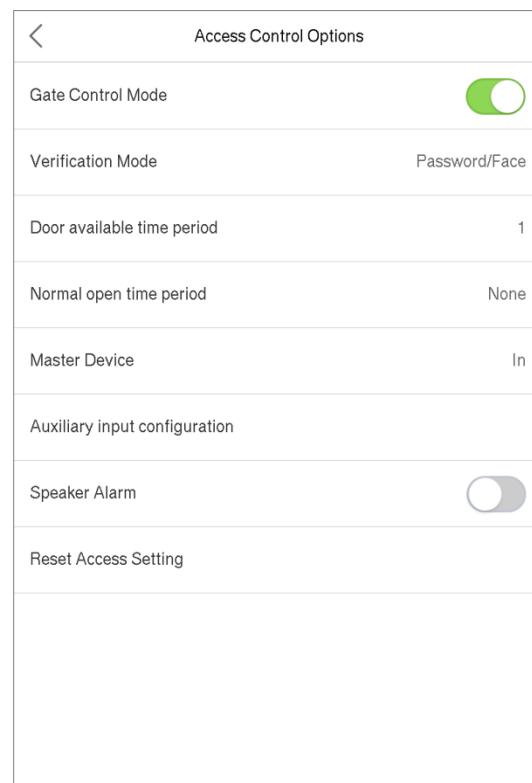
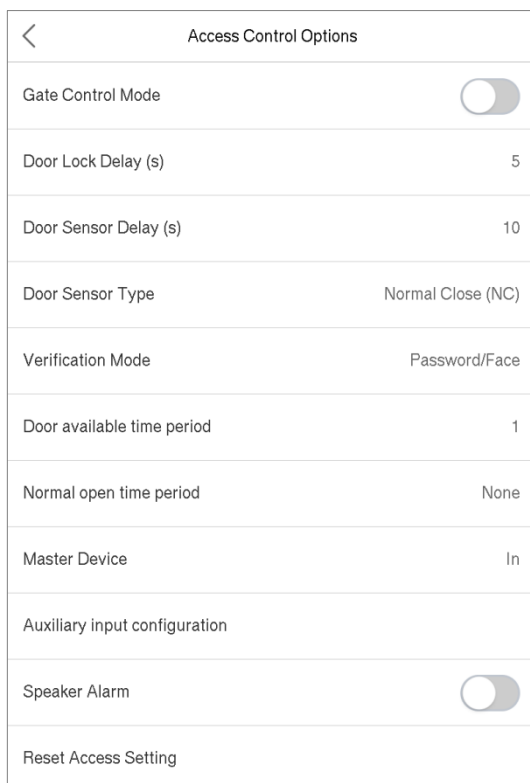
Click **Access Control** on the main menu.



9.1 Access Control Options

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

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



Item	Descriptions
Gate Control Mode	Select whether to enable the Gate Control Mode. When it is enabled, the Door Lock Relay, Door Sensor Relay and Door Sensor Type will not be displayed.
Door Lock Delay (s)	The device controls the opening duration of the electric lock. Valid value: 1~10s; 0 second represents disabling the function.
Door Sensor Delay (s)	If the door is not closed and locked after opening for a certain duration (Door Sensor Delay), an alarm will be triggered. The valid value of Door Sensor Delay ranges from 1 to 255 seconds.
Door Sensor Type	There are three types: None, Normal Open, and Normal Closed. None means door sensor is not in use; Normal Open means the door is always opened when electricity is on; Normal Closed means the door is always closed when electricity is on.
Verification Mode	The supported verification mode includes password/face, User ID only, password, face only, and face + password.
Door Available Time Period	The time period when the door can be unlocked and thus the restricted area can be accessed by the authorized user; it can be set to any of the 50 time rules.
Normal Open Time Period	Scheduled time period for "Normal Open" mode, so that the door is always unlocked during this period.
Master Device	When setting up the master and slave devices, the status of the master device can be set as out or in. Out: The record verified on the host is the exit record. In: The record verified on the host is the entry record.
Auxiliary Input Configuration	Set the door unlock time period and auxiliary output type of the auxiliary terminal device. Auxiliary output types include None, Trigger door open, Trigger Alarm, Trigger door open and Alarm.
Speaker Alarm	To transmit a sound alarm or disassembly alarm from the local. When the door is closed or the verification is successful, the system will cancel the alarm from the local.
Reset Access Setting	The restored access control parameters include door lock delay, door sensor delay, door sensor type, verification mode, door available time period, normal open time period, master device, and alarm. However, it does not include the deleted access control data in Data Management.

9.2 Time Rules

The device 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 gray box to input a time rule to search for. Enter the number of time rules (maximum: 50 rules).

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

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

The screenshot shows a configuration window titled "Time Period 1". At the top left is a back arrow. Below the title, the time range "00:00 23:59" is displayed. Underneath are four input fields for time components: HH, MM, HH, and MM. Each field has an up arrow button above it and a down arrow button below it. The first "HH" field is highlighted with a green border and contains the value "00". The other fields contain "00", "23", and "59" respectively. At the bottom of the window are two buttons: "Confirm (OK)" on the left and "Cancel (ESC)" on the right.

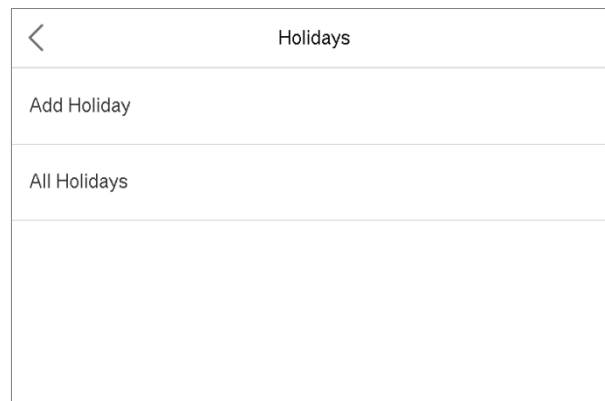
Notes:

- 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, the interval is valid.
- 2. The effective time period to unlock the door: open all day (00:00~23:59) or whenever the ending time is later than the starting time, such as 08:00~23:59.
- 3. The default time rule 1 indicates that door is open all day long.

9.3 Holiday Settings

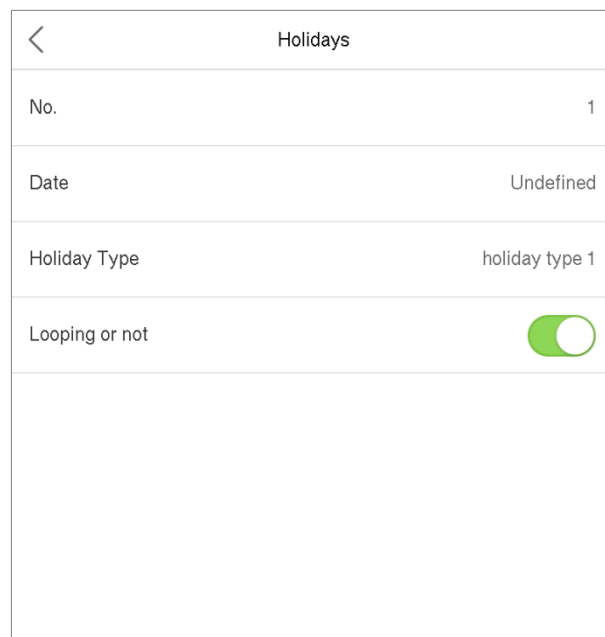
Whenever there is a holiday, you may need a special access time; but changing everyone's access time one by one is extremely cumbersome, so you can set a holiday access time which is applicable to all employees, and the user will be able to open the door during the holidays.

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



- **Add a New Holiday**

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



- **Edit a Holiday**

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

- **Delete a Holiday**

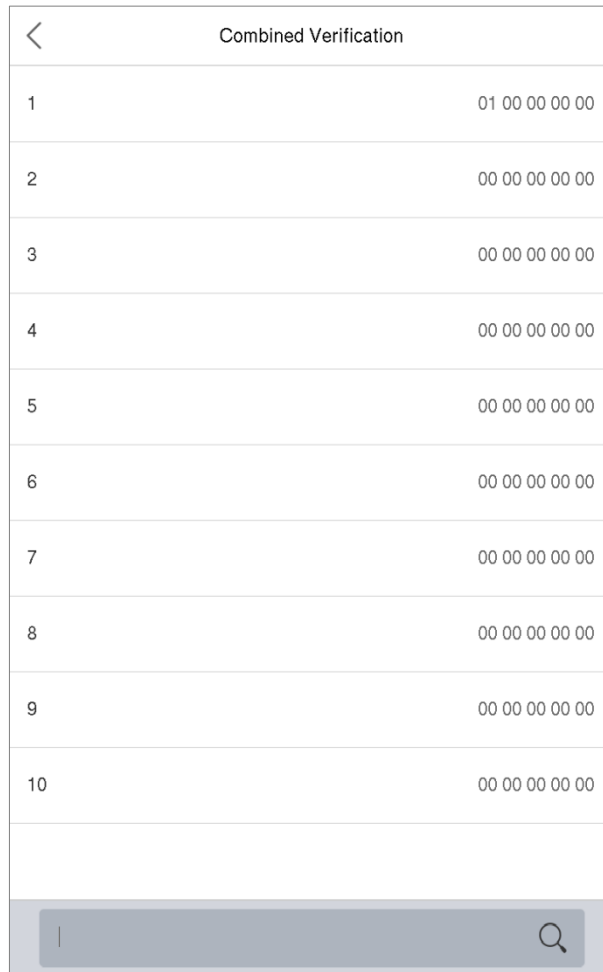
On the Holidays interface, select a holiday item to be deleted and click Delete. Click **OK** to confirm deletion. After deletion, this holiday is no longer displayed on All Holidays interface.

9.4 Combined Verification Settings

Access control groups are arranged into different door-unlocking combinations to achieve verification of multiple people at one time and strengthen the security.

In a door-unlocking combination, the number of the combination ranges from 0 to 5. Members being assigned in that combination may all belong to one access control group or may belong to five different access control 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

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 to (01 03 05 06 08), indicating that the unlocking combination 1 consists of 5 people, and the 5 individuals belong to 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 belong to AC group 2, the next two belong to AC group 4, and the last person belong to 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 belong to 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 belong to AC group 3, the second person belong to AC group 5, and the third person belong to AC group 8.

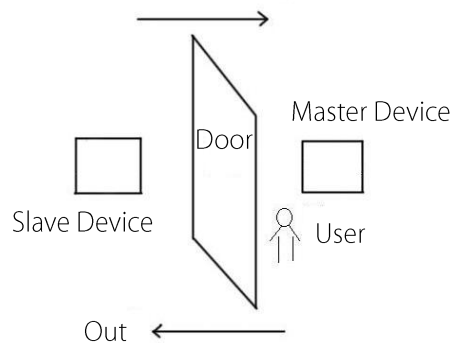
Delete a door-unlocking combination

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

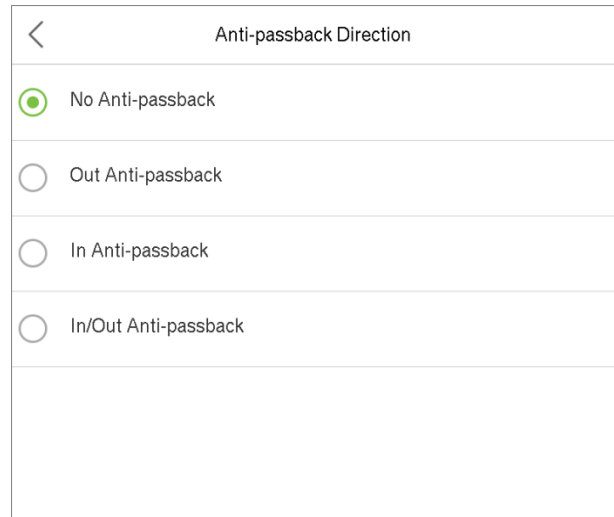
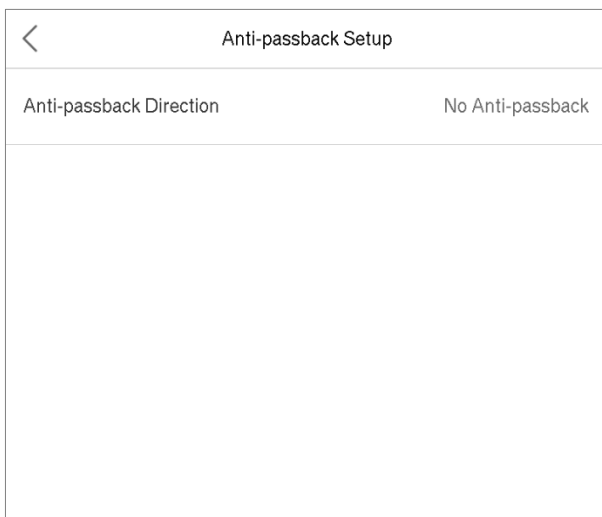
9.5 Anti-passback Setup

To avoid some persons following users and entering the door without verification, resulting in security problem, users can enable anti-passback function. The check-in record must match with the check-out record so as to open the door.

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



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

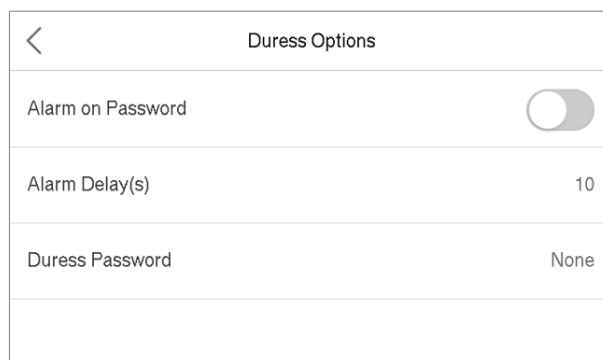


Item	Descriptions
No Anti-passback	Anti-Passback function is disabled, which means passing verification at either master device or slave device can unlock the door. Attendance state is not reserved.
Out Anti-passback	After a user checks out, only if the last record is a check-in record can the user check out again; otherwise, the alarm will be triggered. However, the user can check in freely.
In Anti-passback	After a user checks in, only if the last record is a check-out record can the user check in again; otherwise, the alarm will be triggered. However, the user can check out freely.
In/Out Anti-passback	After a user checks in/out, only if the last record is a check-out record can the user check in again, or a check-in record can the user check out again; otherwise, the alarm will be triggered.

9.6 Duress Options

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

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

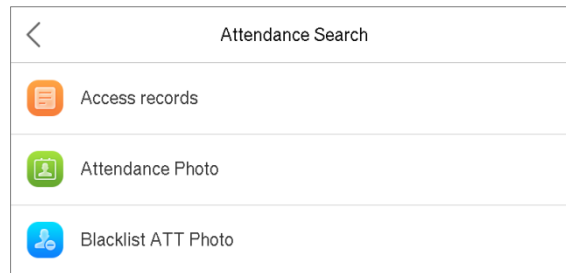


Item	Descriptions
Alarm on Password	When a user uses the password verification method, an alarm signal will be generated, otherwise there will be no alarm signal.
Alarm Delay (s)	Alarm signal will not be transmitted until the alarm delay time is elapsed. The value ranges from 1 to 999 seconds.
Duress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

10. Search for Logs

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.

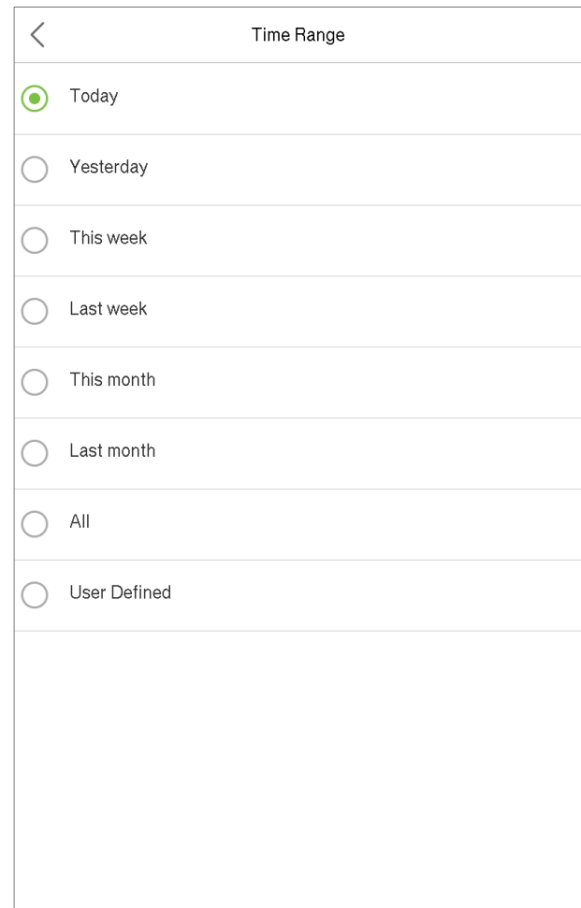
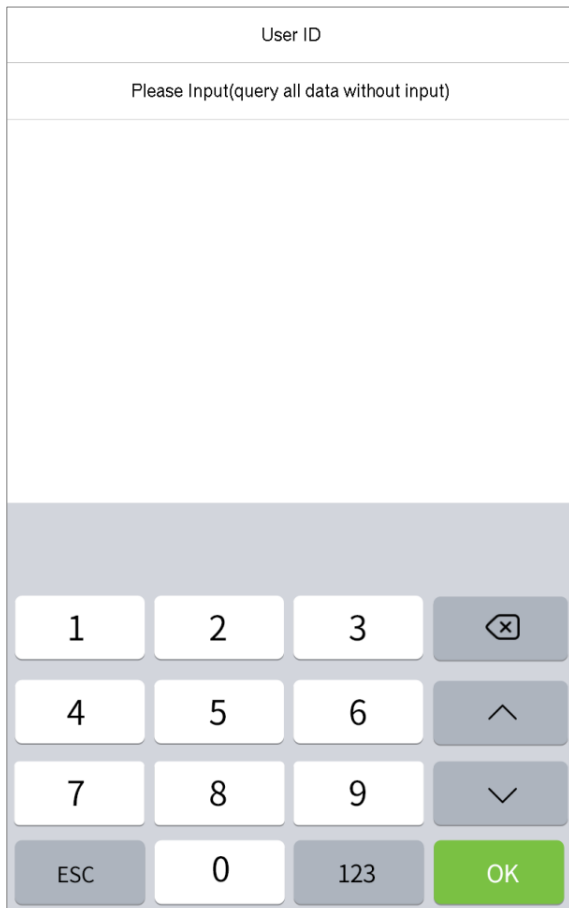


The process of searching for attendance and blacklist photos is similar to that of searching for access records. The following is an example of searching for access records.

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

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

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



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

Personal Record Search		
Date	User ID	Time
09-02		Number of Records:44
	2	14:07 14:07 14:07 14:07 14:07
		13:59 13:59 13:59 13:59 13:59
		13:59 13:59 13:59 13:59 13:59
		13:59 13:58 13:58 13:58 13:58
		13:58 13:58 13:58 13:58 13:58
		13:58 13:58 13:58 11:57 11:57
		11:57 11:57 11:57 11:57 11:57
		11:57 11:57 11:57
	1	13:49 13:46 13:46 13:45
	0	11:03 11:03
08-31		Number of Records:02
	0	15:01 15:01
08-30		Number of Records:31
	0	17:55 17:55 17:34 17:34 17:15
		17:15 17:11 17:11 17:04 17:04
	1	17:53 17:53 17:53 17:53 17:25
		17:25 17:25 17:25 17:25 17:25
		17:23 17:23 17:23 17:23 17:23
		17:23 17:23 17:23 17:23 17:05
		17:05
03-18		Number of Records:02
	0	02:34 02:34

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

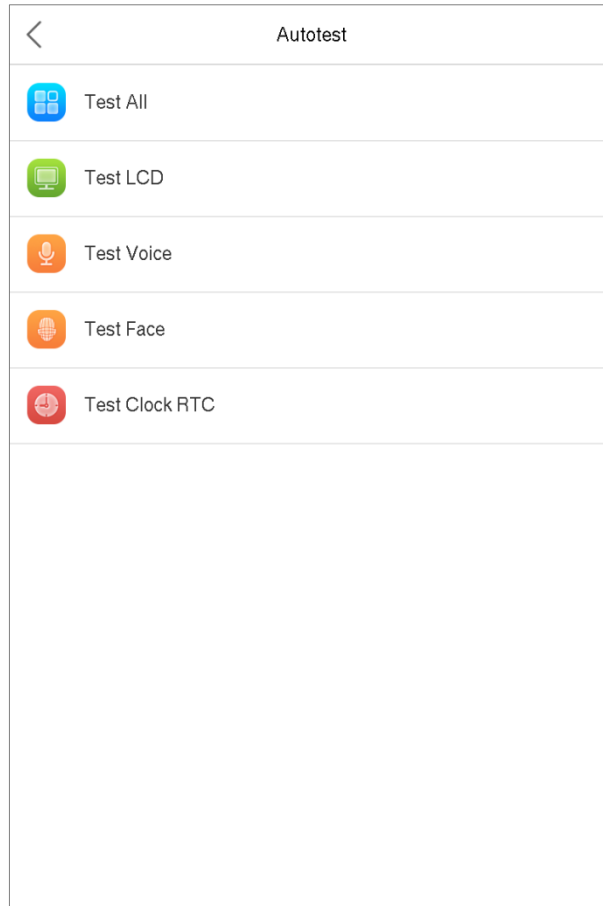
Personal Record Search				
User ID	Name	Time	Mode	State
1	A	09-02 13:49	3	0
1	A	09-02 13:46	3	0
1	A	09-02 13:46	3	0
1	A	09-02 13:45	3	0

Verification Mode : Password Status : In

11. Autotest

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

Click **Autotest** on the main menu.

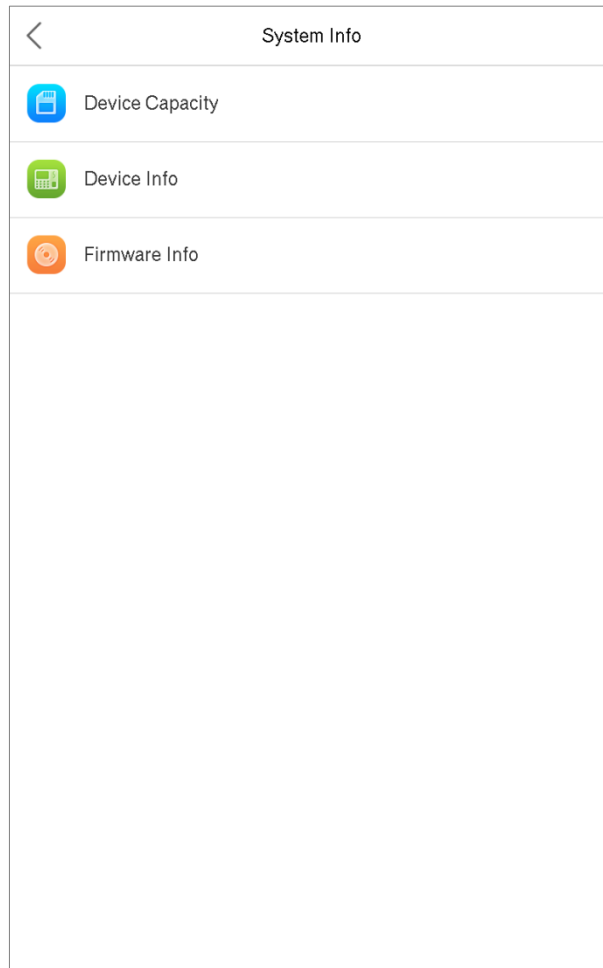


Item	Descriptions
Test All	To automatically test whether the LCD, audio, camera and RTC are normal.
Test LCD	To automatically test the display effect of LCD screen by displaying full-color, pure white, and pure black to check whether the screen displays colors normally.
Test Voice	To automatically test whether the audio files stored in the device are complete and the voice quality is good.
Test Face	To test if the camera functions properly by checking the pictures taken to see if they are clear enough.
Test Clock RTC	To test the RTC. The device tests whether the clock works normally and accurately with a stopwatch. Touch the screen to start counting and press it again to stop counting.

12. System Information

Here you can view the storage status, the version information of the device, and so on.

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



Item	Descriptions
Device Capacity	Display the current device's user storage, password and face storage, administrators, access records, attendance and blacklist photos, and user photos.
Device Info	Display the device's name, serial number, MAC address, face algorithm version, platform information, and manufacturer.
Firmware Info	Display the firmware version and other version information of the device.

13. Connection to ZKBioSecurity Software

13.1 Set the Communication Address

➤ Device

1. Click **COMM.** > **Ethernet** in the main menu to set IP address and gateway of the device. (**Note:** The IP address should be able to communicate with the ZKBioSecurity 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 the IP address of ZKBioSecurity server.

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

Ethernet	
IP Address	192.168.163.200
Subnet Mask	255.255.255.0
Gateway	0.0.0.0
DNS	0.0.0.0
TCP COMM.Port	4370
DHCP	<input type="checkbox"/>
Display in Status Bar	<input checked="" type="checkbox"/>

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"/>

➤ Software

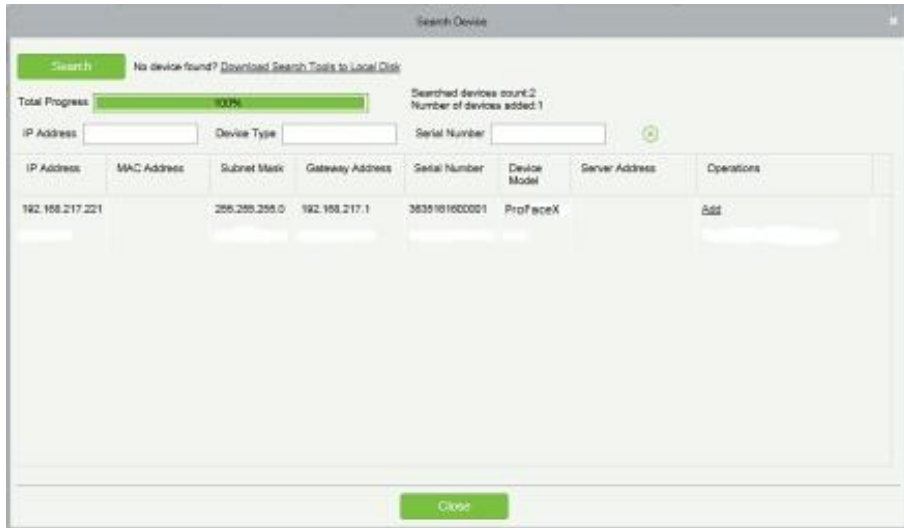
Log in to ZKBioSecurity software, click **System** > **Communication** > **Communication Device** to set the adms service port, as shown below:



13.2 Add a Device on the Software

Add devices by searching. The process is as follows:

- 1) Click **Access Control > Device > Search Device**, to open the Search interface.
- 2) Click **Search**, and the system will prompt [Searching.....].
- 3) After searching, the list and total number of access controllers will be displayed.



- 4) Select the device and click **Add**.

13.3 Add Personnel on the Software

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

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

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

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 Use



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.

Green Label

ZK Building, Wuhe Avenue, Gangtou, Bantian, Buji Town,
Longgang District, Shenzhen, China 518129

Tel: +86 755-89602345

Fax: +86 755-89602394

www.zkteco.com

