

User Manual

ProFaceX

Version: 1.0

Date: May 2019

Important Statement

Thank you for choosing our product. Before using this product, please read this user manual carefully to avoid risks of danger to the users of this product or those nearby and damaging the device. Follow these instructions to ensure that your product functions properly and completes verifications in a timely manner.

Unless authorized by our company, no group or individual shall take excerpts of or copy all or part of these instructions nor transmit the contents of these instructions by any means.

The products described in this manual may include software that is copyrighted by our company and its possible licensors. No one may copy, publish, edit, take excerpts of, decompile, decode, reverse-engineer, rent, transfer, sublicense, or otherwise infringe upon the software's copyright unless authorized by the copyright holder(s). This is subject to relevant laws prohibiting such restrictions.



As this product is regularly updated, we cannot guarantee exact consistency between the actual product and the written information in this manual. Our company claims no responsibility for any disputes that arise due to differences between the actual technical parameters and the descriptions in this document. The manual is subject to change without prior notice.

Contents

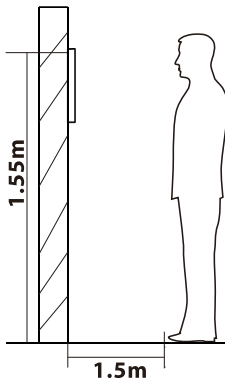
1 Notice for Use	1
1.1 Standing Position, Facial Expression and Standing Posture	1
1.2 Face Registration	2
1.3 Standby Interface	3
1.4 Virtual Keyboard	4
1.5 Verification Mode.....	5
1.5.1 Password Verification	5
1.5.2 Facial Verification	9
1.5.3 Combined Verification	13
2 Main Menu	14
3 User Management.....	16
3.1 Adding Users	16
3.2 Search for Users	19
3.3 Edit Users.....	20
3.4 Deleting Users.....	21
4 User Role	22
5 Communication Settings.....	25
5.1 Network Settings	25
5.2 Serial Port Settings.....	27
5.3 PC Connection	27
5.4 WIFI Setting.....	28
5.5 Cloud Server Setting.....	29
5.6 Wiegand Setup.....	30
6 System Settings.....	34
6.1 Date and Time.....	34
6.2 Access Logs Setting	35
6.3 Face Parameters.....	37
6.4 Factory Reset	38
6.5 Temperature Management.....	40
7. Personalize Settings.....	41
7.1 Interface Settings.....	41
7.2 Voice Settings.....	43
7.3 Bell Schedules.....	43
8. Data Management	46
8.1 Delete Data.....	46
9. Access Control.....	49
9.1 Access Control Options	50

9.2 Time Rule Setting.....	51
9.3 Holiday Settings.....	54
9.4 Combined Verification Settings.....	56
9.5 Duress Options Settings.....	57
10. Attendance Search.....	59
11. Autotest.....	62
12. System Information.....	63
13. Connect to ZKBioSecurity Software.....	64
13.1 Set the Communication Address.....	64
13.2 Add Device on the Software.....	65
13.3 Add Personnel on the Software.....	65
Statement on the Right to Privacy.....	67
Eco-friendly Use.....	68

1 Notice for Use

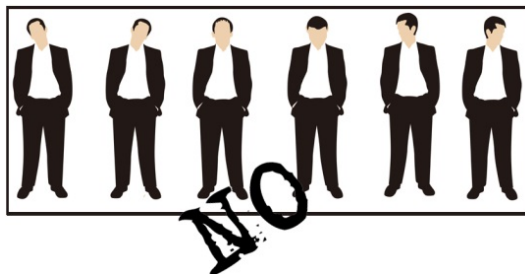
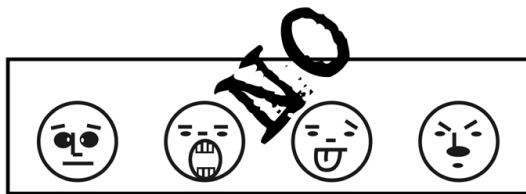
1.1 Standing Position, Facial Expression and Standing Posture

- 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 enrolment and verification, please remain natural facial expression and standing posture.

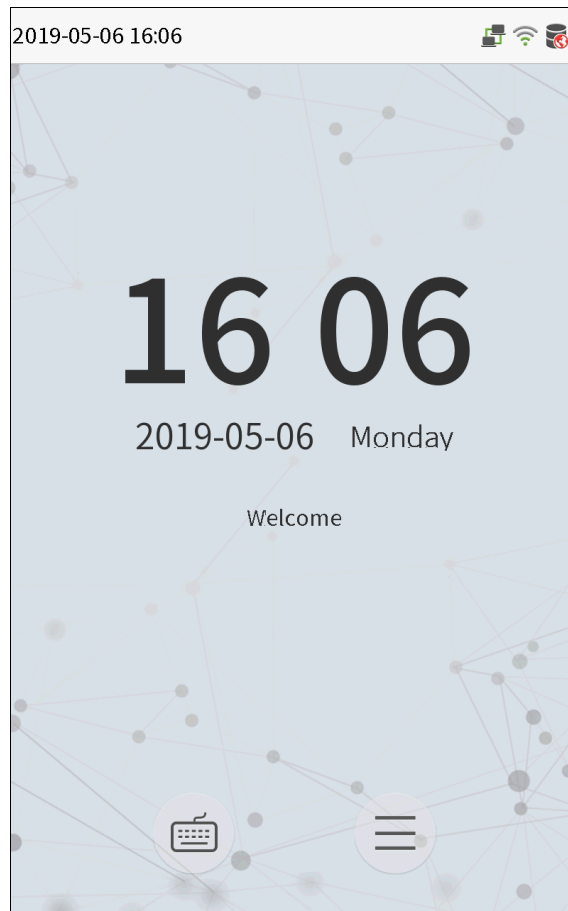
1.2 Face Registration

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





1.3 Standby Interface

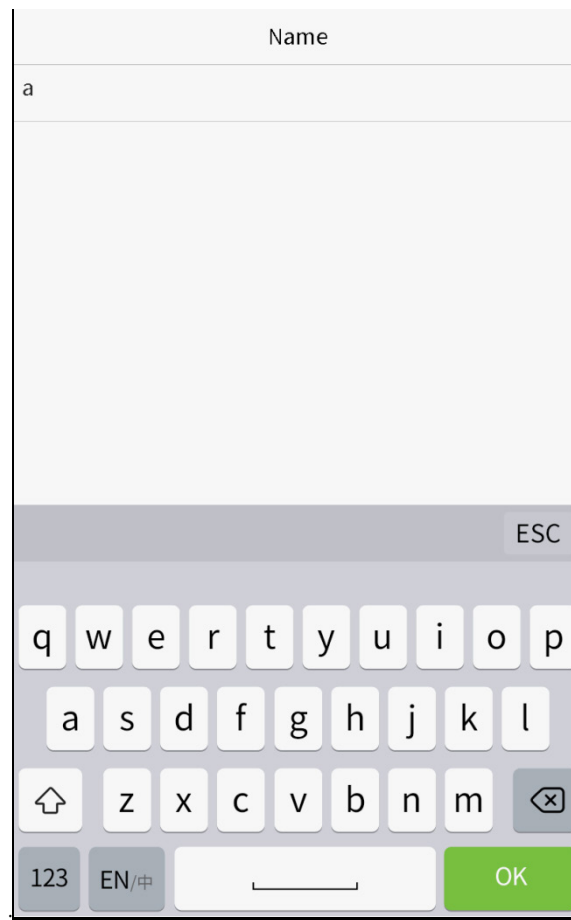
After connecting the power supply, enter the following standby interface:



Notes:

1. Click  to enter the User ID input interface.
2. When there is no super administrator set in the device, click  to enter the menu. After setting the super administrator, it requires the super administrator's verification before entering the menu operation. For the security of the device, it is recommended to register super administrator the first time you use the device.

1.4 Virtual Keyboard




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

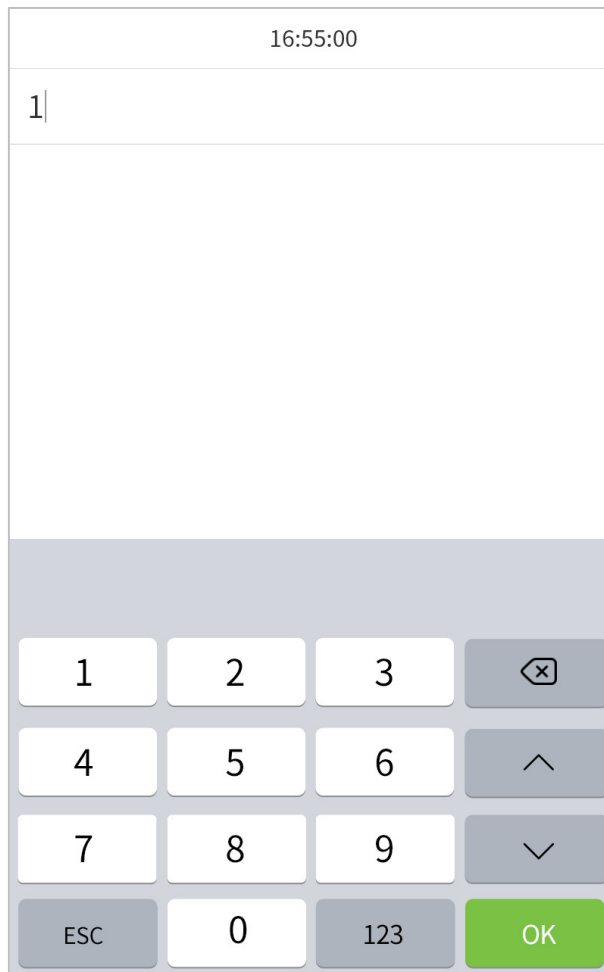
1.5 Verification Mode

1.5.1 Password Verification


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

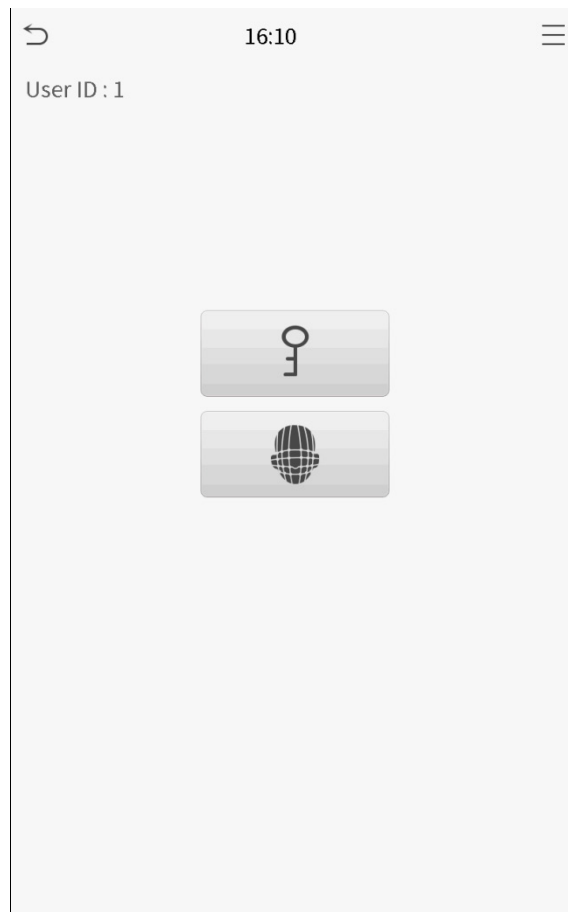
Click the  button on the main screen to enter the 1:1 password verification mode.

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

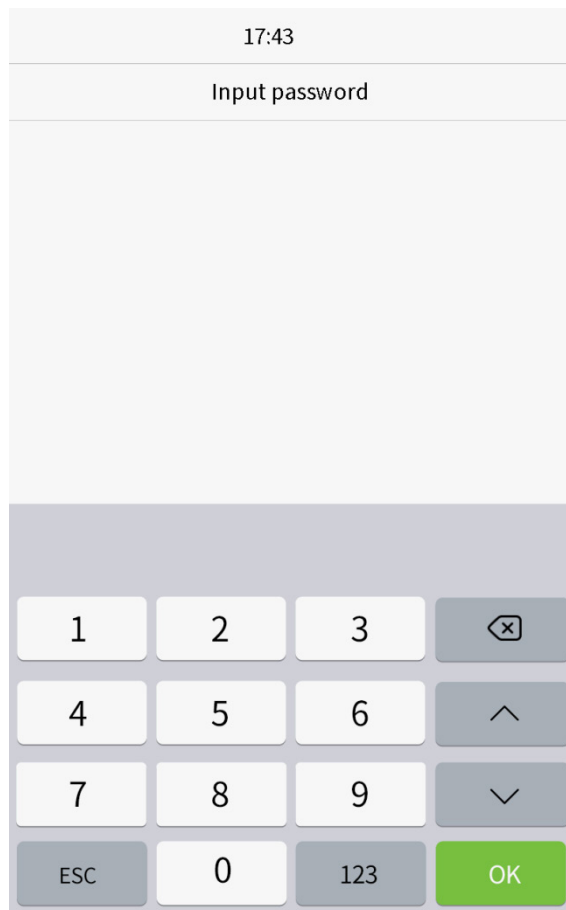


16:55:00			
1			
1	2	3	⌫
4	5	6	^
7	8	9	∨
ESC	0	123	OK

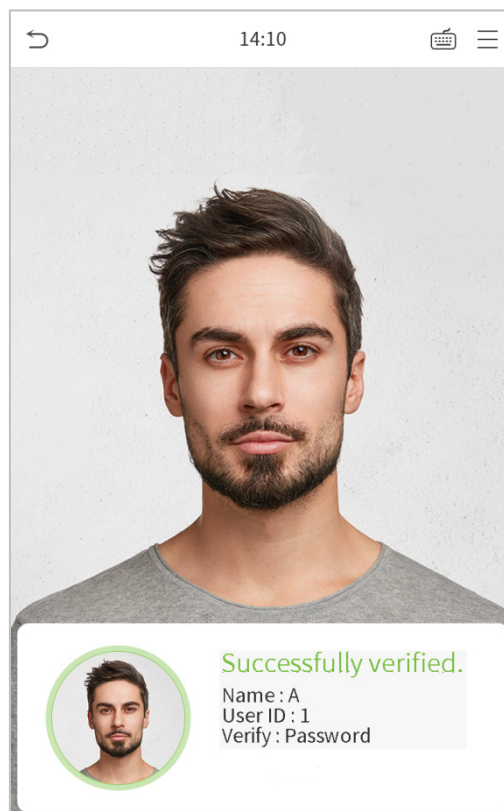
If an employee registers face in addition to password, the following screen will appear. Select the  icon to enter password verification mode.



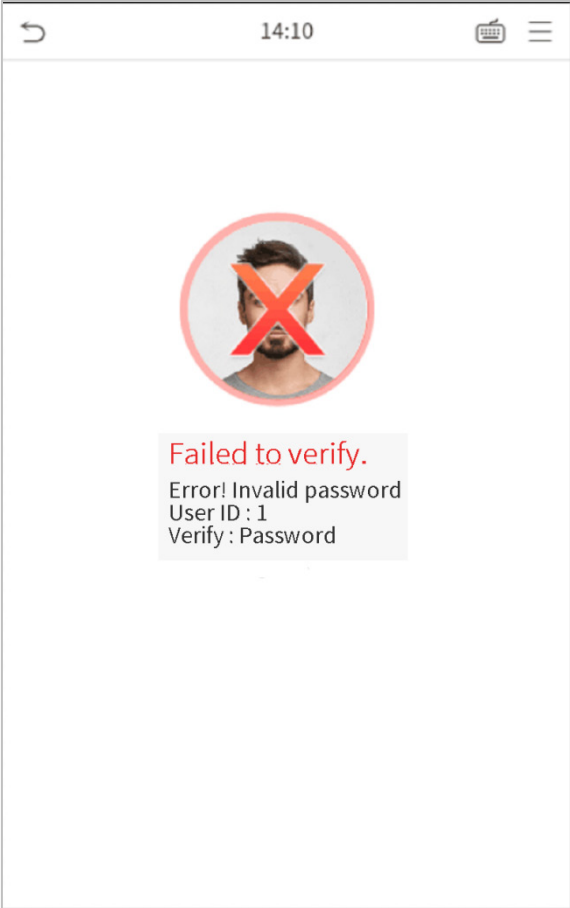
2. Input the password and press [OK].



Verification is successful.



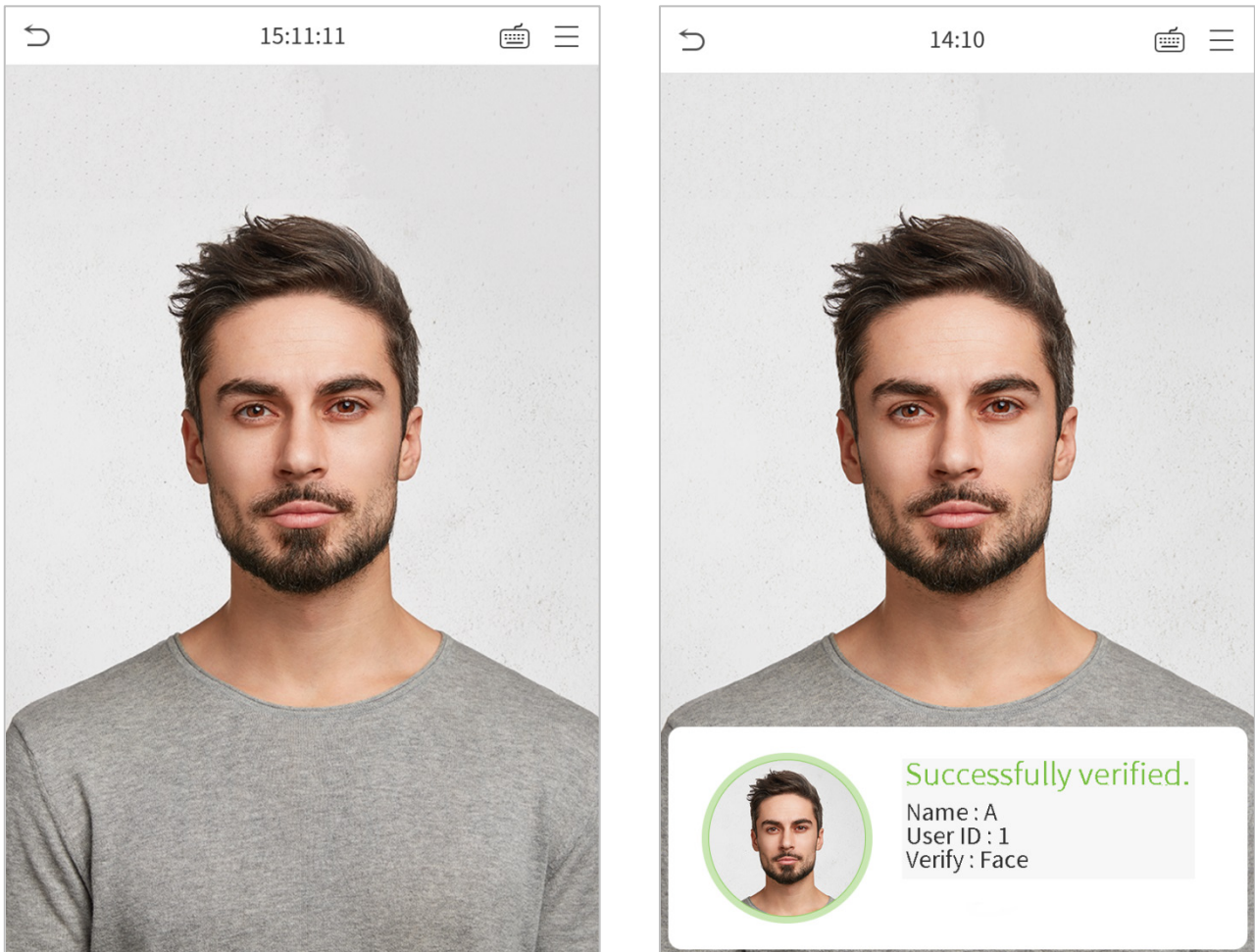
Verification is failed.



1.5.2 Facial Verification


- **1:N face verification**

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

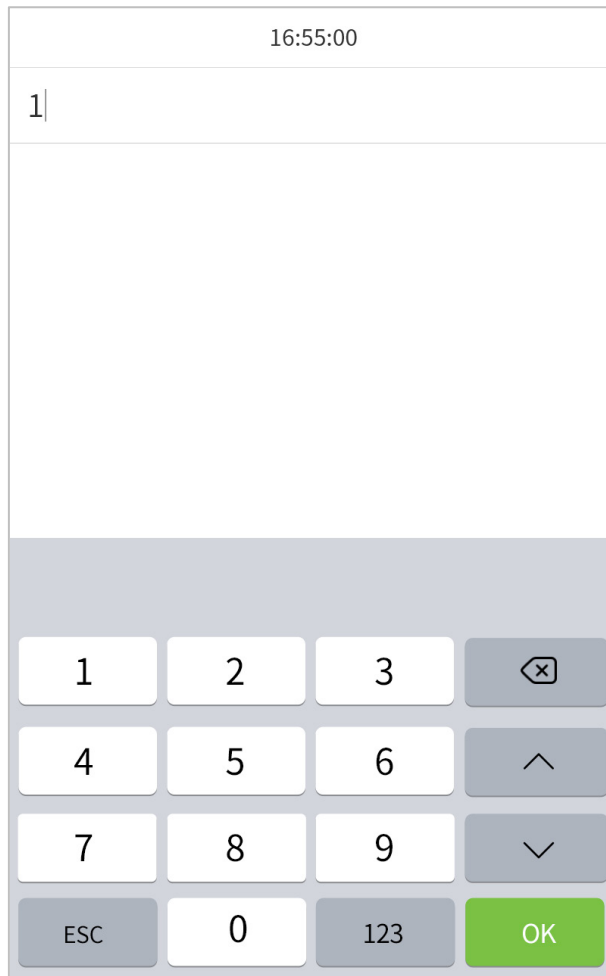



- **1:1 face verification**

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.

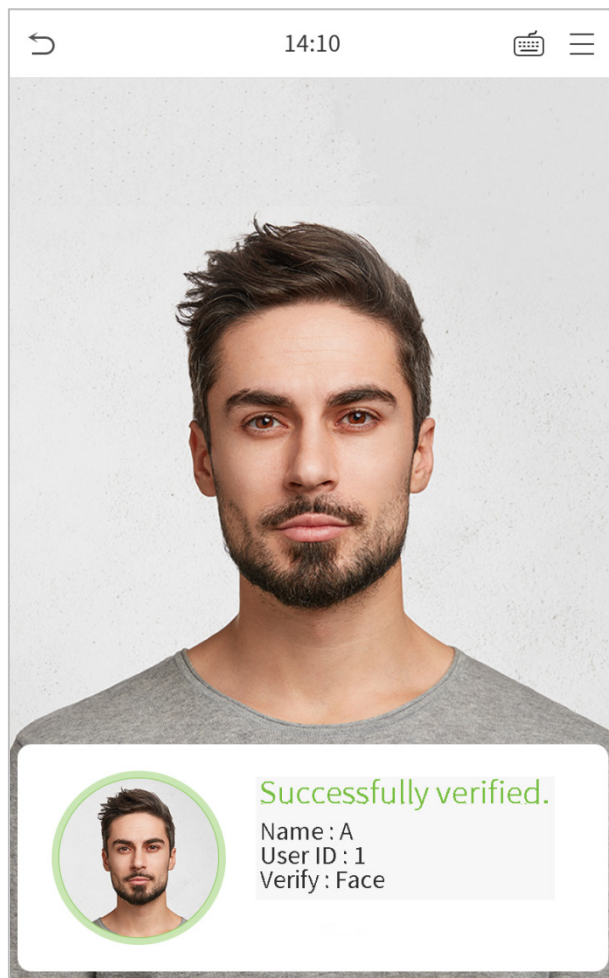
1. Enter the user ID and click [OK].



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



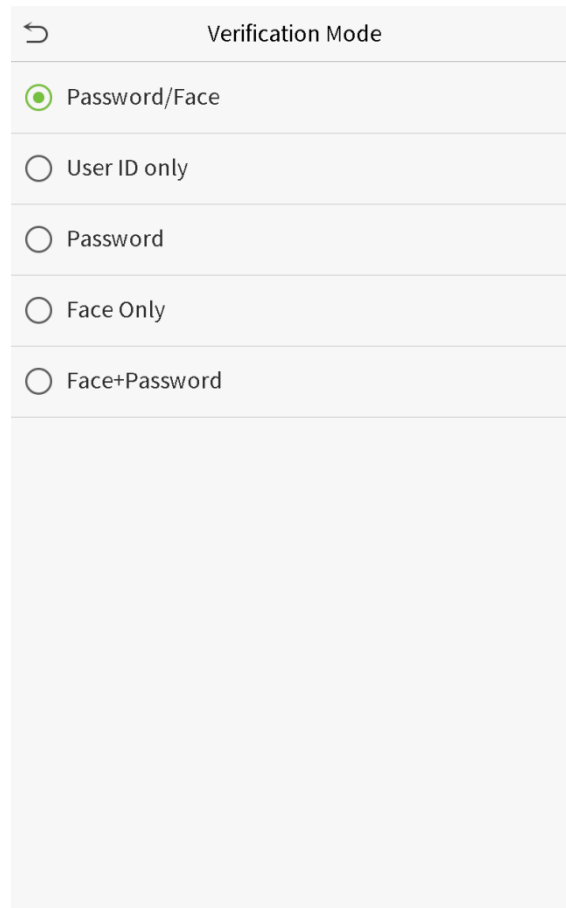
After successful verification, the prompt box "successfully verified" will appear.



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

1.5.3 Combined Verification


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

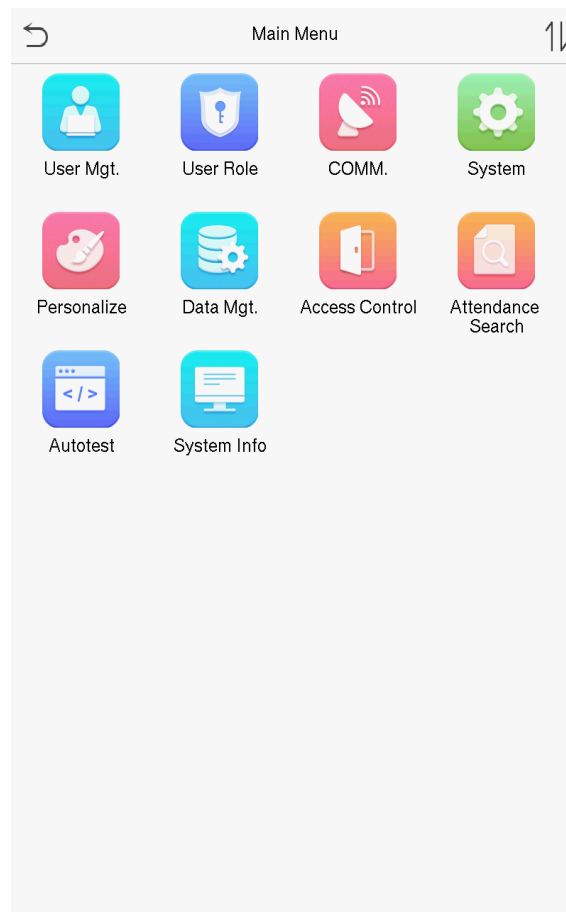


Notes:

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

2 Main Menu

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



Items	Descriptions
User Mgt.	To add, edit, view, and delete basic information about a user.
User Role	To set the permission scope of the custom role and enroller, that is, the rights to operate the system.
COMM.	To set the relevant parameters of network, serial communication, PC connection, WIFI, 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.

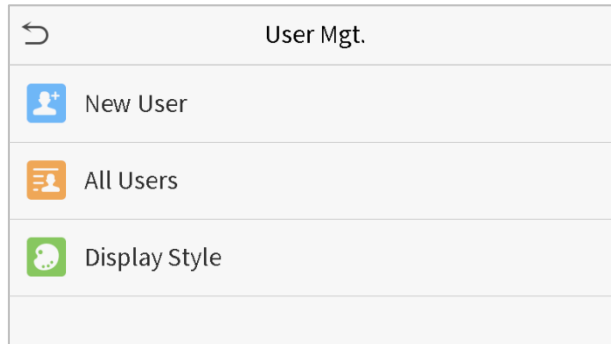
System Info

To view data capacity, device and firmware information of the current device.

3 User Management

3.1 Adding Users

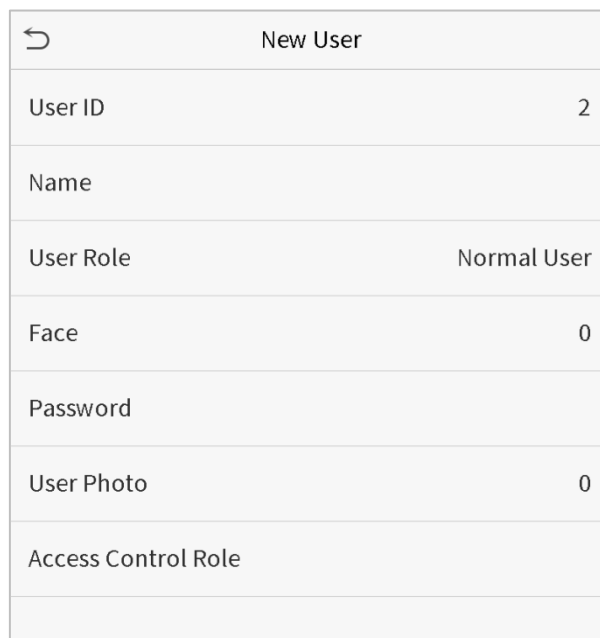
Click **User Mgt.** on the main menu.



Click **New User**.

- **Register a User ID and Name**

Enter the user ID and name.



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

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 users** 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.

User Role	
<input checked="" type="radio"/>	Normal User
<input type="radio"/>	Enroller
<input type="radio"/>	User Defined Role 1
<input type="radio"/>	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 Method*.

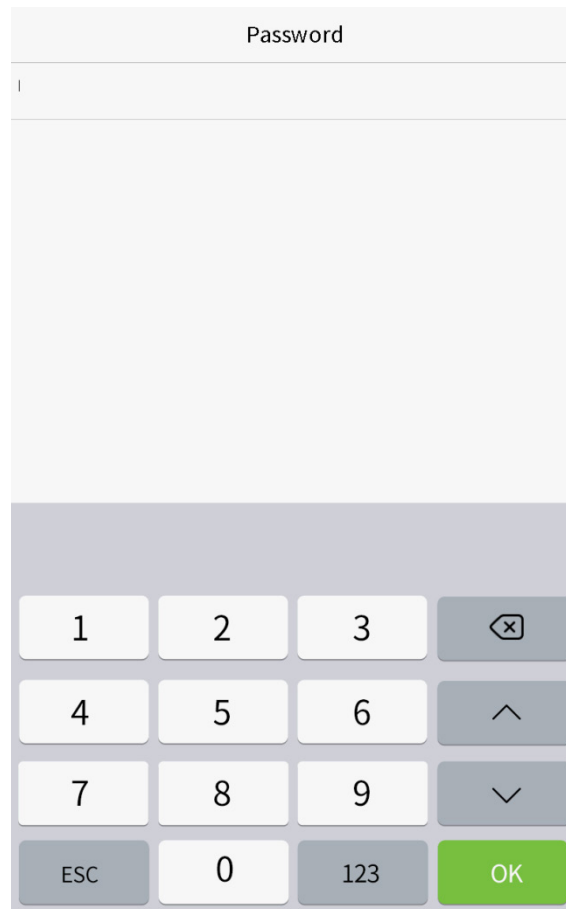
- **Register face**

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



- **Register password**

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



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

- **Register user photo**

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

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

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

- **Access Control Role**

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

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

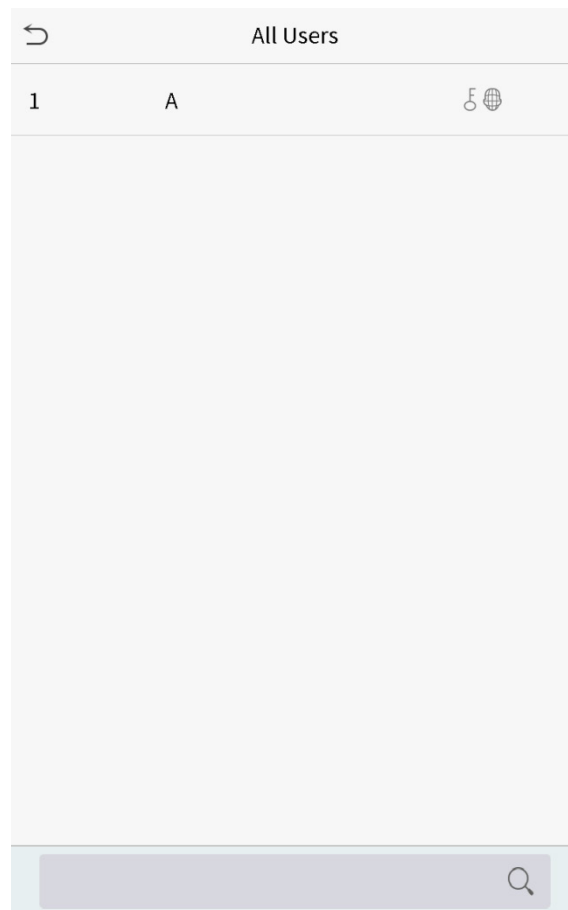
Click **Time Period**, select the time period to use.

The screenshot shows a mobile application interface titled "Access Control". At the top left is a back arrow icon. Below the title, there is a table with two columns: "Access Group" and "Time Period". The "Access Group" column contains the value "1". The "Time Period" column is currently empty. The table is rendered in a light gray style with horizontal lines separating the rows.

Access Group	Time Period
1	

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	0
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 Deleting Users

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

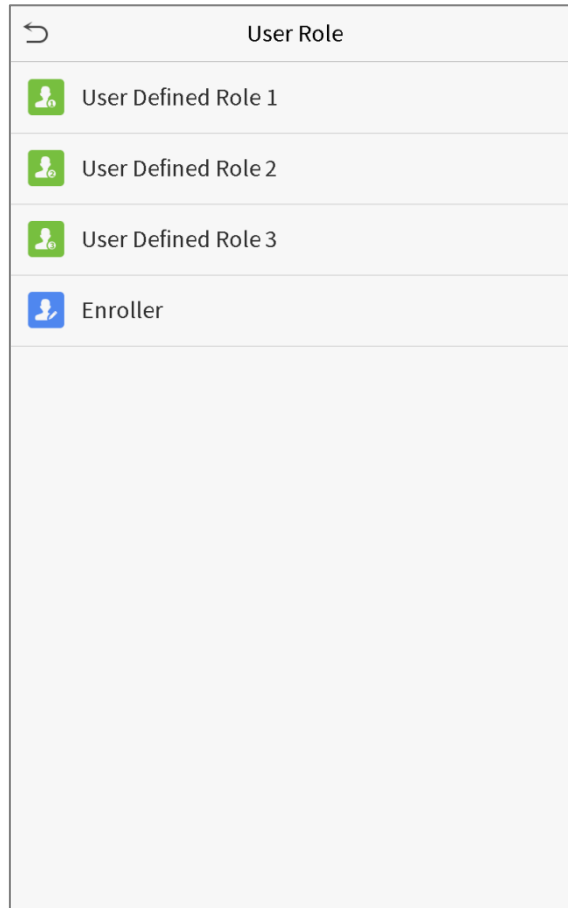
Note: If you select **Delete User**, all information of the user will be deleted.

4 User Role

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

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

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



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

↩ User Defined Role 1	
Enable Defined Role	<input type="checkbox"/>
Name	User Defined Role 1
Define User Role	

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

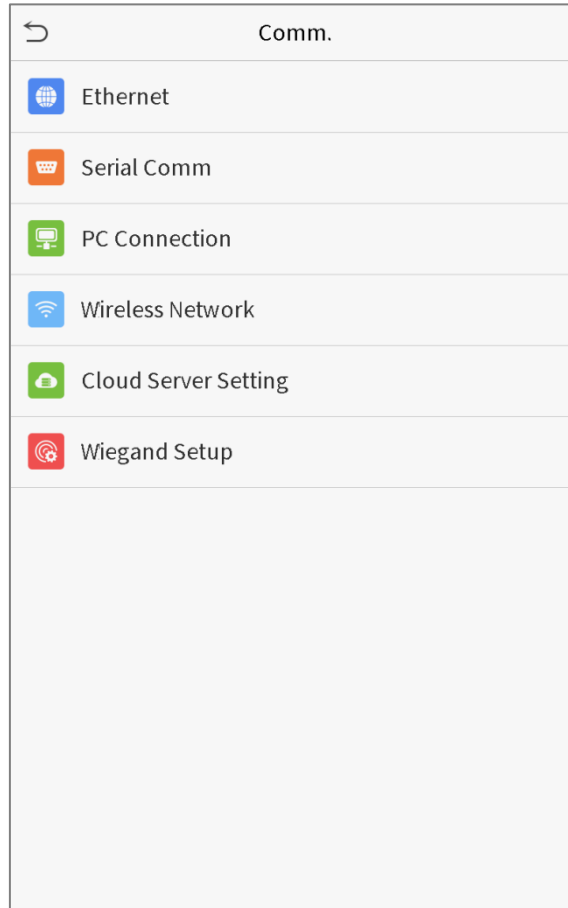
User Role	
<input checked="" type="radio"/> Normal User	
<input type="radio"/> Enroller	
<input type="radio"/> User Defined Role 1	
<input type="radio"/> Super Admin	

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

5 Communication Settings

Set parameters of the network, serial communication, PC connection, WIFI, 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	192.168.163.150
Subnet Mask	255.255.255.0
Gateway	192.168.163.1
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 them according to the actual network situation.
Subnet Mask	The factory default value is 255.255.255.0. Please adjust them according to the actual network situation.
Gateway	The factory default address is 0.0.0.0. Please adjust them according to the actual network situation.
DNS	The factory default address is 0.0.0.0. Please adjust them according to the actual network situation.
TCP COMM. Port	The factory default value is 4370. Please adjust them according to the actual network situation.
DHCP	Dynamic Host Configuration Protocol, which is to dynamically allocate IP addresses for clients via server.
Display in Status Bar	To set whether to display the network icon on the status bar.

5.2 Serial Port Settings

To establish communication with the device through a serial port (RS232/RS485), you need to configure **Serial Comm.**

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

Serial Comm	
Serial port	RS232(PC)
Baudrate	115200

Item	Descriptions
Serial port	Select whether to use RS232 or RS485 for communication.
Baudrate	The rate of the communication with PC; there are four options of baud: 115200 (default), 57600, 38400 and 19200.

5.3 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.

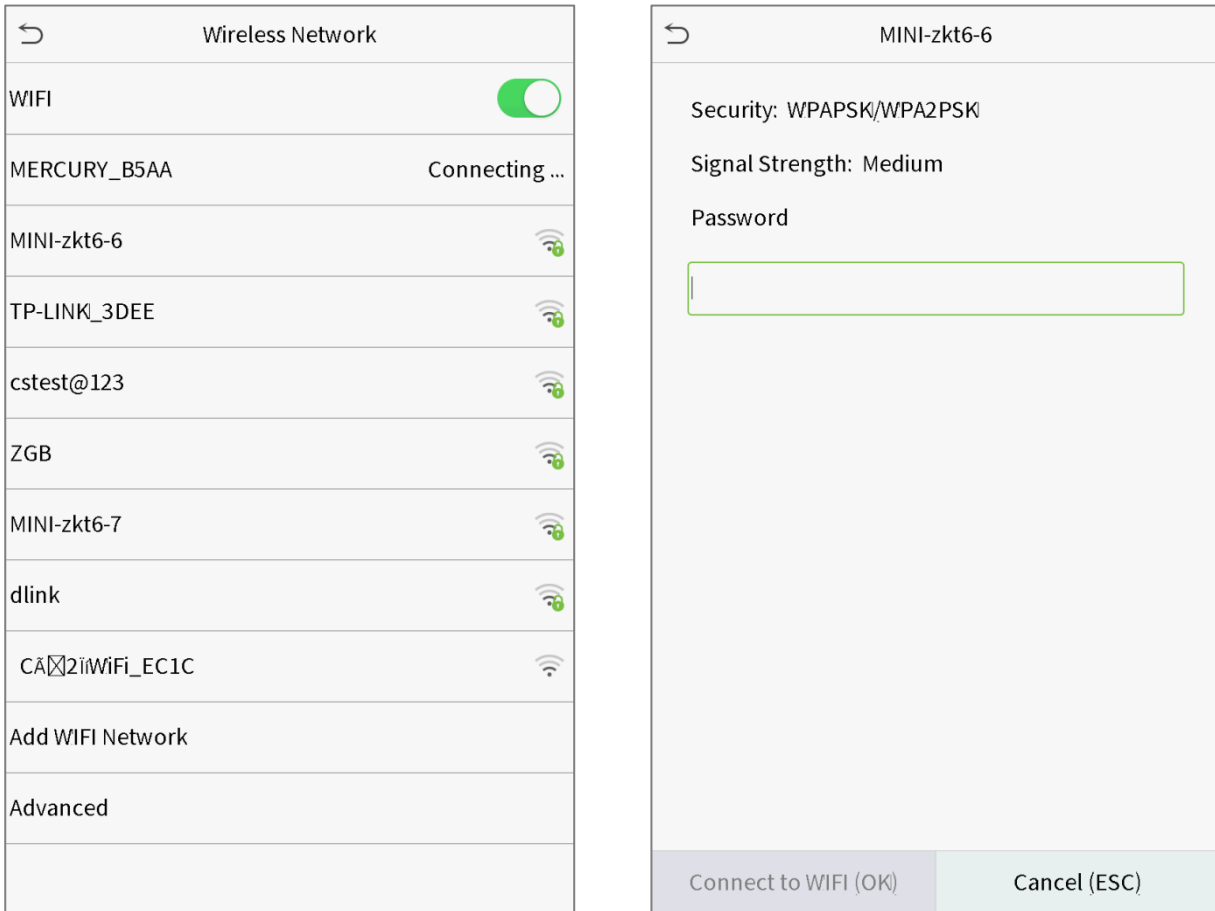
Click **PC Connection** on the Comm. Settings interface.


PC Connection	
Comm Key	0
Device ID	1

Item	Descriptions
Comm Key	Comm Key: The default password is 0, which can be changed. 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 in the software communication interface.

5.4 WIFI Setting

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



When WIFI is enabled, tap the searched network. Enter the password, and tap Connect to WIFI (OK). The connection succeeds, with icon  displayed on the status bar.

➤ Adding WIFI Network

If the desired Wi-Fi network is not in on the list, you can add the Wi-Fi network manually.

Click  and Add WIFI Network. Enter the parameters of the Wi-Fi network. (The added network must exist.)

Add WIFI Network	
SSID	
Network Mode	ADHOC
Auth. Mode	SHARED
Encrypt Mode	WEP
Password	

After adding, find the newly added Wi-Fi network in list and connect to it in the above way.

➤ **Advanced**

This is used to set Wi-Fi network parameters.

Ethernet	
DHCP	<input checked="" type="checkbox"/>
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Gateway	0.0.0.0

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

5.5 Cloud Server Setting

This represents settings used for connecting with 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"/>

Item	Description
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	
Server Port	Port used by the ADMS server.
Enable Proxy Server	When you choose to enable the proxy, you need to set the IP address and port number of the proxy server.

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

Definitions of various common Wiegand formats:

Wiegand Format	Definitions
Wiegand26	<p>ECCCCCCCCCCCCCCCCCCCCCCCCCO</p> <p>Consists of 26 bits of binary code. The 1st bit is the even parity bit of the 2nd to 13th bits, while the 26th bit is the odd parity bit of the 14th to 25th bits. The 2nd to 25th bits are the card numbers.</p>
Wiegand26a	<p>ESSSSSSSCCCCCCCCCCCCCCCCCCO</p> <p>Consists of 26 bits of binary code. The 1st bit is the even parity bit of the 2nd to 13th bits,</p>

	while the 26 th bit is the odd parity bit of the 14 th to 25 th bits. The 2 nd to 9 th bits are the site codes, while the 10 th to 25 th bits are the card numbers.
Wiegand34	<pre>ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO</pre> Consists of 34 bits of binary code. The 1 st bit is the even parity bit of the 2 nd to 17 th bits, while the 34 th bit is the odd parity bit of the 18 th to 33 rd bits. The 2 nd to 25 th bits are the card numbers.
Wiegand34a	<pre>ESSSSSSSCCCCCCCCCCCCCCCCCCCCCCCO</pre> Consists of 34 bits of binary code. The 1 st bit is the even parity bit of the 2 nd to 17 th bits, while the 34 th bit is the odd parity bit of the 18 th to 33 rd bits. The 2 nd to 9 th bits are the site codes, while the 10 th to 25 th bits are the card numbers.
Wiegand36	<pre>OFFFFFFFFFCCCCCCCCCCCCCCCCMME</pre> Consists of 36 bits of binary code. The 1 st bit is the odd parity bit of the 2 nd to 18 th bits, while the 36 th bit is the even parity bit of the 19 th to 35 th bits. The 2 nd to 17 th bits are the device codes. The 18 th to 33 rd bits are the card numbers, and the 34 th to 35 th bits are the manufacturer codes.
Wiegand36a	<pre>EFFFFFFFFFCCCCCCCCCCCCCCCCCCO</pre> Consists of 36 bits of binary code. The 1 st bit is the even parity bit of the 2 nd to 18 th bits, while the 36 th bit is the odd parity bit of the 19 th to 35 th bits. The 2 nd to 19 th bits are the device codes, and the 20 th to 35 th bits are the card numbers.
Wiegand37	<pre>OMMMMMSSSSSSSSSCCCCCCCCCCCCCCCCE</pre> Consists of 37 bits of binary code. The 1 st bit is the odd parity bit of the 2 nd to 18 th bits, while the 37 th bit is the even parity bit of the 19 th to 36 th bits. The 2 nd to 4 th bits are the manufacturer codes. The 5 th to 16 th bits are the site codes, and the 21 st to 36 th bits are the card numbers.
Wiegand37a	<pre>EMMMFFFFFFFSSSSSCCCCCCCCCCCCCCCCO</pre> Consists of 37 bits of binary code. The 1 st bit is the even parity bit of the 2 nd to 18 th bits, while the 37 th bit is the odd parity bit of the 19 th to 36 th bits. The 2 nd to 4 th bits are the manufacturer codes. The 5 th to 14 th bits are the device codes, and 15 th to 20 th bits are the site codes, and the 21 st to 36 th bits are the card numbers.
Wiegand50	<pre>ESSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCO</pre> Consists of 50 bits of binary code. The 1 st bit is the even parity bit of the 2 nd to 25 th bits, while the 50 th bit is the odd parity bit of the 26 th to 49 th bits. The 2 nd to 17 th bits are the site codes, and the 18 th to 49 th bits are the card numbers.

"C" denotes the card number; "E" denotes the even parity bit; "O" denotes the odd parity bit; "F" denotes the facility code; "M" denotes the manufacturer code; "P" denotes the parity bit; and "S" denotes the site code.

➤ **Wiegand output**

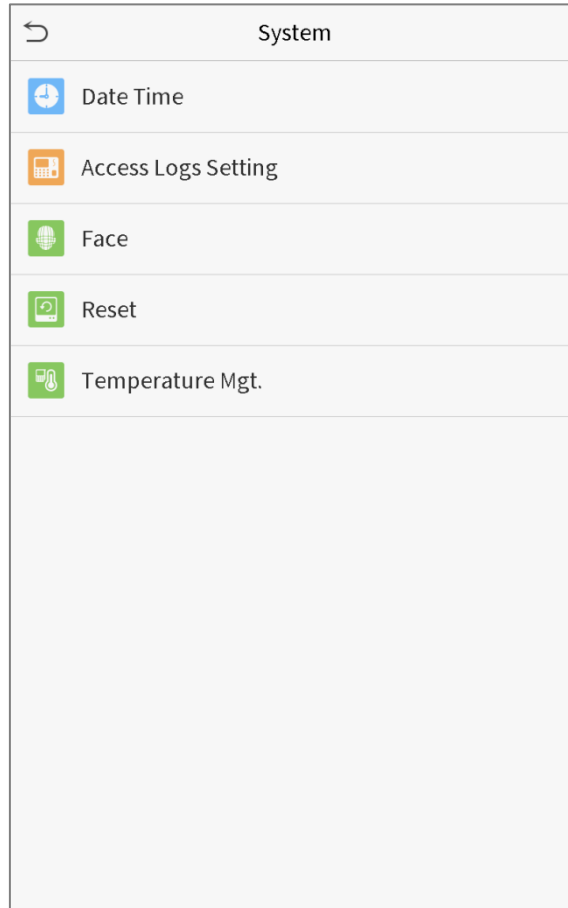
Wiegand Options	
Wiegand Format	
wiegand output bits	26
Failed ID	0
Site Code	0
Pulse Width(us)	100
Pulse interval(us)	1000
ID Type	Badge Number

Item	Descriptions
Wiegand Format	Values range from 26 bits, 34 bits, 36 bits, 37 bits, and 50 bits.
Wiegand output bits	After choosing the Wiegand format, you can select one of the corresponding output digits in the Wiegand format
Failed ID	If the verification is failed, the system will send the failed ID to the device and replace the card number or personnel ID with the new ones.
Site Code	It is similar to the device ID. The difference is that a site code can be set manually, and is repeatable in a different device. The valid value ranges from 0 to 256 by default.
Pulse Width(us)	The time width represents the changes of the quantity of electric charge with high-frequency capacitance regularly within a specified time.
Pulse Interval(us)	The time interval between pulses.
ID Type	Select between User ID and badge number.

6 System Settings

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

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




6.1 Date and Time

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



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

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

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

6.2 Access Logs Setting

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

Access Logs Setting	
Camera Mode	No photo
Display User Photo	<input checked="" type="checkbox"/>
Alphanumeric User ID	<input type="checkbox"/>
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 detect interval(s)	1

Item	Description
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.
Alphanumeric User ID	Whether to support letters in an User ID.

Access Logs Warning	When remaining record space reaches a set value, the device will automatically display a remaining record memory warning. Users may disable the function or set a valid value between 1 and 9999.
Cyclic 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 Detect 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:N Match Threshold	76
1:1 Match Threshold	63
Face registration thresholds	70
Pitch angle thresholds	30
Rotation angle thresholds	25
Image quality	40
Thresholds of turning on the supplement LED	80
Alive body detection switch	<input checked="" type="checkbox"/>
Alive body detection thresholds	70

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

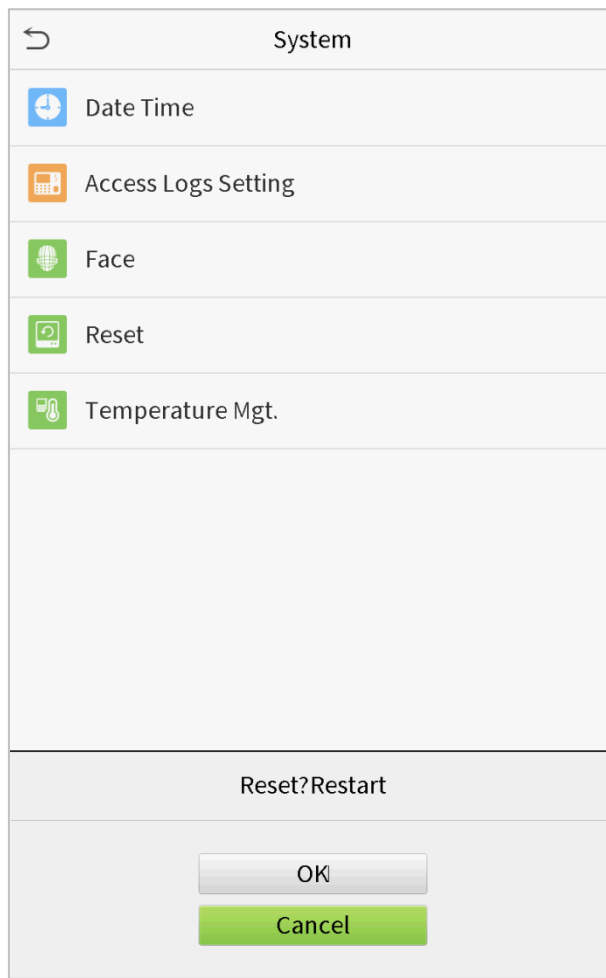
Item	Description
1:N Match Threshold	Under 1:N verification mode, the verification will only be successful when the similarity between the acquired facial image and all registered facial templates is greater than the set value. The valid value ranges from 65 to 120. The higher the thresholds set, the 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 registration threshold	During face registration, 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.

Pitch angle threshold	To limit the pitch angle of face in face recognition, the recommended threshold is 20.
Rotation angle threshold	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.
Threshold of turning on the supplement LED	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.
Alive body detection switch	If enabled, it will automatically detect whether there is a moving person in front of the device.
Alive body 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.
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 (Do not clear registered user data).

Click **Reset** on the System interface.

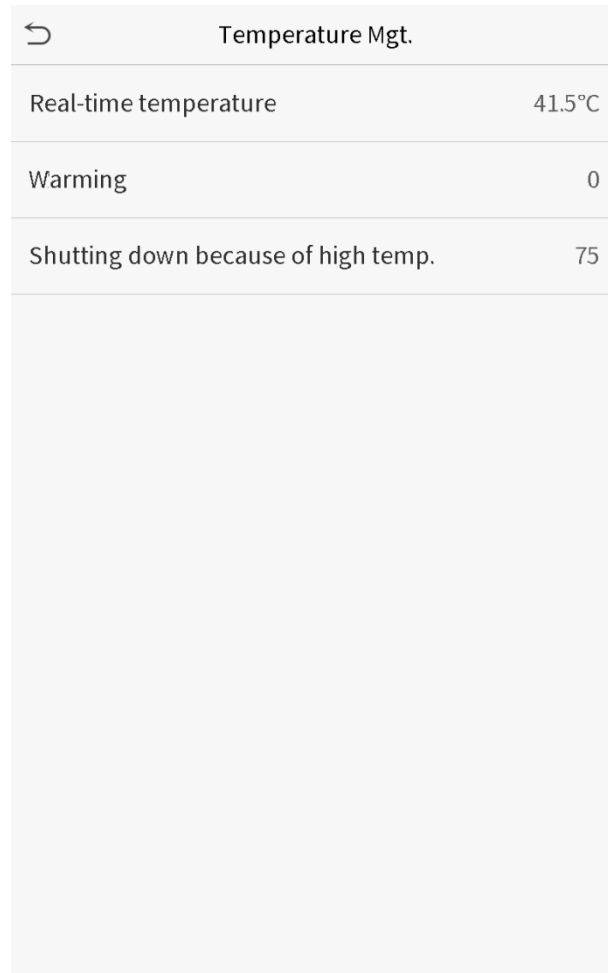


Click **OK** to reset.

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.



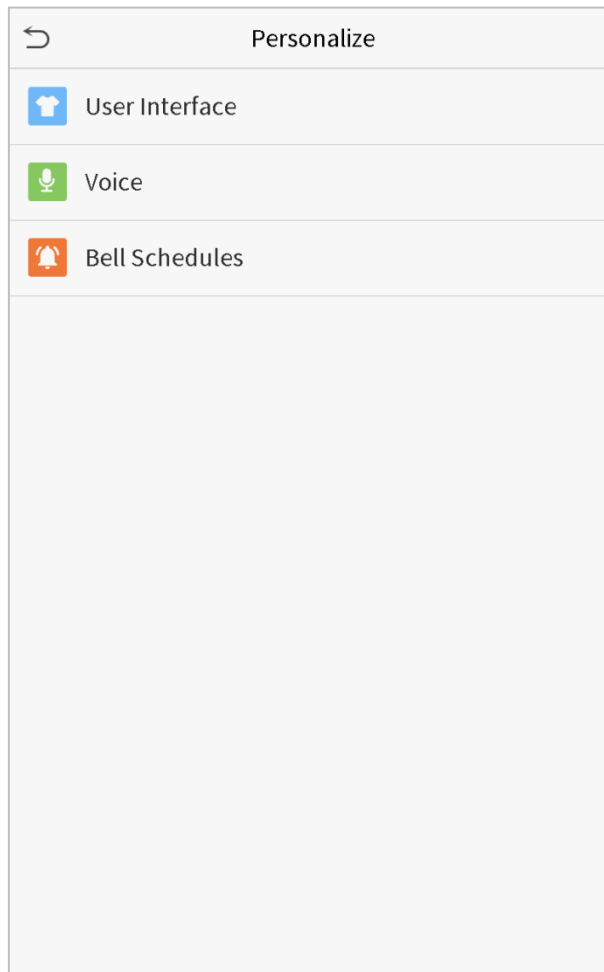
Temperature Mgt.	
Real-time temperature	41.5°C
Warming	0
Shutting down because of high temp.	75

Item	Description
Real-time temperature	This column shows real time inner temperature of terminal.
Low temp. to heat	Once terminal temperature is lower than set value, terminal will start self-heating, the set range is 0~10(°C).
High temp. to reset	When the terminal temperature is high than set value, it will shut down automatically to protect hardware, the set range is 60~80 (°C).

7. Personalize Settings

You may customize interface settings, audio and bell.

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



7.1 Interface Settings

You can customize the display style of the main interface.

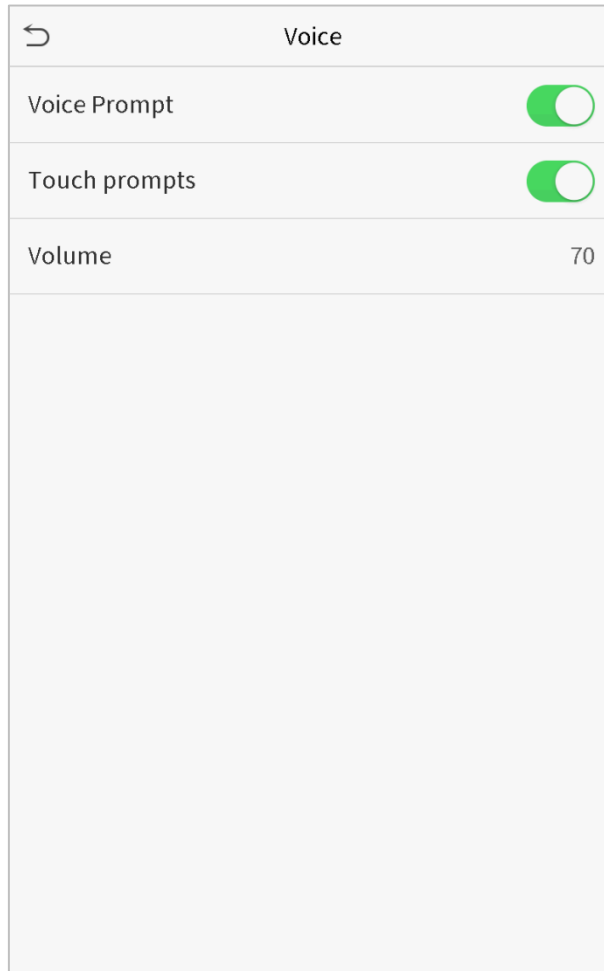
Click **User Interface** on the Personalize interface.

User Interface	
Wallpaper	
Language	English
Menu Screen Timeout(s)	99999
Idle Time To Slide Show(s)	60
Slide Show Interval(s)	30
Idle Time To Sleep(m)	Disabled
Main Screen Style	Style 1

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

7.2 Voice Settings

Click **Voice** on the Personalize interface.



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

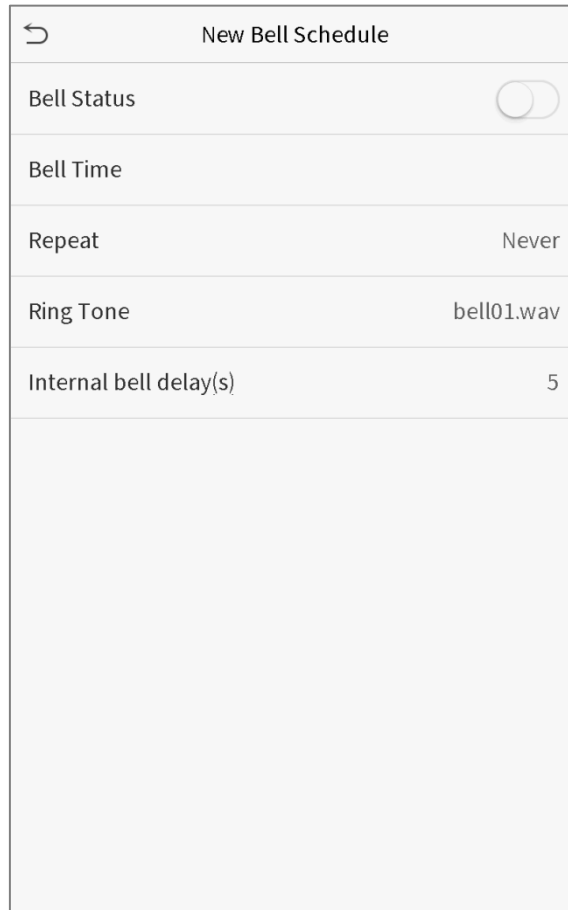
7.3 Bell Schedules

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



- **Add a bell**

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



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

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

- **Edit a bell**

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

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

- **Delete a bell**

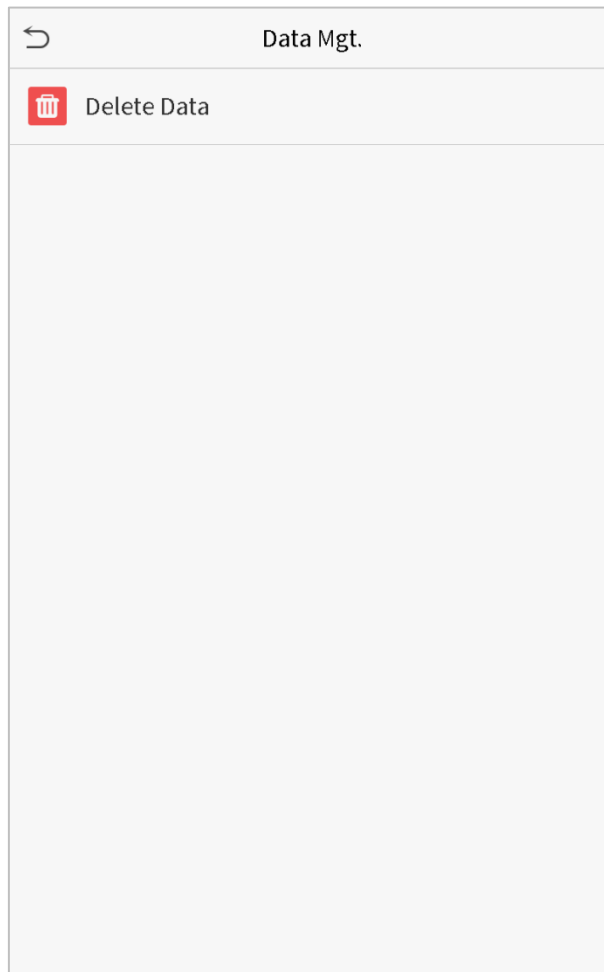
On the All Bell Schedules interface, tap the bell to be deleted.

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

8. Data Management

To delete the relevant data in the device.

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



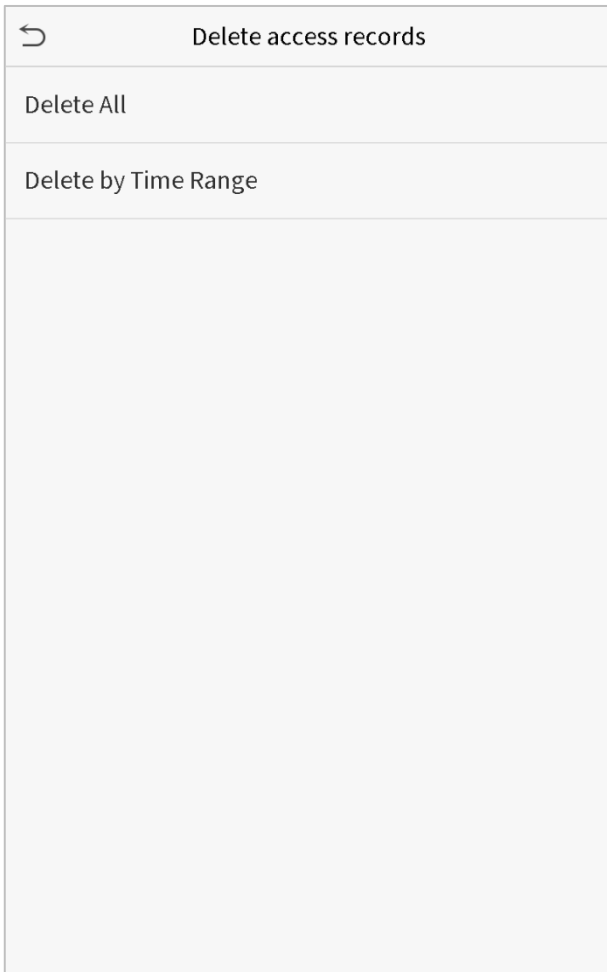
8.1 Delete Data

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

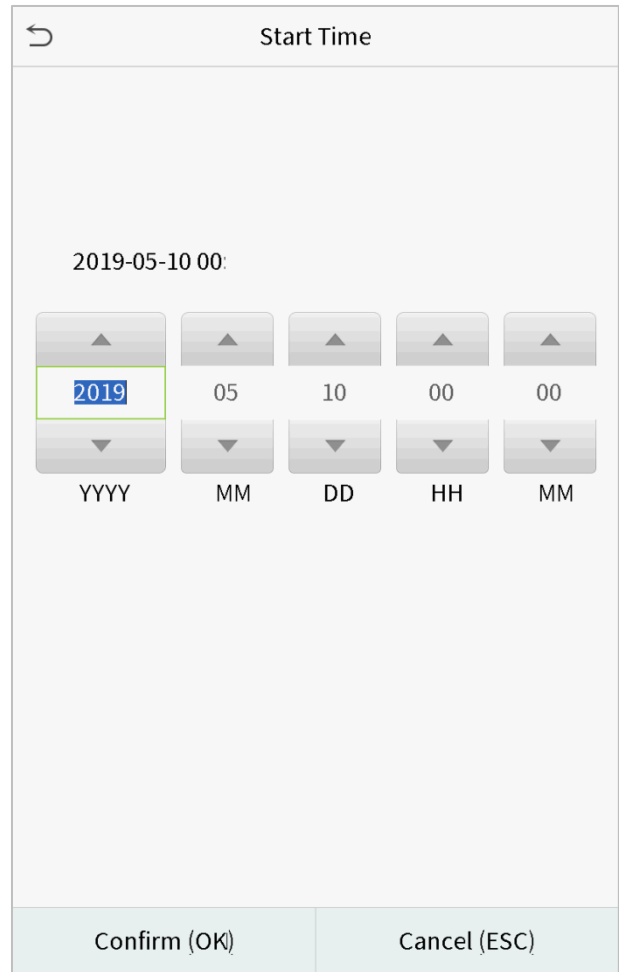
↩	Delete Data
	Delete access records
	Delete Attendance Photo
	Delete Blacklist Photo
	Delete All Data
	Delete Admin Role
	Delete Access Control
	Delete User Photo
	Delete Wallpaper
	Delete Screen Savers

Item	Description
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 verifications which are failed.
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.

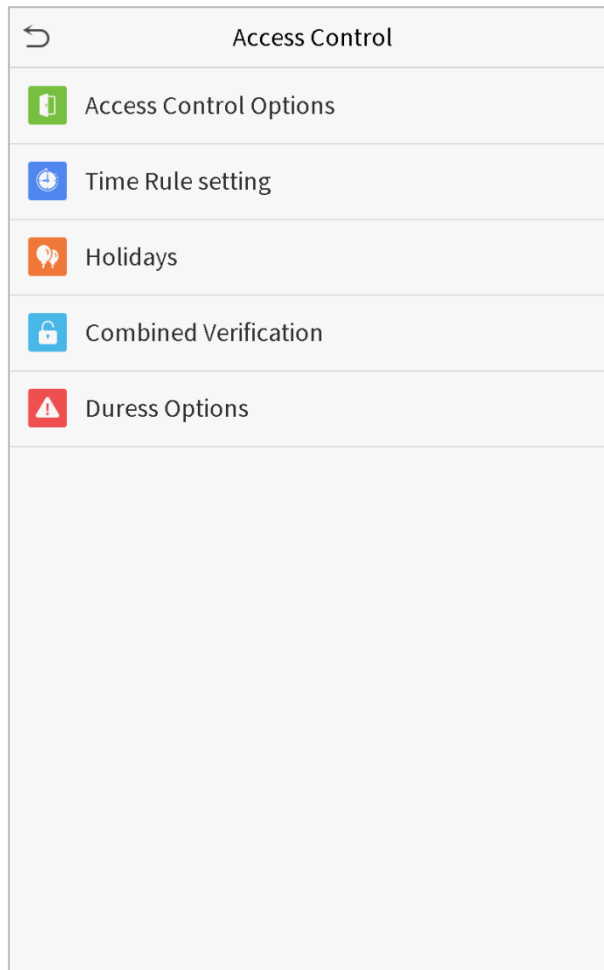


Set the time range and click OK.

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 interface.



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.

Access Control Options	
Gate mode	<input type="checkbox"/>
Door Lock Delay (s)	5
Door Sensor Delay (s)	10
Door Sensor Type	Normal Open (NO)
Verification Mode	Password/Face
Door available time period	1
Normal open time period	None
Master device	In
Verify mode by RS485	Badge Only
Speaker Alarm	<input type="checkbox"/>
Reset Access Setting	

Access Control Options	
Gate mode	<input checked="" type="checkbox"/>
Verification Mode	Password/Face
Door available time period	1
Normal open time period	None
Master device	In
Verify mode by RS485	Badge Only
Speaker Alarm	<input type="checkbox"/>
Reset Access Setting	

Item	Description
Gate Mode	Whether to turn on the gate control mode or not, when set to ON, on this interface will remove Door lock relay, Door sensor relay and Door sensor type function.
Door Lock Delay (s)	The length of time that the device controls the electric lock to be unlock. Valid value: 1~10 seconds; 0 second represents disabling the function.
Door Sensor Delay (s)	If the door is not closed and locked after opening for a certain duration (Door Sensor Delay), an alarm will be triggered. The valid value of Door Sensor Delay ranges from 1 to 255 seconds.
Door Sensor Type	There are three types: None, Normal Open, and Normal Closed. None means door sensor is not in use; Normal Open means the door is always opened when electricity is on; Normal Closed means the door is always closed when electricity is on.
Verification Mode	The supported verification mode includes password/face, User ID only, password, face only, and face + password.
Door available	To set time period for door, so that the door is available only during this.

time period	
Normal Open Time Period	Scheduled time period for "Normal Open" mode, so that the door is always unlocked during this period.
Master Device	When setting up the master and slave, the status of the master can be set to exit on enter. Exit: The record verified on the host is the exit record. Enter: The record verified on the host is the entry record.
Verify mode by RS485	The verification mode used when the device is used as host or slave.
Speaker Alarm	To transmit a sound alarm or disassembly alarm from the local. When the door is closed or the verification is successful, the system will cancel the alarm from the local.
Reset Access Setting	The restored access control parameters include door lock delay, door sensor delay, door sensor type, verification mode, door available time period, normal open time period, master device, and alarm. However, erased access control data in Data Mgt. is excluded.

9.2 Time Rule Setting

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

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

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

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

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 dialog box titled "Time Period 1" with a back arrow icon in the top left corner. The main content area displays the time range "00:00 23:59". Below this, there are four columns of controls for selecting hours and minutes. Each column has an up arrow button above a text field and a down arrow button below it. The text fields contain "00", "00", "23", and "59" respectively. Below the text fields are labels "HH", "MM", "HH", and "MM". The first "00" text field is highlighted with a green border. At the bottom of the dialog box, there are two buttons: "Confirm (OK)" on the left and "Cancel (ESC)" on the right.

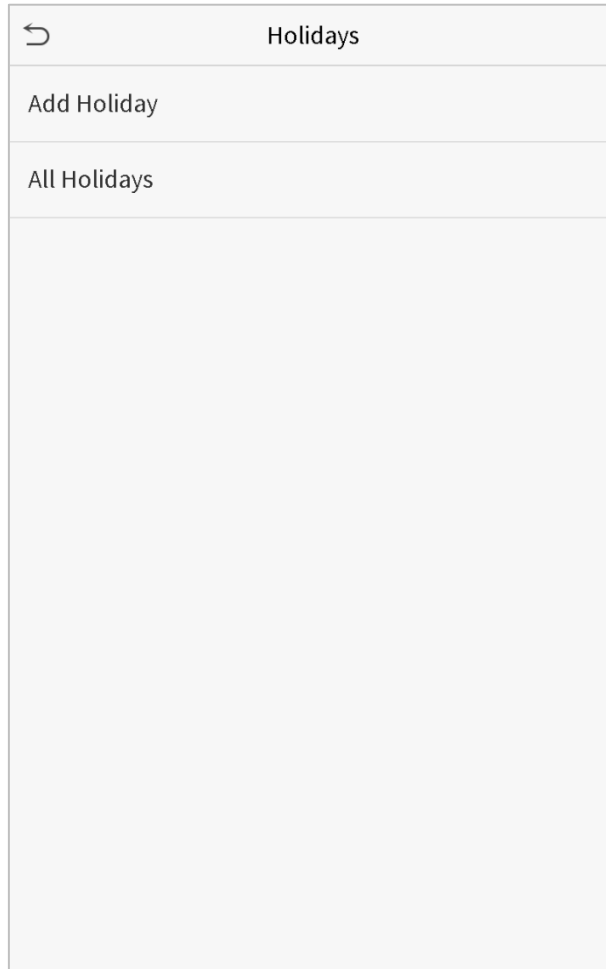
Notes:

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, 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 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.

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**

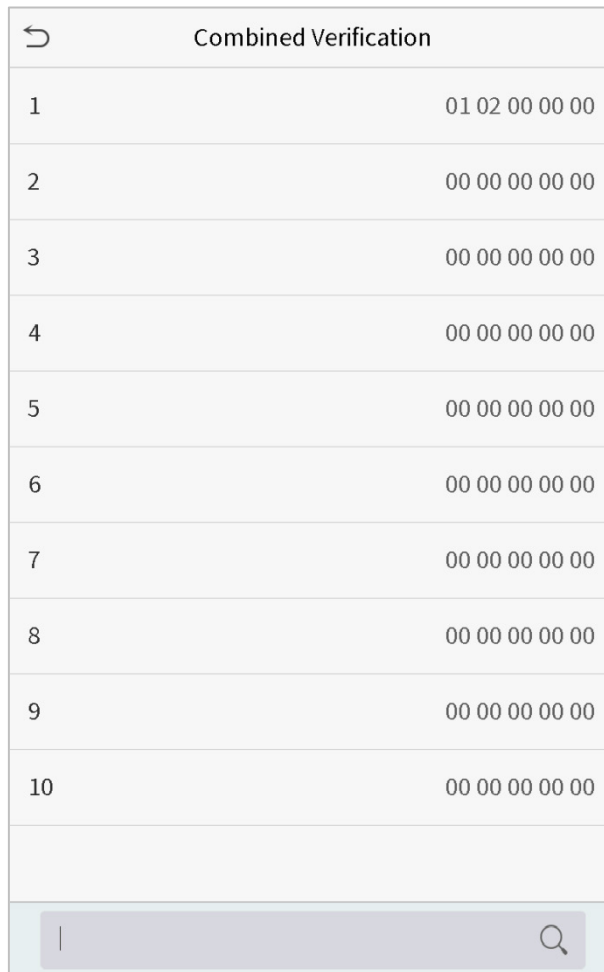
On the Holidays interface, select a holiday item to be deleted and click Delete. Click OK to confirm deletion. After deletion, this holiday is no longer displayed on All Holidays interface.

9.4 Combined Verification Settings

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

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

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



Combined Verification	
1	01 02 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 as (01 03 05 06 08), indicating that the unlocking combination 1 consists of 5 people, and the 5 individuals are from 5 groups, namely, access control group 1 (AC group 1), AC group 3, AC group 5, AC group 6, and AC group 8, respectively.

The door-unlocking combination 2 is set as (02 02 04 04 07), indicating that the unlocking combination 2 consists of 5 people; the first two are from AC group 2, the next two are from AC group 4, and the last person is from AC group 7.

The door-unlocking combination 3 is set as (09 09 09 09 09), indicating that there are 5 people in this combination; all of which are from AC group 9.

The door-unlocking combination 4 is set as (03 05 08 00 00), indicating that the unlocking combination 4 consists of three people. The first person is from AC group 3, the second person is from AC group 5, and the third person is from AC group 8.

Delete a door-unlocking combination

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

9.5 Duress Options Settings

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

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

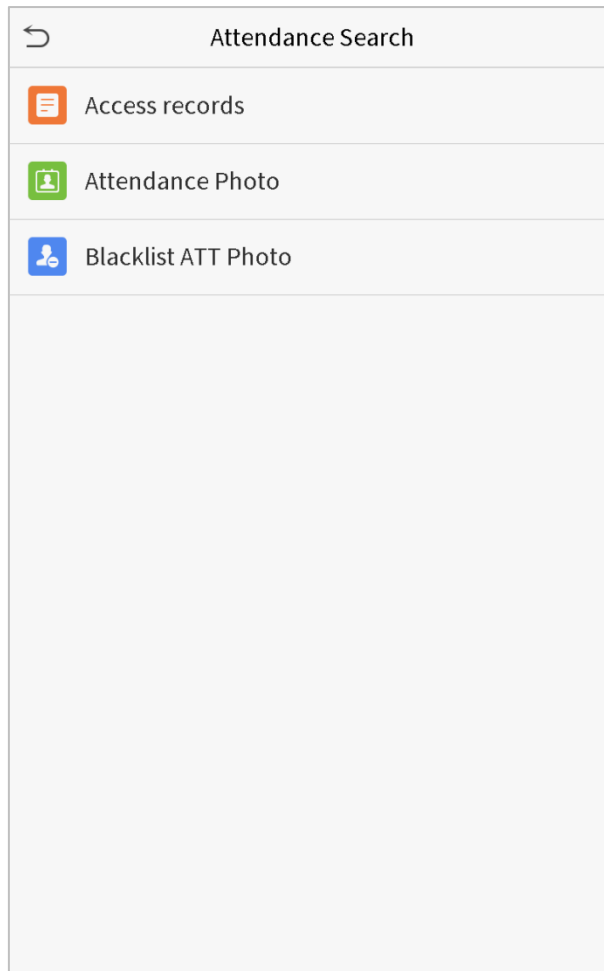
Duress Options	
Alarm on 1:1 Match	<input type="checkbox"/>
Alarm on 1: N Match	<input type="checkbox"/>
Alarm on Password	<input type="checkbox"/>
Alarm Delay(s)	10
Duress Password	None

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

10. Attendance Search

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

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



The process of searching for attendance and 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.

User ID			
Please Input(query all data without input)			
1	2	3	⌫
4	5	6	⬆
7	8	9	⬇
ESC	0	123	OK

⏪	Time Range
<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

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

Personal Record Search		
Date	User ID	Access records
05-10		Number of Records:01
	0	09:09
05-09		Number of Records:02
	1	12:25
	0	08:53
05-08		Number of Records:03
	1	09:17 09:15
	0	09:03
05-07		Number of Records:01
	0	16:06
05-06		Number of Records:04
	0	18:20 15:55
	1	17:28 17:28
05-05		Number of Records:01
	0	10:12
04-30		Number of Records:01
	0	13:56
04-29		Number of Records:05
	1	10:06 10:06 10:06 10:06
	0	08:56
04-28		Number of Records:01
	0	08:57
04-27		Number of Records:06
	0	18:00 17:58 17:57 17:56 17:44 17:40

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

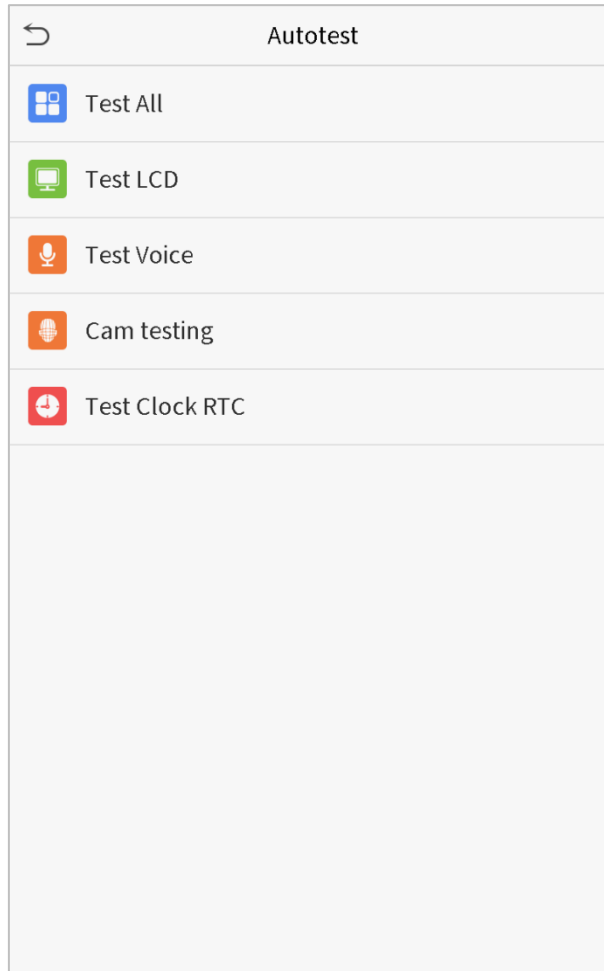
Personal Record Search				
User ID	Name	Access record	Mode	State
1	A	05-09 12:25	15	0

Verification Mode : Face 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 interface.

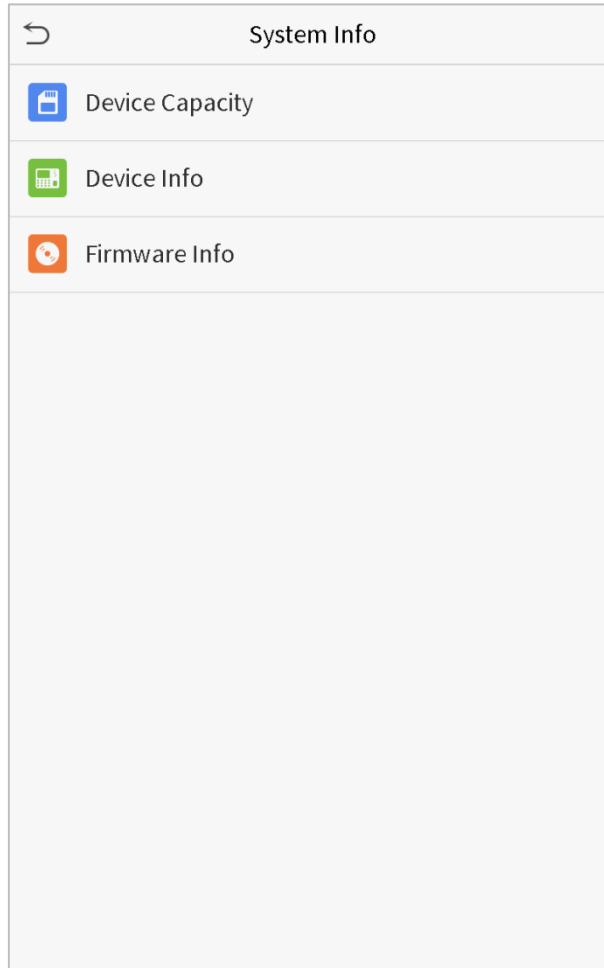


Item	Description
Test All	To automatically test whether the LCD, audio, camera and RTC are normal.
Test LCD	To automatically test the display effect of LCD screen by displaying full-color, pure white, and pure black to check whether the screen displays colors normally.
Test Voice	To automatically test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

12. System Information

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

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



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

13. Connect to ZKBioSecurity Software

13.1 Set the Communication Address

➤ Device side

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

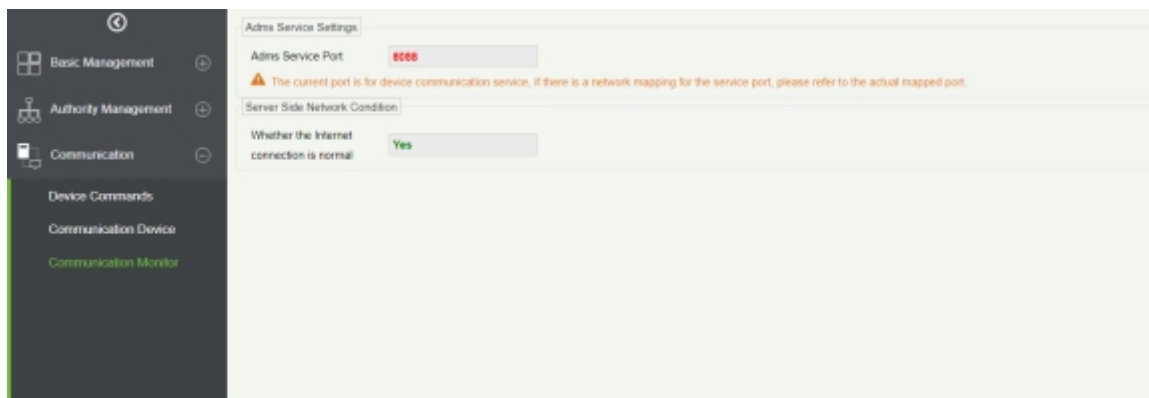
Server port: Set as the service port of ZKBioSecurity (The default is 8088).

Ethernet	
IP Address	192.168.163.150
Subnet Mask	255.255.255.0
Gateway	192.168.163.1
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 side

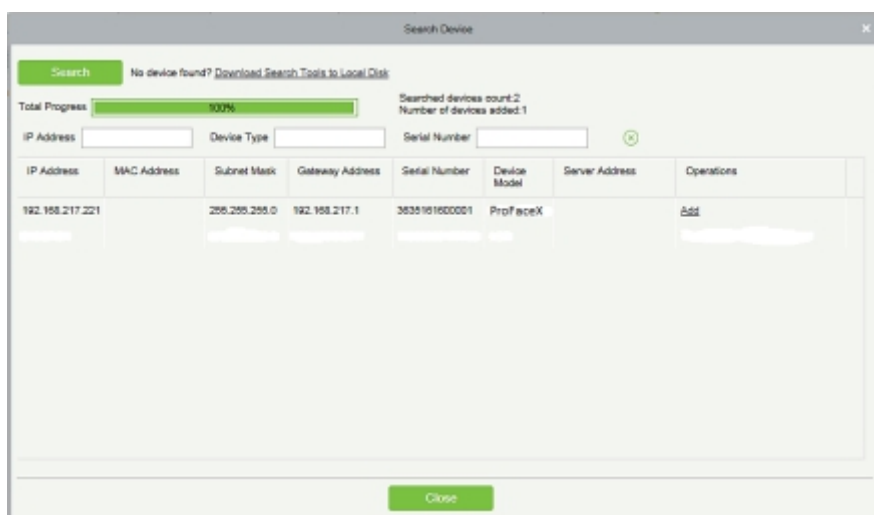
Login to ZKBioSecurity software, click **System** > **Communication** > **Communication Device** to set the adms service port, as shown in the figure below:



13.2 Add Device on the Software

Add device by searching. The process is as follows:

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




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

13.3 Add Personnel on the Software

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

New ✕

Personnel ID*	<input type="text" value="2"/>	Department*	<input type="text" value="General"/>	 <small>(Optimal Size 120*140).</small> <input type="button" value="Browse"/> <input type="button" value="Capture"/>
First Name	<input type="text"/>	Last Name	<input type="text"/>	
Gender	<input type="text" value="-----"/>	Password	<input type="text"/>	
Certificate Type	<input type="text" value="ID"/>	Certificate Number	<input type="text"/>	
Social Security Number	<input type="text"/>	Mobile Phone	<input type="text"/>	
Reservation Code	<input type="text" value="123456"/>	Birthday	<input type="text"/>	
Position	<input type="text"/>	Card Number	<input type="text"/>	
Biological Template Quantity	<input type="text" value="0"/> <input type="text" value="0"/>	Hire Date	<input type="text"/>	

Access Control
Time Attendance
Elevator Control
Plate Register
Personnel Detail

Levels Settings <input checked="" type="checkbox"/> Master	Add Check All Clear All	Superuser <input type="text" value="No"/> Device Operation Role <input type="text" value="Ordinary User"/> Delay Passage <input type="checkbox"/> Disabled <input type="checkbox"/> Set Valid Time <input type="checkbox"/>
--	---	---

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 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 employer.

Our other police fingerprinting devices or development tools can capture original images of citizens' fingerprints. As to whether or not this constitutes infringement of your rights, please contact your government or the final supplier of the device. As the manufacturers of the device, we will assume no legal liability.

Note:

Chinese law includes the following provisions on the personal freedoms of its citizens:

1. There shall be no illegal arrest, detention, search, or infringement of persons;
2. Personal dignity as related to personal freedom 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 law.

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

Eco-friendly Use



- This product's "eco-friendly use period" refers to the period during which this product will not leak toxic or hazardous substances, when used in accordance with the conditions in this manual.
- The eco-friendly use period indicated 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 use 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 of the homogeneous materials is below the limit requirements specified in SJ/T 11363—2006.

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

Note: 80% of this project's components are made using non-toxic, eco-friendly materials. Those which contain toxins or harmful materials or elements are included due to current economic or technical limitations which prevent their replacement with non-toxic materials or elements.

Green
Label

www.zkteco.eu

Copyright©2019 ZKTECO CO., LTD. All rights reserved.