User Manual

5/7-inch Linux Visible Light Product

Version: 1.0

Date: June 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.

About This Manual

- This manual introduces the operations, interfaces and functions of Linux Visible Light Product. For installation, please refer to the Quick Start Guide of the product accordingly.

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

- All pictures shown are for illustration purpose only. Pictures in this manual may not be exactly consistent with the actual products.

Contents

1 Notice for Use

1.1 Finger Positioning★

Recommended fingers: index, middle, or ring fingers; avoid using the thumb or pinky, as they are difficult to accurately press onto the fingerprint reader.

➢ Proper fingerprint placement:
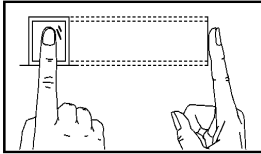
Press your finger onto the fingerprint reader.

Ensure that the center of your finger is aligned with the fingerprint reader.

➢ Improper fingerprint placement:
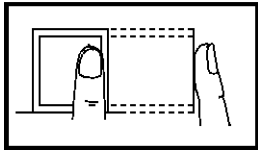
| Too close to the edge | Vertical | Crooked | Too low |
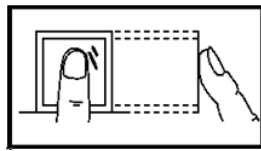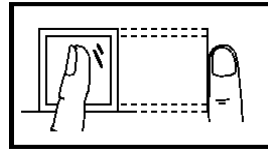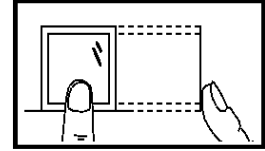
NOTE: Please use the correct method when pressing your fingers onto the fingerprint reader for registration and identification. Our company will assume no liability for recognition issues that may result from incorrect usage of the product. We reserve the right of final interpretation and modification concerning this point.

1.2 Standing Position, Facial Expression and Standing Posture

● **The recommended distance**
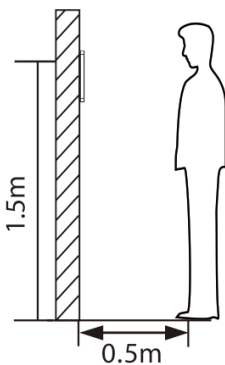
The distance between the device and a user whose height is within 1.4m-1.8m is recommended to be 0.5m. Users may slightly move forwards and backwards to improve the quality of facial images captured.

● **Facial expression and standing posture**

YES

NO
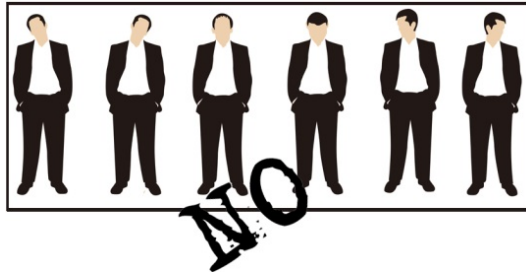
Note: During enrolment and verification, please remain natural facial expression and standing posture.

1.3 Face Registration

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

1.4 Standby Interface

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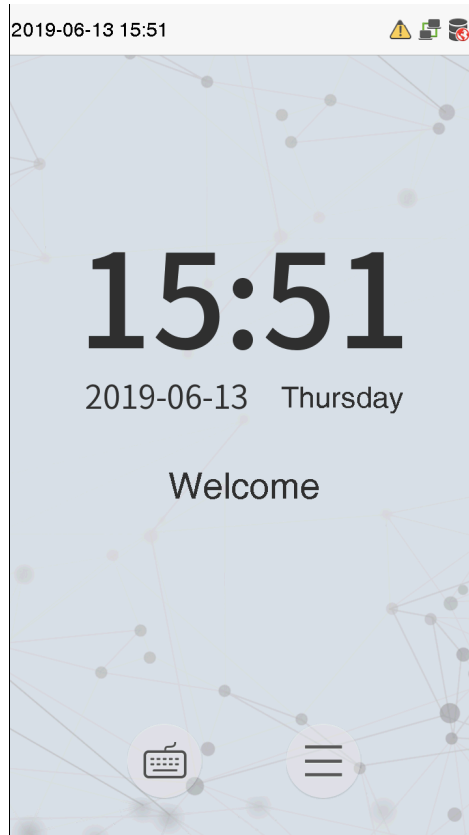
Notes:

1. Click ⌨ to enter the User ID input interface.

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

3. ★The switch of punch state can be done directly by using the screen shortcut keys. Click anywhere on the screen without icons, and six shortcut keys appear, as shown in the figure below:
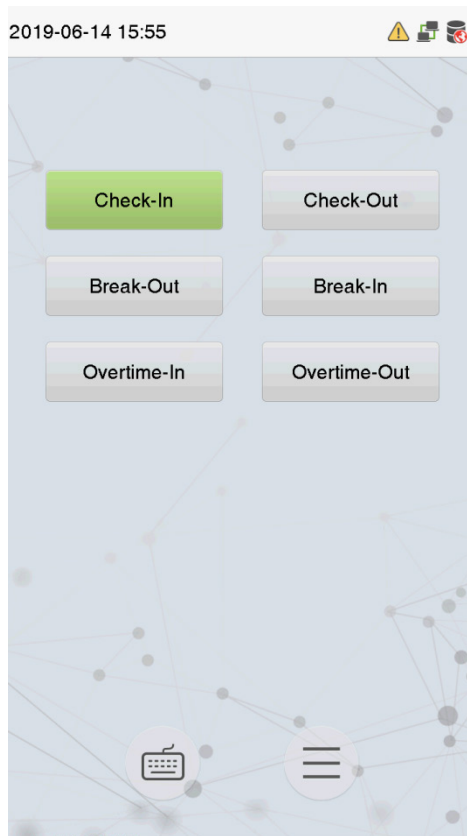
Press the corresponding shortcut key to select the current punch state, which is shown in green. Please refer to "7.5 Shortcut Key Mappings" below for the specific operation method.

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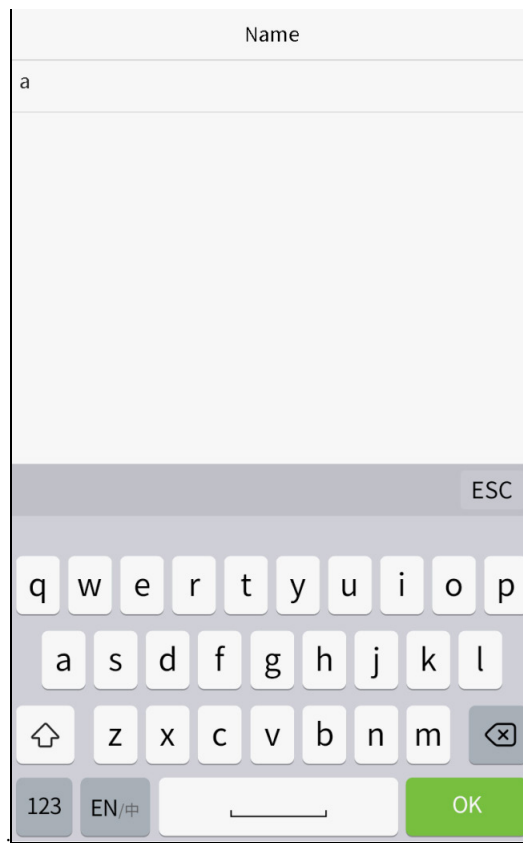
Note: The device supports the input of English, numbers and symbols. Click [**En**] to switch to English keyboard. Press [**123**] to switch to the numeric and symbolic keyboard, and click [**ABC**] to return to the alphabetic keyboard. Click the input box, virtual keyboard appears. Click [**ESC**] to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

1.6 Verification Mode

1.6.1 Fingerprint Verification★

- **1: N fingerprint verification mode**

Compares the fingerprint that is being pressed onto the fingerprint reader with all of the fingerprint data that is stored in the device.

The device will enter the fingerprint authentication mode when a user presses his/her finger onto the fingerprint scanner.

Please follow the correct way to place your finger onto the sensor. For details, please refer to section *1.1 Finger Positioning*.

Verification is successful.
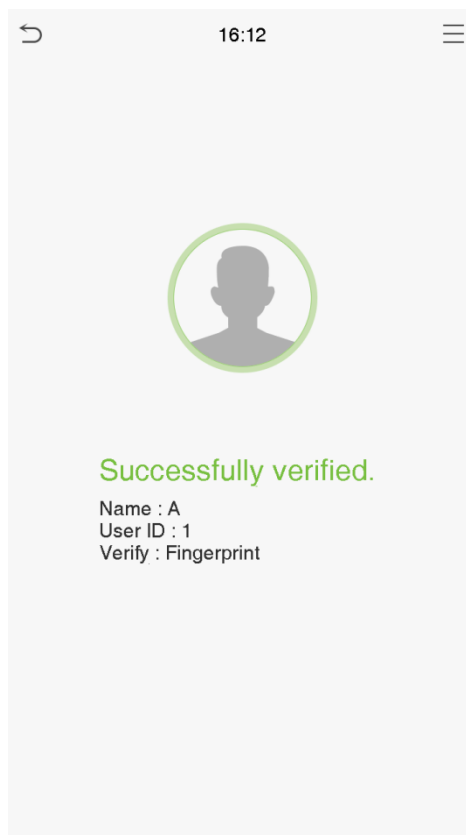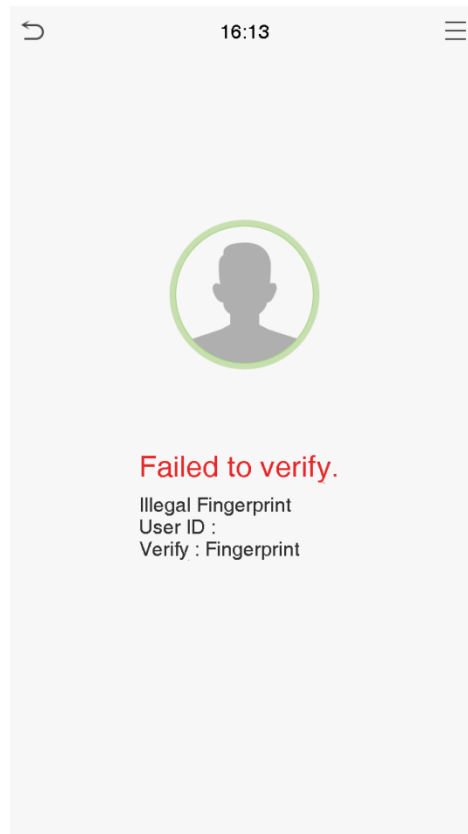
Verification is failed.

- **1: 1 fingerprint verification mode**

Compares the fingerprint that is being pressed onto the fingerprint reader with the fingerprints that are linked to User ID input via the virtual keyboard.

Users may try verifying their identities with 1:1 verification mode when they cannot gain access with 1: N authentication method.

Click the 🖮 button on the main screen to enter 1:1 fingerprint 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
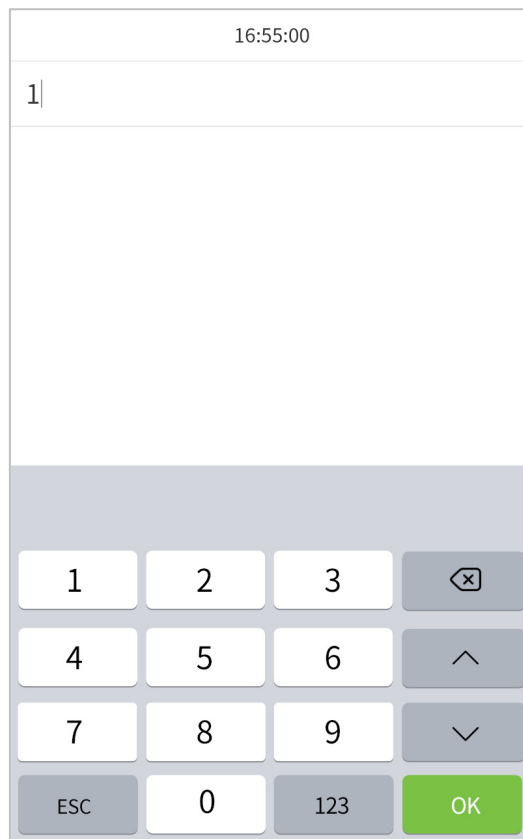
If the user has registered face and password in addition to his/her fingerprints and the verification method is set to

fingerprint/ password/ face verification, the following screen will appear. Select the fingerprint icon ⑲ to enter fingerprint verification mode.

⤾   16:27   ☰

User ID : 1

2. Press the fingerprint to verify.

3. Verification is successful.

Successfully verified.

Name : A
User ID : 1
Verify : Fingerprint

4. Verification is failed.

Failed to verify.

Illegal Fingerprint
User ID : 1
Verify : Fingerprint
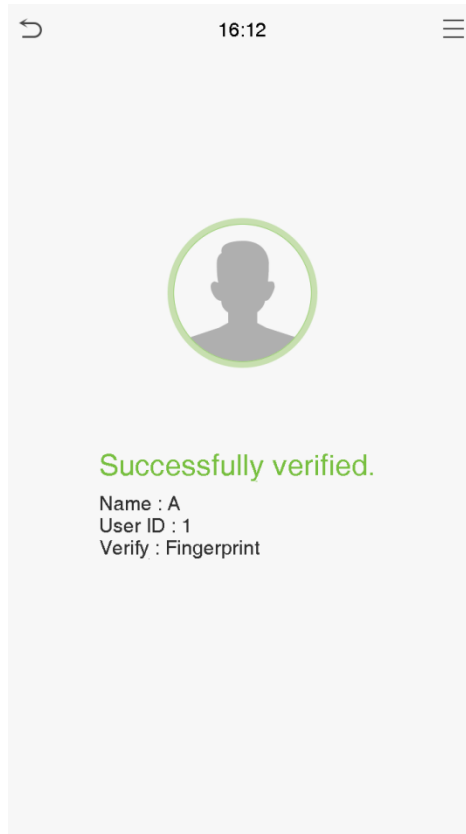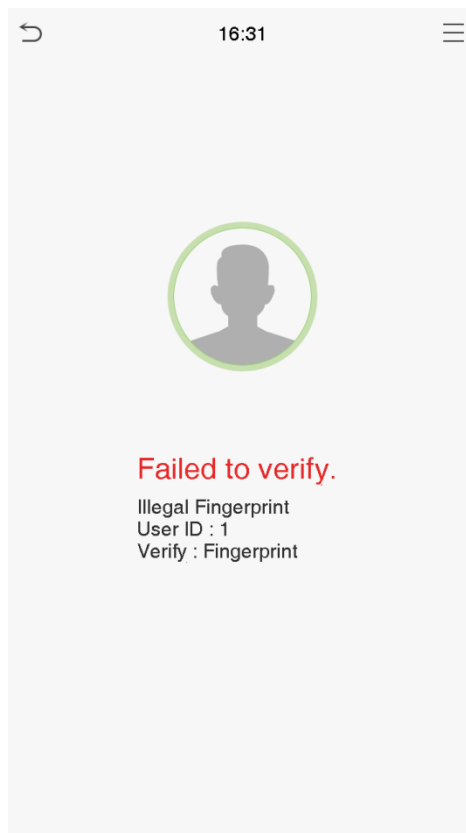
1.6.2 Password Verification

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

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

1. Input the user ID and press [OK].
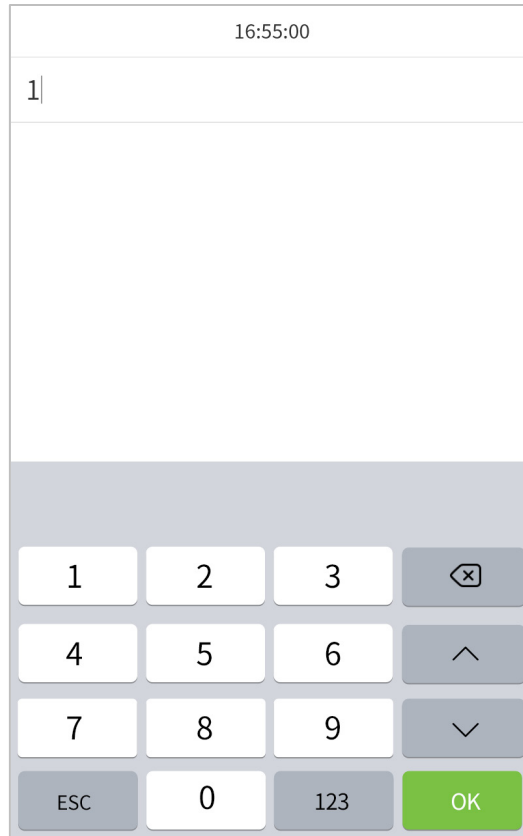
If an employee registers face and fingerprint in addition to password, the following screen will appear. Select the ⚿ icon to enter password verification mode.

2. Input the password and press [OK].
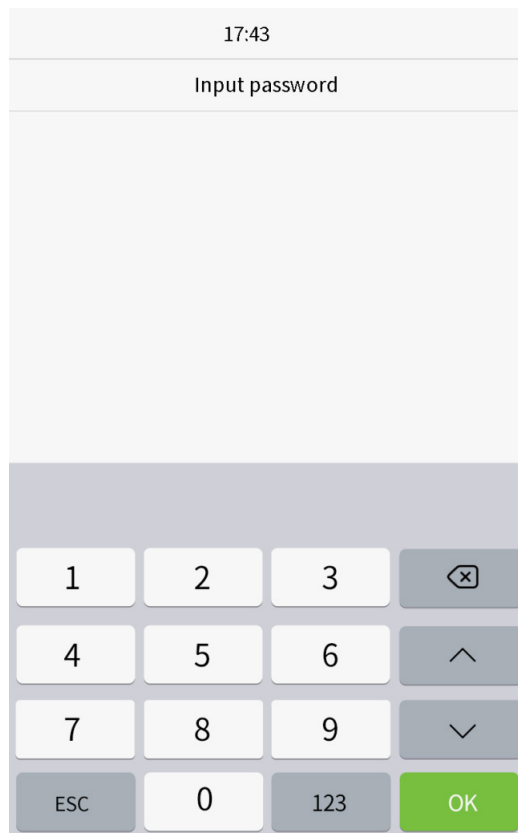
Verification is successful.
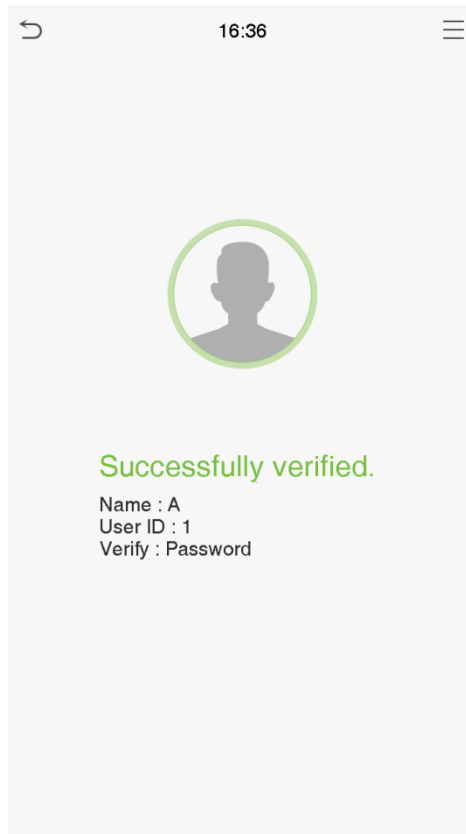
Verification is failed.
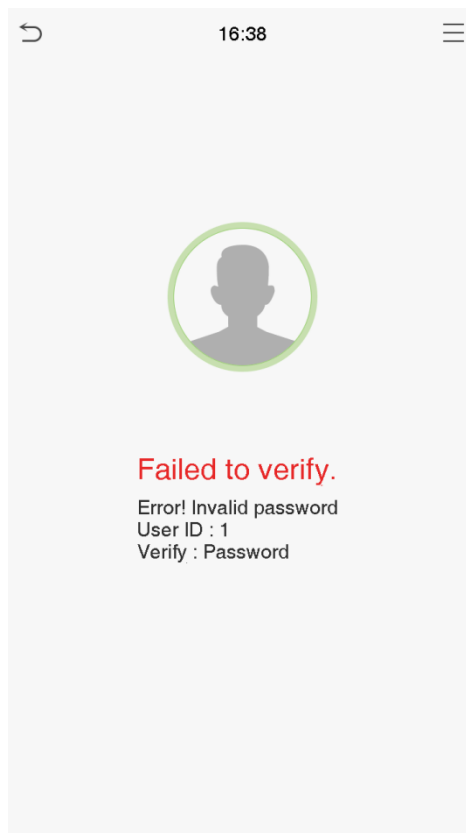
1.6.3 Facial Verification

- **1:N 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.
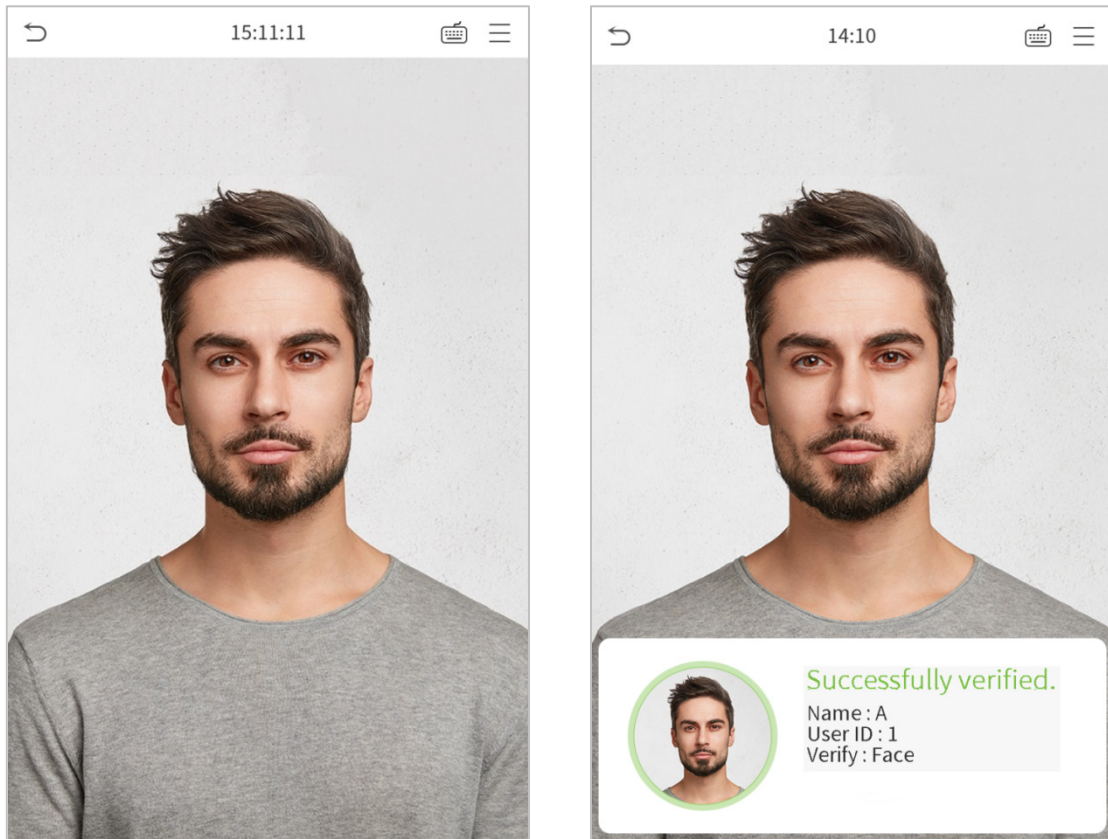
- **1:1 face verification**

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].
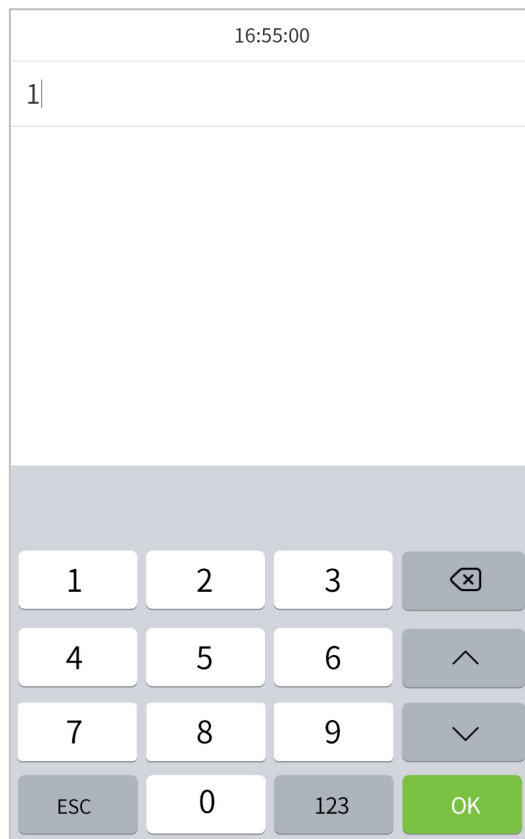
If an employee registers password and fingerprint in addition to face, the following screen will appear. Select the

 icon to enter face verification mode.
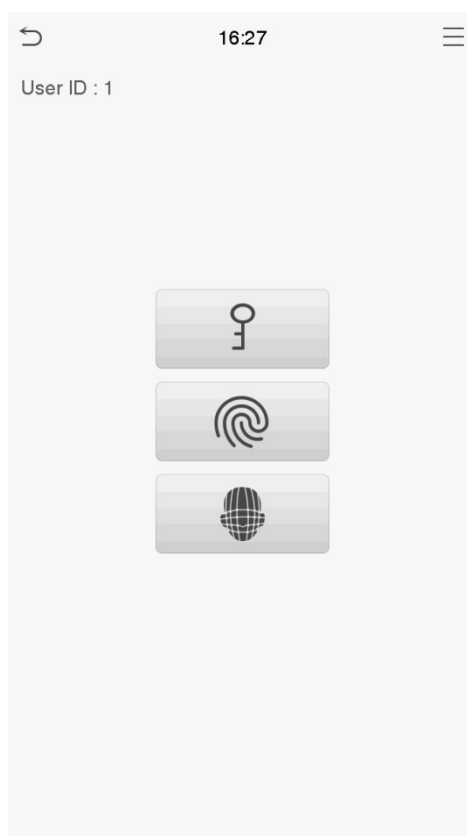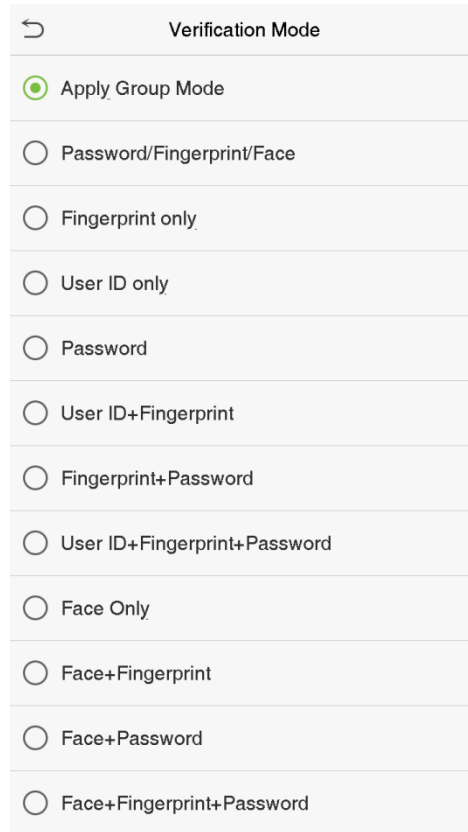
After successful verification, the prompt box "successfully verified" will appear.

Successfully verified.
Name : A
User ID : 1
Verify : Face
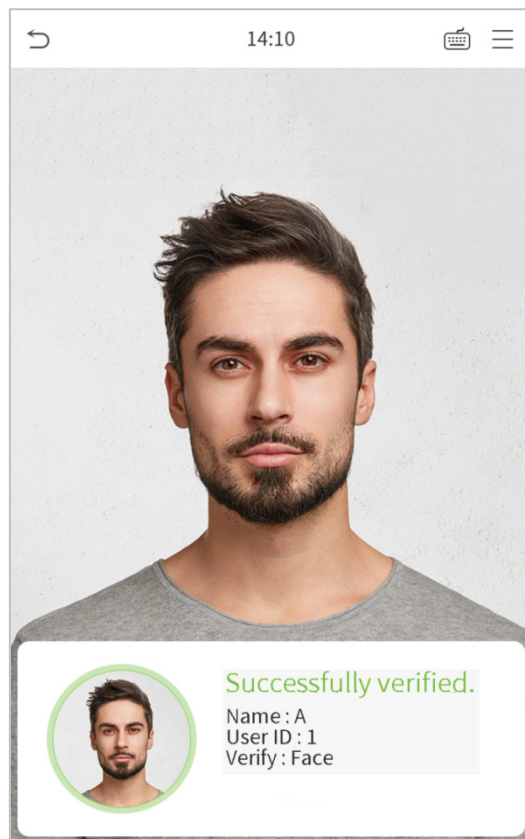
If the verification is failed, it will prompts "Please adjust your position!".

1.6.4 Combined Verification★

To increase security, this device offers the option of using multiple forms of verification methods. A total of 11 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 ![menu icon] on the initial interface to enter the main menu, as shown below:
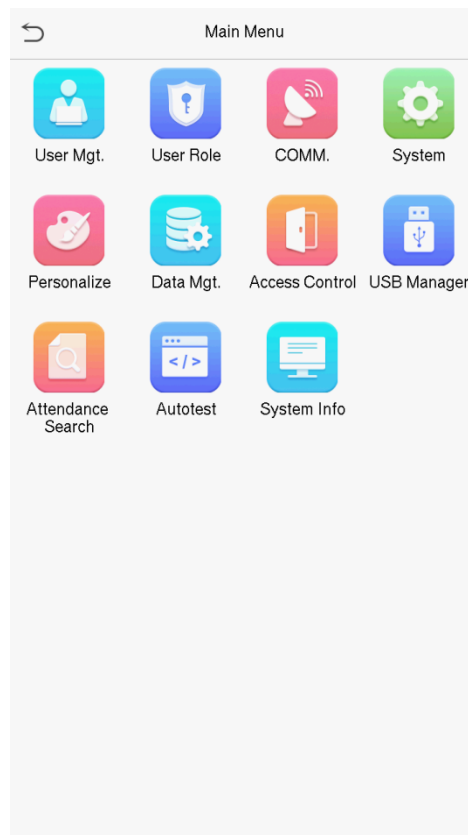
Items	Descriptions
User Mgt.	To add, edit, view, and delete basic information about a user.
User Role	To set the permission scope of the custom role and enroller★, that is, the rights to operate the system.
COMM.	To set the relevant parameters of network, PC connection, cloud server and Wiegand.
System	To set parameters related to the system, including date & time, attendance/access logs setting, face, fingerprint★ parameters , reset to factory and USB upgrade★.
Personalize	To customize settings of interface display, voice, bell, punch state options and shortcut key★.
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.
USB Manager ★	To upload or download specific data from a USB drive.
Attendance Search	Query the specified attendance/access record, check attendance photos and blacklist photos.

Autotest	To automatically test whether each module functions properly, including the LCD, voice, fingerprint sensor★, camera and real-time clock.
System Info	To view data capacity, device and firmware information of the current device.

3 User Management

3.1 Adding Users
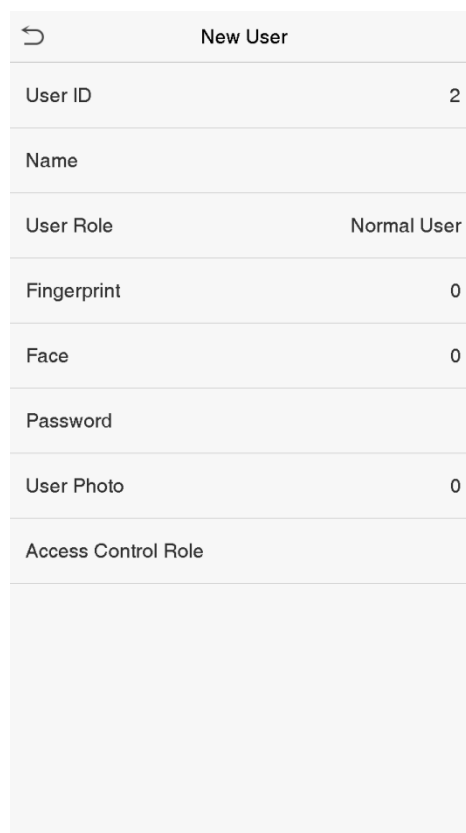
Click **User Mgt.** on the main menu.
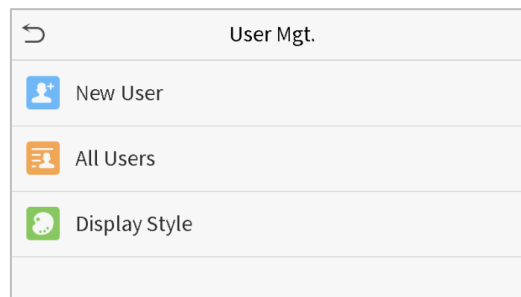
Click **New User**.

● **Register a User ID and Name**

Enter the user ID and name.

Notes:

1) A user name may contain 17 characters.
2) The user ID may contain 1-9 digits by default.
3) During the initial registration, you can modify your ID, which cannot be modified after registration.

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

- **Setting the User Role**

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

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

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

- **Register fingerprint★**

Click **Fingerprint** to enter the fingerprint registration page. Select the finger to be enrolled.

Please select the finger to be enrolled
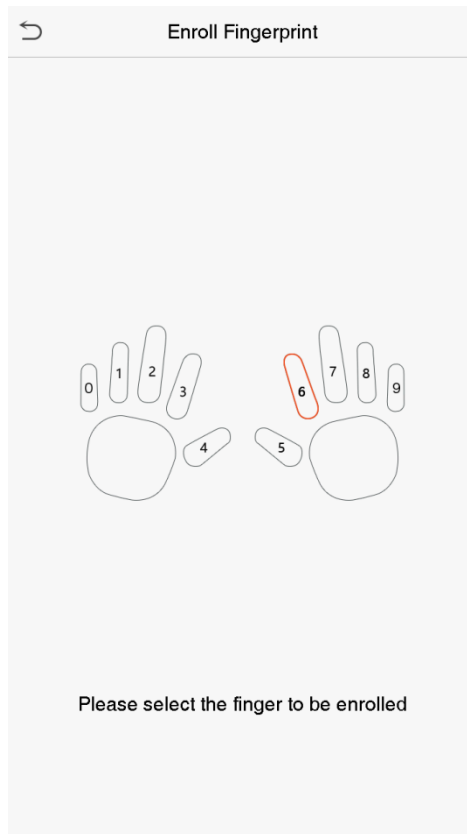
Press the same finger on the fingerprint reader three times. Green indicates that the fingerprint was enrolled successfully.

Enroll Fingerprint(2-6)

Enrolled successfully

73

1   2   3
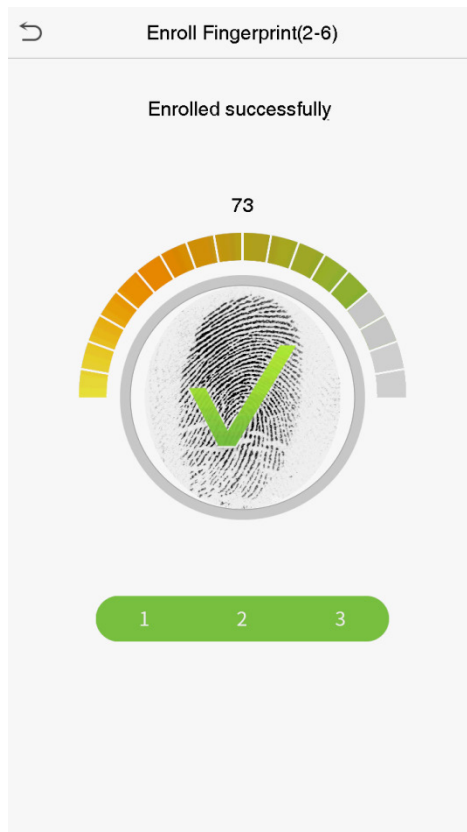
⚫ **Register face**

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

⚫ **Register password**

Click **Password** to enter the password registration page. Enter a password and re-enter it. Click **OK**. If the two entered passwords are different, the prompt "Password not match" will appear.
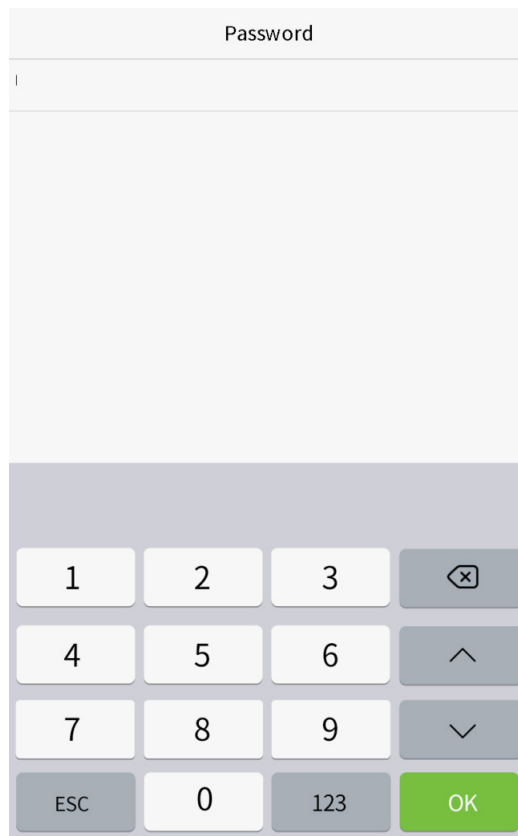
Note: The password may contain one to eight digits by default.

● **Register user photo**

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

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

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

● **Access Control Role★**

User access control sets the door unlocking rights of each person, including the group that the user belongs to, the verification mode, duress fingerprint and whether to apply group time period.

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.

Select verification mode for the user, click **Access Control Role** > **Verification Mode**.

Duress Fingerprint: The user may specify one or more fingerprints that have been registered as a duress fingerprint(s). When press the finger corresponding to the duress fingerprint on the sensor and pass the verification, the system will immediately generate a duress alarm.

Select whether to apply group time period.

Access Control		
Access Group		1
Verification Mode		Apply Group Mode
Duress Fingerprint		Undefined
Apply Group Time Period		⬤

Verification Mode	
⦿	Apply Group Mode
○	Password/Fingerprint/Face
○	Fingerprint only
○	User ID only
○	Password
○	User ID+Fingerprint
○	Fingerprint+Password
○	User ID+Fingerprint+Password
○	Face Only
○	Face+Fingerprint
○	Face+Password
○	Face+Fingerprint+Password
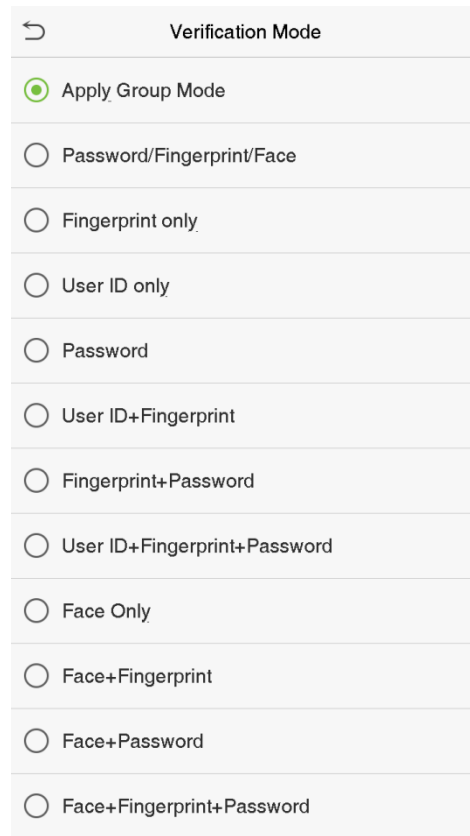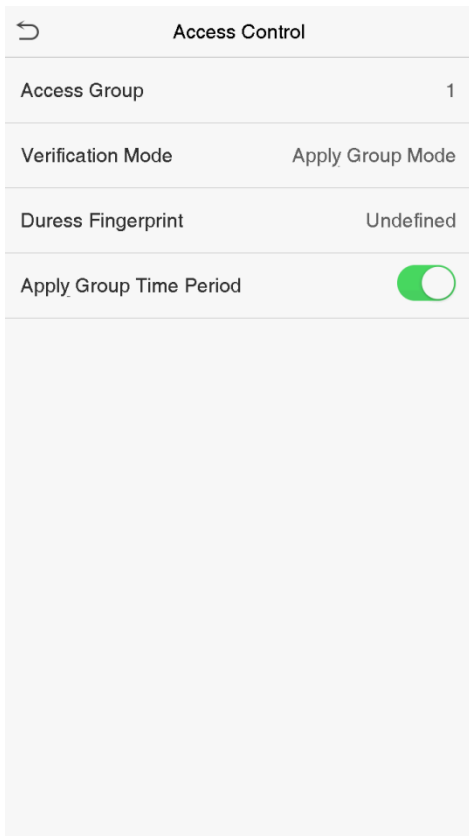
3.2 Search for Users

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.

All Users	
1	A
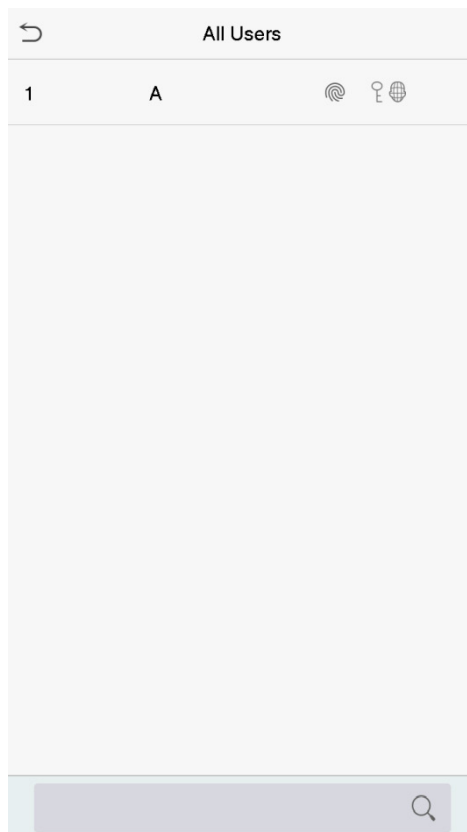
3.3 Edit Users

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
Fingerprint	1
Face	1
Password	********
User Photo	0
Access Control Role	
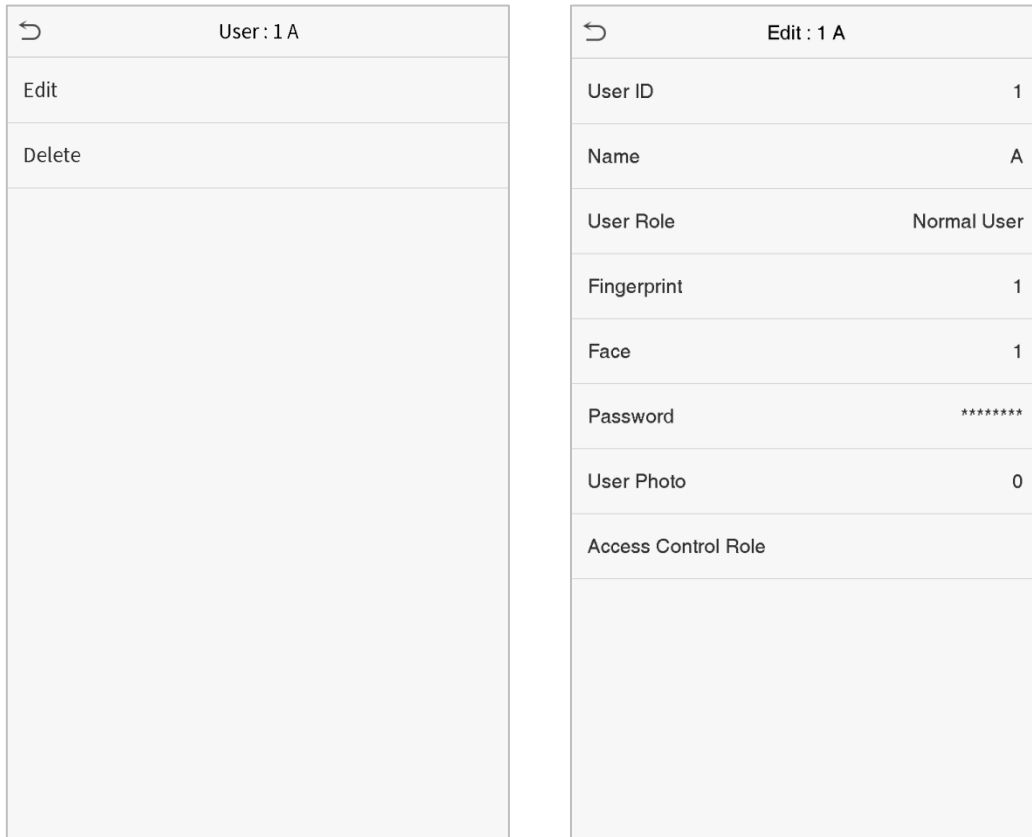
Note: The operation of editing a user is the same as that of adding a user, except that the user ID cannot be modified when editing a user. Operation method refers to "3.1 new users".

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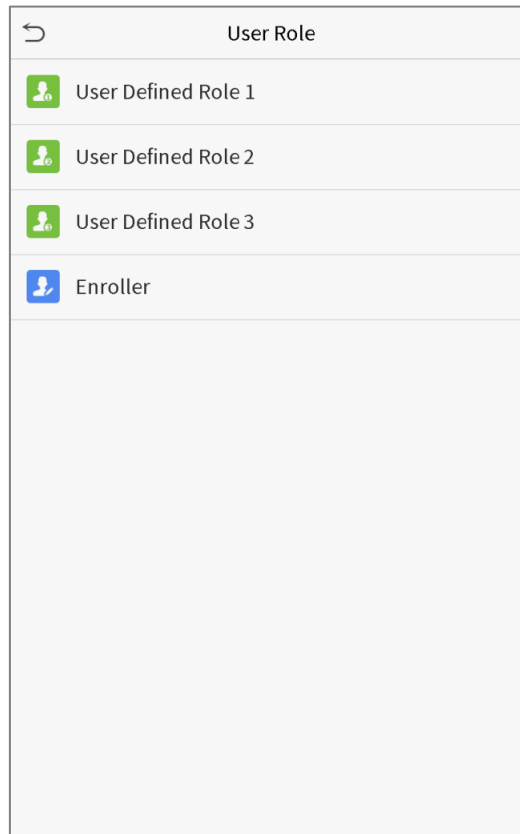
1. Click any item to set a defined role. Click the row of **Enable Defined Role** to enable this defined role. Click **Name** and enter the name of the role.

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

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

If no super administrator is registered, the device will prompt "Please enroll super admin 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.
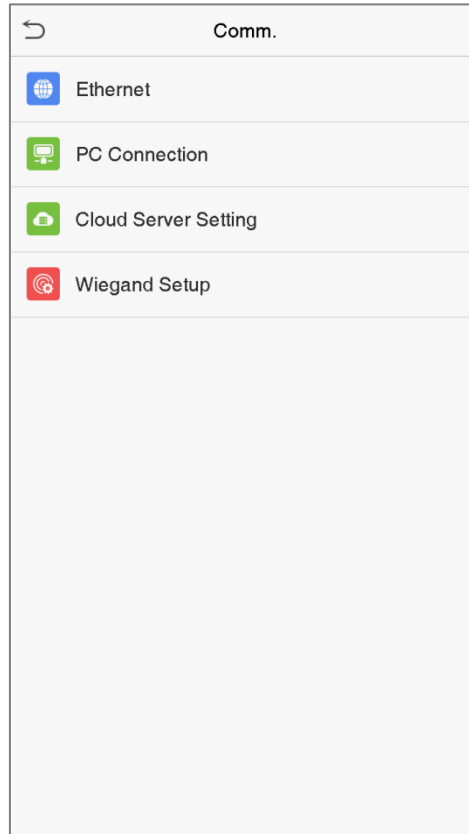
5.1 Network Settings

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.

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

5.2 PC Connection

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

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

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

⤺	PC Connection	
Comm Key		0
Device ID		1

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

5.3 Cloud Server Setting

This represents settings used for connecting with the ADMS server.

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

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

5.4 Wiegand Setup

To set the Wiegand input and output parameters.

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

➢ **Wiegand input**

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

Definitions of various common Wiegand formats:

Wiegand Format	Definitions
Wiegand26	ECCCCCCCCCCCCCCCCCCCCCCCCCO

	Consists of 26 bits of binary code. The 1st bit is the even parity bit of the 2nd to 13th bits, while the 26th bit is the odd parity bit of the 14th to 25th bits. The 2nd to 25th bits are the card numbers.
Wiegand26a	ESSSSSSSSCCCCCCCCCCCCCCCCO Consists of 26 bits of binary code. The 1st bit is the even parity bit of the 2nd to 13th bits, while the 26th bit is the odd parity bit of the 14th to 25th bits. The 2nd to 9th bits are the site codes, while the 10th to 25th bits are the card numbers.
Wiegand34	ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO Consists of 34 bits of binary code. The 1st bit is the even parity bit of the 2nd to 17th bits, while the 34th bit is the odd parity bit of the 18th to 33rd bits. The 2nd to 25th bits are the card numbers.
Wiegand34a	ESSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCO Consists of 34 bits of binary code. The 1st bit is the even parity bit of the 2nd to 17th bits, while the 34th bit is the odd parity bit of the 18th to 33rd bits. The 2nd to 9th bits are the site codes, while the 10th to 25th bits are the card numbers.
Wiegand36	OFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCCMME Consists of 36 bits of binary code. The 1st bit is the odd parity bit of the 2nd to 18th bits, while the 36th bit is the even parity bit of the 19th to 35th bits. The 2nd to 17th bits are the device codes. The 18th to 33rd bits are the card numbers, and the 34th to 35th bits are the manufacturer codes.
Wiegand36a	EFFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCCO Consists of 36 bits of binary code. The 1st bit is the even parity bit of the 2nd to 18th bits, while the 36th bit is the odd parity bit of the 19th to 35th bits. The 2nd to 19th bits are the device codes, and the 20th to 35th bits are the card numbers.
Wiegand37	OMMMMSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCE Consists of 37 bits of binary code. The 1st bit is the odd parity bit of the 2nd to 18th bits, while the 37th bit is the even parity bit of the 19th to 36th bits. The 2nd to 4th bits are the manufacturer codes. The 5th to 16th bits are the site codes, and the 21st to 36th bits are the card numbers.
Wiegand37a	EMMMFFFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCCCCO Consists of 37 bits of binary code. The 1st bit is the even parity bit of the 2nd to 18th bits, while the 37th bit is the odd parity bit of the 19th to 36th bits. The 2nd to 4th bits are the manufacturer codes. The 5th to 14th bits are the device codes, and 15th to 20th bits are the site codes, and the 21st to 36th bits are the card numbers.
Wiegand50	ESSSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO Consists of 50 bits of binary code. The 1st bit is the even parity bit of the 2nd to 25th bits, while the 50th bit is the odd parity bit of the 26th to 49th bits. The 2nd to 17th bits are the site codes, and the 18th to 49th bits are the card numbers.

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

➢ **Wiegand output**

Item	Descriptions
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.
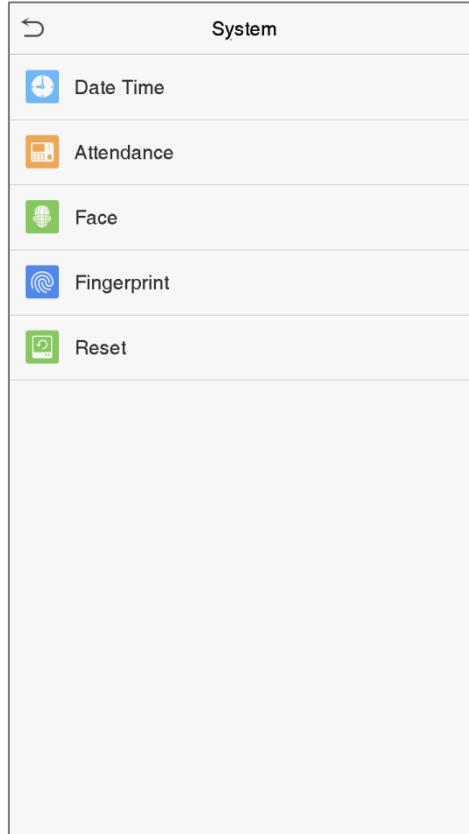
6.1 Date and Time

Click **Date Time** on the System interface.
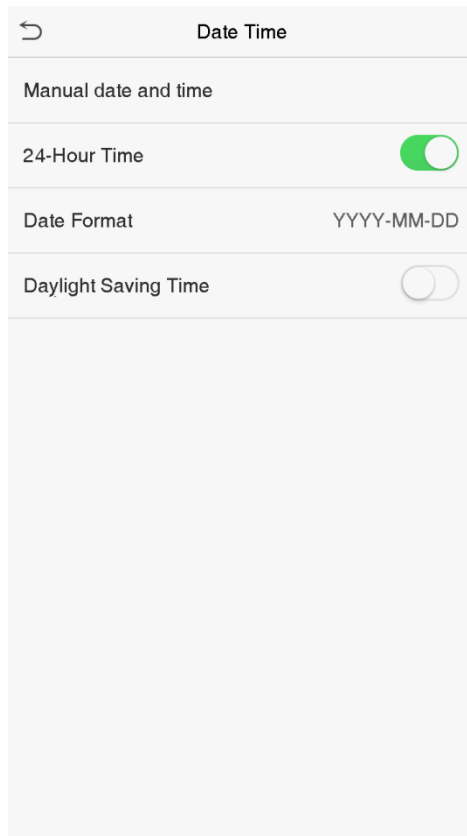
1. You can manually set date and time and click Confirm to save.

2. Click 24-Hour Time to enable or disable this format and select the date format.

★3. Click Daylight Saving Time to enable or disable the function. If enabled, select a daylight saving mode and set

the switch time.

<center>Week mode   Date mode</center>

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 Attendance/Access Logs Setting

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

Item	Description
Duplicate Punch Period (m)	Within the set time range, the attendance record of the same person will not be saved; the valid value ranges from 1 to 999999 minutes.
Camera Mode	Whether to capture and save the current snapshot image during verification. There are 5 modes: **No Photo:** No photo is taken during user verification. **Take photo, no save:** Photo is taken but is not saved during verification. **Take photo and save:** Photo is taken and saved during verification. **Save on successful verification:** Photo is taken and saved for each successful verification. **Save on failed verification:** Photo is taken and saved during each failed verification.

Display User Photo	Whether to display the user photo when the user passes verification.
Alphanumeric User ID	Whether to support letters in a User ID.
Attendance Log Alert/ 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 ATT Data/Access Records	When attendance/access records have reached full capacity, the device will automatically delete a set value of old attendance/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.

		Recommended matching thresholds	
FRR	**FAR**	**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 enrollment 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.
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.
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.
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 Fingerprint Parameters★

Click **Fingerprint** on the System interface.

	Fingerprint	
1:1 Match Threshold		15
1:N Match Threshold		35
FP Sensor Sensitivity		Low
1:1 Retry Times		3
Fingerprint Image		Always show

FRR	FAR	Recommended matching thresholds	
		1:N	1:1
High	Low	45	25
Medium	Medium	35	15
Low	High	25	10

| Item	Descriptions
1:1 Match Threshold	Under 1:1 verification method, the verification will only be successful when the similarity between the acquired fingerprint data and the fingerprint template associated with the entered user ID enrolled in the device is greater than the set value.
1:N Match Threshold	Under 1:N verification method, the verification will only be successful when the similarity between the acquired fingerprint data and the fingerprint templates enrolled in the device is greater than the set value.
FP Sensor Sensitivity	To set the sensibility of fingerprint acquisition. It is recommended to use the default level "**Medium**". When the environment is dry, resulting in slow fingerprint detection, you can set the level to "**High"** to raise the sensibility; when the environment is humid, making it hard to identify the fingerprint, you can set the level to "**Low**".
1:1 Retry Times	In 1:1 Verification, users might forget the registered fingerprint, or press the finger improperly. To reduce the process of re-entering user ID, retry is allowed.
Fingerprint Image	To set whether to display the fingerprint image on the screen during fingerprint enrollment or verification. Four choices are available:

Item	Descriptions
	Show for enroll: to display the fingerprint image on the screen only during enrollment.
	Show for match: to display the fingerprint image on the screen only during verification.
	Always show: to display the fingerprint image on screen during enrollment and verification.
	None: not to display the fingerprint image.

6.5 Factory Reset

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

Click **Reset** on the System interface.
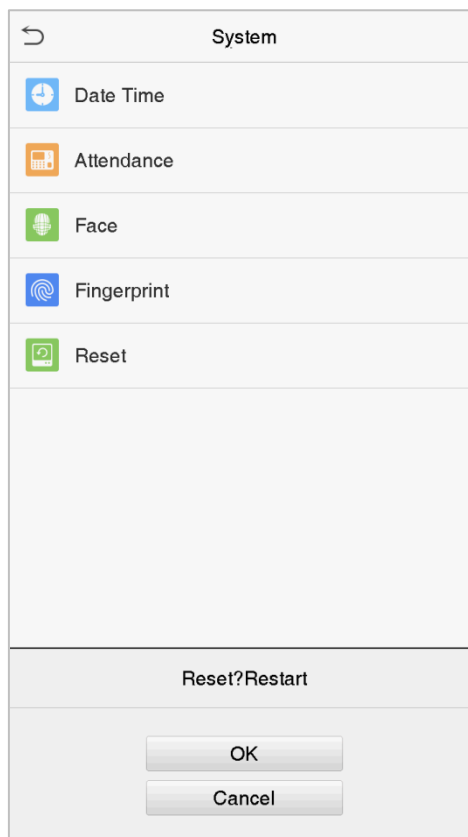
Click **OK** to reset.

6.6 USB Upgrade★

Click **USB Upgrade** on the System interface.

The device's firmware program can be upgraded with the upgrade file in a USB drive. Before conducting this operation, please ensure that the USB drive contains the correct upgrade file and is properly inserted into the device.

7. Personalize Settings

You may customize interface settings, voice, bell, punch state options and shortcut key mappings★.

Click **Personalize** on the main menu interface.
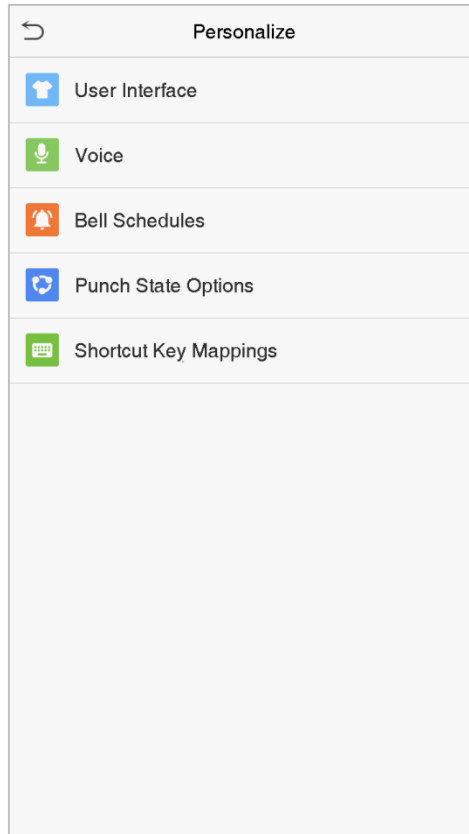
7.1 Interface Settings

You can customize the display style of the main interface.

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

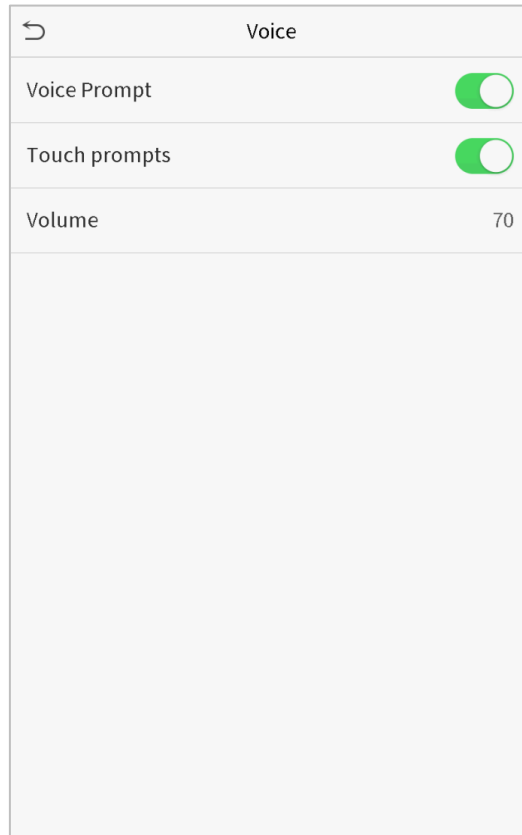| Item	Description
Wallpaper	To select the main screen wallpaper according to your personal preference.
Language	To select the language of the device.
Menu Screen Timeout (s)	When there is no operation, and the time exceeds the set value, the device will automatically go back to the initial interface.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

7.2 Voice Settings

Click **Voice** on the Personalize interface.

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

7.3 Bell Schedules★

Click **Bell Schedules** on the Personalize interface.
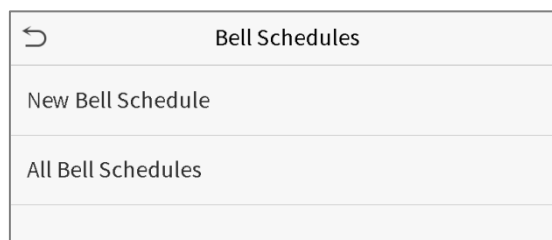
- **Add a bell**

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

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

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

- **Edit a bell**

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

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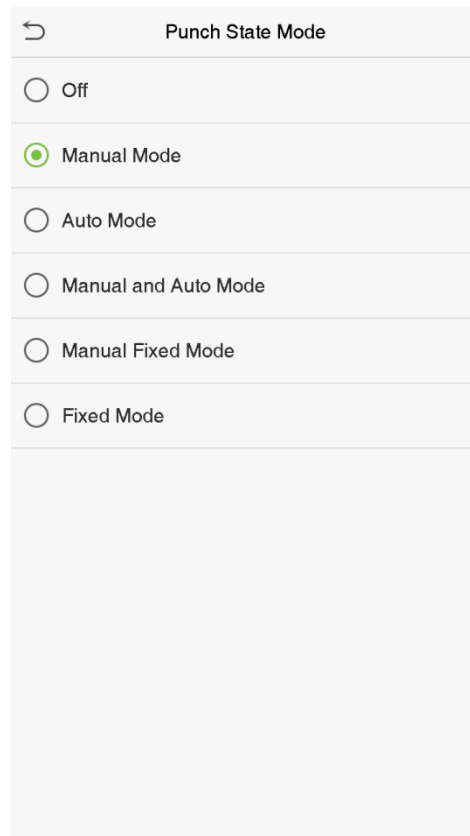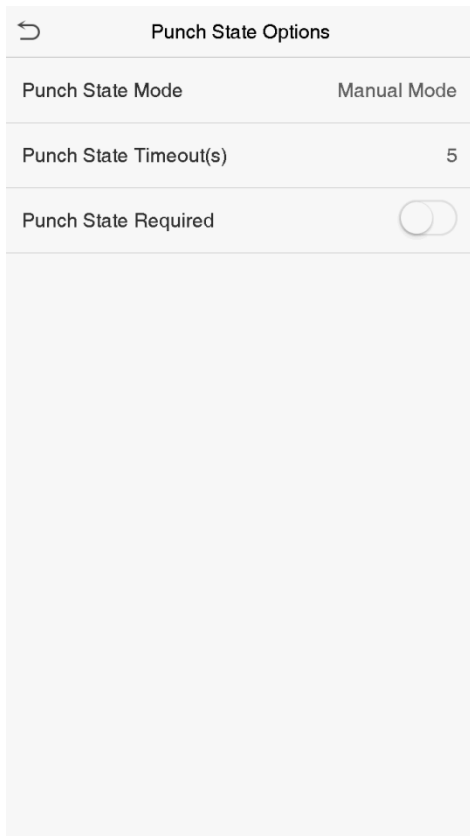
- **Delete a bell**

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

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

7.4 Punch State Options★

Click **Punch State Options** on the Personalize interface.
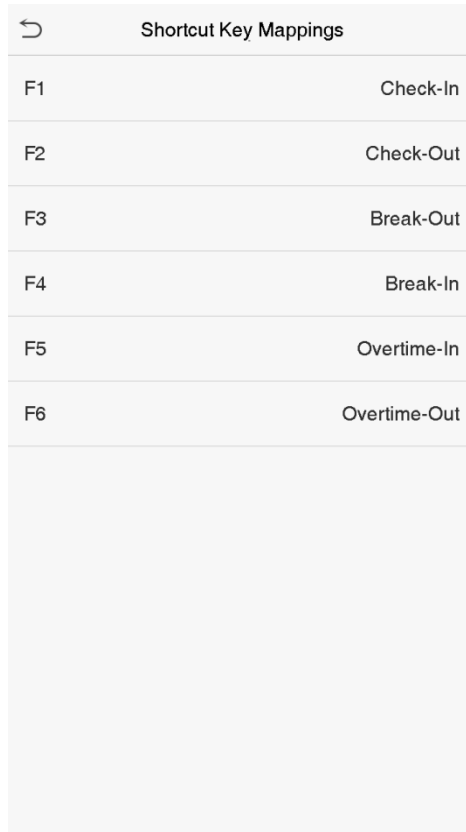
Item	Description
Punch State Mode	To select a punch state mode, which can be: **Off:** To disable the punch state key function. The punch state key set under Shortcut Key Mappings menu will not work. **Manual Mode:** To switch the punch state key manually; the attendance status will be automatically reset after timeout. **Auto Mode:** The punch state key will switch to a specified status according to the predefined schedule set under Shortcut Key Mappings. **Manual and Auto Mode:** The main interface will display the auto-switch punch state key. However, users are still able to select alternative attendance statuses. After timeout, the manually switching punch state key will become auto-switch punch state key. **Manual Fixed Mode:** After the punch state key is manually switched, the punch state key will remain unchanged until being manually switched again. **Fixed Mode:** Only the fixed punch state key will be shown. Users cannot change the status by pressing other keys
Punch State Timeout (s)	The time duration for the time out, i.e. remaining inactive in the main menu.
Punch State Required	To set whether an attendance status must be selected during verification.

7.5 Shortcut Key Mappings★

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

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

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

1. Click the shortcut key to enter the shortcut key setting interface, and select the **function** as punch state key or function key (such as new user, all users, etc.), as shown in the figure below:

↰	F1		↰	F1
Punch State Value	0		Function	New User
Function	Punch State Options			
Name	Check-In			
Set Switch Time				
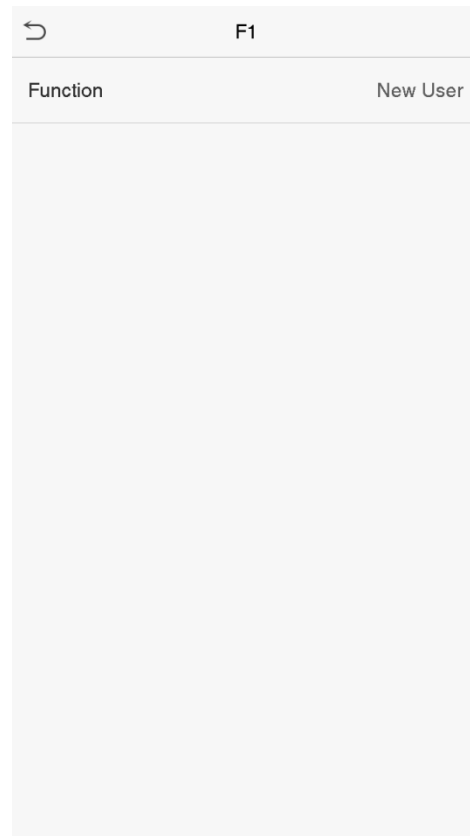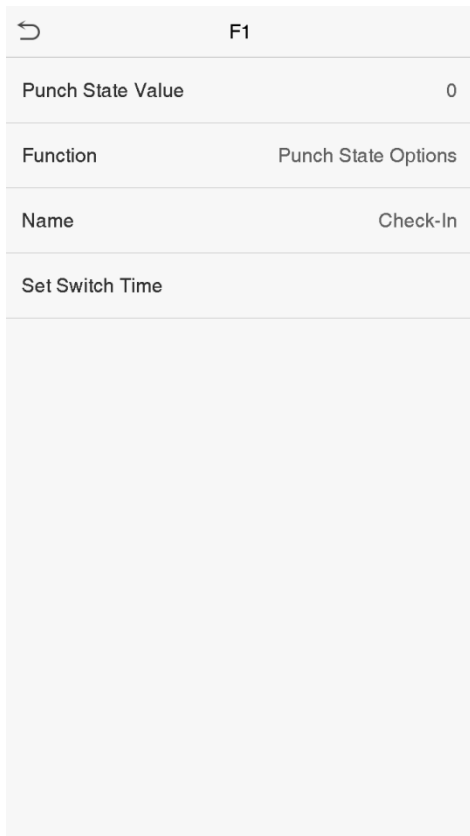
2. If the key is defined as a function key, the setting is completed; If set to a punch state key, set the punch state value (valid value 0~250), the name and switch time.

How to set the switch time?

The switch time is used in conjunction with the **punch state options**. When the **punch state mode** is set to **auto mode**, the switch time should be set. Select the switch period and set the switch time every day, as shown in the figure below:

Switch Cycle	
✅ Monday	
✅ Tuesday	
✅ Wednesday	
✅ Thursday	
✅ Friday	
☐ Saturday	
☐ Sunday	

Set Switch Time	
Switch Cycle	Monday Tuesday W...
Monday	
Tuesday	
Wednesday	
Thursday	
Friday	

Monday

13:55

▲   ▲

13   55

▼   ▼

HH   MM

Confirm (OK)	Cancel (ESC)

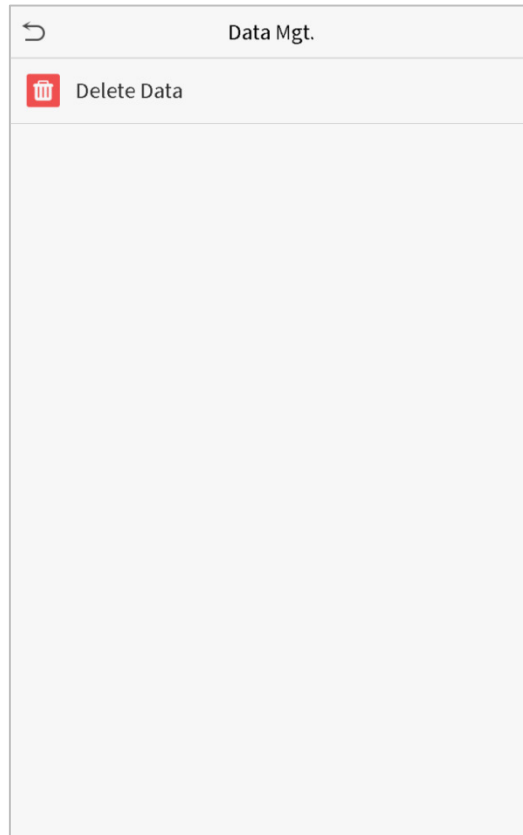| Set Switch Time	
Switch Cycle	Monday Tuesday W...
Monday	08:00
Tuesday	
Wednesday	
Thursday	
Friday	

Note: When the function is set to Undefined, the device will not enable the punch state key.
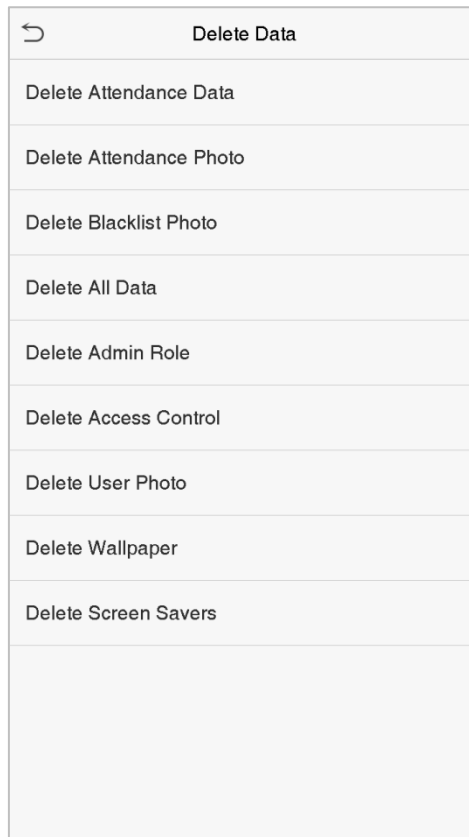
8. Data Management

To delete the relevant data in the device.

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

8.1 Delete Data

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

Item	Description
Delete Attendance Data/Access Records	To delete attendance data/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 attendance logs/access records of all registered users.
Delete Admin Role	To remove administrator privileges.
Delete Access Control	To delete all access data.
Delete User Photo	To delete all user photos in the device.
Delete Wallpaper	To delete all wallpapers in the device.
Delete screen savers	To delete the screen savers in the device.

Note: When deleting the attendance data/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.

Delete Attendance Data	Start Time
Delete All	2019-05-10 00:
Delete by Time Range	
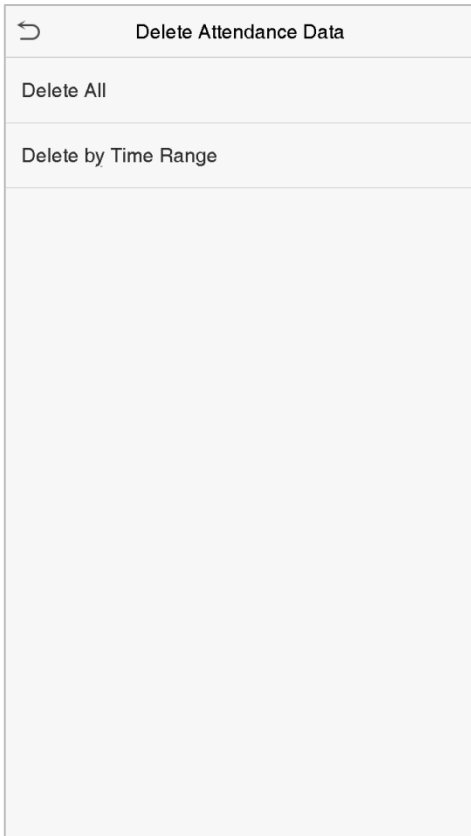
Select Delete by Time Range.   Set the time range and click OK.
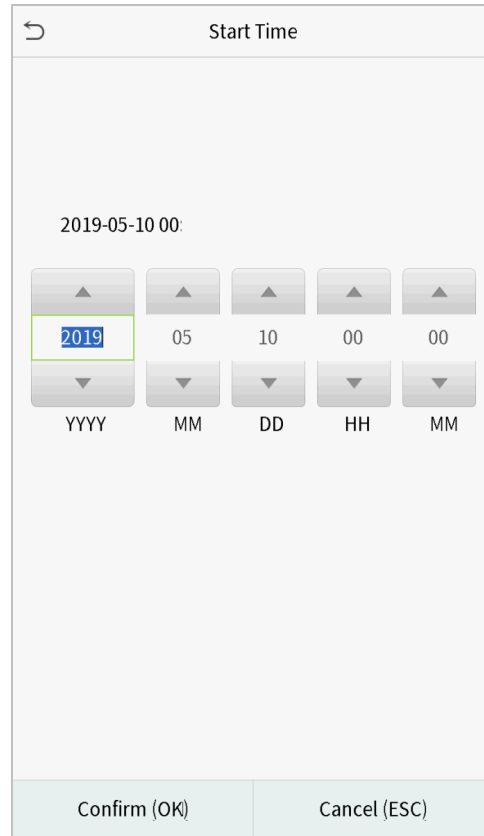
9. Access Control

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

Click **Access Control** on the main menu interface.
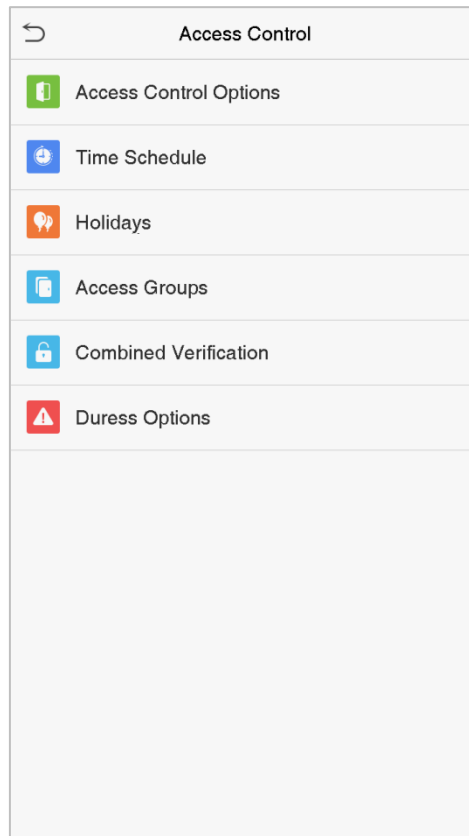
To gain access, the registered user must meet the following conditions:

1. The current door unlock time should be within any valid time zone of the user time period.

2. The user's group must be in the door unlock combination (when there are other groups in the same access combo, verification of members of those groups are also required to unlock the door).

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

9.1 Access Control Options

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

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

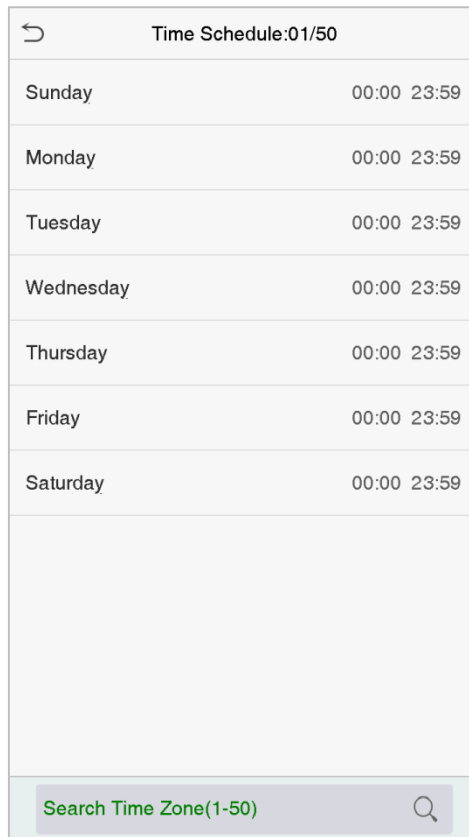| Item	Description
Gate control mode ★	Whether to turn on the gate control mode or not, when set to ON, on this interface will remove Door lock relay, Door sensor relay and Door sensor type function.
Door Lock Delay (s)	The length of time that the device controls the electric lock to be unlock. Valid 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 Close. None means door sensor is not in use; Normal Open means the door is always opened when electricity is on; Normal Close means the door is always closed when electricity is on.
Door Alarm Delay (s)	When the state of the door sensor is inconsistent with that of the door sensor type, an alarm will be triggered after a specified time period, i.e. the Door Alarm Delay. The valid value ranges from 1 to 999 seconds. 0 means immediate alarm.
Retry Times to Alarm	When the number of failed verification reaches a set value, which ranges from 1 to 9 times, an alarm will be triggered. If the set value is "None", the alarm will never be

	triggered due to failed verifications.
Door available time period★	To set time period for door, so that the door is available only during this.
Normal Close Time Period	Scheduled time period for "Normal Close" mode, so that no one can gain access during this 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 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.
Valid holidays	To set if Normal Close Period or Normal Open Period settings are valid in set holiday time period. Choose ON to enable the functions during holiday.
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, normal close time period, normal open time period, auxiliary input configuration and alarm. However, erased access control data in Data Mgt. is excluded.

9.2 Time Schedule

The entire system can define up to 50 time periods. Each time period represents seven time zones, i.e. one week, and each time zone is a valid time period within 24 hours per day. User can only verify within the valid time period. Each time zone format of the time period: HH MM-HH MM, which is accurate to minutes according to the 24-hour clock.

Click **Time Schedule** on the Access Control interface.

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

Sunday	00:00 23:59
Monday	00:00 23:59
Tuesday	00:00 23:59
Wednesday	00:00 23:59
Thursday	00:00 23:59
Friday	00:00 23:59
Saturday	00:00 23:59

Search Time Zone(1-50)

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

Monday

00:00 23:59

| 00 | 00 | 23 | 59 |
| HH | MM | HH | MM |

Confirm (OK)   Cancel (ESC)
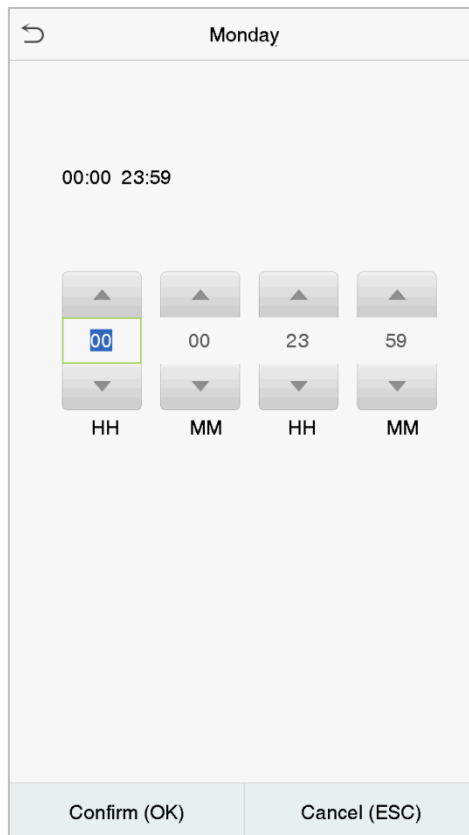
Notes:

1. When the ending time is earlier than the starting time, such as 23:57~23:56, it indicates that access is prohibited all day; when the ending time is later than the starting time, such as 00:00~23:59, it indicates that the interval is valid.

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

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

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.
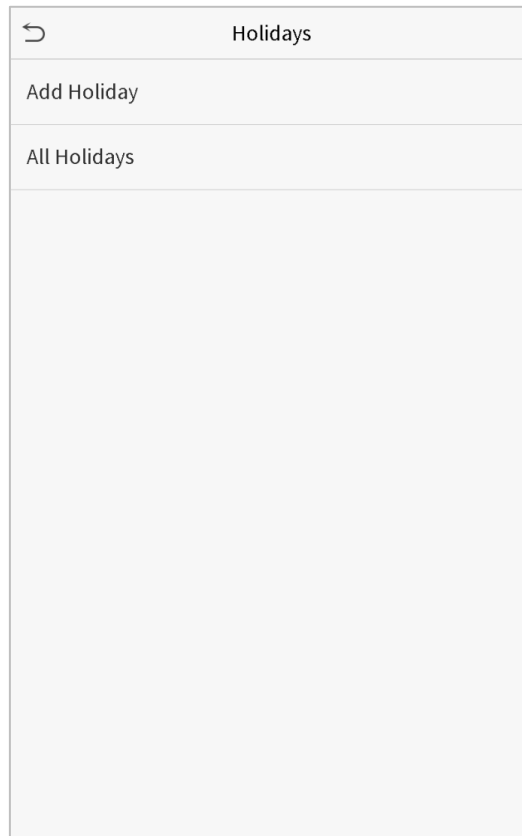
● **Add a New Holiday**

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

⤺	Holidays
No.	1
Start Date	Undefined
End Date	Undefined
Time Period	1

● **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.
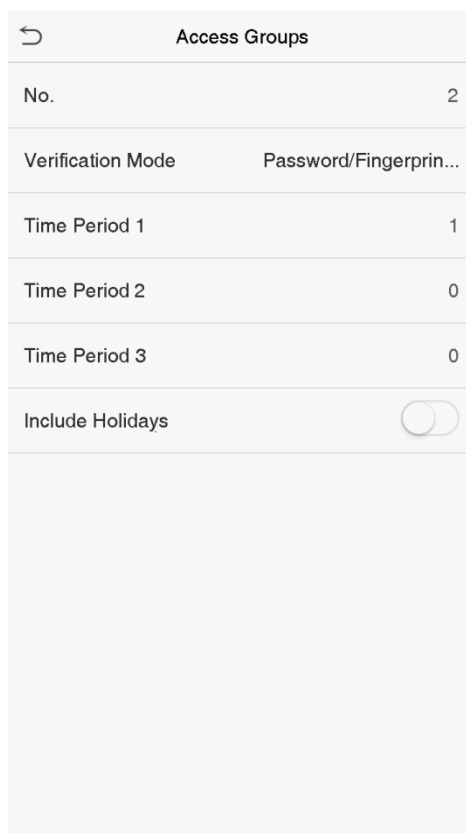
9.4 Access Groups★

This is to easily manage groupings and users in different access groups. Settings of an access group such as access time zones are applicable to all members in the group by default. However, users may manually set the time zones as needed. User authentication takes precedence over group authentication when group authentication modes overlap with the individual authentication methods. Each group can set a maximum of three time zones. By default, newly enrolled users are assigned to Access Group 1; they can be assigned to other access groups.

Click **Access Groups** on the Access Control interface.
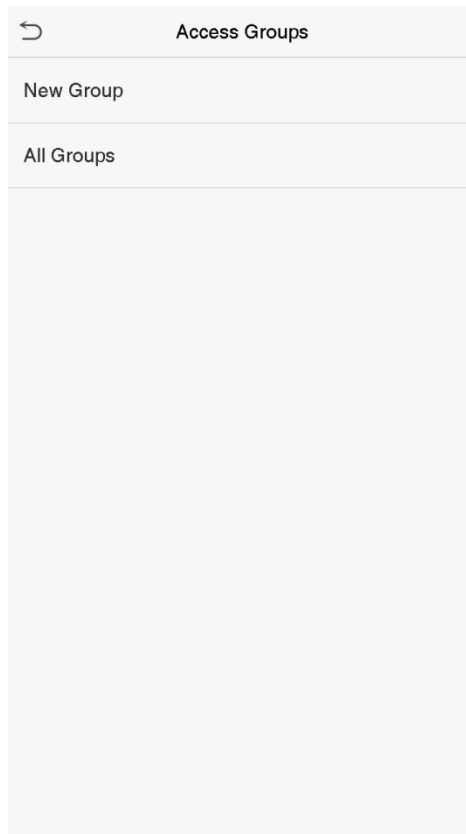
● **Add a New Group**

Click **New Group** on the Access Groups interface and set access group parameters.

Note:

1. There is a default access group numbered 1, which cannot be deleted, but can be modified.

2. A number cannot be modified after being set.

3. When the holiday is set to be valid, personnel in a group may only open the door when the group time zone overlaps with the holiday time period.

4. When the holiday is set to be invalid, the access control time of the personnel in a group is not affected during holidays.

- **Edit a Group**

On the All Groups interface, select the access group item to be modified. Click Edit and modify access group parameters.
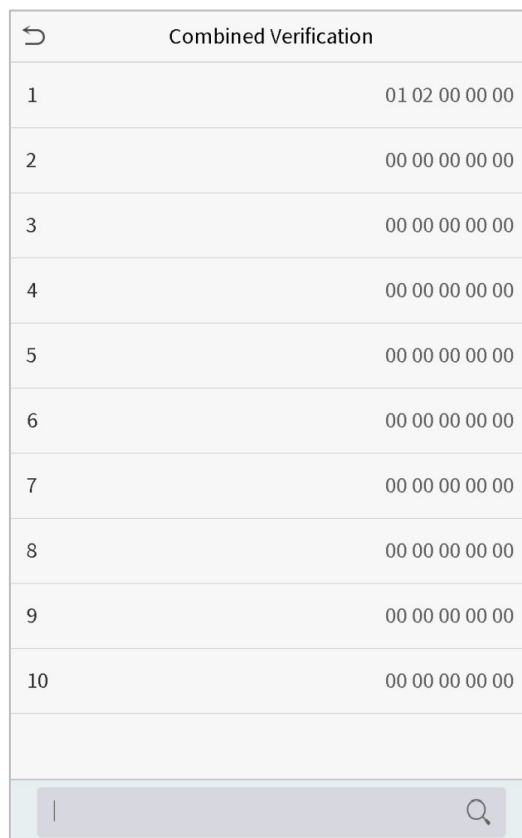
- **Delete a Group**

On the All Groups interface, select the access group item to be deleted and click Delete. Click OK to confirm deletion. The deleted access group is no longer displayed in All Groups.

9.5 Combined Verification Settings

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

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

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

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

Examples:

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

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

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

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

Delete a door-unlocking combination

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

9.6 Duress Options Settings

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

Click **Duress Options** on the Access Control interface.
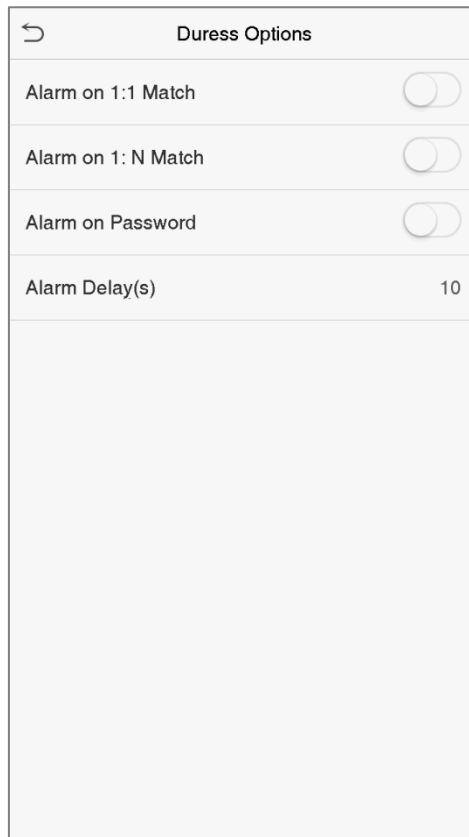
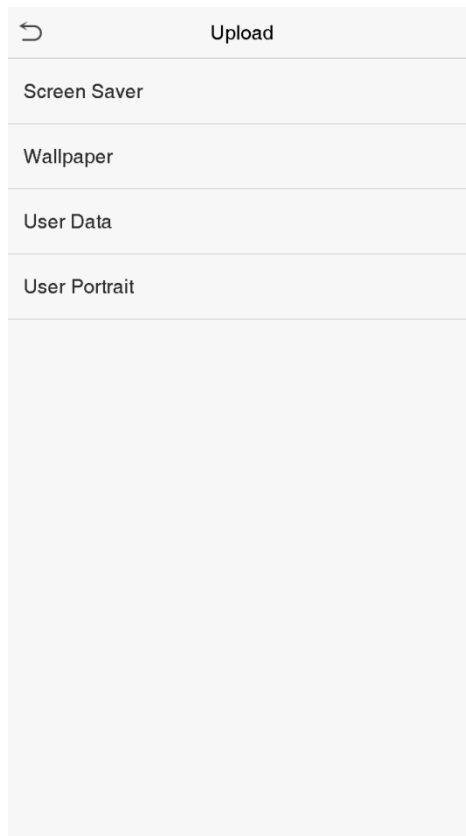| Item	Description
Alarm on 1:1 Match	When a user uses any fingerprint to perform the 1:1 verification, an alarm signal will be generated, otherwise there will be no alarm signal.
Alarm on 1:N Match	When a user uses any fingerprint to perform 1:N verification, an alarm signal will be generated, otherwise 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. USB Manager★

You can import user information, access data and other data from a USB drive to computer or other devices.
Before uploading or downloading data from or to the USB drive, insert the USB drive into the USB slot first.
Click **USB Manager** on the main menu interface.

10.1 Download
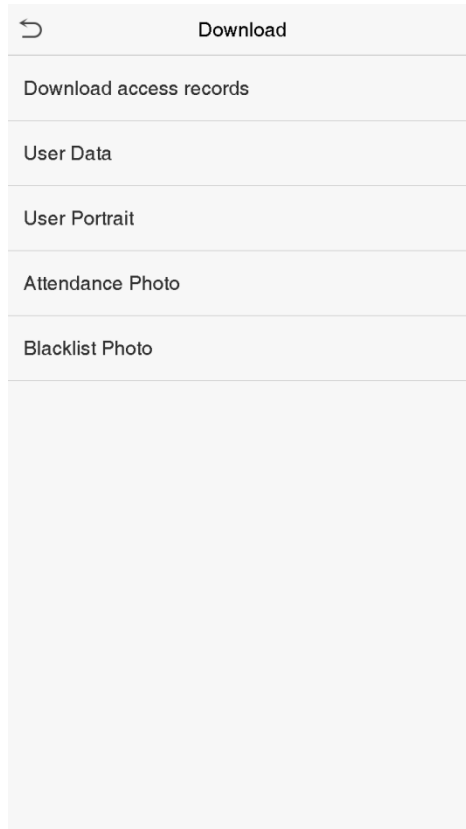
| Item	Descriptions
Download access records	To download access data within a specified time period or all data to a USB drive
User Data	To download all user information from the device to a USB drive
User Portrait	To download all user pictures from the device to a USB drive
Attendance Photo	To download attendance photos stored in the device within a specified time period or all attendance photos from the device to a USB drive. Picture format is JPG
Blacklist Photo	To download blacklisted photos taken after failed verifications within a specified time period or all pictures taken after failed verifications from the device to a USB drive

10.2 Upload

Item	Descriptions
Screen Saver	To upload a screen saver from a USB drive to the device. Before uploading, you may select **Upload selected picture** or **Upload all pictures**.
Wallpaper	To upload a wallpaper from a USB drive to the device. Before uploading, you may select **Upload selected picture** or **Upload all pictures**. The images will be displayed on the screen after manual settings.
User Data	To upload all user information from a USB drive to the device.
User Portrait	To upload a JPG picture named with a user ID from a USB drive to the device. Before uploading, you may select **Upload Current Picture** or **Upload All Pictures**.

11. Attendance Search

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

Click **Attendance Search** on the main menu interface.
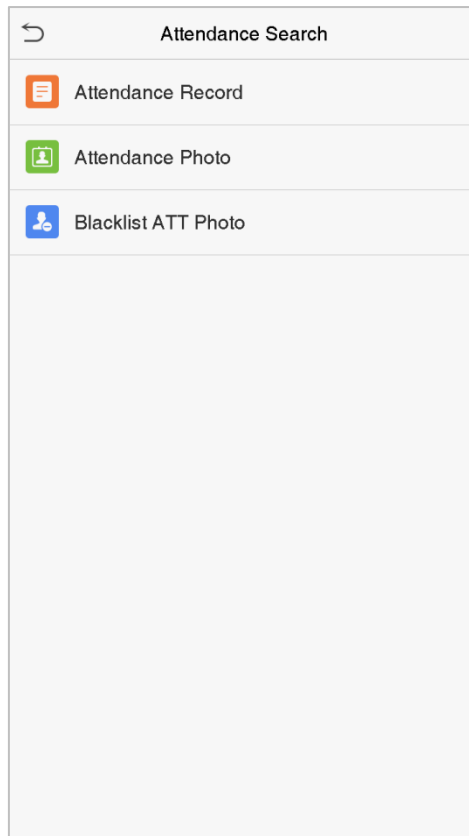
The process of searching for attendance and blacklist photos is similar to that of searching for attendance/access records. The following is an example of searching for attendance/access records.

On the Attendance Search interface, click **Attendance/Access Record**.

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
⦿ Today	
○ Yesterday	
○ This week	
○ Last week	
○ This month	
○ Last month	
○ All	
○ User Defined	

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

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

12. Autotest

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

Click **Autotest** on the main menu interface.
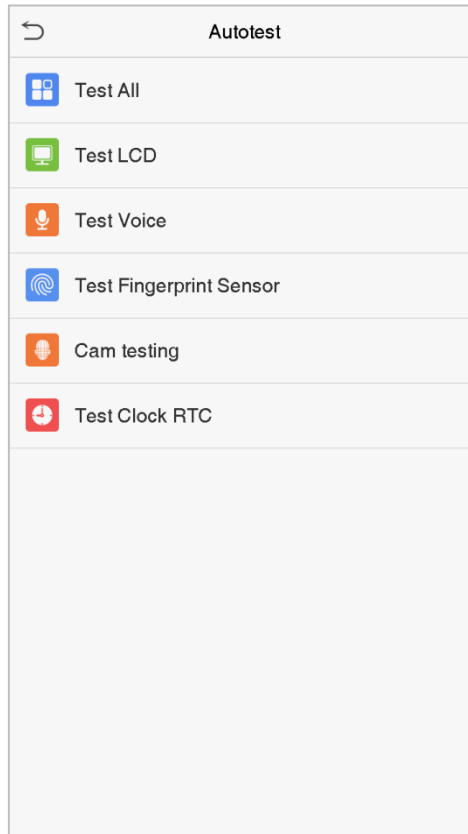
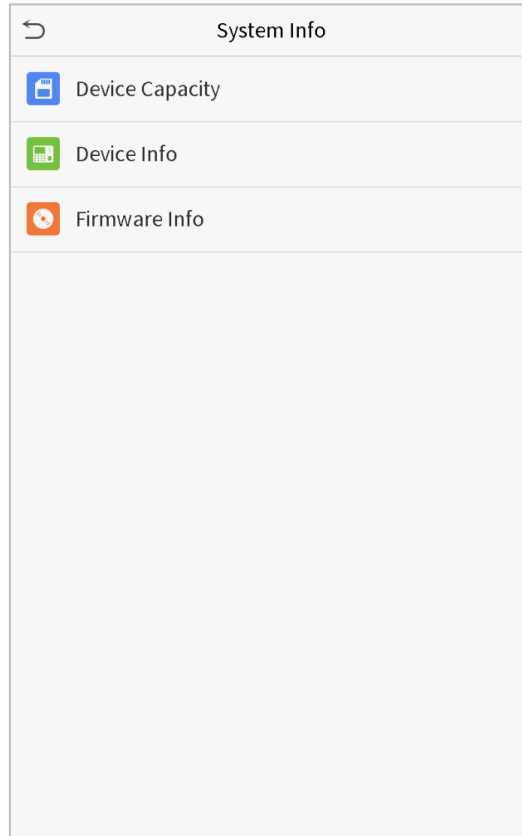| Item	Description
Test All	To automatically test whether the LCD, audio, camera and RTC are normal.
Test LCD	To automatically test the display effect of LCD screen by displaying full-color, pure white, and pure black to check whether the screen displays colors normally.
Test Voice	To automatically test whether the audio files stored in the device are complete and the voice quality is good.
Test Fingerprint Sensor★	To test the fingerprint sensor by pressing a finger on the scanner to check if the acquired fingerprint image is clear. When you are pressing a finger on the scanner, the fingerprint image will display on the screen.
Camera testing	To test if the camera functions properly by checking the pictures taken to see if they are clear enough.
Test Clock RTC	To test the RTC. The device tests whether the clock works normally and accurately with a stopwatch. Touch the screen to start counting and press it again to stop counting.

13. System Information

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

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

Item	Description
Device Capacity	Displays the current device's user storage, password, fingerprint★ and face storage, administrators, attendance/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.

14. Connect to ZKBioSecurity Software

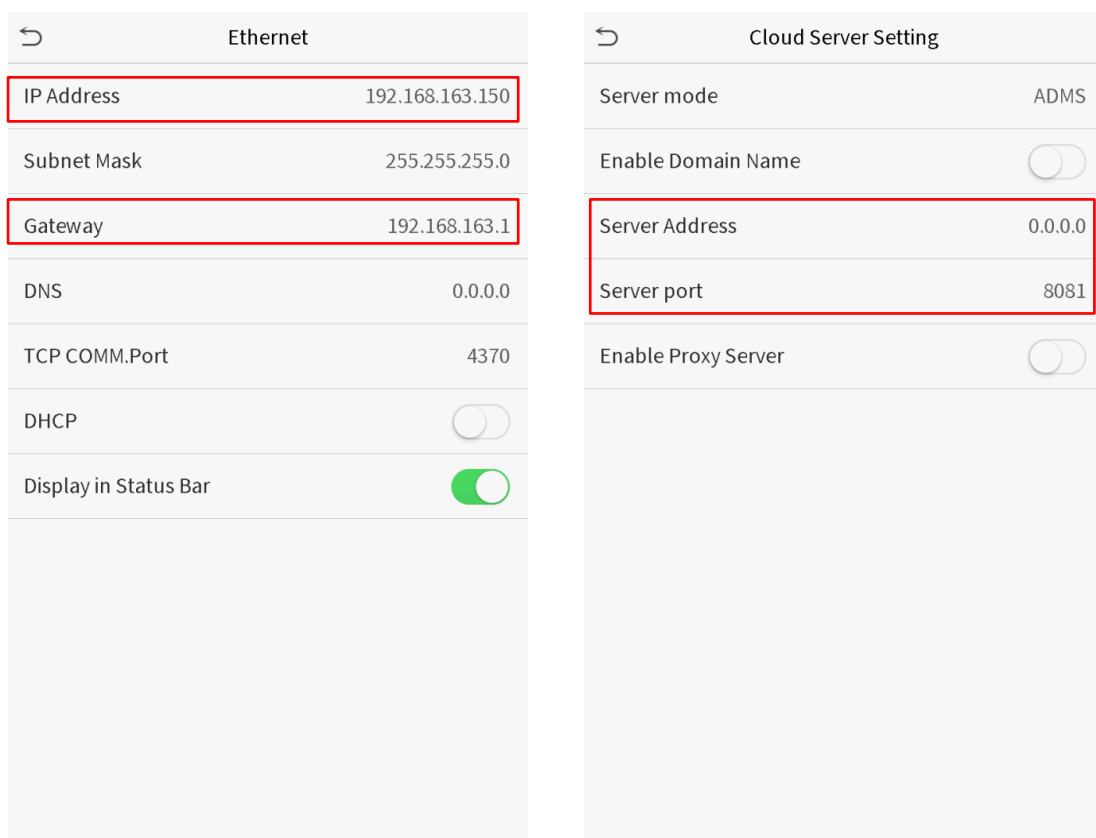## 14.1 Set the Communication Address

➢ **Device side**

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

| Cloud Server Setting	
Server mode	ADMS
Enable Domain Name	
Server Address	0.0.0.0
Server port	8081
Enable Proxy Server	

➢ **Software side**

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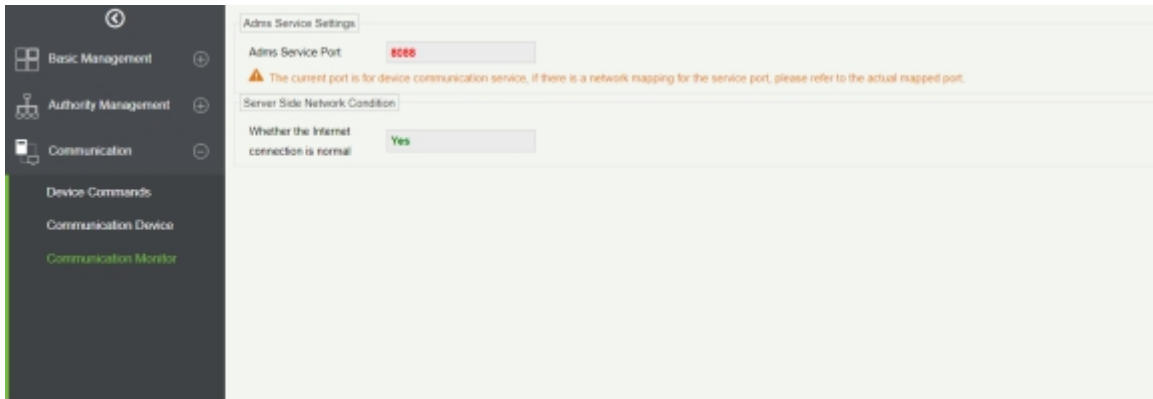
14.2 Add Device on the Software

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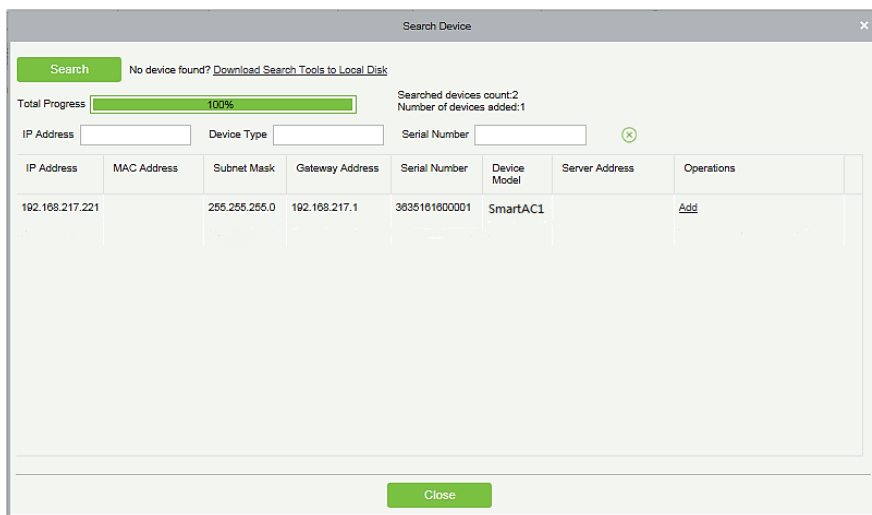
4） Click **Add** after the device to complete adding.

14.3 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 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.

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

Tel: +86 755-89602345

Fax: +86 755-89602394

www.zkteco.com