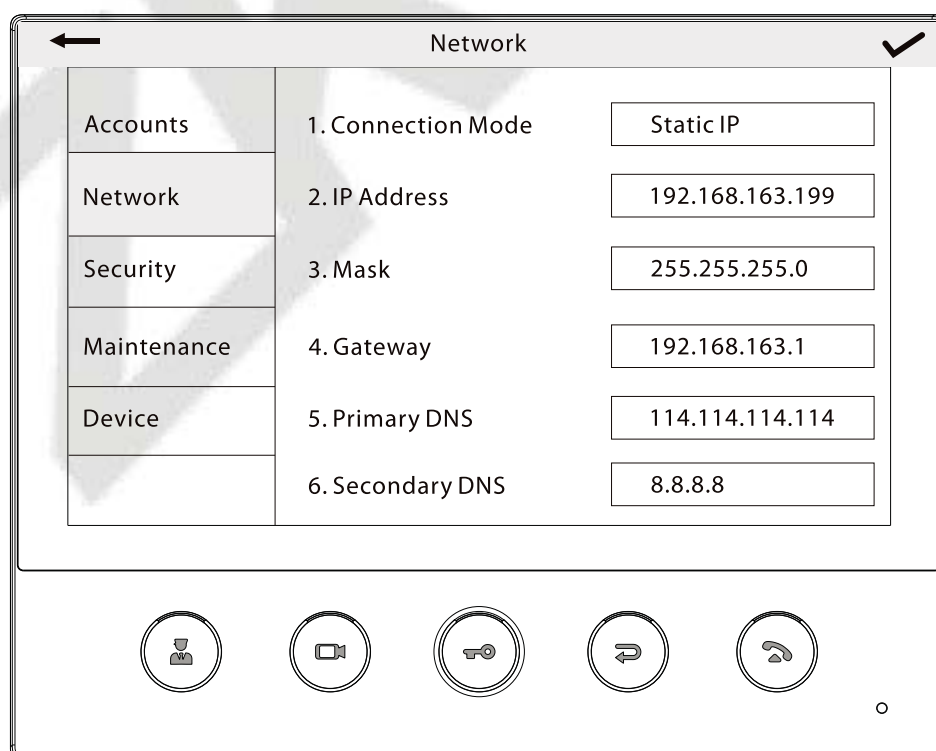


For details on the operation and use of the indoor station, please refer to the **Indoor Station User Manual**.


### 9.1.2 Local Area Network Use

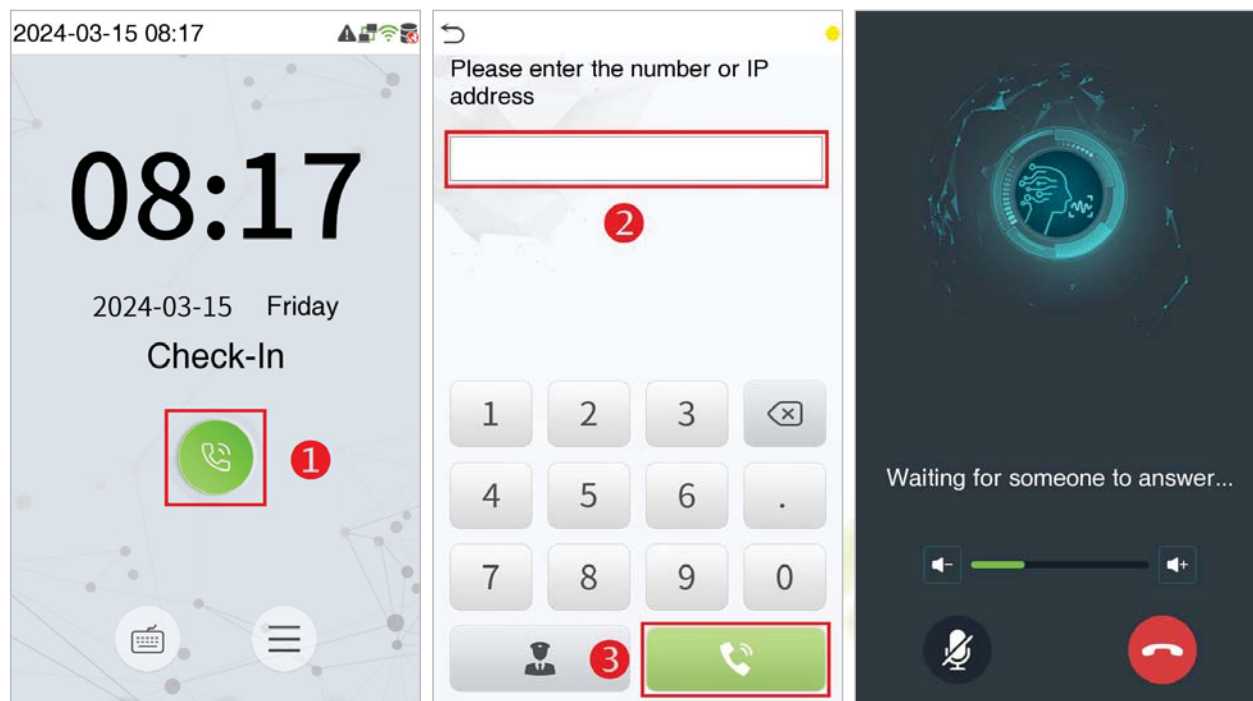
**Note:** To use *Shortcut and Direct Calling Mode*, turn off the SIP Server. When the SIP Server is disabled and the LAN is used, the UDP mode is selected first.

Set the IP address on the indoor station, Tap **Menu > Advanced > Network > 1. Network > 1. IPv4**.



### ● Directly Enter the IP Address of the Indoor Station

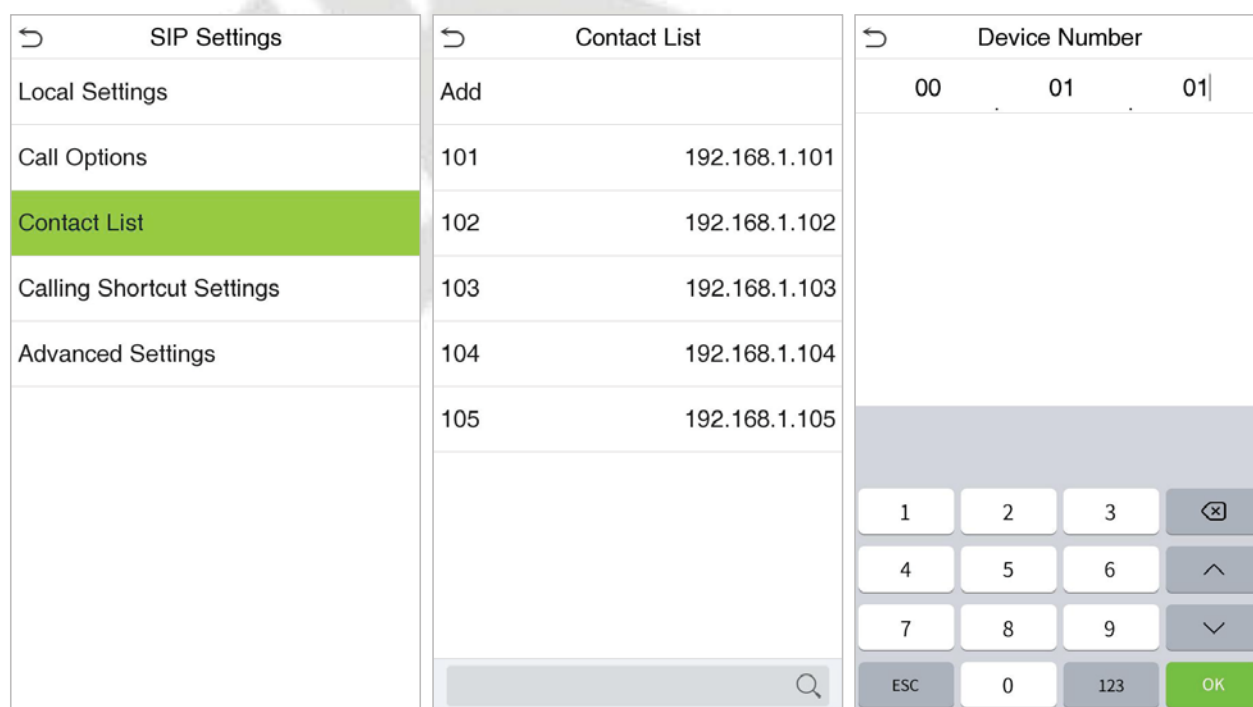
Once the indoor station is configured with the network, the video intercom function can be realized by tap the icon  on the SenseFace 7 Series device screen and entering the IP address of the indoor station in the jumping interface.



### ● Contact List

**Note:** When the SIP server is enabled, the Contact List are not displayed.

1. Tap **SIP Settings > Contact List** on the **Video intercom Parameters** interface.



2. Click **Add**, input device number and call address to add a new contact member.

**Note:** Call address and the SenseFace 7 Series device must be in the same network segment.

↶

Add

Device Number

Call Address

Function Description

Function Name	Description
Device Number	It is the dialing number in the configuration data, you can enter the value on SenseFace 7 Series device to call the indoor station quickly for video intercom. (For example, 101 corresponds to 00.01.01 in the Device Number setting.)
Call Address	The IP address on the indoor station.

9.1.3 Calling Shortcut Settings

1. On SenseFace 7 Series device, tap **Calling Shortcut Settings**, select any item except admin, and enter the form information you just uploaded.

↶

Calling Shortcut Se...

Management Center101

Call ModeStandard Mode

ROOM1Enable

ROOM2Enable

ROOM3Enable

ROOM4Enable

↶

Device Number : 0

Enable☒

NameROOM1

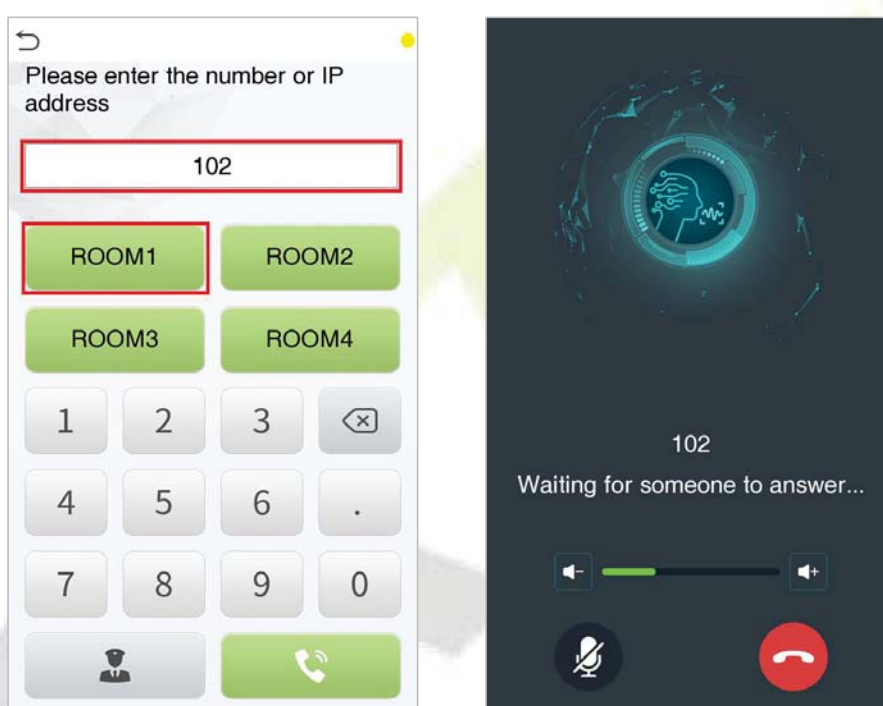
Device Number0

IP Address0.0.0.0

## Function Description

Function Name	Description
<b>Name</b>	You can customize any character (support Chinese, English, numbers, symbols, etc.) that will be displayed on the call page.
<b>Device Number</b>	It is the dialing number in the configuration data, you can enter the value on SenseFace 7 Series device to call the indoor station quickly for video intercom.
<b>IP Address</b>	Enter the device number set in the <b>Contact List</b> , then automatically match the IP address.

- Then you can enter the device number or click shortcut key in the call screen to directly implement the video intercom.

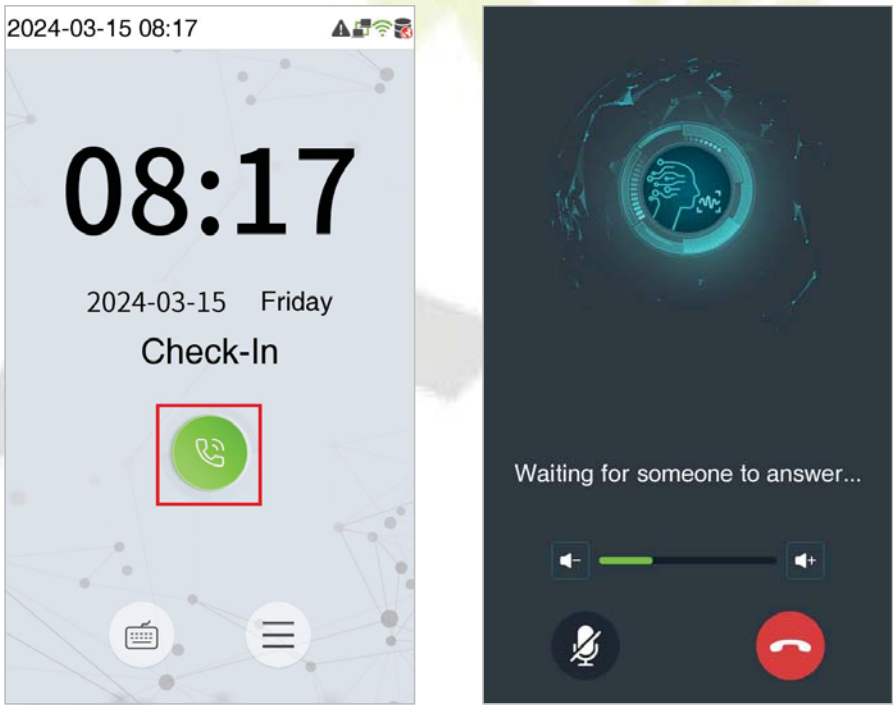


### 9.1.4 Direct Calling Mode

- On the **SIP Settings** interface, click on **Calling Shortcut Settings** > **Call Mode** > **Direct Calling Mode** > **Add**. Select the IP addresses of the indoor stations that you want to call, then the indoor stations will be displayed in the list.

<div><div>← SIP Settings</div><div>Local Settings</div><div>Call Options</div><div>Contact List</div><div>Calling Shortcut Settings</div><div>Advanced Settings</div></div>	<div><div>← Calling Shortcut Se...</div><div>Management Center101</div><div>Call ModeStandard Mode</div><div>ROOM1Enable</div><div>ROOM2Enable</div><div>ROOM3Enable</div><div>ROOM4Enable</div></div>	<div><div>← Calling Shortcut Se...</div><div><div><input checked="" type="radio"/> Standard Mode</div><div><input type="radio"/> Direct Calling Mode</div></div></div>
---	--	--

2. Then you can tap the  icon on the device to call the indoor stations at the same time.









## 9.2 Doorbell Setting

Tap **Doorbell Setting** on the **Video intercom Parameters** interface to go to the monitoring doorbell setting.





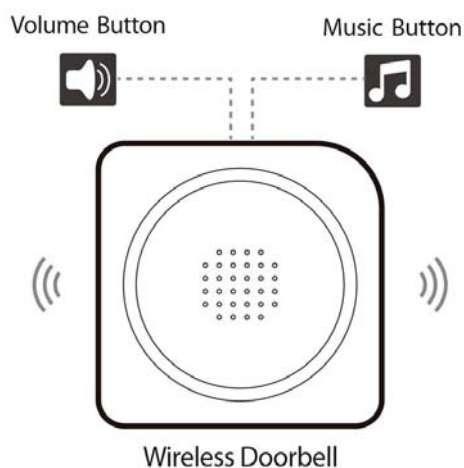
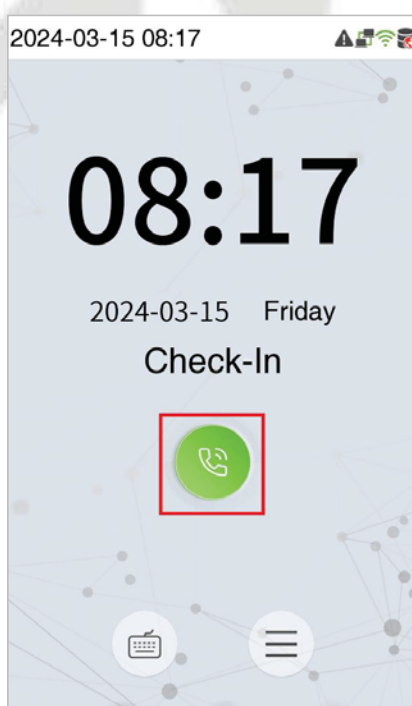
## Function Description


Function Name	Description
<b>Doorbell Only</b>	Tap  or  icon on standby interface, the doorbell ring.
<b>Video Intercom Only</b>	Tap  or  icon on standby interface, calling indoor unit for video intercom.
<b>Doorbell + Video Intercom</b>	Tap  or  icon on standby interface, the doorbell ring and calling indoor unit for video intercom.

### 9.2.1 Connect the Wireless Doorbell ★

**Note:** This function needs to be used with the wireless doorbell.


1. First, power on the wireless doorbell. Then, press and hold the music button  for 1.5 seconds until the indicator flashes to indicate it's in pairing mode. After that, click on the SenseFace 7 Series device icon , if the wireless doorbell rings and the indicator flashes, it means the connection is successful.



- After a successful pairing, clicking the icon  of SenseFace 7 Series device will ring the wireless doorbell.

**Note:** Generally, each SenseFace 7 Series device connects to wireless doorbell.

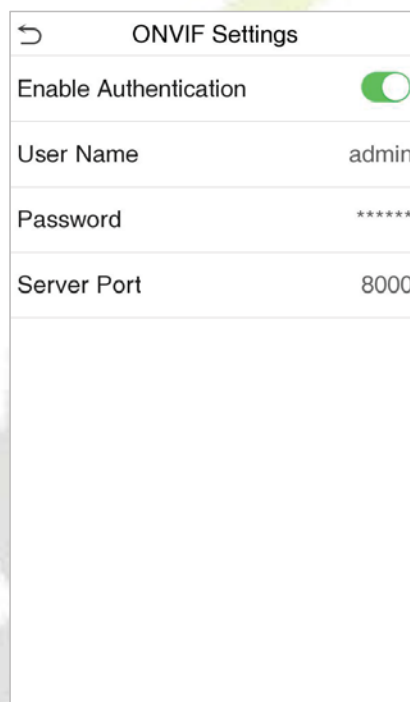
### ● Unbinding the Wireless Doorbell

Power off the wireless doorbell first, then re-installing the batteries while pressing and holding the music button  until the indicator is on, indicating that the unbinding is successful.

## 9.3 ONVIF Settings

**Note:** This function needs to be used with the network video recorder (NVR).

- Set the device to the same network segment as the NVR.
- Tap **ONVIF Settings** on the **Video intercom Parameters** interface.



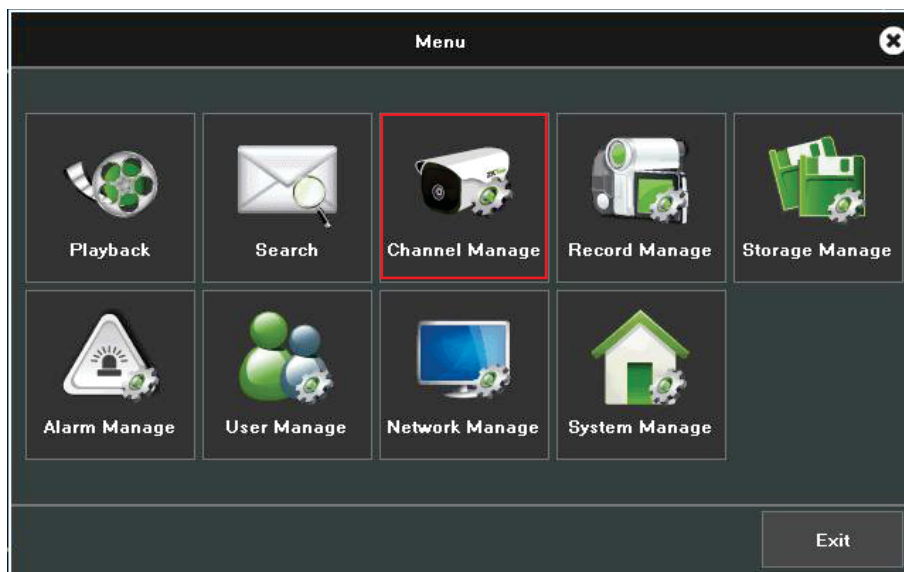
ONVIF Settings	
Enable Authentication	<input checked="" type="checkbox"/>
User Name	admin
Password	*****
Server Port	8000

### Function Description

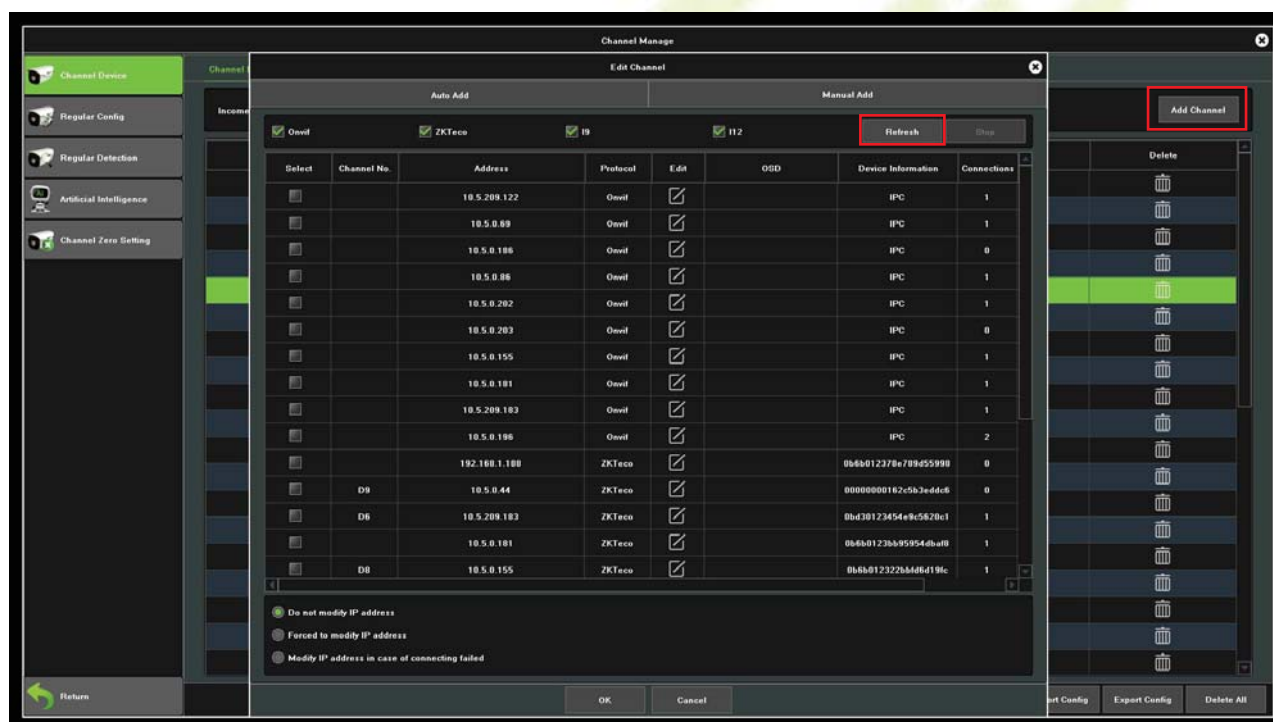
Function Name	Description
<b>Enable Authentication</b>	Enable/Disable the Authentication Function. When it is disabled, there is no need to input the User Name and Password when adding the device to the NVR.
<b>User Name</b>	Set the User Name. The default is admin.
<b>Password</b>	Set the password. The default is admin.
<b>Server Port</b>	The default is 8000, and cannot be modified.



3. On the NVR system, click on **[Start]** > **[Menu]**, then the main menu will pop up.

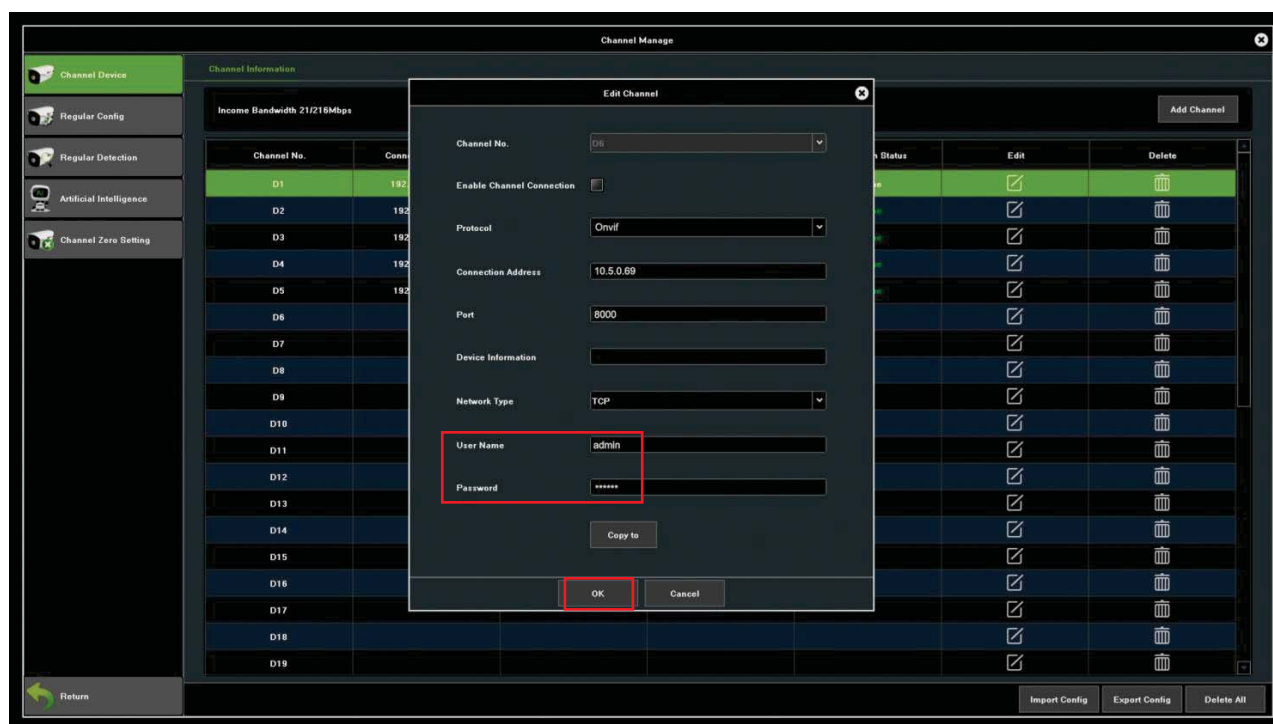


4. Click **[Channel Manage]** > **[Add Channel]** > **[Refresh]** to search for the device.



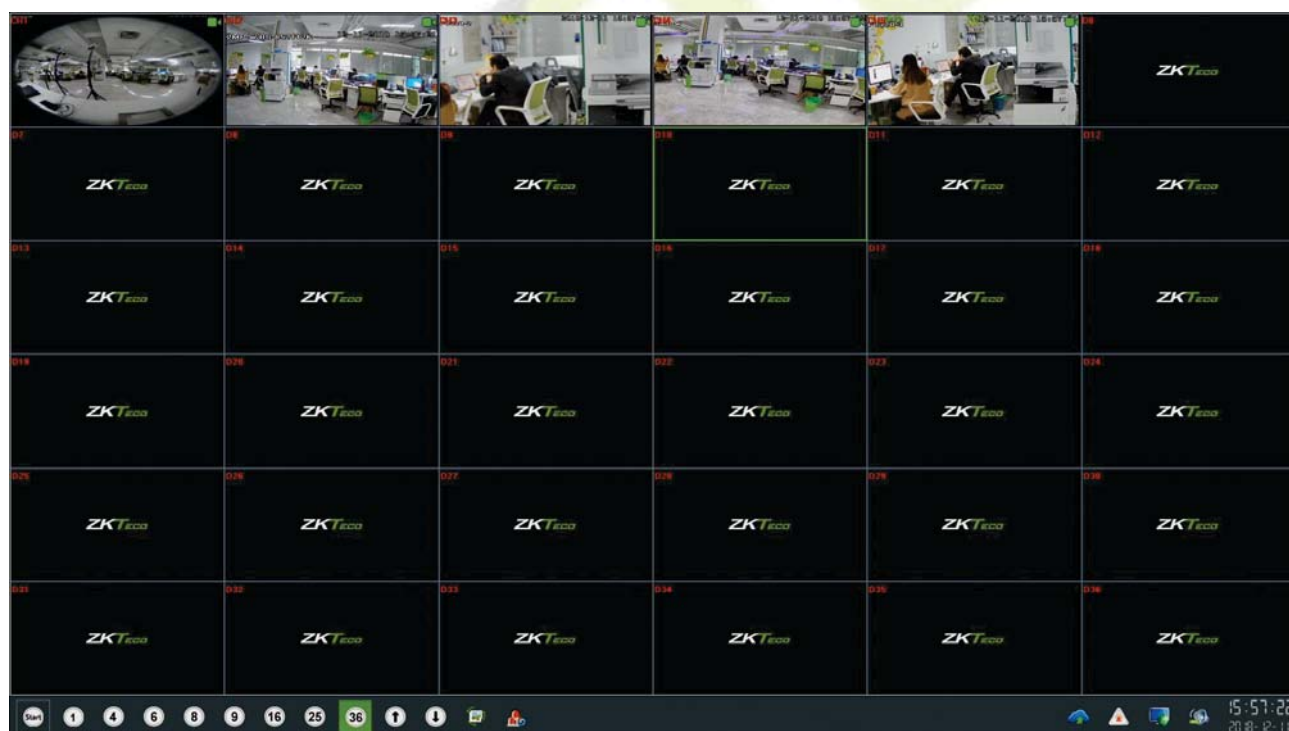
5. Select the checkbox for the device you want to add and edit the parameters in the corresponding text field, then click on **[OK]** to add it to the connection list.





**Note:** The User Name and Password is set in the **ONVIF Settings** of the device.

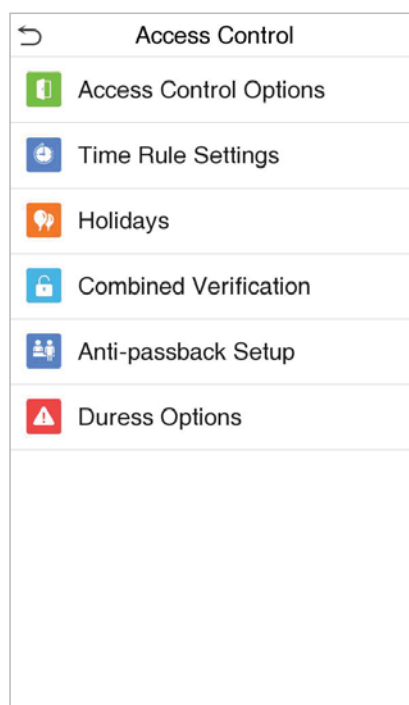
6. After adding successfully, the video image obtaining from the device can be viewed in real-time.



For more details, please refer to the **NVR User Manual**.

## 10. Access Control

On the **Main Menu**, tap **Access Control** to set the schedule of door opening, locks control and to configure other parameters settings related to access control.



- **To gain access, the registered user must meet the following conditions:**
  - The relevant door's current unlock time should be within any valid time zone of the user time period.
  - The corresponding user's group must be already set in the door unlock combination (and if there are other groups, being set in the same access combo, then the verification of those group's members are also required to unlock the door).
  - In default settings, new users are allocated into the first group with the default group time zone, where the access combo is "1" and is set in unlock state by default.

## 10.1 Access Control Options

Tap **Access Control Options** on the **Access Control** interface to set the parameters of the control lock of the terminal and related equipment.

Access Control Opti...	1↓	Access Control Opti...	1↓
Gate Control Mode	<input type="checkbox"/>	Door Sensor Type	Normal Close(NC)
Door Lock Delay(s)	5	Verification Mode	Password/Fingerprint/Card/Face
Door Sensor Delay(s)	10	Door Available Time Period	1
Door Sensor Type	Normal Close(NC)	Normal Open Time Period	None
Verification Mode	Password/Fingerprint/Card/Face	Master Device	In
Door Available Time Period	1	Slave Device	Out
Normal Open Time Period	None	Auxiliary Input Configuration	
Master Device	In	Verify Mode by RS485	Card Only
Slave Device	Out	Speaker Alarm	<input type="checkbox"/>
Auxiliary Input Configuration		Reset Access Settings	

### Function Description

Function Name	Description
<b>Gate Control Mode</b>	Toggle between ON or OFF switch to get into gate control mode or not. When set to <b>ON</b> , on this interface will remove Door lock relay, Door sensor relay and Door sensor type options.
<b>Door Lock Delay (s)</b>	The length of time that the device controls the electric lock to be in unlock state. Valid value: 1~10 seconds; 0 second represents disabling the function.
<b>Door Sensor Delay (s)</b>	If the door is not locked and is being left open for a certain duration (Door Sensor Delay), an alarm will be triggered. The valid value of Door Sensor Delay ranges from 1 to 255 seconds.
<b>Door Sensor Type</b>	There are three Sensor types: <b>None</b> , <b>Normal Open</b> and <b>Normal Closed</b> . <b>None</b> : It means door sensor is not in use. <b>Normal Open</b> : It means the door is always left opened when electric power is on. <b>Normal Closed</b> : It means the door is always left closed when electric power is on.
<b>Verification Mode</b>	The supported verification mode includes Password/Fingerprint/Card/Face, Fingerprint Only, User ID Only, Password, Card Only, Fingerprint/Password, Fingerprint/Card, User ID + Fingerprint, Fingerprint + Password, Fingerprint + Card, Fingerprint + Password + Card, Password + Card, Password/Card, User ID + Fingerprint + Password, Fingerprint + (Card/User ID), Face Only, Face + Fingerprint, Face + Password, Face + Card, Face + Fingerprint+ Card, and Face + Fingerprint + Password.

<b>Door Available Time Period</b>	To set time period for door, so that the door is available only during that period.
<b>Normal Open Time Period</b>	Scheduled time period for "Normal Open" mode, so that the door is always left open during this period.
<b>Master Device</b>	When setting up the master, the status of the master can be set to exit on enter. <b>Out:</b> The record verified on the host is the exit record. <b>In:</b> The record verified on the host is the entry record.
<b>Slave Device</b>	When setting up the slave, the status of the slave can be set to exit on enter. <b>Out:</b> The record verified on the host is the exit record. <b>In:</b> The record verified on the host is the entry record.
<b>Auxiliary Input Configuration</b>	Sets the door unlock time period and auxiliary output type of the auxiliary terminal device. Auxiliary output types include None, Trigger door open, Trigger Alarm, Trigger door open and Alarm.
<b>Verify Mode by RS485</b>	The verification mode is used when the device is used either as a host or slave. The supported verification mode includes Card Only and Card + Password.
<b>Speaker Alarm</b>	Transmits 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.
<b>Reset Access Settings</b>	The access control reset 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.

## 10.2 Time Rule Setting

Tap **Time Rule Setting** on the Access Control interface to configure the time settings.

- The entire system can define up to 50 Time Periods.
- Each Time Period represents **10** Time Zones, i.e. **1** week and **3** holidays, and each time zone is a standard 24 hour period per day and the user can only verify within the valid time period.
- One can set a maximum of 3 time periods for every time zone. The relationship among these time periods is "**OR**". Thus, when the verification time falls in any one of these time periods, the verification is valid.
- The Time Zone format of each Time Period: HH MM-HH MM, which is accurate to minutes according to the 24-hour clock.

Tap the grey box to search the required Time Zone and specify the required Time Zone number (maximum: up to 50 zones).

Time Rule[2/50]	
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...]
Holiday Type 1	[00:00 23:59...]
Holiday Type 2	[00:00 23:59...]

On the selected Time Zone number interface, tap on the required day (that is Monday, Tuesday etc.) to set the time.

Time Period 1

00:00 23:59

▲	▲	▲	▲
00	00	23	59
▼	▼	▼	▼
HH	MM	HH	MM

Confirm (OK) Cancel (ESC)

Specify the start and the end time, and then tap **OK**.

**Notes:**

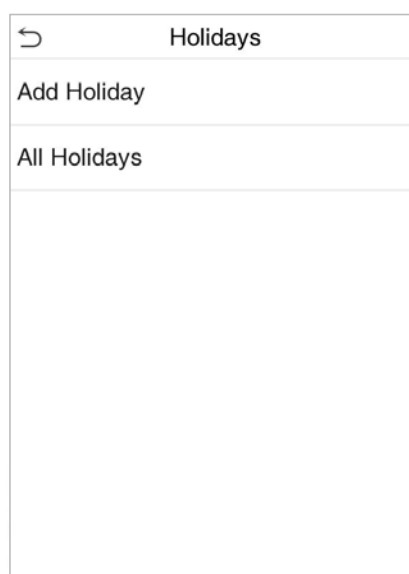
- When the End Time is earlier than the Start Time, (such as 23:57~23:56), it indicates that access is prohibited all day.
- When the End Time is later than the Start Time, (such as 00:00~23:59), it indicates that the interval is valid.

- The effective Time Period to keep the Door Unlock or open all day is (00:00~23:59) or also when the Ending Time is later than the Starting Time, (such as 08:00~23:59).
- The default Time Zone 1 indicates that door is open all day long.

## 10.3 Holidays

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.

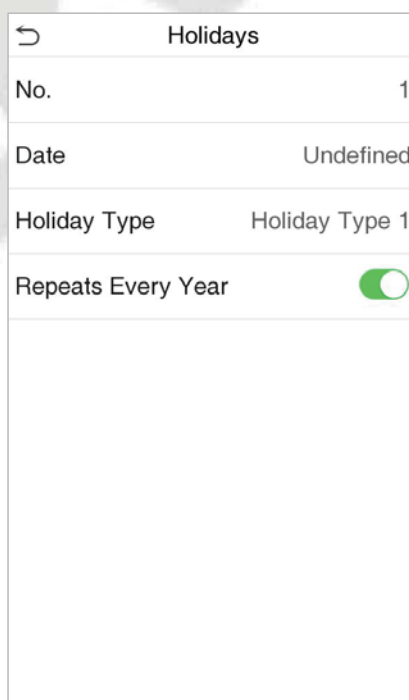
Tap **Holidays** on the **Access Control** interface to set the Holiday access.



Holidays	
Add Holiday	
All Holidays	

### ● Add a new holiday:

Tap **Add Holiday** on the **Holidays** interface and set the holiday parameters.



Holidays	
No.	1
Date	Undefined
Holiday Type	Holiday Type 1
Repeats Every Year	<input checked="" type="checkbox"/>

- **Edit a holiday:**

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

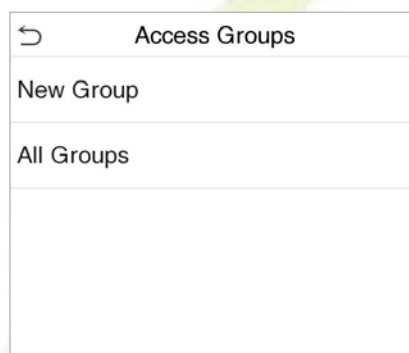
- **Delete a Holiday:**

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

## 10.4 Access Groups ★

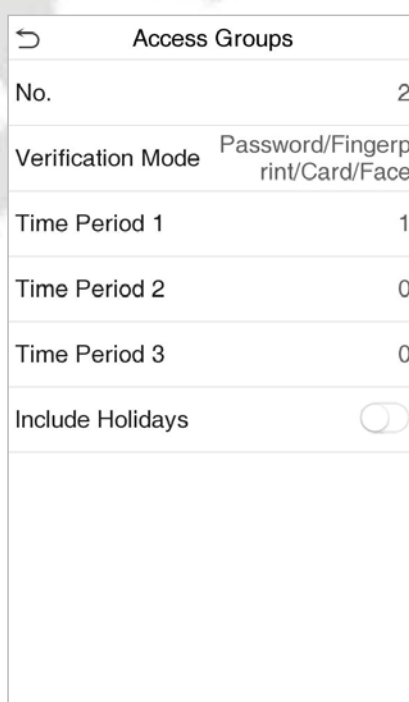
This is to easily manage groupings and users in different access groups. Settings of an access group such as access time zones are applicable to all members in the group by default. However, users may manually set the time zones as needed. User authentication takes precedence over group authentication 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.





**Notes:**

- This function is only used under attendance push (T&A PUSH).
- There is a default access group numbered 1, which cannot be deleted, but can be modified.
- A number cannot be modified after being set.
- 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.

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

## 10.5 Combined Verification

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.

Tap **Combined Verification** on the **Access Control** interface to configure the combined verification setting.

Combined Verification	
1	01 00 00 00 00
2	00 00 00 00 00
3	00 00 00 00 00
4	00 00 00 00 00
5	00 00 00 00 00
6	00 00 00 00 00
7	00 00 00 00 00
8	00 00 00 00 00
9	00 00 00 00 00

On the combined verification interface, tap the Door-unlock combination to be set, and tap the **up** and **down** arrows to input the combination number, and then press **OK**.

**For Example:**

- The **Door-unlock combination 1** is set as **(01 03 05 06 08)**, indicating that the unlock 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-unlock combination 2** is set as **(02 02 04 04 07)**, indicating that the unlock 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-unlock 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-unlock combination 4** is set as **(03 05 08 00 00)**, indicating that the unlock combination 4 consists of only 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.

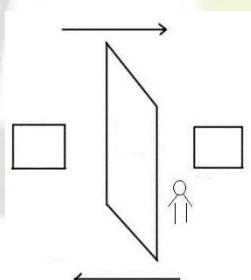
- **Delete a Door-unlocking Combination:**

Set all Door-unlock combinations to 0 if you want to delete door-unlock combinations.

## 10.6 Anti-passback Setup

It is possible that users may be followed by some persons to enter the door without verification, resulting in a security breach. So, to avoid such a situation, the Anti-Passback option was developed. Once it is enabled, the check-in record must match with the check-out record so as to open the door.

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



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

Anti-passback Setup	
Anti-passback Direction	No Anti-passback

## Function Description

Function Name	Description
<b>Anti-passback Direction</b>	<p><b>No Anti-passback:</b> Anti-passback function is disabled, which means successful verification through either the master device or slave device can unlock the door. The attendance state is not saved in this option.</p> <p><b>Out Anti-passback:</b> After a user checks out, only if the last record is a check-in record, the user can check-out again; otherwise, the alarm will be triggered. However, the user can check-in freely.</p> <p><b>In Anti-passback:</b> After a user checks in, only if the last record is a check-out record, the user can check-in again; otherwise, the alarm will be triggered. However, the user can check-out freely.</p> <p><b>In/Out Anti-passback:</b> After a user checks in/out, only if the last record is a check-out record, the user can check-in again; or if it is a check-in record, the user can check-out again; otherwise, the alarm will be triggered.</p>

## 10.7 Duress Options

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

On **Access Control** interface, tap **Duress Options** to configure the duress settings.

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

## Function Description

Function Name	Description
<b>Alarm on Password</b>	When a user uses the password verification method, an alarm signal will be generated, otherwise there will be no alarm signal.

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

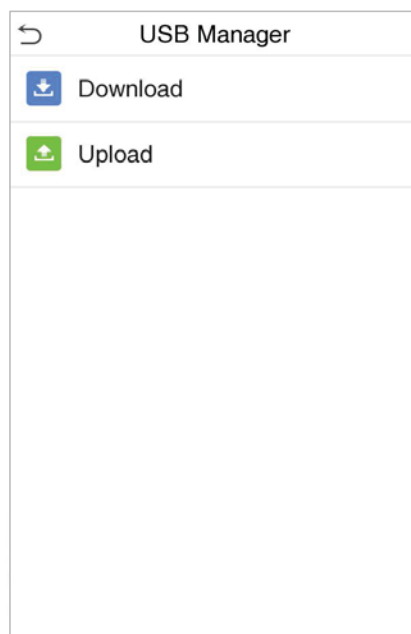
## 11. USB Manager

You can import the user information, and attendance data in the machine to matching attendance software for processing by using a USB disk, or import the user information to other devices for backup.

Before uploading/downloading data from/to the USB disk, insert the USB disk into the USB slot first.

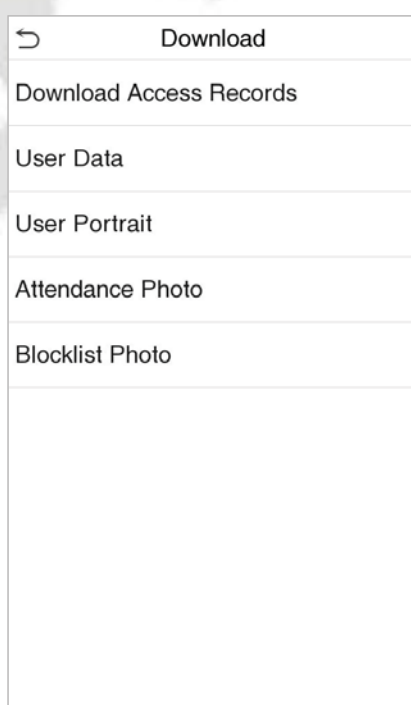
**Note:** Only FAT32 format is supported when downloading data using USB disk.

Tap **USB Manager** on the main menu interface.



### 11.1 USB Download

On the **USB Manager** interface, tap **Download**.

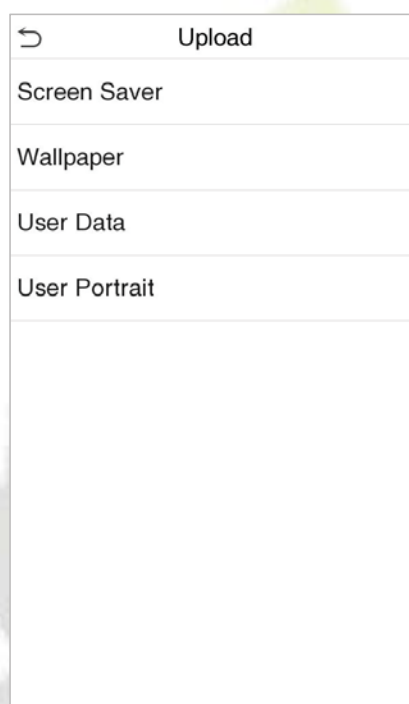


## Function Description

Function Name	Description
<b>Download Access Records</b>	To download all access records in specified time period into USB disk.
<b>User Data</b>	To download all user information from the device into USB disk.
<b>User Portrait</b>	To download all user portraits from the device into USB disk.
<b>Attendance Photo</b>	To download all attendance photos from the device into USB disk.
<b>Blocklist Photo</b>	To download all blocklisted photos (photos taken after failed verifications) from the device into USB disk.

## 11.2 USB Upload

On the **USB Manager** interface, tap **Download**.



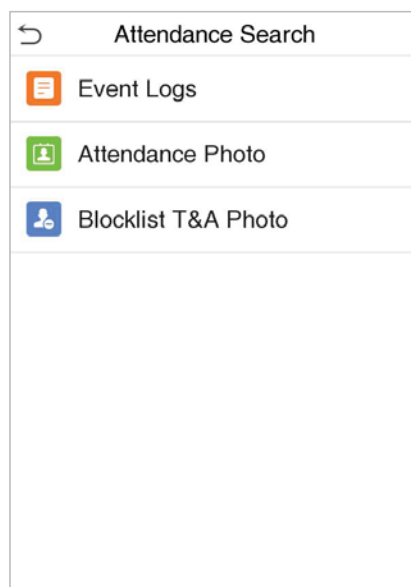
## Function Description

Function Name	Description
<b>Screen Saver</b>	To upload all screen savers from USB disk into the device. You can choose Upload selected photo or upload all photos. The images will be displayed on the device's main interface after upload.
<b>Wallpaper</b>	To upload all wallpapers from USB disk into the device. You can choose Upload selected photo or upload all photos. The images will be displayed on the screen after upload.
<b>User Data</b>	To upload all the user information from USB disk into the device.
<b>User Portrait</b>	To upload all user portraits from USB disk into the device.

## 12. Attendance Search

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

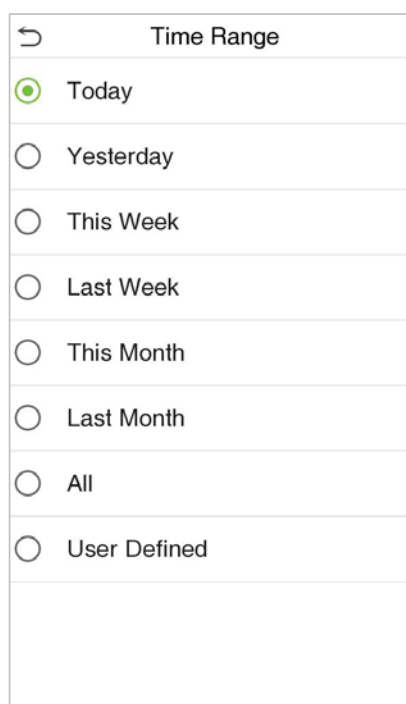
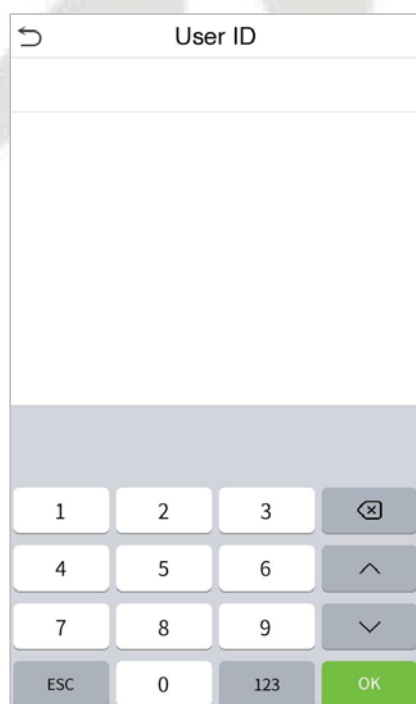
Click **Attendance Search** on the **Main Menu** interface to search for the required Access/Attendance log.



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

On the **Attendance Search** interface, tap **Event Logs** to search for the required record.

1. Enter the user ID to be searched and click OK. If you want to search for logs of all users, click OK without entering any user ID.
2. Select the time range in which the logs need to be searched.





3. Once the log search succeeds. Tap the login highlighted in green to view its details.

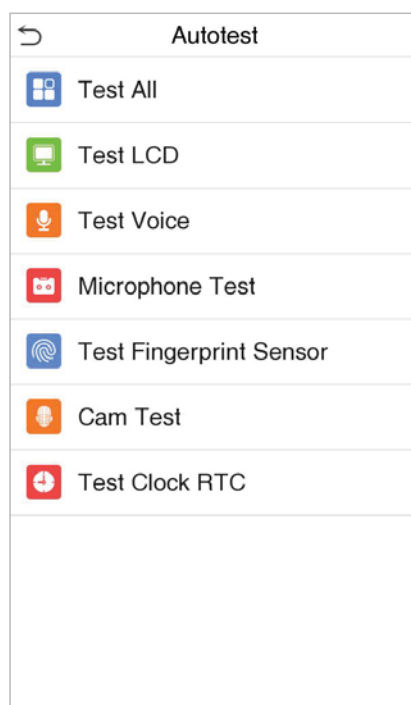
Personal Record S...		
Date	User ID	Time
03-19	Number of Records:7	
	0	09:47 09:47 09:32 09:32
		07:13 07:13 07:13

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

Personal Record S...	
User ID	Time
0	03-19 09:47
0	03-19 09:47
0	03-19 09:32
0	03-19 09:32
0	03-19 07:13
0	03-19 07:13
0	03-19 07:13
Name : Status : Other Verification Mode : Other	

## 13. Autotest

On the **Main Menu**, tap **Autotest** to automatically test whether all modules in the device function properly, which include the LCD, Voice, Camera and Real-Time Clock (RTC).

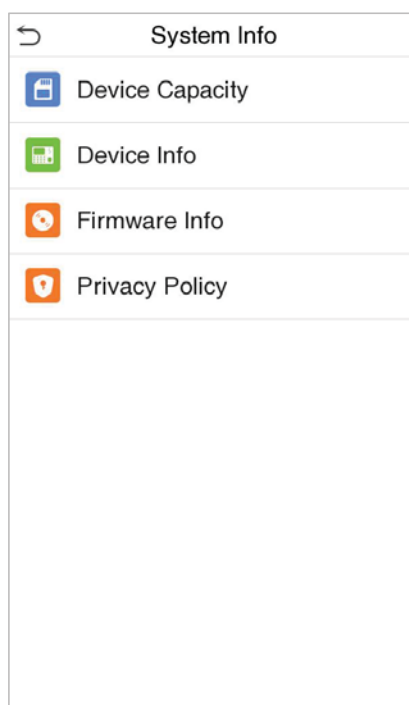


### Function Description

Function Name	Description
<b>Test All</b>	To automatically test whether the LCD, Audio, Camera and RTC are normal.
<b>Test LCD</b>	To automatically test the display effect of LCD screen by displaying full-color, pure white, and pure black to check whether the screen displays colors normally.
<b>Test Voice</b>	To automatically test whether the audio files stored in the device are complete and the voice quality is good.
<b>Microphone Test</b>	Check whether the microphone is working by speaking to microphone and playing the microphone recording.
<b>Test Fingerprint Sensor</b>	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.
<b>Cam Test</b>	To test if the camera functions properly by checking the photos taken to see if they are clear enough. Same as " <b>Test Face</b> ".
<b>Test Clock RTC</b>	To test the RTC. The device tests whether the clock works normally and accurately with a stopwatch. Tap the screen to start counting and press it again to stop counting.

## 14. System Information

On the **Main Menu**, tap **System Info** to view the storage status, the version information of the device, and firmware information.



### Function Description

Function Name	Description
<b>Device Capacity</b>	Displays the current device's user storage, password, face template, fingerprint and card storage, access records, attendance and blocklist photos, and profile photos.
<b>Device Info</b>	Displays the device's name, serial number, MAC address, fingerprint algorithm★, face template algorithm, platform information, MCU Version and manufacture date.
<b>Firmware Info</b>	Displays the firmware version and other version information of the device.
<b>Privacy Policy</b>	<p>The privacy policy control will appear when the gadget turns on for the first time. After clicking "<b>I have read it</b>," the customer can use the product regularly. Click <b>System Info &gt; Privacy Policy</b> to view the content of the privacy policy. The privacy policy's content does not allow for U disc export.</p> <p><b>Note:</b> The current privacy policy's text is only available in Simplified Chinese/ English. However, translation of other multi-language content is underway, with more iterations.</p>

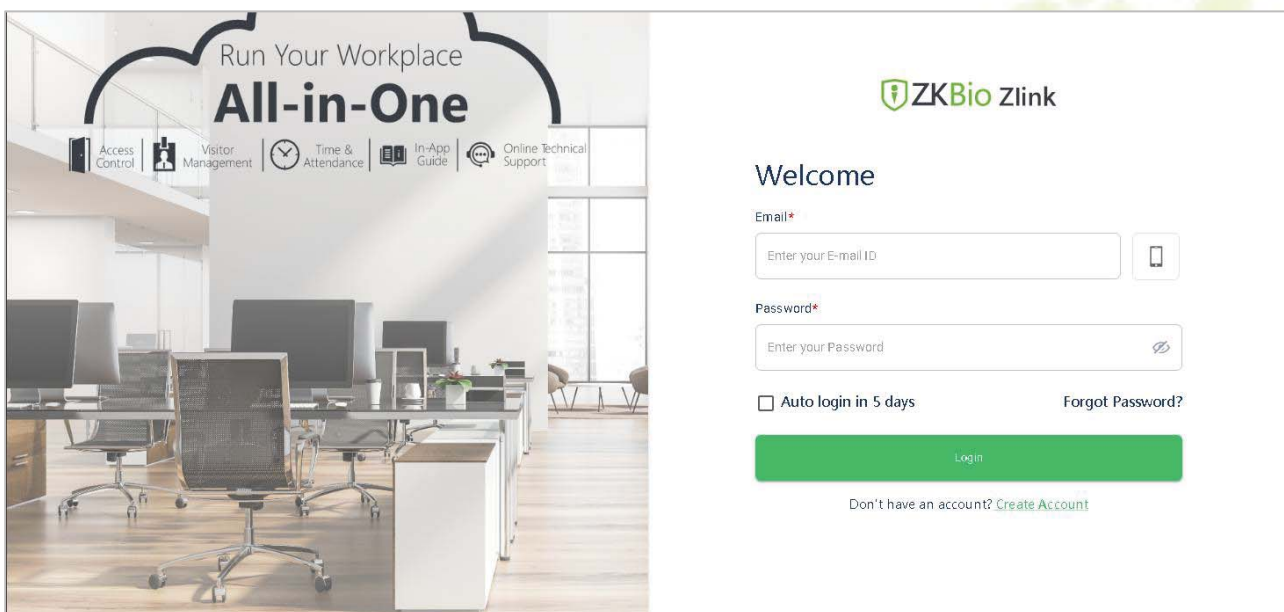
## 15. Connecting to ZKBio Zlink Web

Change the device communication protocol to BEST protocol, then the device can be managed by ZKBio Zlink, please refer to [6.5 Device Type Setting](#).

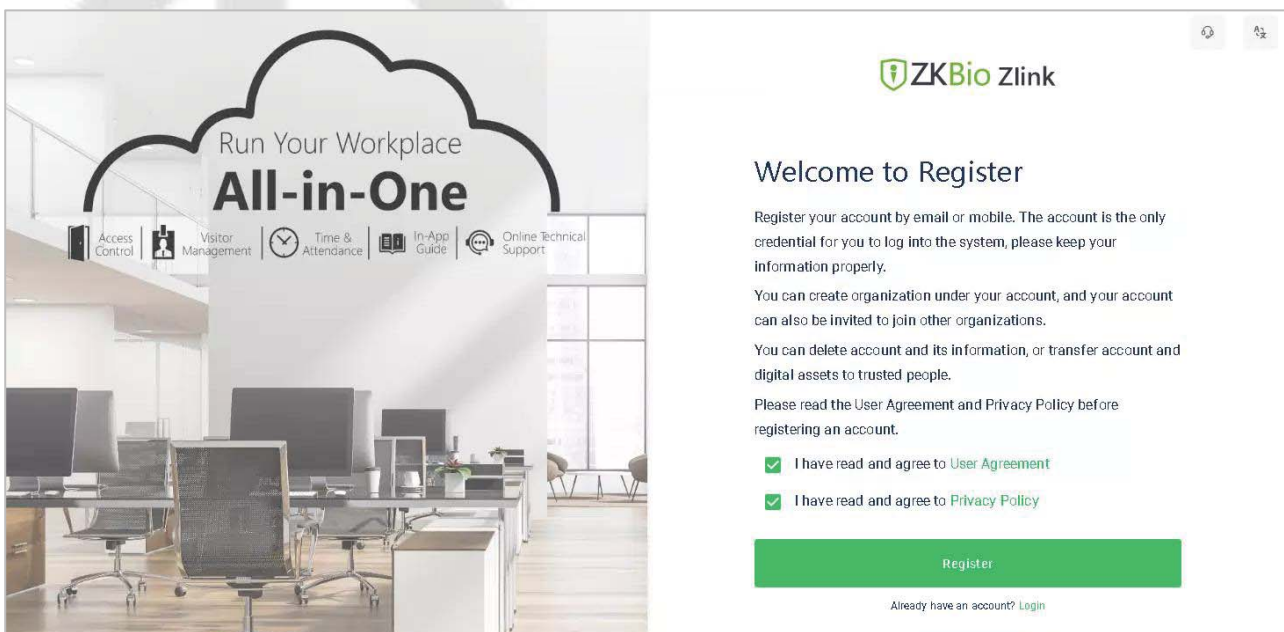
Users can use the created account to access ZKBio Zlink Web to connect devices, add new personnel, register the verification method of registered personnel, synchronize personnel to devices and query records.

### 15.1 Register Account

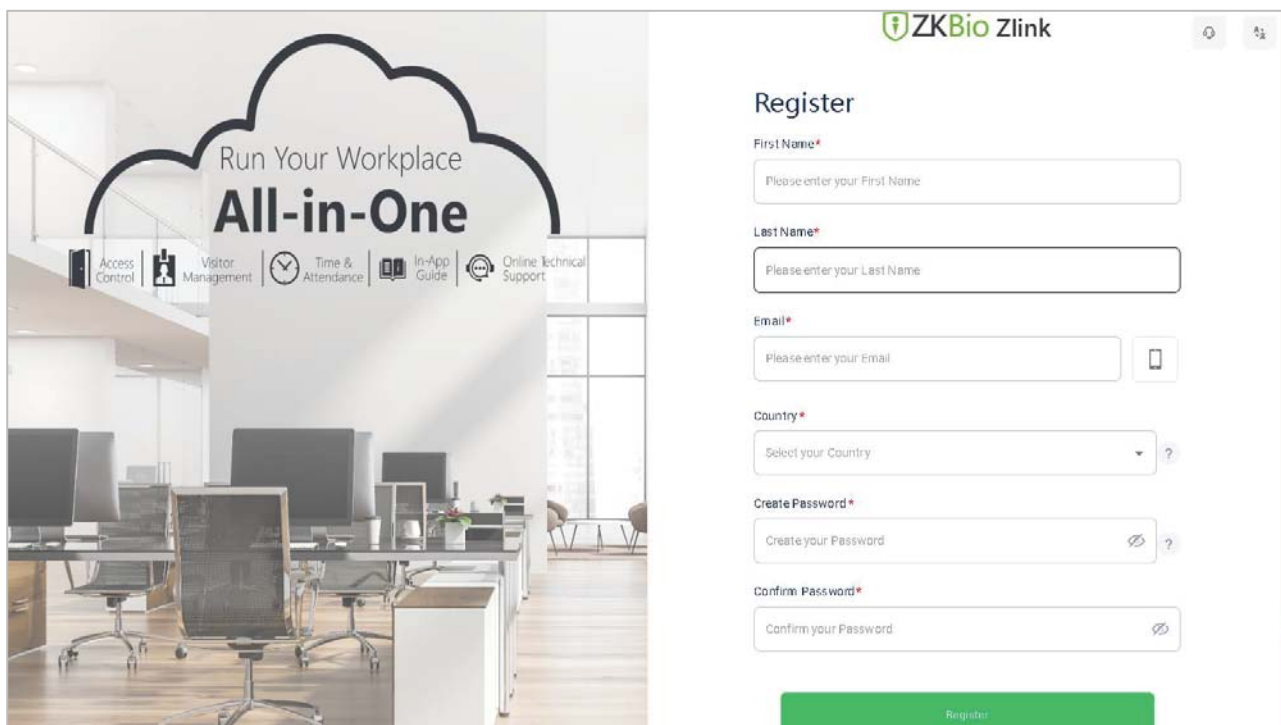
1. Access the ZKBio Zlink website (<http://zlink.minervaiot.com>).
2. If you do not have an account, please click **create account** to add a new account.



3. Read and agree to User Agreement and Privacy Policy, then click **Register**.



4. Enter user's information and set password, then click **Register**.



**ZKBio Zlink**

### Register

First Name\*  
Please enter your First Name

Last Name\*  
Please enter your Last Name

Email\*  
Please enter your Email

Country\*  
Select your Country

Create Password\*  
Create your Password

Confirm Password\*  
Confirm your Password

Register

5. Set the organization's name and Organization code, click **Create**, then complete registration. If you do have an organization, please click **Select an Organization**.



**ZKBio Zlink**

### Create Organization

Organization Name\*  
Please enter your Organization Name

Organization Code\*  
Please enter your Organization Code

Create

Already have an Organization? [Select an Organization](#)

[Back to Login](#)

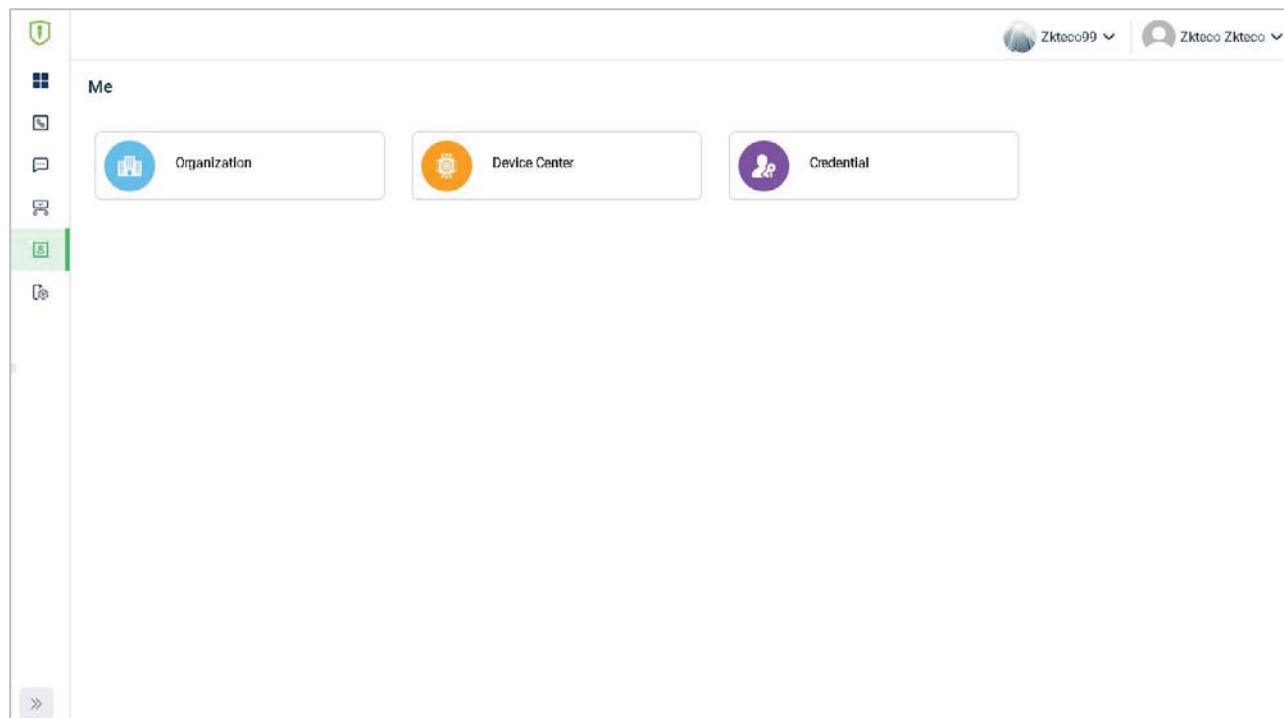
\*Functions will be limited subject to region, please contact support team for details


Powered by MINERVAULT

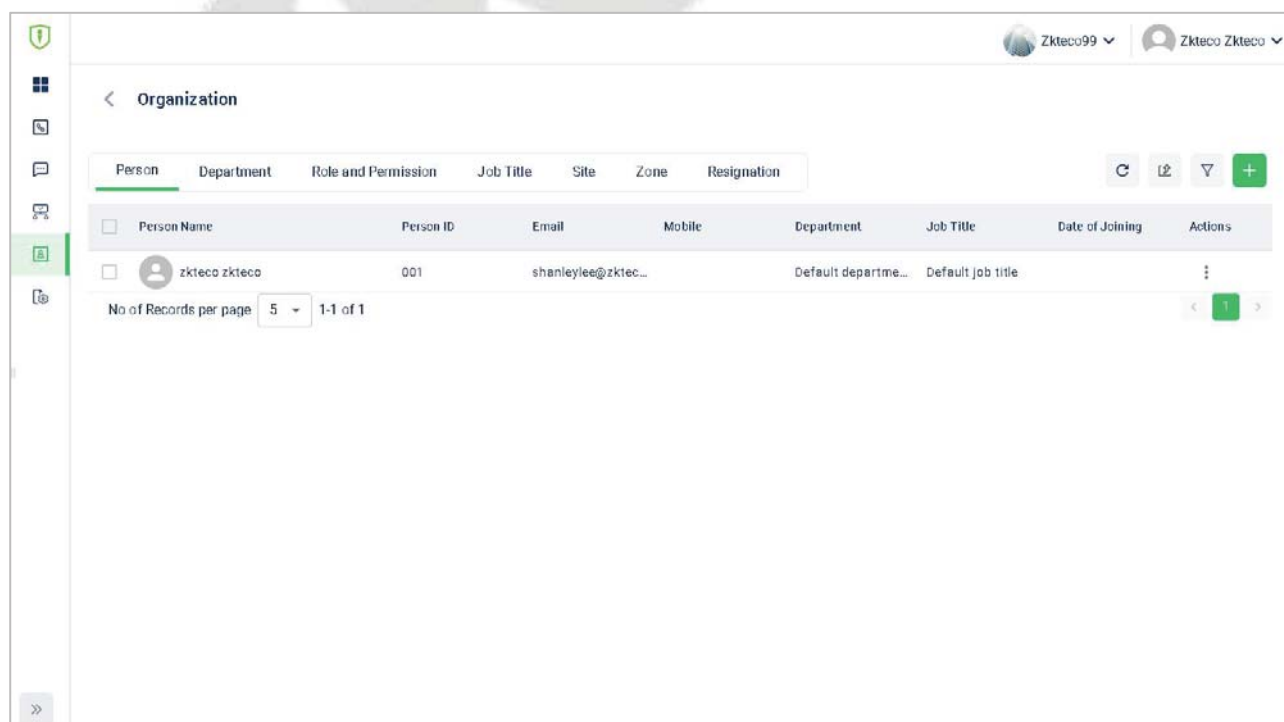
## 15.2 Add Device

### 15.2.1 Set Organization (Add Person)

1. Click **Me > Organization** on the main menu.



2. Click **Add** icon  to add a new person (Repeat adding the department, role and permission, job title, site list, and zone list).



- Enter the person's details and click **Save** (Repeat adding the department, role and permission, job title, site list, and zone list).

**Add Person Details**

Allowed only \*.JPG, \*.JPG, \*.PNG  
Maximum size of 2 MB

First Name\*  
Enter your First Name

Last Name\*  
Enter your Last Name

Person ID\*  
Enter your Person ID

Email\*  
Enter your Email

Mobile\*  
Country Code: Enter your Mobile Number

Role and Permission  
Role and Permission

Department  
Select your Department

Job Title  
Select your Job Title

Date of Joining  
DD-MM-YYYY (Please select Date)

Date of Birth  
DD-MM-YYYY (Please select Date)

Gender  
Select your Gender

Country\*  
Select your Country

Province/State  
Enter your Province/State

City\*  
Enter your City

Address Line 1\*  
Enter your Address

Address Line 2  
Enter your Address

## 15.2.2 Add Device

- Tap **COMM. > Ethernet** in the main menu on the device to set the IP address and gateway of the device.

**Ethernet**

Display in Status Bar ☒

IPv4

IP Address 192.168.163.199

Subnet Mask 255.255.255.0

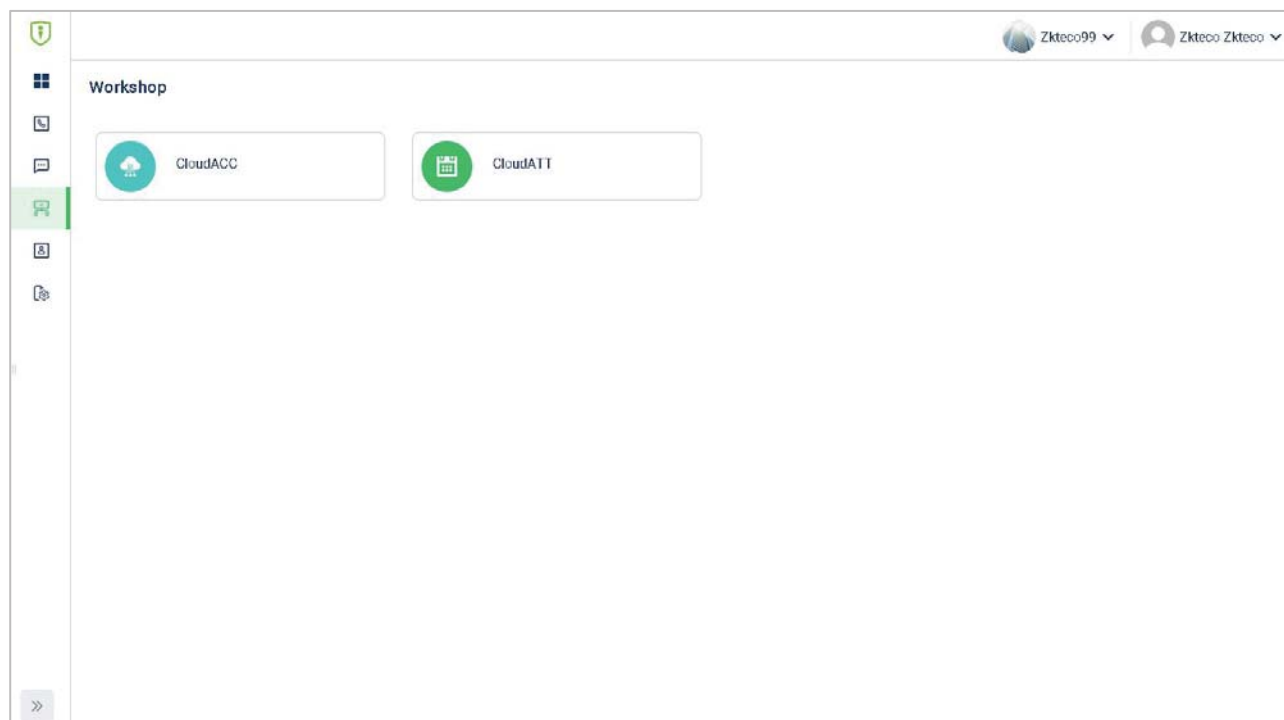
Gateway 192.168.163.1

DNS 0.0.0.0

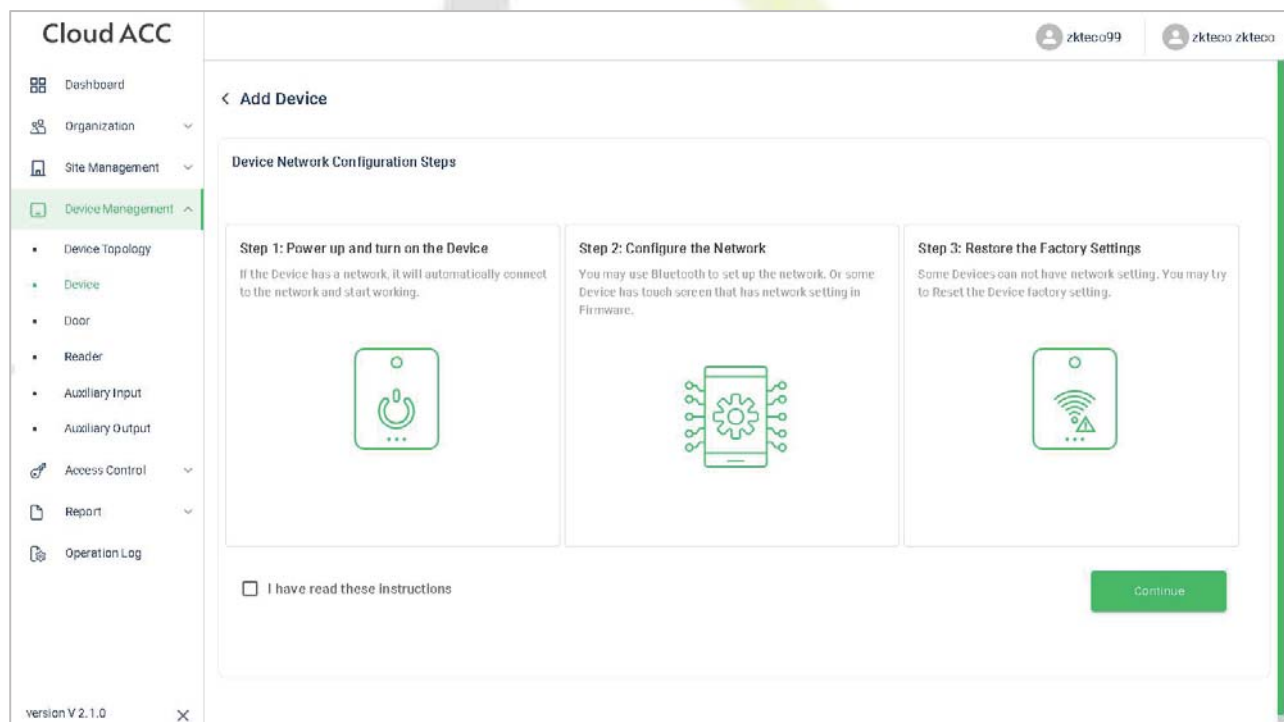
DHCP ☐



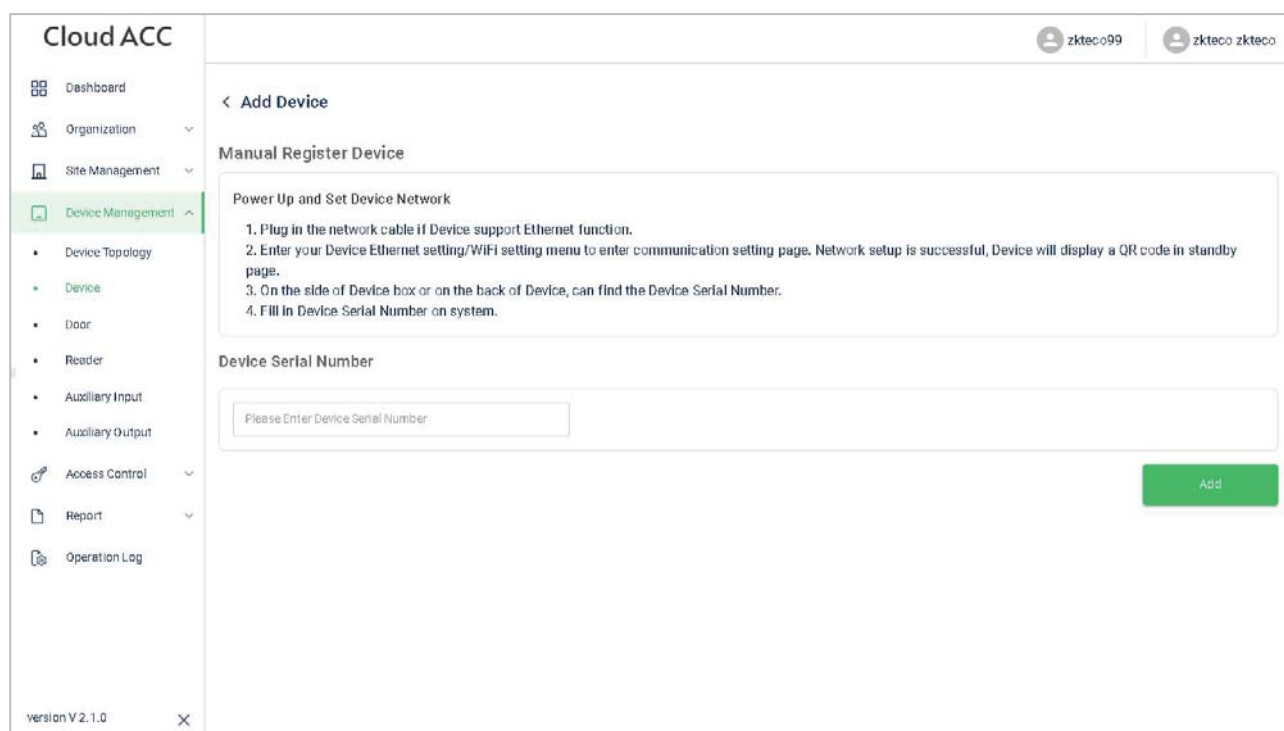
- Click **Workshop > CloudACC** on the main menu to enter the **ZKBio Cloud Access** interface.



- Click **Device Management > Device** to enter the **Device** interface in the **ZKBio Cloud Access**
- Click **+Add Device** button to add a new device.
- Read and check to the instructions, then click **Continue**.

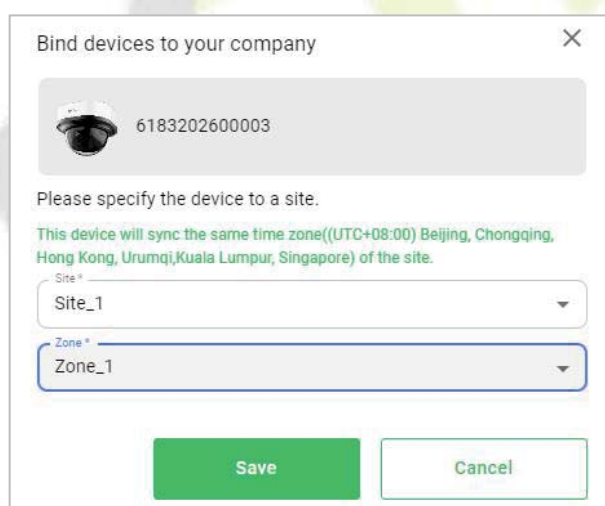


6. Enter the device's serial number, then click **Add**. (Click **System Info > Device Info** on the device to view the serial number)



The screenshot shows the 'Cloud ACC' web interface. On the left is a sidebar menu with options: Dashboard, Organization, Site Management, Device Management (highlighted), Device Topology, Device, Door, Reader, Auxiliary Input, Auxiliary Output, Access Control, Report, and Operation Log. The main content area is titled '< Add Device' and 'Manual Register Device'. It contains a section 'Power Up and Set Device Network' with four numbered instructions: 1. Plug in the network cable if Device support Ethernet function. 2. Enter your Device Ethernet setting/WiFi setting menu to enter communication setting page. Network setup is successful, Device will display a QR code in standby page. 3. On the side of Device box or on the back of Device, can find the Device Serial Number. 4. Fill in Device Serial Number on system. Below this is a 'Device Serial Number' section with a text input field labeled 'Please Enter Device Serial Number' and a green 'Add' button.

7. Choose a site and a zone, then click **Save** to finish.



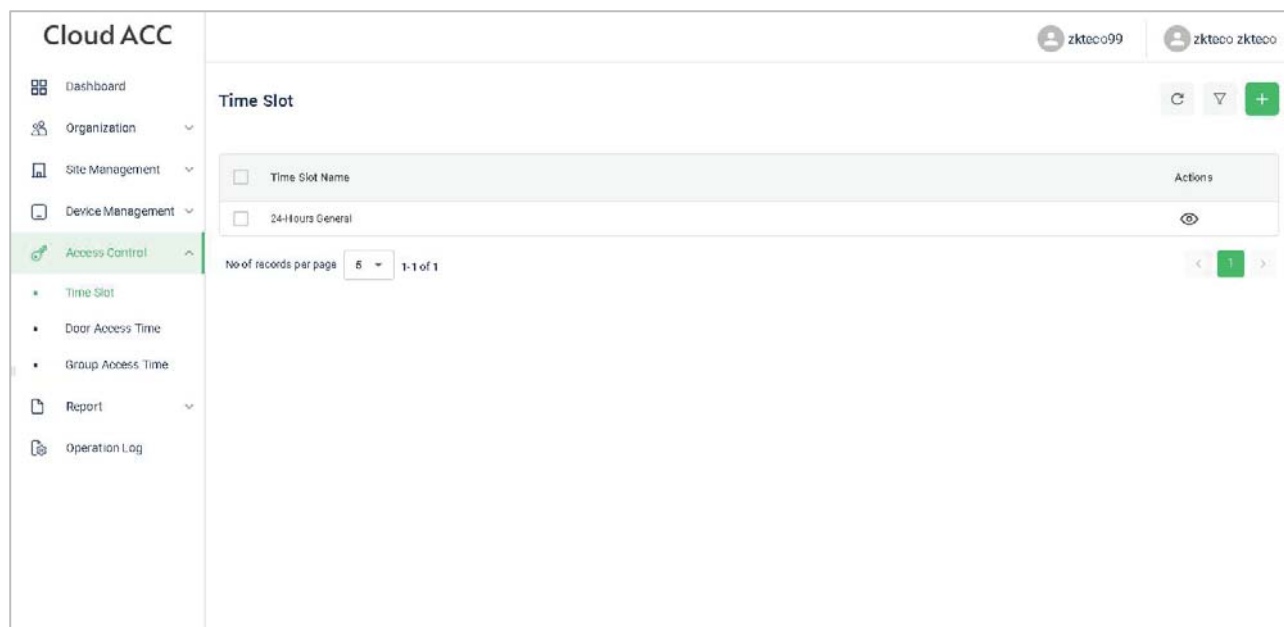
The screenshot shows a dialog box titled 'Bind devices to your company'. It displays a device icon and the serial number '6183202600003'. Below this, it says 'Please specify the device to a site.' and 'This device will sync the same time zone((UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi, Kuala Lumpur, Singapore) of the site.' There are two dropdown menus: 'Site \*' with 'Site\_1' selected, and 'Zone \*' with 'Zone\_1' selected. At the bottom are 'Save' and 'Cancel' buttons.


## 15.3 Time Slot

Time Slot is used to set the access time period for person or doors.

### 15.3.1 Set Time Slot

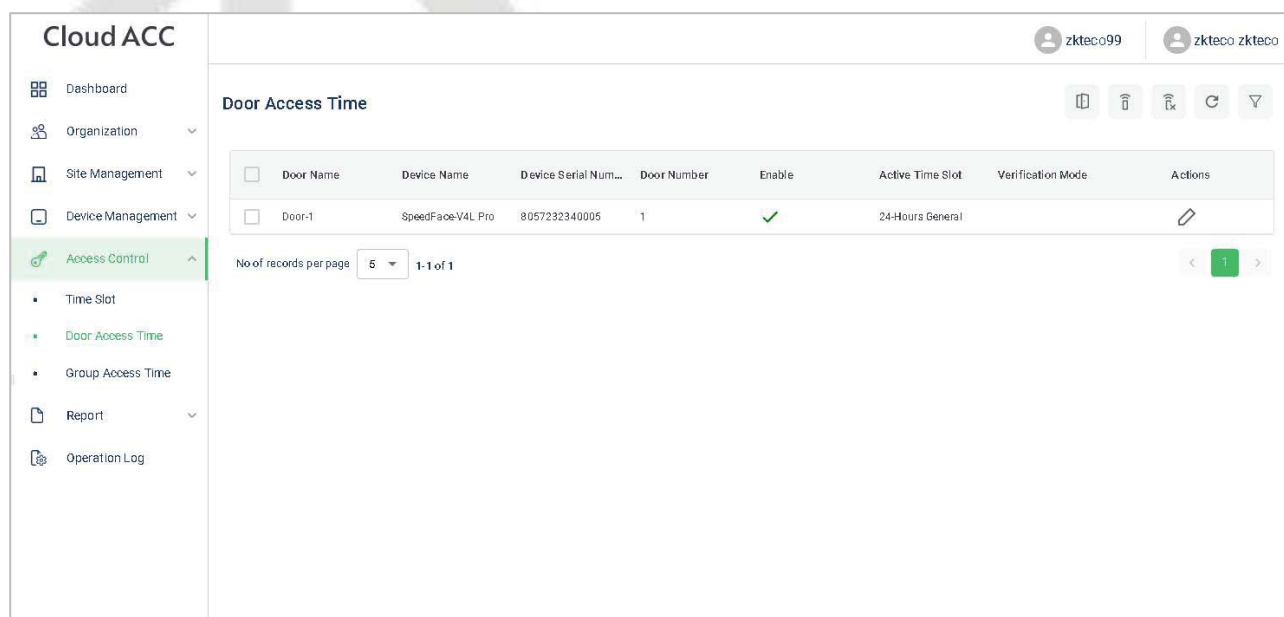
In **ZKBio Cloud Access** interface, click **Access Control > Time Slots** to set time slot.



Click **+Add Time slots** to add a new slot, or click  to modify an existing slot.

### 15.3.2 Set Door Access Time

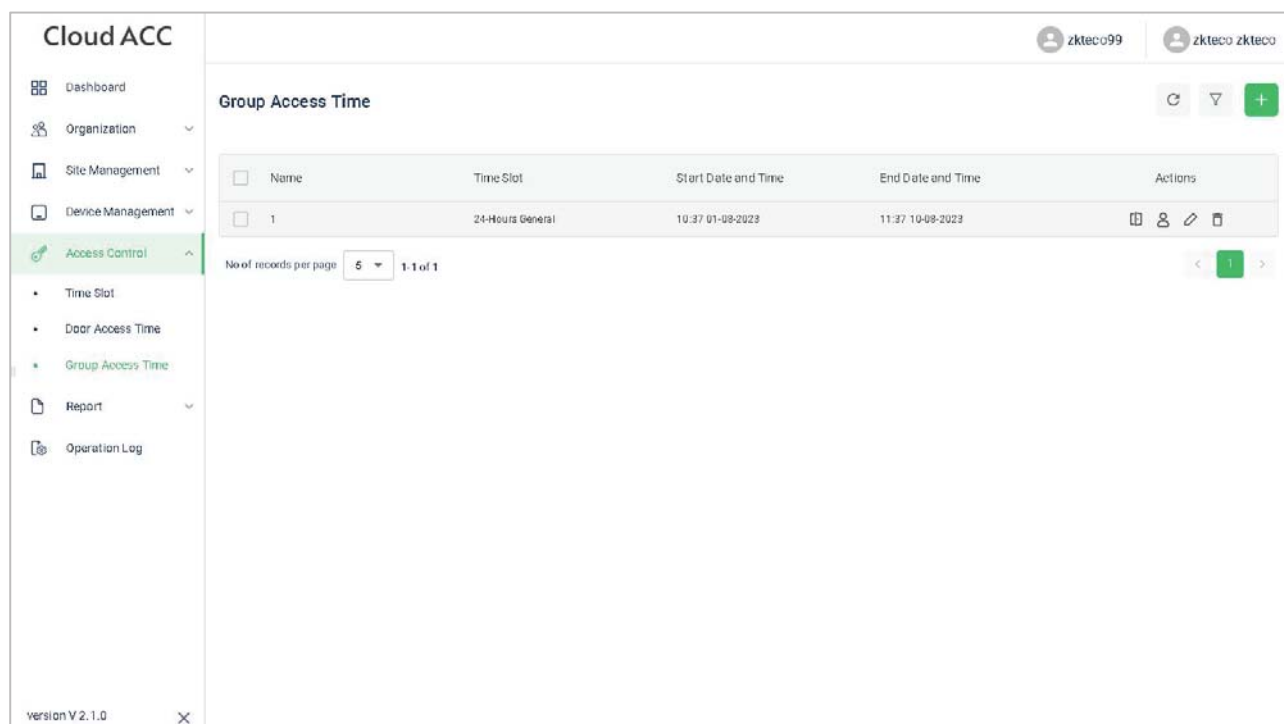
In **ZKBio Cloud Access** interface, click **Access Control > Door Access Time** and click  to allocate a time slot to this door.




### 15.3.3 Set Group Access Time


You can set a group to control the access time of the person and the door at the same time.


In **ZKBio Cloud Access** interface, click **Access Control > Group Access Time**.



Click **+ Add Group Access Time** to add a new group.

Click  to allocate doors to this group.

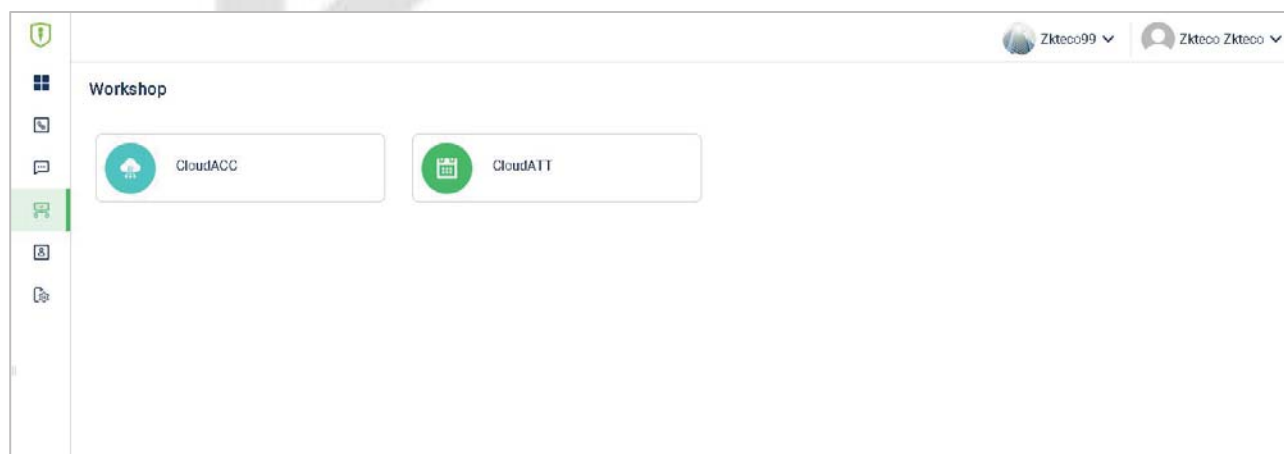
Click  to allocate person to this group.

Click  to allocate a time slot to this group.

Click  to delete this group.

## 15.4 Synchronize Person to Device

1. Click **Workshop > CloudACC** on the main menu to enter the **ZKBio Cloud Access** interface.



## 2. Click **Access Control > Group Access Time**.

**Cloud ACC**

zkteco99 | zkteco zkteco

**Group Access Time**

<input type="checkbox"/>	Name	Time Slot	Start Date and Time	End Date and Time	Actions
<input type="checkbox"/>	1	24-Hours General	10:37 01-08-2023	11:37 10-08-2023	

No of records per page: 5 | 1-1 of 1

## 3. Click > to choose a device.

**Cloud ACC**

zkteco99 | zkteco zkteco

**< Manage Door**

Door Name	Device Name	Device Serial Number	Door Number	Verification Mode	Actions
Door-1	SpeedFace-V4L Pro	8057232340005	1		

No of records per page: 5 | 1-1 of 1

## 4. Click > to allocate person to this device.

**Cloud ACC**

zkteco99 | zkteco zkteco

**< Add Person**

<input type="checkbox"/>	First Name	Last Name	Person ID
<input type="checkbox"/>	Mike	Mike	1
<input type="checkbox"/>	zkteco	zkteco	001

No of records per page: 5 | 1-2 of 2

**Add** **Clear**

5. Click **Device Management** > **Device** to enter the **Device** interface.

The screenshot shows the Cloud ACC web interface. On the left is a sidebar menu with 'Device Management' highlighted. The main content area is titled 'Device' and contains a table of devices. The table has columns for Device Name, Serial Number, IP Address, Device Model, Firmware Version, Status, and Actions. One device is listed: SpeedFace-V4L Pro with status 'Online'. Below the table is a pagination control showing '1' of 1 records.

Device Name	Serial Number	IP Address	Device Model	Firmware Version	Status	Actions
SpeedFace-V4L Pro	8057232340005	192.168.163.175	SpeedFace-V4L Pro	ZAM180-NF4.0VB-Ver3.5.2	Online	[Icons for edit, delete, etc.]

6. Choose a device and click **Persons in the Device** icon to view the person list.

The screenshot shows the 'Person In This Device' view within the Cloud ACC interface. It displays details for the selected device 'SpeedFace-V4L Pro' (Site: 1, Zone: 1). Below this, there is a section titled 'Person & Person Credentials in this Device' which contains a table of person records. The table has columns for Person Name, Person ID, Role, and Person Credentials. One record is shown for 'Mike Mike' with Person ID '1'. The Role is set to 'Select User role'. The Person Credentials column shows various status icons and counts (e.g., 0 for lock, 0 for card, etc.).

Person Name	Person ID	Role	Person Credentials
Mike Mike	1	Select User role	[Icons and counts for various credentials]


## 15.5 User Registration

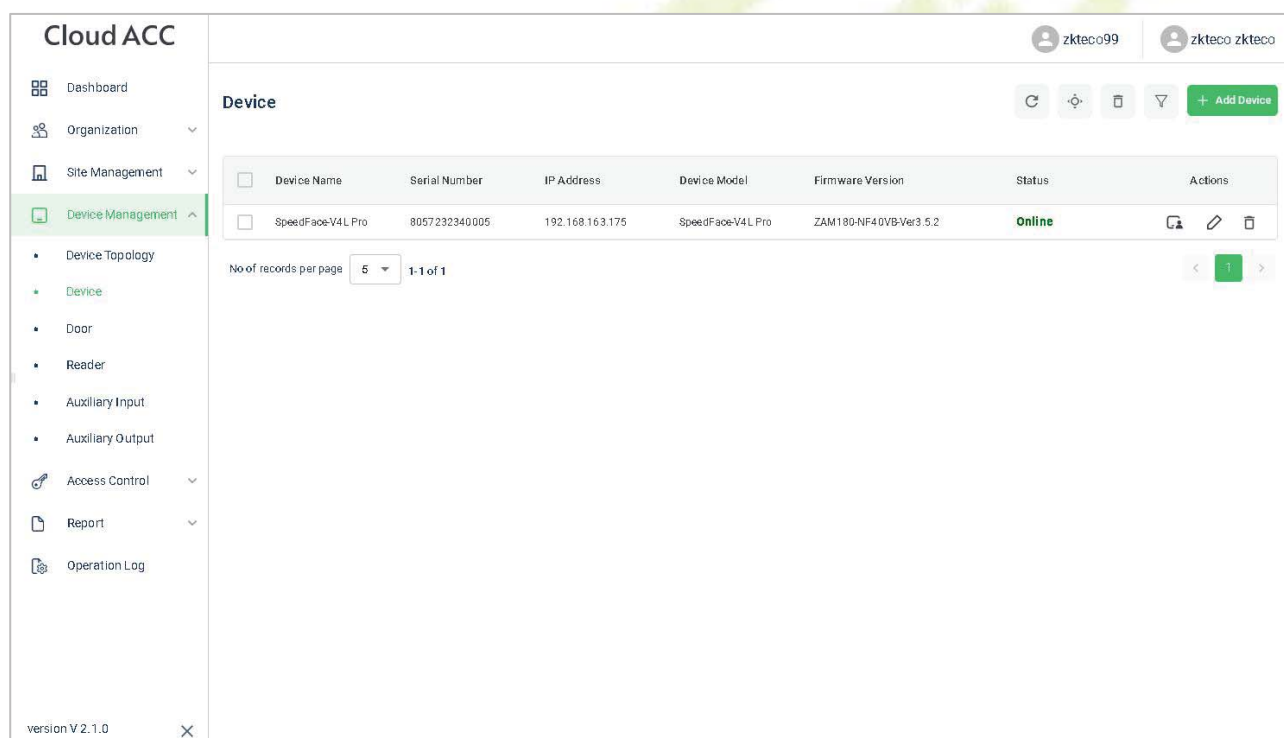
### 15.5.1 Register a User ID and Name

Please refer to the related software user's manual: [14.2.1 Set Organization](#).

### 15.5.2 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.

1. Click **Device Management** > **Device** on **ZKBio Cloud Access** interface to enter the **Device** interface.
2. Choose a device and click **Persons in the Device** icon  to view the person list.



**Cloud ACC**

zkteco99 | zkteco zkteco




**Device Management**

- Dashboard
- Organization
- Site Management
- Device Management**
  - Device Topology
  - Device**
  - Door
  - Reader
  - Auxiliary Input
  - Auxiliary Output
- Access Control
- Report
- Operation Log

version V 2.1.0

**Device**

+ Add Device

<input type="checkbox"/>	Device Name	Serial Number	IP Address	Device Model	Firmware Version	Status	Actions
<input type="checkbox"/>	SpeedFace-V4L Pro	8057232340005	192.168.163.175	SpeedFace-V4L Pro	ZAM180-NF4 0VB-Ver3.5.2	Online	  

No of records per page: 5 | 1-1 of 1



### 3. Choose the **Select User** role.

**Cloud ACC**

Dashboard Organization Site Management **Device Management** Device Topology **Device** Door Reader Auxiliary Input Auxiliary Output Access Control Report Operation Log

version V 2.1.0

**Person In This Device**

SpeedFace-V4L Pro  
Site: 1  
Zone: 1

Person & Person Credentials in this Device ?

Person Name	Person ID	Role	Person Credentials
Mike Mike	1	Select User role	0 0 0 0 0 0 0 0

No of records per page 5 1-1 of 1

## 15.5.3 Register Fingerprint

1. Click **Device Management > Device** on **ZKBio Cloud Access** interface to enter the **Device** interface.
2. Choose a device and click **Persons in the Device** icon to view the person list.

**Cloud ACC**

Dashboard Organization Site Management **Device Management** Device Topology **Device** Door Reader Auxiliary Input Auxiliary Output Access Control Report Operation Log

version V 2.1.0

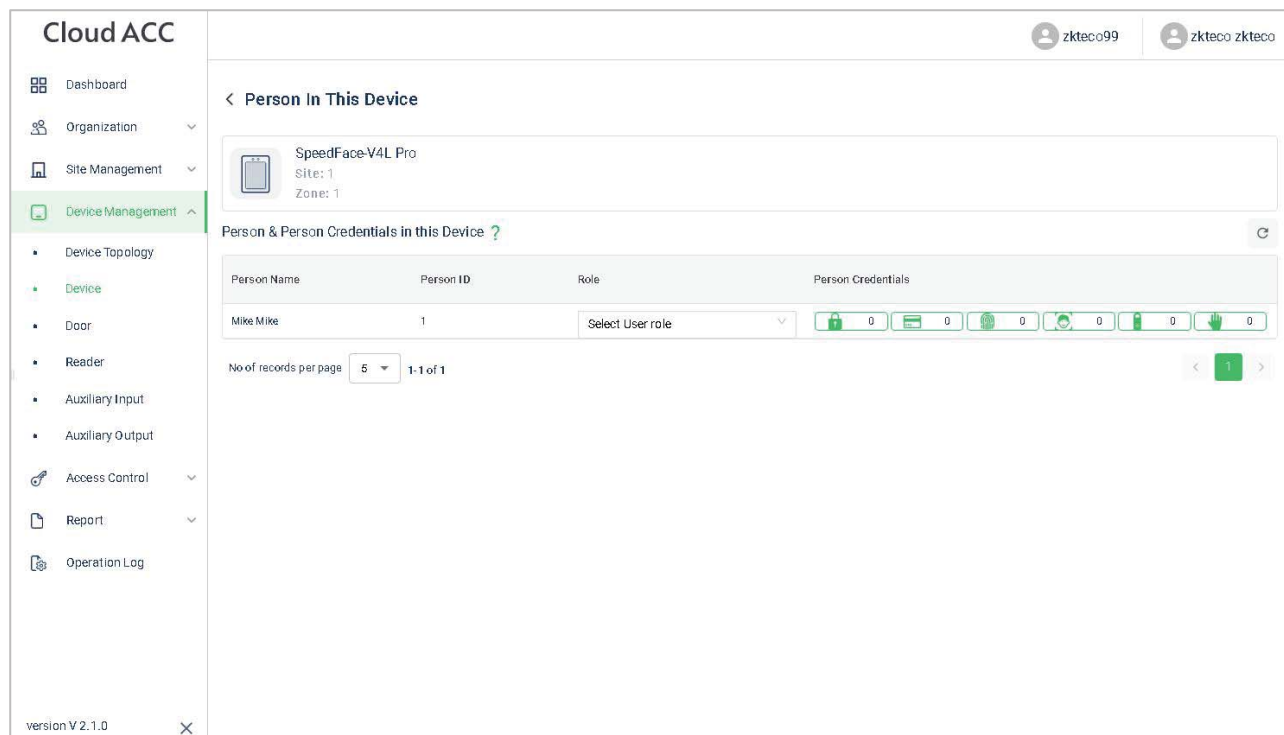
**Device**

+ Add Device

<input type="checkbox"/>	Device Name	Serial Number	IP Address	Device Model	Firmware Version	Status	Actions
<input type="checkbox"/>	SpeedFace-V4L Pro	8057232340005	192.168.163.175	SpeedFace-V4L Pro	ZAM180-NF4 0VB-Ver3.5.2	Online	

No of records per page 5 1-1 of 1

3. Click  icon to choose a finger, click **Submit**, then register fingerprint on the device.



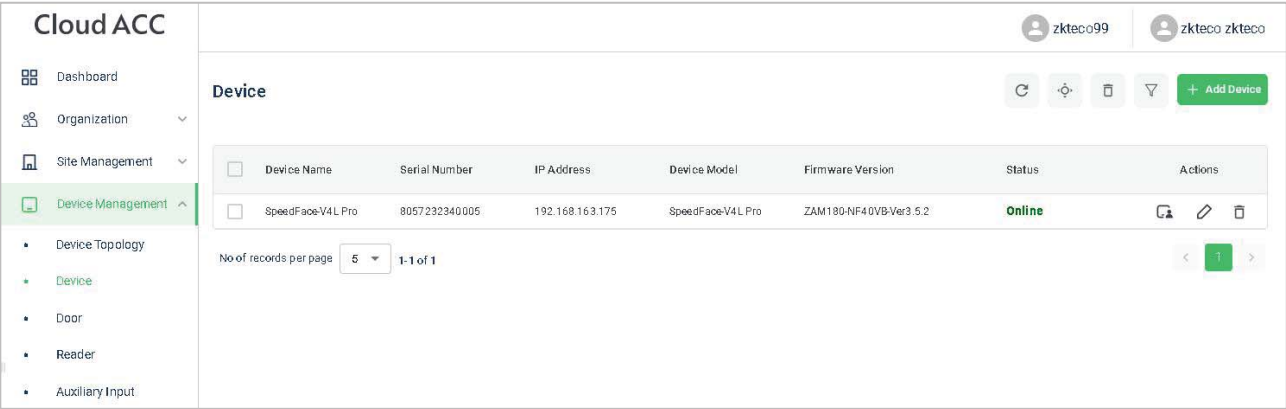
4. Press the same finger on the fingerprint reader three times. Green indicates that the fingerprint was enrolled successfully.



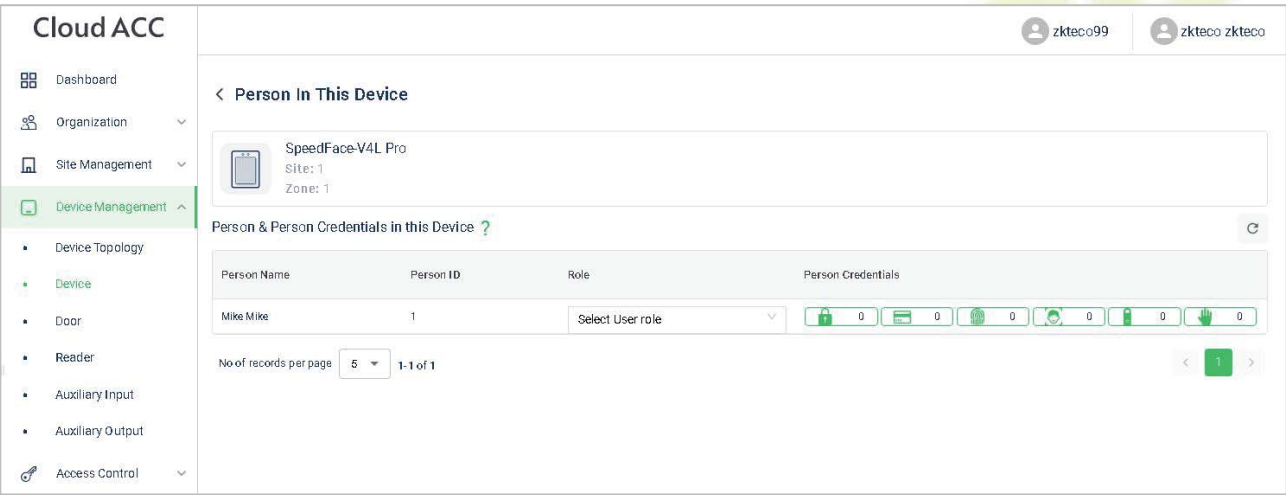
### 15.5.4 Register Face Template

1. Click **Device Management > Device** on **ZKBio Cloud Access** interface to enter the **Device** interface.

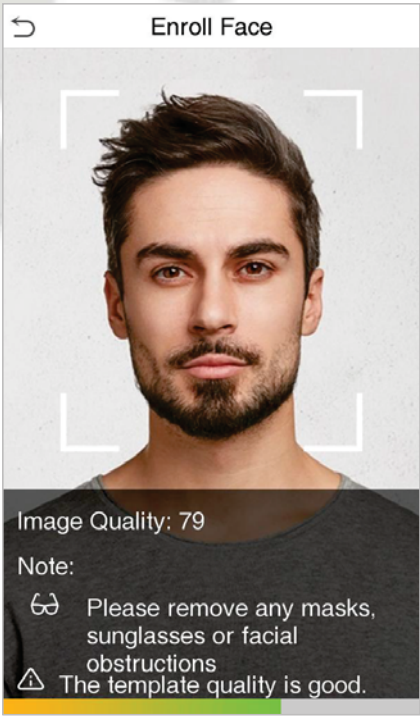
2. Choose a device and click **Persons in the Device** icon  to view the person list.




3. Click  icon to register face template on the device.

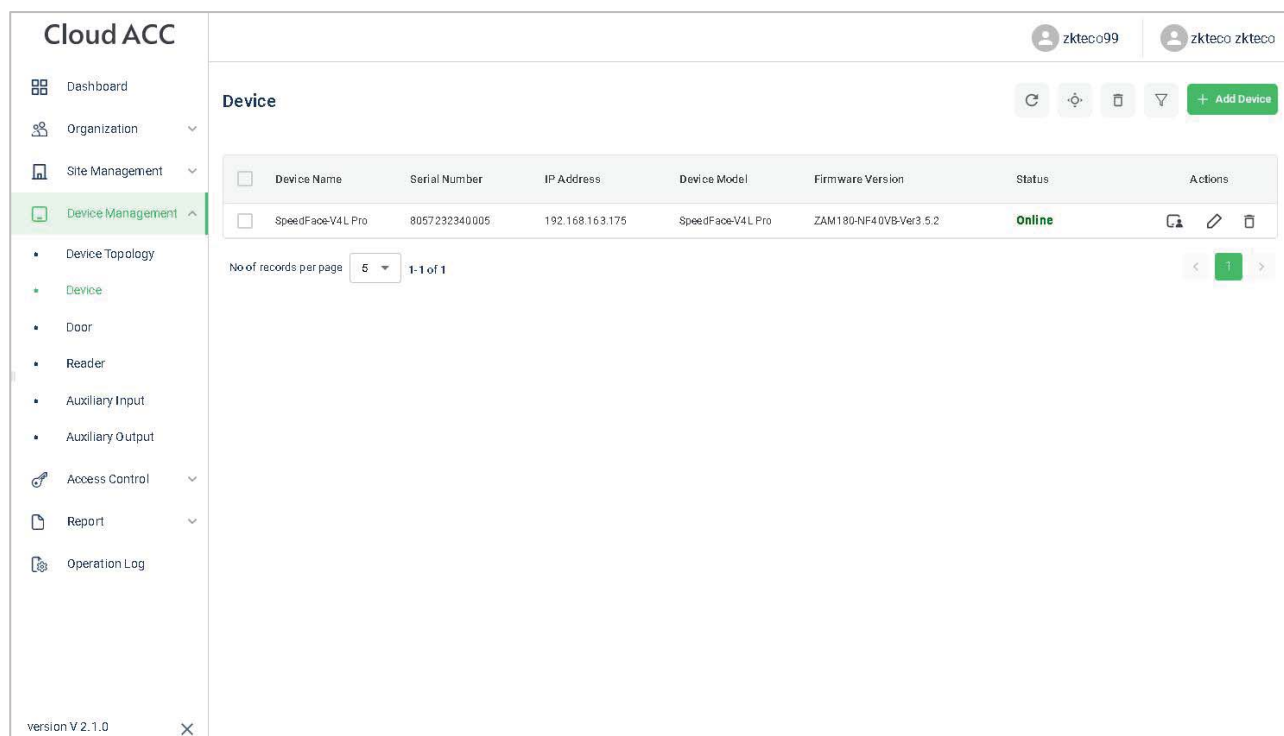


The registration interface is as follows:




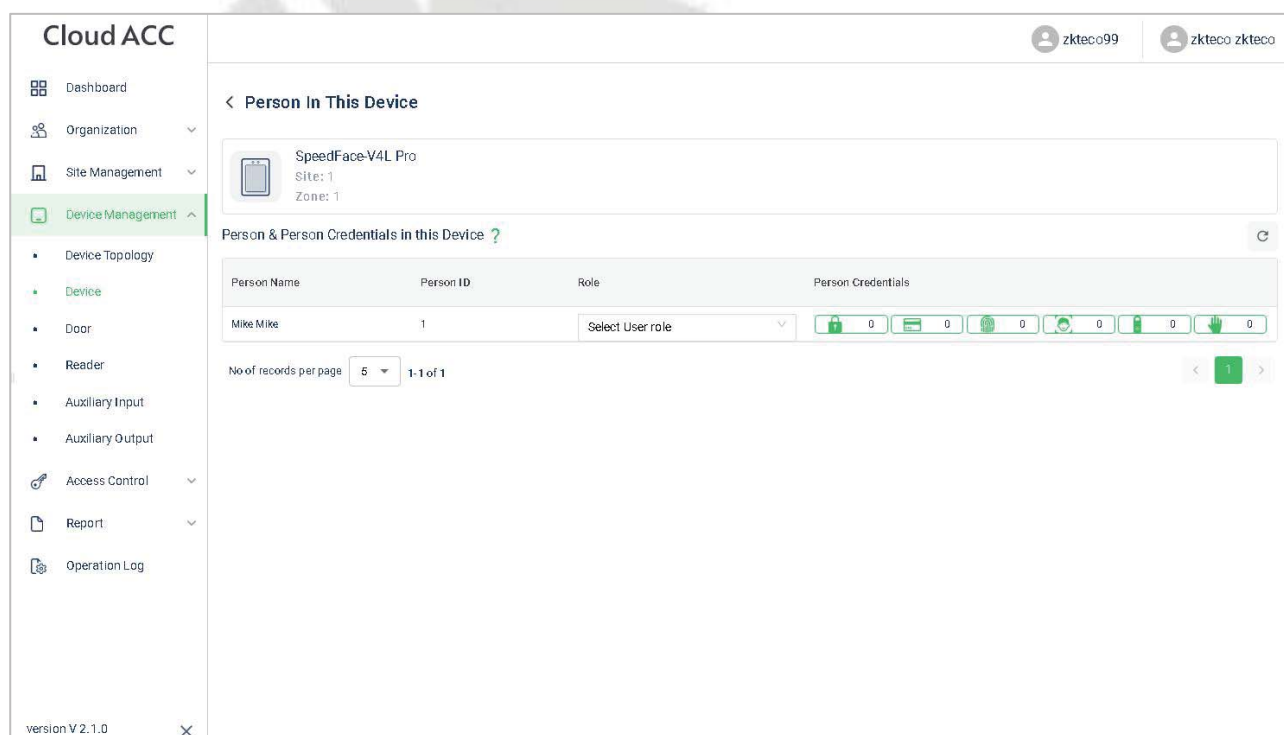
### 15.5.5 Register Password

1. Click **Device Management > Device** on **ZKBio Cloud Access** interface to enter the **Device** interface.
2. Choose a device and click **Persons in the Device** icon  to view the person list.



The screenshot shows the Cloud ACC interface with the left sidebar containing navigation options: Dashboard, Organization, Site Management, Device Management (selected), Device Topology, Device, Door, Reader, Auxiliary Input, Auxiliary Output, Access Control, Report, and Operation Log. The main content area is titled 'Device' and displays a table of devices. The table has columns: Device Name, Serial Number, IP Address, Device Model, Firmware Version, Status, and Actions. One device is listed: SpeedFace-V4L Pro, Serial Number 8057232340005, IP Address 192.168.163.175, Device Model SpeedFace-V4L Pro, Firmware Version ZAM180-NF40VB-Ver3.5.2, and Status Online. Below the table, there is a pagination control showing 'No of records per page' as 5 and '1-1 of 1'. A green '+ Add Device' button is located in the top right corner of the device list area.

3. Click  icon to register password on the device.



The screenshot shows the Cloud ACC interface with the left sidebar containing navigation options: Dashboard, Organization, Site Management, Device Management (selected), Device Topology, Device, Door, Reader, Auxiliary Input, Auxiliary Output, Access Control, Report, and Operation Log. The main content area is titled 'Person In This Device' and displays a card for the selected device: SpeedFace-V4L Pro, Site: 1, Zone: 1. Below the card, there is a section titled 'Person & Person Credentials in this Device' with a table. The table has columns: Person Name, Person ID, Role, and Person Credentials. One person is listed: Mike Mike, Person ID 1, Role Select User role, and Person Credentials 0 0 0 0 0 0 0 0. Below the table, there is a pagination control showing 'No of records per page' as 5 and '1-1 of 1'. A green '+ Add Device' button is located in the top right corner of the person list area.

The registration interface is as follows:




The image shows a mobile interface for password registration. At the top, there is a back arrow and the title 'Password'. Below the title, it says 'Please re-type the password.' There is a large empty rectangular box for input. At the bottom, there is a numeric keypad with buttons for digits 1-9, 0, and a '123' button. There are also buttons for backspace (X), up arrow, down arrow, and an 'OK' button.

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

### 15.5.6 Register Card

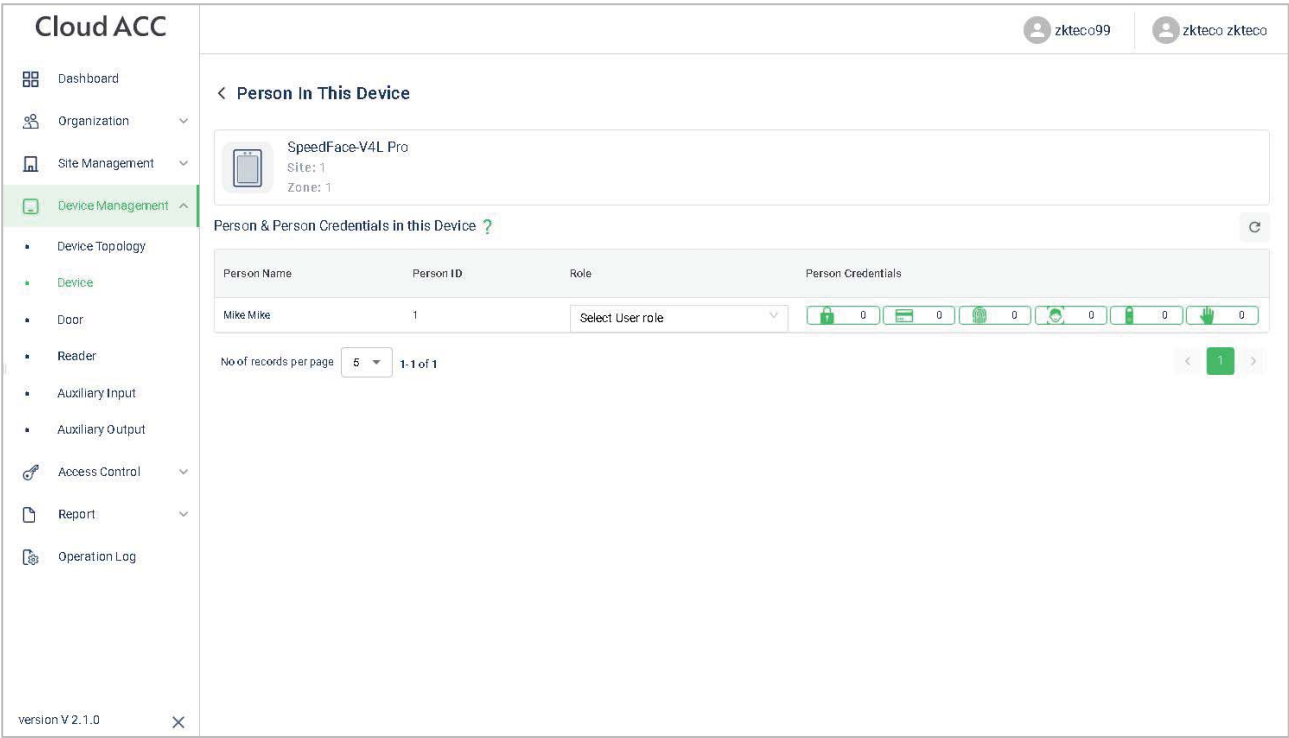
1. Click **Device Management** > **Device** on **ZKBio Cloud Access** interface to enter the **Device** interface.
2. Choose a device and click **Persons in the Device** icon  to view the person list.

The screenshot shows the 'Cloud ACC' interface. On the left is a sidebar menu with options: Dashboard, Organization, Site Management, Device Management (highlighted), Device Topology, Door, Reader, Auxiliary Input, Auxiliary Output, Access Control, Report, and Operation Log. The main area is titled 'Device' and contains a table with the following data:

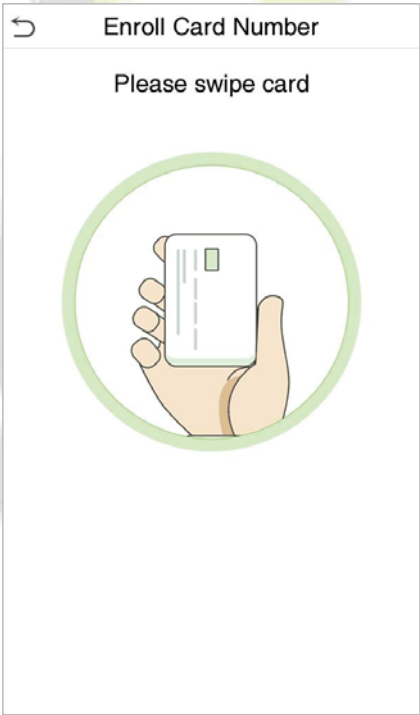
<input type="checkbox"/>	Device Name	Serial Number	IP Address	Device Model	Firmware Version	Status	Actions
<input type="checkbox"/>	SpeedFace-V4L Pro	8057232340005	192.168.163.175	SpeedFace-V4L Pro	ZAM180-NF4.0VB-Ver3.5.2	Online	  

Below the table, it says 'No of records per page' with a dropdown set to '5' and '1-1 of 1'. There are also navigation arrows and a page number '1'.

3. Click  icon to register password on the device.



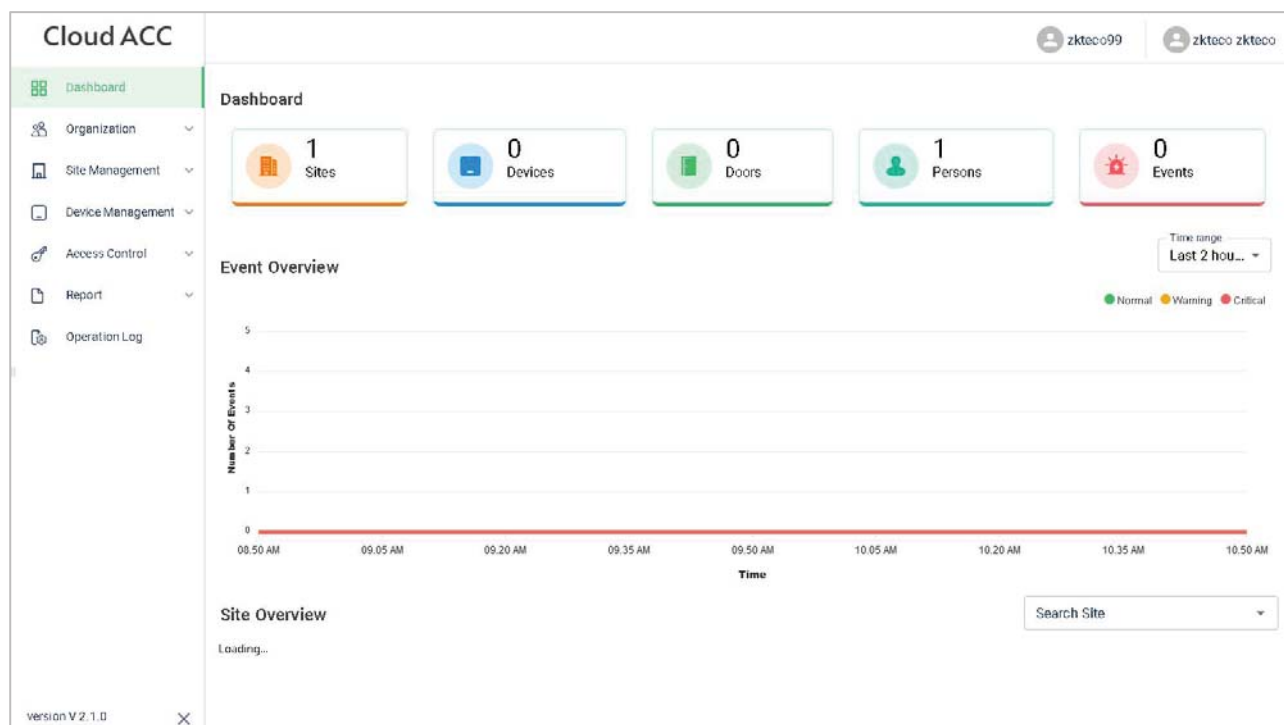
The registration interface is as follows:



## 15.6 Data Search

### 15.6.1 Dashboard

In **ZKBio Cloud Access** interface, click **Dashboard** to check the sites, devices, doors, person of this application, events overview graph, and sites overview map.



### 15.6.2 Event Report

In **ZKBio Cloud Access** interface, click **Report > Events** to check the specific information of all devices' events.

**Cloud ACC**

zkteco99 zkteco zkteco

**Events**

Person ID	Person Name	Device Name	Device Serial Number	Event Time	Event Address	Event Name	Verification Mode
		SpeedFace-V4L ...	8057232340005	2023-08-11 10:4...	1		
		SpeedFace-V4L ...	8057232340005	2023-08-11 10:4...	1		
10220		SpeedFace-V4L ...	8057232340005	2023-08-11 10:4...	1		
			8057232340005	2023-08-11 10:3...	1		
			8057232340005	2023-08-11 10:3...	1		

No of records per page 5 1-5 of 12



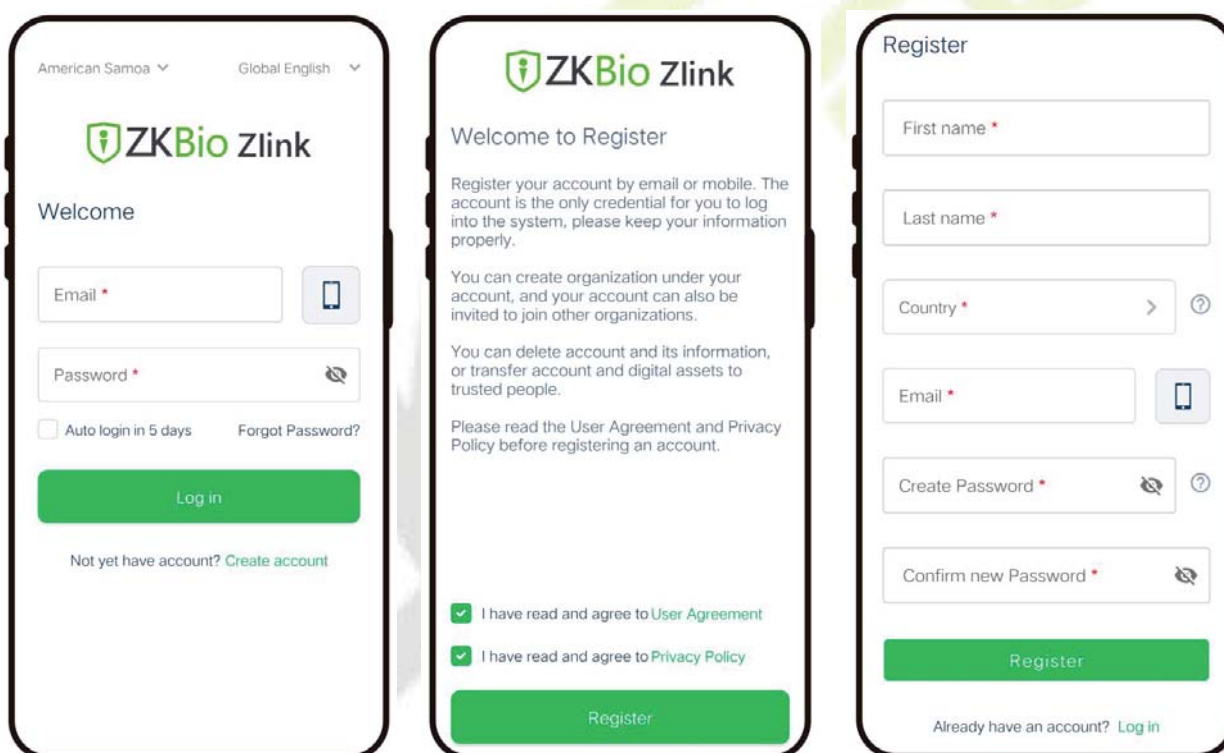
## 16. Connecting to ZKBio Zlink App

Change the device communication protocol to BEST protocol, then the device can be managed by ZKBio Zlink, please refer to [6.5 Device Type Setting](#).

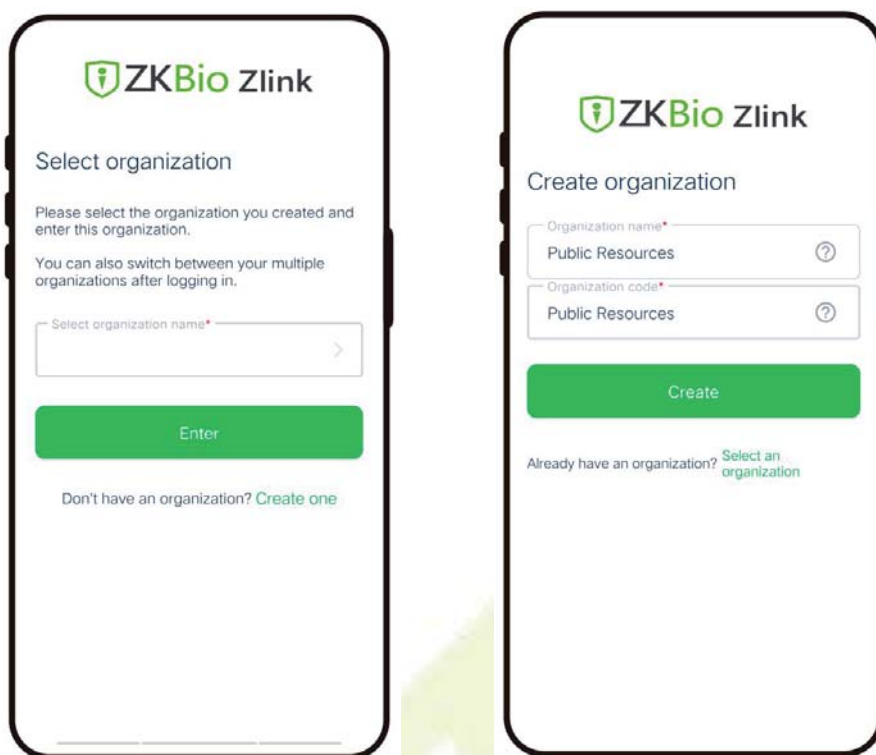
Users can use the created account to access ZKBio Zlink App to connect devices, unlock the device remotely and query records.

### 16.1 Register Account


1. Search for the ZKBio Zlink App in Apple App Store or Google Play Store and download the App to your smartphone.
2. Open the ZKBio Zlink App and if you do not have an account, please click **create account** to add a new account.
3. Read and agree to User Agreement and Privacy Policy, then click **Register**.
4. Enter user's information and set password, then click **Register**.

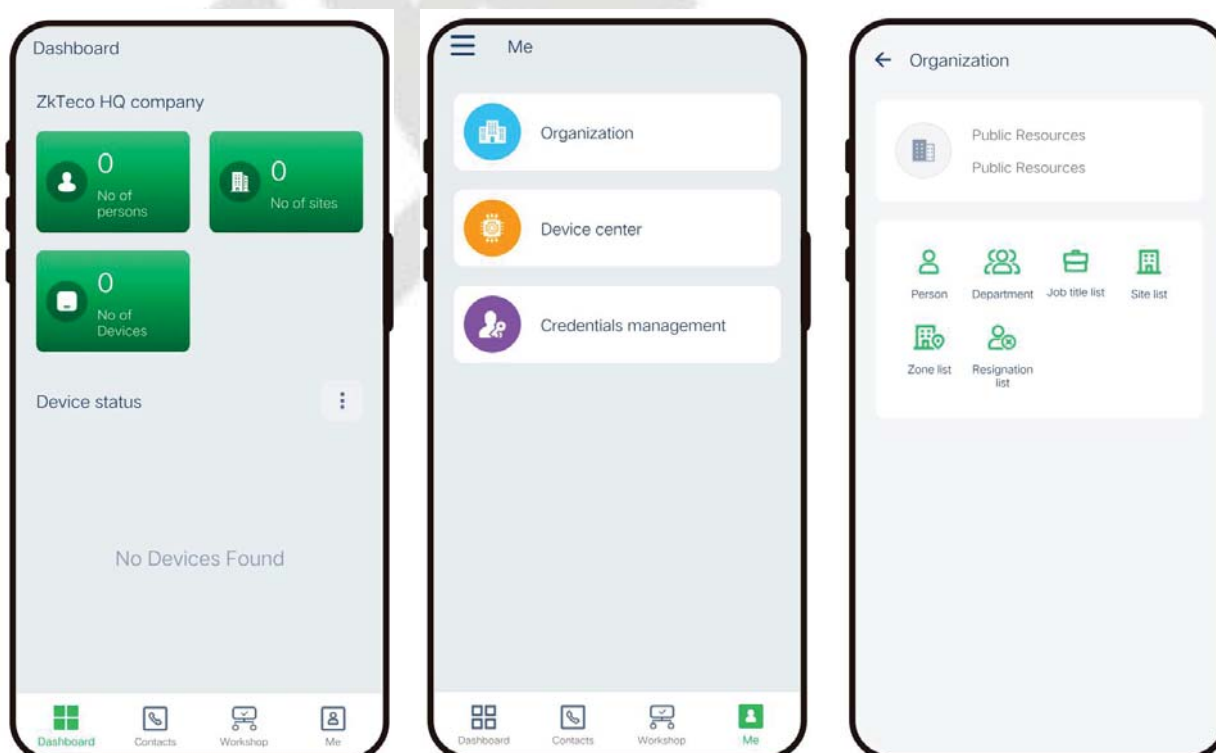


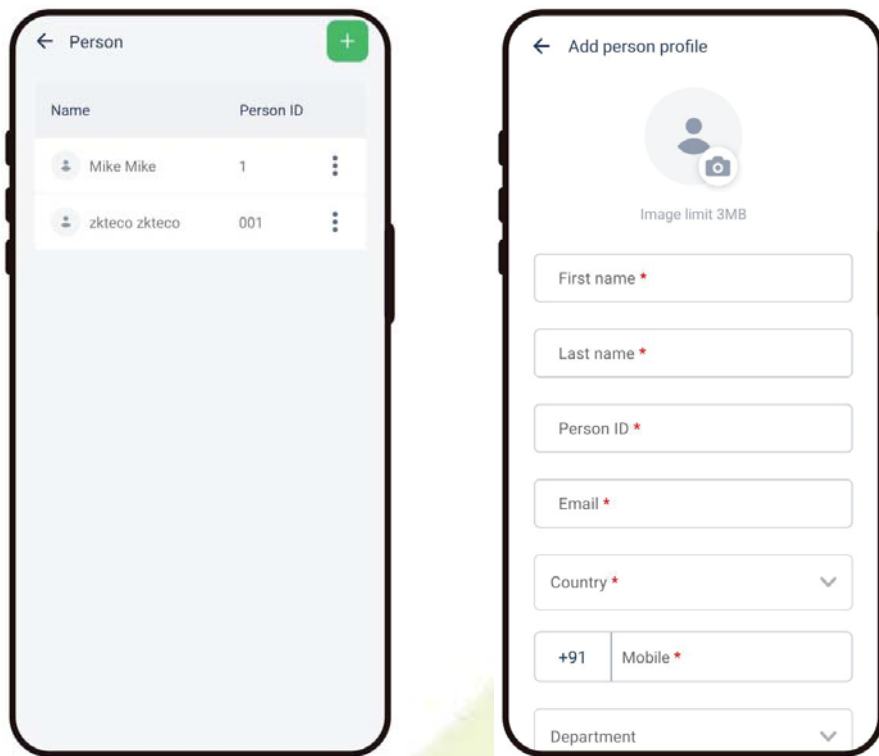
- Choose an organization, click **Enter**, then complete registration. If you do not have an organization, please click **Create one**.



## 16.2 Add Person


- Click **Me > Organization > Person** on the main menu.
- Click  icon to add a new person. Enter the information, and click **Save**.

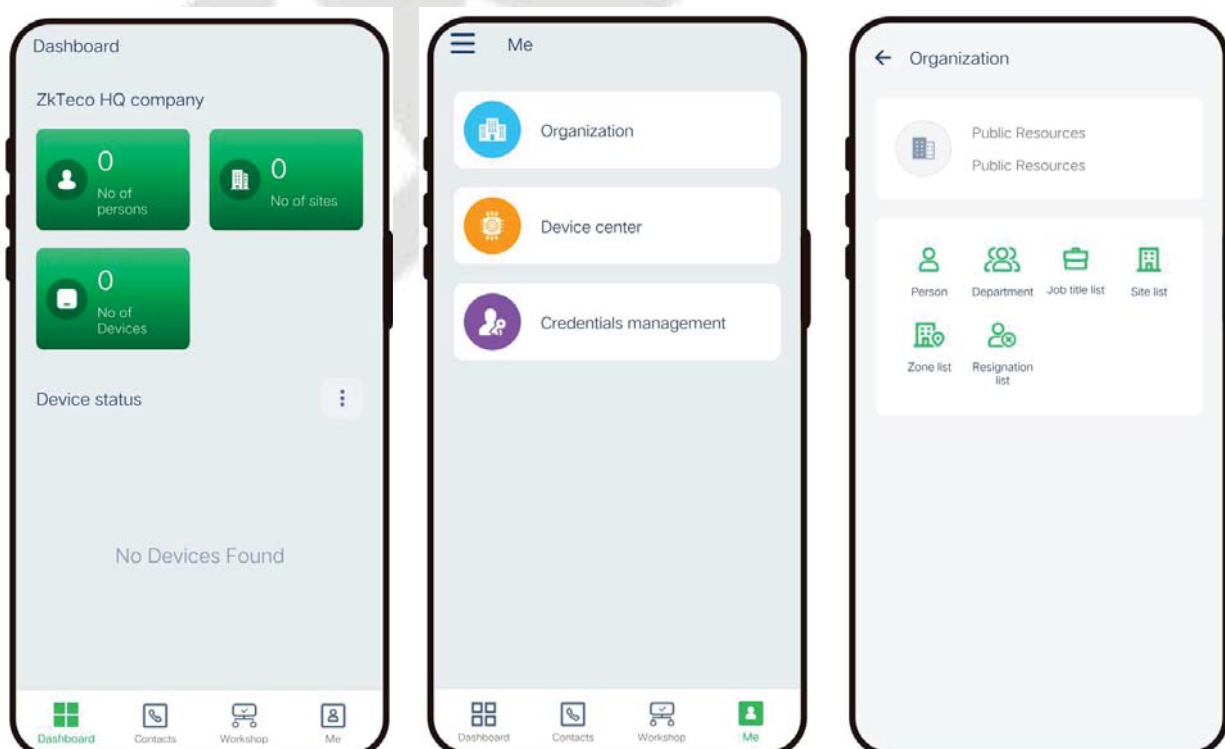


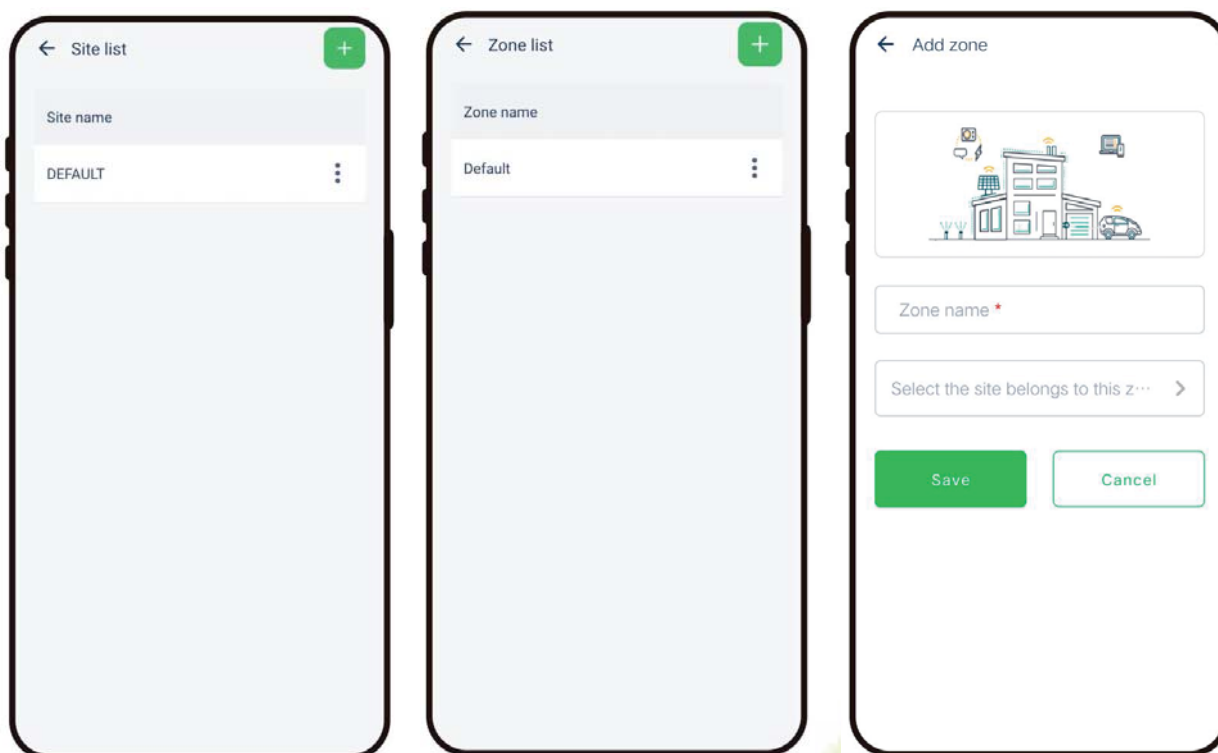


## 16.3 Add Device

### 16.3.1 Add Site and Zone

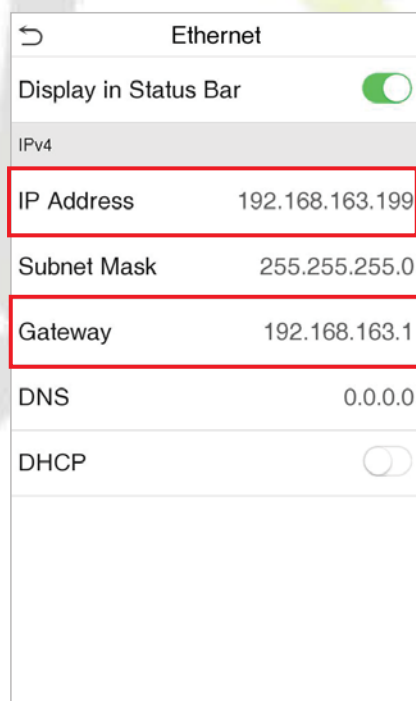
1. Click **Me > Organization > Site (or Zone)** on the main menu.
2. Click  icon to add a new site or zone. Enter the information, and click **Save**.






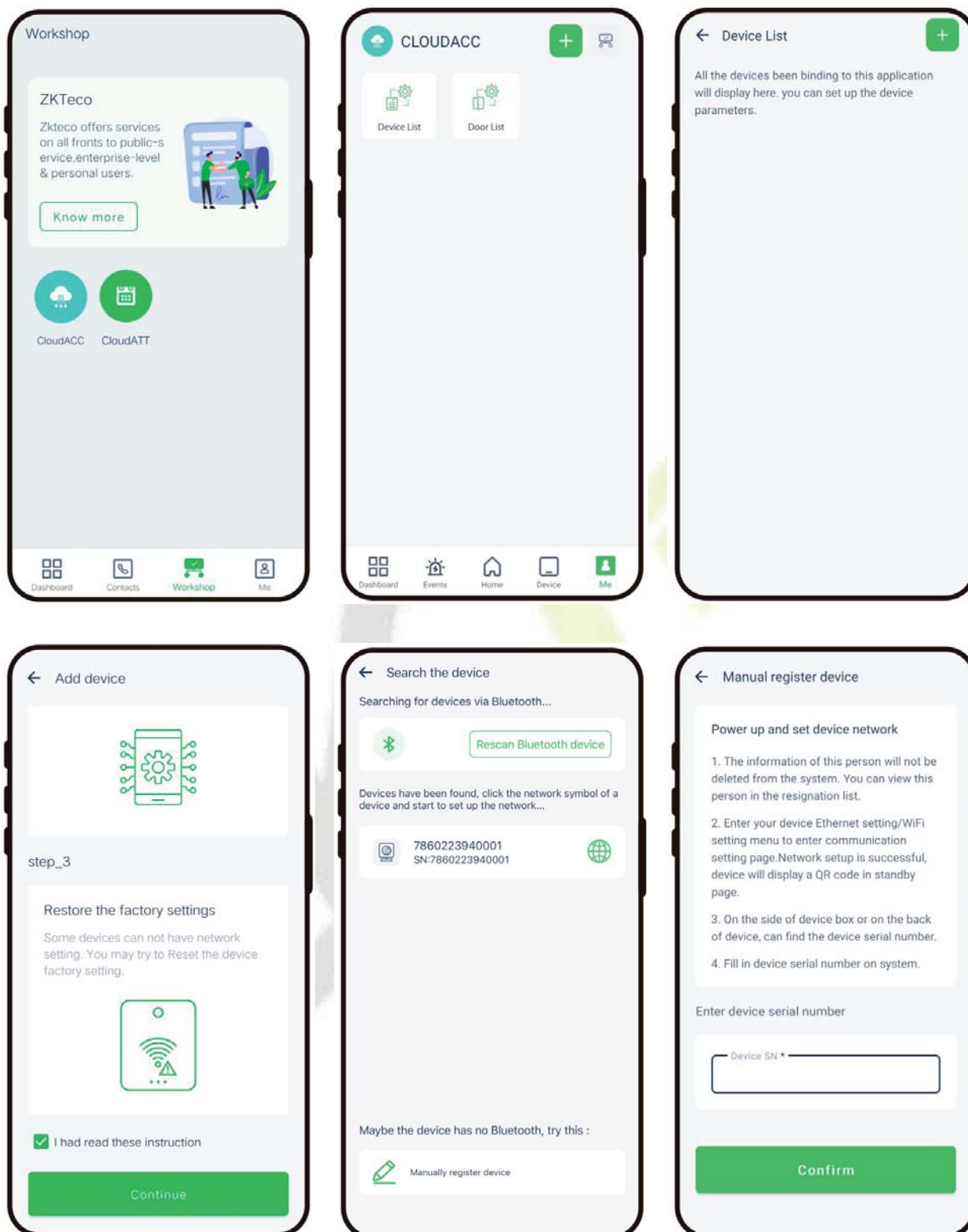
### 16.3.2 Add Device

1. Tap **COMM.** > **Ethernet** in the main menu on the device to set the IP address and gateway of the device.

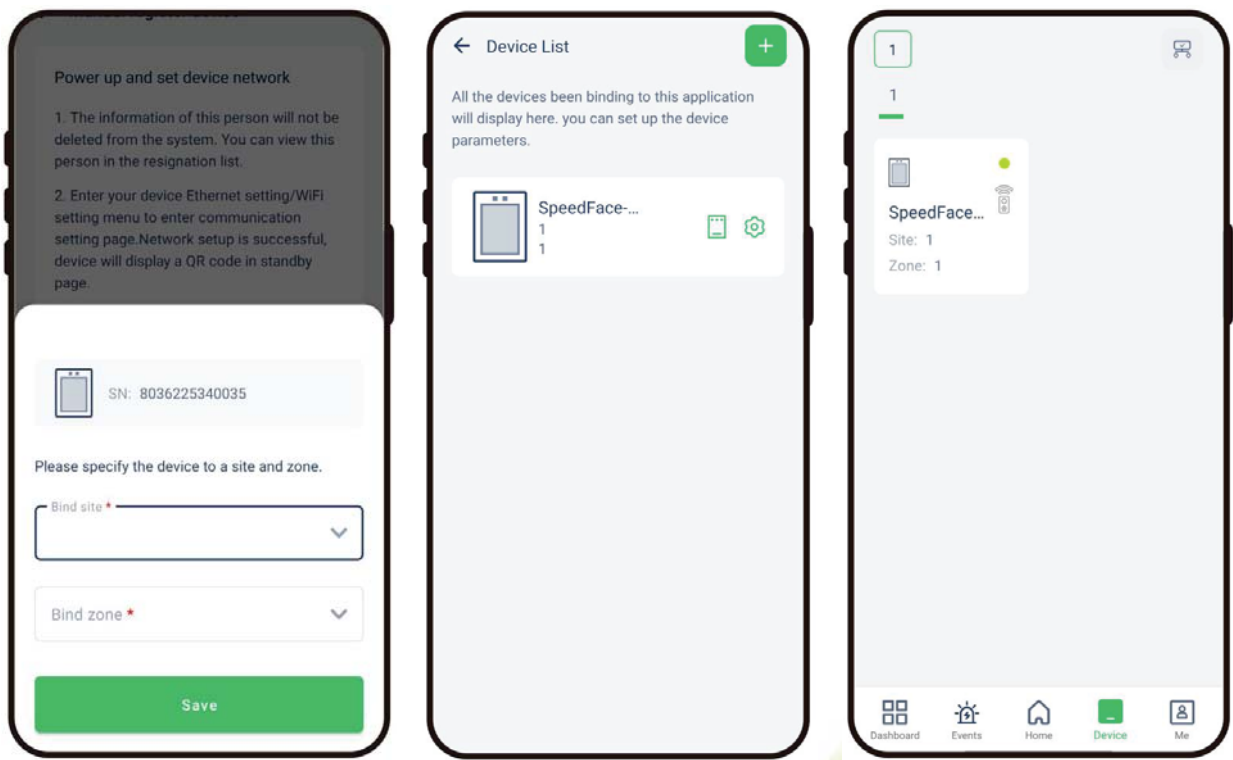


2. Click **Workshop** > **CloudACC** on the main menu to enter the **ZKBio Cloud Access** interface.
3. Click **Me** > **Device List** to enter the **Device** interface. And click  icon to add a new device.
4. Click **Manually register device**.

5. Read and check to the instructions, then click **Continue**.
6. Enter the device's serial number, then click **Confirm**. (Click **System Info > Device Info** on the device to view the serial number.)



7. Choose a site and a zone, then click **Save** to finish.
8. Then click **Device**, users can view the device status and unlock remotely in this interface.



## 17. Connect to ZKBio CVAccess Software

### 17.1 Set the Communication Address

#### ● Device Side

1. Tap **COMM.** > **Ethernet** in the main menu to set the IP address and gateway of the device.

**Note:** Please ensure that the IP address is in the same network segment as the server address and can communicate with the ZKBio CVAccess server.

2. In the main menu, click **COMM.** > **Cloud Server Setting** to set the server address and server port.

**Server address:** Set the IP address as of ZKBio CVAccess server.

**Server port:** Set the server port as of ZKBio CVAccess.

Ethernet	
Display in Status Bar	<input checked="" type="checkbox"/>
IPv4	
IP Address	192.168.163.199
Subnet Mask	255.255.255.0
Gateway	192.168.163.1
DNS	0.0.0.0
DHCP	<input type="checkbox"/>

Cloud Server Settings	
Server Mode	ADMS
Enable Domain Name	<input type="checkbox"/>
Server Address	192.168.163.61
Server Port	8081
Enable Proxy Server	<input type="checkbox"/>

#### ● Software Side

Login to ZKBio CVAccess software, click **System** > **Communication** > **Communication Monitor** to set the ADMS service port, as shown in the figure below:

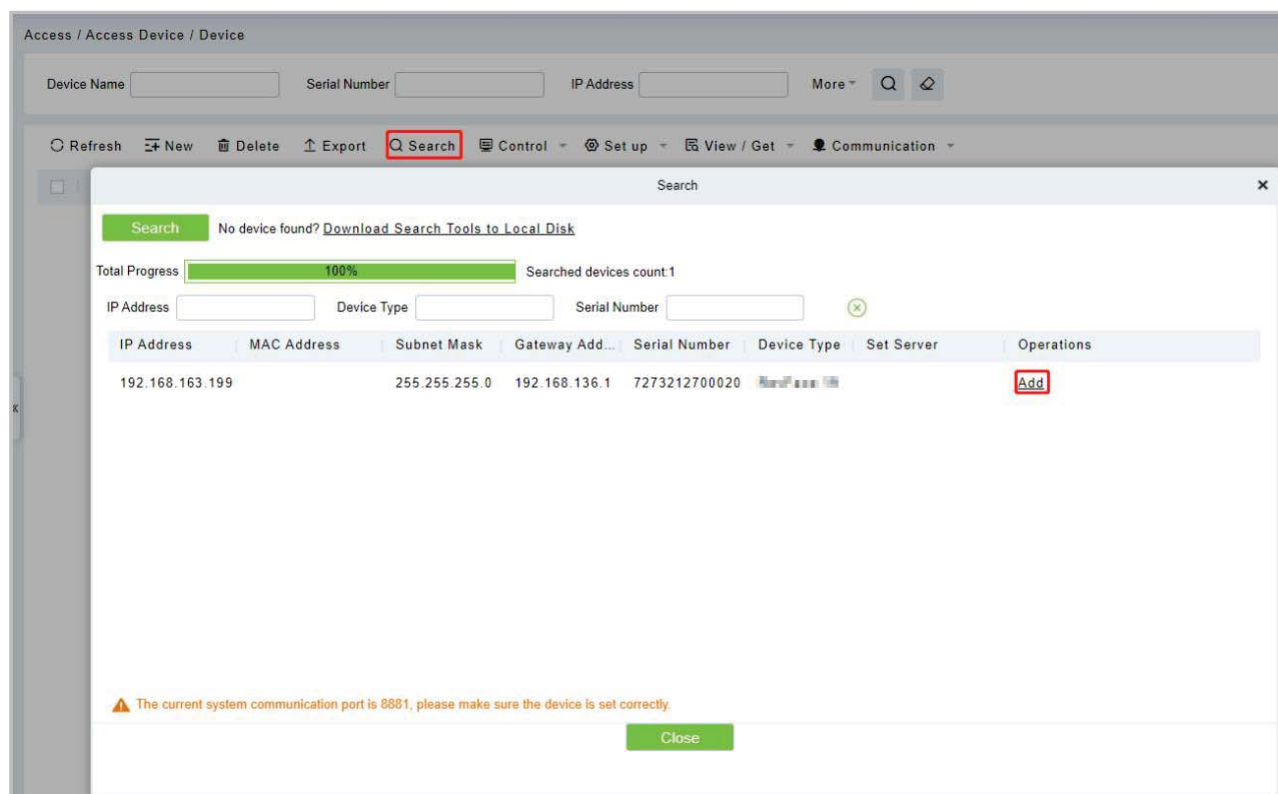
Adms Service Settings	
Adms Service Port	8081
<p>⚠ The current port is for device communication service. If there is a network mapping for the service port, please refer to the actual mapped port.</p>	
Project control file version	None
Turn on encrypted transmission	<input checked="" type="checkbox"/> Yes



## 17.2 Add Device on the Software

Add the device by searching. The process is as follows:

1. Click **Access > Device > Search Device**, to open the Search interface in the software.
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** in operation column, a new window will pop-up. Select Icon type, Area, and Add to Level from each dropdown and click **OK** to add the device.

## 17.3 Add Personnel on the Software

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

The screenshot shows the 'New' personnel registration window. The 'Personal Information' section contains the following fields:

- Personnel ID\*: 2842
- First Name
- Gender
- Certificate Type
- Birthday
- Hire Date
- Device Verification Password
- Biometrics Type
- Enable app login

The 'Access Control' section includes the following options:

- Levels Settings: General (checked)
- Superuser: No
- Device Operation Role: Ordinary User
- Extend Passage
- Access Disabled
- Set Valid Time

At the bottom of the window, there are three buttons: 'Save and New', 'OK', and 'Cancel'.

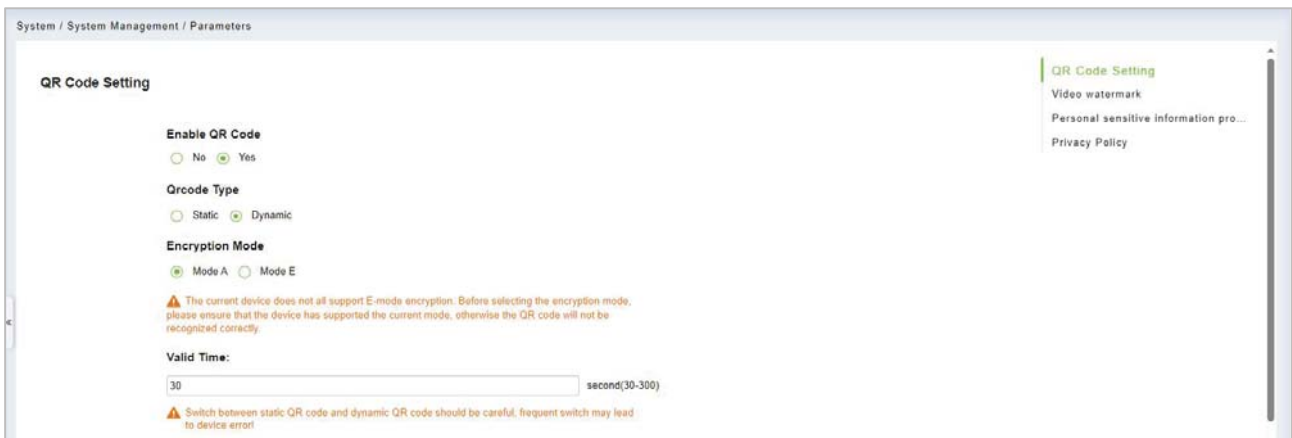
2. Fill in all the required fields and click **OK** to register a new user.
3. Click **Access > Device > Control > Synchronize All Data to Devices** to synchronize all the data to the device including the new users.

## 17.4 Mobile Credential ★

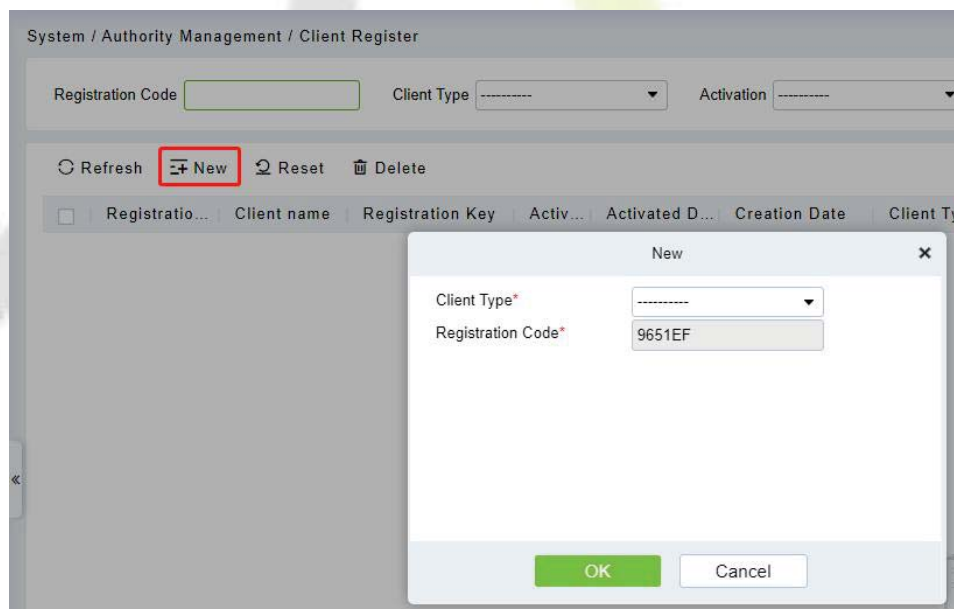
**Note:** This function is only for SenseFace 7C.

After downloading and installing the ZKBioAccess Mobile Page, the user needs to set the Server before login. The steps are given below:

1. In **ZKBio CVAccess > System > System Management > Parameters**, set **Enable QR Code** to "Yes", and select the QR code status according to the actual situation. The default is **Dynamic**, the valid time of the QR code can be set.



2. On the Server, choose **System > Authority Management > Client Register** to add a registered App client.

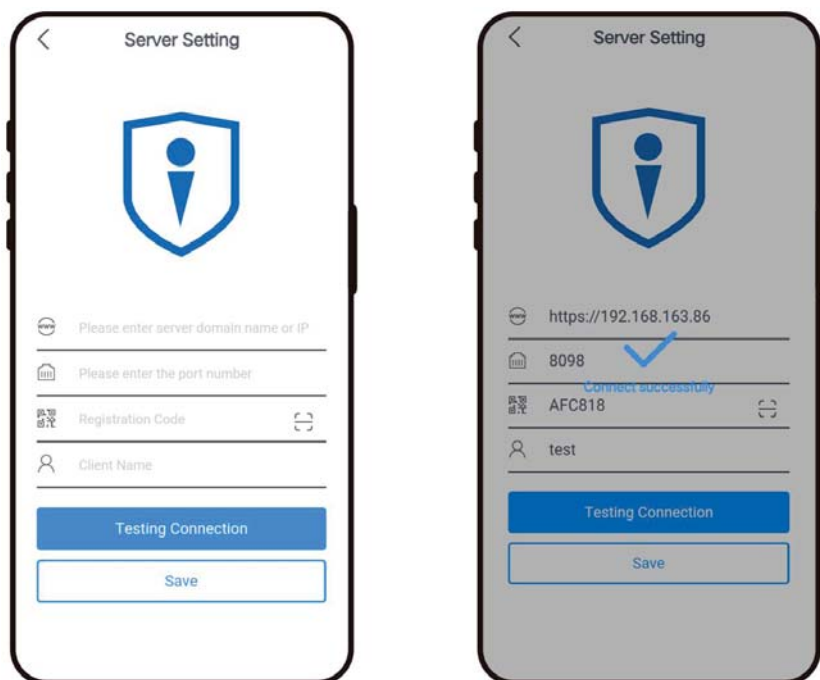


3. Open the App on the Smartphone. On the login screen, tap **Server Setting** and type the IP Address or the domain name of the Server, and its port number.

**Note:** Smartphone and the Server must be in the same network segment.

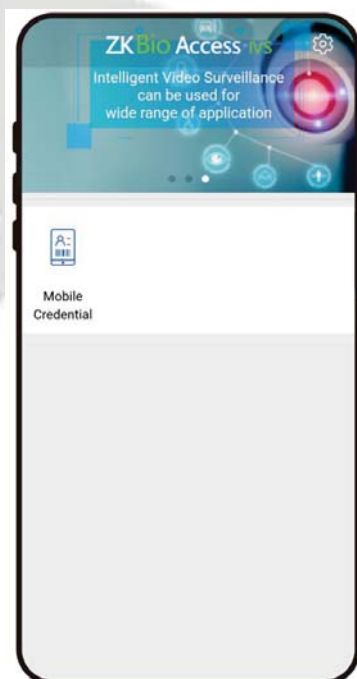
4. Tap the **QR Code** icon to scan the QR code of the new App client. After the client is identified successfully, set the client's name and tap **Connection Test**.

5. After the network is connected successfully, tap **Save**.

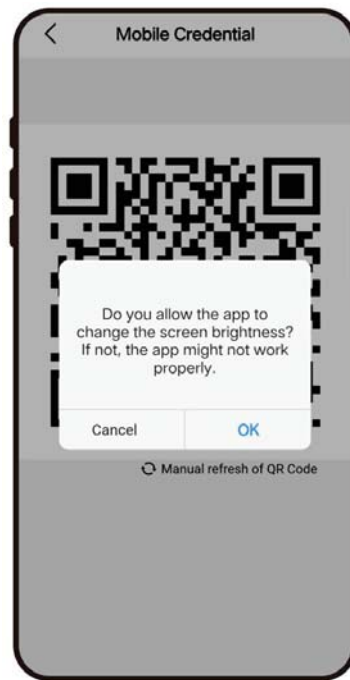


The Mobile Credential function is only valid when logging in as an employee, tap on Employee to switch to employee login screen. Enter the employee ID and password (Default: 123456) to login.

6. Tap **Mobile Credential** on the App, and a QR code will appear, which includes employee ID and card number (static QR code only includes card number) information.
7. The QR code can replace a physical card on a specific device to achieve contactless authentication to open the door.



8. When using this function for the first time, the App will prompt to authorize the modification of screen brightness settings, as shown in the figure:



9. The QR code refreshes automatically for every 30s and supports manual refresh.



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

## 18. Connect to ZKBioTime Software

### 18.1 Set the Communication Address

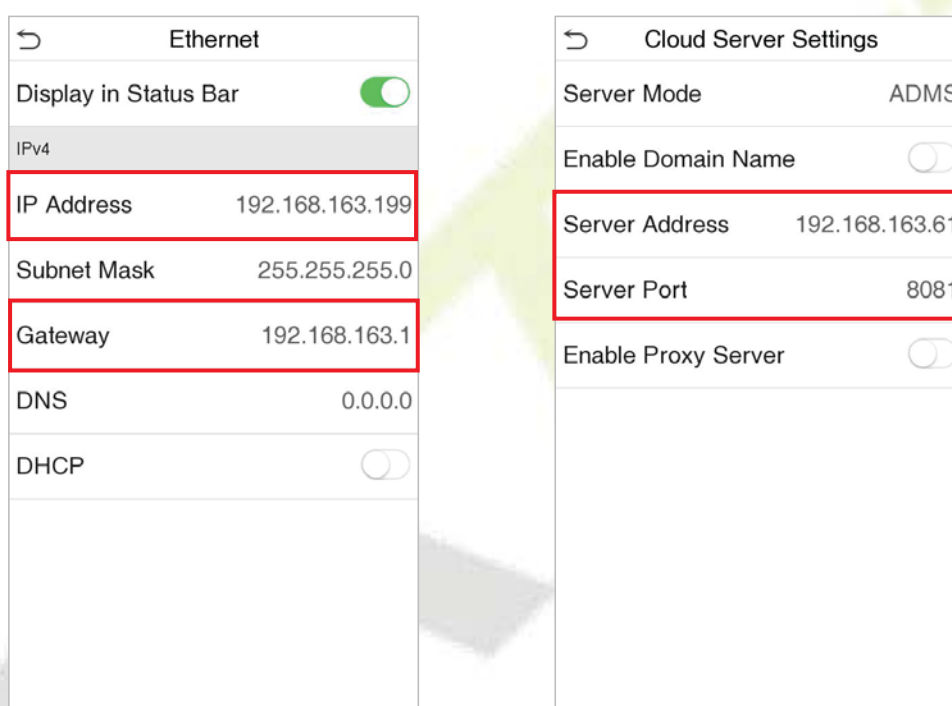
1. Tap **COMM.** > **Ethernet** in the main menu to set the IP address and gateway of the device.

**Note:** Please ensure that the IP address is in the same network segment as the server address and can communicate with the ZKBio CVAccess server.

2. In the main menu, click **COMM.** > **Cloud Server Setting** to set the server address and server port.

**Server address:** Set the IP address as of BioTime server.

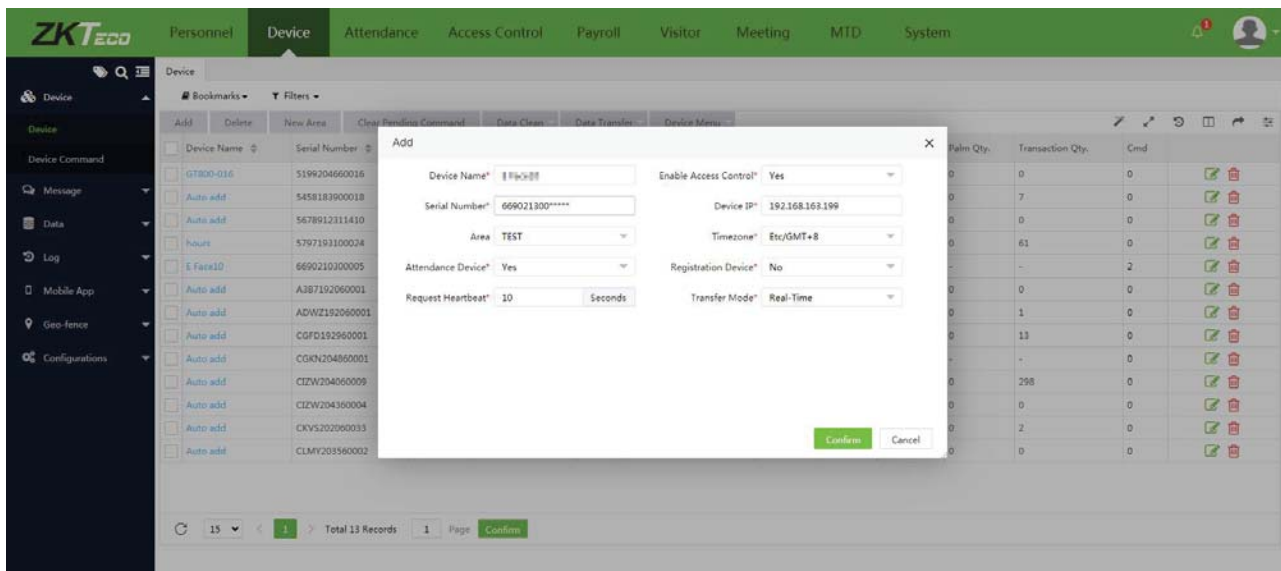
**Server port:** Set the server port as of BioTime (The default is 8081).



### 18.2 Add Device on the Software

Add the device by searching. The process is as follows:

1. Click **Device** > **Device** > **Add**, to add the device on the software.
2. A new window pops-up on clicking **Add**. Enter the required information about the device and click **Confirm**, then the added devices are displayed automatically.



## 18.3 Add Personnel on the Software

1. Click **Personnel > Employee > Add**:

2. Fill in all the required fields and click **Confirm** to register a new user.
3. Click **Device > Device > Data Transfer > Sync Data to Device** to synchronize all the data to the device including the new users.



## Appendix 1

### Requirements of Live Collection and Registration of Visible Light Face Templates

- 1) It is recommended to perform registration in an indoor environment with an appropriate light source without underexposure or overexposure.
- 2) Do not place the device towards outdoor light sources like door or window or other harsh light sources.
- 3) Dark-color apparels, different from the background color is recommended for registration.
- 4) Please expose your face template and forehead properly and do not cover your face template and eyebrows with your hair.
- 5) It is recommended to show a plain facial expression. (A smile is acceptable, but do not close your eyes, or incline your head to any orientation).
- 6) Two templates are required for a person with eyeglasses, one template with eyeglasses and the other without the eyeglasses.
- 7) Do not wear accessories like a scarf or mask that may cover your mouth or chin.
- 8) Please face template right towards the capturing device, and locate your face template in the template capturing area as shown in the template below.
- 9) Do not include more than one face template in the capturing area.
- 10) A distance of 50cm to 80cm is recommended for capturing the template. (The distance is adjustable, subject to body height).



## Requirements for Visible Light Digital Face Template Data

The digital photo should be straight-edged, colored, half-portrayed with only one person, and the person should be uncharted and in casuals. Persons who wear eyeglasses should remain to put on eyeglasses for getting photo captured.

- **Eye distance**

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

- **Facial expression**

Neutral face template or smile with eyes naturally open are recommended.

- **Gesture and angel**

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

- **Accessories**

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

- **Face template**

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

- **Template format**

Should be in BMP, JPG or JPEG.

- **Data requirement**

Should comply with the following requirements:

- 1) White background with dark-colored apparel.
- 2) 24bit true color mode.
- 3) JPG format compressed template with not more than 20kb size.
- 4) Resolution should be between 358 x 441 to 1080 x 1920.
- 5) The vertical scale of head and body should be in a ratio of 2:1.
- 6) The photo should include the captured person's shoulders at the same horizontal level.
- 7) The captured person's eyes should be open and with clearly seen iris.
- 8) Neutral face template or smile is preferred, showing teeth is not preferred.
- 9) The captured person should be clearly visible, natural in color, no harsh shadow or light spot or reflection in face template or background. The contrast and lightness level should be appropriate.

## Appendix 2

### Privacy Policy

#### Notice:

To help you better use the products and services of ZKTeco (hereinafter referred as "we", "our", or "us") a smart service provider, we consistently collect your personal information. Since we understand the importance of your personal information, we took your privacy sincerely and we have formulated this privacy policy to protect your personal information. We have listed the privacy policies below to precisely understand the data and privacy protection measures related to our smart products and services.

**Before using our products and services, please read carefully and understand all the rules and provisions of this Privacy Policy. If you do not agree to the relevant agreement or any of its terms, you must stop using our products and services.**

#### I. Collected Information

To ensure the normal product operation and help the service improvement, we will collect the information voluntarily provided by you or provided as authorized by you during registration and use or generated as a result of your use of services.

1. **User Registration Information:** At your first registration, the feature template (**Fingerprint template/Face template template/Palm template**) will be saved on the device according to the device type you have selected to verify the unique similarity between you and the User ID you have registered. You can optionally enter your Name and Code. The above information is necessary for you to use our products. If you do not provide such information, you cannot use some features of the product regularly.
2. **Product information:** According to the product model and your granted permission when you install and use our services, the related information of the product on which our services are used will be collected when the product is connected to the software, including the Product Model, Firmware Version Number, Product Serial Number, and Product Capacity Information. **When you connect your product to the software, please carefully read the privacy policy for the specific software.**

#### II. Product Security and Management

1. When you use our products for the first time, you shall set the Administrator privilege before performing specific operations. Otherwise, you will be frequently reminded to set the Administrator privilege when you enter the main menu interface. **If you still do not set the Administrator privilege after receiving the system prompt, you should be aware of the possible security risk (for example, the data may be manually modified).**

2. All the functions of displaying the biometric information are disabled in our products by default. You can choose Menu > System Settings to set whether to display the biometric information. If you enable these functions, we assume that you are aware of the personal privacy security risks specified in the privacy policy.
3. Only your user ID is displayed by default. You can set whether to display other user verification information (such as Name, Department, Photo, etc.) under the Administrator privilege. **If you choose to display such information, we assume that you are aware of the potential security risks (for example, your photo will be displayed on the device interface).**
4. The camera function is disabled in our products by default. If you want to enable this function to take pictures of yourself for attendance recording or take pictures of strangers for access control, the product will enable the prompt tone of the camera. **Once you enable this function, we assume that you are aware of the potential security risks.**
5. All the data collected by our products is encrypted using the AES 256 algorithm. All the data uploaded by the Administrator to our products are automatically encrypted using the AES 256 algorithm and stored securely. If the Administrator downloads data from our products, we assume that you need to process the data and you have known the potential security risk. In such a case, you shall take the responsibility for storing the data. You shall know that some data cannot be downloaded for sake of data security.
6. All the personal information in our products can be queried, modified, or deleted. If you no longer use our products, please clear your personal data.

### III. How we handle personal information of minors

Our products, website and services are mainly designed for adults. Without consent of parents or guardians, minors shall not create their own account. If you are a minor, it is recommended that you ask your parents or guardian to read this Policy carefully, and only use our services or information provided by us with consent of your parents or guardian.

We will only use or disclose personal information of minors collected with their parents' or guardians' consent if and to the extent that such use or disclosure is permitted by law or we have obtained their parents' or guardians' explicit consent, and such use or disclosure is for the purpose of protecting minors.

Upon noticing that we have collected personal information of minors without the prior consent from verifiable parents, we will delete such information as soon as possible.

### IV. Others

You can visit [https://www.zkteco.com/cn/index/Index/privacy\\_protection.html](https://www.zkteco.com/cn/index/Index/privacy_protection.html) to learn more about how we collect, use, and securely store your personal information. To keep pace with the rapid development of technology, adjustment of business operations, and to cope with customer needs, we will constantly deliberate and optimize our privacy protection measures and policies. Welcome to visit our official website at any time to learn our latest privacy policy.

## Eco-friendly Operation



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

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

### Hazardous or Toxic substances and their quantities

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

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

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

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

---

## Attachment 1

"Hereby, ZKTECO CO.,LTD declares that this Product is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU.

This device complies with Part 15 of the FCC Rules.

Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference, and
- (2) This device must accept any interference received,  
including interference that may cause undesired operation.

**Warning:** Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

**Note:** This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

"This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment.

This equipment should be installed and operated with a minimum distance of 20 cm between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter."

ZKTeco Industrial Park, No. 32, Industrial Road,  
Tangxia Town, Dongguan, China.  
Phone : +86 769 - 82109991  
Fax : +86 755 - 89602394  
[www.zkteco.com](http://www.zkteco.com)

