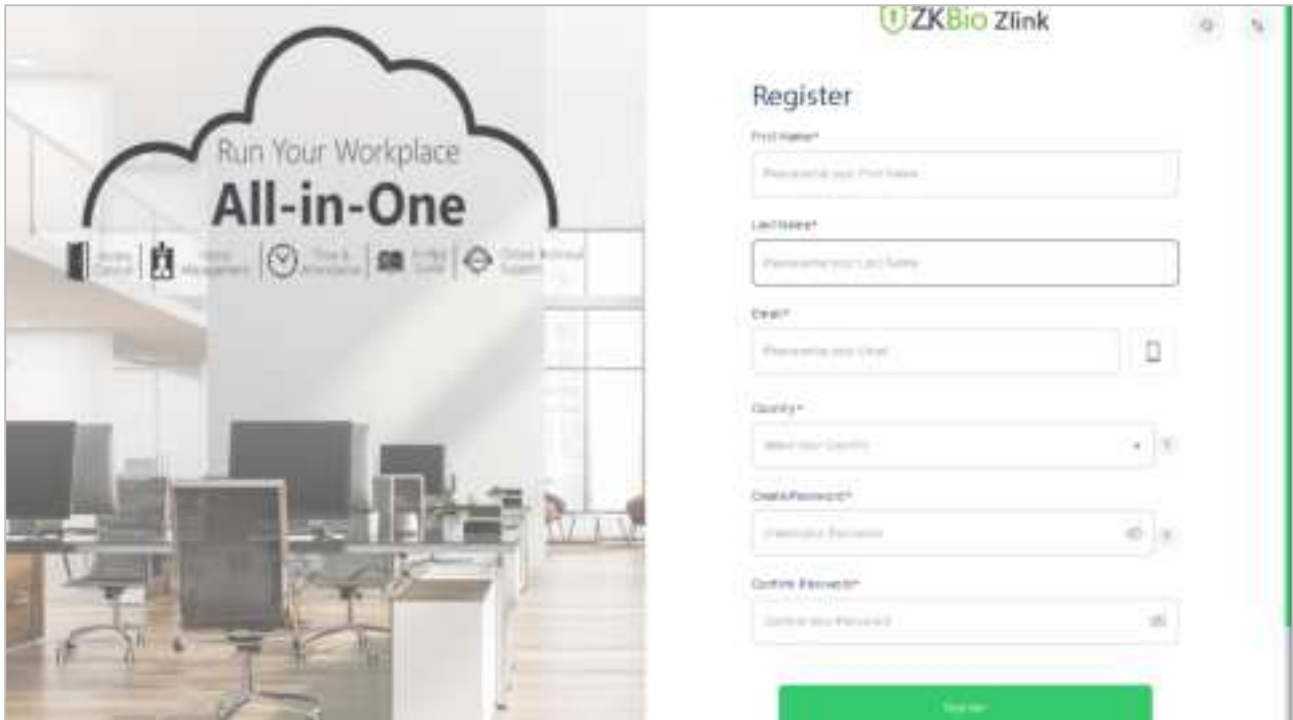


4. Enter user's information and set password, then click **Register**.



The screenshot displays the ZKBio Zlink registration interface. On the left, a background image of an office features a large sign that says "Run Your Workplace All-in-One" with icons for various services. On the right, the "Register" form includes the following fields: "First Name*", "Last Name*", "Email*", "Country*", "Create Password*", and "Confirm Password*". A green "Register" button is positioned at the bottom of the form.

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**.

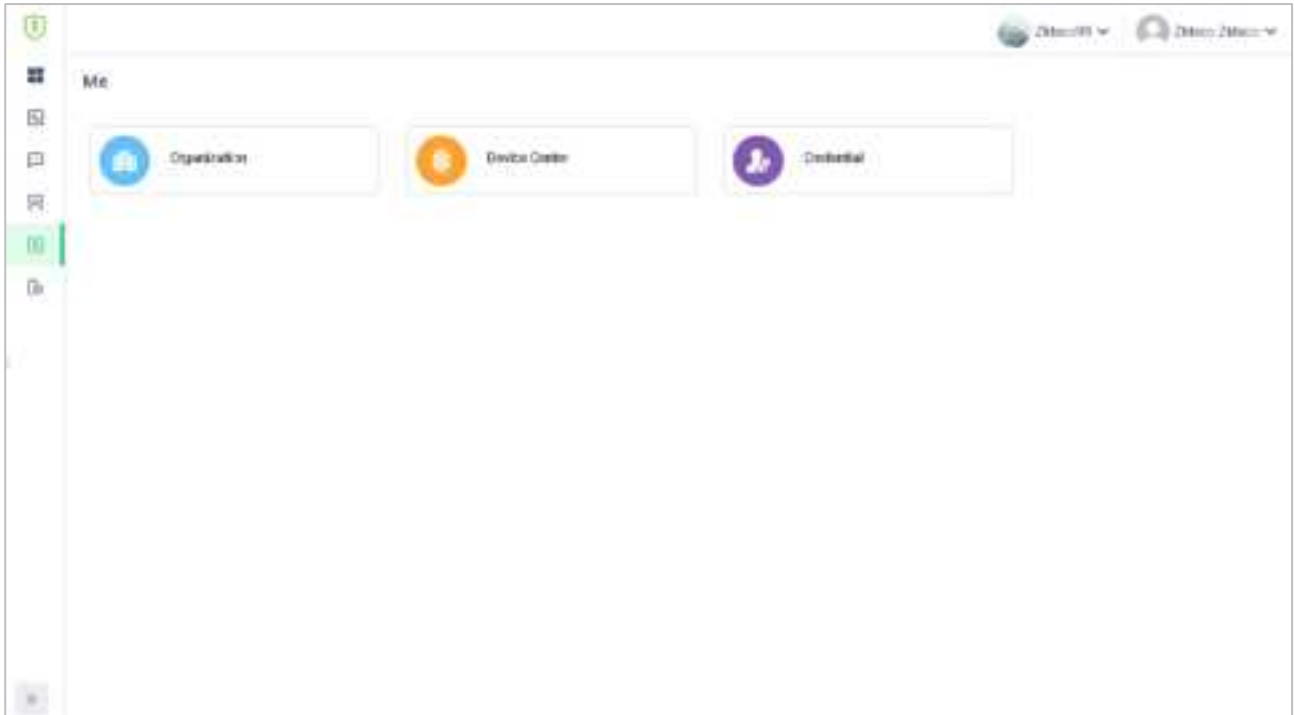



The screenshot shows the ZKBio Zlink "Create Organization" page. The left side features the same office background with the "Run Your Workplace All-in-One" sign. The right side contains the "Create Organization" form with fields for "Organization Name*" and "Organization Code*". A green "Create" button is located below these fields. Underneath the button, there is a link that says "Already have an Organization? Select an Organization".

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).

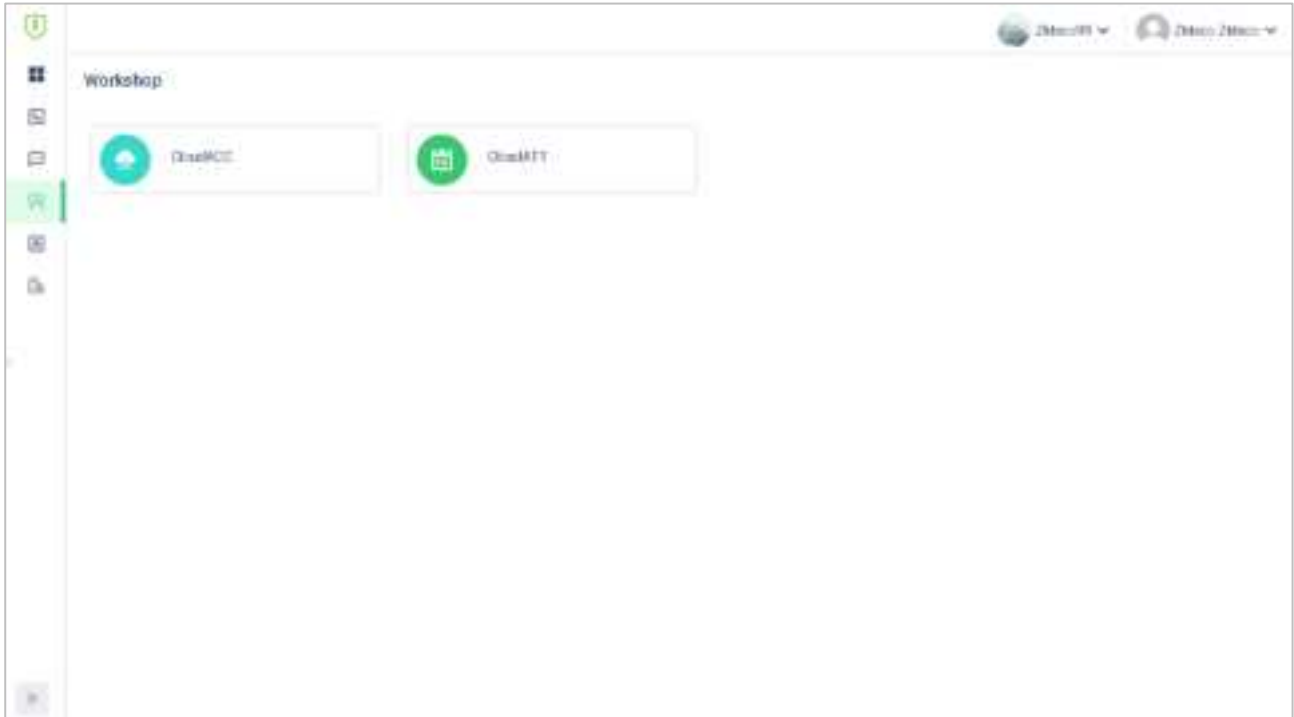


- Enter the person's details and click **Save** (Repeat adding the department, role and permission, job title, site list, and zone list).

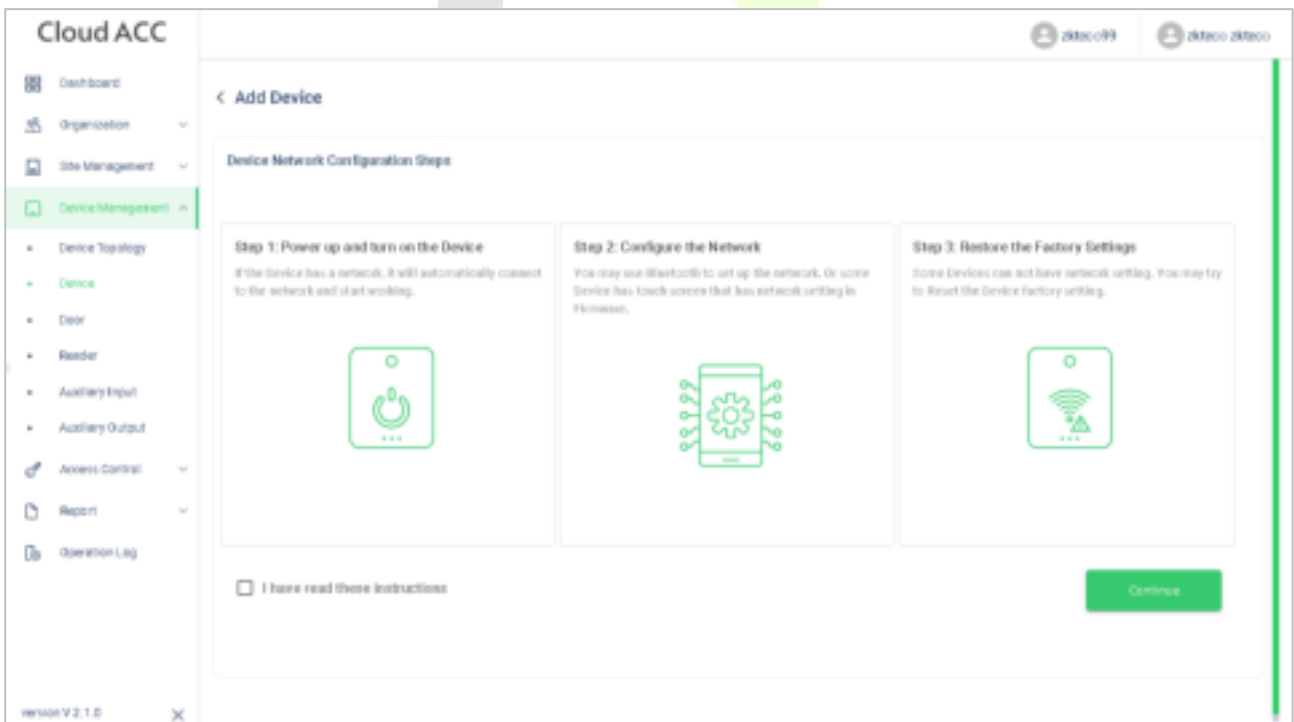
15.2.2 Add Device

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

- 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)

Cloud ACC

< Add Device

Manual Register Device

View Manual Register Device Helpdesk

1. Plug in the device to the Cloud ACC and power it on.
 2. Enter the device's serial number (found on the back of the device) into the 'Device Serial Number' field.
 3. Click the 'Add' button to add the device to the system.
 4. The device will be added to the system.

Device Serial Number

Please Enter Device Serial Number

Add

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

Bind devices to your company

6183202600003

Please specify the device to a site.

This device will sync the same time zone (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi, Kuala Lumpur, Singapore) of the site.

Site: Site_1

Zone: Zone_1

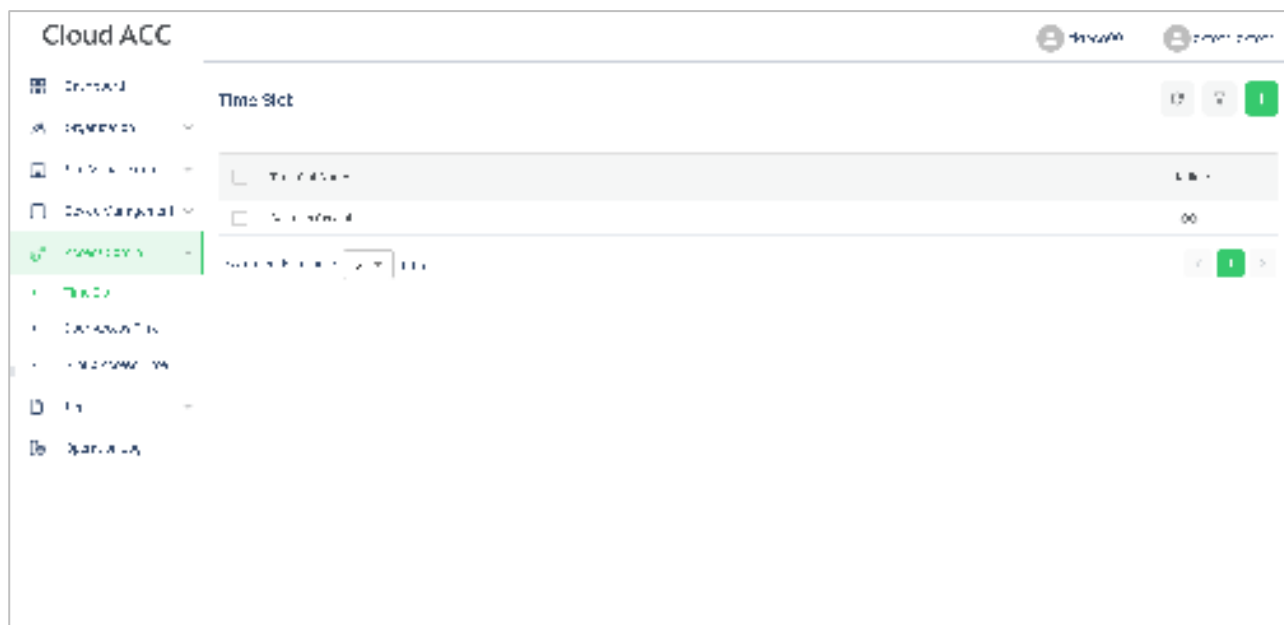
Save Cancel


15.3 Time Slot

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

15.3.1 Set Time Slot

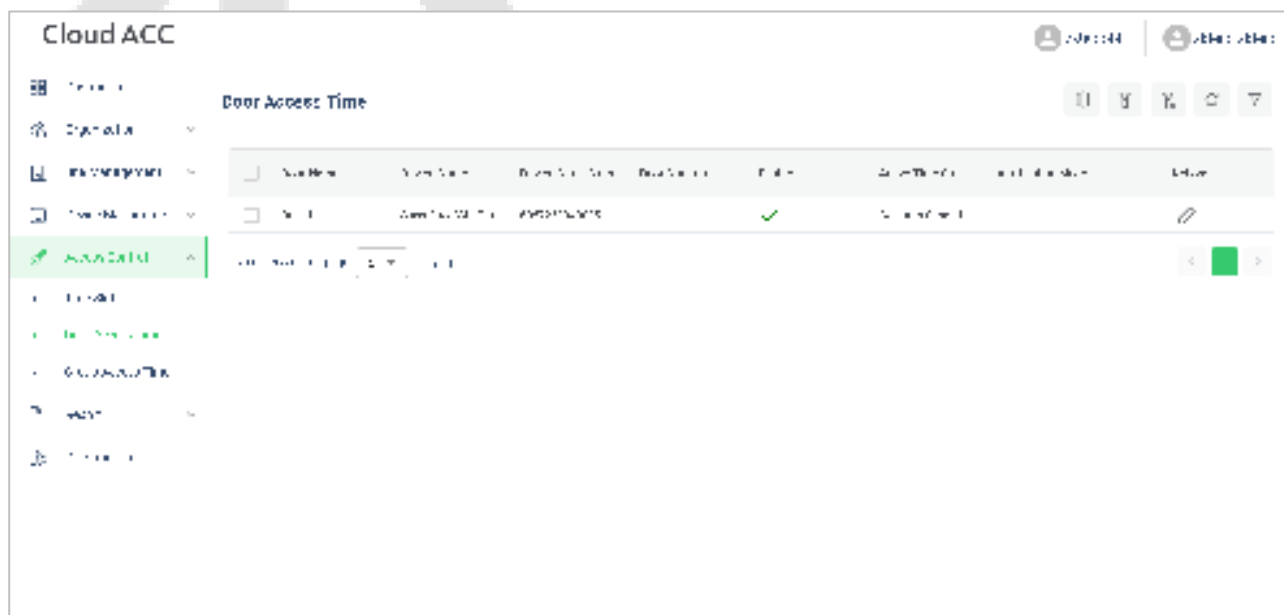
In **ZKBio Cloud Access** interface, click **Access Control > Time Slots** to set time slot.



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

15.3.2 Set Door Access Time

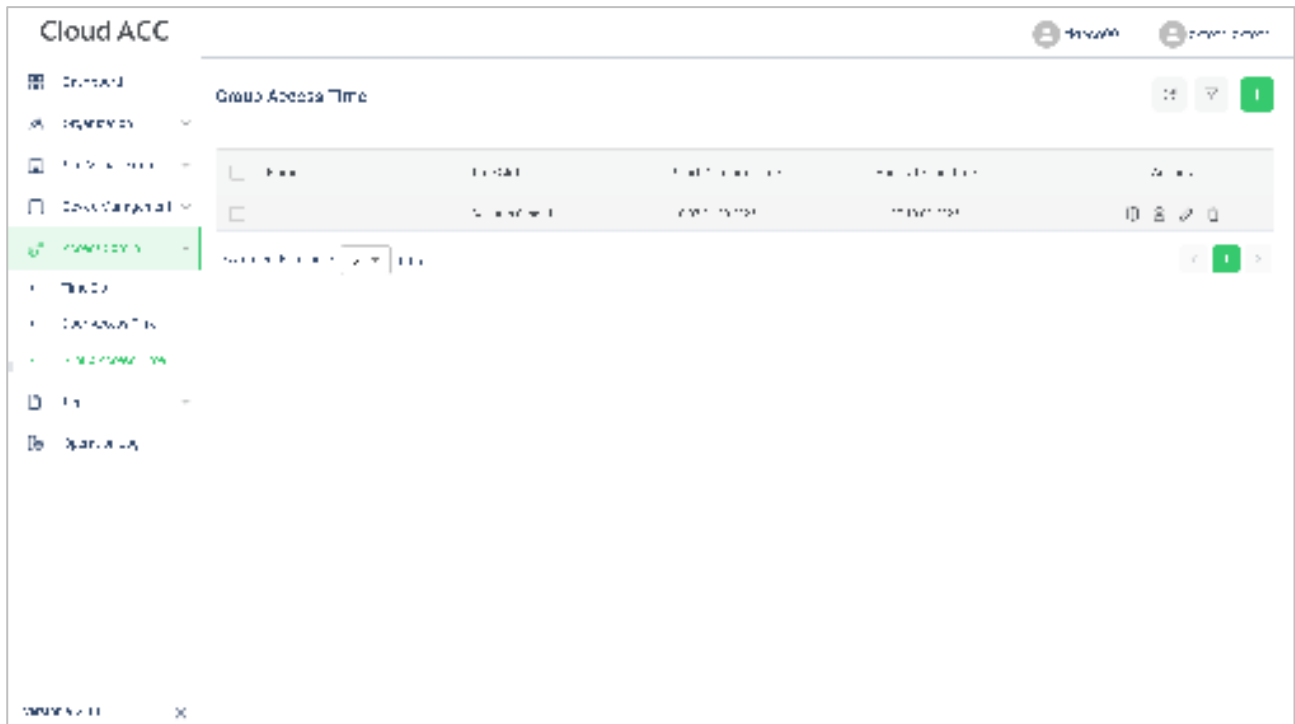
In **ZKBio Cloud Access** interface, click **Access Control > Door Access Time** and click  to allocate a time slot to this door.




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.

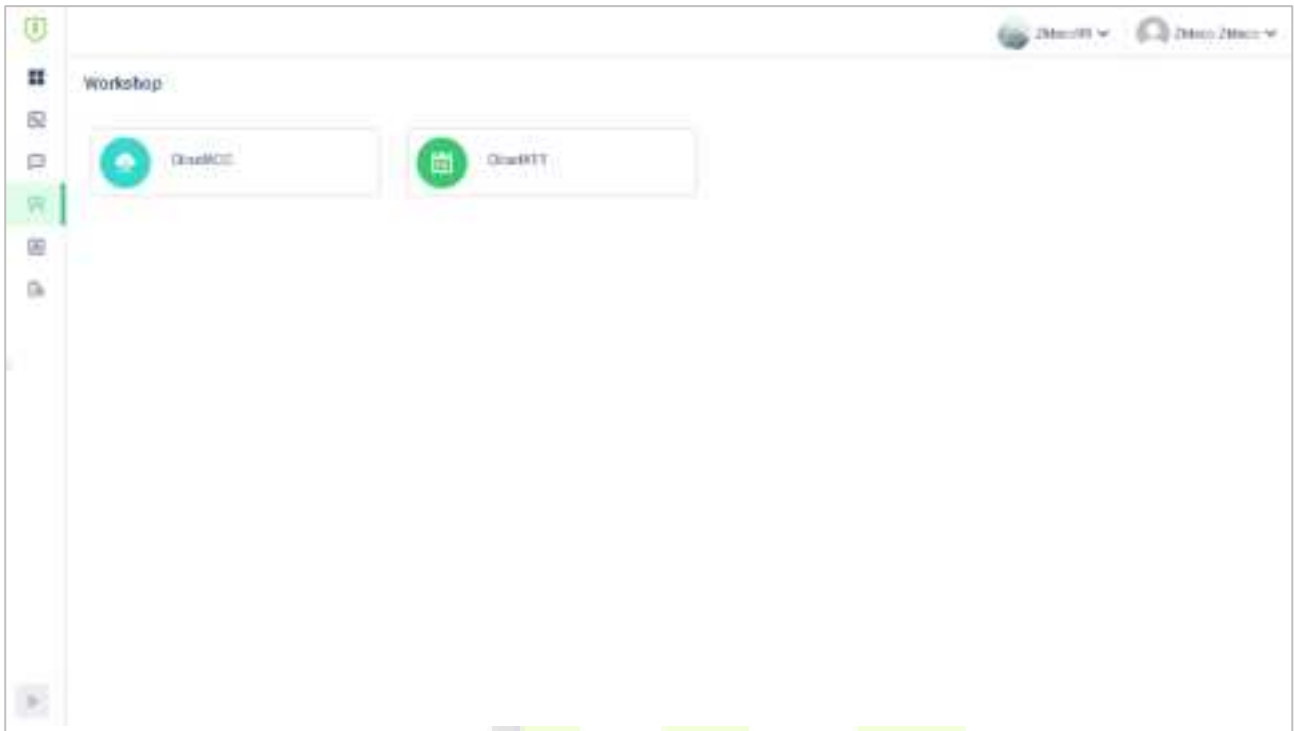
Click  to allocate person to this group.

Click  to allocate a time slot to this group.

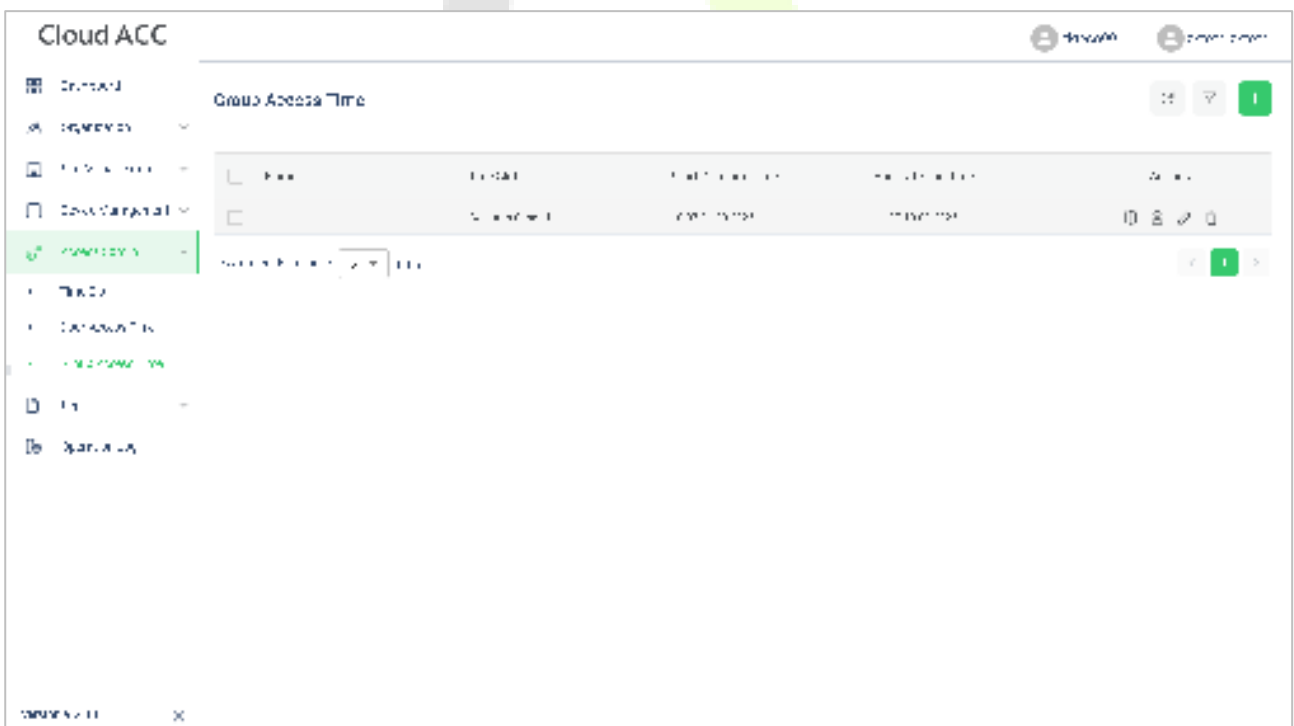
Click  to delete this group.

15.4 Synchronize Person to Device

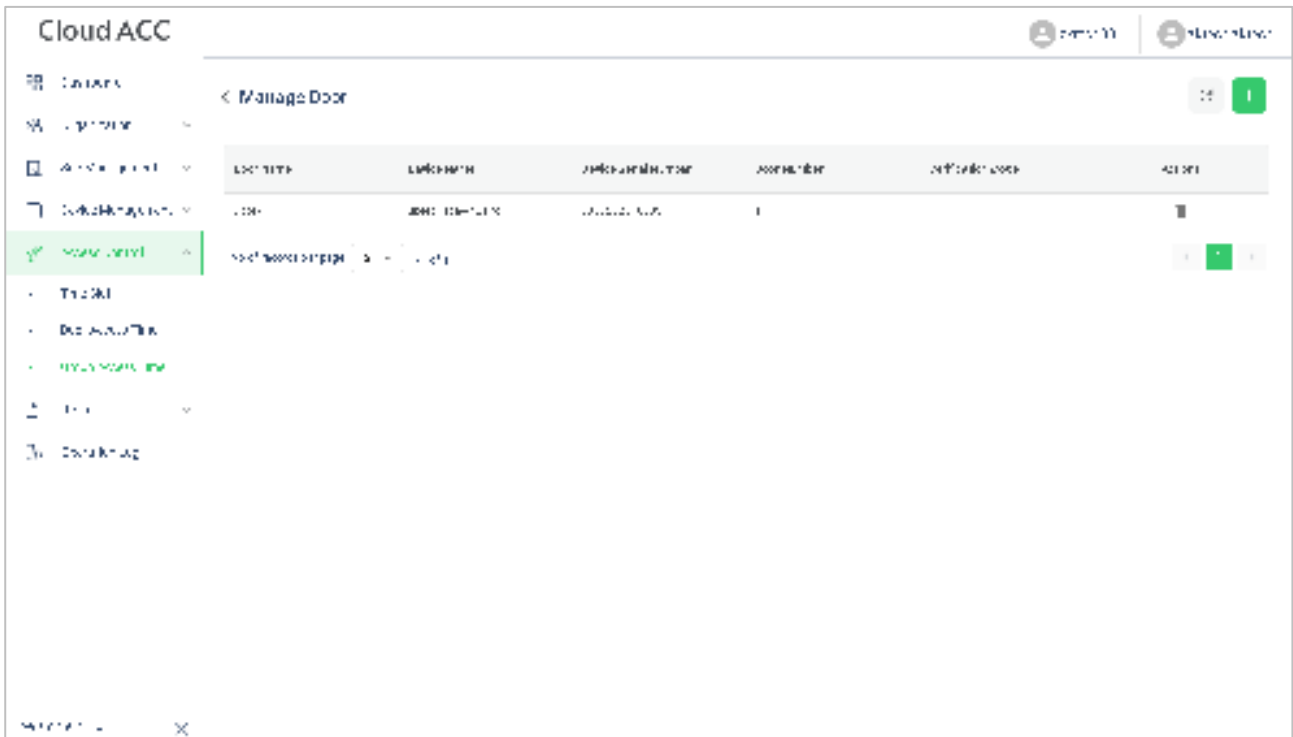
1. Click **Workshop > CloudACC** on the main menu to enter the **ZKBio Cloud Access** interface.



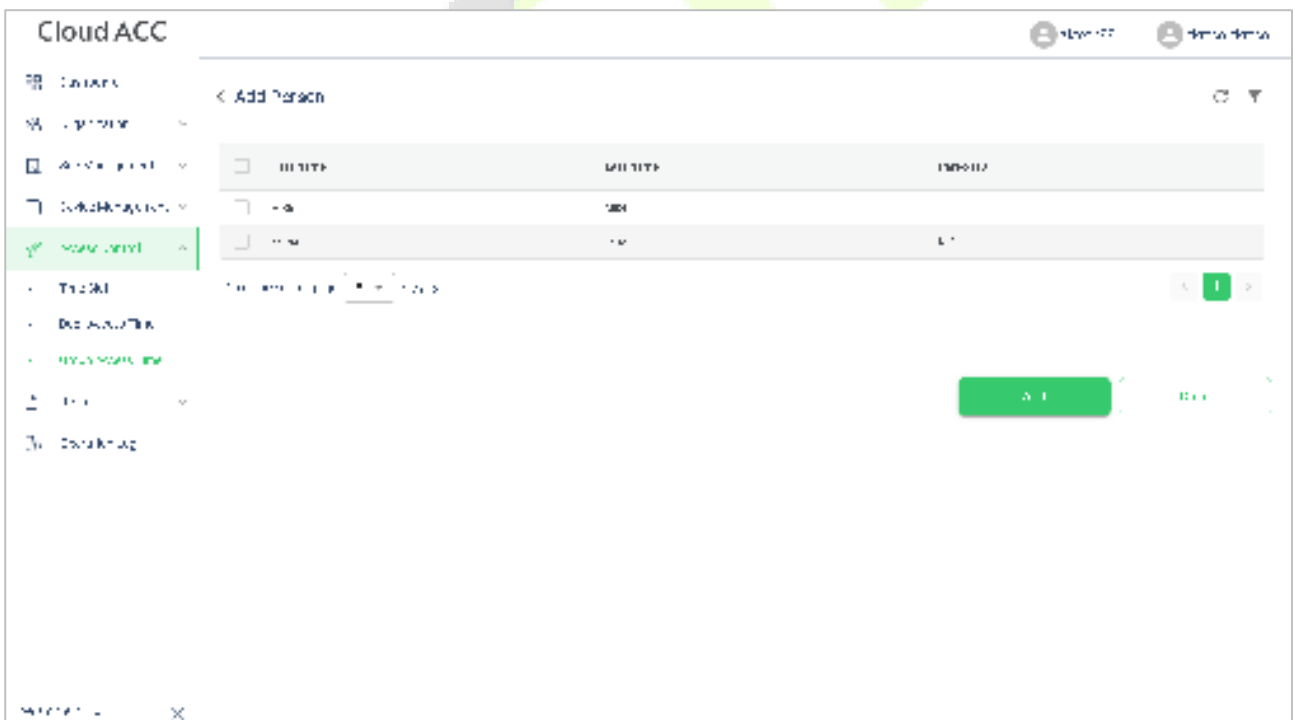
2. Click **Access Control > Group Access Time**.



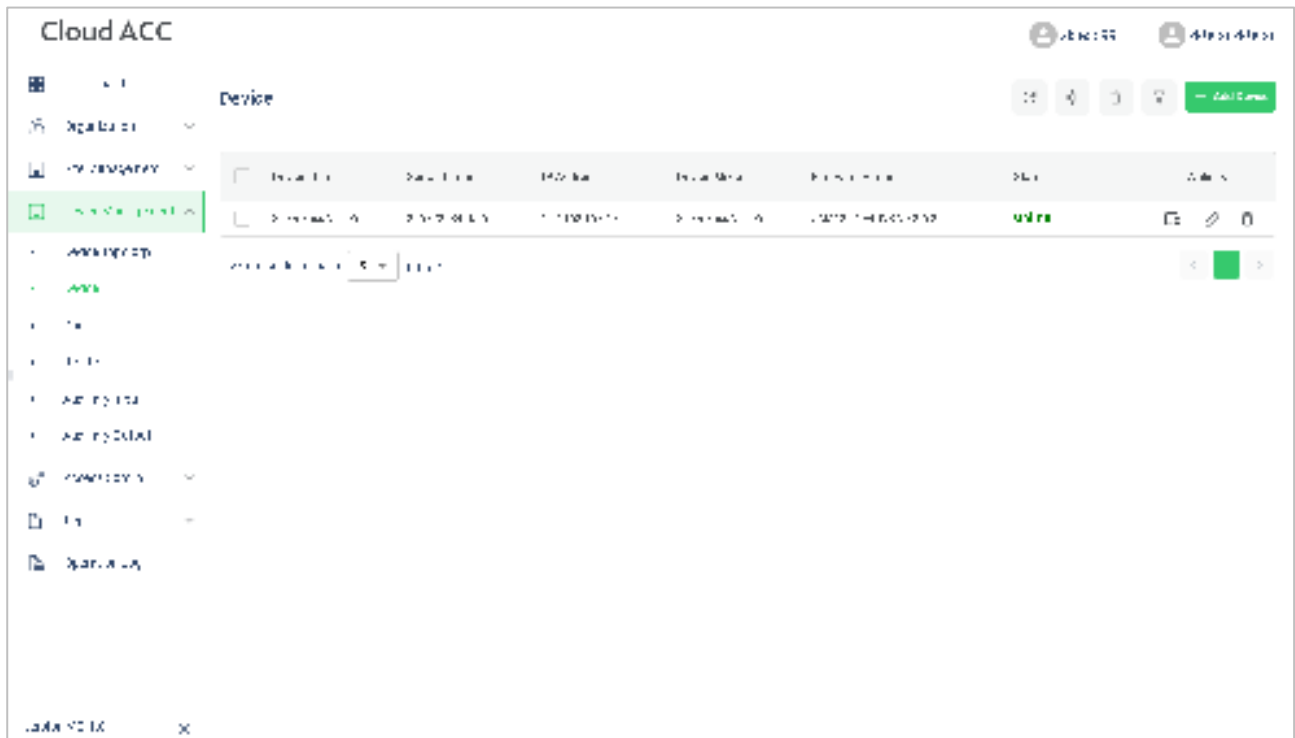
3. Click  >  to choose a device.



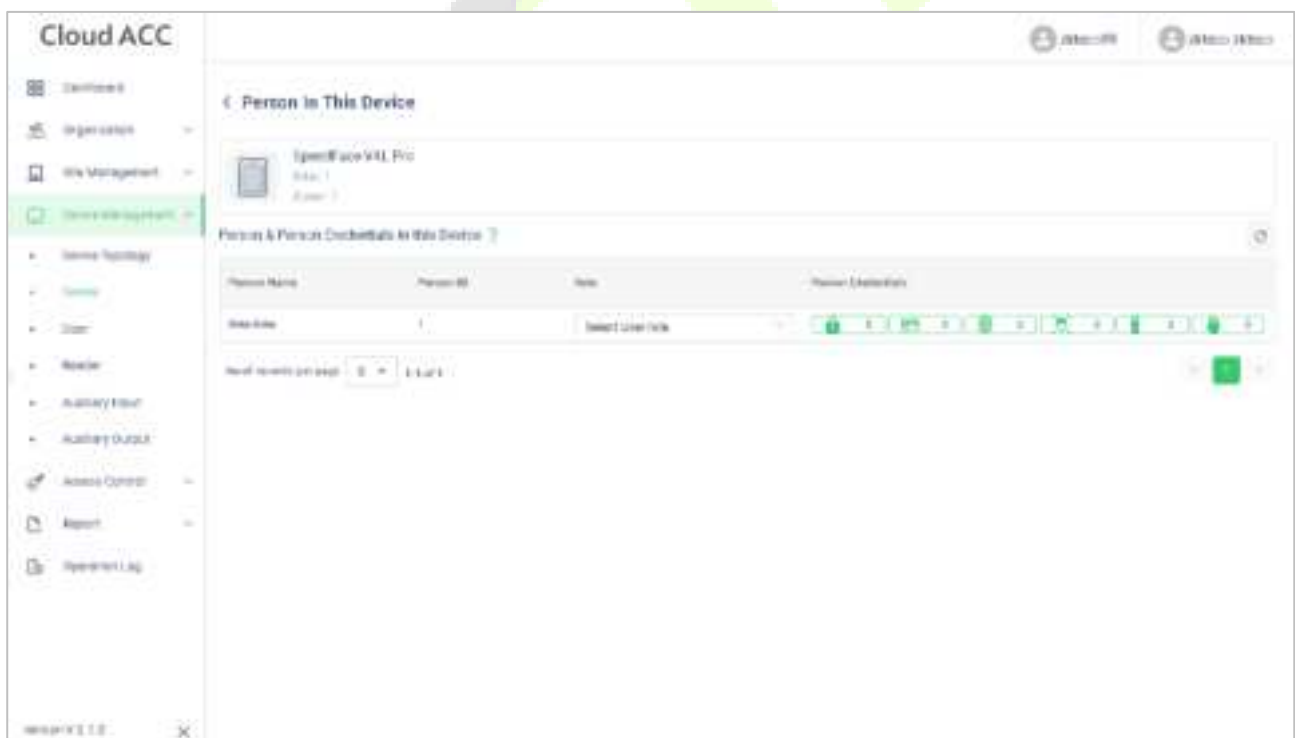
4. Click  >  to allocate person to this device.



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



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




15.5 User Registration

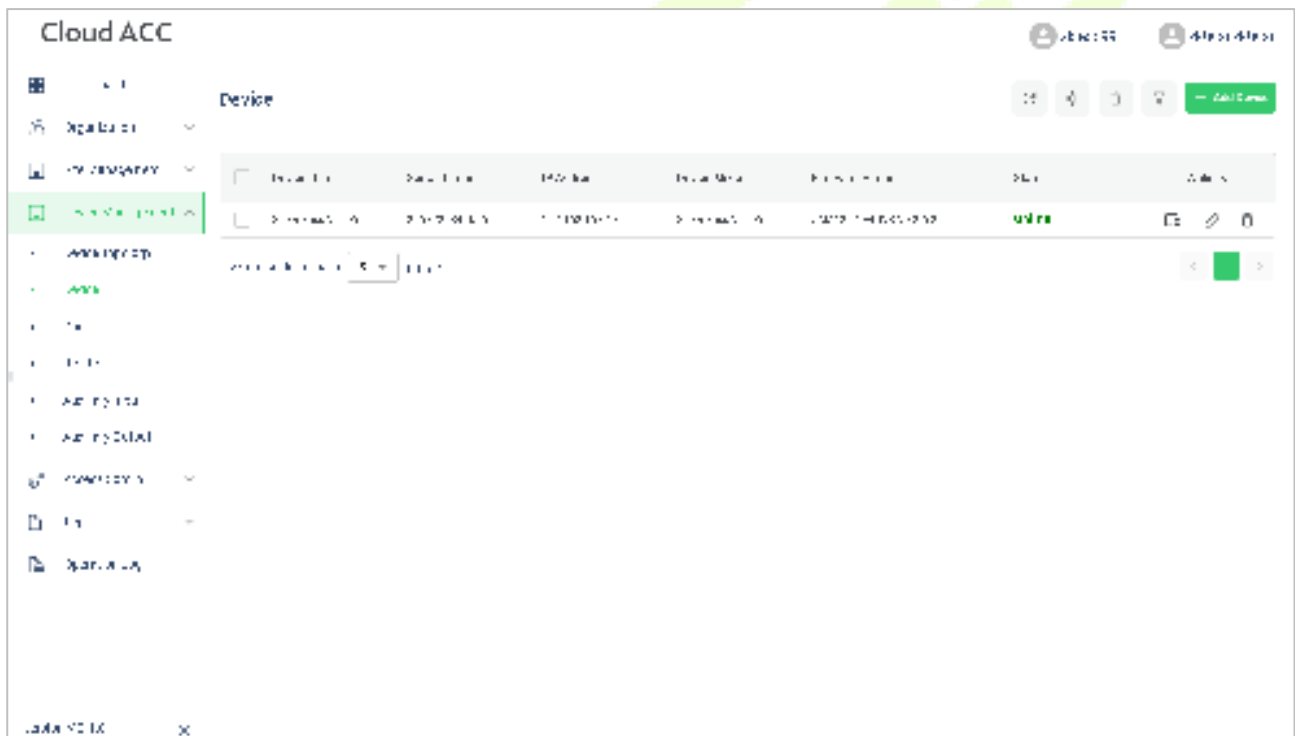
15.5.1 Register a User ID and Name

Please refer to [15.2.1 Set Organization](#).

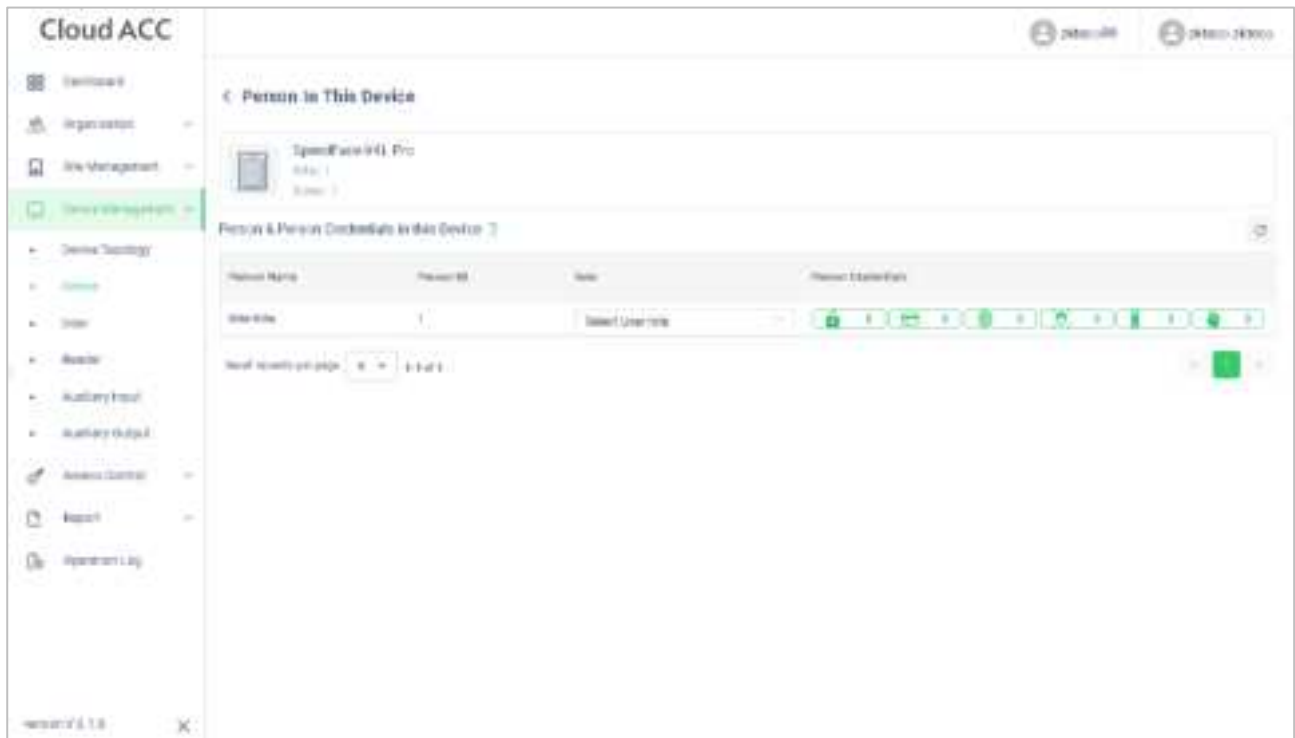
15.5.2 Setting the User Role

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.

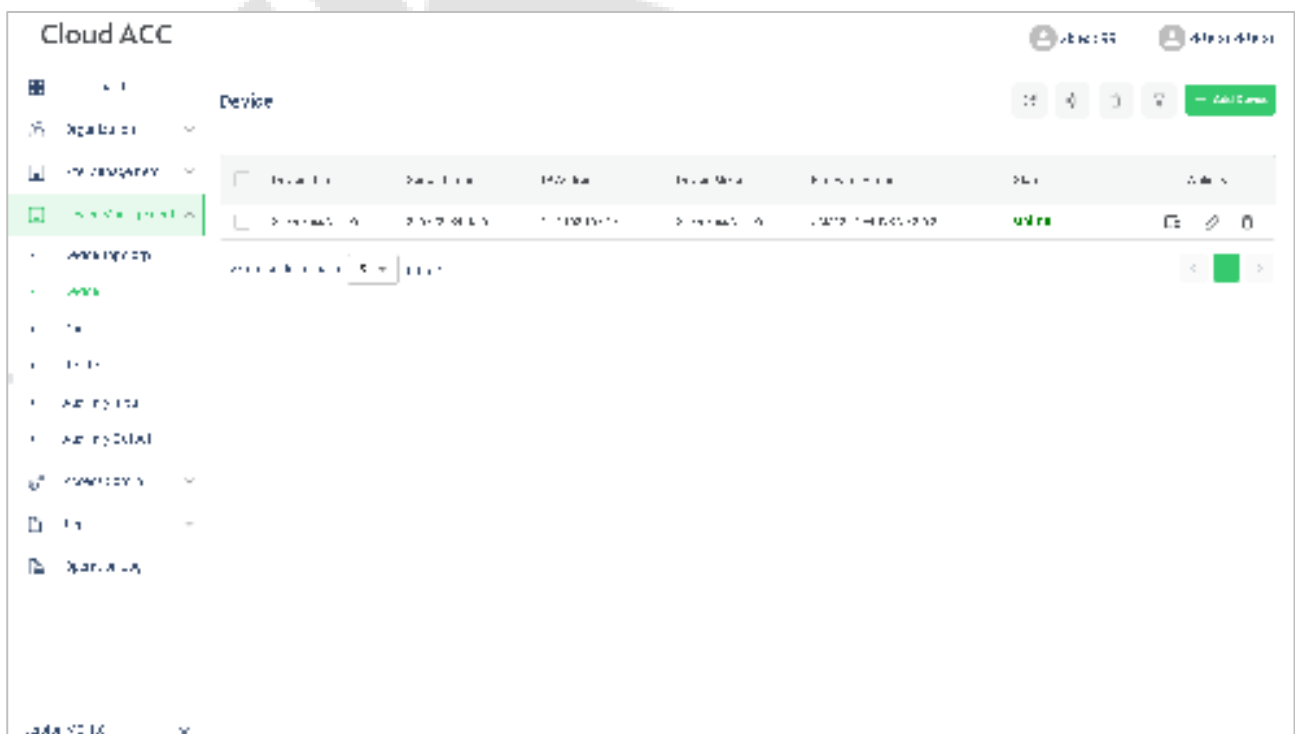


3. Choose the **Select User** role.

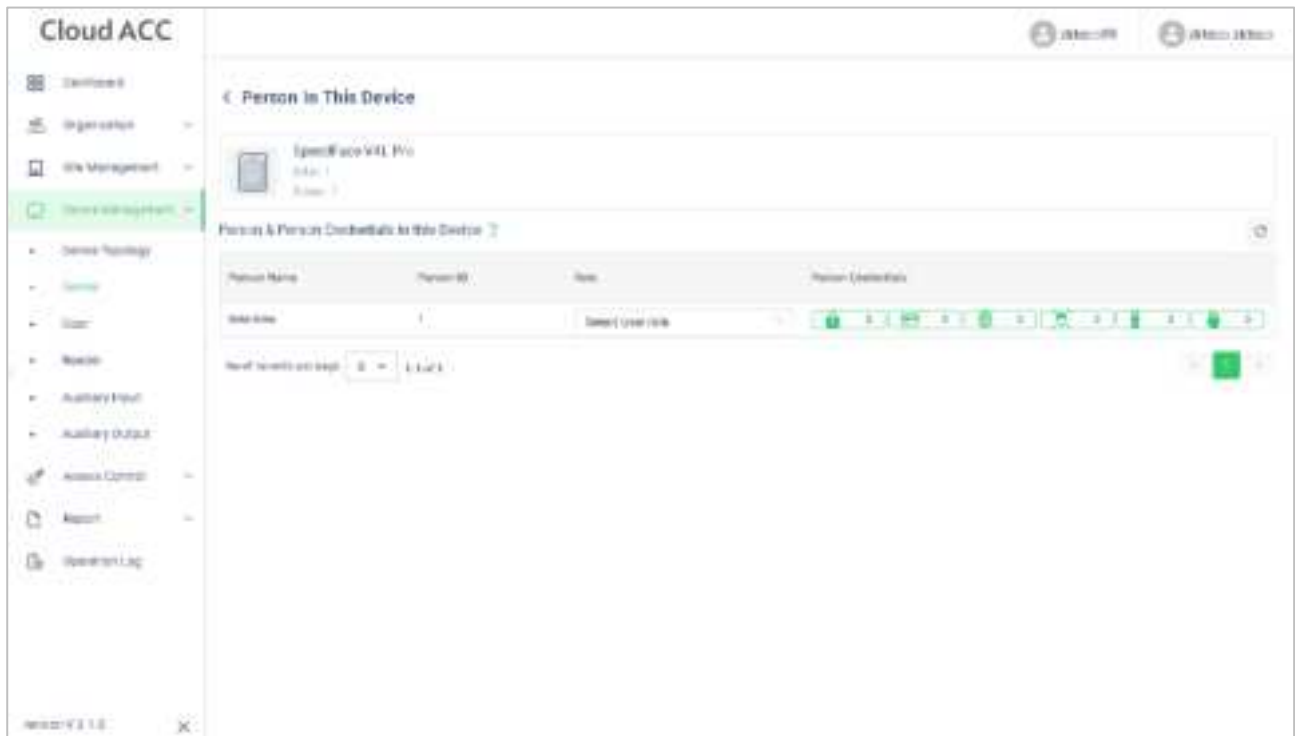


15.5.3 Register Fingerprint

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.




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

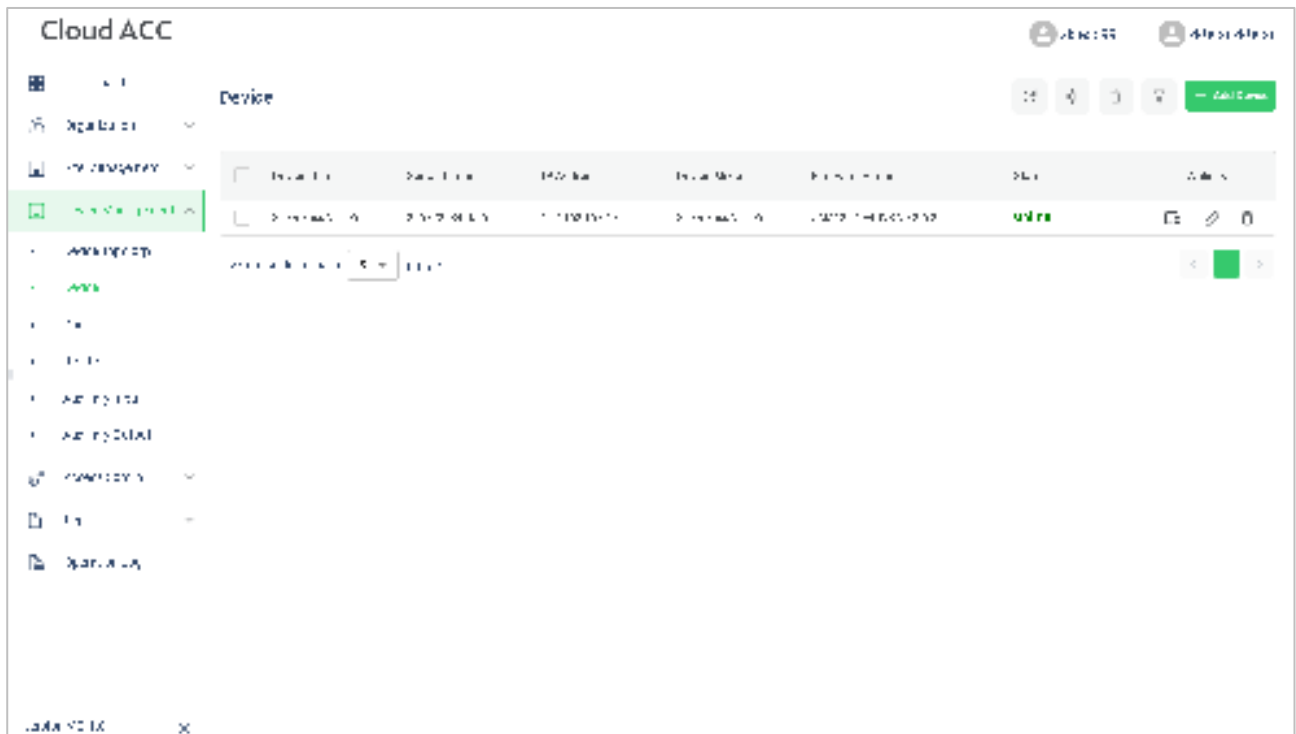


4. Press the same finger on the fingerprint reader three times. Green indicates that the fingerprint was enrolled successfully.

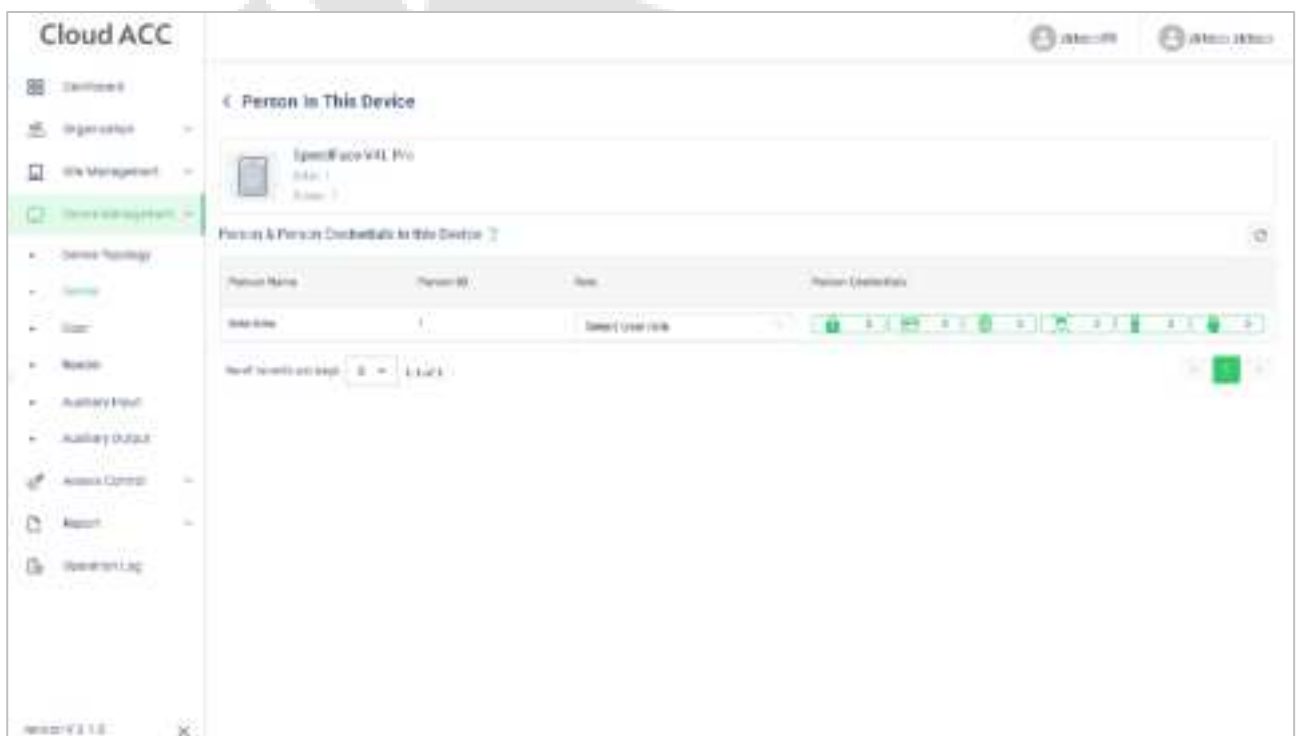


15.5.4 Register Face Template

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.

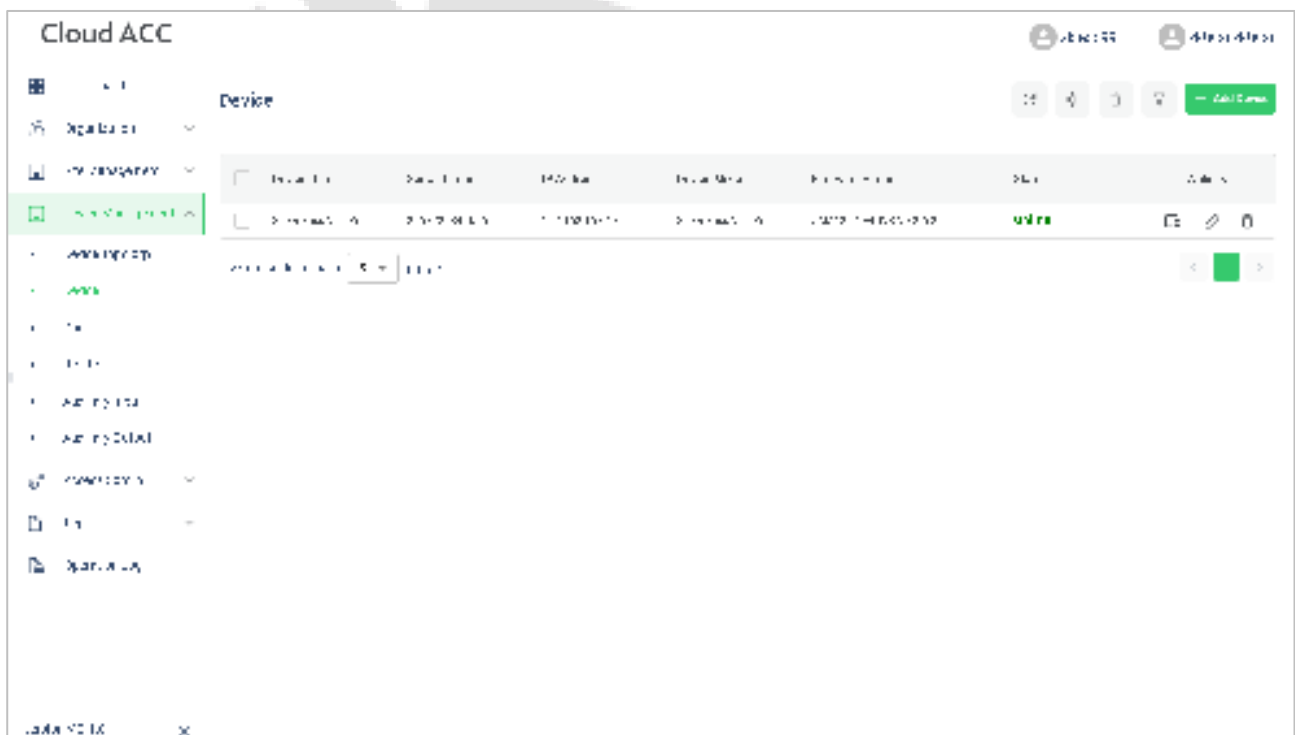


The registration interface is as follows:

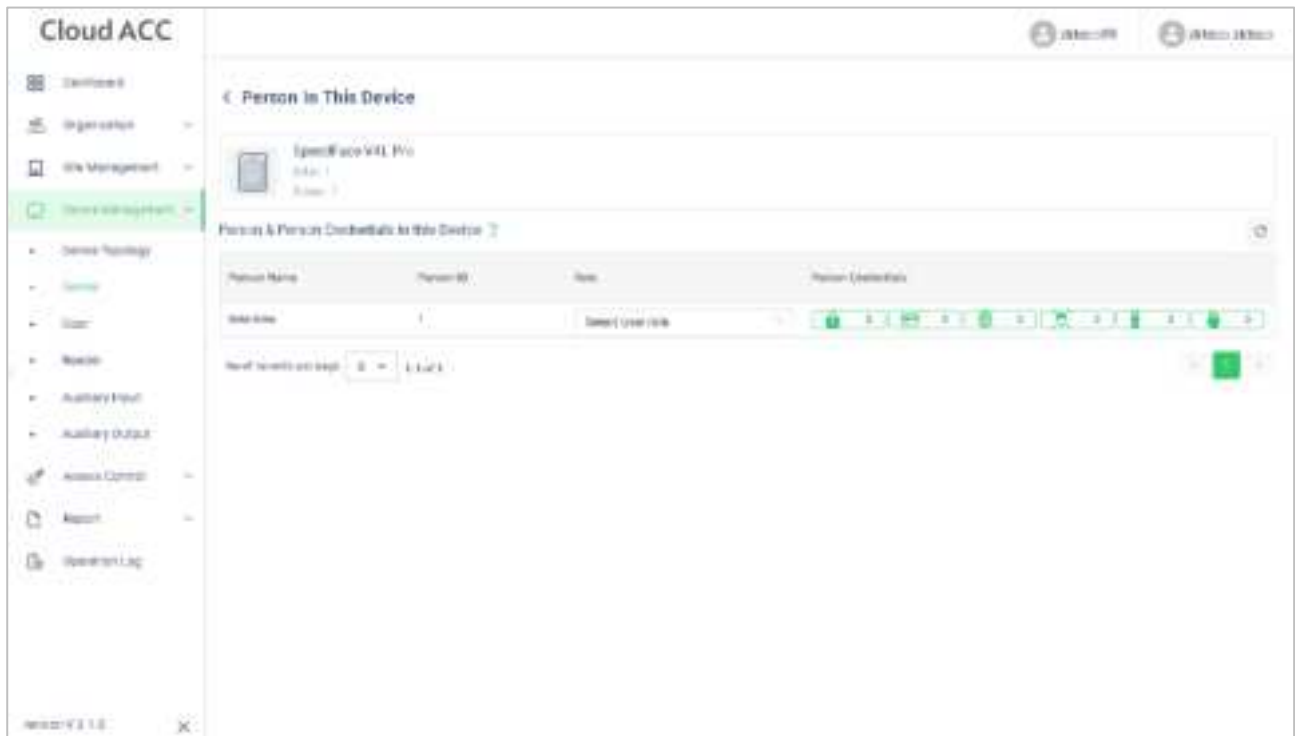


15.5.5 Register Password

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.




3. Click  icon to register password on the device.

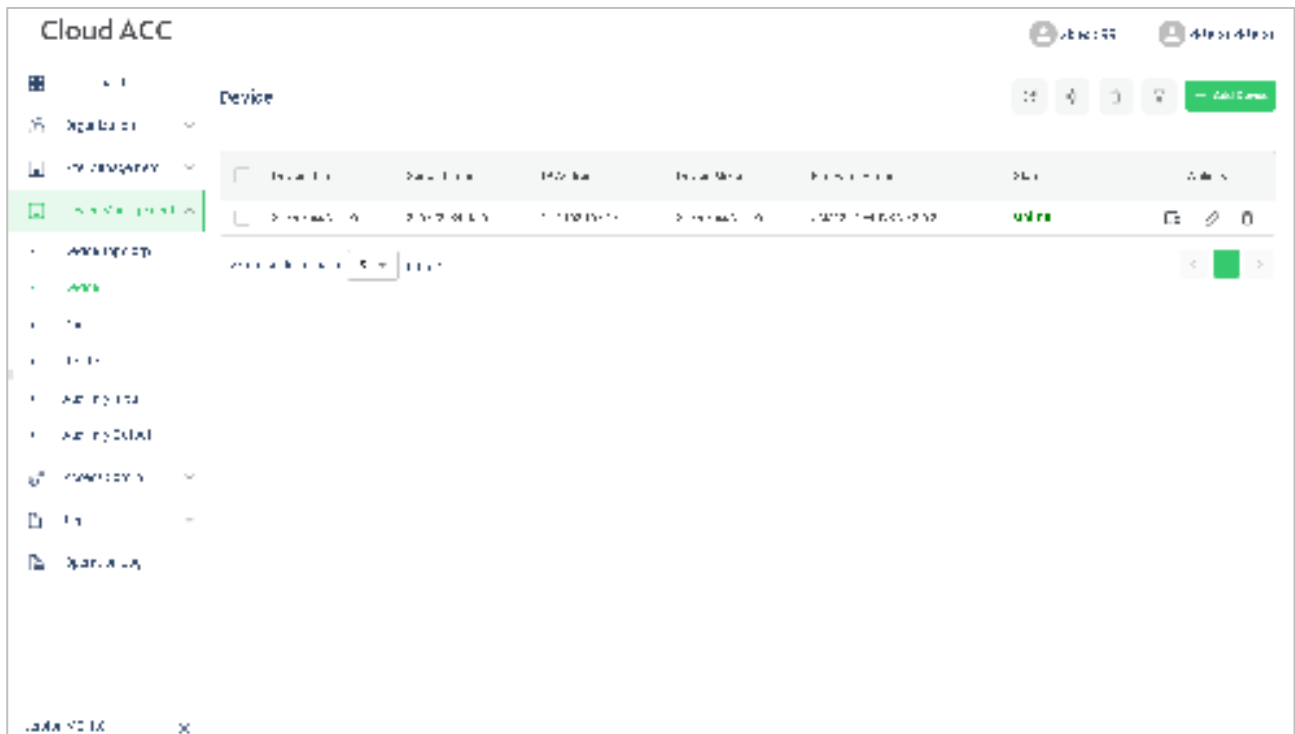


The registration interface is as follows:

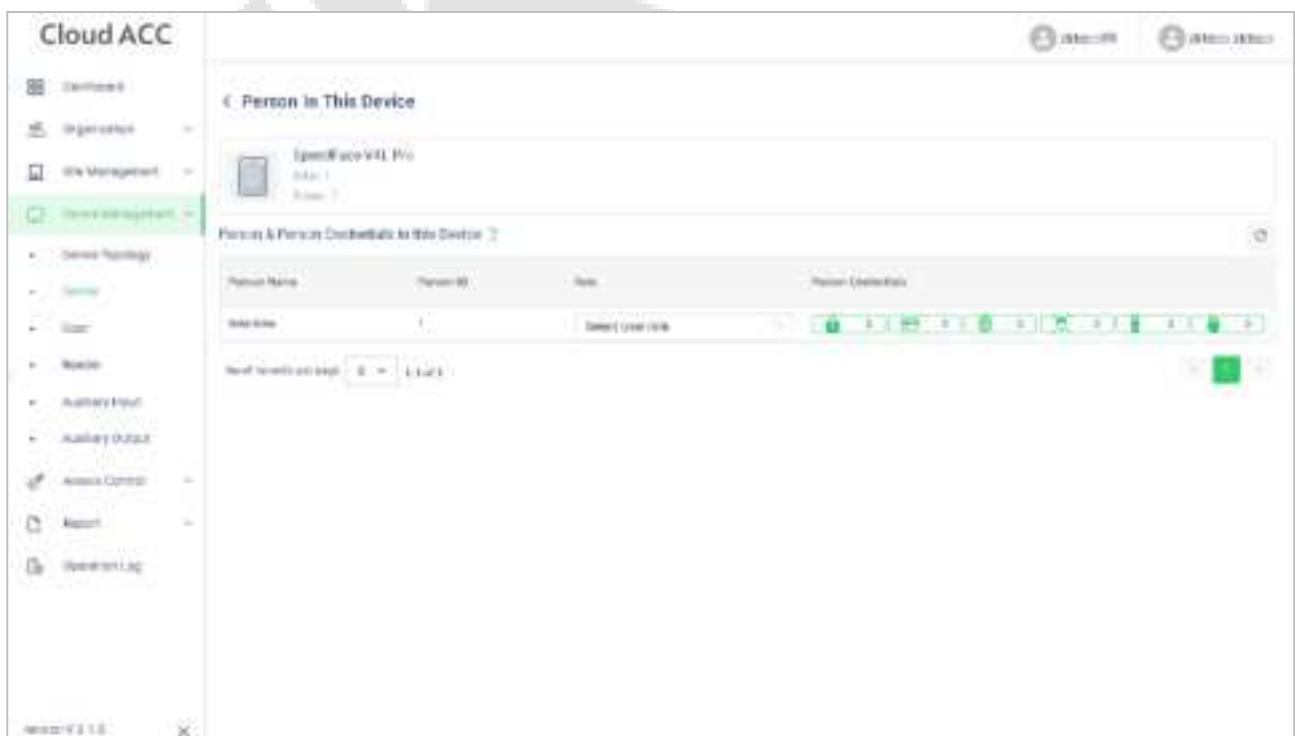
Note: The password may contain one to eight digits by default.

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.



3. Click  icon to register password on the device.



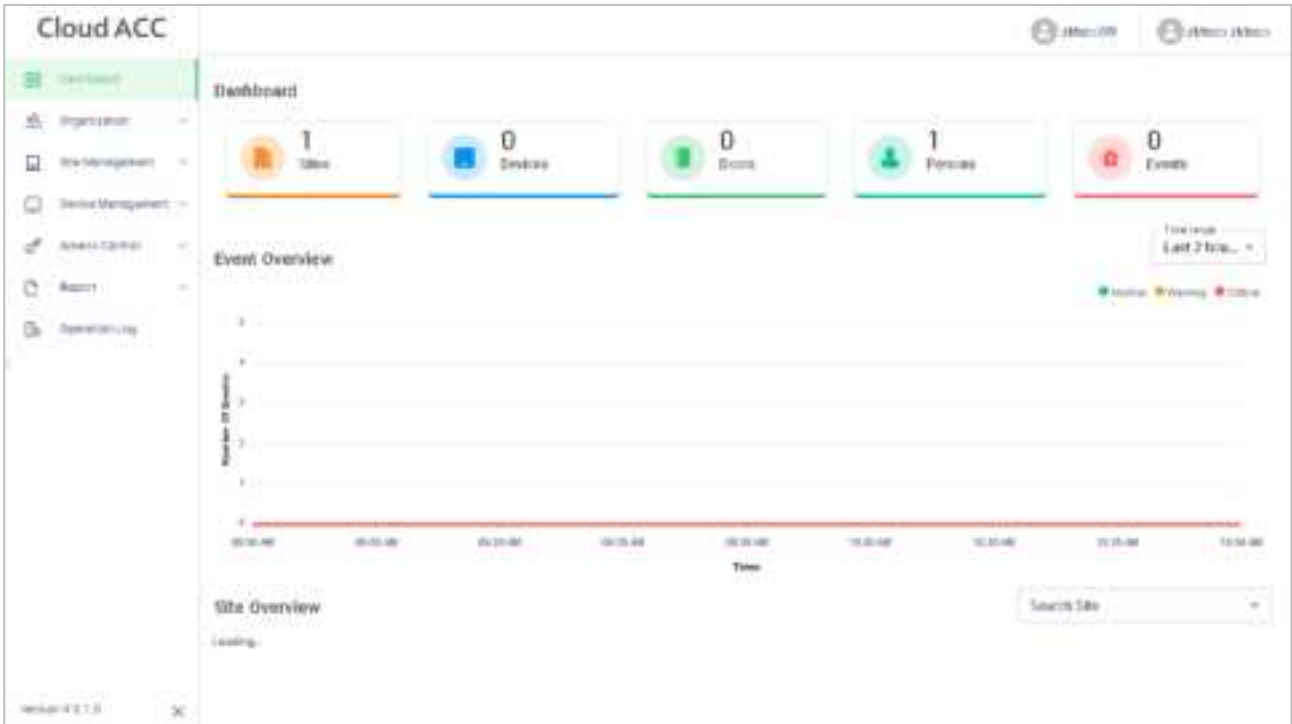
The registration interface is as follows:



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.

The screenshot shows the 'Cloud ACC' interface with the 'Events' report selected. It displays a table of event records. The table has columns: Event ID, Location, Device Name, Device ID, Door ID, Event Type, Event Time, and Device Name. The data is filtered to show events for '10220'.

Event ID	Location	Device Name	Device ID	Door ID	Event Type	Event Time	Device Name
10220		1000000000	1000000000	1000000000	1		
		1000000000	1000000000	1000000000	1		
		1000000000	1000000000	1000000000	1		
		1000000000	1000000000	1000000000	1		
		1000000000	1000000000	1000000000	1		

At the bottom, there is a pagination bar showing '10/10' and a search bar.

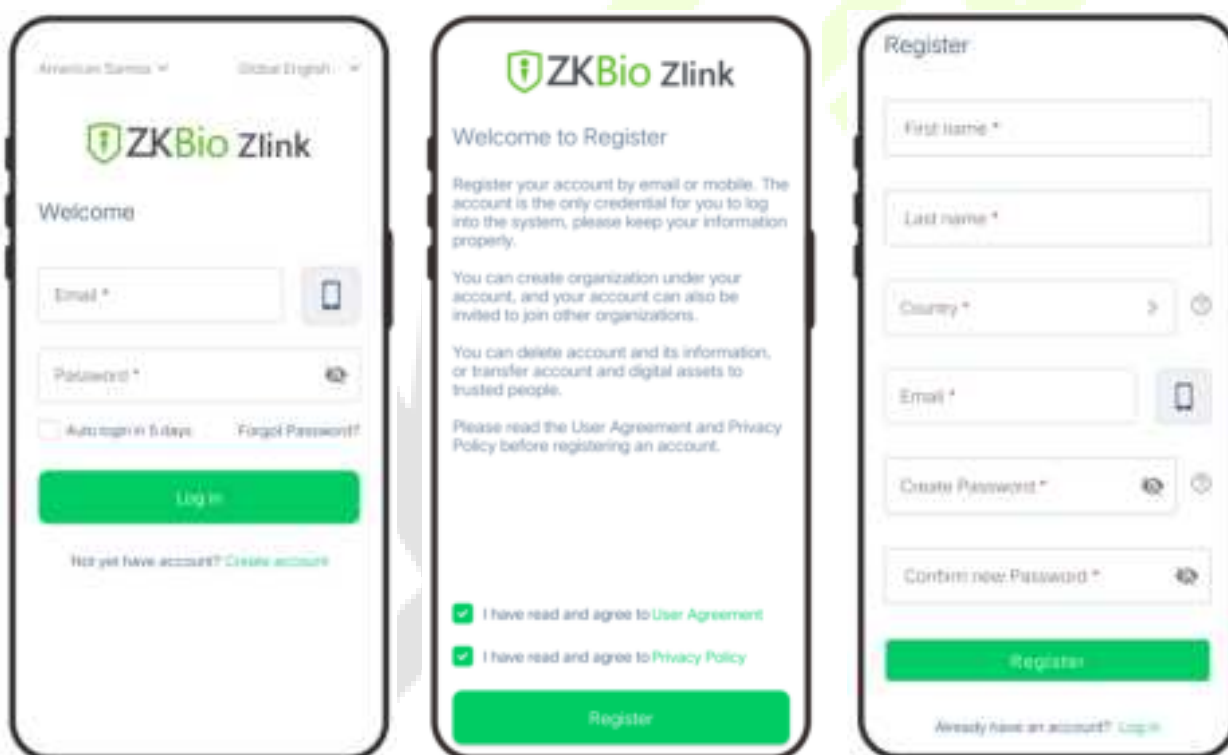
16 Connecting to ZKBio Zlink App

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

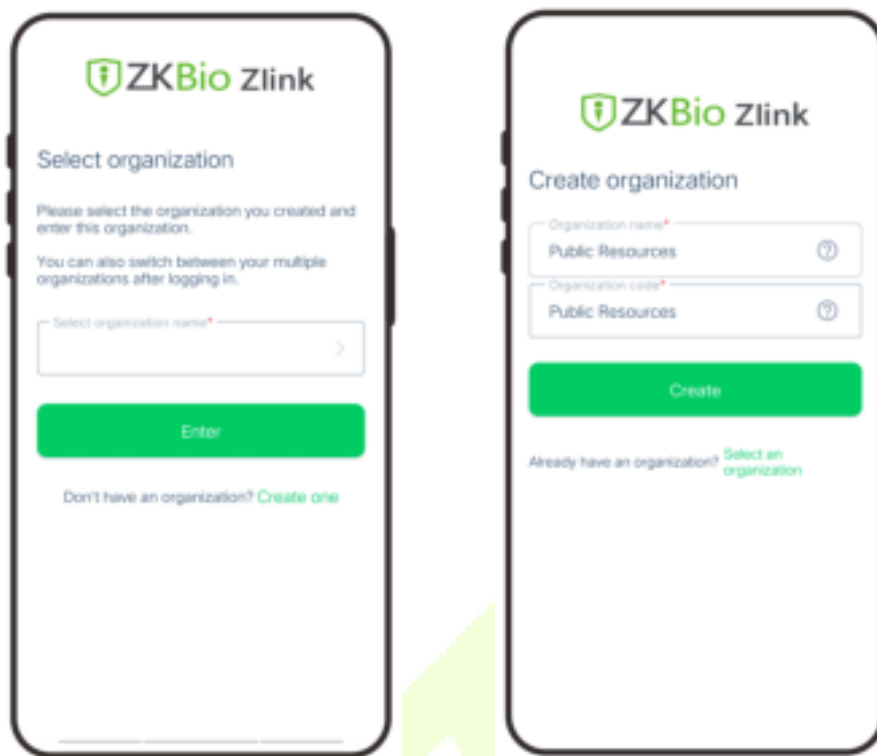
Users can use the created account to access ZKBio Zlink App to connect devices, unlock the device remotely and query records.

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**.

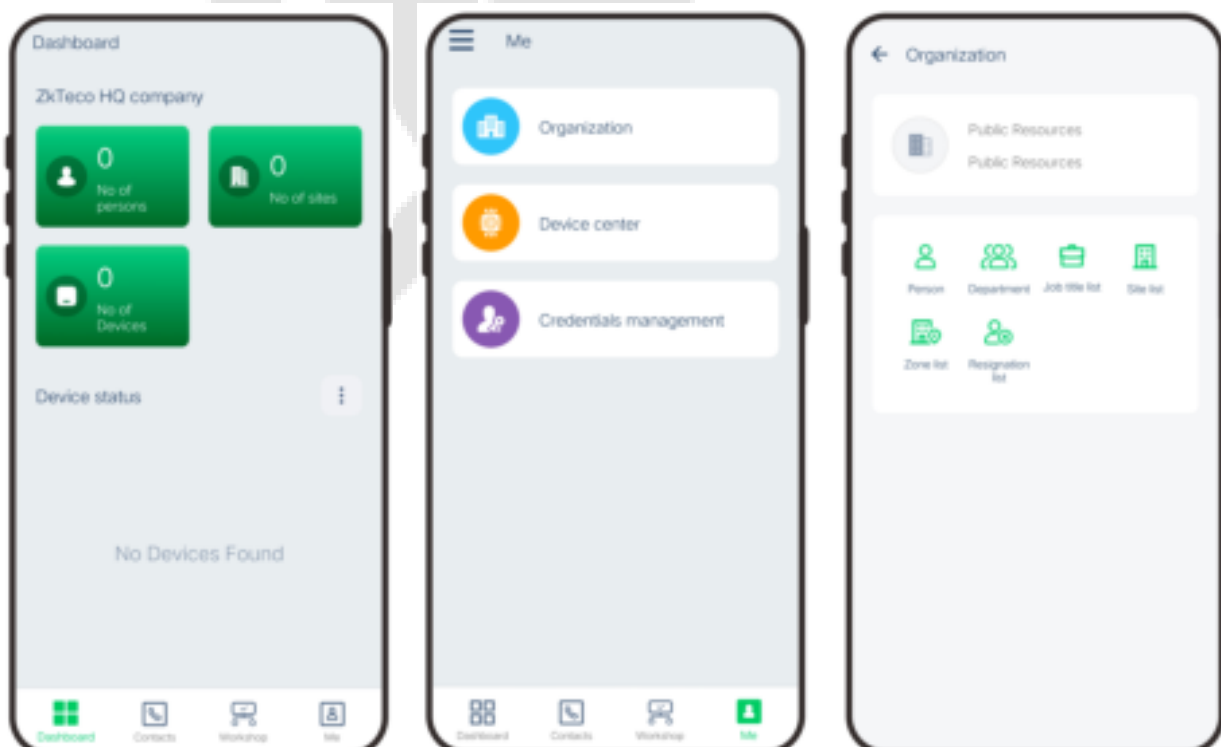


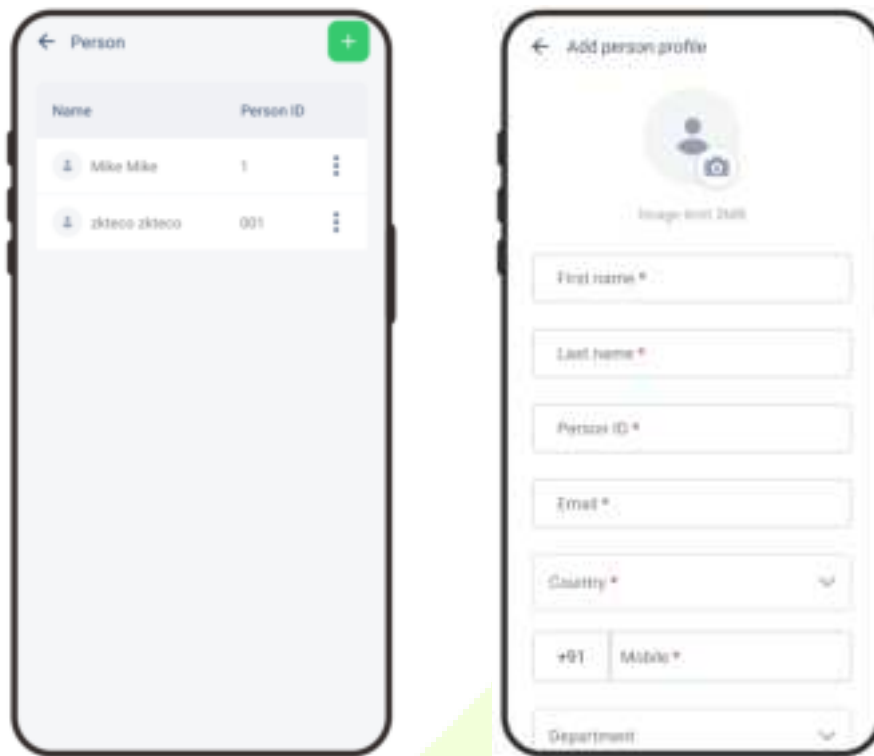
- Choose an organization, click **Enter**, then complete registration. If you do not have an organization, please click **Create one**.



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**.

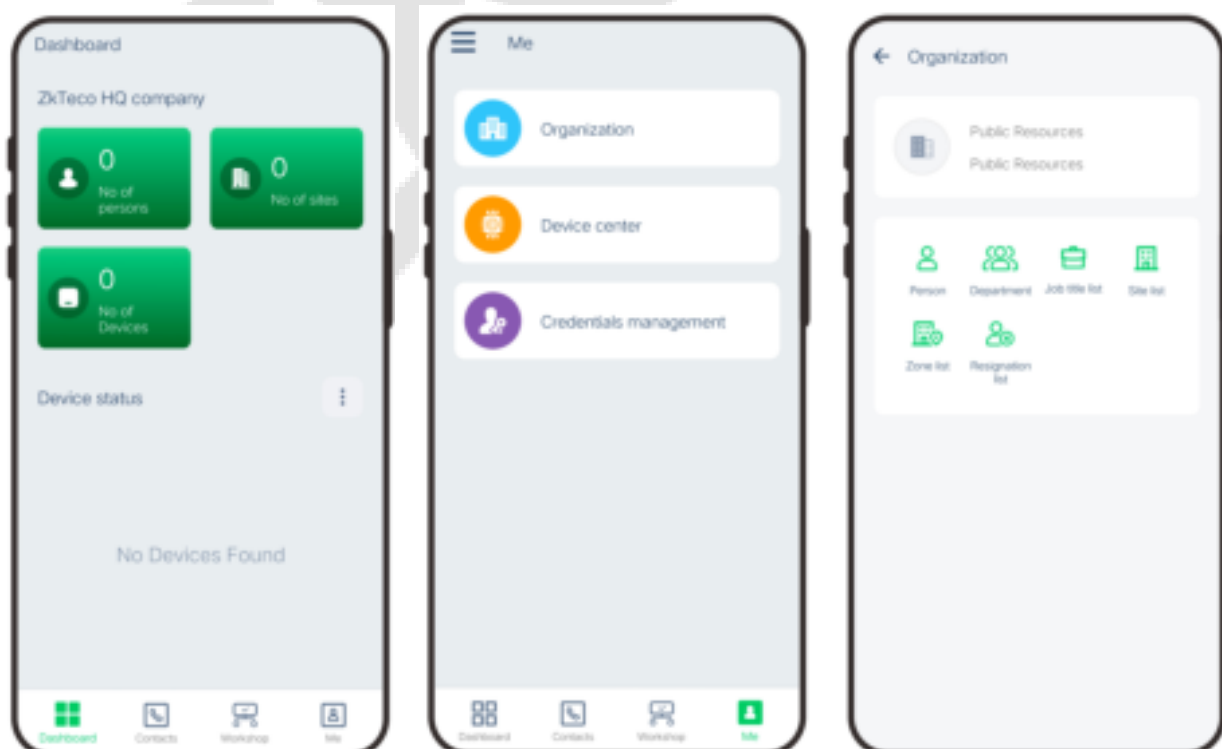


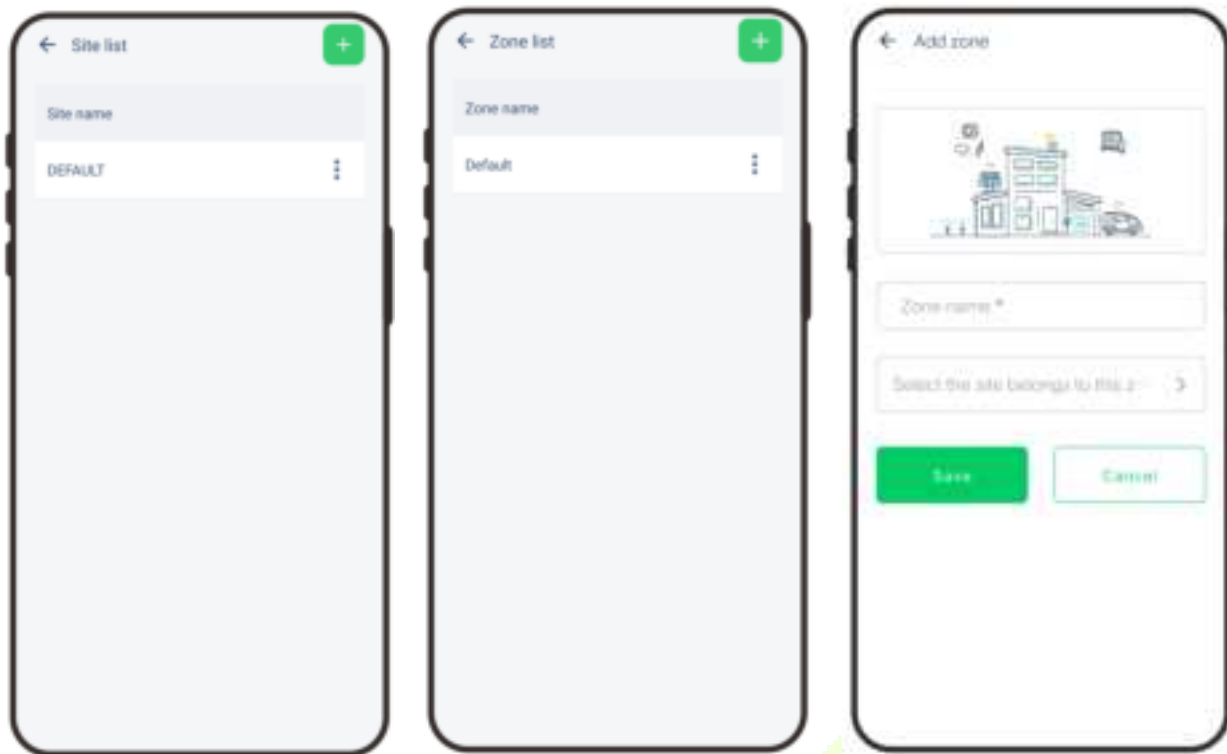


16.3 Add Device

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**.






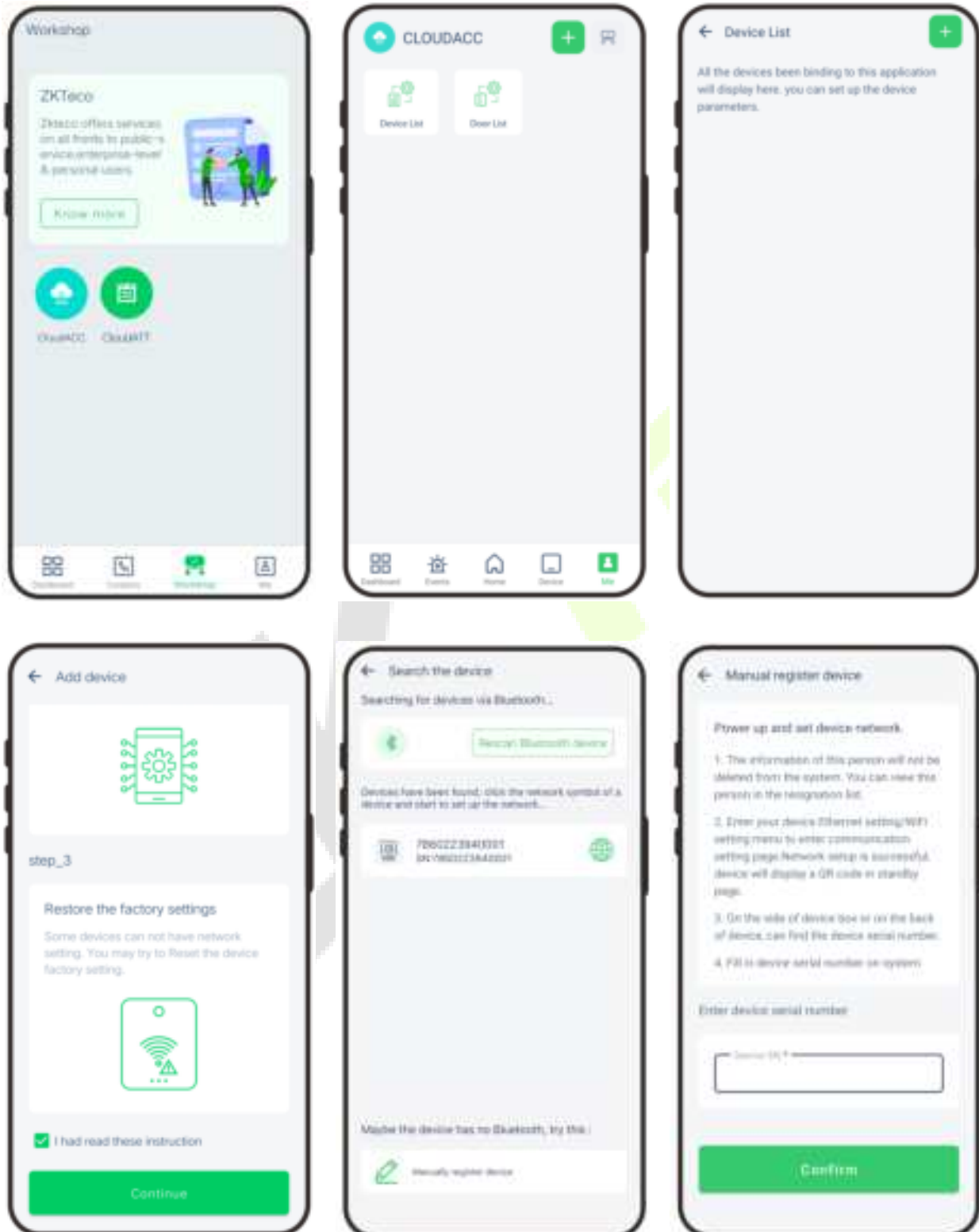
16.3.2 Add Device

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

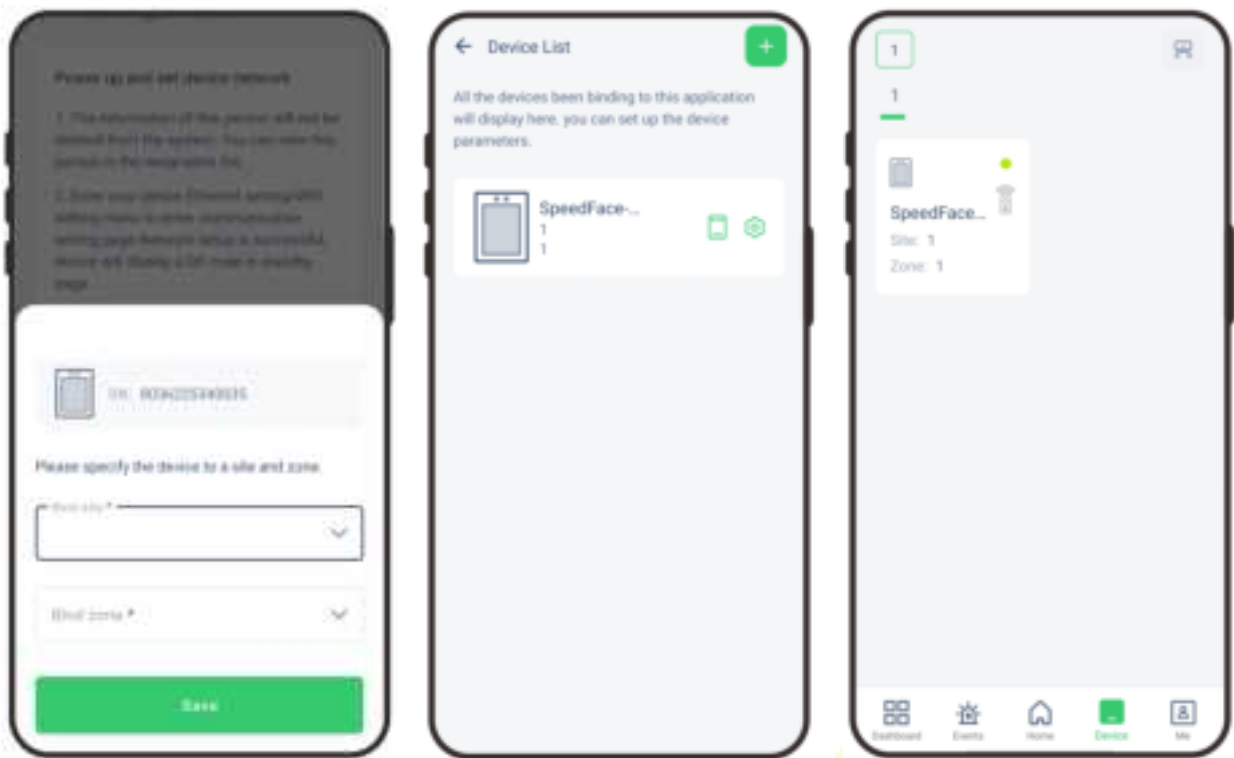


2. Click **Workshop** > **CloudACC** on the main menu to enter the **ZKBio Cloud Access** interface.
3. Click **Me** > **Device List** to enter the **Device** interface. And click  icon to add a new device.

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

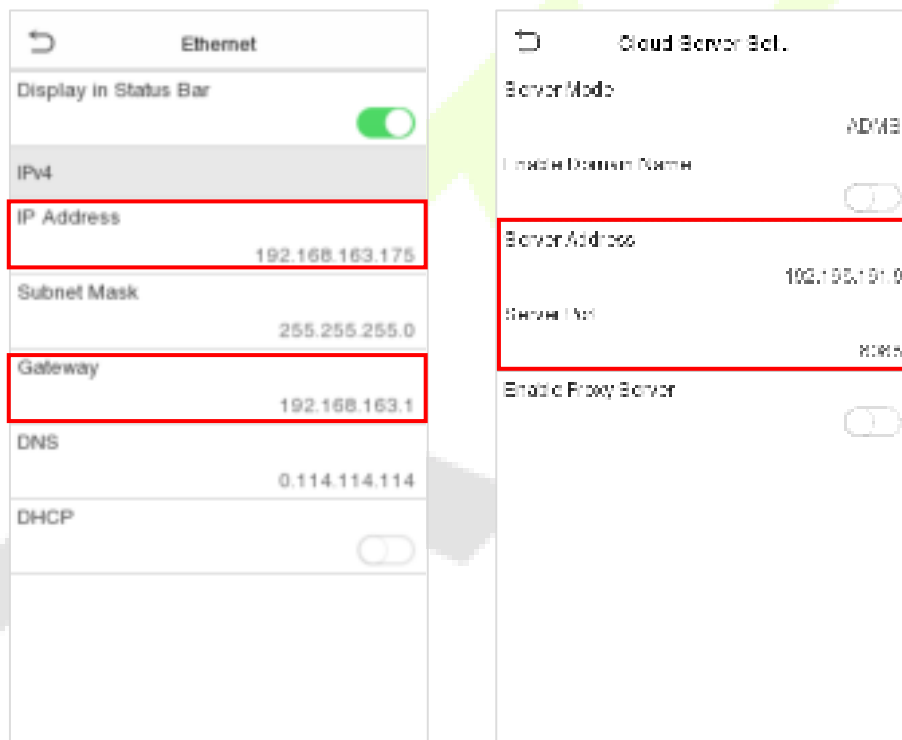
1. Tap **COMM.** > **Ethernet** in the main menu to set the IP address and gateway of the device.

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.

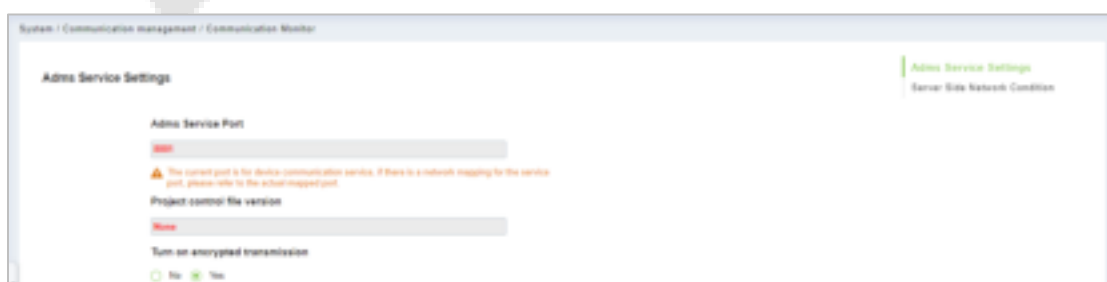
Server address: Set the IP address as of ZKBio CVAccess server.

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



● Software Side

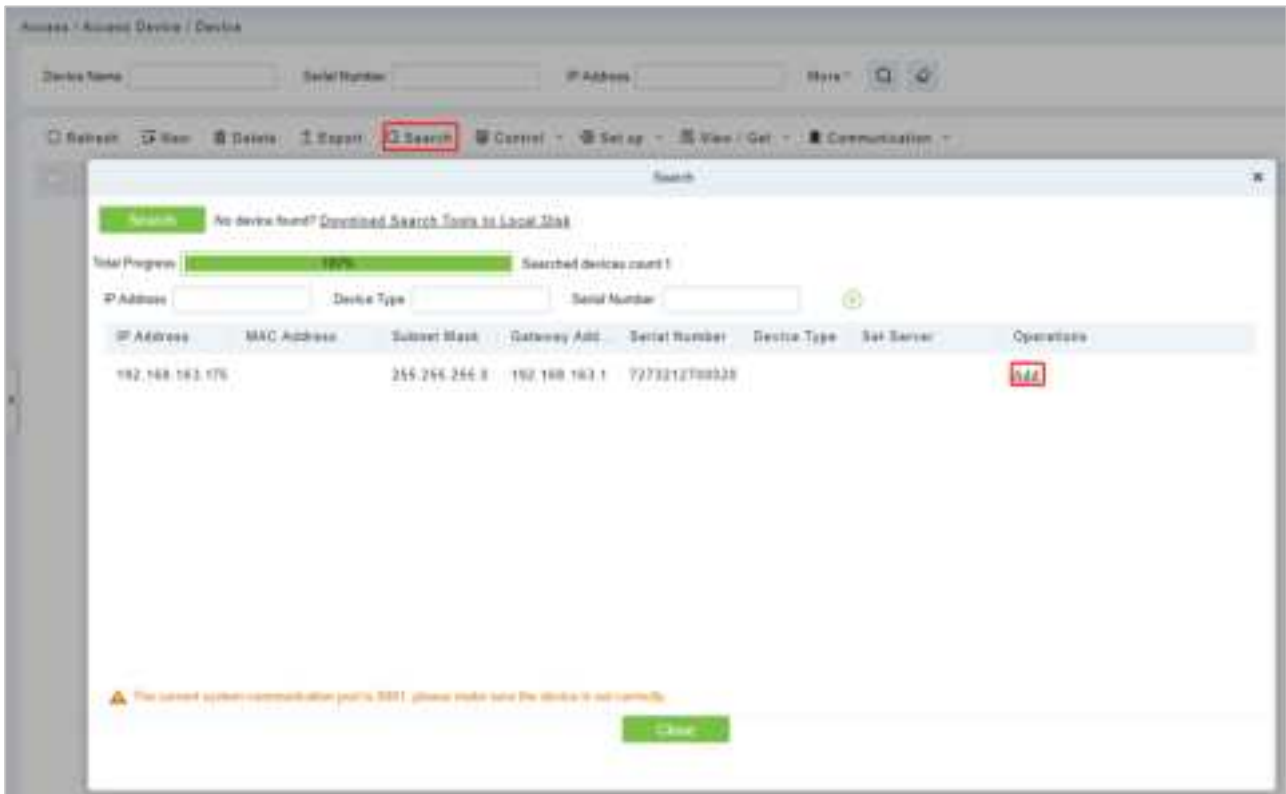
Login to ZKBio CVAccess software, click **System** > **Communication** > **Communication Monitor** to set the ADMS service port, as shown in the figure below:



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. It contains the following fields and controls:

- Personal Information:**
 - Personnel ID*: 2842
 - First Name: [Text Field]
 - Gender: [Dropdown]
 - Certificate Type: [Dropdown]
 - Birthday: [Text Field]
 - Hire Date: [Text Field]
 - Device Verification Password: [Text Field]
 - Biometrics Type: [Text Field]
 - Enable app login: ☐
- Departmental Information:**
 - Department*: Department Name [Dropdown]
 - Last Name: [Text Field]
 - Mobile Phone: [Text Field]
 - Certificate Number: [Text Field]
 - Email: [Text Field]
 - Position Name: [Dropdown]
 - Card Number: [Text Field]
- Image:** Profile picture placeholder with 'Browse' and 'Capture' buttons.
- Access Control:**
 - Levels Settings:
 - General: ☒
 - Permissions:
 - Superuser: No [Dropdown]
 - Device Operation Role: Ordinary User [Dropdown]
 - Extend Passage: ☐
 - Access Disabled: ☐
 - Set Valid Time: ☐
- Buttons:** 'Add', 'Select All', 'Unselect All' (under Levels Settings); 'Save and New', 'OK', 'Cancel' (at the bottom).

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★

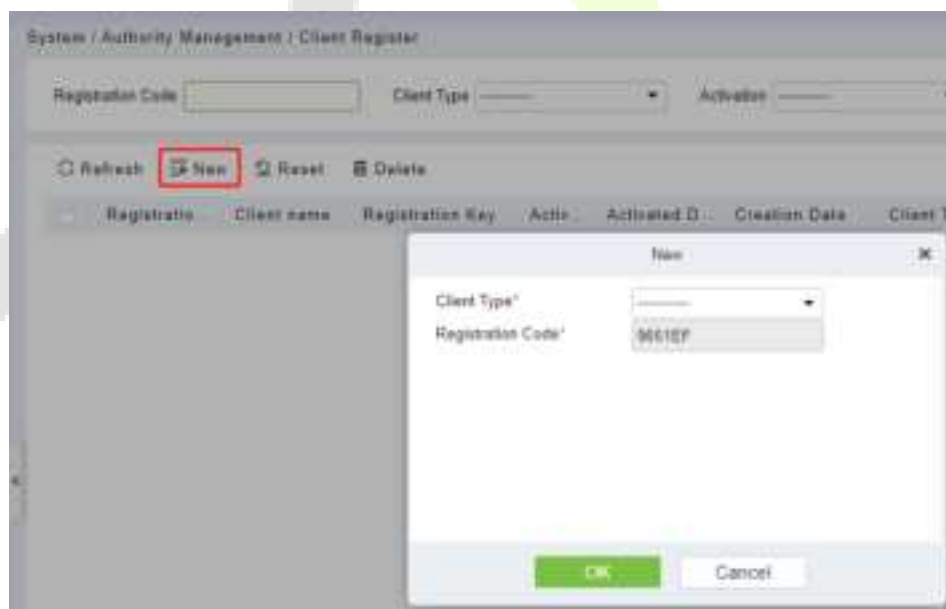
Note: This function is only for SenseFace 4C.

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.

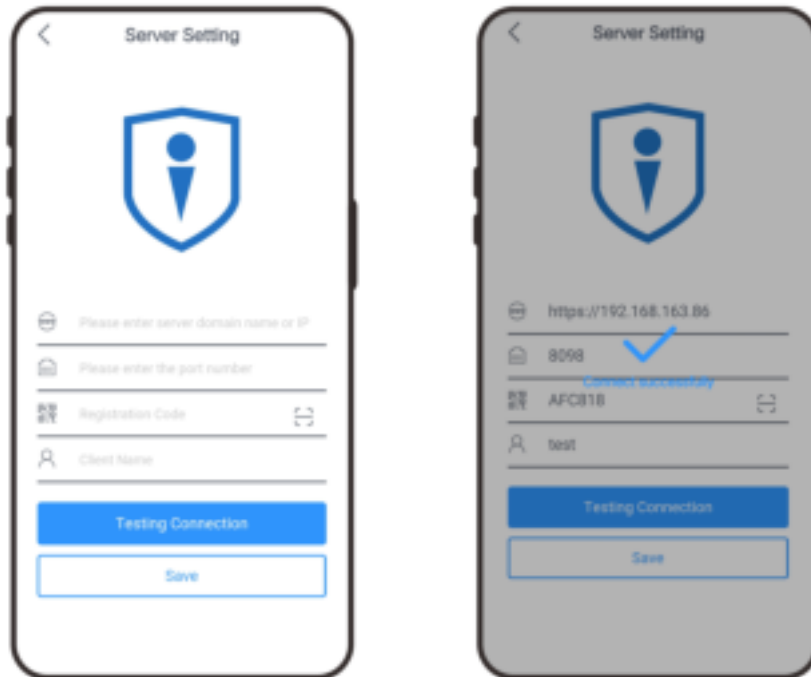


3. Open the App on the Smartphone. On the login screen, tap **Server Setting** and type the IP Address or the domain name of the Server, and its port number.

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**.

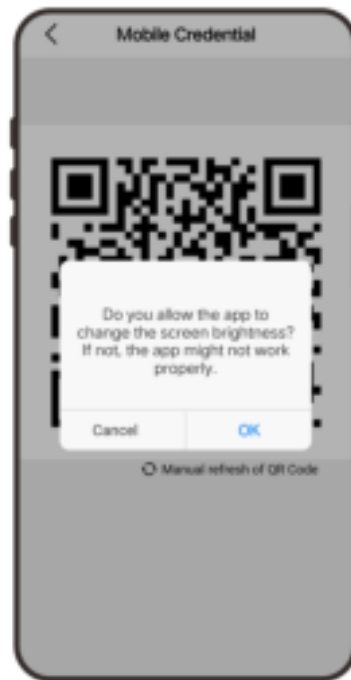


The Mobile Credential function is only valid when logging in as an employee, tap on Employee to switch to employee login screen. Enter the employee ID and password (Default: 123456) to login.

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

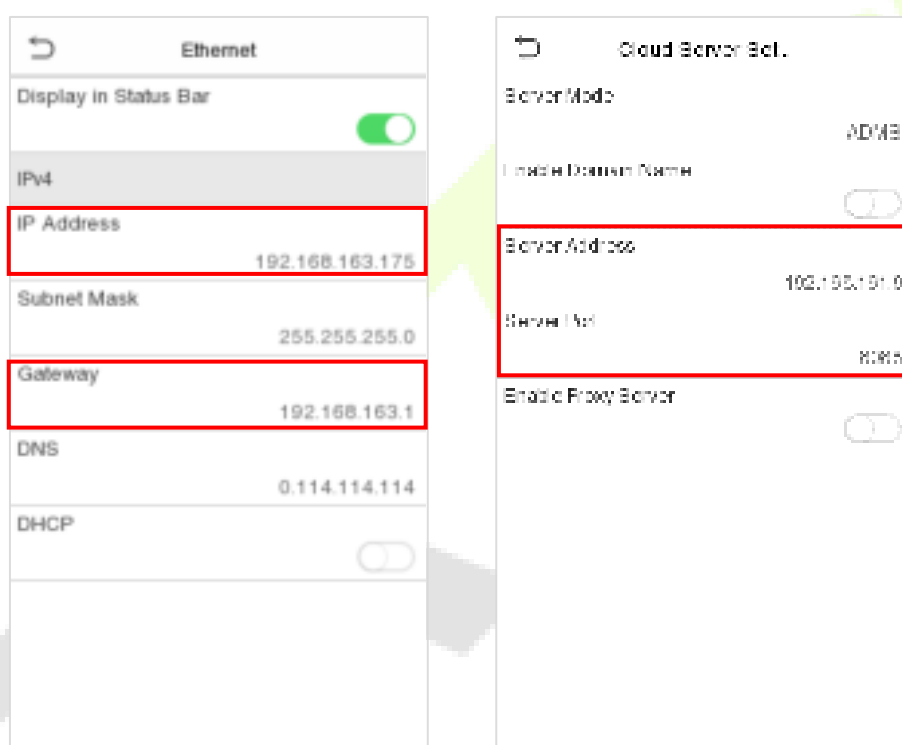
1. Tap **COMM.** > **Ethernet** in the main menu to set the IP address and gateway of the device.

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

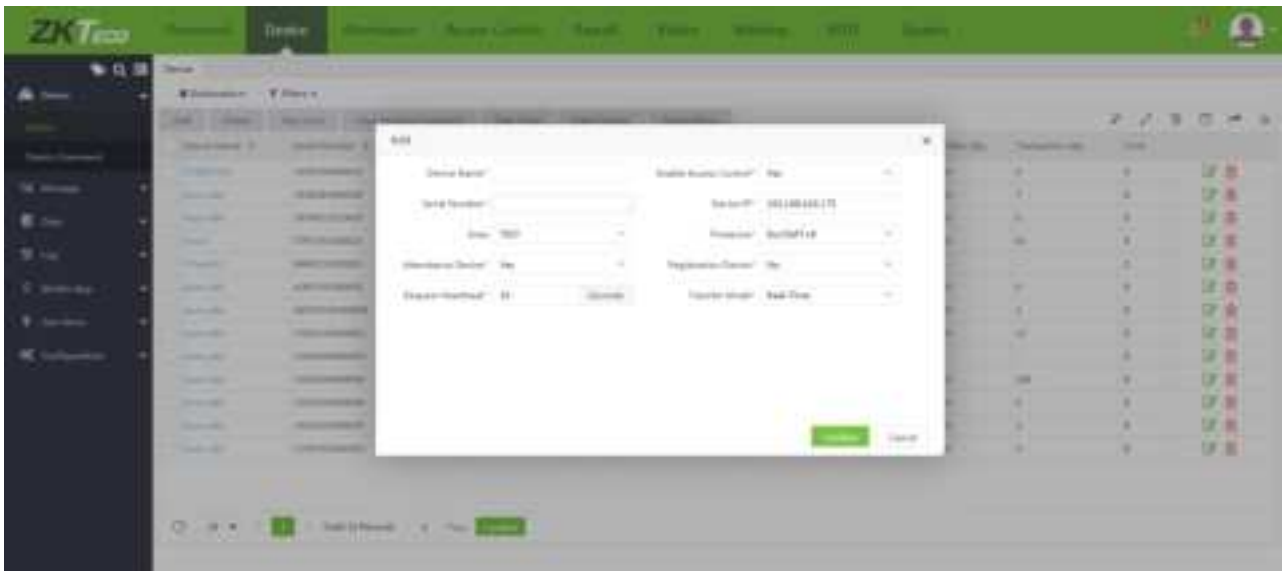
Server port: Set the server port as of ZKBioTime (The default is 8081).



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 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

