

| Function Name                 | Description                                                                                                                                                                                                                                                                    |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Communication Protocol</b> | Set the device communication protocol. It is <b>BEST Protocol</b> by default, which is suitable for ZKBio Zlink.<br><br><b>PUSH Protocol:</b> It can be set as A&C PUSH (which is suitable for ZKBio CVAcess) or T&A PUSH (which is suitable for ZKBio Time Cloud/ZKBio Time). |
| <b>Device Type</b>            | Set the device as an access control terminal or attendance terminal.                                                                                                                                                                                                           |

**Note:** After changing the device type, the device will delete all the data and restart, and some functions will be adjusted accordingly.

### 18.8.4 Access Control Options

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

On the Access Control interface to set the parameters of the control lock of the terminal and related equipment.

#### Access Control Terminal:

| Function Name              | Description                                                                                                                                                                                                        |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Gate Control Mode</b>   | It toggles between <b>ON</b> or <b>OFF</b> switch to get into gate control mode or not.<br><br>When set to <b>ON</b> , the interface removes the Door Lock Delay, Door Sensor Delay, 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.<br><br>Valid value: 1~99 seconds.                                                                                             |

|                                     |                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Door Sensor Delay (s)</b>        | <p>If the door is not locked and is left open for a certain duration (Door Sensor Delay), an alarm will be triggered.</p> <p>The valid value of Door Sensor Delay ranges from 1 to 255 seconds.</p>                                                                                                                                                                       |
| <b>Door Sensor Type</b>             | <p>There are three Sensor types: <b>None</b>, <b>Normal Open</b>, and <b>Normal Close</b>.</p> <p><b>None:</b> It means the door sensor is not in use.</p> <p><b>Normal Open:</b> It means the door is always left open when electric power is on.</p> <p><b>Normal Close:</b> It means the door is always left closed when electric power is on.</p>                     |
| <b>Verification Mode</b>            | <p>The supported verification mode includes Password/Fingerprint/Card, 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).</p> |
| <b>Door Available Time Period</b>   | <p>It sets the timing for the door so that the door is accessible only during that period.</p>                                                                                                                                                                                                                                                                            |
| <b>Normal Open Time Period</b>      | <p>It is the scheduled time-period for "Normal Open" mode so that the door is always open during this period.</p>                                                                                                                                                                                                                                                         |
| <b>Aux Output/Lock Open Time(s)</b> | <p>Sets the door unlock time period of the auxiliary terminal device.</p>                                                                                                                                                                                                                                                                                                 |
| <b>Aux Output Type Settings</b>     | <p>Auxiliary output types include None, Trigger door open, Trigger Alarm, Trigger door open and Alarm.</p>                                                                                                                                                                                                                                                                |
| <b>Verify Mode by RS485</b>         | <p>When the RS485 reader function is turned on, the verification method is used when the device is used as a master or a slave.</p>                                                                                                                                                                                                                                       |
| <b>Embedded Alarm</b>               | <p>If enabled, it transmits a sound alarm or disassembly alarm from the local. When the door is closed or the verification is successful, the system cancels the alarm from the local.</p>                                                                                                                                                                                |
| <b>Master Device</b>                | <p>While configuring the master and slave devices, you may set the state of the master as <b>Out</b> or <b>In</b>.</p> <p><b>Out:</b> A record of verification on the master device is a check-out record.</p> <p><b>In:</b> A record of verification on the master device is a check-in record.</p>                                                                      |

**Slave Device**

While configuring the master and slave devices, you may set the state of the slave as **Out** or **In**.

**Out:** A record of verification on the slave device is a check-out record.

**In:** A record of verification on the slave device is a check-in record.

**Attendance Terminal:**

| Function Name                | Description                                                                                                                                                                                                                                                                                                                                     |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Door Lock Delay (s)</b>   | The length of time that the device controls the electric lock to be in unlock state.<br>Valid value: 0 to 10 seconds.                                                                                                                                                                                                                           |
| <b>Door Sensor Delay (s)</b> | If the door is not locked and is left open for a certain duration (Door Sensor Delay), an alarm will be triggered.<br>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 Close</b> .<br><b>None:</b> It means the door sensor is not in use.<br><b>Normal Open (NO):</b> It means the door is always left open when electric power is on.<br><b>Normal Close (NC):</b> It means the door is always left closed when electric power is on. |
| <b>Door Alarm Delay(s)</b>   | When the state of the door sensor is inconsistent with that of the door sensor type, alarm will be triggered after a time period; this time period is the Door Alarm Delay (the value ranges from 1 to 999 seconds).                                                                                                                            |

|                                     |                                                                                                                                                                                                                 |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Retry Times to Alarm</b>         | When the number of failed verifications reach the set value (value ranges from 1 to 9 times), the alarm will be triggered. If the set value is None, the alarm will not be triggered after failed verification. |
| <b>Normal Close Time Period</b>     | It is the scheduled time-period for "Normal Close" mode so that the door is always closed during this period.                                                                                                   |
| <b>Normal Open Time Period</b>      | It is the scheduled time-period for "Normal Open" mode so that the door is always open during this period.                                                                                                      |
| <b>Aux Output/Lock Open Time(s)</b> | Sets the door unlock time period of the auxiliary terminal device.                                                                                                                                              |
| <b>Aux Output Type Settings</b>     | Auxiliary output types include None, Trigger door open, Trigger Alarm, Trigger door open and Alarm.                                                                                                             |
| <b>Verify Mode by RS485</b>         | When the RS485 reader function is turned on, the verification method is used when the device is used as a master or a slave.                                                                                    |
| <b>Valid Holidays</b>               | To set if <b>Normal Close Time Period</b> or <b>Normal Open Time Period</b> settings are valid in set holiday time period. Choose [ON] to enable the set <b>NC</b> or <b>NO</b> time period in holiday.         |
| <b>Embedded Alarm</b>               | If enabled, it transmits a sound alarm or disassembly alarm from the local. When the door is closed or the verification is successful, the system cancels the alarm from the local.                             |

### 18.8.5 Access Logs Settings/Attendance

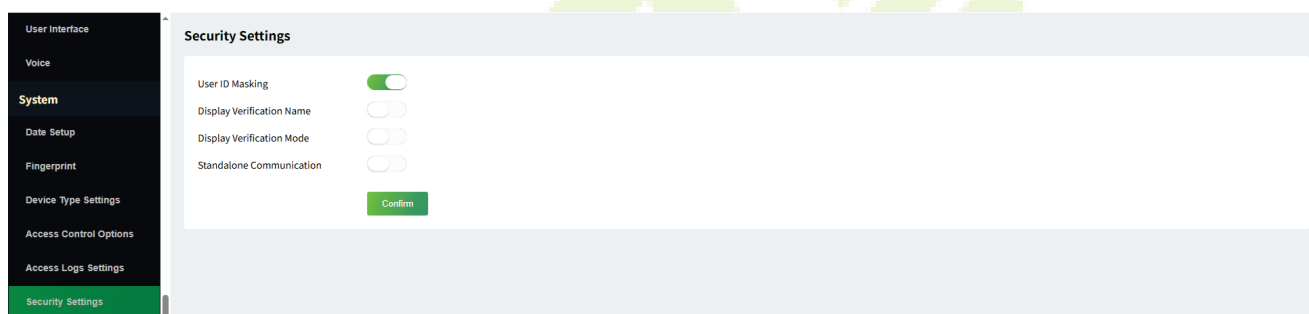
Click **Access Logs Settings/Attendance** on the WebServer.

| Function Name                    | Description                                                                                                                              |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Duplicate Punch Period(m)</b> | Within a set time period (unit: minutes), the duplicated attendance record will not be reserved (value ranges from 1 to 999999 minutes). |
| <b>Alphanumeric User ID</b>      | Enable/Disable the alphanumeric as User ID.                                                                                              |

|                                                 |                                                                                                                                                                                                                                       |
|-------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Access/Attendance Log Alert</b>              | <p>When the record space of the attendance/access reaches the maximum threshold value, the device automatically displays the memory space warning.</p> <p>Users may disable the function or set a valid value between 1 and 9999.</p> |
| <b>Periodic Del of Access Logs/T&amp;A Data</b> | <p>When access/attendance logs reach its maximum capacity, the device automatically deletes a set of old access/attendance logs.</p> <p>Users may disable the function or set a valid value between 1 and 999.</p>                    |
| <b>Authentication Timeout(s)</b>                | <p>The amount of time taken to display a successful verification message.</p> <p>Valid value: 1 to 9 seconds.</p>                                                                                                                     |

### 18.8.6 Security Settings

Click **Security Settings** on the WebServer.

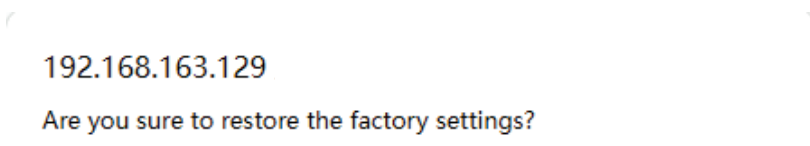


| Function Name                    | Description                                                                                                                                                                                                                            |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>User ID Masking</b>           | When enabled, and then the user is successfully compared and verified, the User ID in the displayed verification result will be replaced with an * to achieve secure protection of sensitive private data.                             |
| <b>Display Verification Name</b> | Set whether to display the username in the verification result interface.                                                                                                                                                              |
| <b>Display Verification Mode</b> | Set whether to display the verification mode in the verification result interface.                                                                                                                                                     |
| <b>Standalone Communication</b>  | By default, this function is disabled. It is used to connect the C/S software (like ZKTime.Net, etc.). When it is switched on, a security prompt appears, and you need to set the Comm Key, the device will restart after you confirm. |

## 18.8.7 Restore

Click **Restore** on the WebServer, and it will pop up the following prompt box. Click Yes to restore the factory settings.

The Restore function restores the device settings such as communication and system settings to the default factory settings (this function does not clear registered user data).

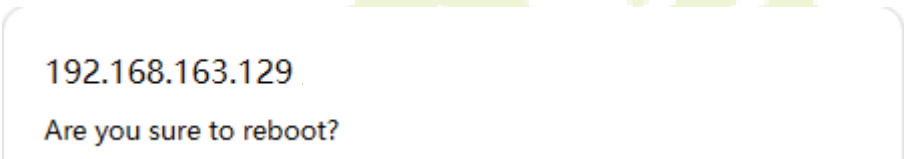


192.168.163.129  
Are you sure to restore the factory settings?

**Note:** After reset, the IP of the device is restored to the original 192.168.1.201, please refer to [18.6.1 Network Settings](#) to modify the IP.

## 18.8.8 Restart

Click **Restart** on the WebServer, and it will pop up the following prompt box. Click Yes to reboot.

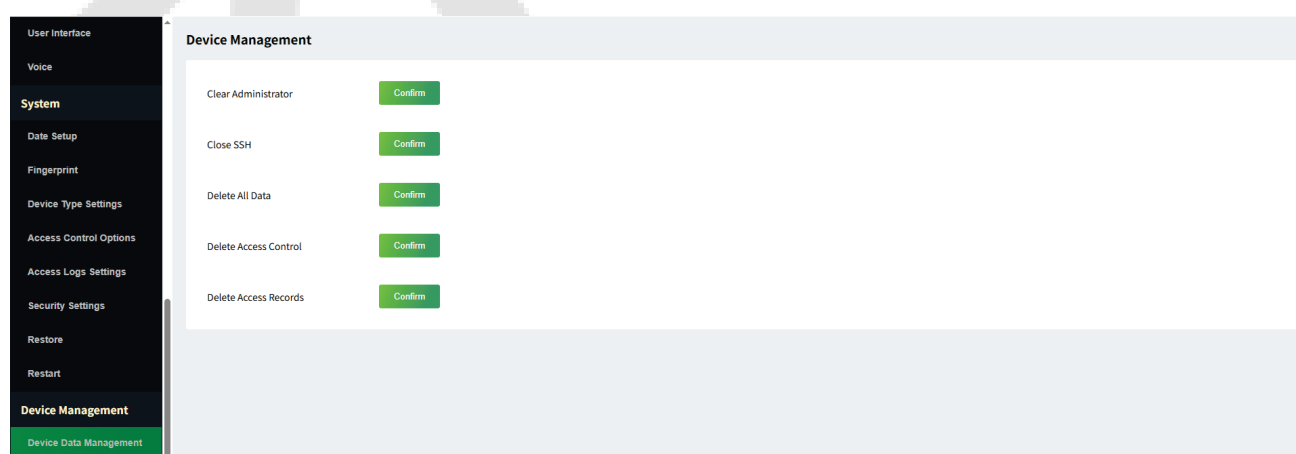


192.168.163.129  
Are you sure to reboot?

# 18.9 Device Management

## 18.9.1 Device Data Management

Click **Device Data Management** on the WebServer.



| Function Name                           | Description                                                                                         |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------|
| <b>Clear Administrator</b>              | Choose whether to change the super administrator into a normal user.                                |
| <b>Close SSH</b>                        | SSH is used to enter the background of the device for maintenance, choose whether to close the SSH. |
| <b>Delete All Data</b>                  | To delete the information and attendance logs/access records of all registered users.               |
| <b>Delete Access Control</b>            | To delete all the access data.                                                                      |
| <b>Delete Access/Attendance Records</b> | To delete all the access/attendance records.                                                        |

## 18.9.2 Update Firmware

Click **Update Firmware** on the WebServer.

Select an upgrade file and click **Confirm** to complete firmware upgrade operation.

**Note:** If the upgrade file is needed, please contact our technical support. Firmware upgrade is not recommended under normal circumstances.

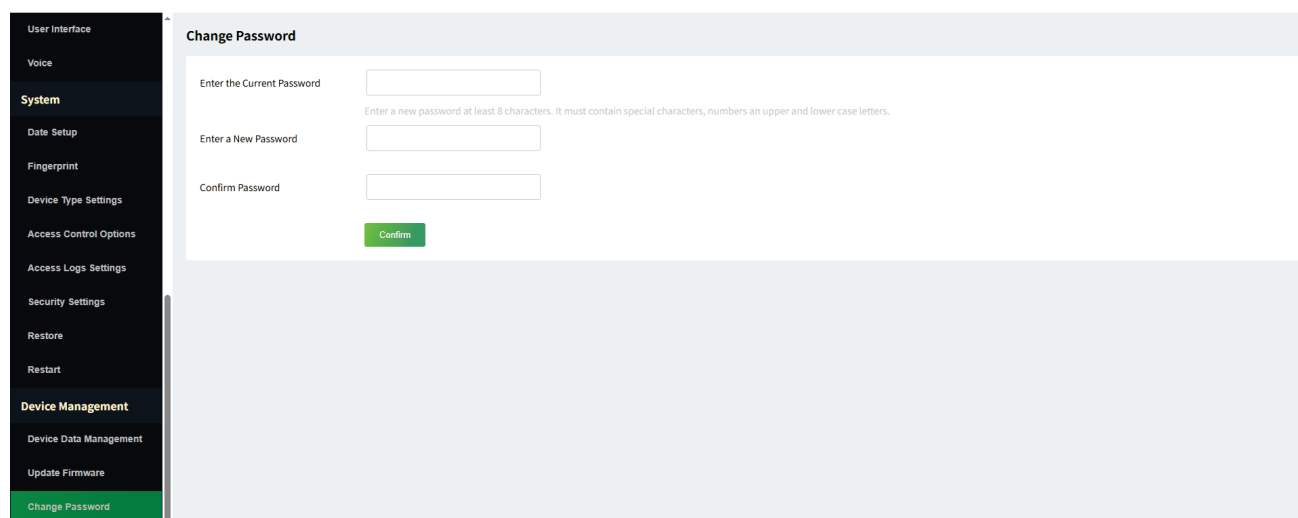
You can also choose to update firmware online. Click **Detection upgrade** it may have the following 3 scenarios:

- If the query fails, the interface will prompt "Query Failed".
- If the firmware version of the device is latest, it will prompt that the current firmware version is already the latest.
- If the firmware version of the device is not the latest, the version number and change log of the latest version will be displayed. Users can choose whether to update to the latest firmware version.

### 18.9.3 Change Password

Click **Change Password** on the WebServer.

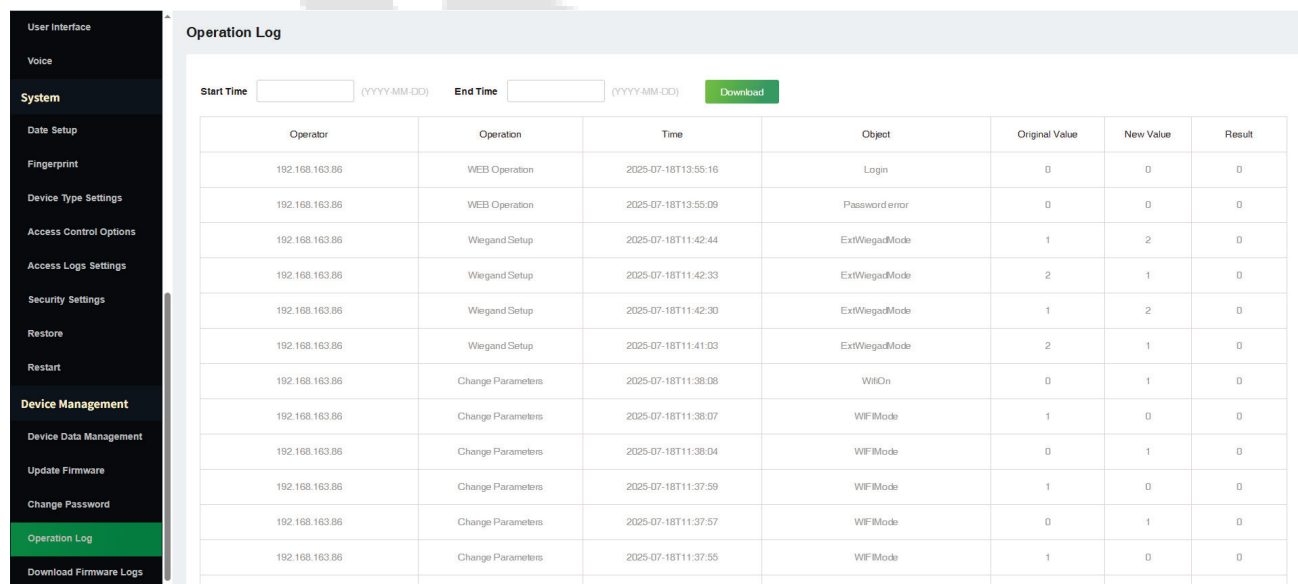
In this interface, you can change the password of WebServer.



### 18.9.4 Operation Log

Click **Operation Log** on the WebServer.

All the user's operation records on the device or WebServer are saved. Users can search and download these logs by time.

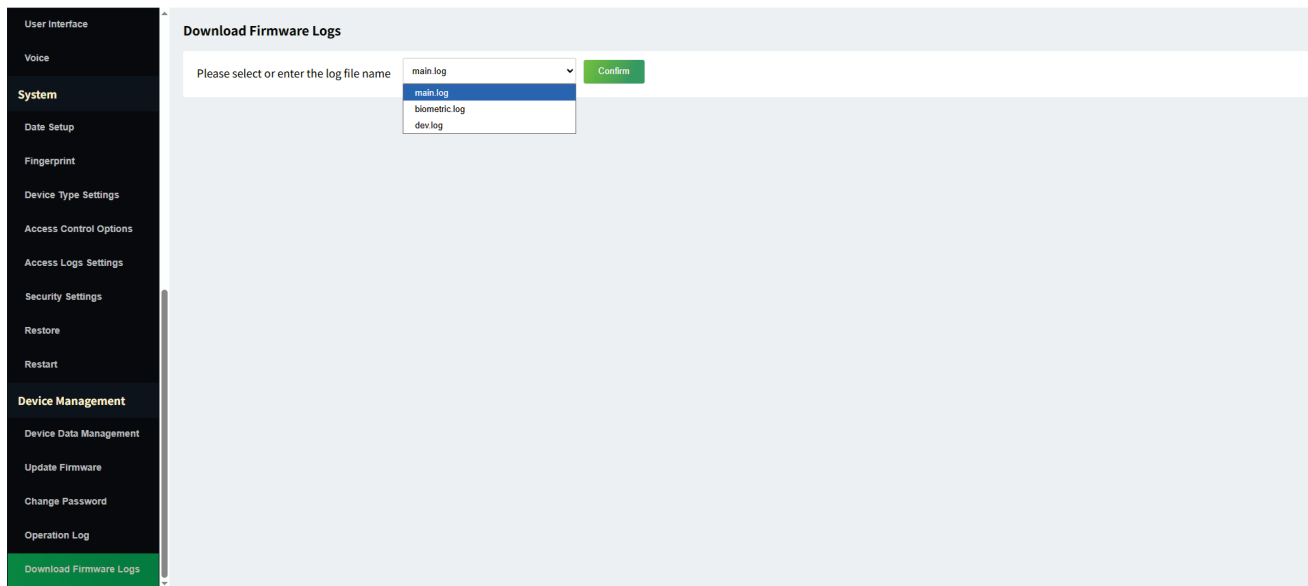


| Operator       | Operation         | Time                | Object         | Original Value | New Value | Result |
|----------------|-------------------|---------------------|----------------|----------------|-----------|--------|
| 192.168.163.86 | WEB Operation     | 2025-07-18T13:55:16 | Login          | 0              | 0         | 0      |
| 192.168.163.86 | WEB Operation     | 2025-07-18T13:55:09 | Password error | 0              | 0         | 0      |
| 192.168.163.86 | Wiegand Setup     | 2025-07-18T11:42:44 | ExtWiegandMode | 1              | 2         | 0      |
| 192.168.163.86 | Wiegand Setup     | 2025-07-18T11:42:33 | ExtWiegandMode | 2              | 1         | 0      |
| 192.168.163.86 | Wiegand Setup     | 2025-07-18T11:42:30 | ExtWiegandMode | 1              | 2         | 0      |
| 192.168.163.86 | Wiegand Setup     | 2025-07-18T11:41:03 | ExtWiegandMode | 2              | 1         | 0      |
| 192.168.163.86 | Change Parameters | 2025-07-18T11:38:08 | WifiOn         | 0              | 1         | 0      |
| 192.168.163.86 | Change Parameters | 2025-07-18T11:38:07 | WifiMode       | 1              | 0         | 0      |
| 192.168.163.86 | Change Parameters | 2025-07-18T11:38:04 | WifiMode       | 0              | 1         | 0      |
| 192.168.163.86 | Change Parameters | 2025-07-18T11:37:59 | WifiMode       | 1              | 0         | 0      |
| 192.168.163.86 | Change Parameters | 2025-07-18T11:37:57 | WifiMode       | 0              | 1         | 0      |
| 192.168.163.86 | Change Parameters | 2025-07-18T11:37:55 | WifiMode       | 1              | 0         | 0      |
| 192.168.163.86 | Change Parameters | 2025-07-18T11:37:54 | WifiMode       | 0              | 1         | 0      |

### 18.9.5 Download Firmware Logs

Click **Download Firmware Logs** on the WebServer.

In this interface, you can select download the main, biometric, or dev.log.



## 19 Connecting to ZKBio Zlink App

The App pages may vary depending on the version, and the document is for reference only.

Change the device communication protocol to BEST protocol, then the device can be managed by ZKBio Zlink, please refer to [9.4 Device Type Settings](#).

### ● Download the ZKBio Zlink App

Search for the "ZKBio Zlink" App in the iOS App Store or Google Play Store. Or scan the QR code below to install the app.



Apple App Store

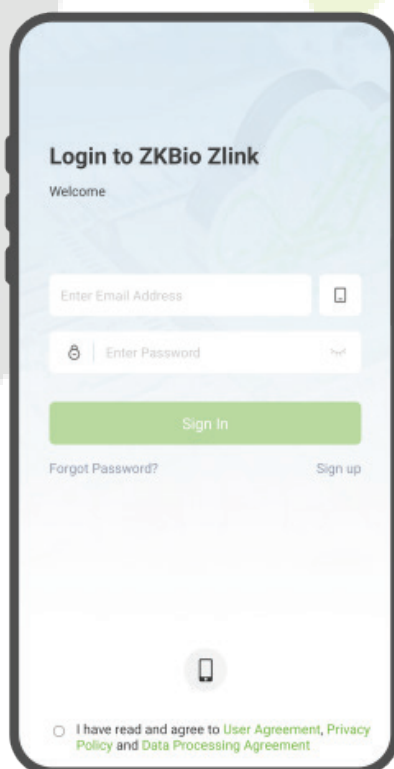


Google Play Store



### 19.1 Login to the App

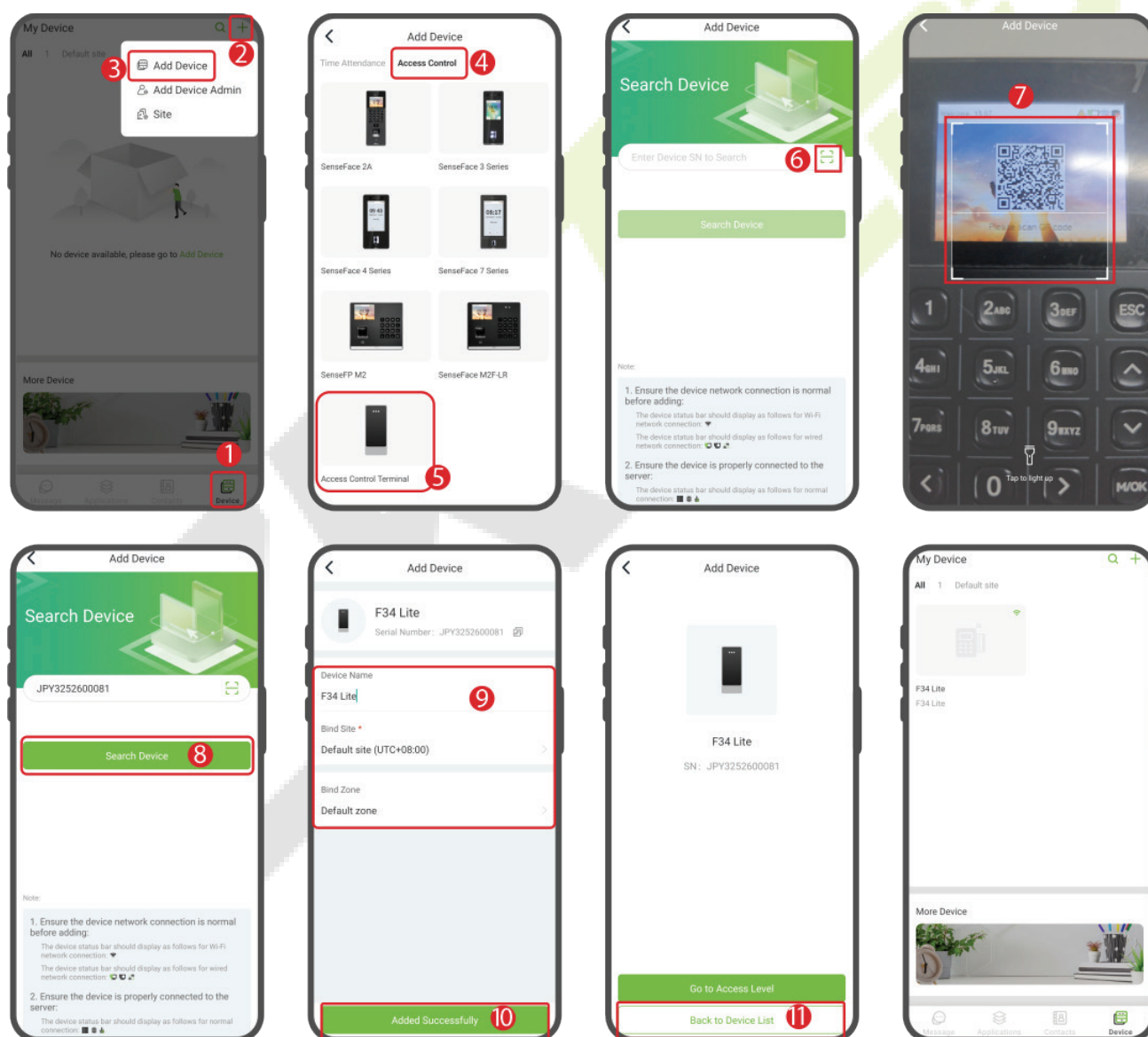
Enter your registered account and password, check "I have read and agree to User Agreement, Privacy Policy and Data Processing Agreement" and click **Sign In** to log in to the App.



**Note:** For more operations, refer to the ZKBio Zlink App's user manual.

## 19.2 Add Device on the App

- Access the ZKBio Zlink App and click on **[Device]** > **+** icon > **[Add Device]** > **[Access Control]** > **[Access Control Terminal]**. (1,2,3,4,5)
- Click  icon to scan the QR code on the device. The serial number of the device will be displayed in the bar. Then click **[Search Device]**. (6,7,8)
- Enter the device name and specify the device to a site and zone. Click **[Added Successfully]** to complete the addition. At the same time, the device voice prompts **"Device is added successfully"** indicating that the addition is complete. (9,10,11)
- Once successfully added, the device is displayed in the list of the device interface.

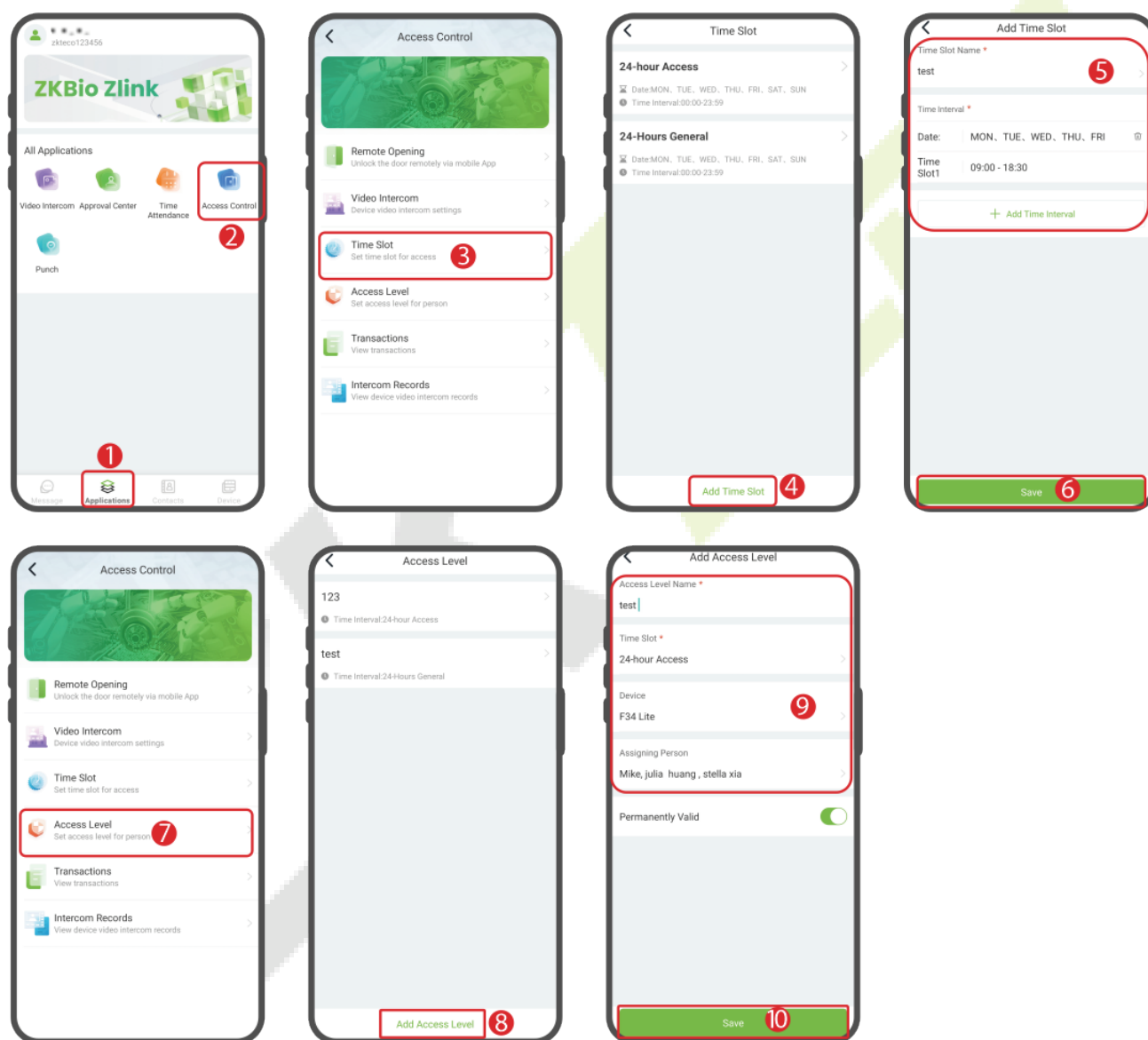


## 19.3 Set Access Levels

- Click [**Applications**] > [**Access Control**] > [**Time Slot**] > [**Add Time Slot**] to add a time slot. (1,2,3,4)
- Set the name and time intervals, and click [**Save**]. Then the time slot will be displayed in the list. (5,6)

**Note:** There is a default timeslot named **24-hour Access** in the system.

- Click [**Access Level**] > [**Add Access Level**] to add an access level. (7,8)
- Set the name, select the time slot, device, and persons, and click [**Save**] to synchronize the access level to the device. (9,10)

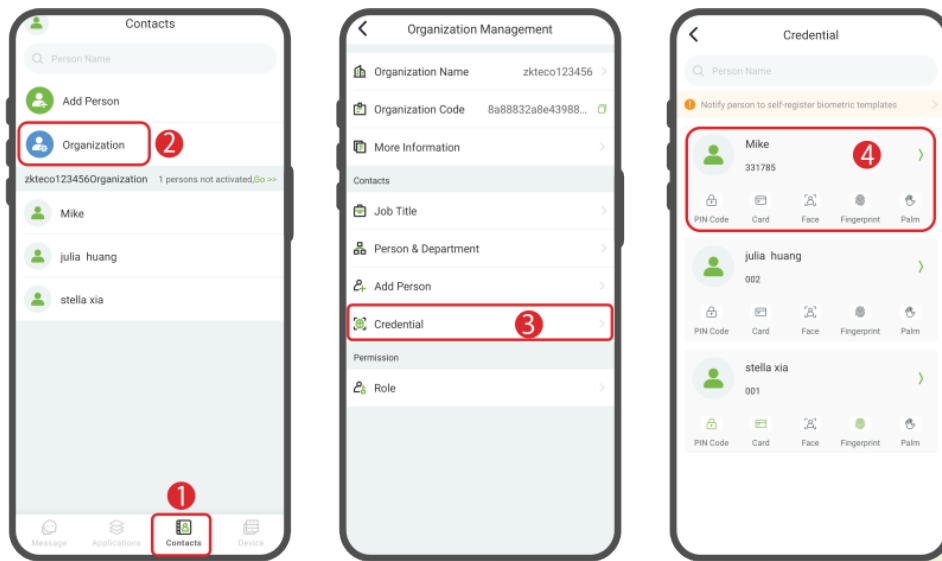


## 19.4 Register Verification Mode on the App

Once you have added persons to the device, you can register verification modes to them.

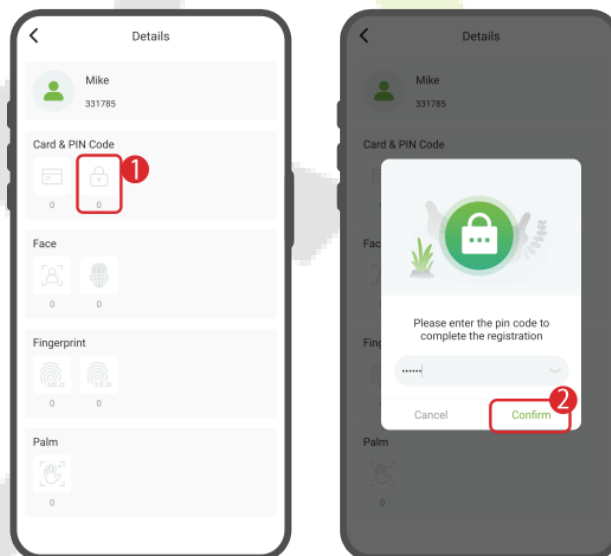
**Note:** It must be based on the functions actually supported by the device.

Click [**Contacts**] > [**Organization**] > [**Credential**] to enter the Credential screen, select the person who needs to register verification mode. (1,2,3,4)



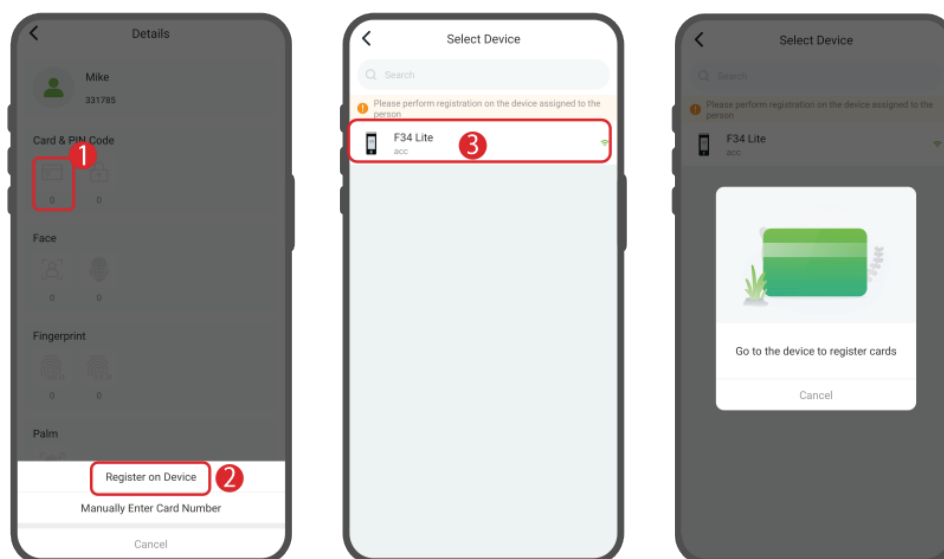
## Register Password

In the Details interface, click on the  icon and enter the password in the pop-up window, then click [**Confirm**]. (1,2)



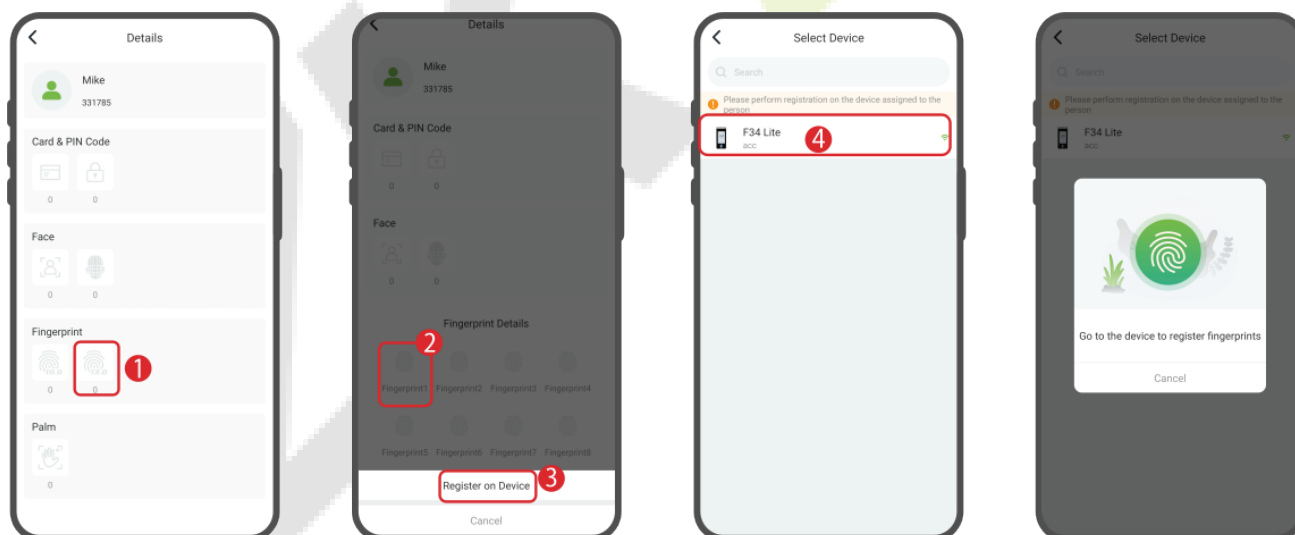
## Register Card

- In the Details interface, click on the  icon. You can select Register on Device or Manually Enter Card Number. If you want to register on device, then click **Register on Device**. (1,2)
- Select the registration device, at the same time, the device displays the Enroll Card Number interface. Place the card in the swipe area, when the display shows **"Card registered successfully"**, it means the card is successfully registered. (3)



## Register Fingerprint

- In the Details interface, click on the or (it depends on the fingerprint algorithm that set in **System > Fingerprint**), select the fingerprint and click **Register on Device > Register on Device**. (1,2,3)
- Select the registration device, at the same time, the device displays the fingerprint registration screen. According to the prompts, place your finger on the fingerprint sensor and press **3** times. When the interface prompts **"Enrolled successfully"**, it means the fingerprint registration is successful. (4)



## 20 Connecting to ZKBio Zlink Web

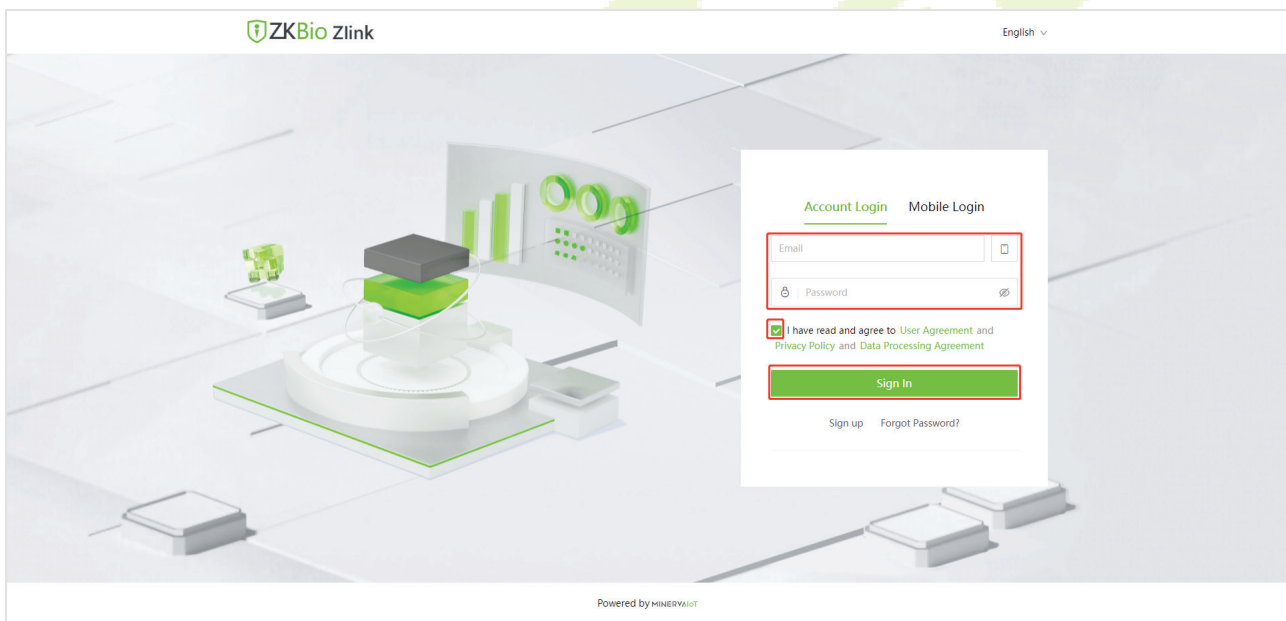
The web pages may vary depending on the version, and the document is for reference only.

Change the device communication protocol to BEST protocol, then the device can be managed by ZKBio Zlink, please refer to [9.4 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.

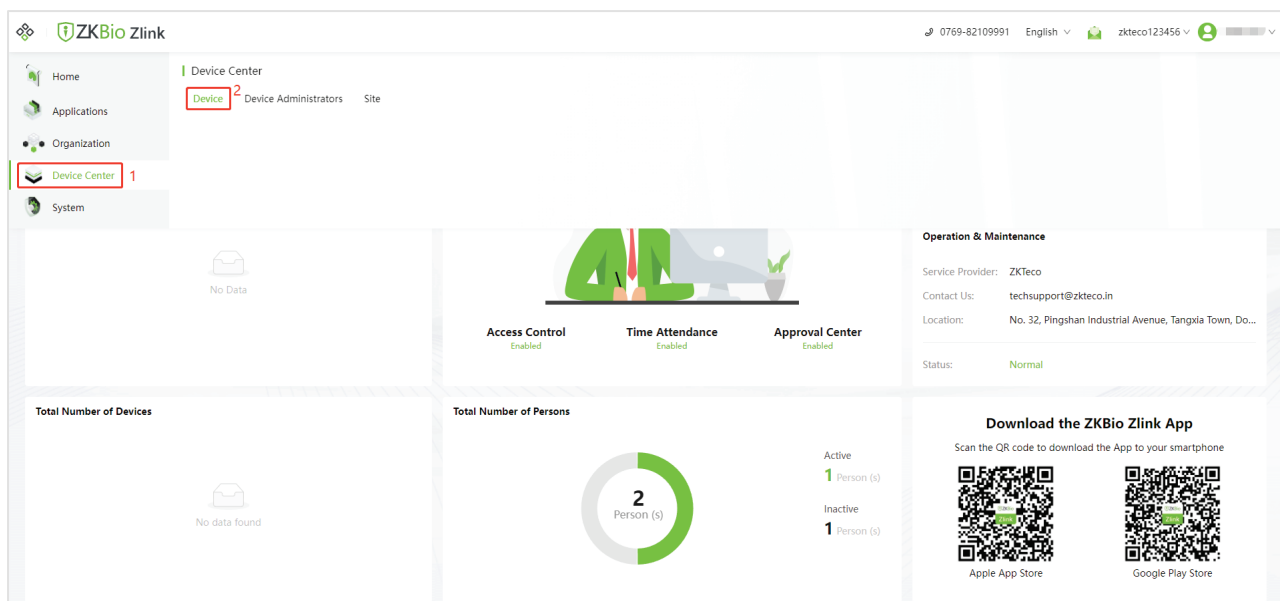
### 20.1 Login to the Web

1. Please open the recommended browser and enter the IP address to access the ZKBio Zlink Web: <http://zlink.minervaiot.com>.
2. Enter your Email ID and password on the login screen, check "I have read and agree to User Agreement and Privacy Policy and Data Processing Agreement" and click [**Sign In**] to login.

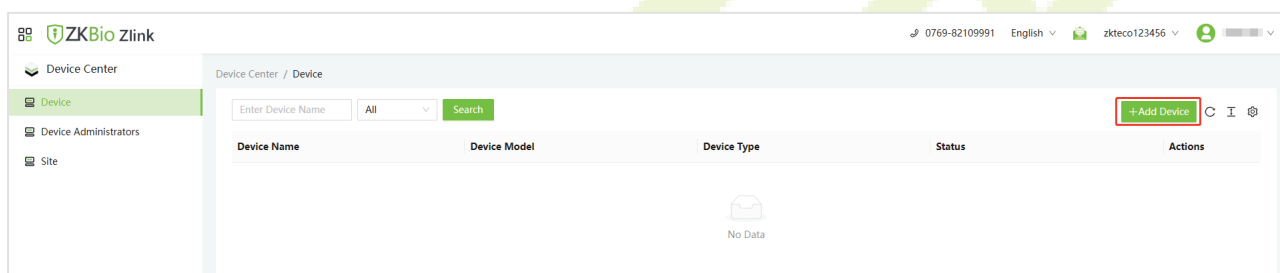


### 20.2 Add Device on the Web

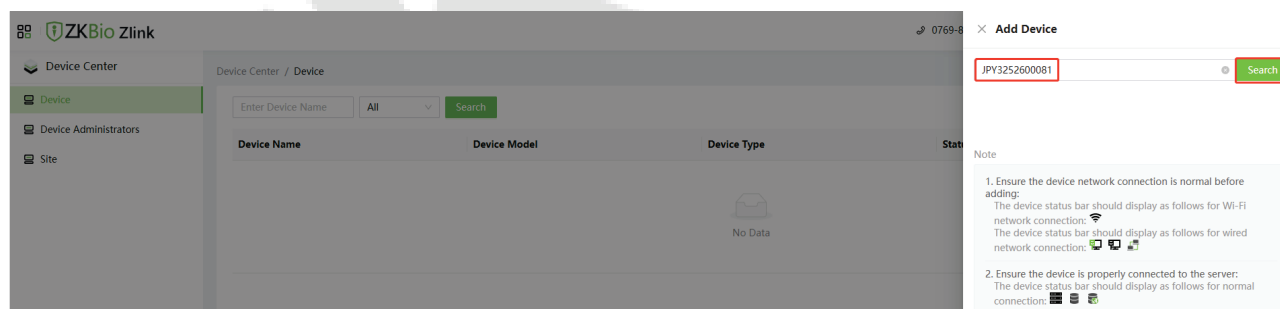
1. Click the  icon on the top left corner, and click [**Device Center**] > [**Device**] to enter the device setting interface.



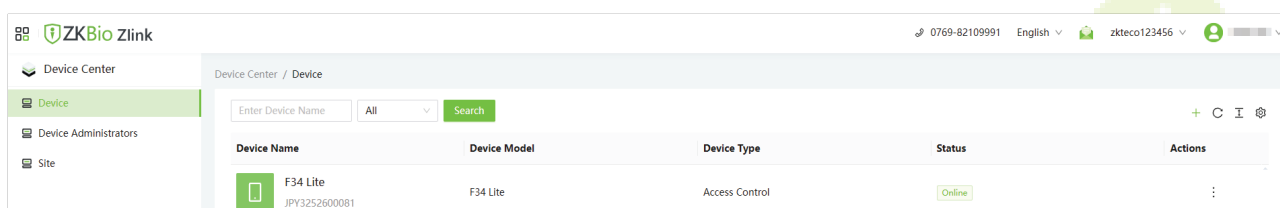
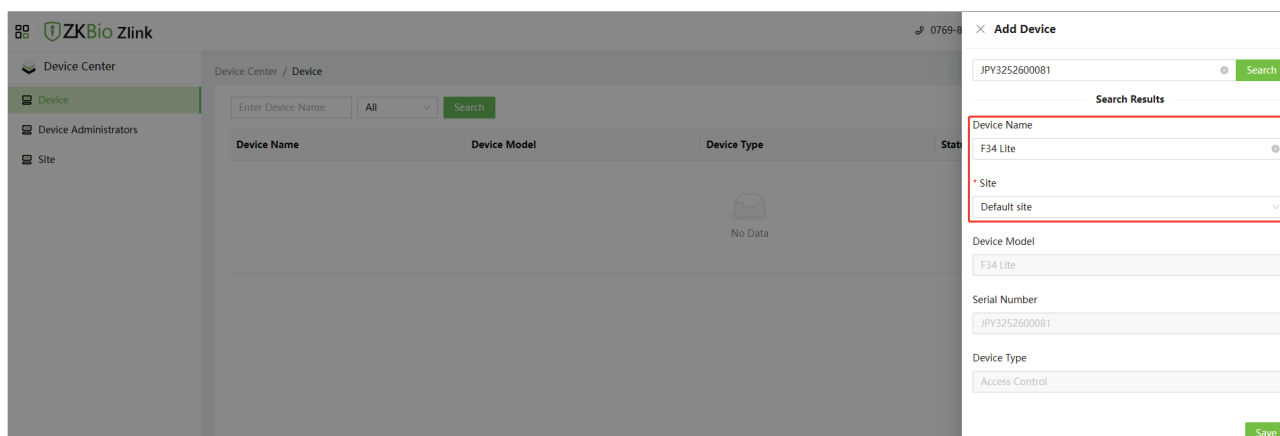
2. Then click **[Add Device]** to enter the Add Device interface.



3. Enter the Serial Number and click **[Search]**.



4. Then enter the device name and specify the device to a site. Select Site from the drop-down menu. Click **[Save]** to complete the addition.



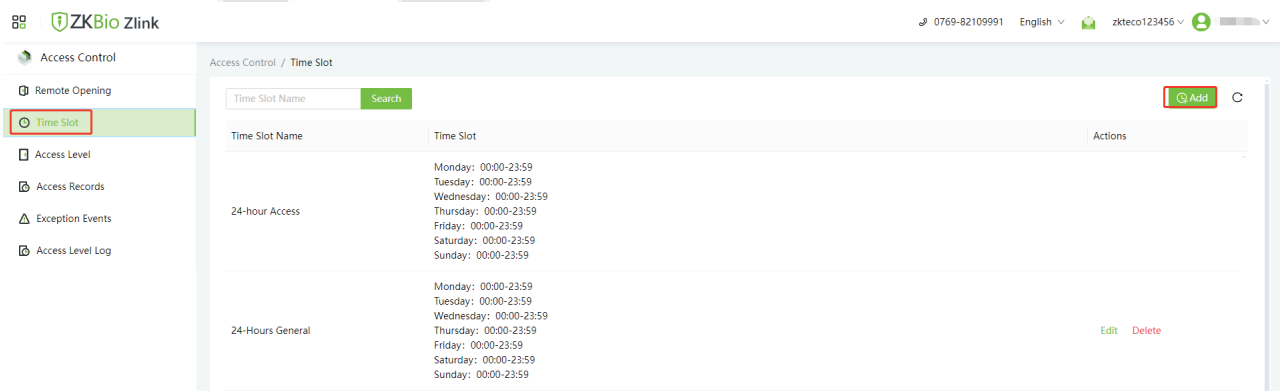
**Note:** Wait a moment for the device status to change from “Offline” to “Online”.

## 20.3 Set Access Levels

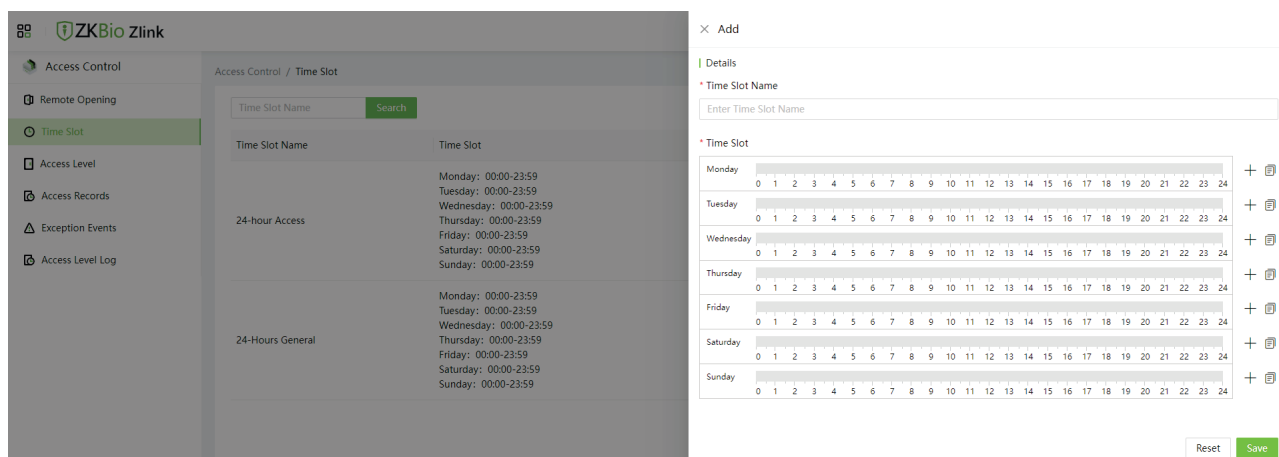
- Click the  icon on the top left corner, and click [Applications] > [Access Control] to enter the access control settings interface.



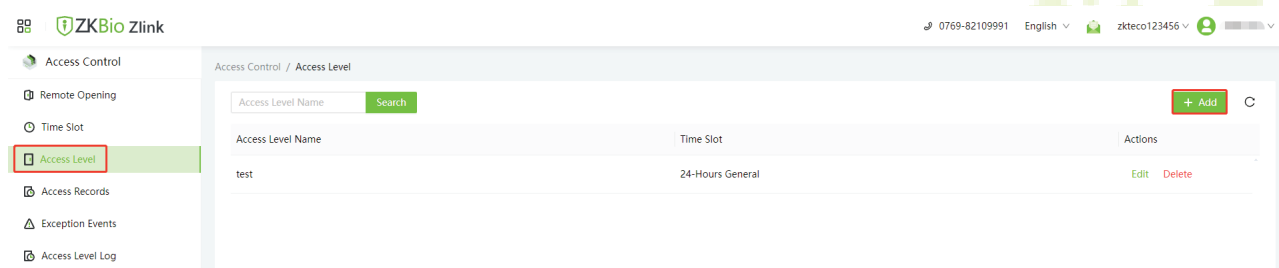
- Click [Time Slot] > [Add] to add a time slot.



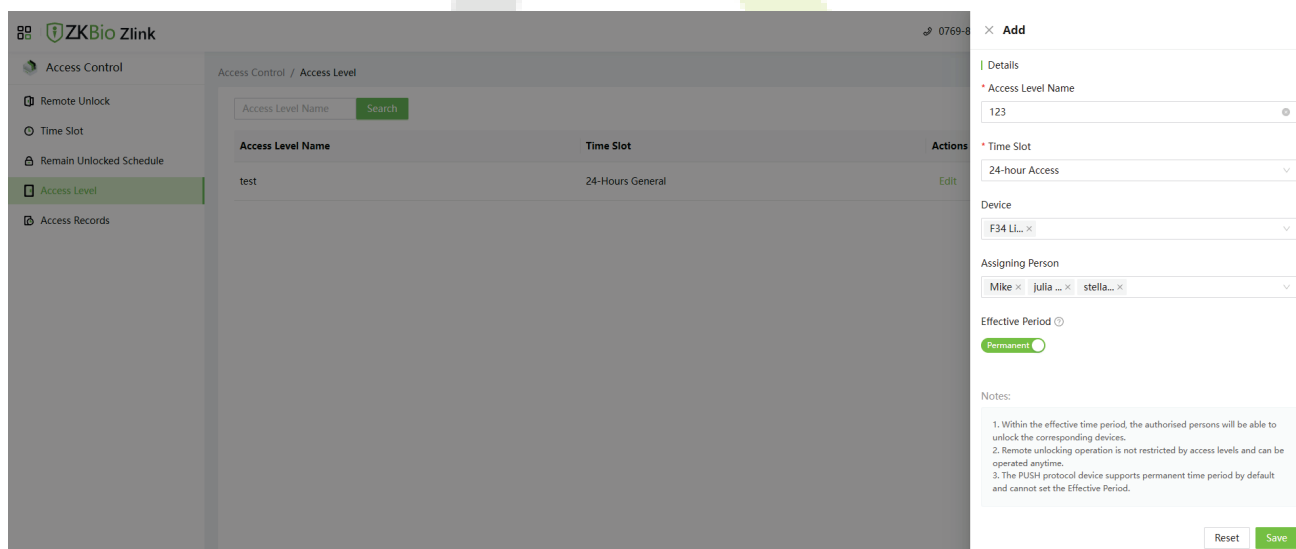
- Set the name and time slot, and click [Save]. Then the time lot will be displayed in the list. (**Note:** There is a default timeslot named **24-hour Access** in the system.)



4. Click **[Access Level]** > **[Add]** to add an access level.

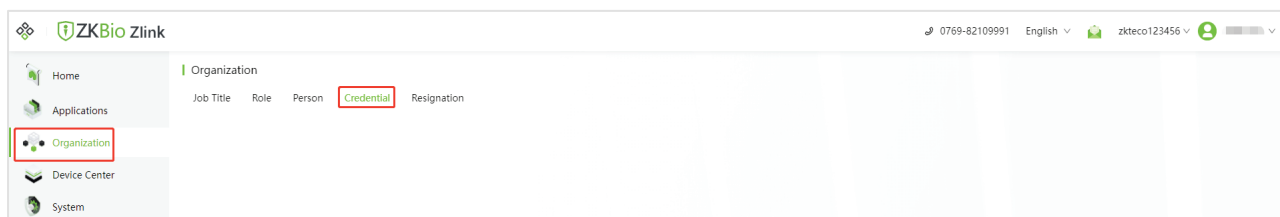


5. Set the access level name, select the time slot, device, and persons, then click **Save** to synchronize the access level to the device.

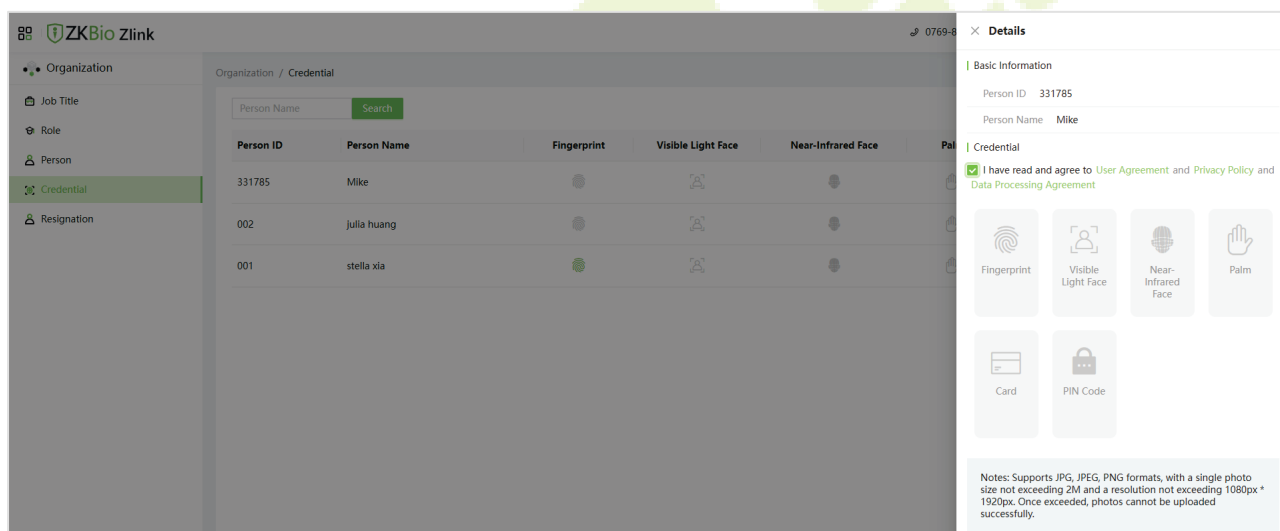
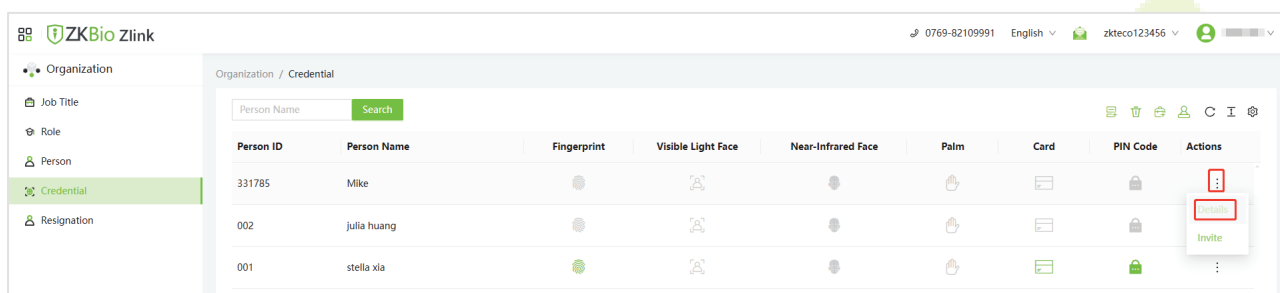


## 20.4 Register Verification Mode on the Web

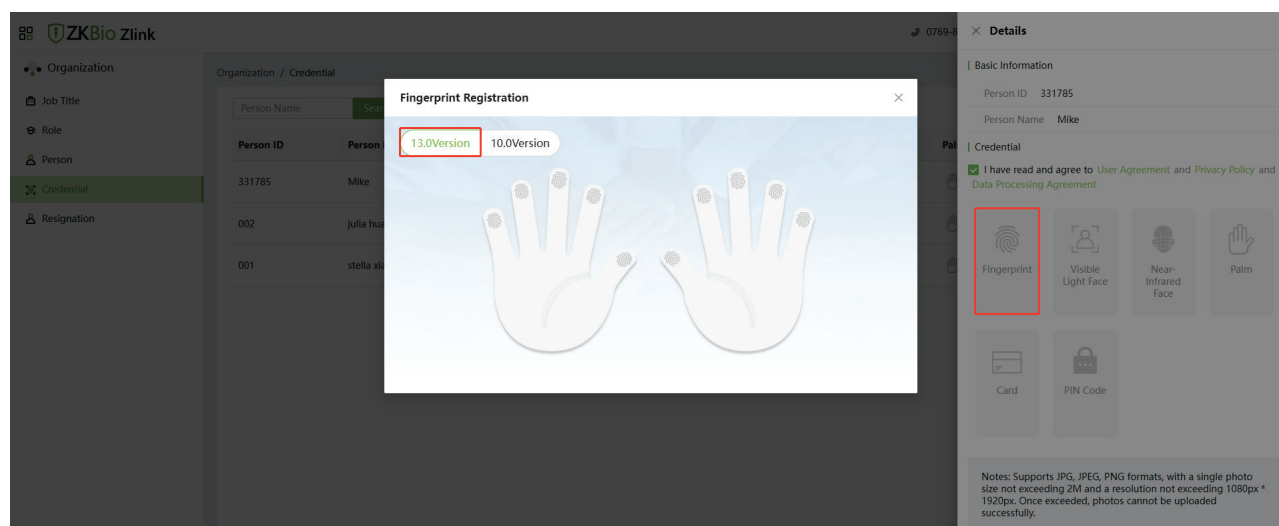
1. Click the  icon on the top left corner, and click **[Organization]** > **[Credential]** to enter the credentials setting interface.



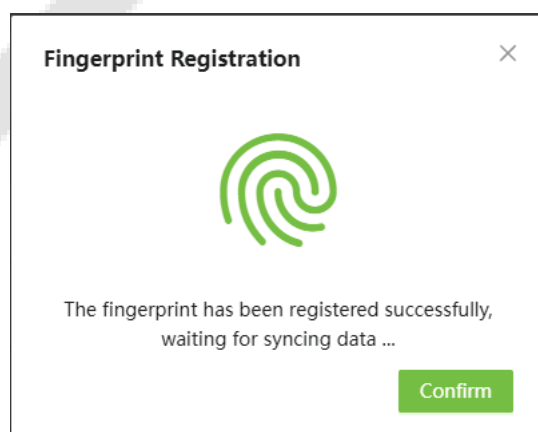
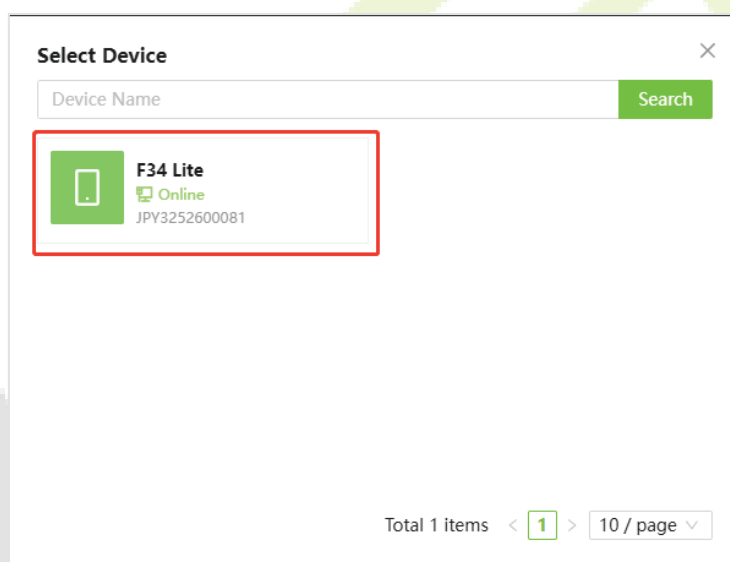
2. Select the person and click the  icon > **Details**, check “I have read and agree to User Agreement and Privacy Policy and Data Processing Agreement” and click **Fingerprint/Card/PIN Code** to remotely register the personnel biometric verification mode.



- **Register Fingerprint**
1. Click **Fingerprint** in the Details page. Click **13.0Version** or **10.0Version** (it depends on the fingerprint algorithm that set in **System > Fingerprint**). Choose the hand and finger to be enrolled in the pop-up prompt window.



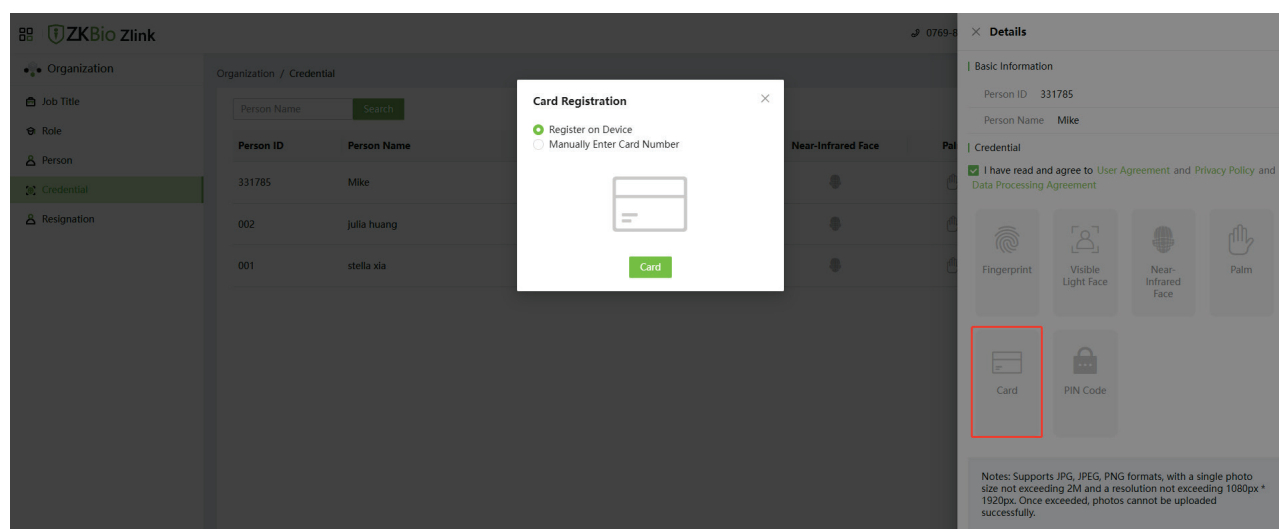
2. Select the registration device, the device will display the fingerprint registration screen. According to the prompts, place your finger on the fingerprint sensor and press 3 times. When the interface prompts “Enrolled Successfully”, it means the fingerprint registration is successful.



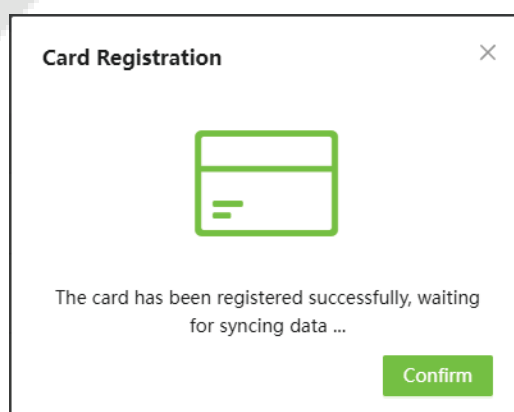
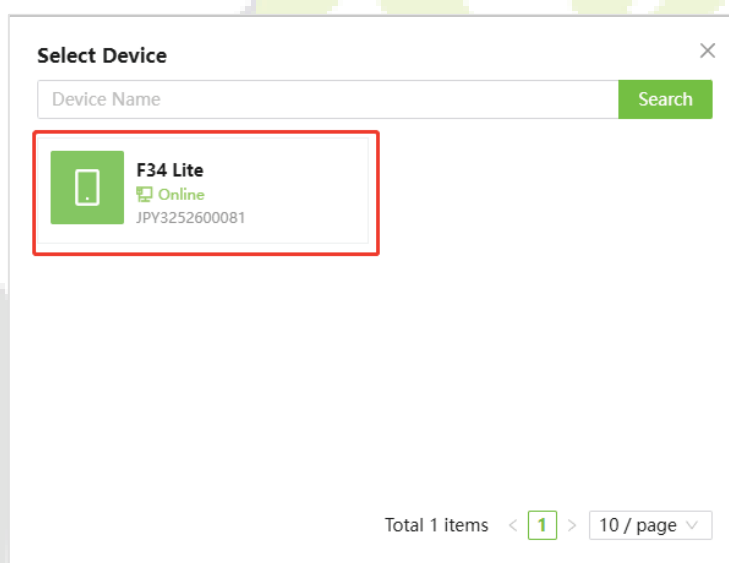
3. And you can repeat the above operation to register other fingers.

## ● Register Card

1. Click **Card** in the Details page. You can select Register on Device or Manually Enter Card Number. If you want to register on device, then click **Register on Device**.

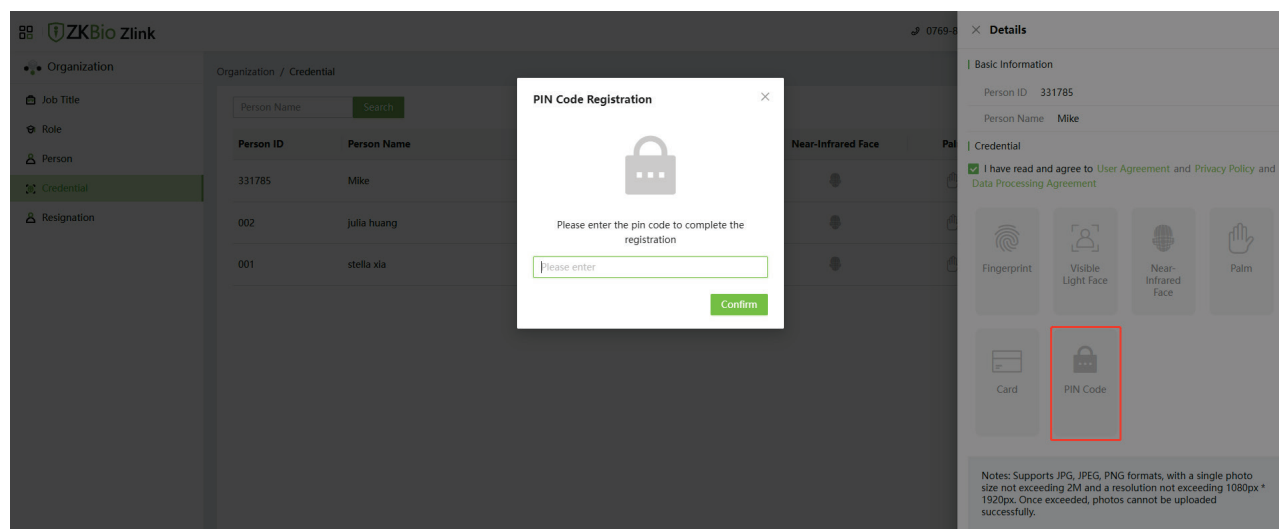


2. Select the registration device, the device will display the **Enroll Card Number** interface. Place the card in the swipe area, when the display shows green ✓, it means the card is successfully registered.



- **Register Password**

Click **PIN Code** in the Details page. Set the password in the pop-up prompt window, and then click **[Confirm]**.



For more details, please refer to the ZKBio Zlink User Manual.

## 21 Connect to ZKBio CVAccess Software

Change the device type as A&C PUSH, then the device can be connected to ZKBio CVAccess, please refer to [9.4 Device Type Setting](#).

### 21.1 Set the Communication Address

1. Press **M/OK** and enter **COMM. > Ethernet** to set the IP address and gateway of the device.  
(**Note:** The IP address should be able to communicate with the ZKBio CVAccess server)
2. Press **M/OK** and enter **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.

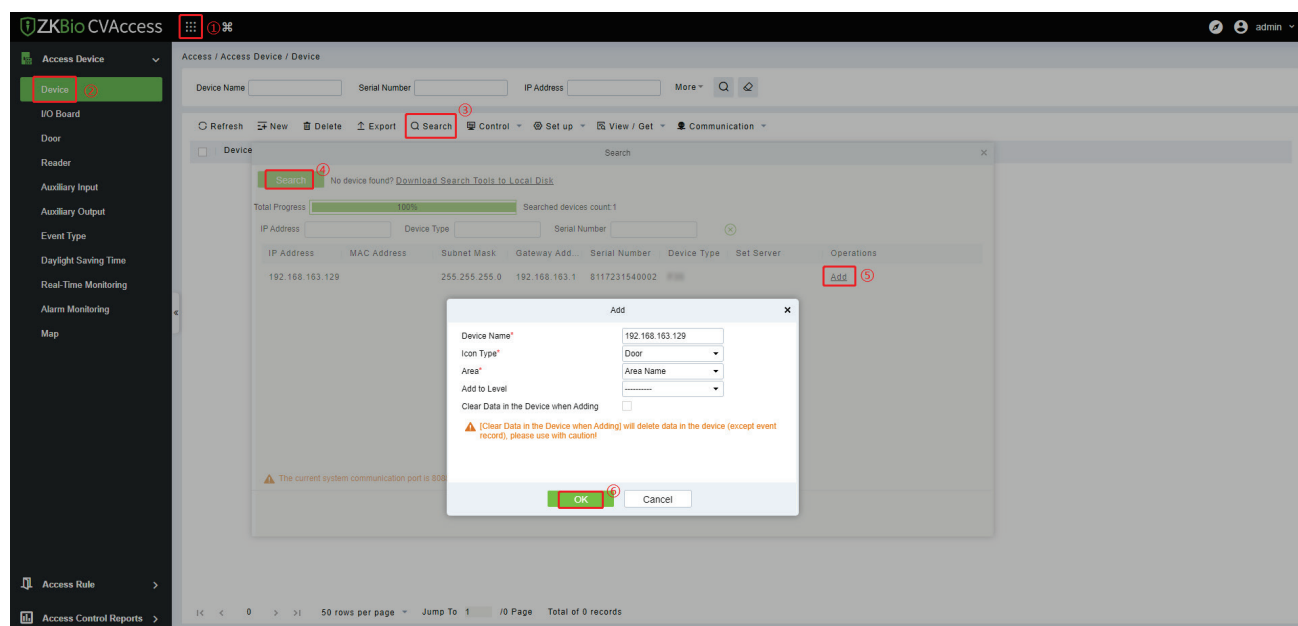
| Ethernet    |                 |
|-------------|-----------------|
| IP Address  | 192.168.163.129 |
| Subnet Mask | 255.255.255.0   |
| Gateway     | 192.168.163.1   |
| DNS         | 8.8.8.8         |

| Cloud Server Settings |                          |
|-----------------------|--------------------------|
| Server Mode           | ADMS                     |
| Enable Domain Name    | <input type="checkbox"/> |
| Server Address        | 58.23.12.98              |
| Server Port           | 8881                     |

### 21.2 Add Device on the Software

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

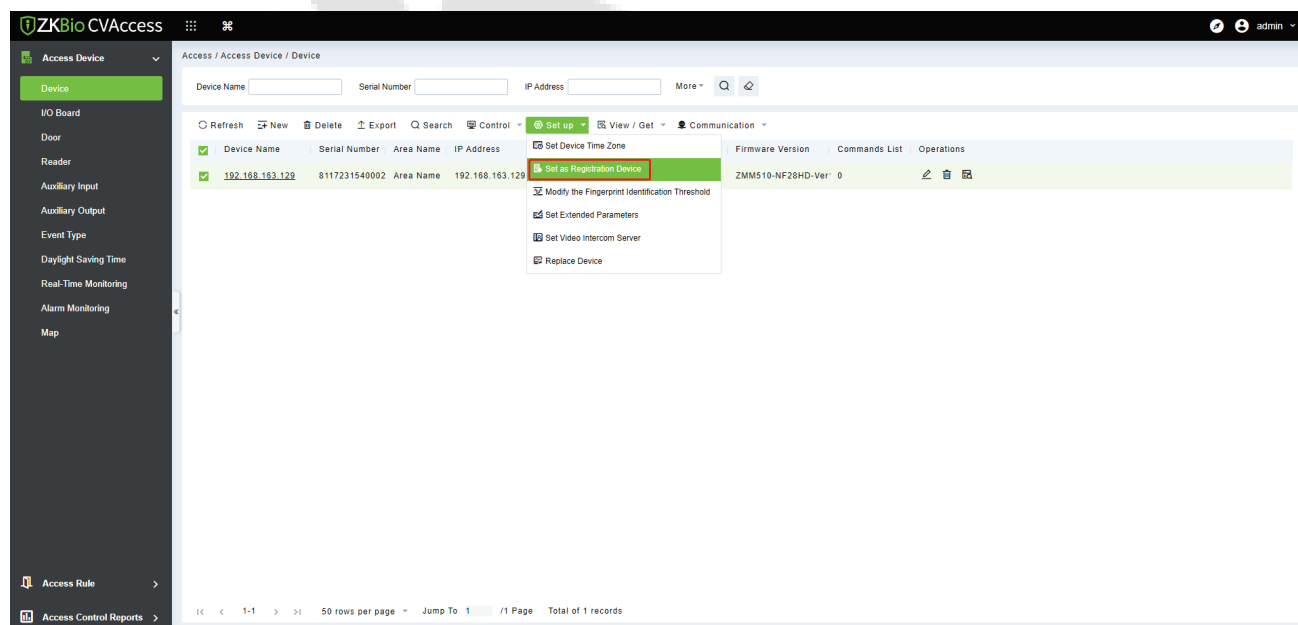
1. Click **Access > Device > Search > Search**, to open the Search interface in the software.
2. Click **Search**, and it will prompt [**Searching.....**].
3. After searching, the list and total number of access controllers will be displayed.



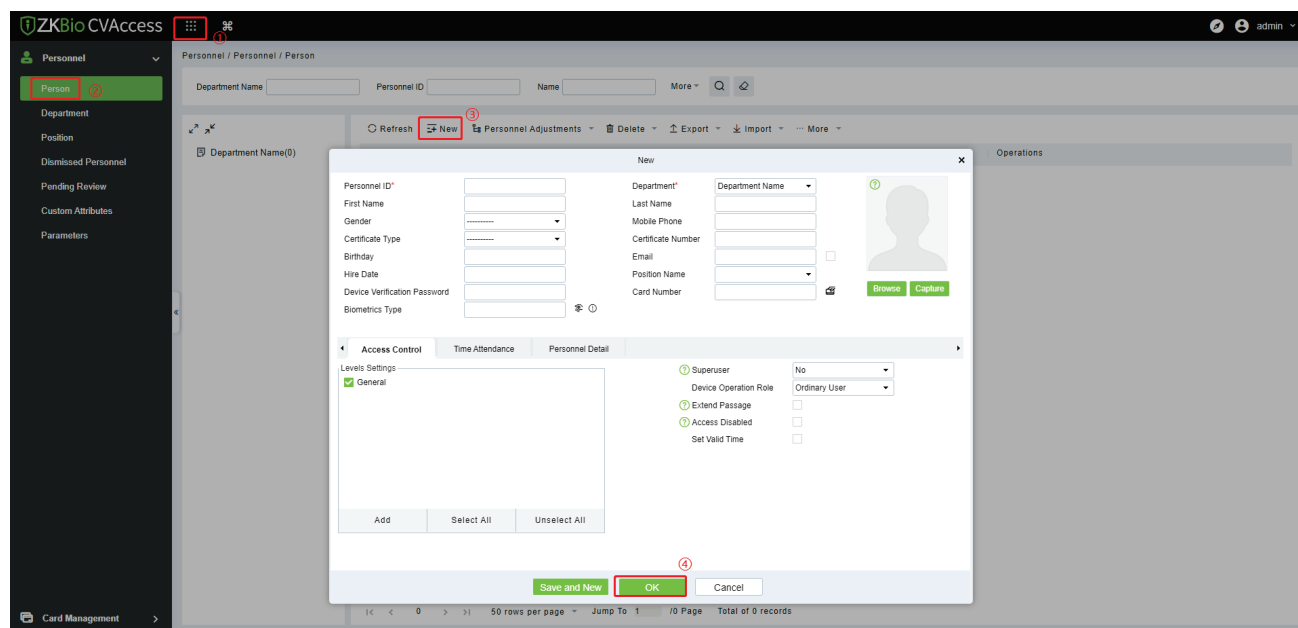
4. Click **[Add]** in operation column, a new window will pop-up. Select Icon type, Area, and Add to Level from each dropdown and click **[OK]** to add the device.
5. After the addition is successful, the device will be displayed in the device list.

## 21.3 Add Personnel on the Software and Online Fingerprint Registration

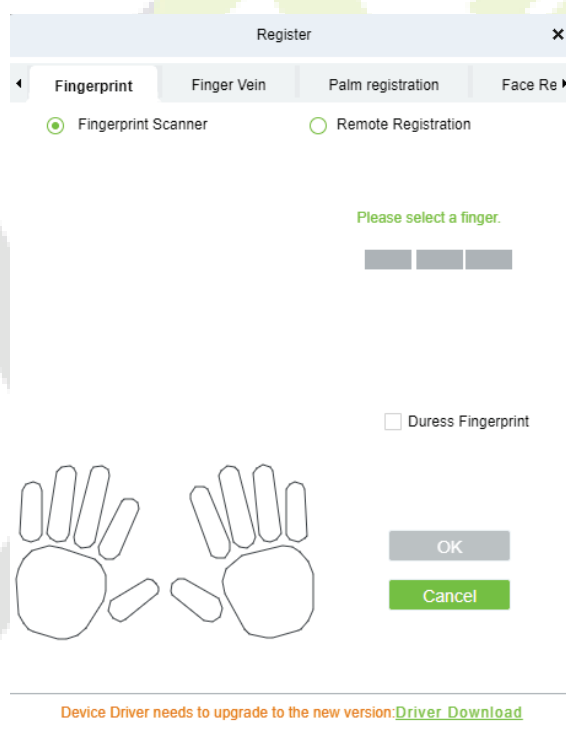
1. In the device list, select the device and click **Set up > Set as Registration Device**.



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



- Fill in all the required fields of the user and click  to enter the online fingerprint registration interface.



- Click **Driver Download** to install the driver first.
- Select **Remote Registration**, then select the IP address of the device and click **Confirm**.