5.2 Cloud Server Setting

When the device is on the initial interface, press **M/OK** button > [**Comm.**] > [**Cloud Server Setting**] to view the cloud server address.

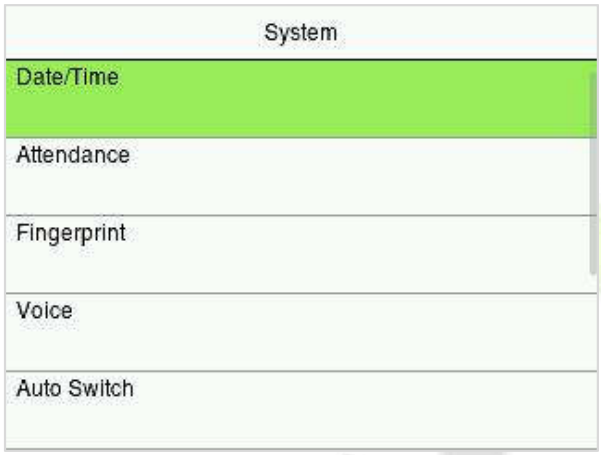
Function Description:

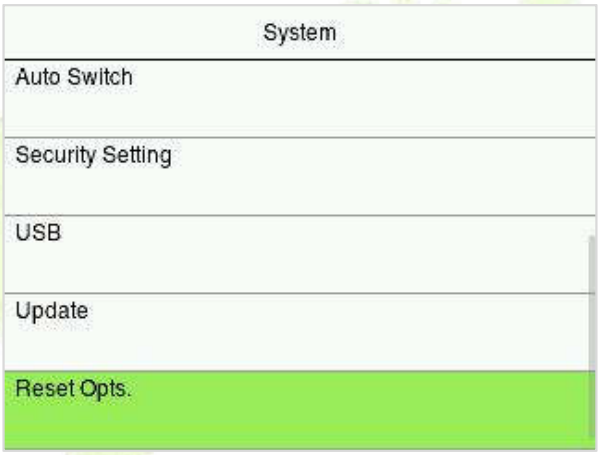
Menu	Descriptions
Server Address	The default is: https://dc.minervalot.com

6 System Settings

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

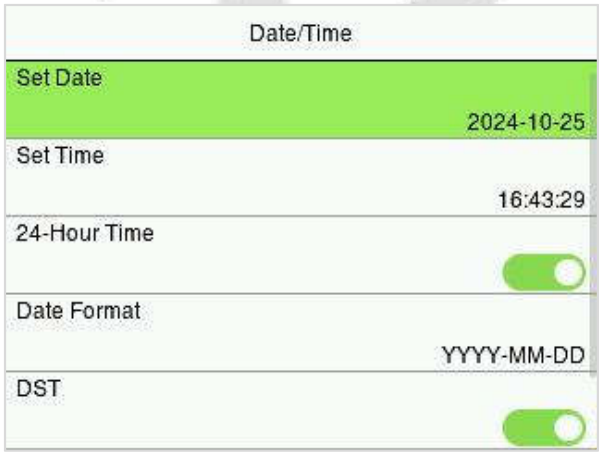
When the device is on the initial interface, press **M/OK** button > [**System**] to set the related system parameters to optimize the performance of the device.

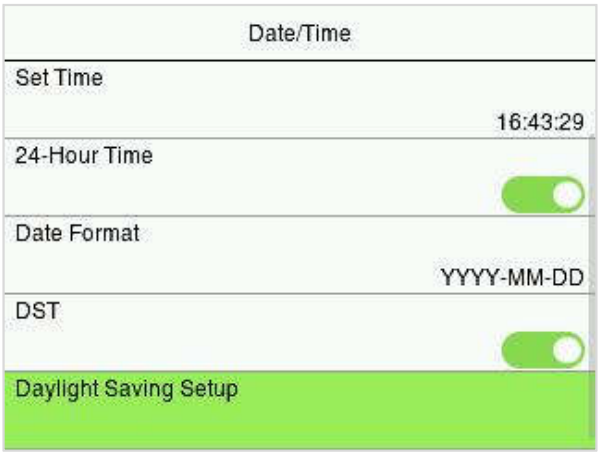




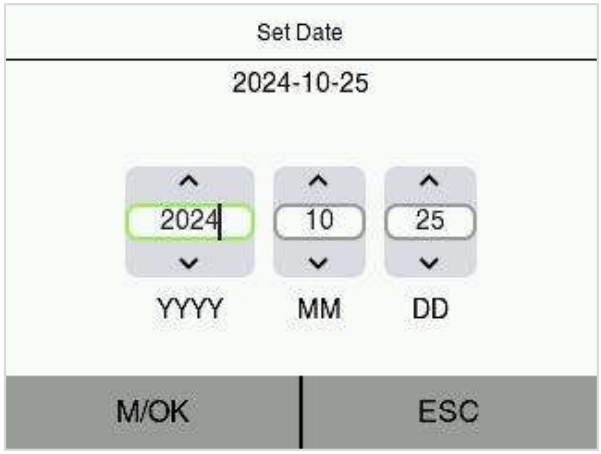
6.1 Date and Time

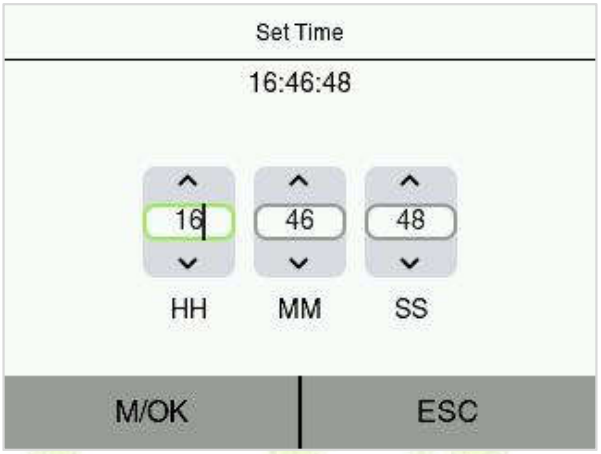
Press **M/OK** button > [**System**] > [**Date/Time**] to set the date and time.



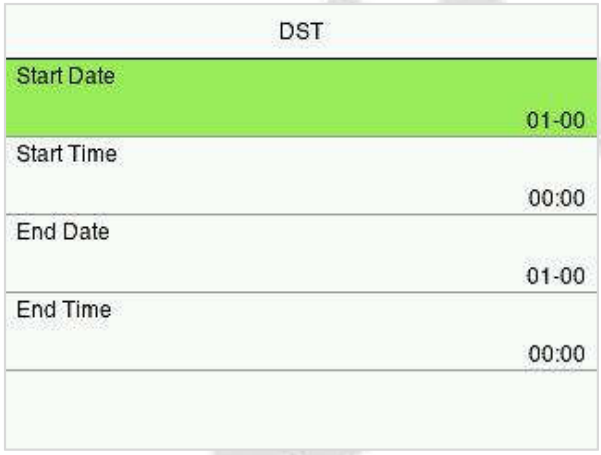


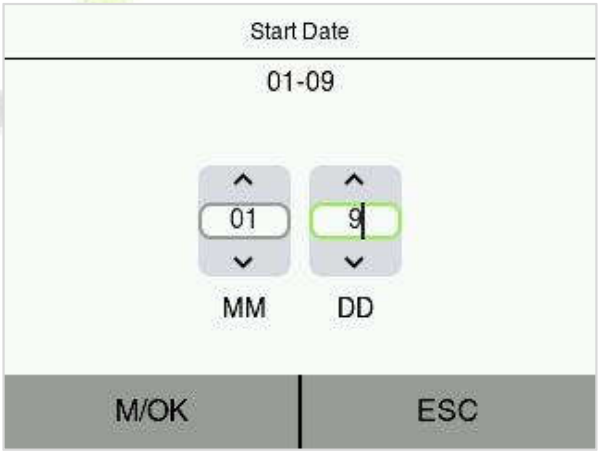
✧ If users need to set the date and time manually, select Set Data and Set Time to set the date and time, then press **M/OK** to save.





- Press **M/OK** to control the icon for **24-Hour Time** to enable or disable this format. If enabled, then select the Date Format to set the date format.
- Press **M/OK** to control the icon for **DST** to enable or disable the Daylight Saving Time function. If enabled, press **Daylight Saving Stetup** to set the switch time.



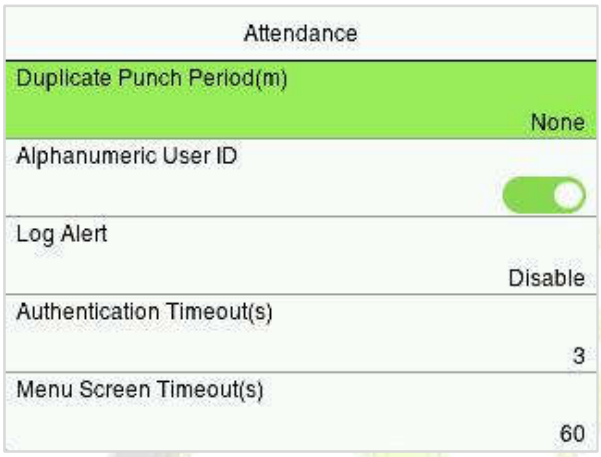


- When restoring the factory settings, the time (24-hour) and date format (YYYY-MM-DD) can be restored, but the device date and time cannot be restored.

Note: *For example, the user sets the time of the device (18:35 on March 15, 2023) to 18:30 on January 1, 2024. After restoring the factory settings, the time of the equipment will remain 18:30 on January 1, 2024.*

6.2 Attendance Settings

When the device is on the initial interface, press **M/OK** button > [**System**] > [**Attendance**] to enter the attendance setting interface.



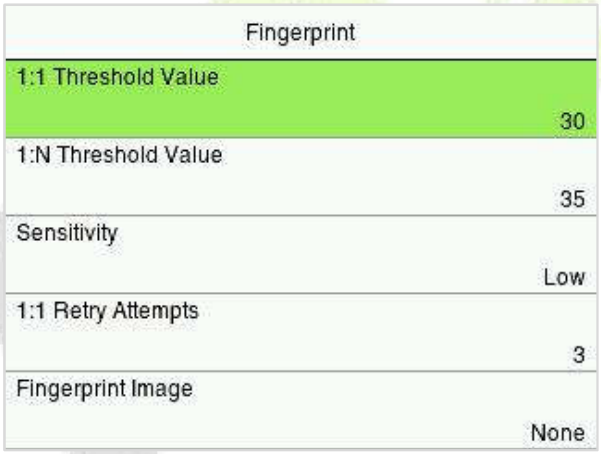
Function Description:

Menu	Description
Duplicate Punch Period(m)	Within a set time period (unit: minutes), the duplicated attendance record will not be reserved (value ranges from 1 to 999999 minutes).
Alphanumeric User ID	Decides whether to support letters in a User ID.
Log Alert	When the record space of the attendance reaches the maximum threshold value, the device automatically displays the memory space warning. Users may disable the function or set a valid value between 1 and 9999.
Authentication Timeout(s)	The time length of the message of successful verification displays. Valid value: 1~9 seconds.

Menu Screen Timeout(s)	Used to set the delay time for exiting from the menu screen to the standby screen. Users may disable the function or set a valid value between 60 and 99999. To disable this function, set the value to 0.

6.3 Fingerprint Parameters

When the device is on the initial interface, press **M/OK** button > [**System**] > [**Fingerprint**] to enter the fingerprint setting interface.



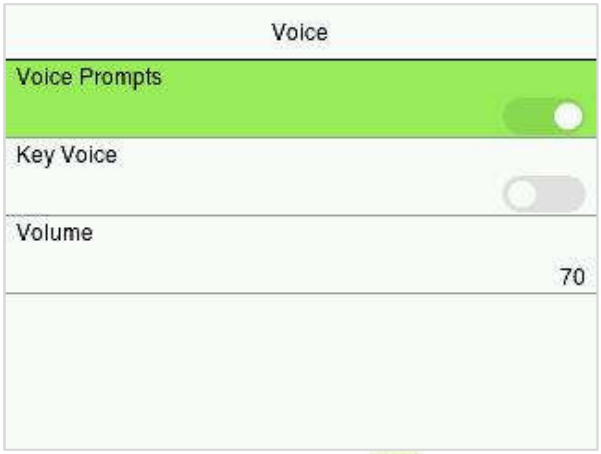
Function Description:

Menu	Descriptions
1:1 Threshold Value	Under 1:1 verification method, the verification will only be successful when the similarity between the acquired fingerprint data and the fingerprint template associated with the entered user ID enrolled in the device is greater than the set value.
1:N Threshold Value	Under 1:N verification method, the verification will only be successful when the similarity between the acquired fingerprint data and the fingerprint templates enrolled in the device is greater than the set value.

Sensitivity	To set the sensibility of fingerprint acquisition. It is recommended to use the default level "**Mid(Medium)**". When the environment is dry, resulting in slow fingerprint detection, you can set the level to "**High**" to raise the sensibility; when the environment is humid, making it hard to identify the fingerprint, you can set the level to "**Low**".
1:1 Retry Attempts	In 1:1 Verification, users might forget the registered fingerprint, or press the finger improperly. To reduce the process of re-entering user ID, retry is allowed.
Fingerprint Image	This function is disabled by default. After disabling it, the fingerprint image will not be displayed when registering and verifying fingerprints. The menu interface allows to enable or disable this function, and there are security prompts when switching. Four choices are available: **Show for enroll**: to display the fingerprint image on the screen only during enrollment. **Show for match**: to display the fingerprint image on the screen only during verification. **Always show**: to display the fingerprint image on screen during enrollment and verification. **None**: not to display the fingerprint image.

6.4 Voice Settings

When the device is on the initial interface, press **M/OK** button > [**System**] > [**Voice**] to configure the voice settings.

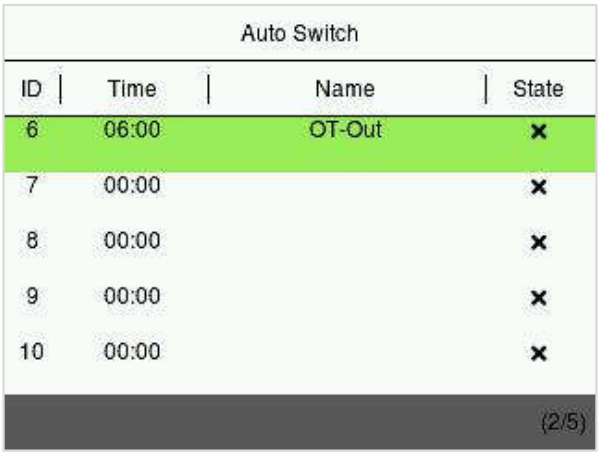


Function Description:

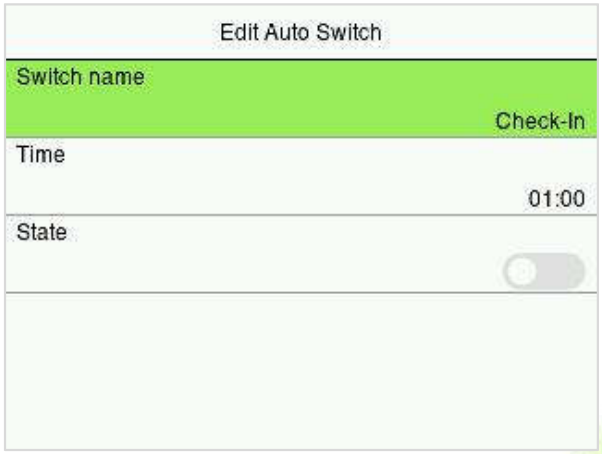
Menu	Descriptions
Voice Prompt	Toggle to enable or disable the voice prompts during function operations.
Key Voice	Toggle to enable or disable the keypad sounds.
Volume	Adjust the volume of the device which can be set between 0 to 100.

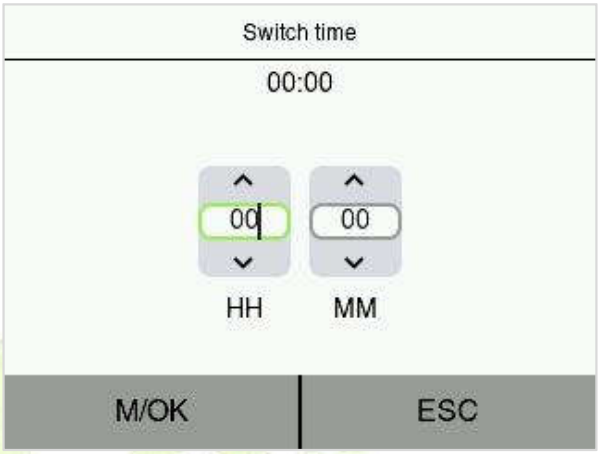
6.5 Auto Switch Settings

When the device is on the initial interface, press **M/OK** button > [**System**] > [**Auto Switch**] to enter the setting interface.



By turning on the auto switch, and setting the switch time. Then within the set time, the standby interface template will automatically display the punch status.

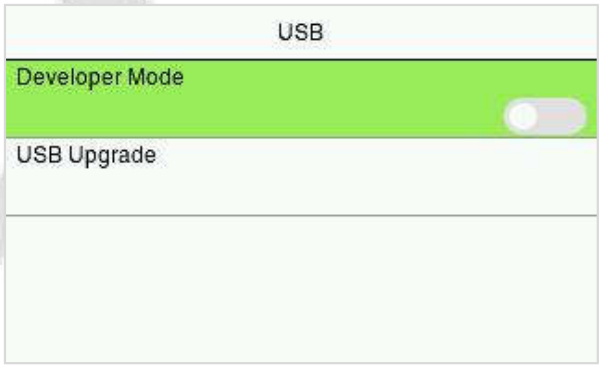




6.6 USB Settings

When the device is on the initial interface, press **M/OK** button > [**System**] > [**USB**] to enter the USB setting interface.

Note: *Only FAT32 format is supported when upgrading firmware using USB disk.*



Function Description:

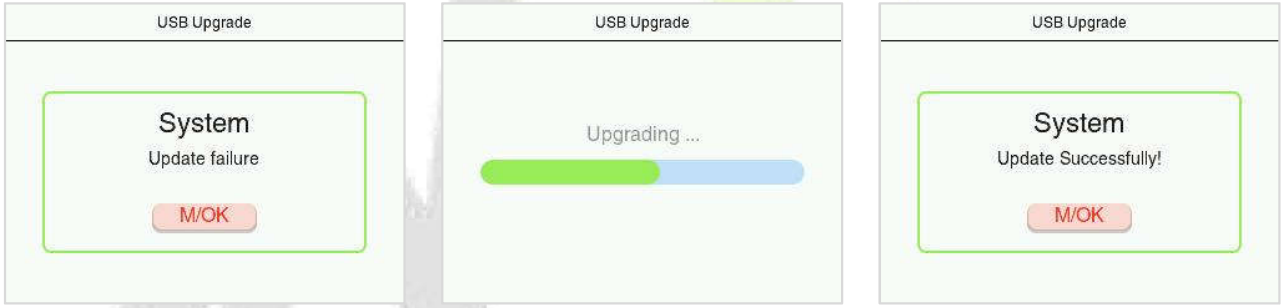
Menu	Descriptions
Developer Mode	When turned on, the device enters developer mode, at which time the USB upgrade function is disabled.

USB Upgrade	Upgrade firmware via USB drive. ***Note:*** *This menu item will not be displayed when Developer Mode is turned on.*

- **USB Upgrade**

The device's firmware program can be upgraded with the upgrade file in a USB drive. Before conducting this operation, please ensure that the USB drive contains the correct upgrade file and is properly inserted into the device. Then select [**USB Upgrade**] and click **M/OK** to upgrade.

If no USB drive is inserted in, the system gives the prompt "**PenDrive not found**" after you tap USB Upgrade on the System interface.

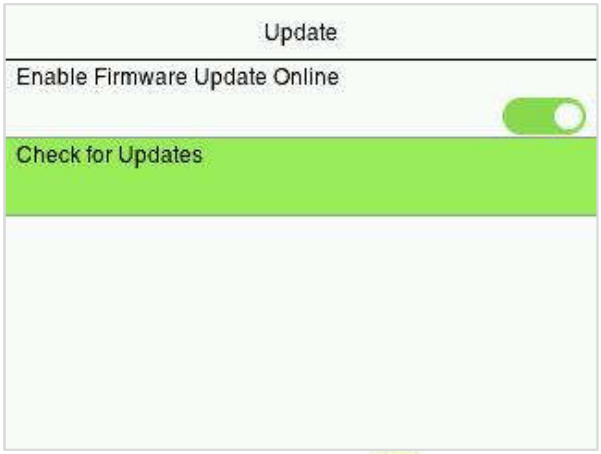


Note: *If upgrade file is needed, please contact our technical support. Firmware upgrade is not recommenced under normal circumstances.*

6.7 Update Firmware Online

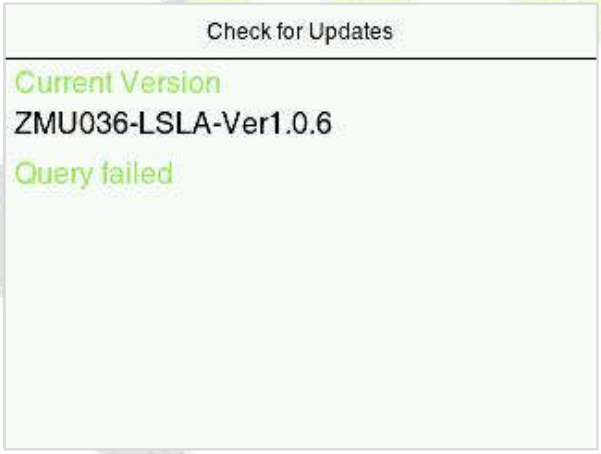
When the device is on the initial interface, press **M/OK** button > [**System**] > [**Update**] to enter the setting interface.

Press **M/OK** button to turn on the **Enable Firmware Update Online** function, the device will prompt that the update may bring some data security risks, which requires manual confirmation by the user (If the security setting function is turned off, the risk warning will not be displayed when the online update is turned on).

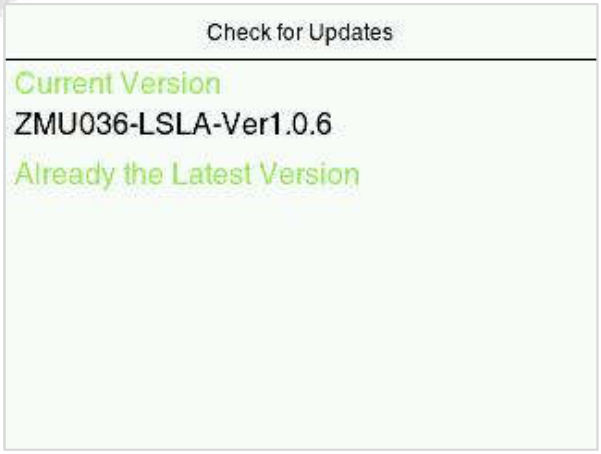


Select [**Check for Updates**] it may have the following 3 scenarios:

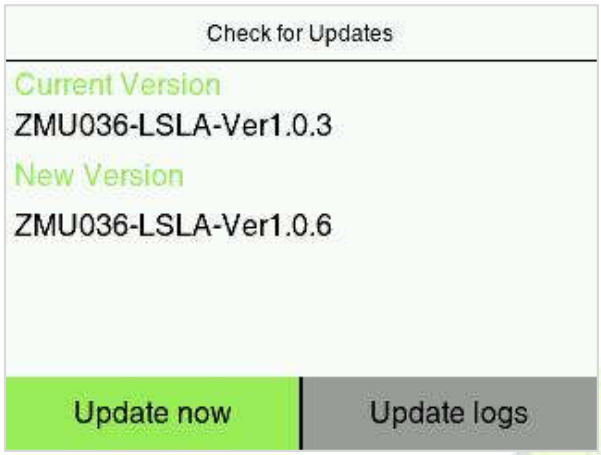
✧ If the query fails, the interface will prompt "**Query failed**".

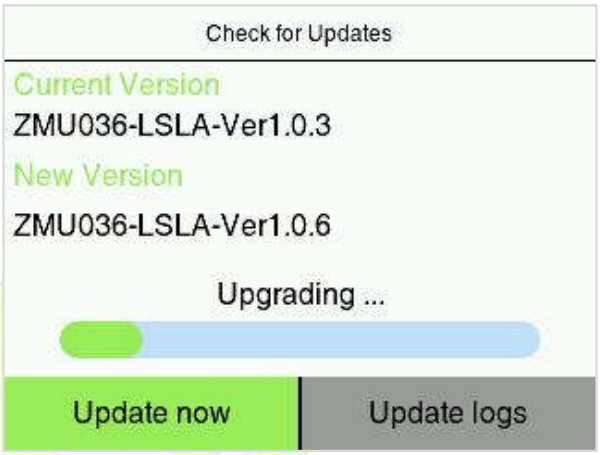


✧ If the firmware version of the device is latest, it will prompt that the current firmware version is already the latest.



✧ 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.

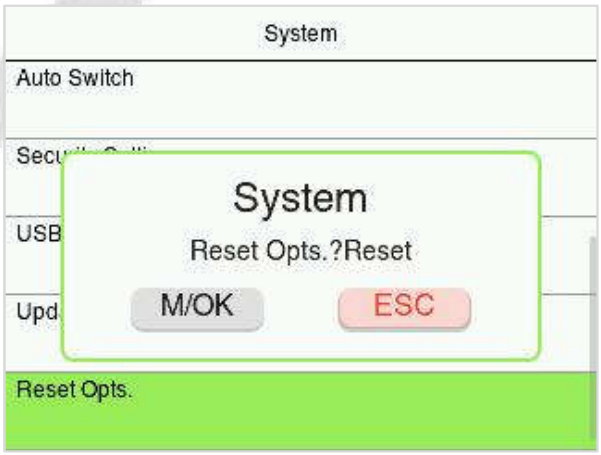




6.8 Factory Reset

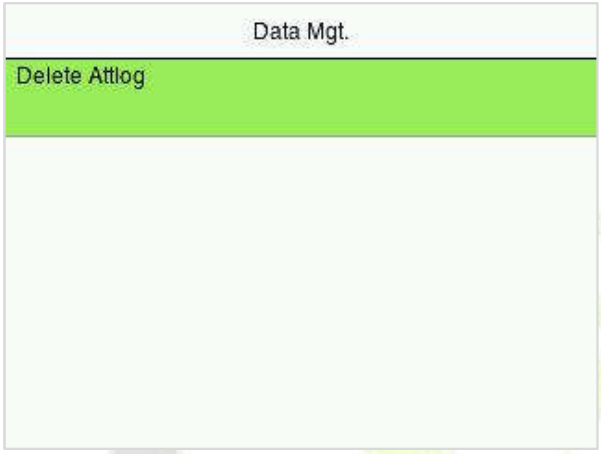
The Factory Reset function restores the device settings such as communication settings and system settings, to the default factory settings (This function does not clear registered user data).

Select [**Reset Opts.**] on the System interface and then press **M/OK** to restore the default factory settings.



7 Data Management

When the device is on the initial interface, press **M/OK** button > [**Data Mgt.**] > [**Delete Attlog**] to delete the specified Attendance log.



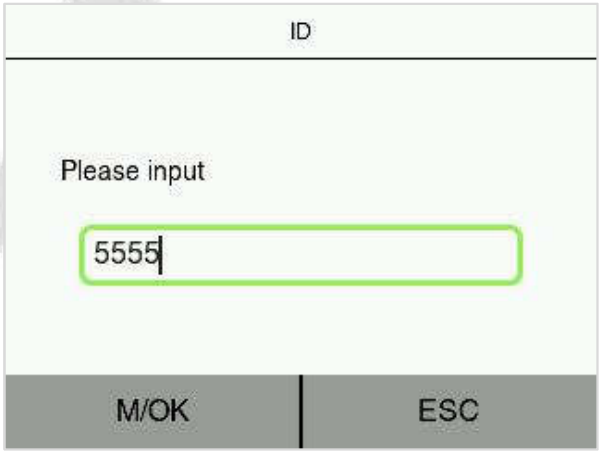
Select [**Delete Attlog**] in the data management interface, and in the pop-up confirmation interface, click **M/OK** to delete all attendance records.

8 Record

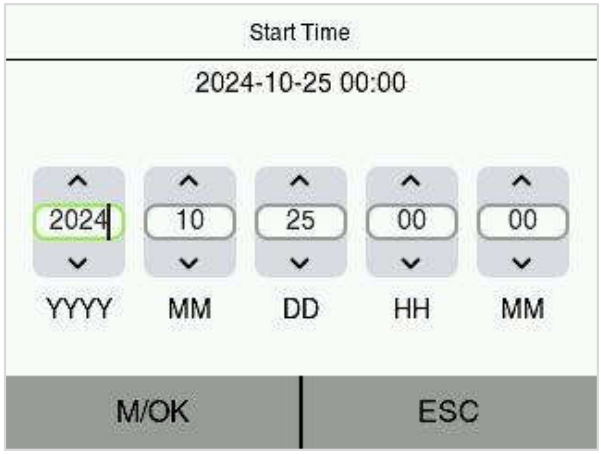
Once the identity of a user is verified, the Event Logs will be saved in the device. This function enables users to check their attendance records.

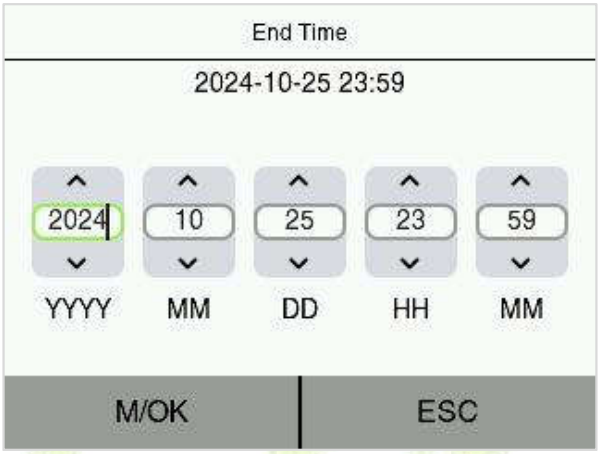
When the device is on the initial interface, press **M/OK** button > [**Record**] to search for the required Attendance log.

1. Enter the user ID to be searched and click **M/OK**. If you want to search for logs of all users, click **M/OK** without entering any user ID.



2. Select the time range in which the logs need to be searched.



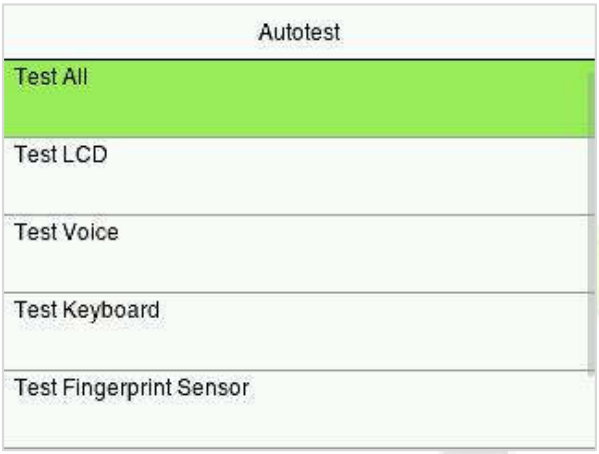


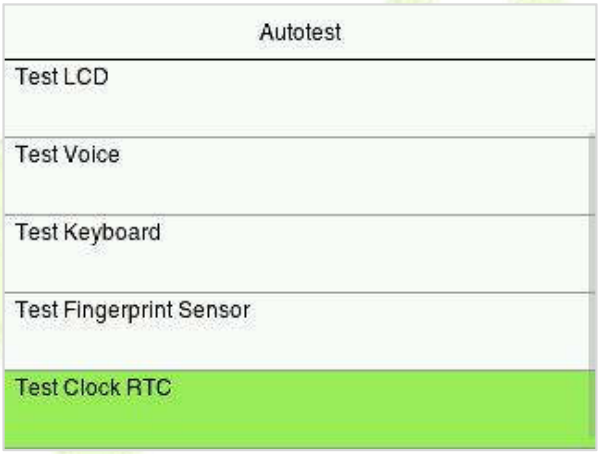
3. Once the log search succeeds. Select the login highlighted in green to view its details.

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

9 Autotest

When the device is on the initial interface, press **M/OK** button > [**Autotest**] to to automatically test whether all modules in the device function properly, which include the LCD, Voice, keyboard and Real-Time Clock (RTC).





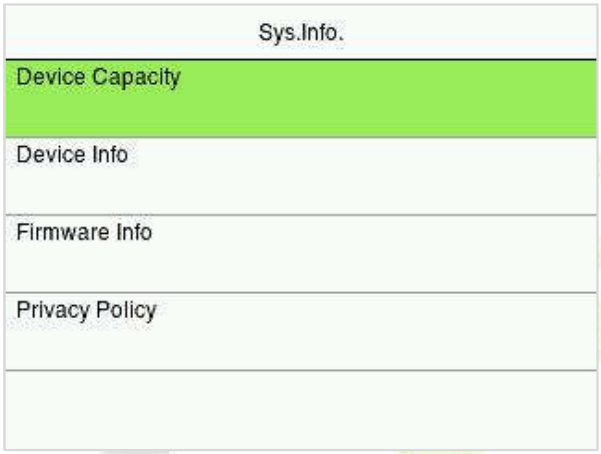
Function Description:

Menu	Descriptions
Test All	To automatically test whether the LCD, Audio, Camera and RTC are normal.
Test LCD	To automatically test the display effect of LCD screen by displaying full-color, pure white, and pure black to check whether the screen displays colors normally.
Test Voice	To automatically test whether the audio files stored in the device are complete and the voice quality is good.
Test Keyboard	The terminal tests whether every key on the keyboard works normally. Press any key on the Keyboard Test interface to check whether the pressed key matches the key displayed on screen. The keys are dark-gray being before pressed, and turn blue after pressed.

Test Fingerprint Sensor	To test the fingerprint sensor by pressing a finger on the scanner to check if the acquired fingerprint image is clear. When you are pressing a finger on the scanner, the fingerprint image will display on the screen.
Test Clock RTC	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.

10 System Information

When the device is on the initial interface, press **M/OK** button > [**Sys. Info.**] to view the storage status, the version information of the device, firmware information and privacy policy.



Function Description:

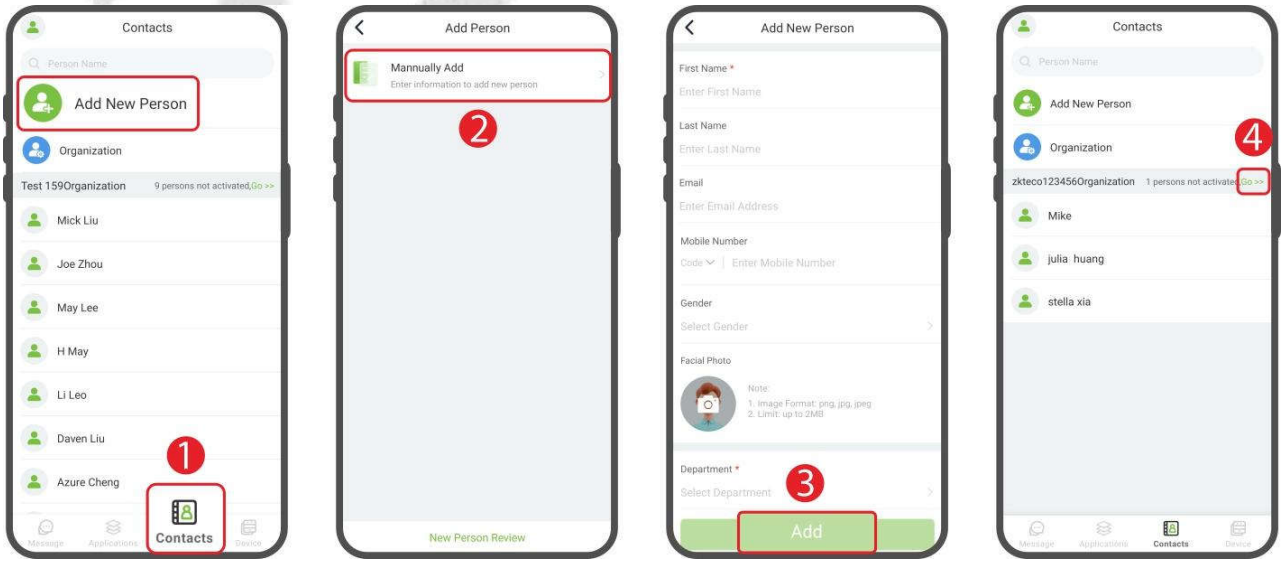
Function Name	Description
Device Capacity	It displays the number of registered users, administrators, passwords, fingerprints, card and attendance records.
Device Info	Displays the device's name, serial number, MAC address, fingerprint algorithm, platform information and vendor.
Firmware Info	Displays the firmware versionof the device.
Privacy Policy	Displays the contents of the privacy policy.

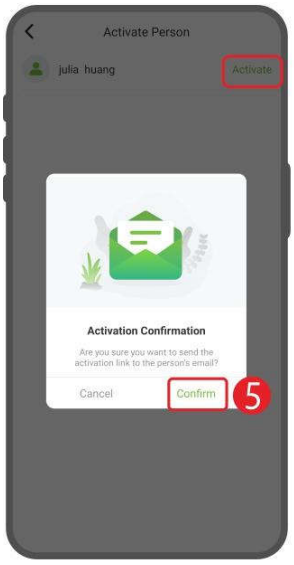
11 Operation on the ZKBio Zlink App

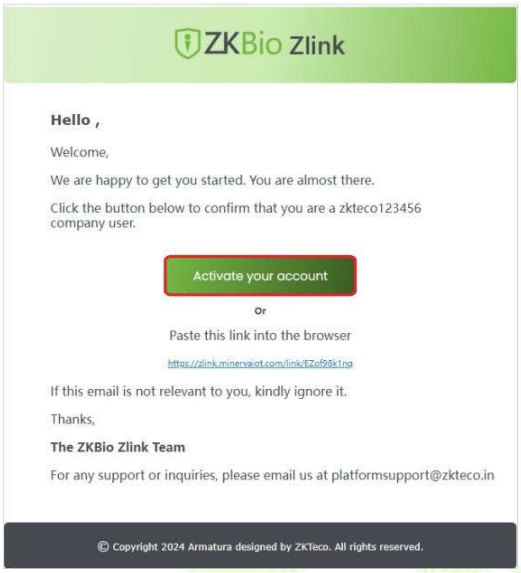
11.1 Add Person

1. Click [**Contacts**] > [**Add New Person**] to enter Add Person interface.
2. Then click [**Manually Add**] to enter the Add person profile interface.
3. After you have entered the personnel information, click [**Add**]. When the interface prompts "**Added successfully**", it means the addition is successful. And the added personnel will be displayed in the personnel list.

   Note: *The Mobile Number or Email needs to be entered so that the person can receive the activation link.*
4. The page displays the number of inactive persons. Click [**Go >>**] > [**Activate**] to send the activation link to the person.
5. Click [**Confirm**] to confirm and exit.
6. Then the person will receive an activation email. After the person activating the account, the person will be activated.

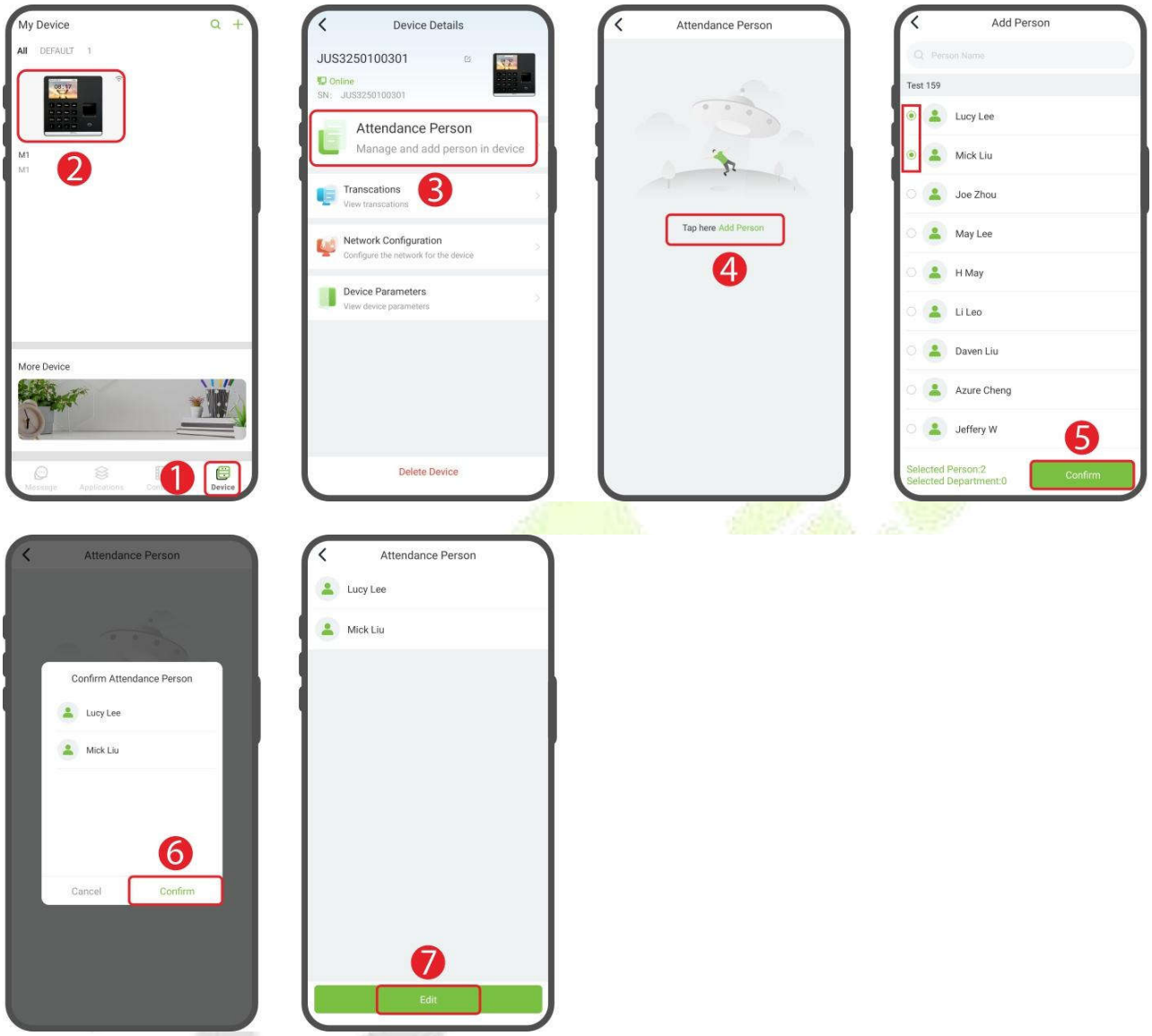






11.2 Manage and Add Person in Device

1. Click [**Device**] to enter the My Device list interface.
2. Then select the device in the list to enter the Device Details interface.
3. Click [**Attendance Person**] to enter the Attendance Person interface.
4. Click [**Add Person**] to enter the add person interface.
5. Select the persons and click [**Confirm**] to add them to the device.
6. Click [**Confirm**] in the pop-up confirmation window.
7. After completion, the personnel will be added to the attendance person list, and you can click [**Edit**] to edit and modify.



11.3 Register Verification Mode on the App

Once you have added people to the device, you can register Verification Modes to them. **Note:** It must be based on the features actually supported by the device.

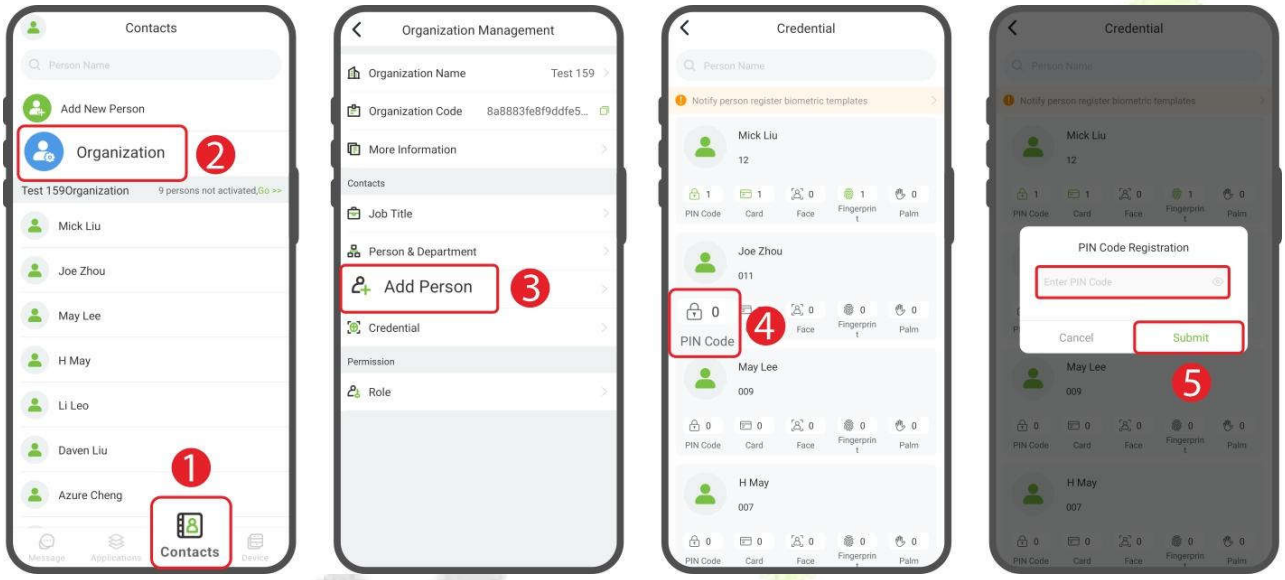
11.3.1 Register Password

1. In the bottom menu of App, click [**Contacts**] > [**Organization**].
2. Click [**Add Person**] to enter the credential management interface.
3. In the credential management screen, select the personnel for whom you

want to register a password.

4. Then click on the icon and enter the password in the pop-up window.

5. Click [**Submit**] to confirm.



11.3.2 Register Card

1. In the bottom menu of App, click [**Contacts**] > [**Organization**] > [**Credential**].

2. In the credential management screen, select the personnel for whom you want to register a card number.

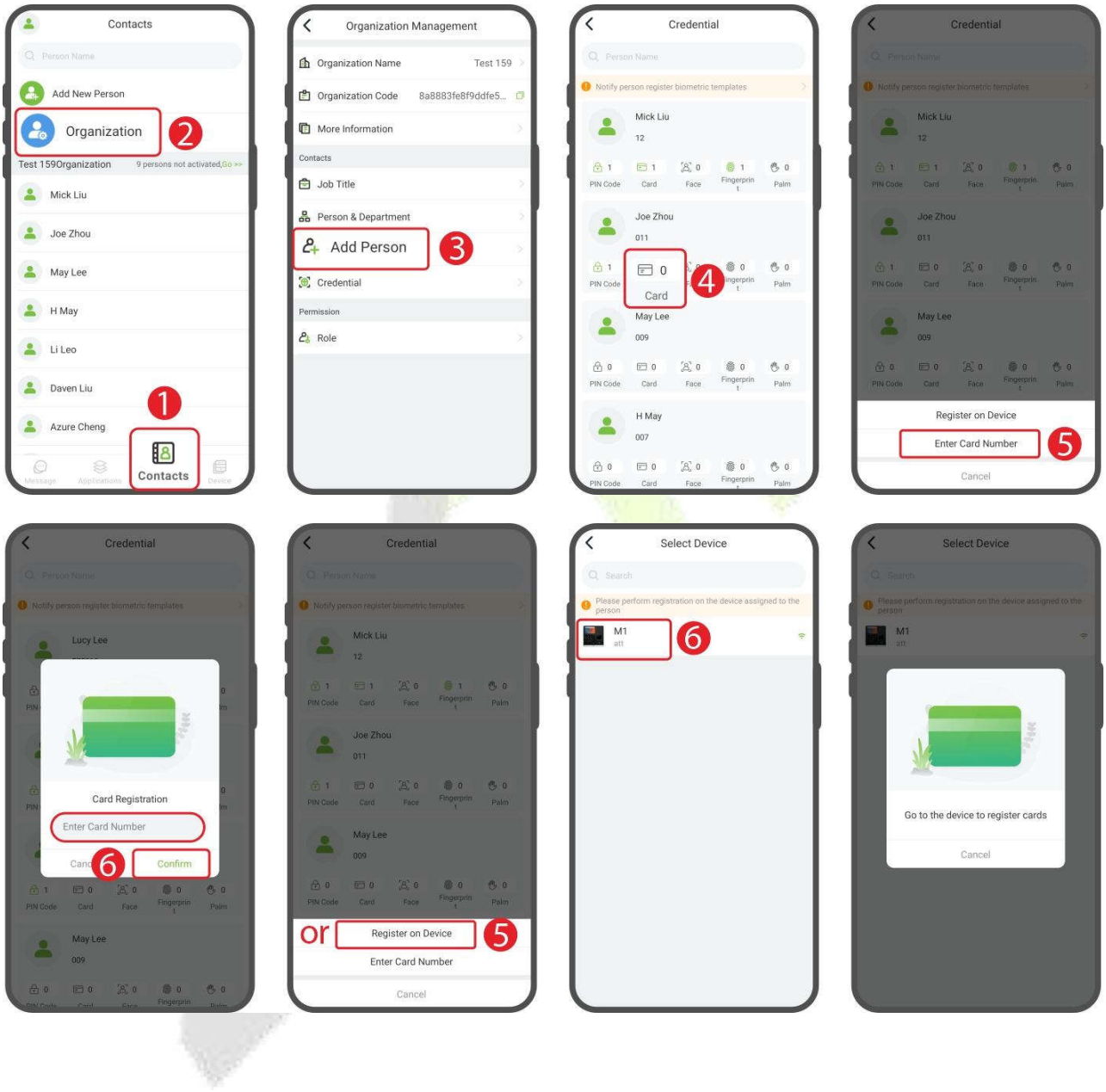
3. Then click on the icon. You can select Register on Device or Manually Enter Card Number.

4. If you select **Enter Card Number**, just enter your card number directly into the registration window that pops up and click [**Confirm**] to finish.

5. If you select **Register on Device**, you need to select the device first in the device list screen.

6. The interface will pop up a prompt, and at the same time the device will display 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.



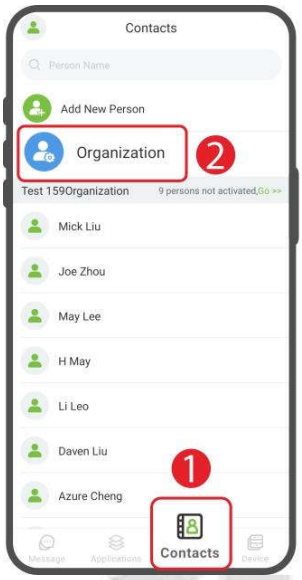
11.3.3 Register Fingerprint

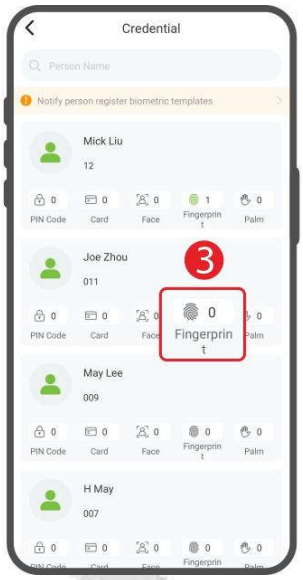
1. In the bottom menu of App, click [**Contacts**] > [**Organization**] > [**Credential**].
2. In the credential management screen, select the personnel for whom you want to register a fingerprint.
3. Then click on the icon.

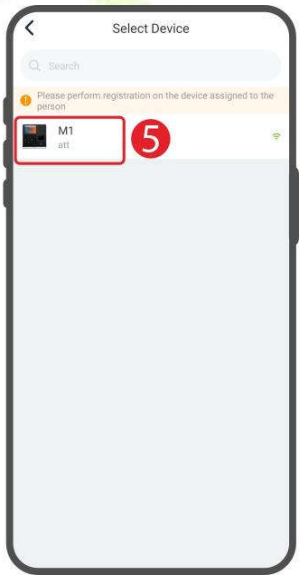
4. Select [**Registration on Device**] in the pop-up menu.

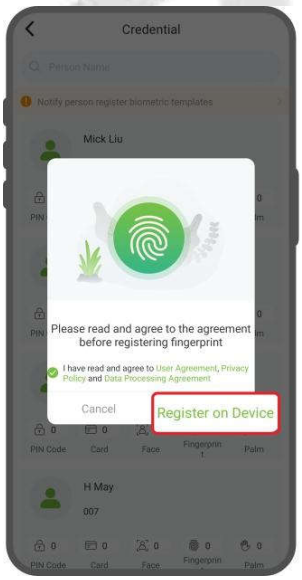
5. Select the **Device** in the device list, at the same time, the device displays the fingerprint registration screen. According to the prompts, place your finger on the fingerprint sensor and press **3** times. When the interface prompts "**Enrolled successfully**", it means the fingerprint registration is successful.

6. Just follow the prompts when finished.





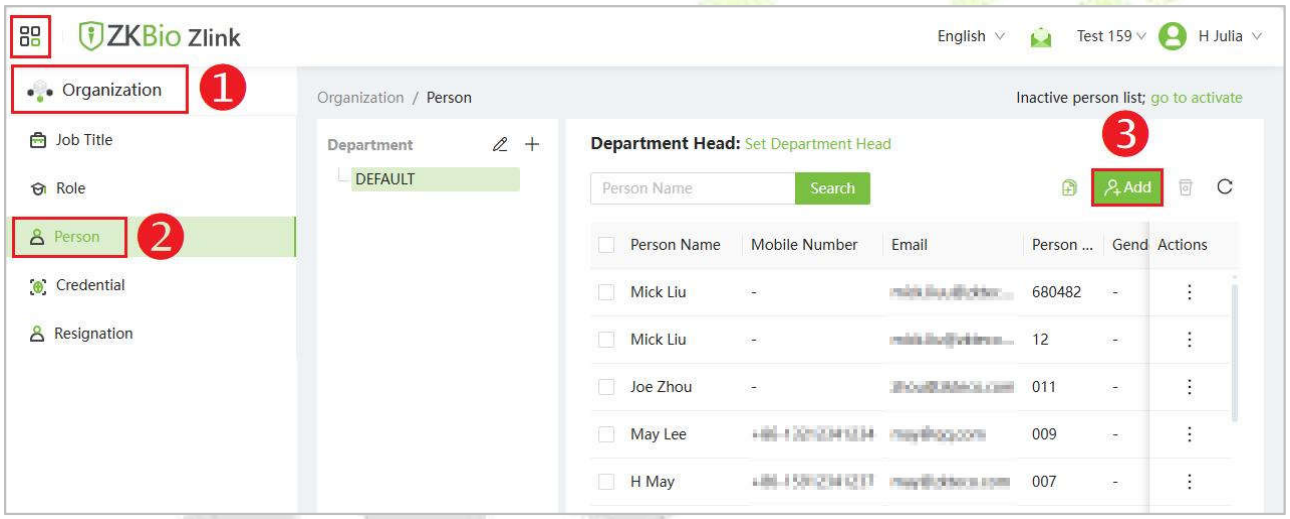




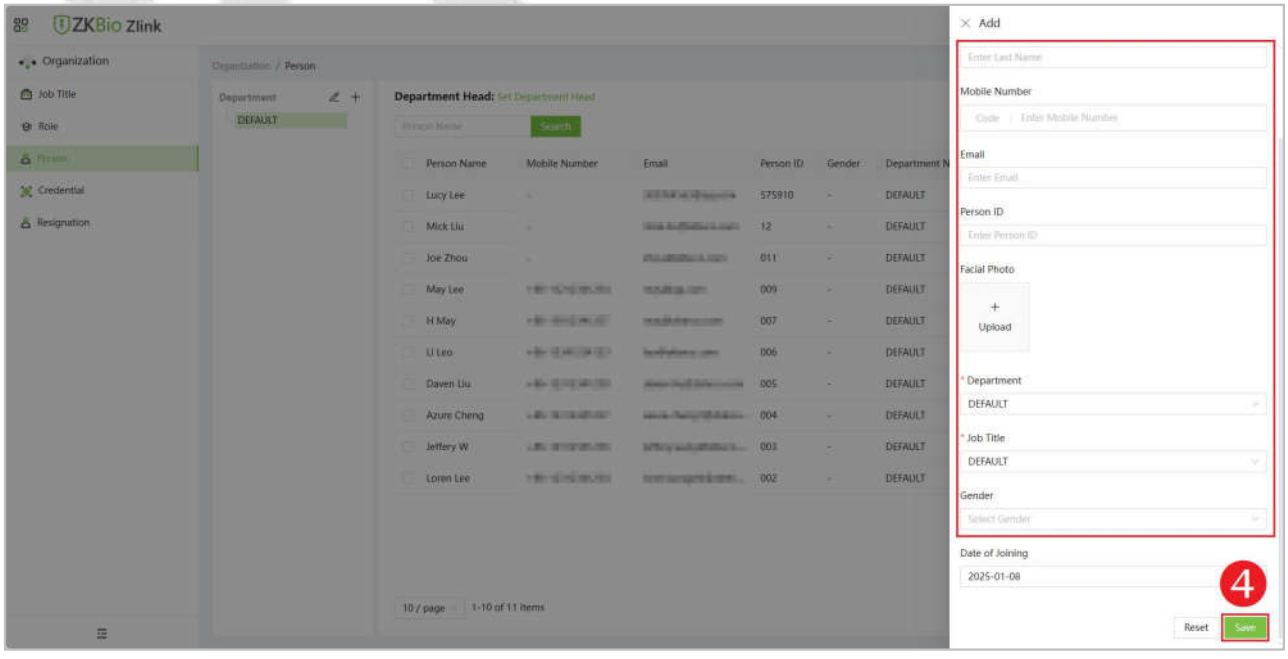
12 Operation on the ZKBio Zlink Web

12.1 Add Person

1. Log in to the ZKBio Zlink Web with the account you have created. Then click the icon on the top left corner, and click [**Organization**] > [**Person**] > [**Add**] to add a new person.

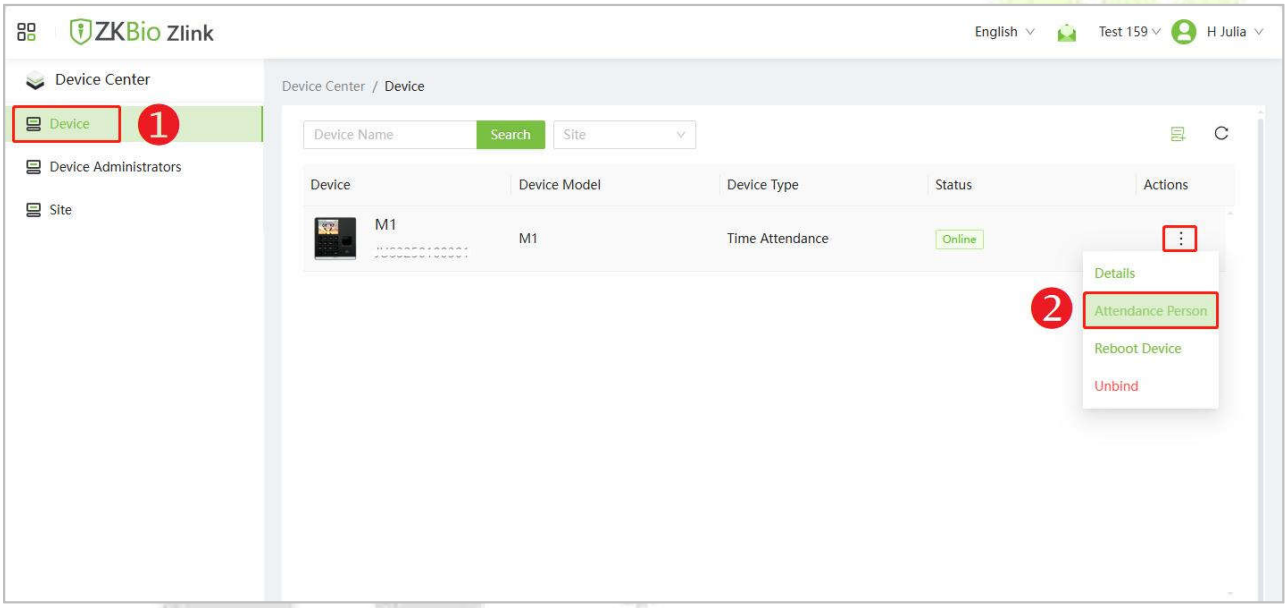


2. Enter the basic information of the person and click [**Save**].

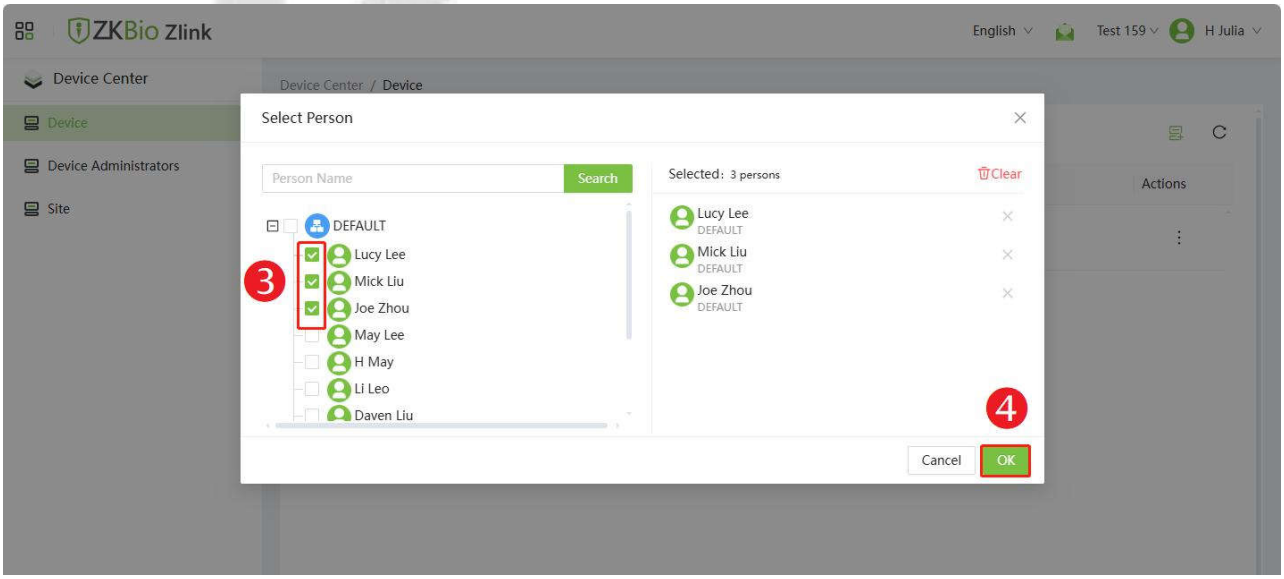


12.2 Manage and Add Person to Device

1. Click the icon on the top left corner, and click [**Device Center**] > [**Device**] to enter the device setting interface. Then select the device you want to synchronize people with, click the icon after it and select [**Attendance Person**] from the pop-up menu to enter the setting interface.

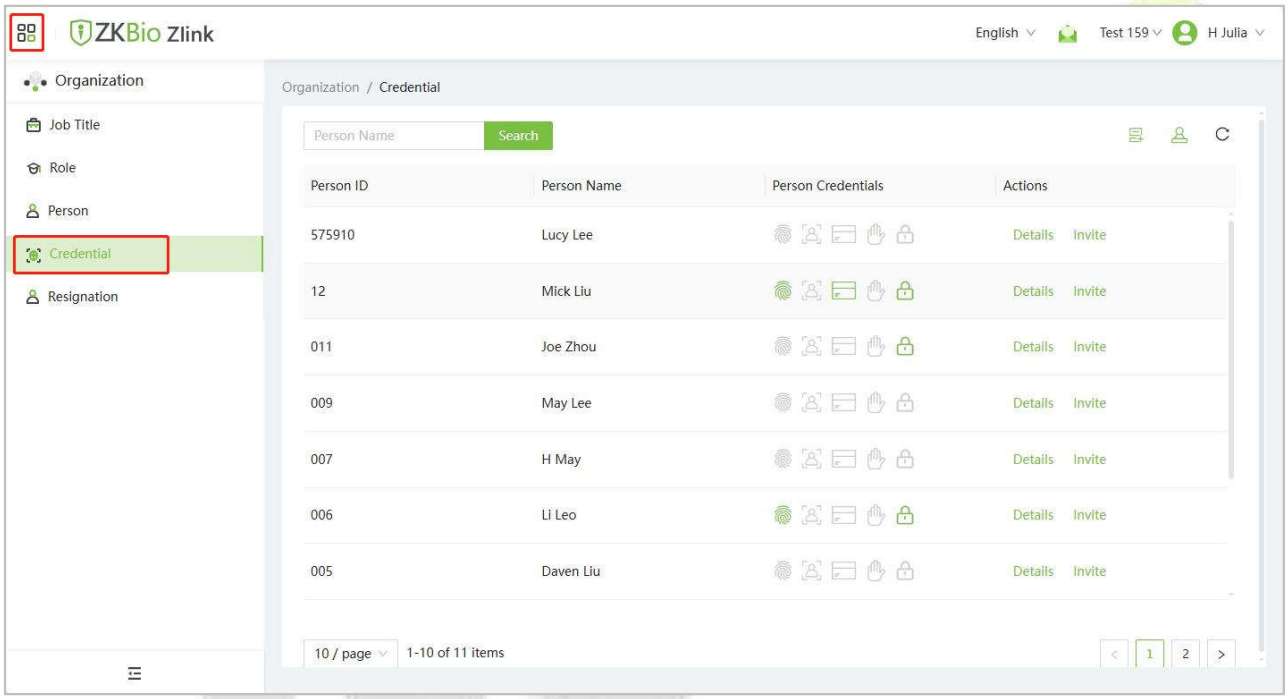


2. Tick the person in the pop-up window and click [**OK**] to add the person to the device.

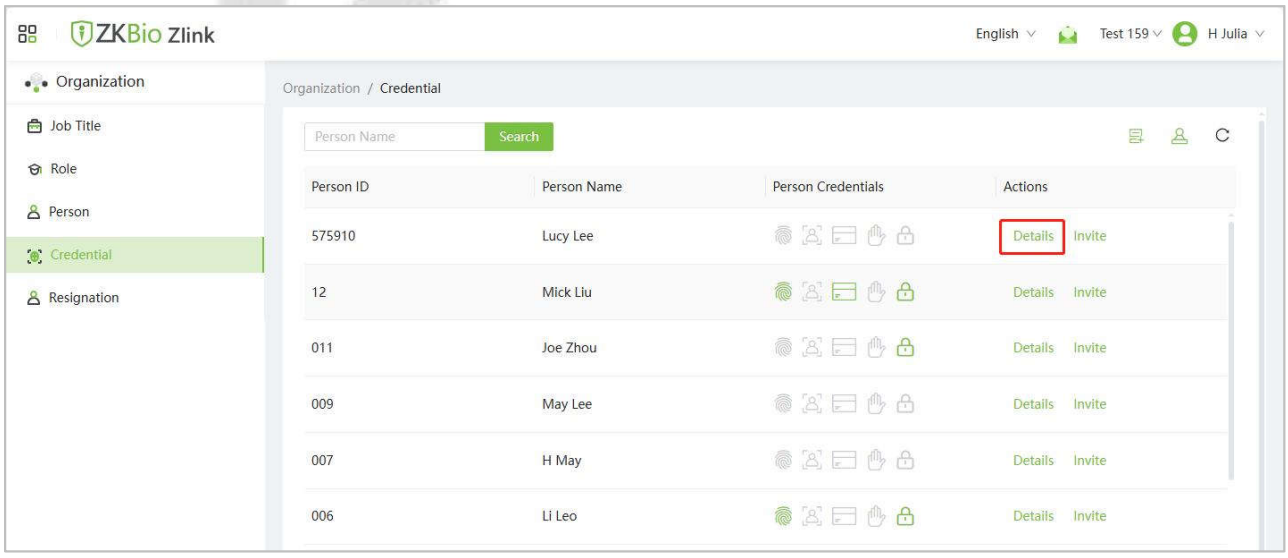


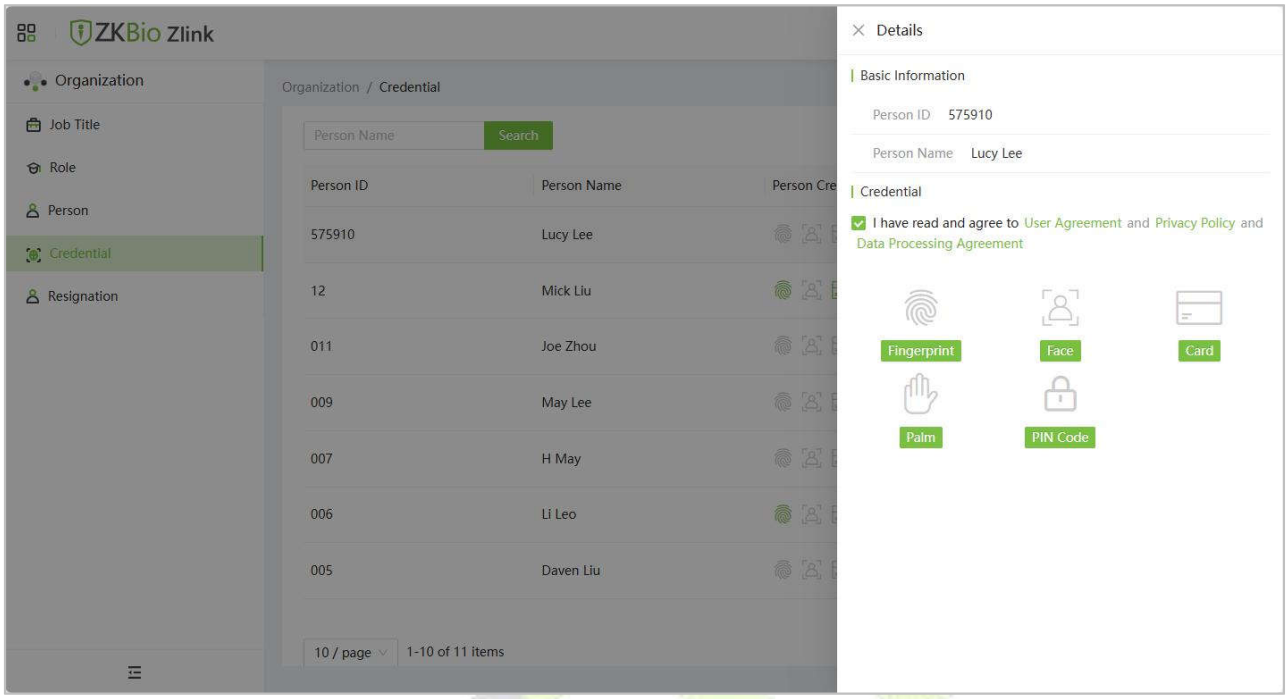
12.3 Register Verification Mode on the Web

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



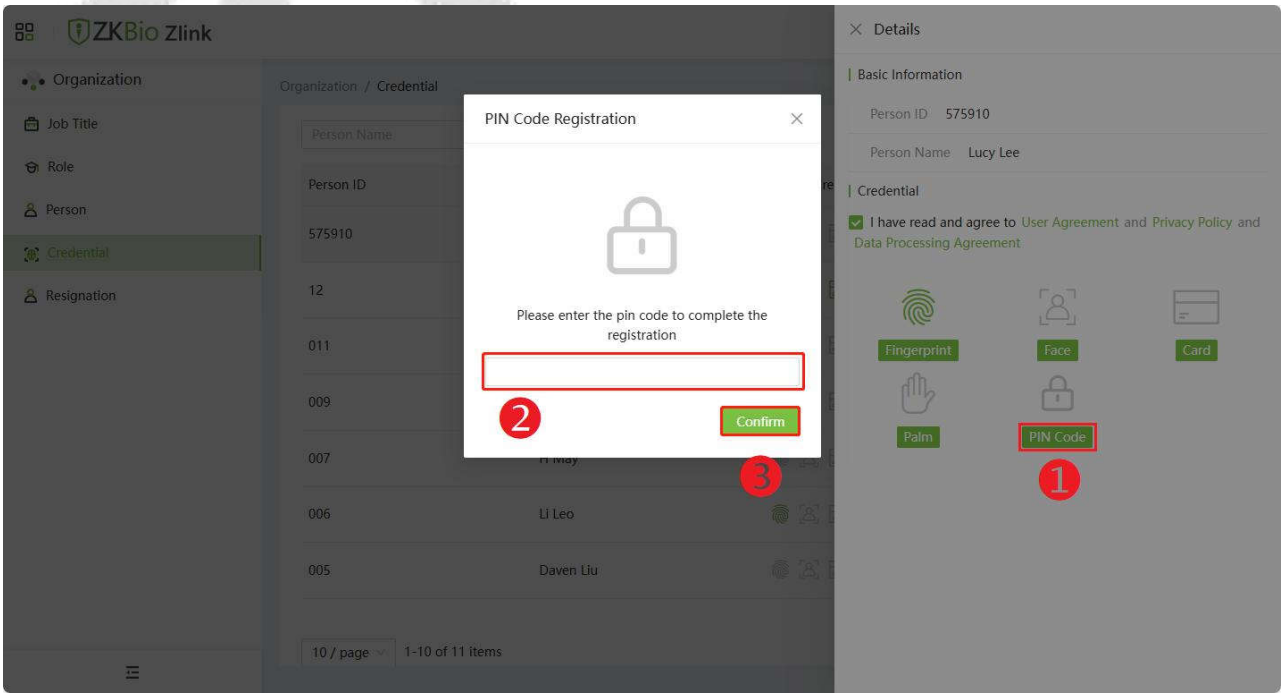
2. Select the person and click [**Details**] that follows, tick Agreement and click **Fingerprint/Card/PIN Code** to remotely register the personnel biometric verification mode.





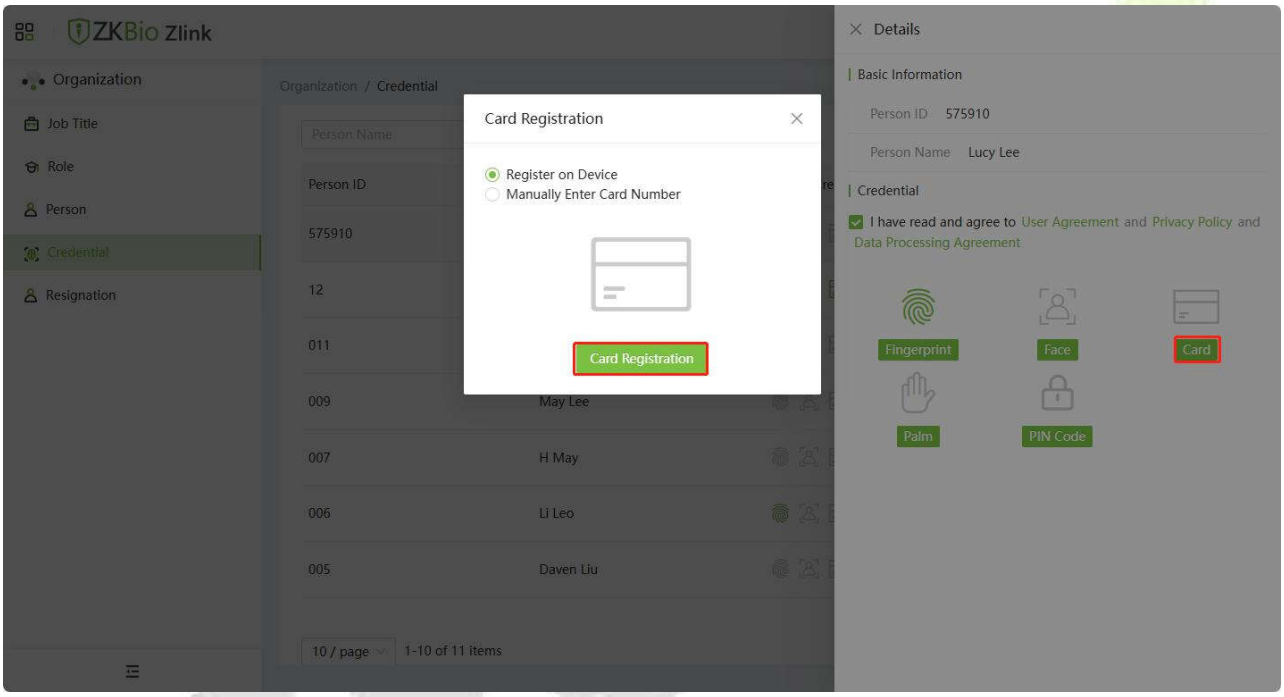
12.3.1 Register Password

Select the person whose password you want to enroll and click [**PIN Code**]. Set the password in the pop-up prompt window, and then click [**Confirm**] to confirm.

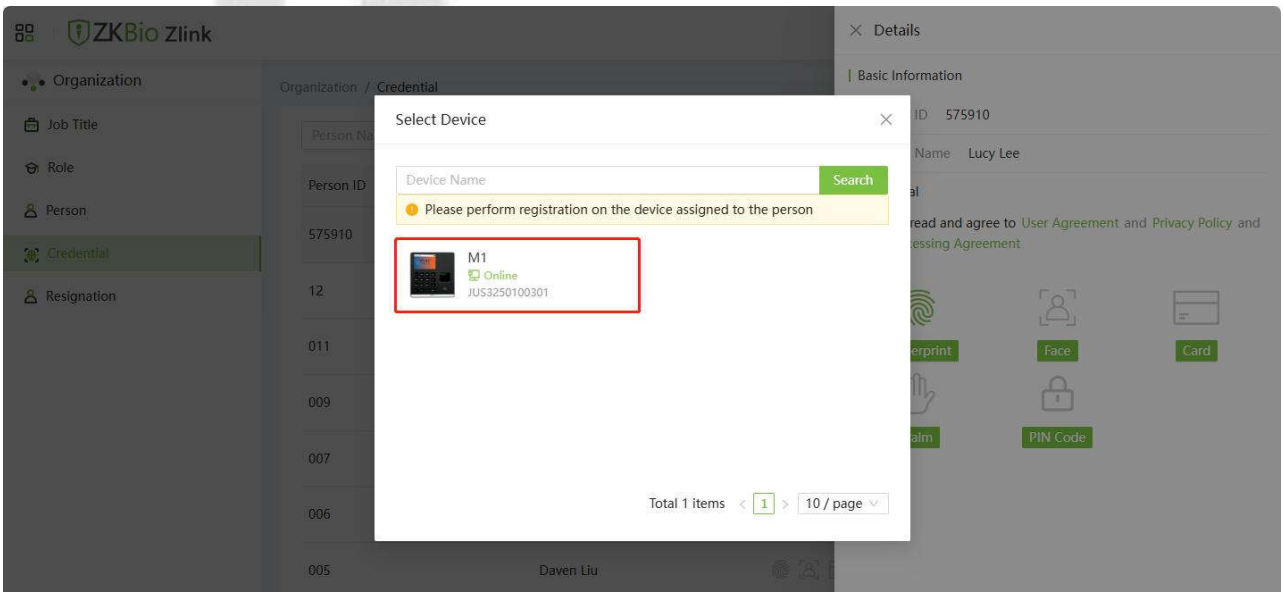


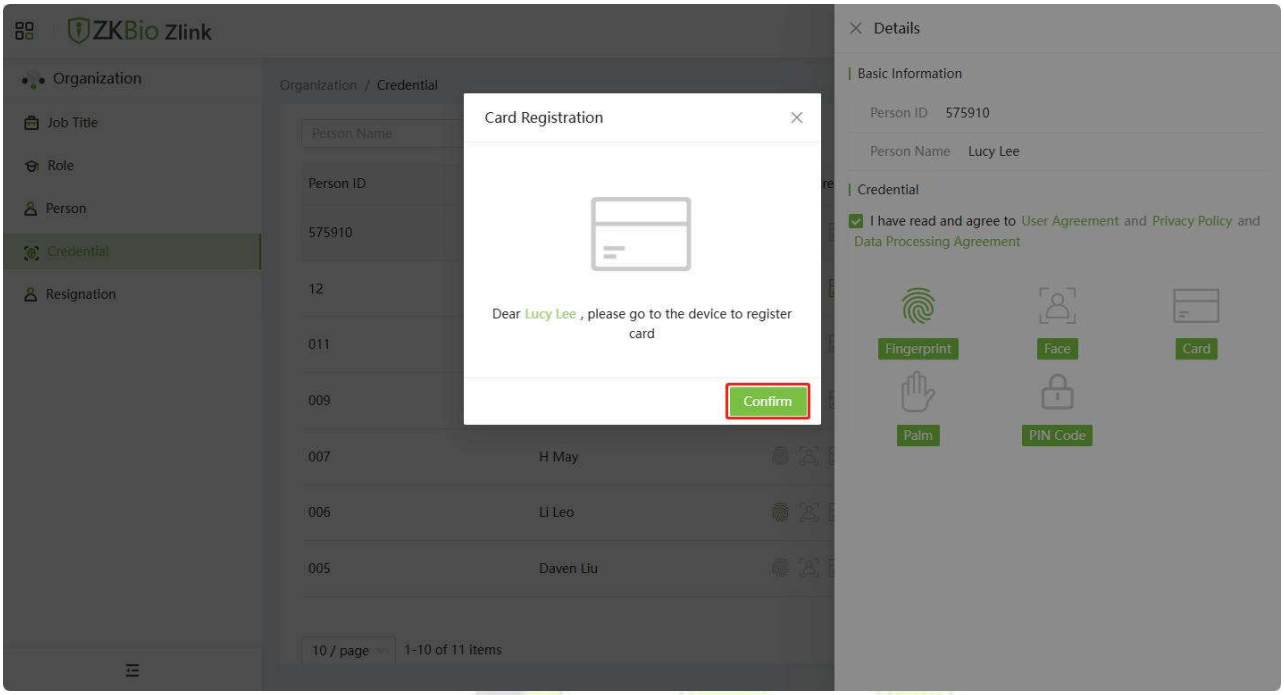
12.3.2 Register Card

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 [**Card Registration**].



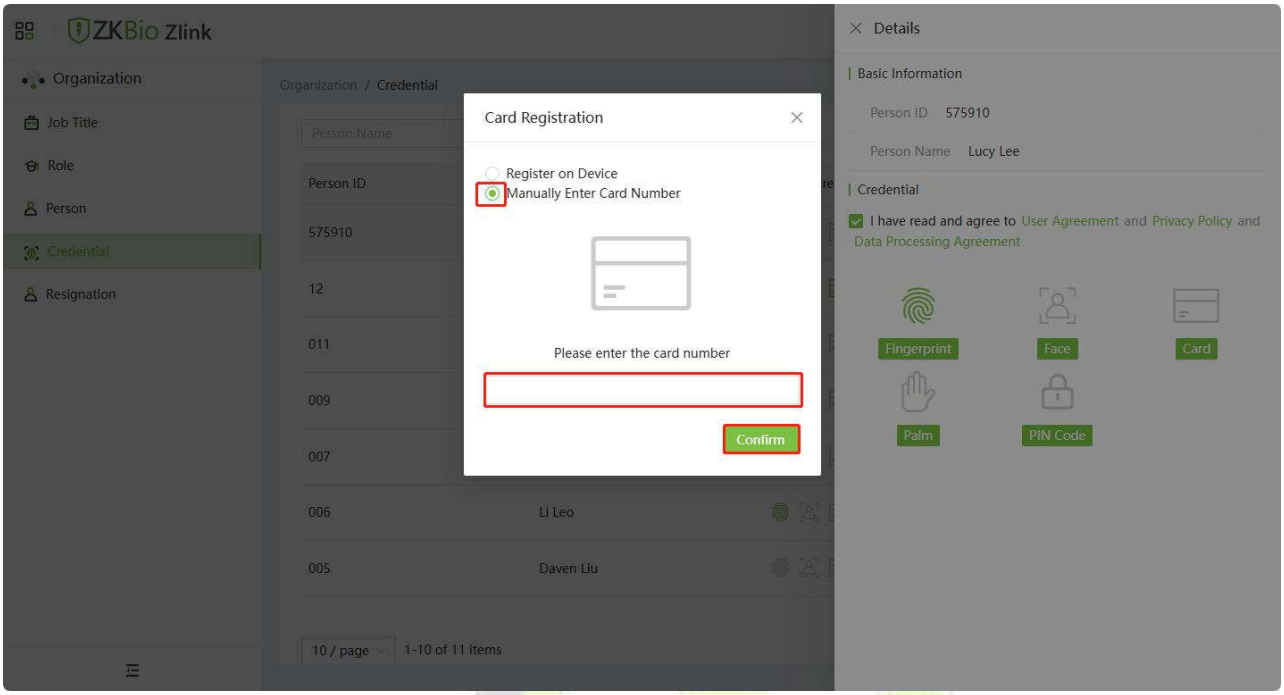
2. Select the registration device, the device will display the **Enroll Card Number** interface. Place the card in the swipe area, when the display shows green √, it means the card is successfully registered.





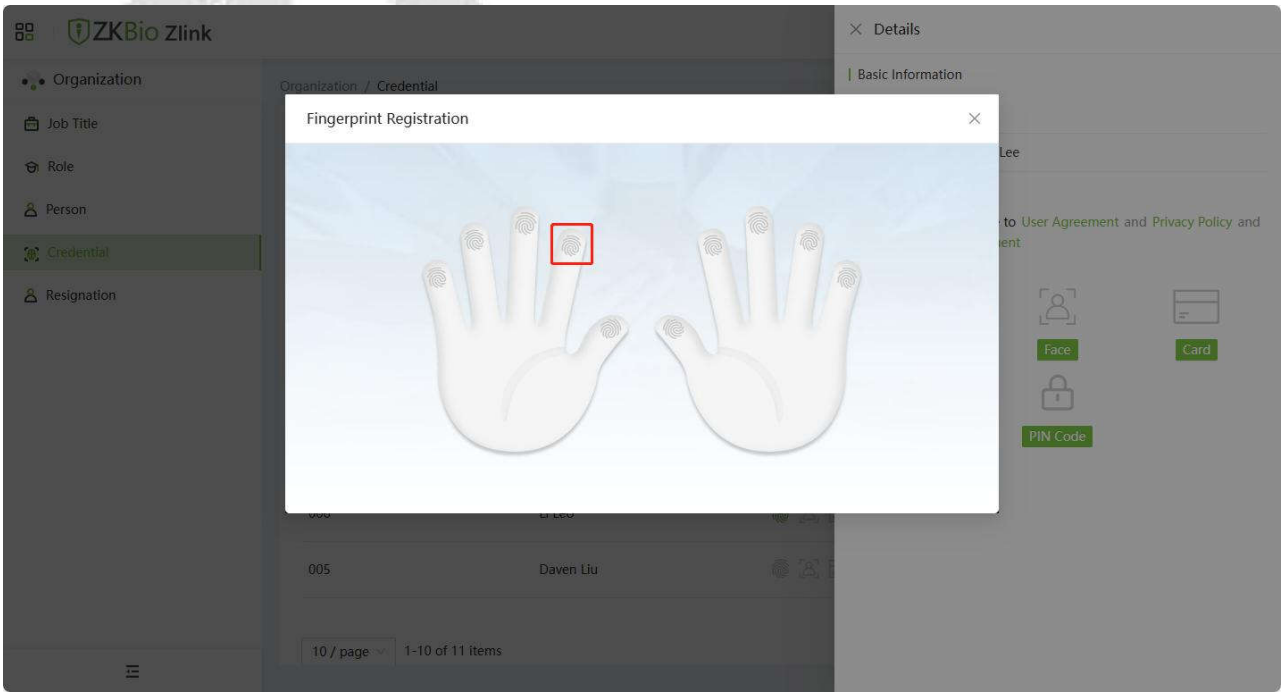
3. When the interface pops up the prompt, the device displays the **Punch Card** interface. Place the card in the swipe area, when the display shows "**Enrolled Sucess**", it means the card is successfully registered.

4. If you select **Manually Enter Card Number**, just enter your card number directly into the registration window that pops up and click [**Confirm**] to finish.

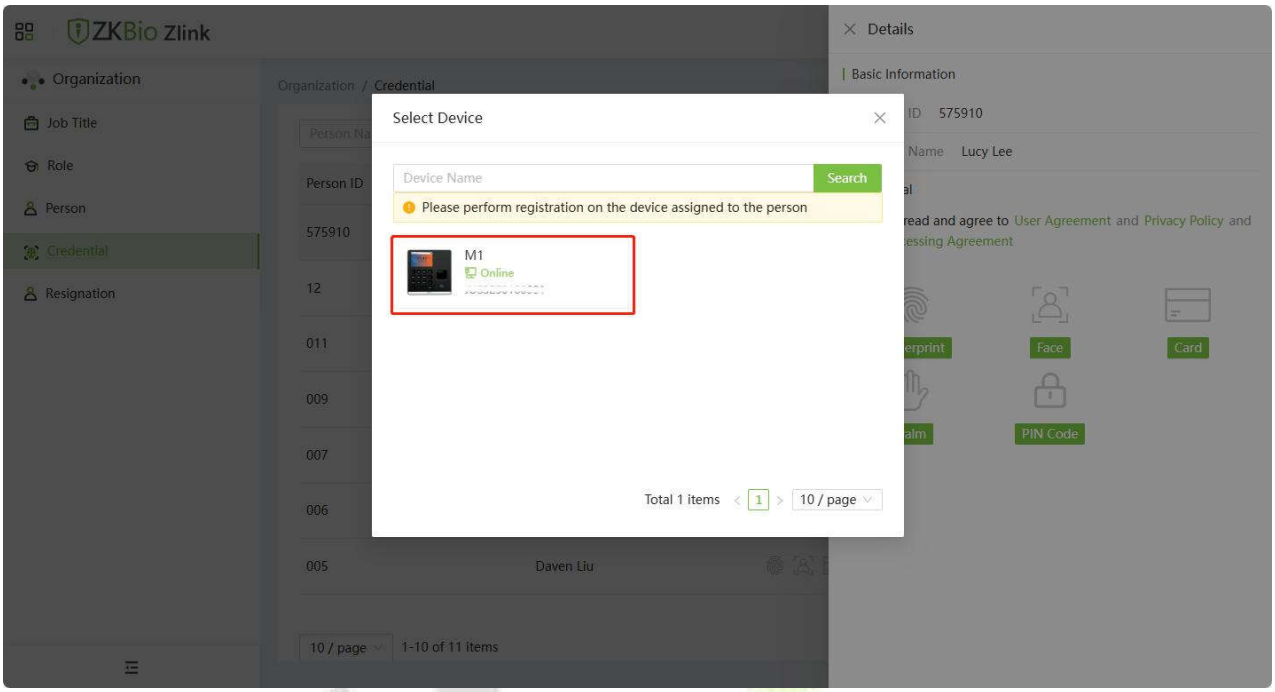


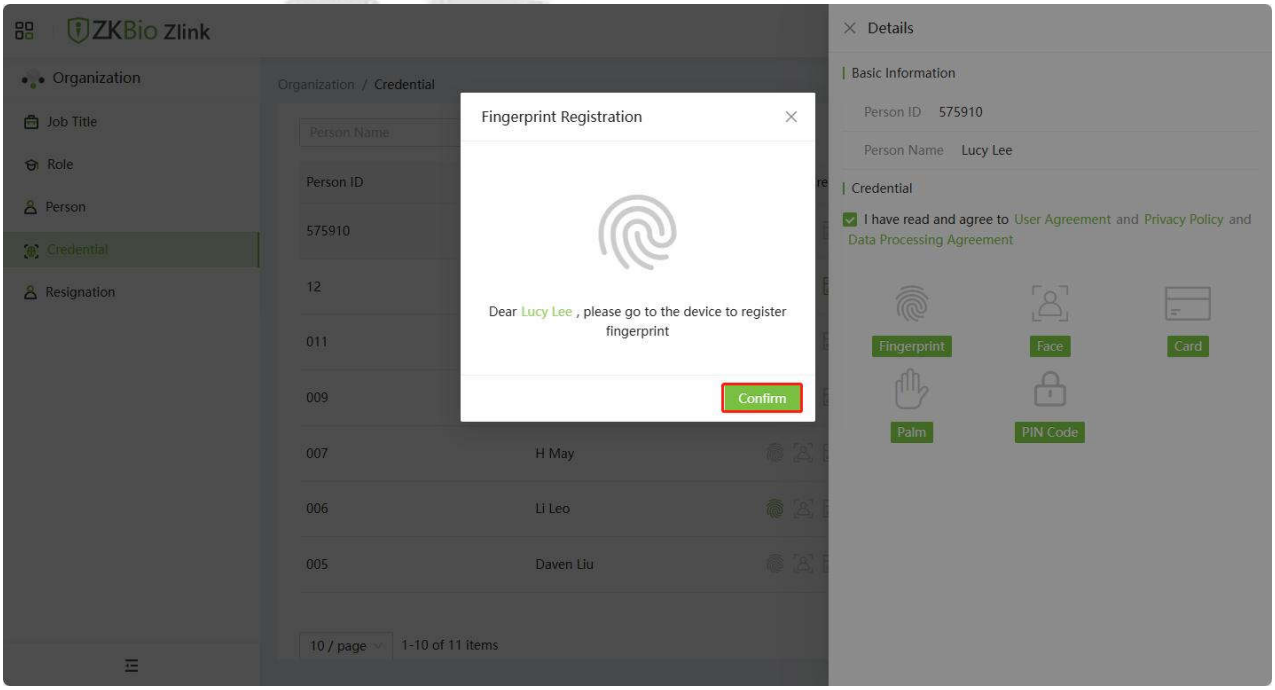
12.3.3 Register Fingerprint

1. Click [**Fingerprint**] in the Details page. Choose the hand and finger to be enrolled in the pop-up prompt window.

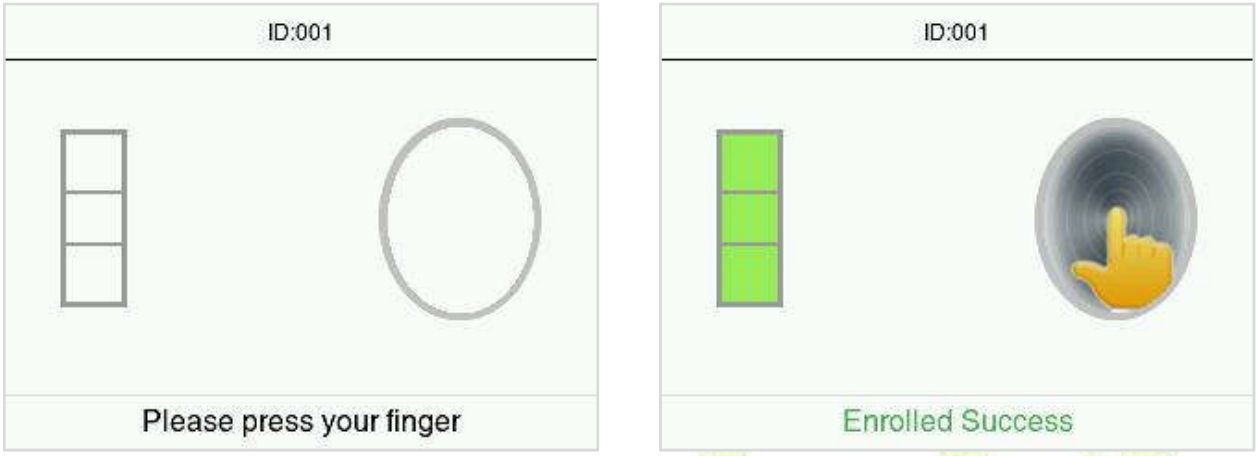


2. Select the registration device, the interface pops up a prompt window, while the device will display the fingerprint registration screen.

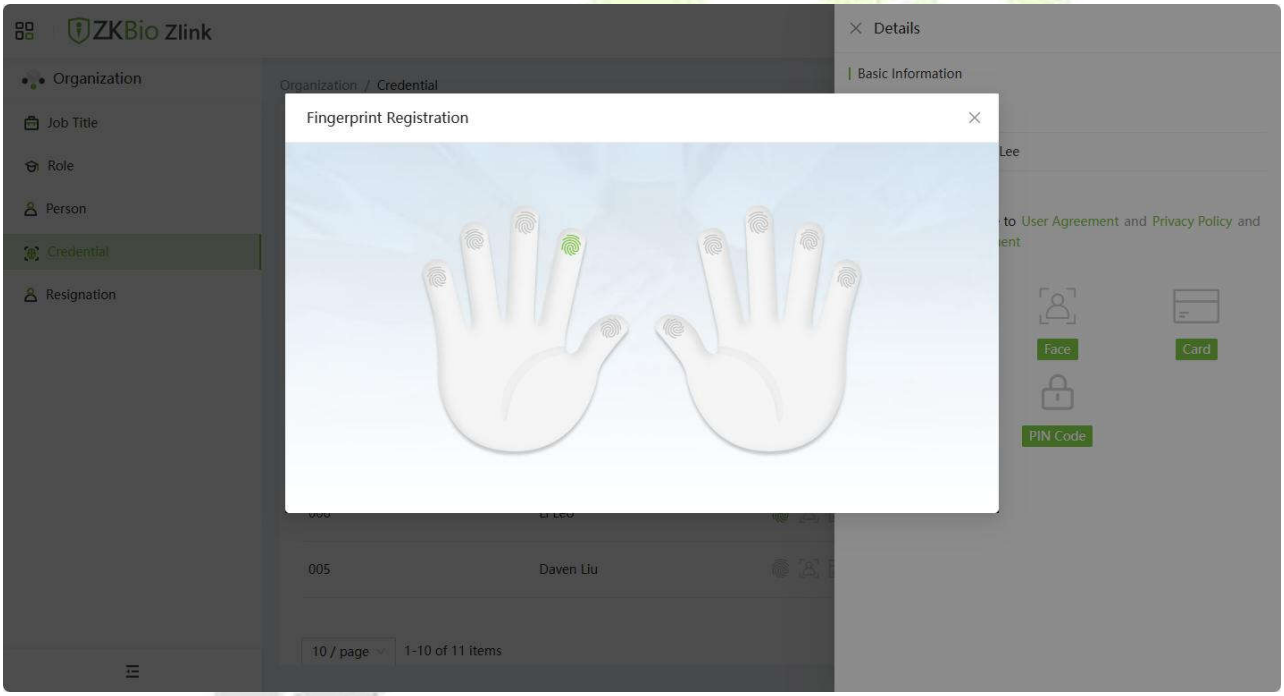




3. According to the prompts, place your finger on the fingerprint sensor and press **3** times. When the interface prompts "**Enrolled Success**", it means the fingerprint registration is successful.



4. Successfully recorded fingerprints will be displayed in green.



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/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/en/index/Index/privacyprotection.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