

User Manual

SenseFace T3

Date: June 2026

Doc Version: 1.0

English

Thank you for choosing our product. Please read the instructions carefully before operation. Follow these instructions to ensure that the product is functioning properly. The images shown in this manual are for illustrative purposes only.



For further details, please visit our Company's website
www.zkteco.com.

Copyright © 2026 ZKTECO CO., LTD. All rights reserved.

Without the prior written consent of ZKTeco, no portion of this manual can be copied or forwarded in any way or form. All parts of this manual belong to ZKTeco and its subsidiaries (hereinafter the "Company" or "ZKTeco").

Trademark

ZKTeco is a registered trademark of ZKTeco. Other trademarks involved in this manual are owned by their respective owners.

Disclaimer

This manual contains information on the operation and maintenance of the ZKTeco equipment. The copyright in all the documents, drawings, etc. in relation to the ZKTeco supplied equipment vests in and is the property of ZKTeco. The contents hereof should not be used or shared by the receiver with any third party without express written permission of ZKTeco.

The contents of this manual must be read as a whole before starting the operation and maintenance of the supplied equipment. If any of the content(s) of the manual seems unclear or incomplete, please contact ZKTeco before starting the operation and maintenance of the said equipment.

It is an essential pre-requisite for the satisfactory operation and maintenance that the operating and maintenance personnel are fully familiar with the design and that the said personnel have received thorough training in operating and maintaining the machine/unit/equipment. It is further essential for the safe operation of the machine/unit/equipment that personnel has read, understood and followed the safety instructions contained in the manual.

In case of any conflict between terms and conditions of this manual and the contract specifications, drawings, instruction sheets or any other contract-related documents, the contract conditions/documents shall prevail. The contract specific conditions/documents shall apply in priority.

ZKTeco offers no warranty, guarantee or representation regarding the completeness of any information contained in this manual or any of the amendments made thereto. ZKTeco does not extend the warranty of any kind, including, without limitation, any warranty of design, merchantability or fitness for a particular purpose.

ZKTeco does not assume responsibility for any errors or omissions in the information or documents which are referenced by or linked to this manual. The entire risk as to the results and performance obtained from using the information is assumed by the user.

ZKTeco in no event shall be liable to the user or any third party for any incidental, consequential, indirect, special, or exemplary damages, including, without limitation, loss of business, loss of profits, business interruption, loss of business information or any pecuniary loss, arising out of, in connection with, or relating to the use of the information contained in or referenced by this manual, even if ZKTeco has been advised of the possibility of such damages.

This manual and the information contained therein may include technical, other inaccuracies or typographical errors. ZKTeco periodically changes the information herein which will be incorporated into new additions/amendments to the manual. ZKTeco reserves the right to add, delete, amend or modify the information contained in the manual from time to time in the form of circulars, letters, notes, etc. for better operation and safety of the machine/unit/equipment. The said additions or amendments are meant for improvement /better operations of the machine/unit/equipment and such amendments shall not give any right to claim any compensation or damages under any circumstances.

ZKTeco shall in no way be responsible (i) in case the machine/unit/equipment malfunctions due to any non-compliance of the instructions contained in this manual (ii) in case of operation of the machine/unit/equipment beyond the rate limits (iii) in case of operation of the machine and equipment in conditions different from the prescribed conditions of the manual.

The product will be updated from time to time without prior notice. The latest operation procedures and relevant documents are available on <http://www.zkteco.com>.

If there is any issue related to the product, please contact us.

ZKTeco Headquarters

Address ZKTeco Industrial Park, No. 32, Industrial Road,
Tangxia Town, Dongguan, China.

Phone +86 769 - 82109991

Fax +86 755 - 89602394

For business related queries, please write to us at: sales@zkteco.com.

To know more about our global branches, visit www.zkteco.com.

About the Company

ZKTeco is one of the world's largest manufacturer of RFID and Biometric (Fingerprint, Facial, Finger-vein) readers. Product offerings include Access Control readers and panels, Near & Far-range Facial Recognition Cameras, Elevator/floor access controllers, Turnstiles, License Plate Recognition (LPR) gate controllers and Consumer products including battery-operated fingerprint and face template-reader Door Locks. Our security solutions are multi-lingual and localized in over 18 different languages. At the ZKTeco state-of-the-art 700,000 square foot ISO9001-certified manufacturing facility, we control manufacturing, product design, component assembly, and logistics/shipping, all under one roof.

The founders of ZKTeco have been determined for independent research and development of biometric verification procedures and the productization of biometric verification SDK, which was initially widely applied in PC security and identity authentication fields. With the continuous enhancement of the development and plenty of market applications, the team has gradually constructed an identity authentication ecosystem and smart security ecosystem, which are based on biometric verification techniques. With years of experience in the industrialization of biometric verifications, ZKTeco was officially established in 2007 and now has been one of the globally leading enterprises in the biometric verification industry owning various patents and being selected as the National High-tech Enterprise for 6 consecutive years. Its products are protected by intellectual property rights.

About the Manual

This manual introduces the operations of **SenseFace T3**.

All figures displayed are for illustration purposes only. Figures in this manual may not be exactly consistent with the actual products.

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

Document Conventions

Conventions used in this manual are listed below:

GUI Conventions

For Software	
Convention	Description
Bold font	Used to identify software interface template names e.g. OK , Confirm , Cancel .
>	Multi-level menus are separated by these brackets. For example, File > Create > Folder.
For Device	
Convention	Description
< >	Button or key names for devices. For example, press <OK>.
[]	Window names, menu items, data table, and field names are inside square brackets. For example, pop up the [New User] window.
/	Multi-level menus are separated by forwarding slashes. For example, File/Create/Folder.

Symbols

Convention	Description
	This represents a note that needs to pay more attention to.
	The general information which helps in performing the operations faster.
	The information which is significant.
	Care taken to avoid danger or mistakes.
	The statement or event that warns of something or that serves as a cautionary example.

TABLE OF CONTENTS

DATA SECURITY STATEMENT	7
SAFETY MEASURES	7
1 INSTRUCTION FOR USE	9
1.1 Finger Positioning	9
1.2 Standing Position, Posture and Facial Expression	9
1.3 Face Template Registration	10
1.4 Palm Registration	11
1.5 Standby Interface	12
1.6 Text Input (T9 Mode)	14
1.7 Verification Mode	15
1.7.1 Fingerprint Verification	15
1.7.2 Card Verification★	17
1.7.3 Palm Verification	18
1.7.4 Facial Verification	20
1.7.5 Password Verification.....	21
2 MAIN MENU	23
3 USER MANAGEMENT	25
3.1 Search for Users.....	25
4 COMMUNICATION SETTINGS.....	26
4.1 Wired Network.....	26
4.2 Wi-Fi Settings	27
4.3 Cloud Server Settings.....	28
5 SYSTEM SETTINGS.....	29
5.1 Set Time.....	29
5.2 Attendance	30
5.3 Face Parameters.....	31
5.4 Palm Parameters	32
5.5 Fingerprint Parameters	34
5.6 Voice	35
5.7 Camera.....	35
5.8 User Interface	36
5.9 Security Settings	37
5.10 Advanced Settings.....	37
6 USB DISK MANAGEMENT	39
6.1 Download to USB Drive.....	39
6.2 Upload from USB Drive	40
7 ATTENDANCE SEARCH	41

8	AUTOTEST	42
9	SYSTEM INFORMATION.....	43
10	CONNECTING TO ZKBIO ZLINK APP.....	44
10.1	Login to the App	44
10.2	Add Device on the App	45
10.3	Manage and Add Person to Device	46
10.4	Register Verification Mode on the App.....	47
11	CONNECTING TO ZKBIO ZLINK WEB	51
11.1	Login to the Web	51
11.2	Add Device on the Web	51
11.3	Manage and Add Person to Device	53
11.4	Register Verification Mode on the Web.....	54
APPENDIX 1		62
	Requirements of Live Collection and Registration of Visible Light Face Templates	62
	Requirements for Visible Light Digital Face Template Data	63
APPENDIX 2		64
	Privacy Policy.....	64
	Eco-friendly Operation	66

Data Security Statement

ZKTeco, as a smart product supplier, may also need to know and collect some of your personal information to better assist you in using ZKTeco's goods and services, and will treat your privacy carefully by developing a Privacy Policy.

Please read and understand completely all the privacy protection policy regulations and key points that appear on the device before using ZKTeco products.

As a product user, you must comply with applicable laws and regulations related to personal data protection when collecting, storing, and using personal data, including but not limited to taking protective measures for personal data, such as performing reasonable rights management for devices, strengthening the physical security of device application scenarios, and so on.

Safety Measures

The following precautions are to keep the user's safety and prevent any damage. Please read carefully before installation.

1. **Read, follow, and retain instructions** - All safety and operational instructions must be properly read and followed before bringing the device into service.
2. **Do not ignore warnings** - Adhere to all warnings on the unit and in the operating instructions.
3. **Accessories** - Use only manufacturer-recommended or product-sold accessories. Please do not use any other components other than manufacturer suggested materials.
4. **Precautions for the installation** - Do not place this device on an unstable stand or frame. It may fall and cause serious injury to persons and damage to the device.
5. **Service** - Do not try to service this unit yourself. Opening or removing covers may expose you to hazardous voltages or other hazards.
6. **Damage requiring service** - Disconnect the system from the main AC or DC power source and refer service personnel under the following conditions:
 - When cord or connection control is affected.
 - When the liquid was spilled, or an item dropped into the system.
 - If the system is exposed to water and/or inclement weather conditions (rain, snow, and more).
 - If the system is not operating normally under operating instructions.

Just change controls defined in operating instructions. Improper adjustment of other controls may result in damage and involve a qualified technician to return the device to normal operation.

7. **Replacement parts** - When replacement parts are required, service technicians must only use replacement parts provided by the supplier. Unauthorized substitutes can lead to the risk of burns, electric shock, or other hazards.
8. **Safety check** - On completion of service or repair work on the unit, ask the service technician to

perform safety checks to ensure proper operation of the unit.

9. **Power sources** - Operate the system only from the label's power source form. If the sort of power supply to use is unclear, call your dealer.
10. **Lightning** – Can install external lightning conductors to protect against electrical storms. It stops power-ups destroying the system.

The devices should be installed in areas with limited access.

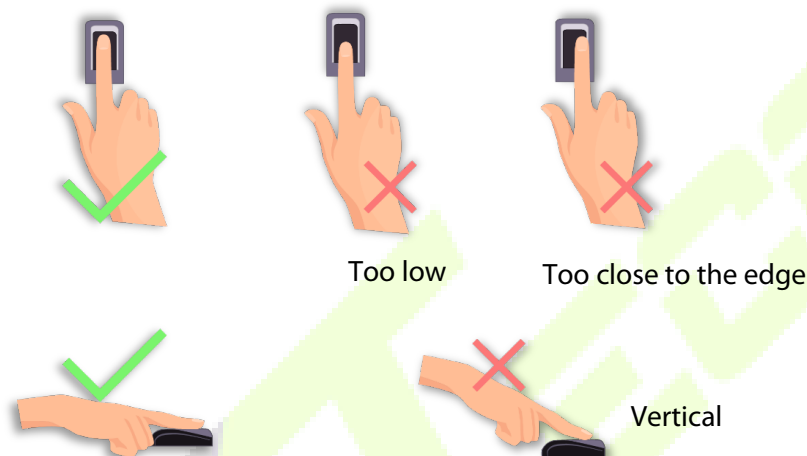


1 Instruction for Use

Before getting into the Device features and functions, it is recommended to be familiar with the below fundamentals.

1.1 Finger Positioning

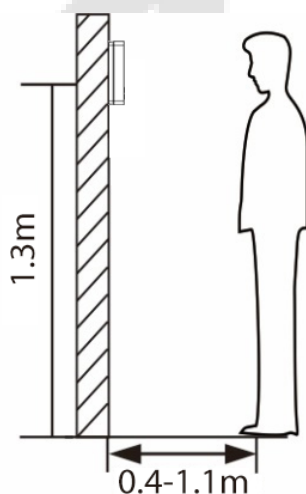
Recommended fingers: The index, middle, or ring fingers are recommended fingers to use, and avoid using the thumb or pinky, as they are difficult to position correctly onto the fingerprint reader.



Note: Please use the correct method when pressing your fingers onto the fingerprint reader for registration and identification. Our company will assume no liability for recognition issues that may result from incorrect usage of the product. We reserve the right of final interpretation and modification concerning this point.

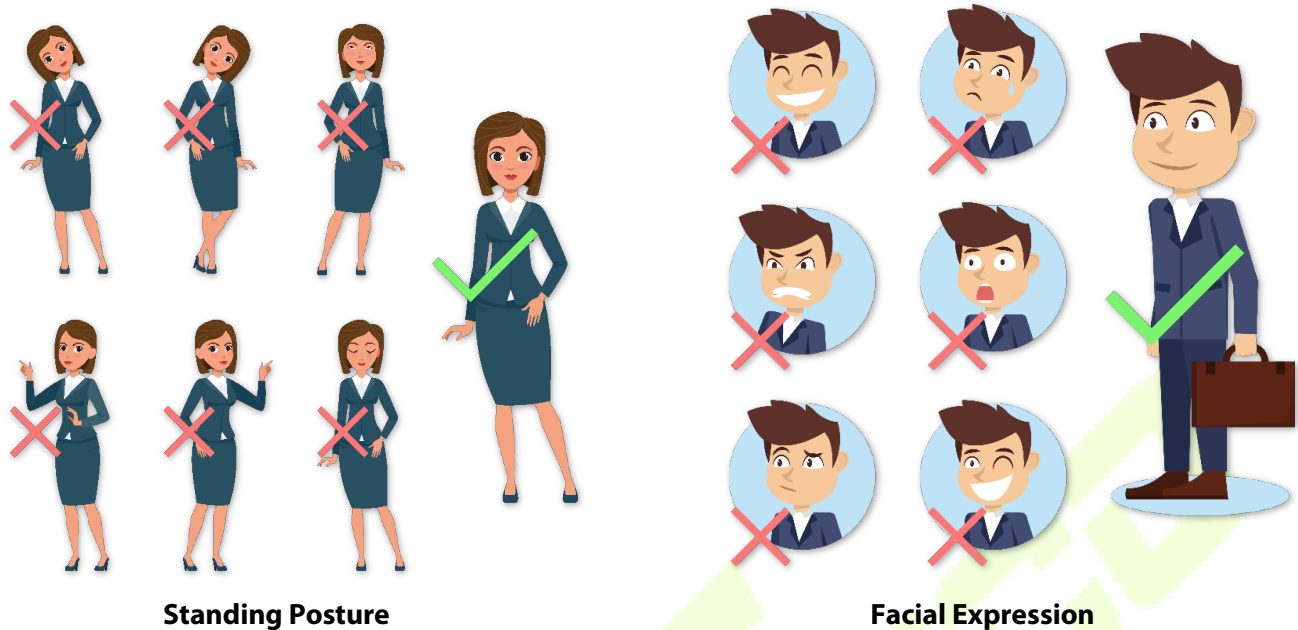
1.2 Standing Position, Posture and Facial Expression

➤ The recommended distance



The distance between the device and a user whose height is in a range of 1.55 m to 1.85 m is recommended to be 0.4 m to 1.1m. Users may slightly move forward or backward to improve the quality of facial images captured.

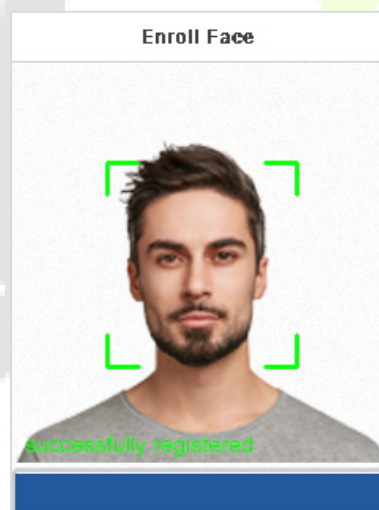
➤ **Recommended Standing Posture and Facial Expression:**



Note: During enrollment and verification, please remain natural facial expression and standing posture.

1.3 Face Template Registration

Please make sure that the face template is in the centre of the screen during registration. Please face towards the camera and stay still during face template registration. The screen should look like the image below:



Correct face Registration and Authentication Method

➤ **Recommendation for Registering a Face Template**

- When registering a face template, maintain a distance of 40 cm to 80 cm space between the device and the face template.
- Be careful not to change your facial expression. (Smiling face template, drawn face template, wink, etc.)

- If you do not follow the instructions on the screen, the face template registration may take longer or may fail.
- Be careful not to cover the eyes or eyebrows.
- Do not wear hats, masks, sunglasses, or eyeglasses.
- Ensure only one person is visible in the camera's frame during face template registration.
- It is recommended for a user wearing glasses to register both face templates with and without glasses.

➤ **Recommendation for Authenticating a Face Template**

- Ensure that the face template appears inside the guideline displayed on the screen of the device.
- If the glasses have been changed, authentication may fail. If the face template without glasses has been registered, authenticate the face template without glasses further. If the face template with glasses has been registered, authenticate the face template with the previously worn glasses.
- If a part of the face template is covered with a hat, a mask, an eye patch, or sunglasses, authentication may fail. Do not cover the face template, allow the device to recognize both the eyebrows and the face template.

1.4 Palm Registration

Place your palm in the palm multi-mode collection area, such that the palm is placed parallel to the device.

Make sure to keep space between your fingers.

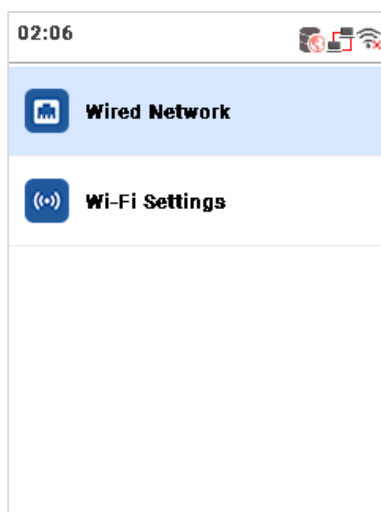


Note:

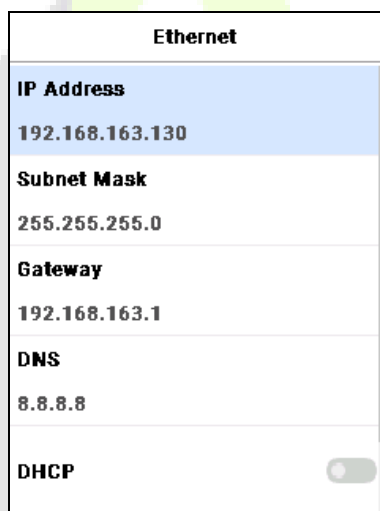
- 1) Place your palm within 8 to 25 cm of the device.
- 2) Place your palm in the palm collection area, such that the palm is placed parallel to the device.
- 3) Make sure to keep space between your fingers.

1.5 Standby Interface

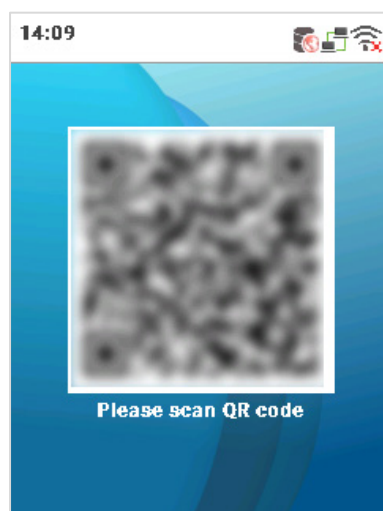
The device uses a 2.4-inch color screen, which all operations are performed through the keypad. After connecting the power supply for the first time, press **M/OK** to configure the network.



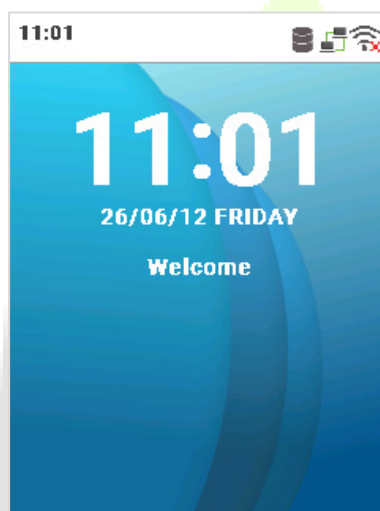
Select **Wired Network** or **Wi-Fi Settings**. Here take Wired Network as an example. Connect an Ethernet cable to the device and set the relevant parameters of network.



If the network connection is successful, the device will prompt "The network setting is successful, please use the App to add a device" and a QR code scanning interface will pop up. Then bind the device through the ZKBio Zlink App or ZKBio Zlink Web.



Once the device is connected to ZKBio Zlink, the QR code will disappear, the following standby interface is displayed:

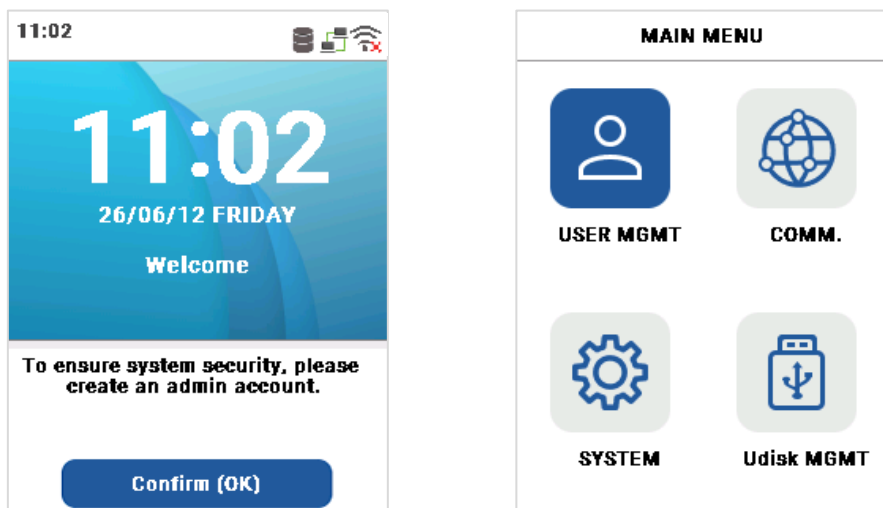


- Enter any number to access the User ID input interface.

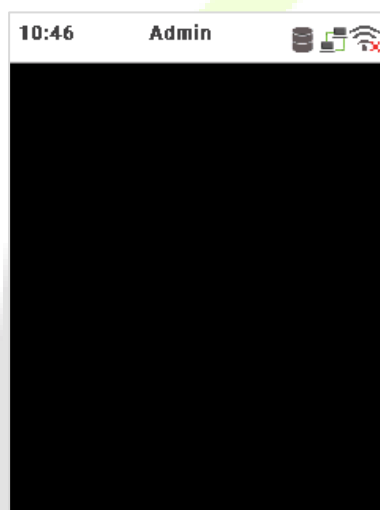
User ID
Please input
118
Please input user ID.
Up/down key switch input method, to the left key to delete the key
[123]

User ID:118
☒ Password
☐ Face
☐ Palm
☐ Fingerprint
☐ Card Number

- When there is no Administrator set in the device, press **M/OK** to go to the menu.



- After adding an Administrator on the device, it requires the Administrator's verification before opening the menu functions.

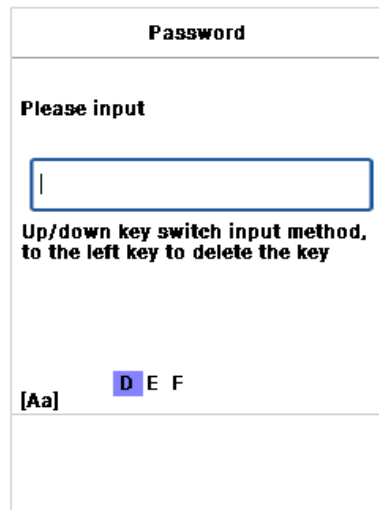


Note: For the security of the device, it is recommended to register administrator the first time you use the device.

1.6 Text Input (T9 Mode)

T9 mode allows you to enter the Uppercase, Lowercase, Number and Special characters in the text input fields. You can enter the alphabets and special characters by pressing one keystroke per letter. Press the Up/Down key in the text box to activate T9 mode.

- Navigate to the required text field and press **<M/OK>**.



- Each key on the keypad has a few letters printed above them. For example, pressing 3 can enter D, E, and F. To enter "F", press 3 thrice. This is accomplished by comparing the number of keystrokes with the internal syntactical dictionary to determine the letter.
- Press Up/Down key to switch between Uppercase, Lowercase, Number and Special characters.
- To add the special character, press the corresponding key once. For example, to enter ";" press 2 once.
- After the input is complete, press the <M/OK> key to save.

1.7 Verification Mode

1.7.1 Fingerprint Verification

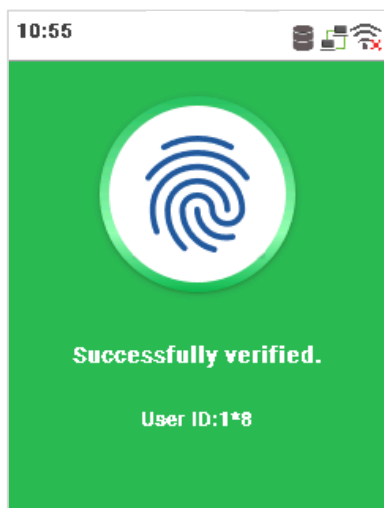
➤ 1: N Fingerprint Verification Mode

The device compares the current fingerprint with the available fingerprint data stored in its database.

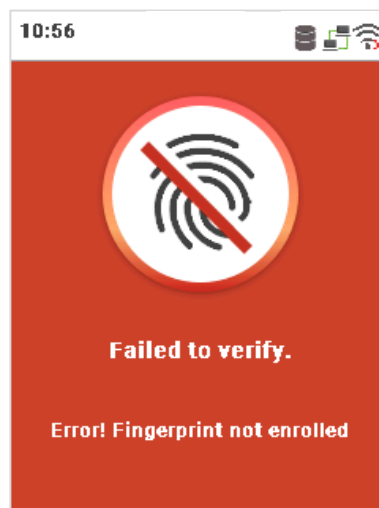
Fingerprint authentication mode is activated when a user places their finger onto the fingerprint scanner.

Please follow the recommended way to place your finger onto the sensor. For details, please refer to section [Finger Positioning](#).

Verification is successful:



Verification is failed:

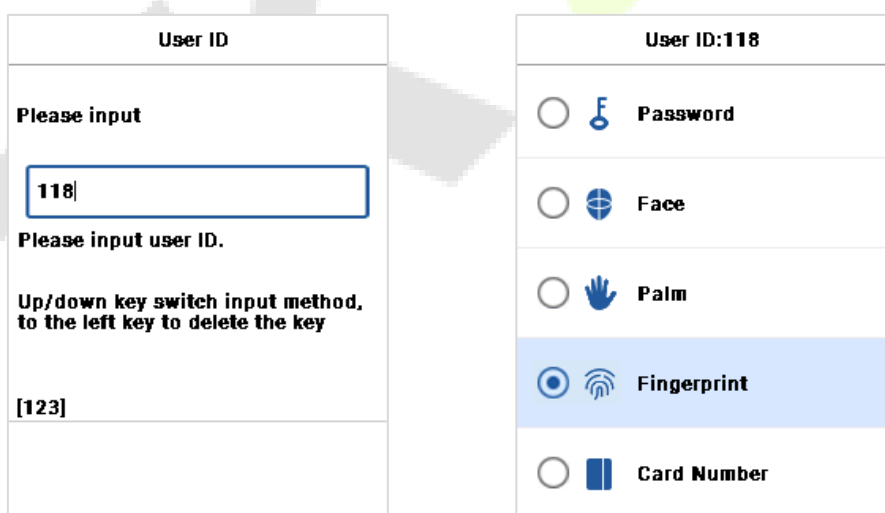


➤ 1: 1 Fingerprint Verification Mode

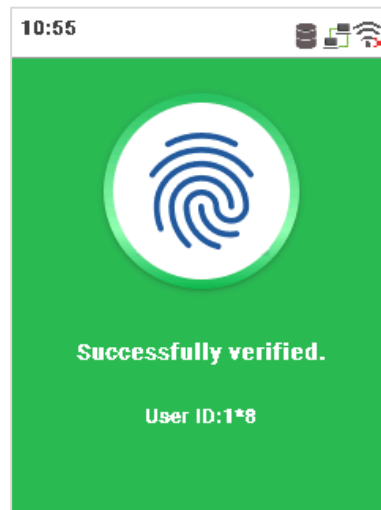
The device compares the current fingerprint with the fingerprints linked to the entered User ID through the keyboard.

In case users are unable to gain access using the 1:N authentication method, they can attempt to verify their identity using the 1:1 verification mode.

Enter the user ID and press **M/OK**. If the user has registered card, face, palm and password in addition to the fingerprint, the following screen will appear. Select **Fingerprint** to enter the 1:1 fingerprint verification mode.



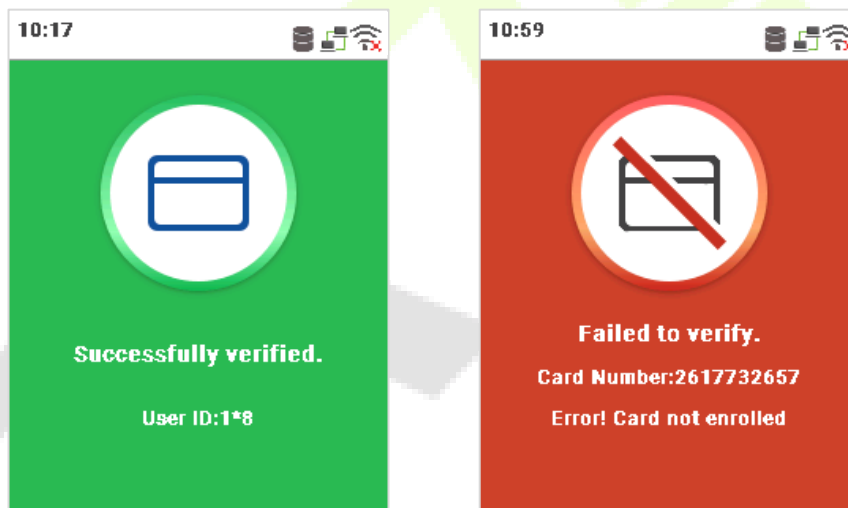
Press the fingerprint to verify. After successful verification, the prompt box displays "**Successfully verified**", as shown below:



1.7.2 Card Verification★

➤ 1:N card verification

The 1:N card verification mode compares the card number in the card induction area with all the card number data registered in the device; The following screen displays on the card verification:



➤ 1:1 Card Verification

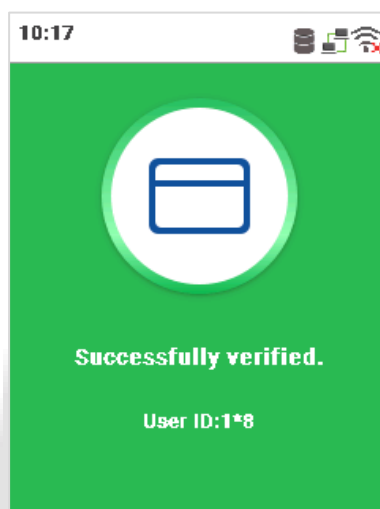
The 1:1 card verification mode compares the card number in the card induction area with the number associated with the employee's User ID registered in the device.

Enter the user ID and press **M/OK**. If the user has registered fingerprint, face, palm and password in addition to the card, the following screen will appear. Select **Card Number** to enter the 1:1 card verification mode.

User ID
Please input
118
Please input user ID.
Up/down key switch input method, to the left key to delete the key
[123]

User ID:118
☐ Password
☐ Face
☐ Palm
☐ Fingerprint
☒ Card Number

After successful verification, the prompt box displays "**Successfully verified**", as shown below:

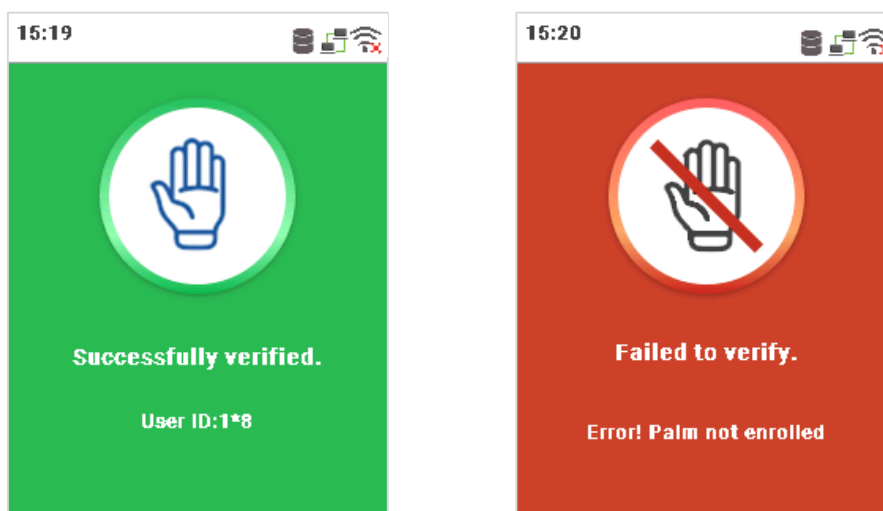


1.7.3 Palm Verification

➤ 1:N Palm Verification Mode

This verification mode compares the palm image collected by the palm module with all the palm data template in the device.

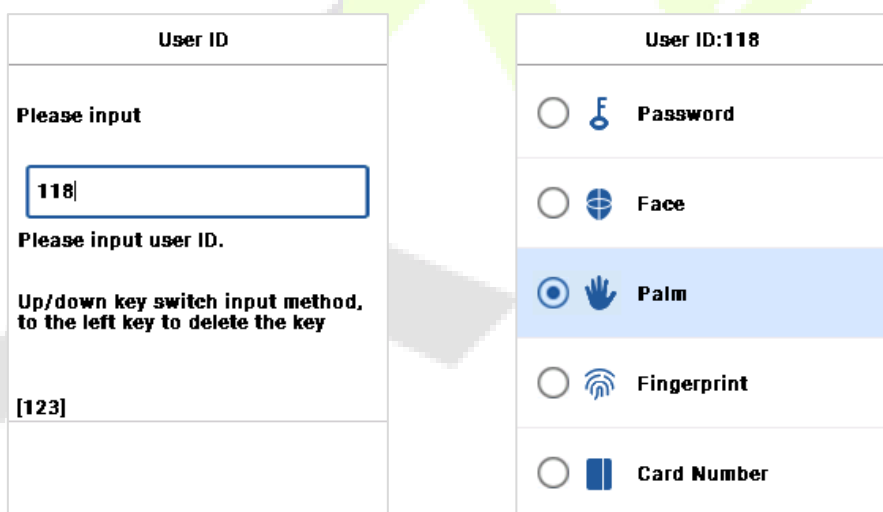
The device will automatically distinguish between the palm and face verification mode. Place the palm in the area that can be collected by the palm module, so that the device will automatically switch to palm verification mode.



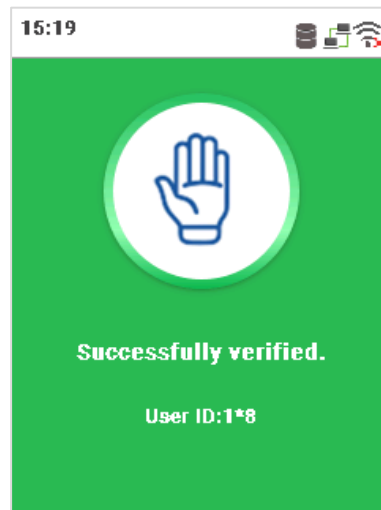
➤ 1:1 Palm Verification Mode

In this verification mode, the device compares the palm image collected by the palm module with the palm data template related to the entered user ID.

Enter the user ID and press **M/OK**. If the user has registered fingerprint, face, card and password in addition to the palm, the following screen will appear. Select **Palm** to enter the 1:1 palm verification mode.



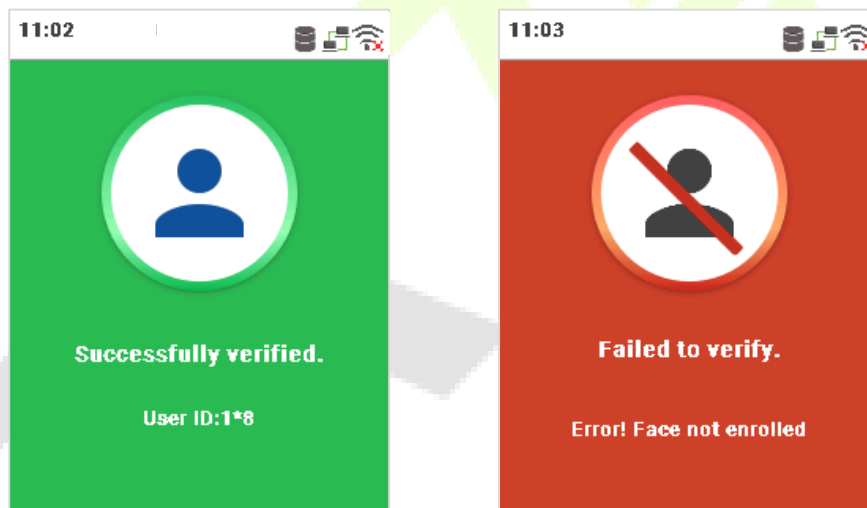
After successful verification, the prompt box displays "**Successfully verified**", as shown below:



1.7.4 Facial Verification

➤ 1:N Facial Verification

Device compares the currently acquired facial images with all the registered face template data stored in its database. The following is the pop-up prompt box displaying the result of the comparison.



➤ 1:1 Facial Verification

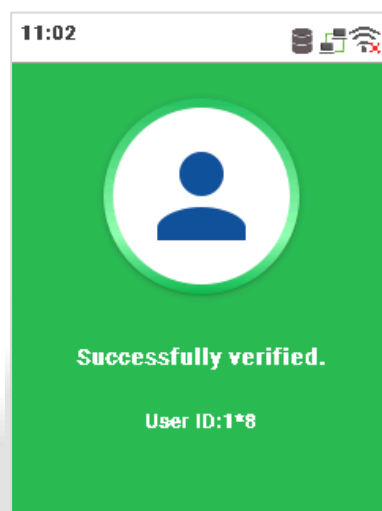
In this verification mode, the device compares the face captured by the camera with the facial template related to the entered user ID.

Enter the user ID and press **M/OK**. If the user has registered fingerprint, palm, card and password in addition to the face, the following screen will appear. Select **Face** to enter the 1:1 face verification mode.

User ID
Please input
118
Please input user ID.
Up/down key switch input method, to the left key to delete the key
[123]

User ID:118
☐ Password
☒ Face
☐ Palm
☐ Fingerprint
☐ Card Number

After successful verification, the prompt box displays "**Successfully verified**", as shown below:



1.7.5 Password Verification

The device compares the entered password with the registered password and User ID.

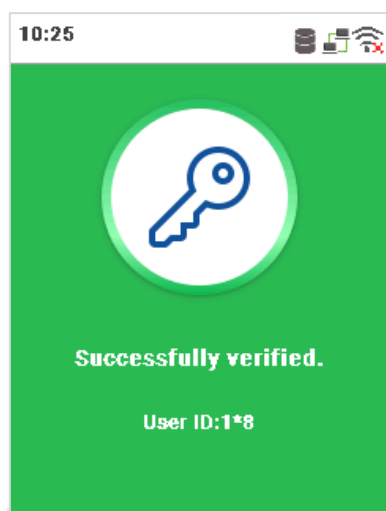
Enter the user ID and press **M/OK**. If the user has registered fingerprint, palm, card and face in addition to the password, the following screen will appear. Select **Password** to enter the password verification mode.

User ID
Please input
118
Please input user ID.
Up/down key switch input method, to the left key to delete the key
[123]

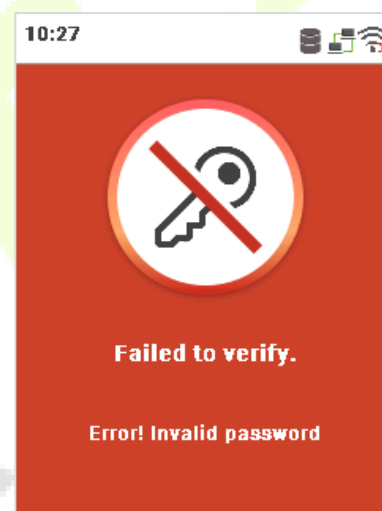
User ID:118
☒ Password
☐ Face
☐ Palm
☐ Fingerprint
☐ Card Number

The following screen displays, after inputting a correct password and a wrong password respectively.

Verification is successful:

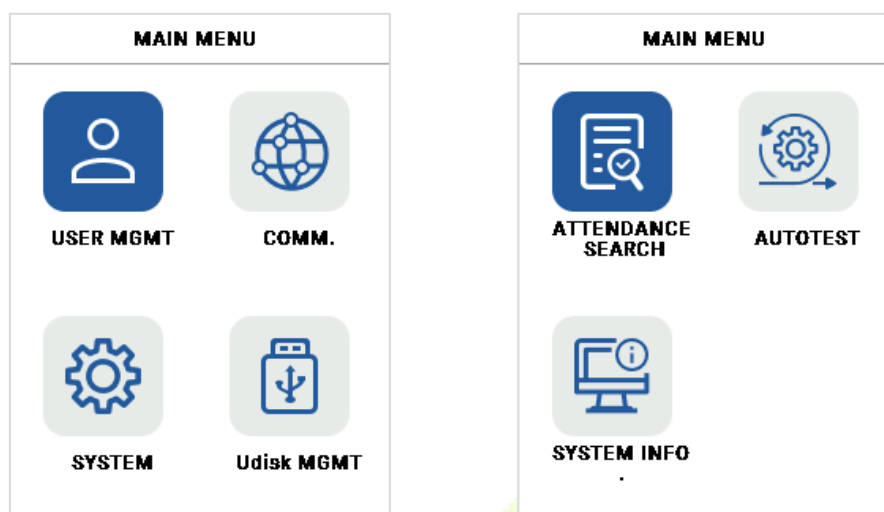


Verification is failed:



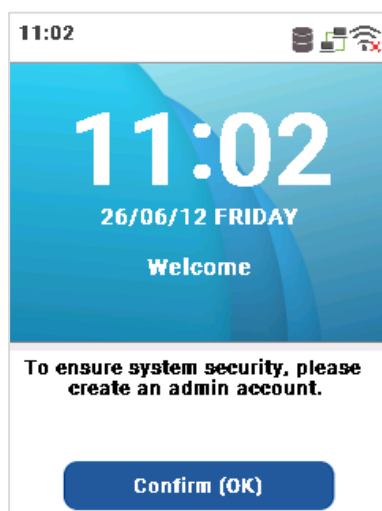
2 Main Menu

Press **M/OK** to enter the **MAIN MENU**, the following screen will be displayed:



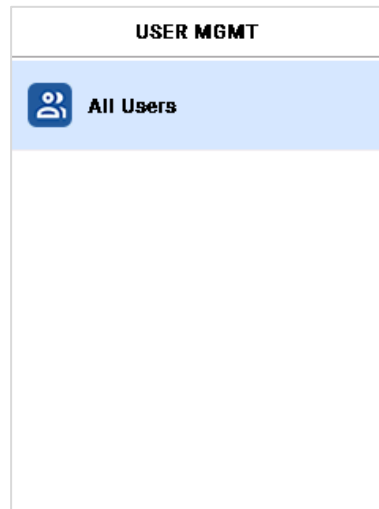
Menu	Descriptions
USER MGMT	To view the basic information of a User.
COMM.	To set the relevant parameters of wired network, Wi-Fi and cloud server.
SYSTEM	To set the parameters related to the system, including time, attendance, face, palm & fingerprint parameters, voice, camera, user interface, security and advanced settings.
Udisk MGMT	To upload or download the specific data by a USB drive.
ATTENDANCE SEARCH	To query the specified event logs.
AUTOTEST	To automatically test whether each module functions properly, including the display, camera, fingerprint sensor, card★, voice and real-time clock.
SYSTEM INFO.	To view data capacity, device and firmware information and privacy policy of the device.

Note: When users use the product for the first time, they should operate it after setting administrator privileges. Add the device administrator on **ZKBio Zlink**. If the product does not have an administrator setting, the system will show an administrator setting command prompt every time you enter the device menu.



3 User Management

When the device is on the initial interface, press **M/OK** and enter **USER MGMT.**



3.1 Search for Users

When the device is on the initial interface, press **M/OK** and enter **USER MGMT > All Users.**

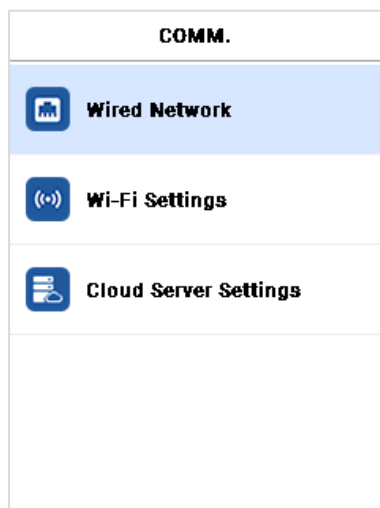
- On the **All Users** interface, enter the required user ID and the system will search for the related user information.



4 Communication Settings

Communication Settings are used to set the parameters of the Wired Network, Wi-Fi and Cloud Server.

When the device is on the initial interface, press **M/OK** and select **COMM.**



4.1 Wired Network

When the device needs to communicate with a PC over the Ethernet, you need to configure network settings and ensure that the device and the PC are connecting to the same network segment.

Select **Wired Network** on the COMM. Settings interface.



Menu	Description
IP Address	The factory default value is 192.168.1.201. Please set the IP Address as per the requirements.
Subnet Mask	The factory default value is 255.255.255.0. Please set the value as per the requirements.

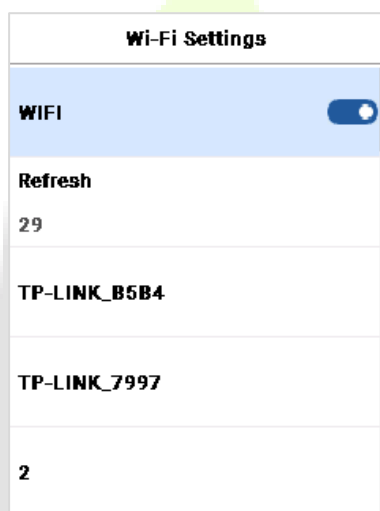
Gateway	The factory default address is 0.0.0.0. Please set the value as per the requirements.
DNS	The factory default address is 0.0.0.0. Please set the value as per the requirements.
DHCP	Dynamic Host Configuration Protocol, which is to dynamically allocate IP addresses for clients via server.
Display in Status Bar	To set whether to display the network icon on the status bar.

4.2 Wi-Fi Settings

The device provides a Wi-Fi module, which can be built-in within the device mould.

The Wi-Fi module enables data transmission via Wi-Fi (Wireless Fidelity) and establishes a wireless network environment. Wi-Fi is enabled by default in the device. If you don't need to use the Wi-Fi network, you can toggle the Wi-Fi to disable button.

Select **Wi-Fi Settings** on the **COMM.** Settings interface to configure the Wi-Fi settings.



➤ Search the Wi-Fi Network

- Wi-Fi is enabled in the Device by default. Toggle on  button to enable or disable Wi-Fi.
- Once the Wi-Fi is turned on, the device will search for the available Wi-Fi within the network range.
- Choose the appropriate Wi-Fi name from the available list, and input the correct password in the password interface, and then press **M/OK**.

Wi-Fi Settings
Password
SSID
TP-LINK_B5B4
Security
WPAPSK/WPA2PSK
Signal Strength
Very Strong

Select the required network from the searched network list.

Password
Please input
Up/down key switch input method, to the left key to delete the key
[a]

Enter the password, and then press on **M/OK**.

- When the Wi-Fi is connected successfully, the initial interface will display the Wi-Fi  logo.

4.3 Cloud Server Settings

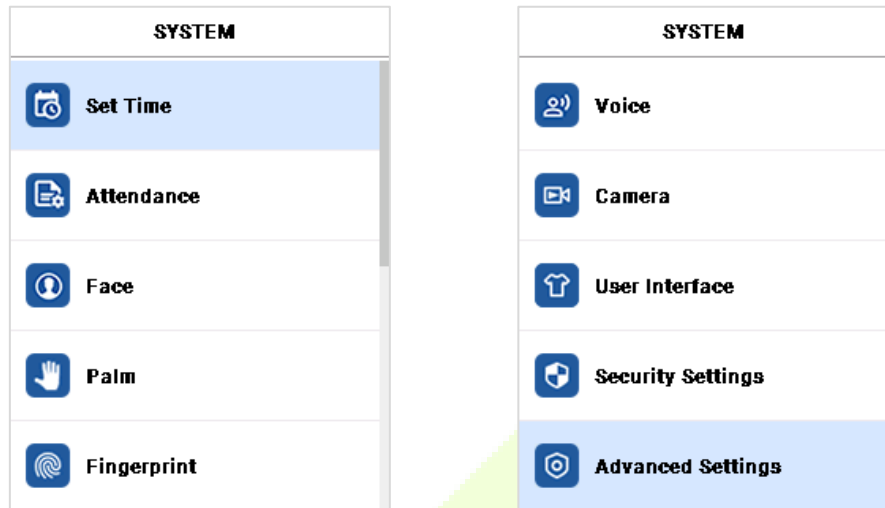
Select **Cloud Server Settings** on the **COMM.** Settings interface to view the server address.

Cloud Server Settings
Server Address
https://gdms.minervaiot.com

5 System Settings

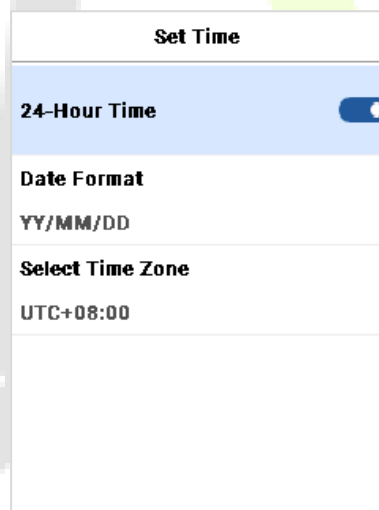
Set related system parameters to optimize the performance of the device.

When the device is on the initial interface, press **M/OK** and select **SYSTEM**.



5.1 Set Time

Select **Set Time** on the **SYSTEM** interface to set the time.



- Enable or disable the **24-Hour Time**.
- Select the **Date Format** to set the date format.

5.2 Attendance

Select **Attendance** on the SYSTEM interface.

Attendance	Attendance
Duplicated Punch Period(s)	Attendance Log Alert
3	2000
Attendance Log Alert	Periodic Del of T&A Data
2000	0
Periodic Del of T&A Data	Verification Failed Time(s)
0	15
Verification Failed Time(s)	Authentication Timeout(s)
15	2
Authentication Timeout(s)	Recognition Interval(s)
2	2

Function Name	Description
Duplicate Punch Period(s)	Within a set time period (unit: seconds), the duplicated attendance record will not be reserved (value ranges from 0 to 999999 seconds).
Attendance 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.
Periodic Del of T&A Data	When attendance records reach its maximum storage capacity, the device automatically deletes a set of old attendance records. Users may disable the function or set a valid value between 1 and 999.
Verification Failed Time(s)	It refers to the number of seconds of consecutive face/palm comparison failures after which a recognition failure prompt is triggered. Valid value: 10 to 3600 seconds.
Authentication Timeout(s)	The amount of time taken to display a successful verification message. Valid value: 1~9 seconds.
Recognition Interval(s)	After the interval identifying is clicked (selected), for example, if the comparison interval is set to 5 seconds, then the face recognition will verify the face every 5 seconds. Valid value: 0 to 9 seconds. 0 means continuous identifying, 1 to 9 means identifying at intervals.

5.3 Face Parameters

Select **Face** on the **SYSTEM** interface to go to the face template parameter settings.

Face	Recognition Settings	Liveness Settings
Recognition Settings	1:N Threshold 82	Binocular Live Detection ☒
Liveness Settings	1:1 Threshold 72	Binocular Live Detection Threshold 99
	Enrollment Threshold 82	
	Image Quality 30	
	Minimum Width Size 60	

Function Name	Description
Recognition Settings	1: N Threshold: The verification will be successful only if the similarity between the acquired facial image and all registered facial templates is greater than the set value in the 1: N verification mode. The valid value ranges from 0 to 100. The higher the thresholds, the lower the misjudgement rate and higher is the rejection rate, and vice versa. It is recommended to set the default value of 82.
	1:1 Threshold: Under 1:1 verification mode, the verification will only be successful when the similarity between the acquired facial image and the user's facial templates enrolled in the device is greater than the set value. The valid value ranges from 0 to 100. The higher the thresholds, the lower the misjudgement rate and the higher is the rejection rate, and vice versa. It is recommended to set the default value of 72.
	Enrollment Threshold: During face template enrollment, 1:N comparison is used to determine whether the user has already registered before. When the similarity between the acquired facial image and all registered facial templates is greater than this threshold, it indicates that the face template has already been registered.
	Image Quality: Image quality for facial registration and comparison. The higher the value, the clearer the image requires.

	Minimum Width Size: It sets the minimum face size required for facial registration and comparison. If the minimum size of the captured image is smaller than the set value, then it will be filtered off and not recognized as a face. This value can also be interpreted as the face comparison distance. The farther the individual is, the smaller the face, and the smaller number of pixels of the face obtained by the algorithm. Therefore, adjusting this parameter can adjust the farthest comparison of distance of faces. When the value is 0, the face comparison distance is not limited.
Liveness Settings	Binocular Live Detection: It uses near-infrared spectra imaging to identify and prevent fake photos and video attacks. Binocular Live Detection Threshold: It is convenient to judge whether the near-infrared spectral imaging is a fake photo and video. The larger the value, the better the anti-spoofing performance of near-infrared spectral imaging.

Note: Improper adjustment of the exposure and quality parameters may severely affect the performance of the device. Please adjust the exposure parameter only under the guidance of the after-sales service personnel of our company.

5.4 Palm Parameters

Select **Palm** on the SYSTEM interface.

Palm	Recognition Settings	Recognition Settings
Recognition Settings	1:N Threshold 52	Enrollment Threshold 52
Liveness Settings	1:1 Threshold 40	Image Quality 40
	Enrollment Threshold 52	NIR Image Quality 30
	Image Quality 40	Minimum Width Size 120
	NIR Image Quality 30	Maximum Width Size 400

Liveness Settings	
Binocular Live Detection	☒
Binocular Live Detection Threshold	82

Function Name	Description
Recognition Settings	1: N Threshold: Under 1:N Verification Method, only when the similarity between the verifying palm and all registered palm is greater than this value, the verification succeeds.
	1:1 Threshold: Under 1:1 Verification Method, only when the similarity between the verifying palm and the user's registered palm is greater than this value, the verification succeeds.
	Enrollment Threshold: During palm template enrollment, 1:N comparison is used to determine whether the user has already registered before. When the similarity between the acquired palm image and all registered palm templates is greater than this threshold, it indicates that the palm template has already been registered.
	Image Quality: Image quality for palm registration and comparison. The higher the value, the clearer the image requires.
	NIR Image Quality: NIR Image quality for palm registration and comparison. The higher the value, the clearer the NIR image requires.
	Minimum/Maximum Width Size: The minimum/maximum palm size is used to limit the palm size recognized by the device, thereby eliminating background interference or misjudgment. This parameter is usually related to the distance from the camera to the palm. This value can be understood as the palm comparison distance. The farther the person is, the smaller the palm is, and the smaller the palm pixel will be obtained by the algorithm. Therefore, adjusting this parameter can adjust the furthest comparison distance of palms. When the value is 0, the palm comparison distance is not limited.

Liveness Settings	Binocular Live Detection: It uses near-infrared spectra imaging to identify and prevent fake photos and video attacks. Binocular Live Detection Threshold: It is convenient to judge whether the near-infrared spectral imaging is a fake photo and video. The larger the value, the better the anti-spoofing performance of near-infrared spectral imaging.
--------------------------	--

5.5 Fingerprint Parameters

Select **Fingerprint** on the **SYSTEM** interface to go to the Fingerprint parameter settings.

Fingerprint
1:N Threshold
35
1:1 Threshold
15
Enrollment Threshold
25
Image Quality
20
Image Enroll Quality
30

Function Name	Descriptions
1:N Threshold	Under 1:N verification method, the verification will only be successful when the similarity between the acquired fingerprint data and the fingerprint templates enrolled in the device is greater than the set value.
1:1 Threshold	Under 1:1 verification method, the verification will only be successful when the similarity between the acquired fingerprint data and the fingerprint template associated with the entered user ID enrolled in the device is greater than the set value.
Enrollment Threshold	During fingerprint enrollment, 1:N comparison is used to determine whether the user has already registered before. When the similarity between the acquired fingerprint and all registered fingerprints is greater than this threshold, it indicates that the fingerprint has already been registered.
Image Quality	Image quality for fingerprint comparison. The higher the value, the clearer the image requires.
Image Enroll Quality	Image quality for fingerprint registration. The registration process requires higher quality standards.

5.6 Voice

Select **Voice** on the **SYSTEM** interface to configure the voice settings.

Voice	
Voice Prompt	☒
Keyboard Prompt	☒
Volume	80

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

5.7 Camera

Select **Camera** on the **SYSTEM** interface.

Camera	
Motion Detection Sensitivity	98
LED Light Trigger Threshold	10
Anti-flicker Mode	50HZ
Binocular Live IOU	20

Function Name	Description
Motion Detection Sensitivity	It is used for detecting whether there is a moving person in front of the device to determine whether the face recognition function is enabled. The default value is 98.

LED Light Trigger Threshold	This value controls the turning on and off of the LED light. The larger the value, the LED light will turn on or off more frequently.
Anti-flicker Mode	This helps reduce flicker when the device's screen flashes at the same frequency as the light.
Binocular Live IOU	In binocular liveness detection, the algorithm detects faces in the images captured by the RGB (visible light) camera and the IR (infrared) camera respectively, and generates a face bounding box for each. The IoU value ranges between 0 and 100, and a larger value indicates a higher degree of overlap between the two boxes. It is used to determine whether the two detection boxes from the RGB and IR images refer to the same person.

5.8 User Interface

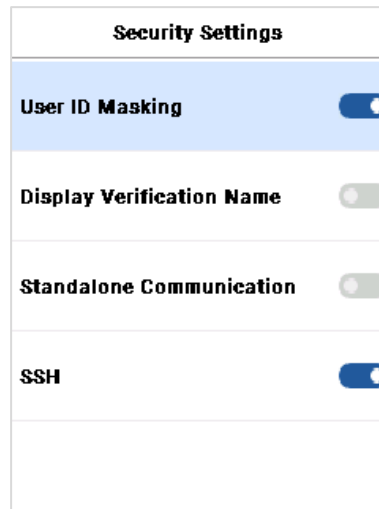
Select **User Interface** on the **SYSTEM** interface.

User Interface
Language
English
Menu Timeout(s)
60
Idle Time to Sleep(m)
30

Function Name	Description
Language	Select the language of the device.
Menu Timeout (s)	When there is no operation, and the time exceeds the set value, the device will automatically go back to the initial interface. The function either can be disabled or set the required value between 60 and 99999 seconds.
Idle Time to Sleep (m)	If the sleep mode is activated, and when there is no operation in the device, then the device will enter standby mode. This function can be disabled or set a value within 1-999 minutes.

5.9 Security Settings

Select **Security Settings** on the **SYSTEM** interface to go to the Security settings.



Function Name	Description
User ID Masking	After enabled, the User ID will be partially displayed after the personnel verification result (only the User ID with more than 2 digits supports the masking display), and it is enabled by default.
Display Verification Name	After enabled, the user's name will be displayed after the personnel verification result. The verification result will not show the name after disabling it.
Standalone Communication	By default, this function is disabled. This function can be enabled or disabled via the menu interface. When it is switched on, a security prompt appears, and the device will restart after you confirm.
SSH	The device does not support the Telnet feature, hence SSH is typically used for remote debugging. By default, SSH is enabled. The menu interface allows you to enable and disable SSH. When enabled, there will be a security prompt, but the device will not need to be restarted after confirmation.

5.10 Advanced Settings

● Debug Mode

When testing features, you can keep **Debug Mode** enabled. Visit http://Device_IPAddress:8080 to download the logs.

1. After the device restarts, previous logs will be cleared.
2. If the firmware crashes, you may not be able to access logs via the browser. In that case, check the “/dev/tmp/log” directory on the backend.
3. Logs are saved up to approximately 6 MB; when this limit is exceeded, older logs will be overwritten.
4. After enabling debug mode, a text prompt “Debug Mode” will appear on the main interface.

● Reset

Select **Reset** on the **Advanced Settings** interface and then press **M/OK** to restore the default factory settings.

The 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).

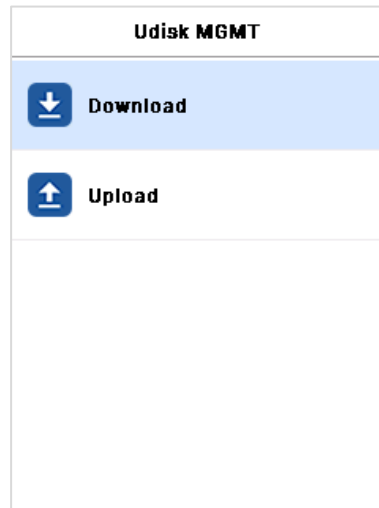


6 USB Disk Management

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

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

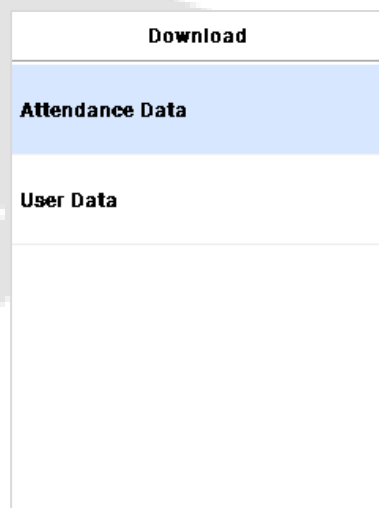
Select **Udisk MGMT** on the main menu interface.



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

6.1 Download to USB Drive

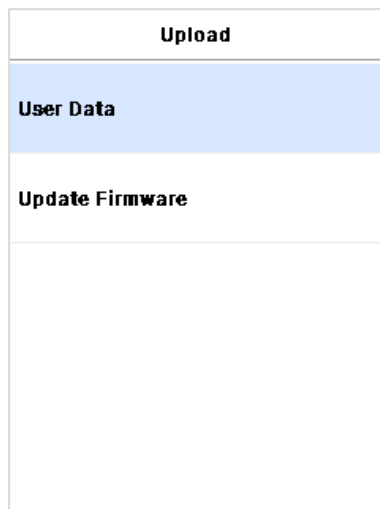
On the **Udisk MGMT** interface, select **Download**.



Function Name	Description
Attendance Data	To download all attendance data in specified time period into USB disk.
User Data	To download all user information from the device into USB disk.

6.2 Upload from USB Drive

On the **Udisk MGMT** interface, select **Upload**.

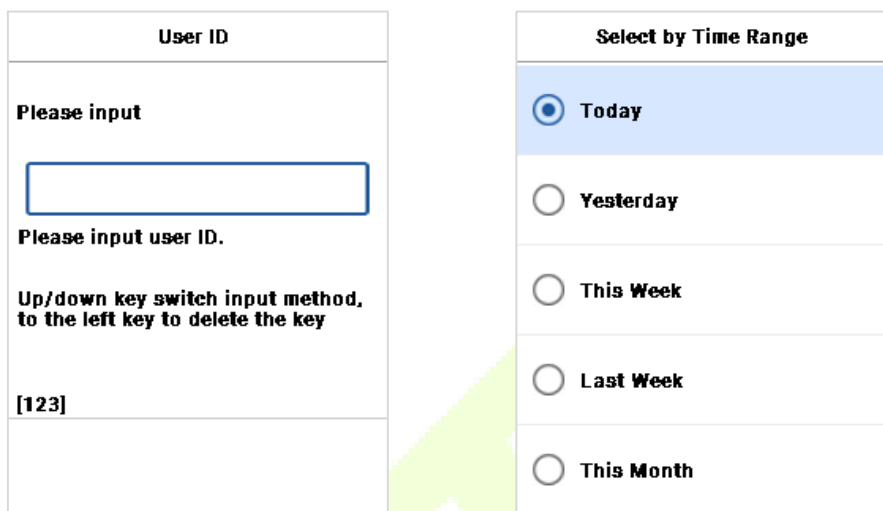


Function Name	Description
User Data	To upload all the user information from USB disk into the device.
Update Firmware	The device's firmware program can be upgraded with the upgrade file in a USB drive. Before conducting this operation, please ensure that the USB drive contains the correct upgrade file and is properly inserted into the device. Note: If upgrade file is needed, please contact our technical support. Firmware upgrade is not recommended under normal circumstances.

7 Attendance Search

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

When the device is on the initial interface, press **M/OK** and select **ATTENDANCE SEARCH** to search for the required attendance record.



User ID

Please input

Please input user ID.

Up/down key switch input method, to the left key to delete the key

[123]

Select by Time Range

☒ Today

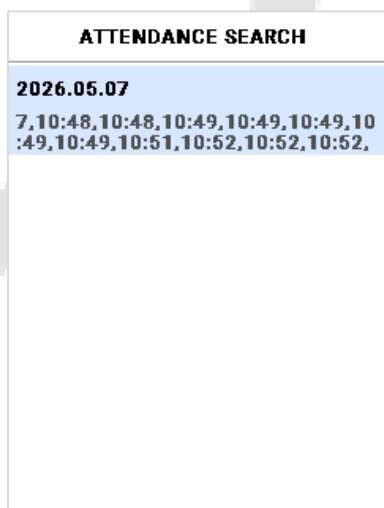
☐ Yesterday

☐ This Week

☐ Last Week

☐ This Month

1. Enter the user ID to be searched and press **M/OK**.
2. Select the time range in which the records need to be searched.



ATTENDANCE SEARCH

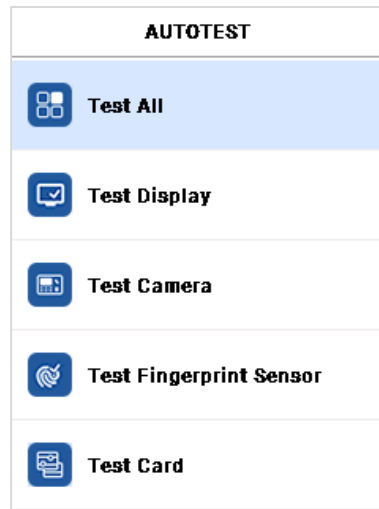
2026.05.07

7,10:48,10:48,10:49,10:49,10:49,10:49,10:49,10:49,10:51,10:52,10:52,10:52,

3. The record search completes.

8 Autotest

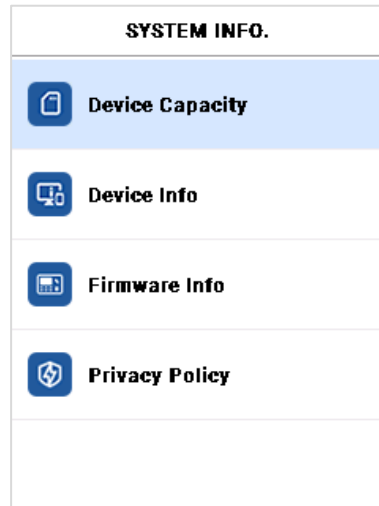
When the device is on the initial interface, press **M/OK** and select **AUTOTEST**, it enables the system to automatically test whether the functions of various modules are working normally, including the display, camera, fingerprint sensor, card★, voice and real-time clock (RTC).



Function Name	Description
Test All	To automatically test whether the display, camera, fingerprint sensor, card, voice and real-time clock are normal.
Test Display	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 Camera	To test if the RGB (visible light) camera and the IR (infrared) camera function properly.
Test Fingerprint Sensor	To test the fingerprint sensor by pressing a finger on the scanner to check if the acquired fingerprint image is clear.
Test Card★	To test the card module by swiping the card on the card reading area.
Test Voice	To automatically test whether the audio files stored in the device are complete and the voice quality is good.
Test Clock RTC	To test the RTC. The device tests whether the clock works normally and accurately with a stopwatch. Press M/OK to start counting and press it again to stop counting.

9 System Information

When the device is on the initial interface, press **M/OK** and select **SYSTEM INFO.** to view the storage status, version information of the device, firmware information and privacy policy.



Function Name	Description
Device Capacity	Displays the current device's user, T&A records, fingerprint, face template, palm, card★, super admin, and password storage.
Device Info	Displays the device's name, serial number, MAC address, WIFI MAC address, platform information and manufacturer.
Firmware Info	Displays the firmware version and other version information of the device. 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 "No new versions". • 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.
Privacy Policy	To view the content of the privacy policy. The privacy policy's content does not allow for U disc export.

10 Connecting to ZKBio Zlink App

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

- **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

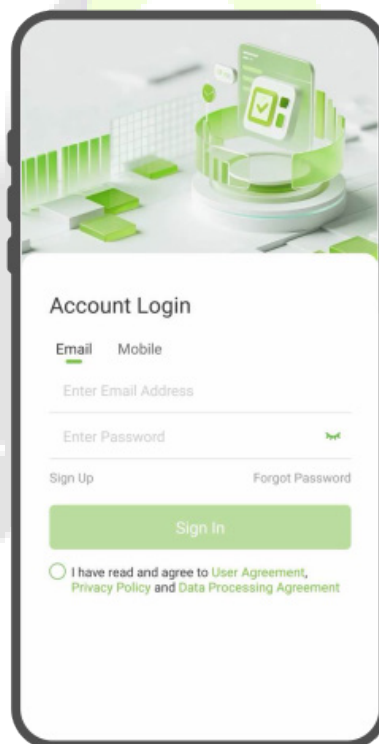


Google Play Store



10.1 Login to the App

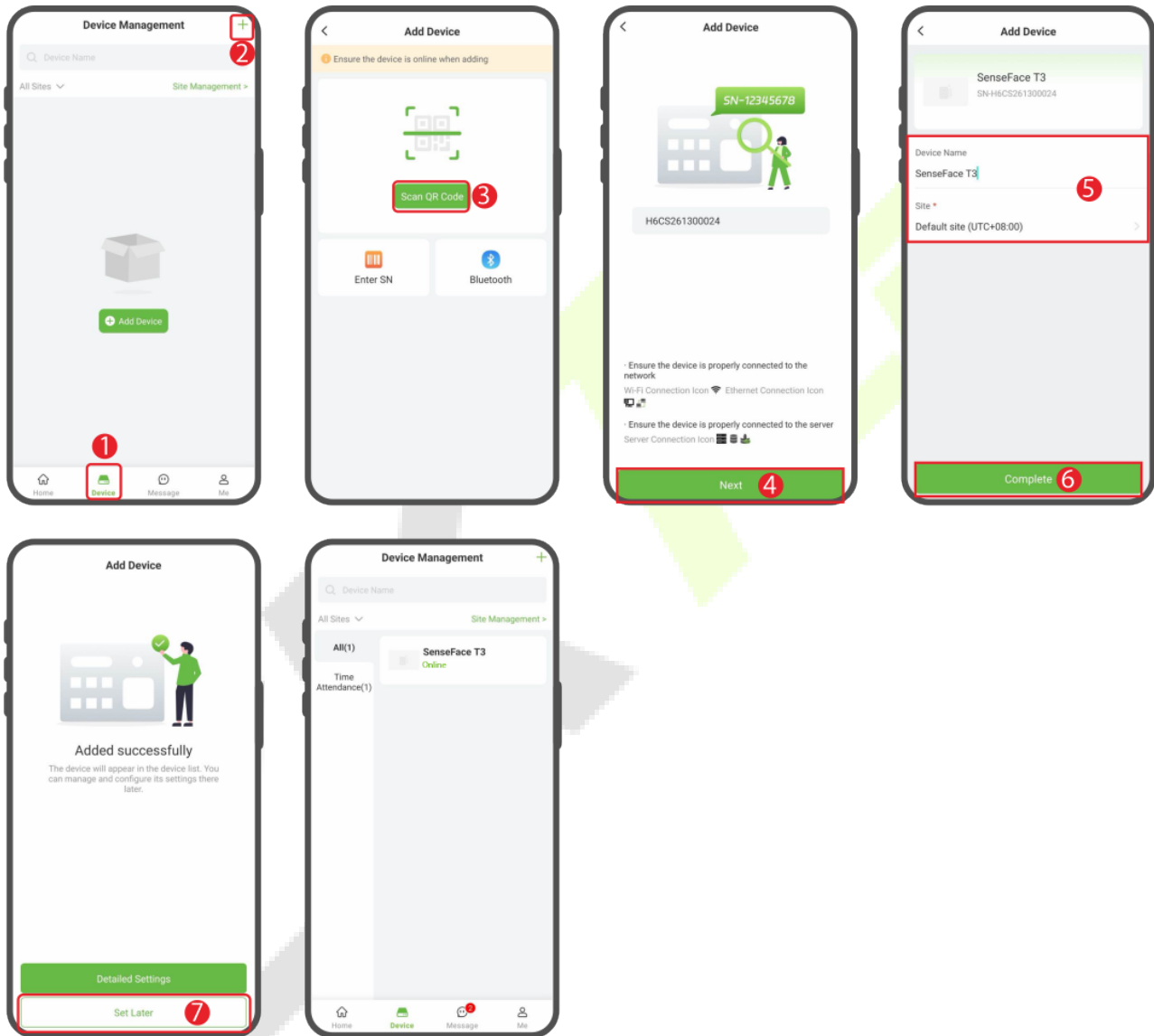
Enter your registered account and password, check "I have read and agree to User Agreement, Privacy Policy and Data Processing Agreement" and click **Sign In** to log in to the App.



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

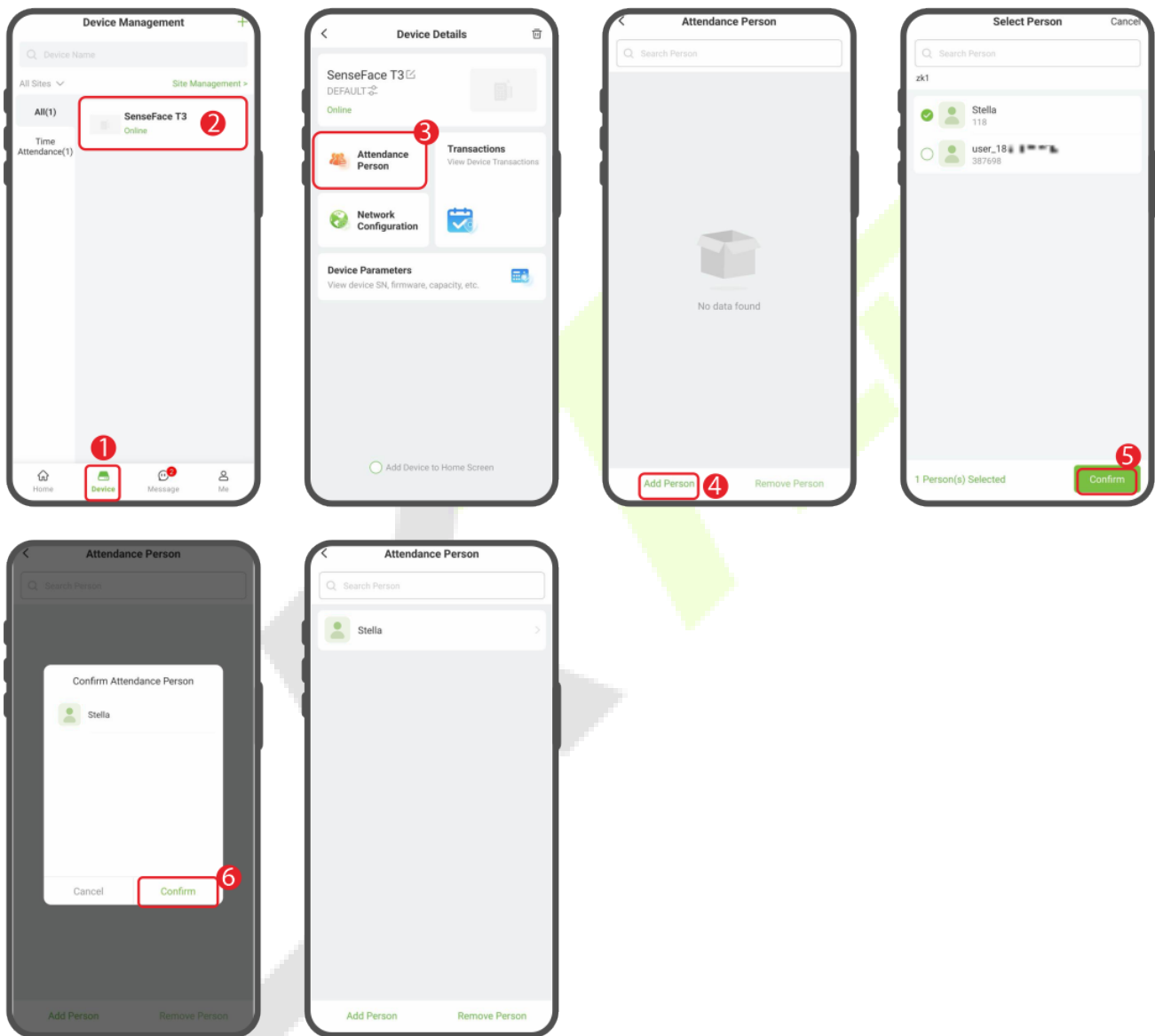
10.2 Add Device on the App

- Access the ZKBio Zlink App and click on **[Device]** > **+** icon > **[Scan QR Code]** to scan the QR code on the device. Then click **[Next]**. (1,2,3,4)
- Enter the device name and specify the device to a site. Click **[Complete]** to complete the addition. At the same time, the device voice prompts **"Device is added successfully"** indicating that the addition is complete. (5,6,7)
- Once successfully added, the device is displayed in the list of the device interface.



10.3 Manage and Add Person to Device

- Click [**Device**], select the device in the list to enter the Device Details interface. (1,2)
- Click [**Attendance Person**] > [**Add Person**], select the persons and click [**Confirm**] to add them to the device. (3,4,5)
- Click [**Confirm**] in the pop-up confirmation window. (6)
- After completion, the personnel will be synchronized to the device.

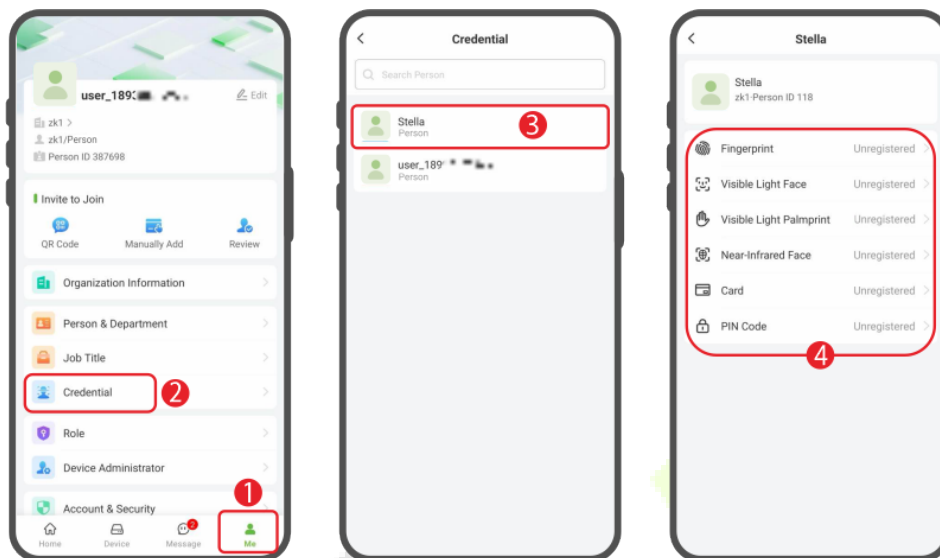


10.4 Register Verification Mode on the App

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

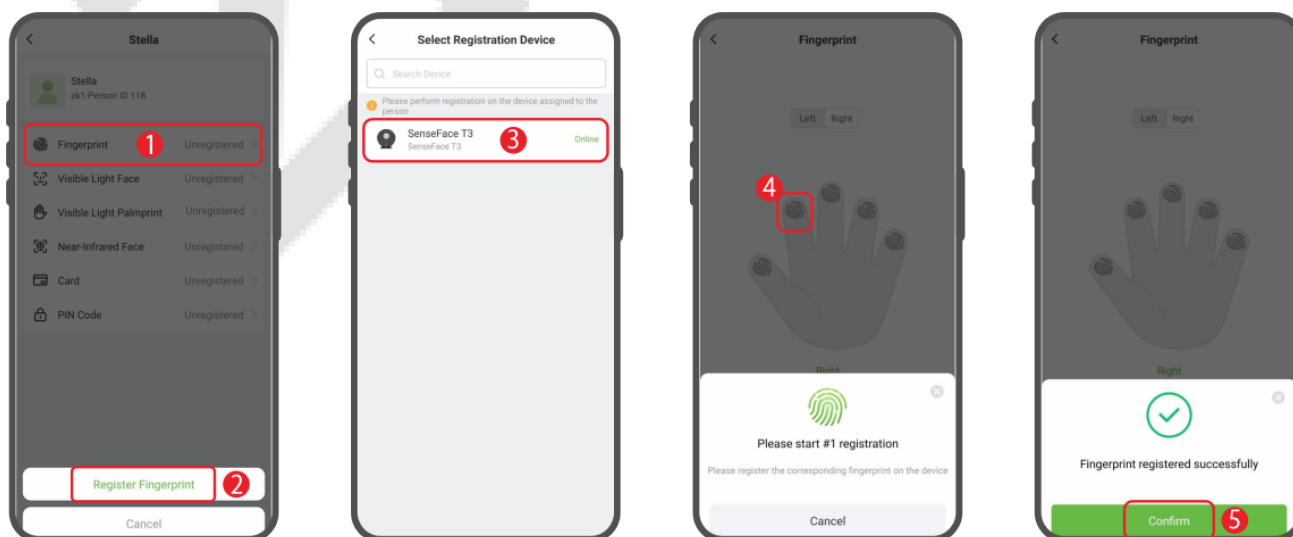
Note: It must be based on the functions actually supported by the device.

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



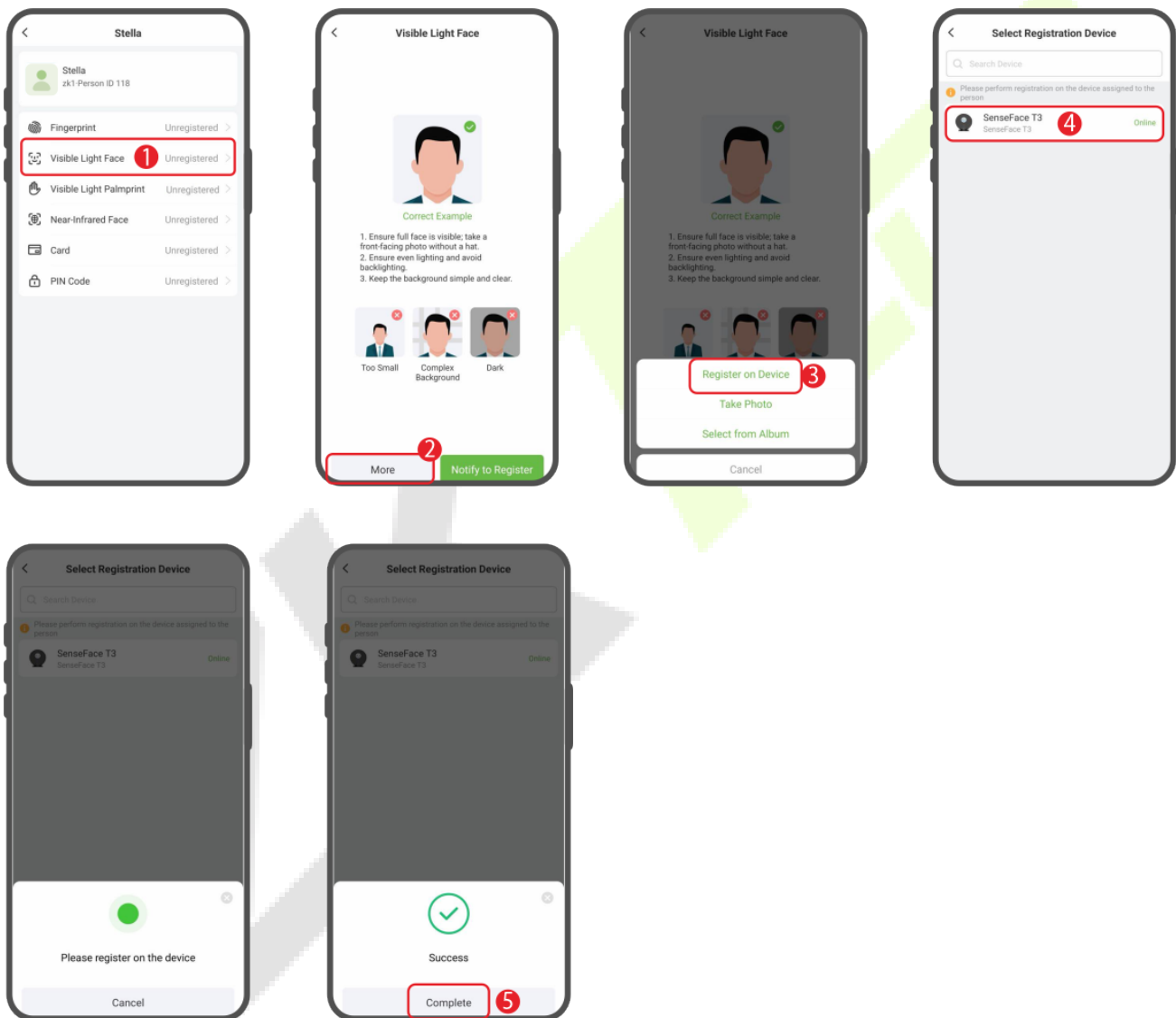
Register Fingerprint

- Click the  icon > **[Register Fingerprint]**, select the registration device and the finger to be enrolled. (1,2,3,4)
- Then 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 **"Successfully registered"**, it means the fingerprint registration is successful.
- Click **[Confirm]** to return. And you can repeat the above operation to register other fingers. (5)



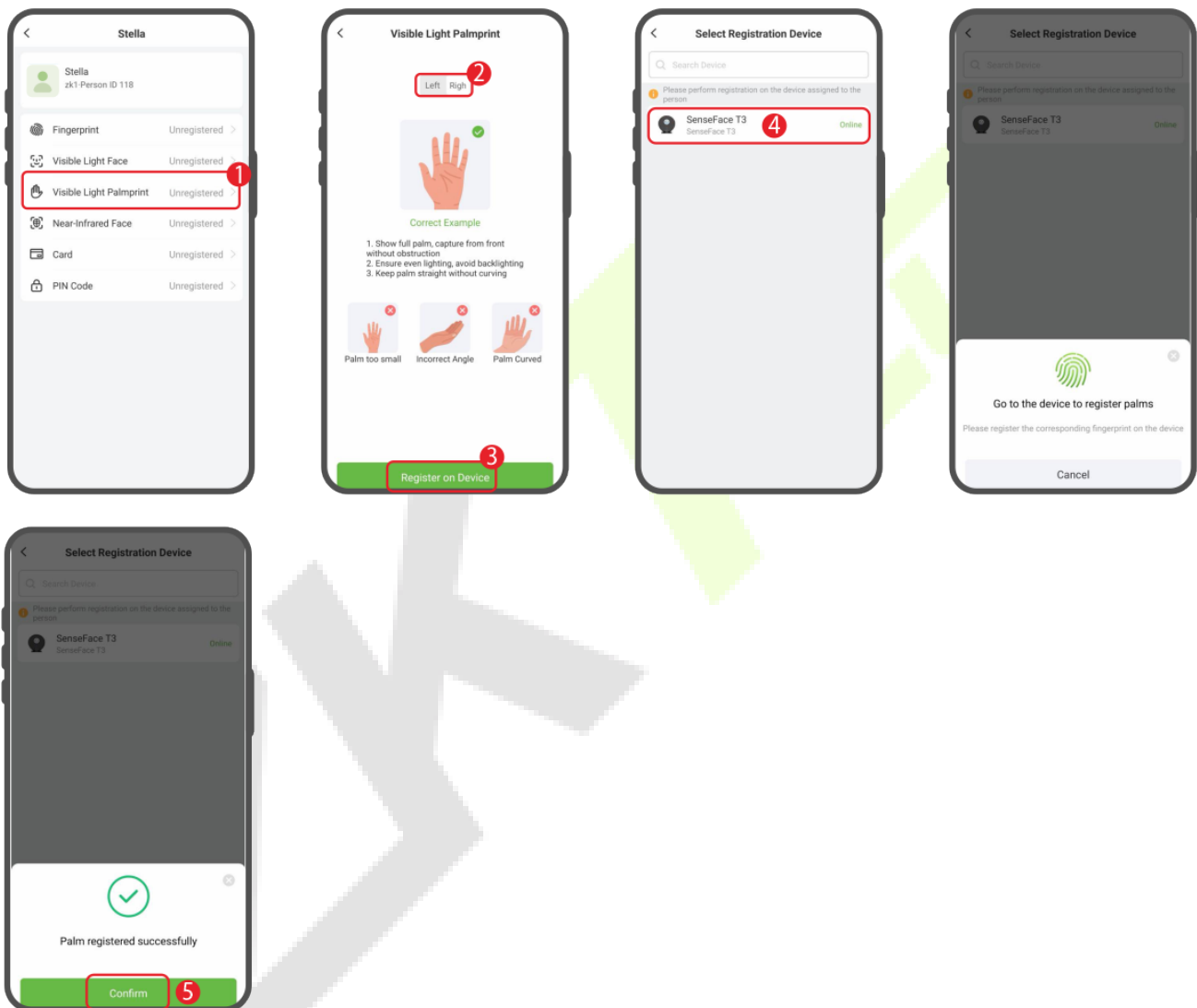
Register Face

- Click the  icon > **[More]** > **[Register on Device]**, select the registration device. (1,2,3,4)
- Then the device displays the face registration screen. According to the prompts, face towards the camera and stay still during face template registration. When the interface prompts **“Successfully registered”**, it means the face registration is successful.
- Click **[Complete]** to return. (5)
- You can also choose **Take Photo**, **Select form Album** or **Notify to Register** to send a message to the person to upload the facial photo. (**Note:** The person should be activated.)



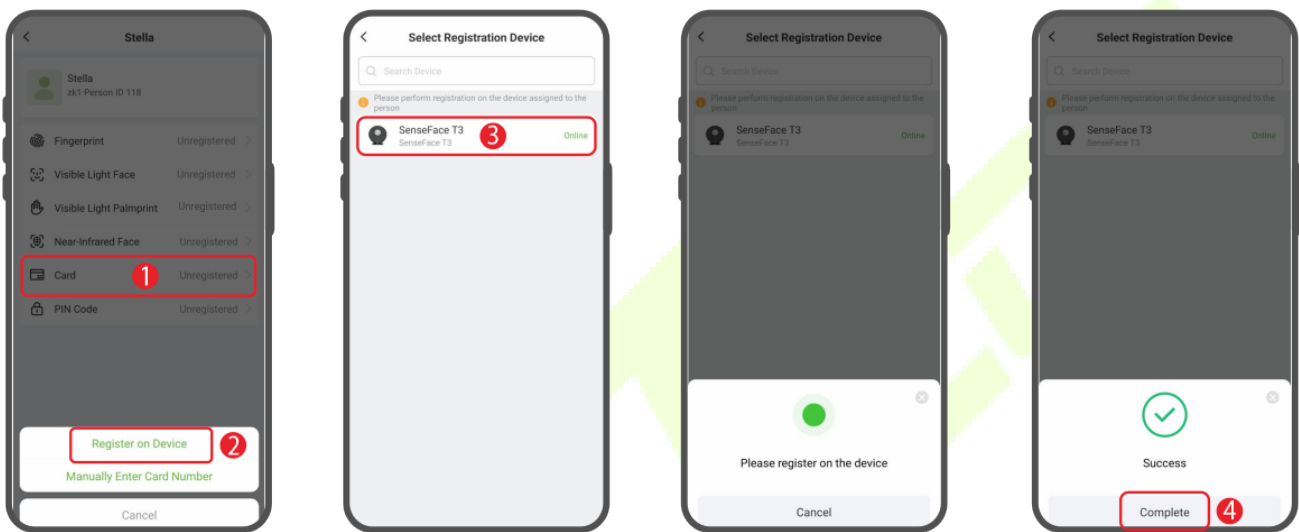
Register Palm

- Click the  icon, select the left or right hand to be enrolled and click [**Register on Device**], select the registration device. (1,2,3,4)
- Then the device displays the palm registration screen. According to the prompts, place your palm in the palm multi-mode collection area. When the interface prompts “**Successfully registered**”, it means the palm registration is successful.
- Click [**Confirm**] to return. (5)



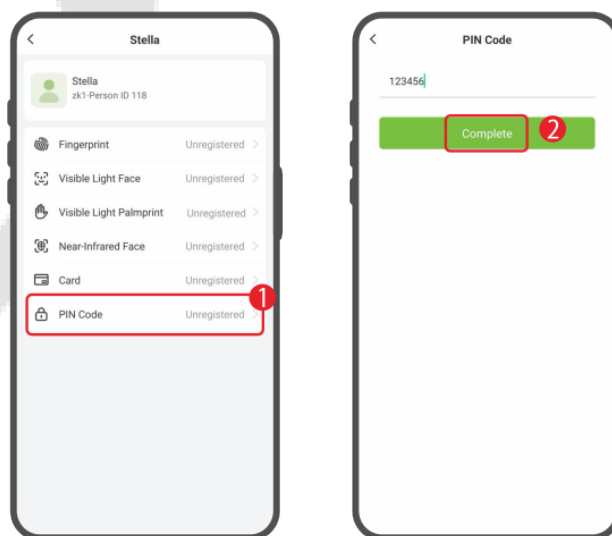
Register Card★

- 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 it prompts **“Thank you”**, it means the card is successfully registered. (3)
- Click [**Complete**] to return. (4)



Register Password

Click on the  icon and enter the password in the pop-up window, then click [**Complete**]. (1,2)



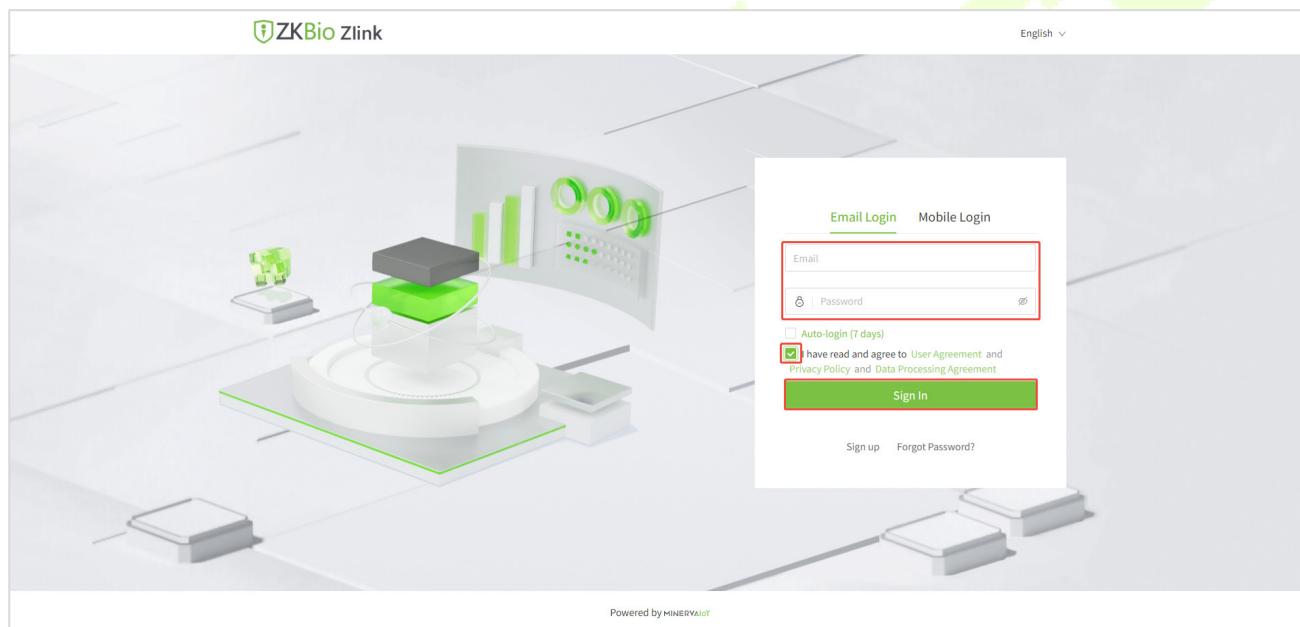
11 Connecting to ZKBio Zlink Web

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

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.

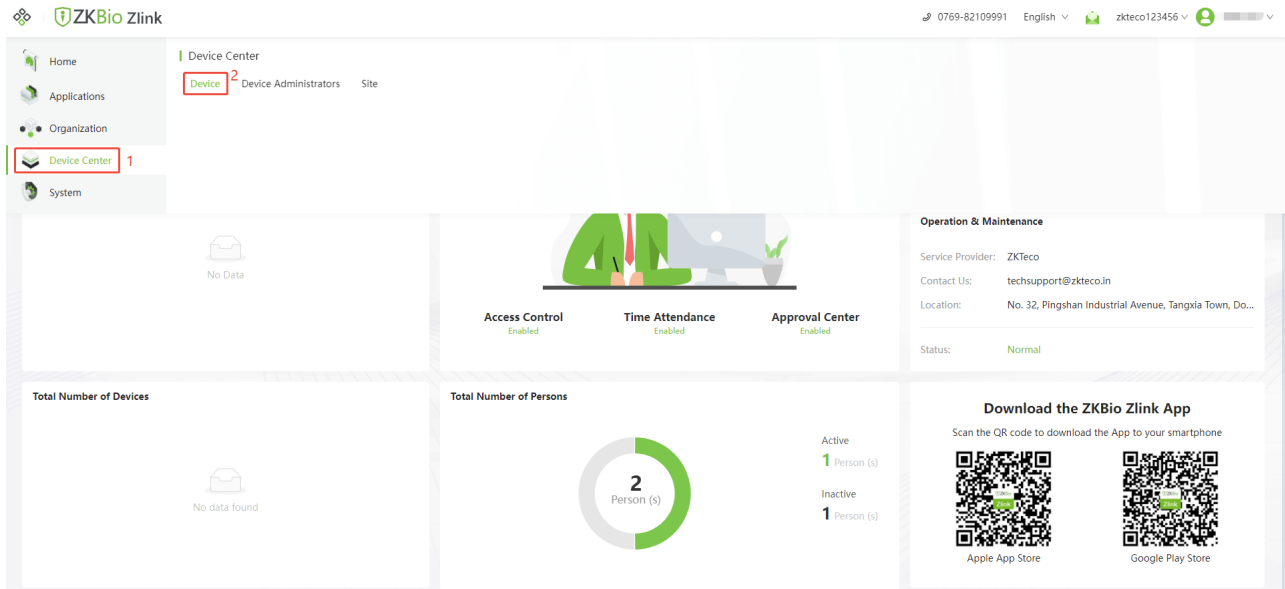
11.1 Login to the Web

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.

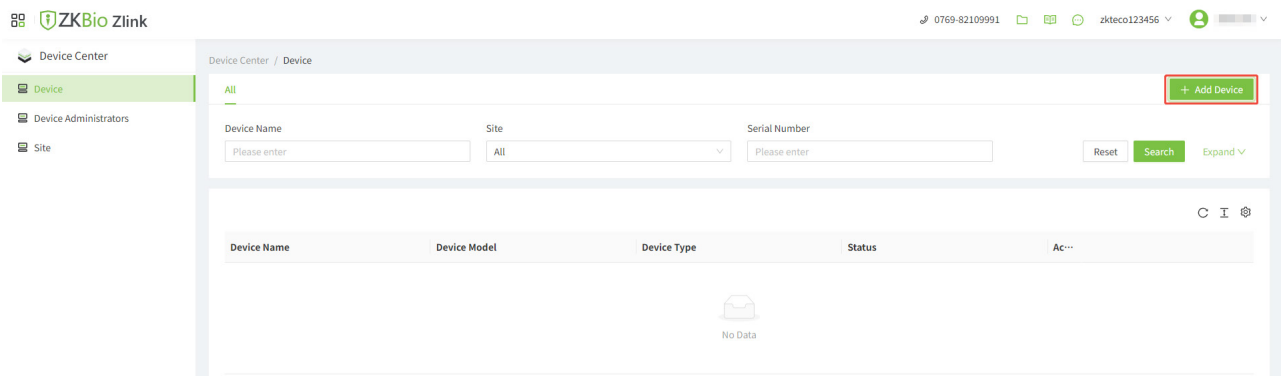


11.2 Add Device on the Web

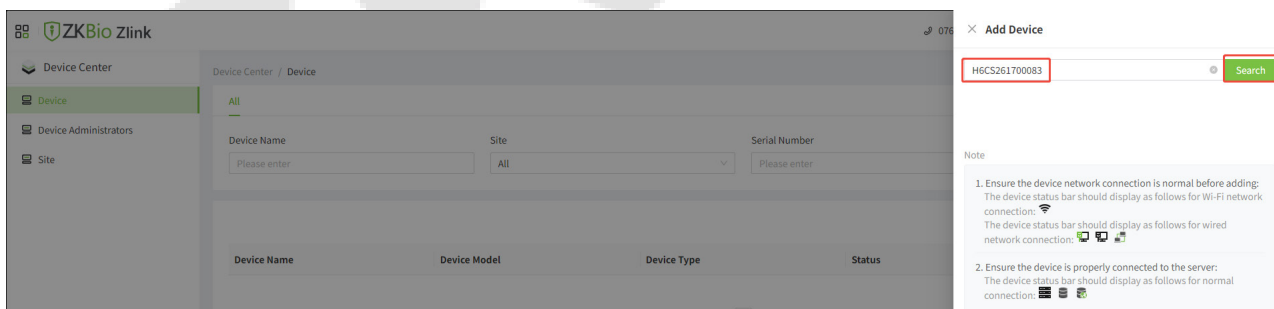
1. Click the  icon on the top left corner, and click [**Device Center**] > [**Device**] to enter the device setting interface.



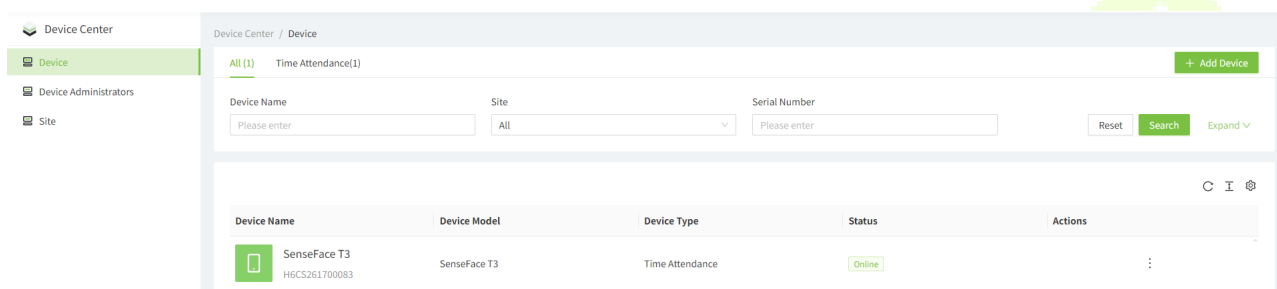
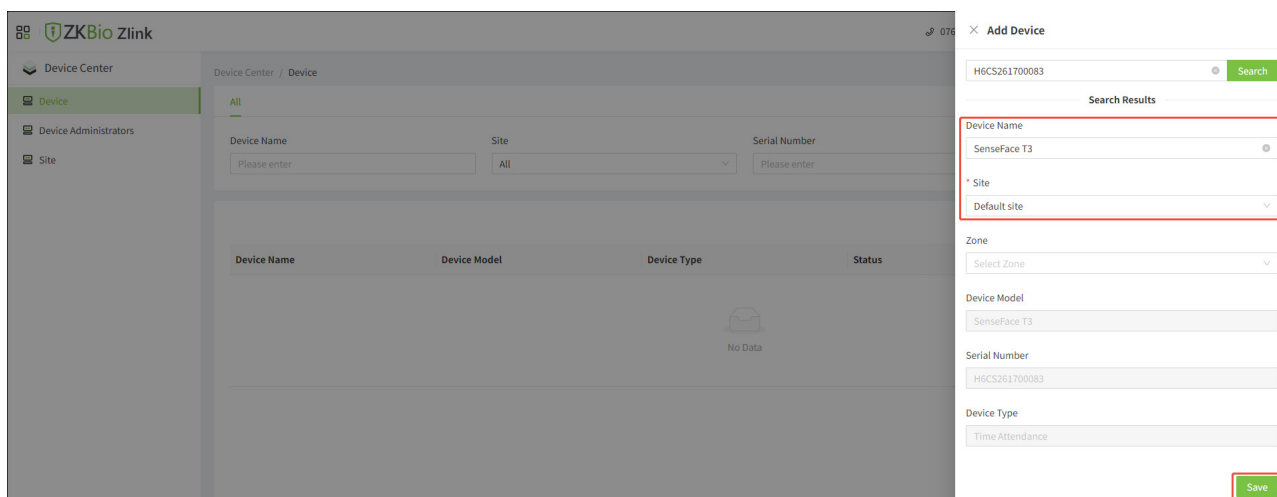
2. Then click [+Add Device] to enter the Add Device interface.



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



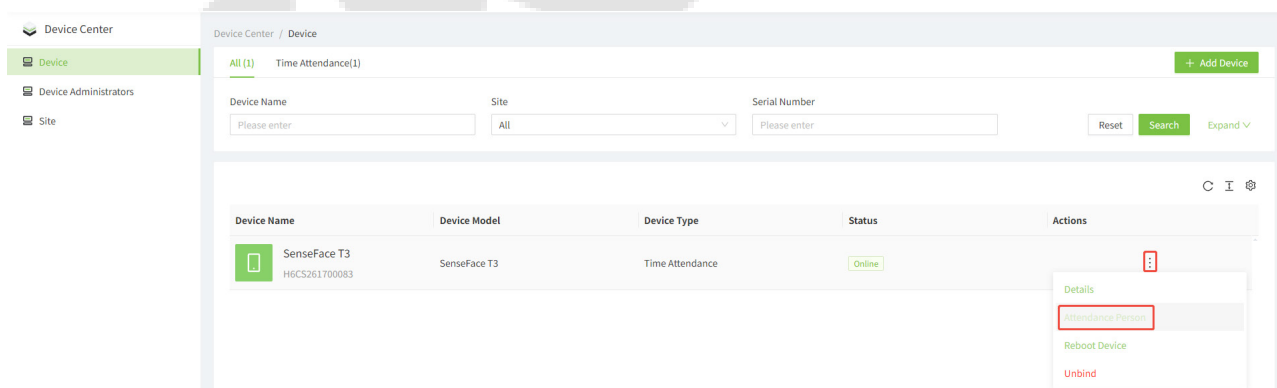
4. Then enter the device name and specify the device to a site. Select Site from the drop-down menu. Click [Save] to complete the addition.



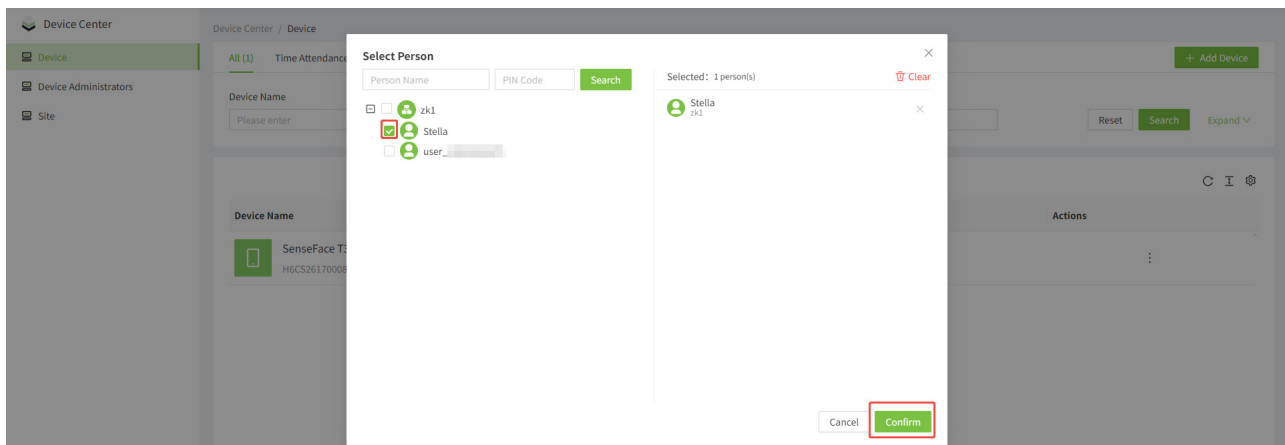
Note: Wait a moment for the device status to change from “Offline” to “Online”.

11.3 Manage and Add Person to Device

- Click the  icon on the top left corner, and click [Device Center] > [Device] to enter the device setting interface. Select the device in the list, click the  icon > [Attendance Person] to enter the Select Person interface.

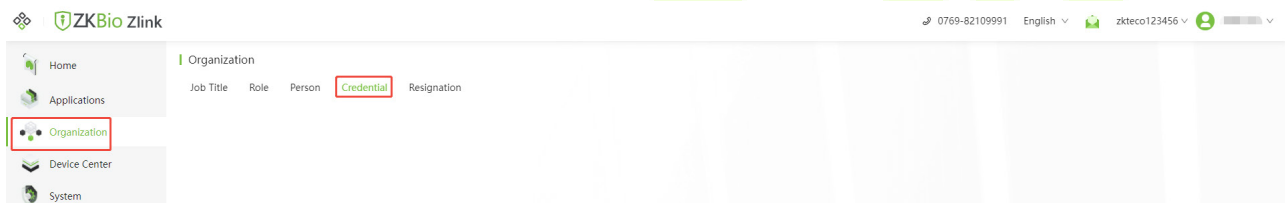


- Tick the person in the pop-up window and click [Confirm] to add the person to the device.

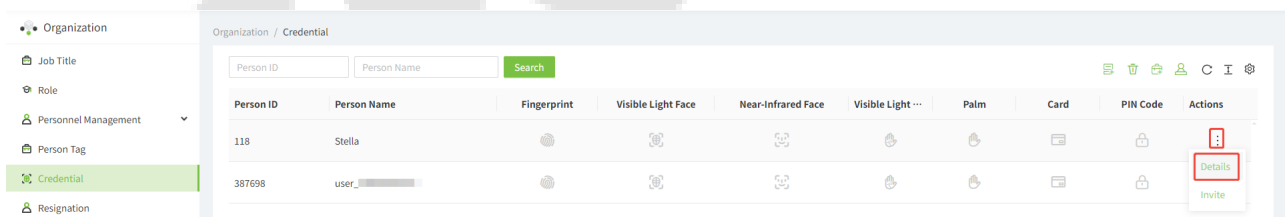


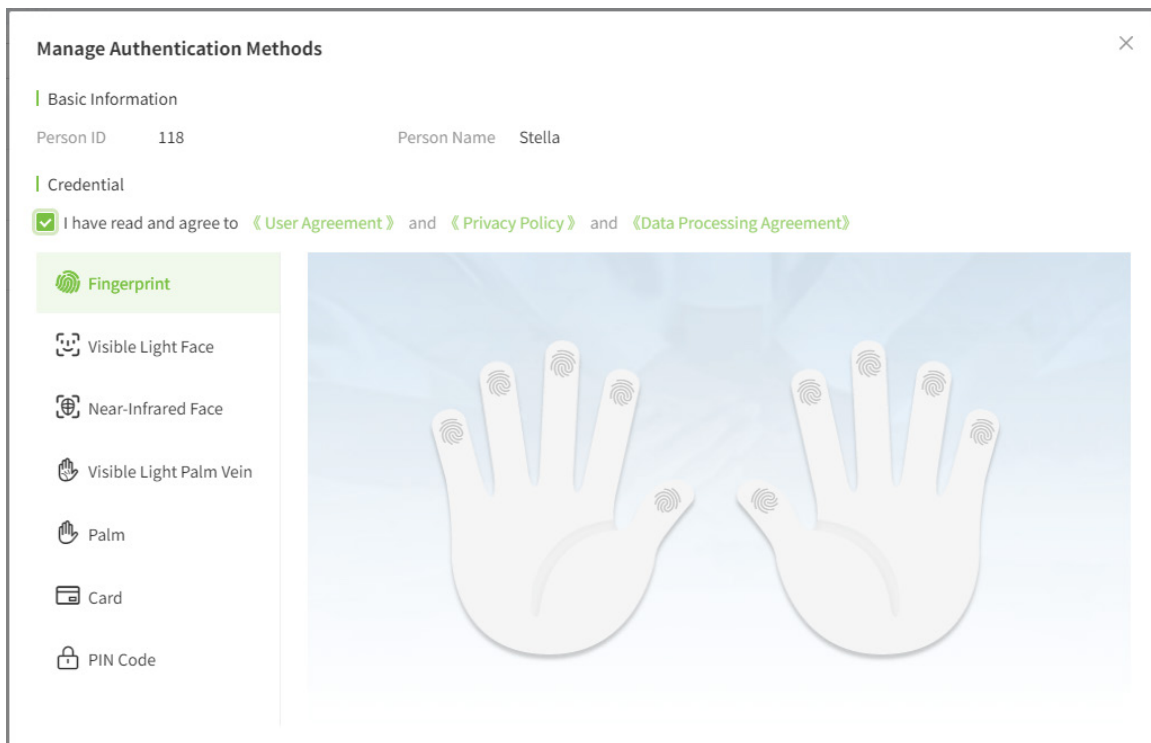
11.4 Register Verification Mode on the Web

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



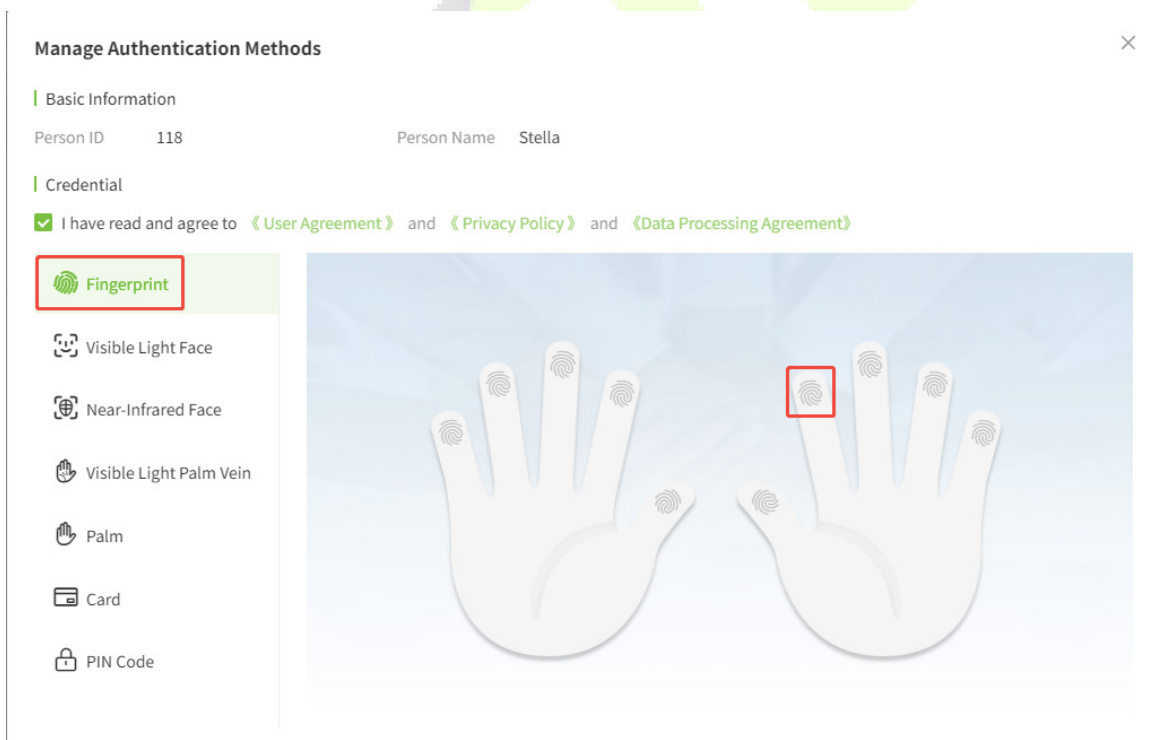
2. Select the person and click the  icon > **Details**, check "I have read and agree to User Agreement and Privacy Policy and Data Processing Agreement" and click **Fingerprint/Visible Light Face/Visible Light Palm Vein/Card/PIN Code** to remotely register the personnel biometric verification mode.



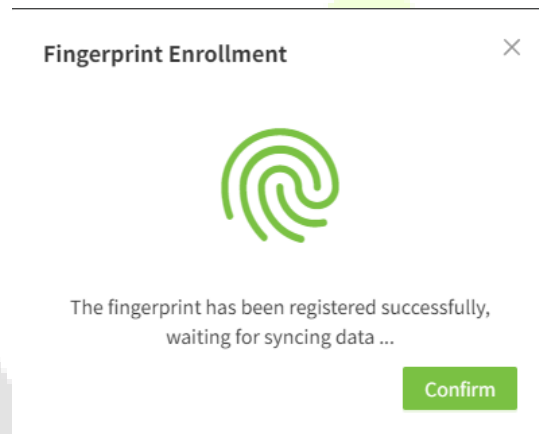
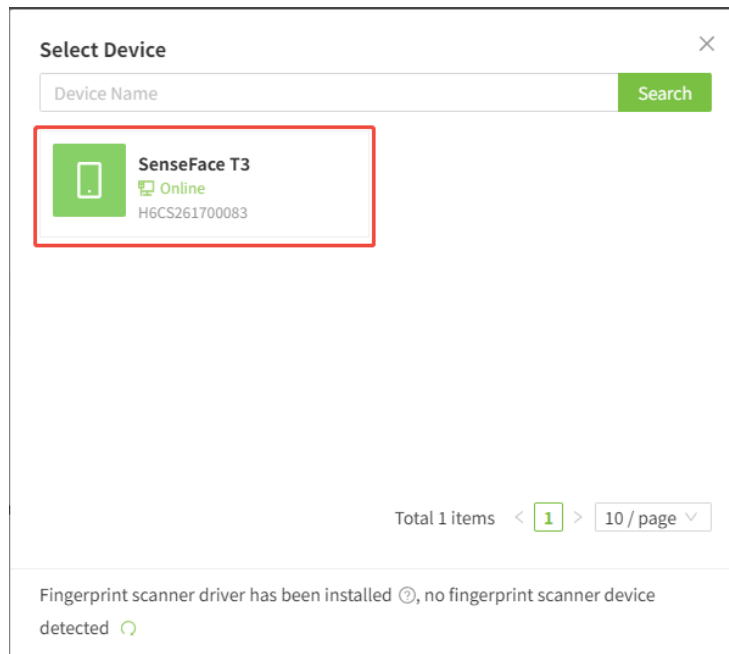


- **Register Fingerprint**

1. Click **Fingerprint** in the Details page. Choose the finger to be enrolled.



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 "Successfully registered", it means the fingerprint registration is successful.



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

- **Register Face**

1. Click **Visible Light Face** in the Details page. You can select Remote Enrollment or Upload photo. If you want to register on device, then click **Remote Enrollment**.

Manage Authentication Methods



Basic Information

Person ID 118

Person Name Stella

Credential

☒ I have read and agree to [《User Agreement》](#) and [《Privacy Policy》](#) and [《Data Processing Agreement》](#)

Fingerprint

Visible Light Face

Near-Infrared Face

Visible Light Palm Vein

Palm

Card

PIN Code



Visible Light Face

Upload photo

Remote Enrollment

Notes: Supports JPG, JPEG, PNG formats, with a single photo size not exceeding 2M and a resolution not exceeding 1080px * 1920px. Once exceeded, photos cannot be uploaded successfully.

2. Select the registration device, at the same time, the device displays the Enroll Face interface. Face towards the camera and stay still during face template registration, when the display shows "Successfully registered", it means the face is successfully registered.

Select Device

Device Name

Search

SenseFace T3

Online

H6CS261700083

Total 1 items < 1 > 10 / page

Fingerprint scanner driver has been installed ⓘ, no fingerprint scanner device detected ⓘ

Visible Light Face Enrollment

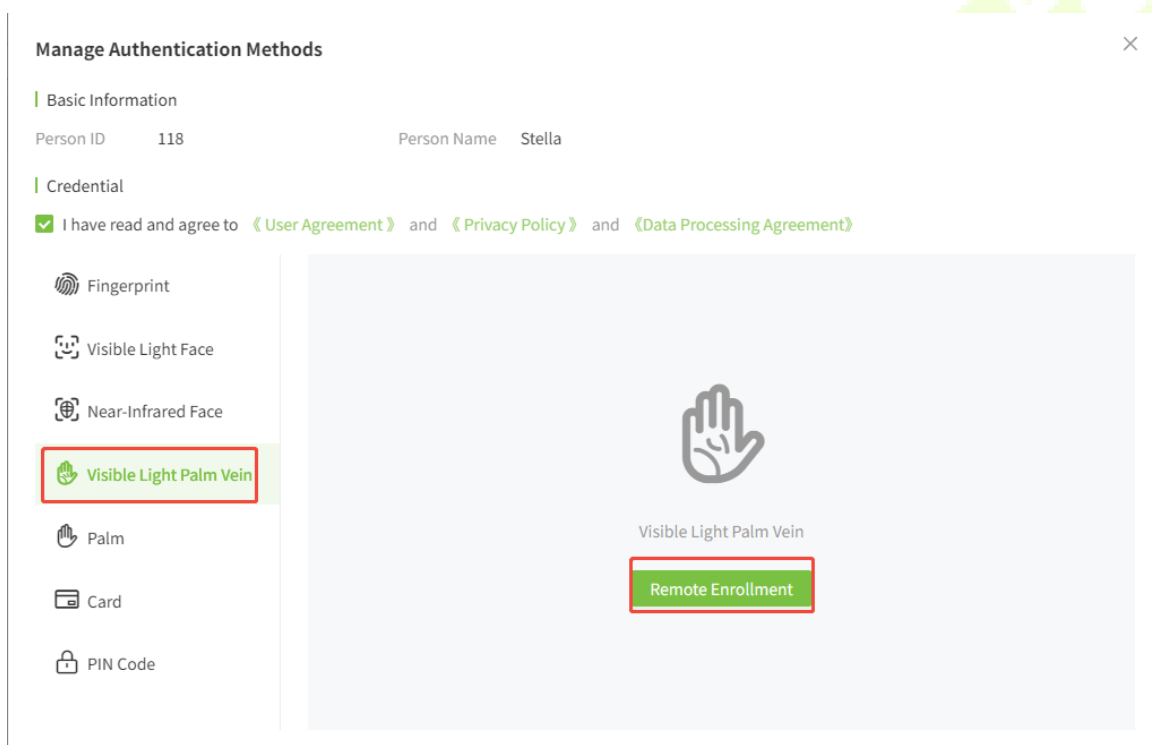


The visible light face has been registered successfully,
waiting for syncing data ...

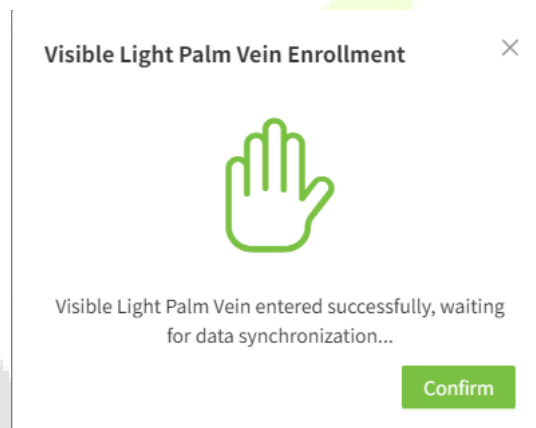
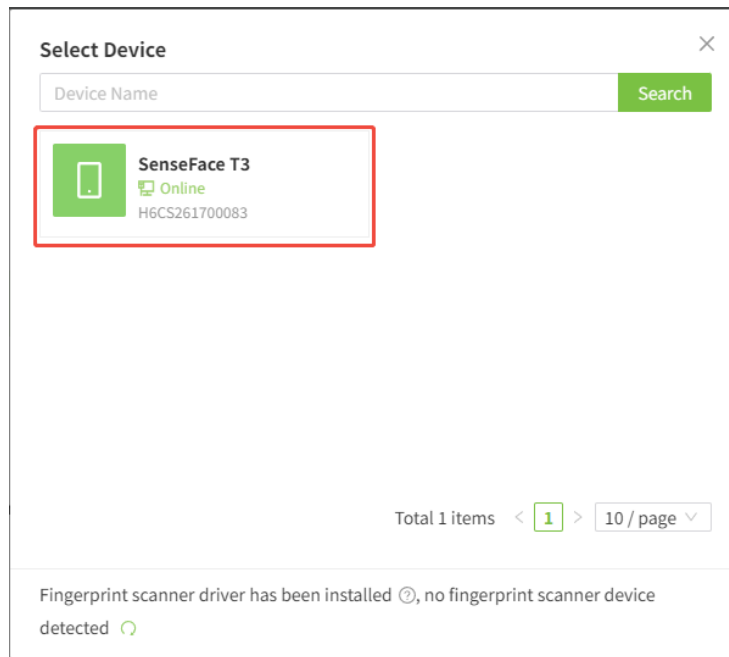
Confirm

- **Register Palm**

1. Click **Visible Light Palm Vein** in the Details page. Then click **Remote Enrollment**.

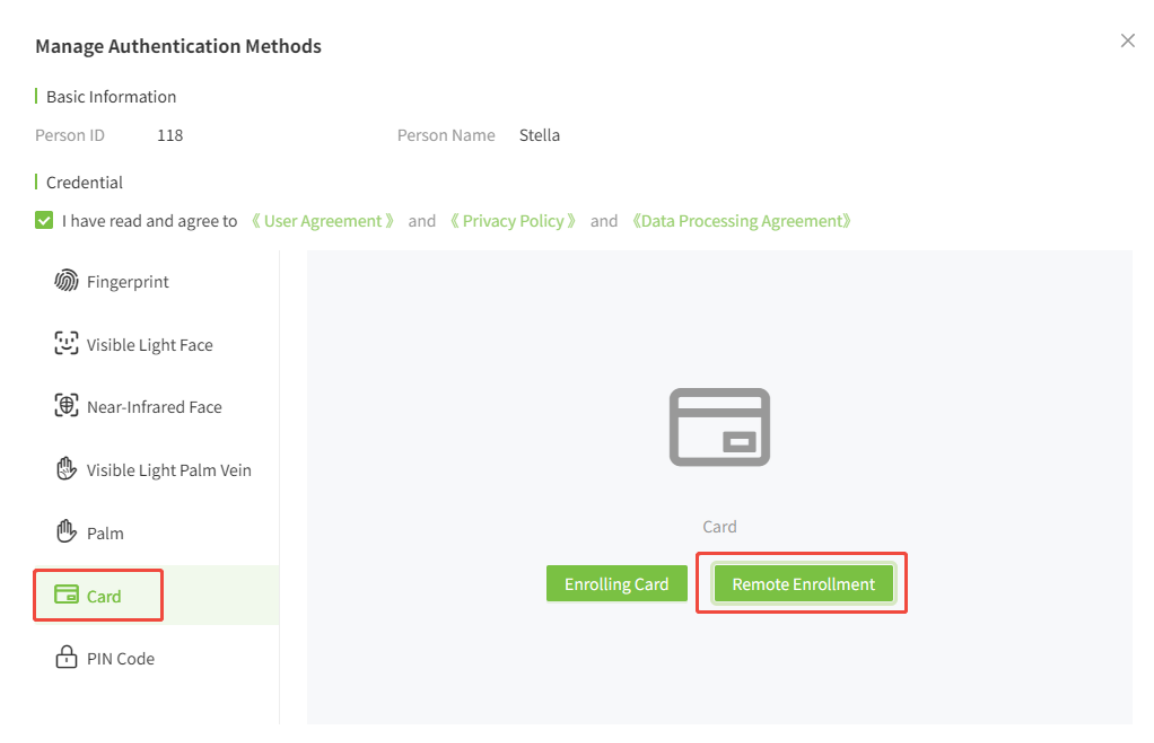


2. Select the registration device, at the same time, the device displays the Enroll Palm interface. Place your palm in the palm multi-mode collection area, when the display shows “Successfully registered”, it means the palm is successfully registered.

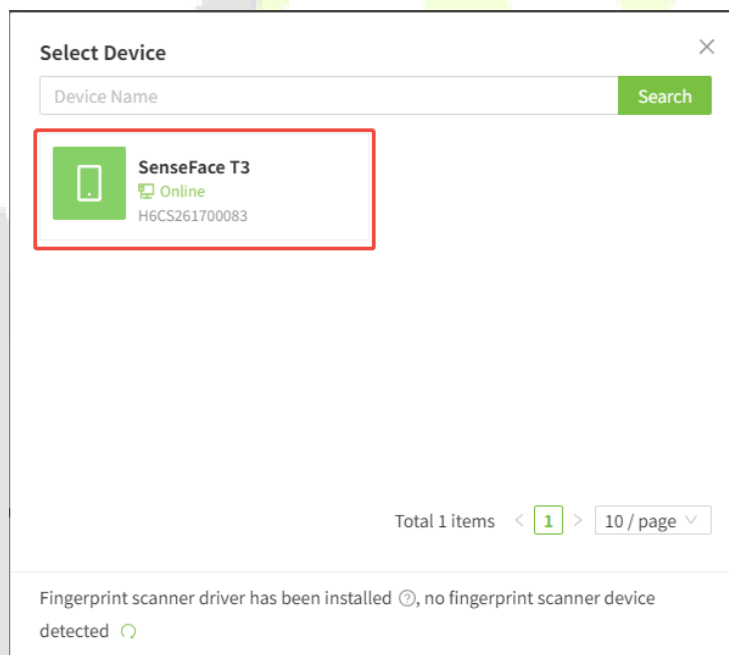


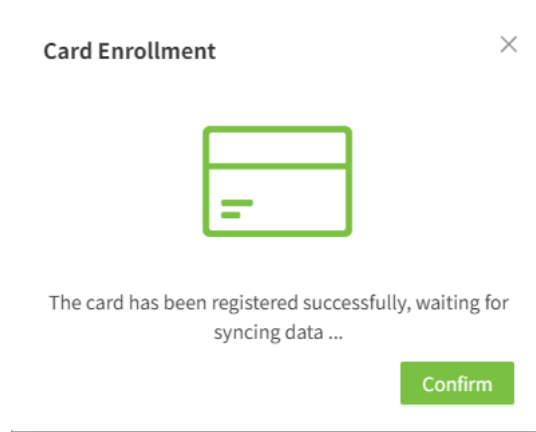
- **Register Card★**

1. Click **Card** in the Details page. You can select Remote Enrollment or Enrolling Card. If you want to register on device, then click **Remote Enrollment**.



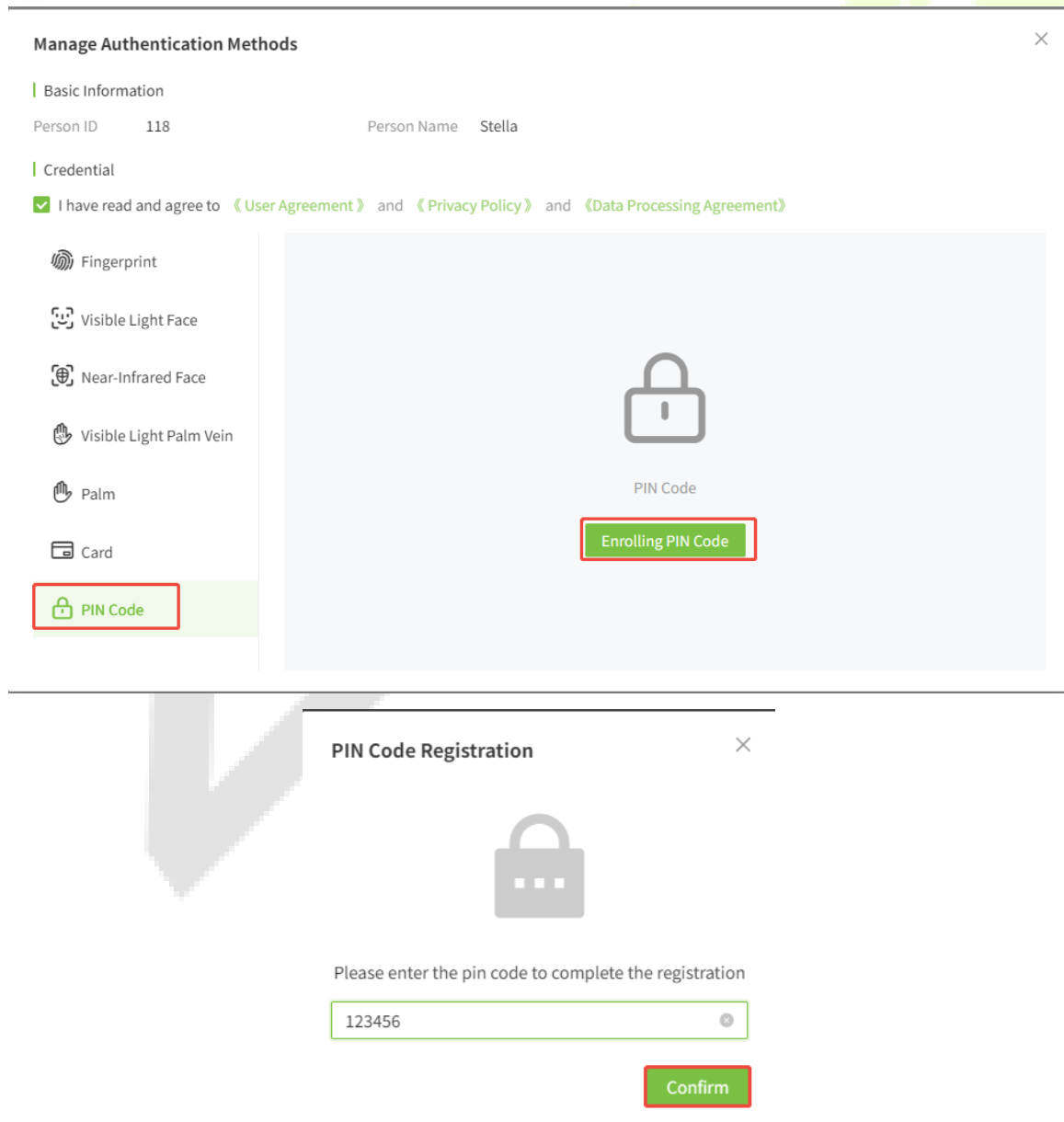
2. Select the registration device, the device will display the **Enroll Card Number** interface. Place the card in the swipe area, when the device prompts "Thank you", it means the card is successfully registered.





- **Register Password**

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



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

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 appropriate lighting to avoid 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 tilt your head to any direction).
- 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 example 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 angle**

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) A neutral facial expression or a slight smile is preferred, but showing teeth is not recommended.
- 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	○	○	○	×	○	○

This table is prepared in accordance with the provisions of SJ/T 11364.

○ indicates that the total amount of toxic content in all the homogeneous materials is below the limit as specified in GB/T 26572.

× indicates that the total amount of toxic content in all the homogeneous materials exceeds the limit as specified in GB/T 26572.

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.

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

