

User Manual

FaceDepot-7BL

Date: June 2022

Doc Version: 1.2

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 © 2022 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-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 **FaceDepot-7BL** Product.

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 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 INSTRUCTIONS TO USE | 10 |
| 1.1 FINGER POSITIONING★ | 10 |
| 1.2 STANDING POSITION, POSTURE AND FACIAL EXPRESSION..... | 10 |
| 1.3 PALM REGISTRATION | 12 |
| 1.4 FACE REGISTRATION | 12 |
| 1.5 STANDBY INTERFACE | 13 |
| 1.6 VIRTUAL KEYBOARD..... | 15 |
| 1.7 VERIFICATION MODES | 15 |
| 1.7.1 PALM VERIFICATION | 15 |
| 1.7.2 FINGERPRINT VERIFICATION★ | 17 |
| 1.7.3 FACIAL VERIFICATION | 22 |
| 1.7.4 CARD VERIFICATION ★ | 25 |
| 1.7.5 PASSWORD VERIFICATION..... | 27 |
| 1.7.6 COMBINED VERIFICATION..... | 30 |
| 2 MAIN MENU | 31 |
| 3 USER MANAGEMENT | 33 |
| 3.1 ADDING USERS..... | 33 |
| 3.2 SEARCH FOR USERS..... | 38 |
| 3.3 EDIT USERS..... | 39 |
| 3.4 DELETING USERS..... | 39 |
| 4 USER ROLE | 40 |
| 5 COMMUNICATION SETTINGS..... | 42 |
| 5.1 NETWORK SETTINGS | 42 |
| 5.2 PC CONNECTION | 43 |
| 5.3 CLOUD SERVER SETTING..... | 44 |
| 5.4 WIEGAND SETUP | 45 |
| 5.4.1 WIEGAND INPUT | 45 |
| 5.4.2 WIEGAND OUTPUT | 47 |
| 6 SYSTEM SETTINGS..... | 48 |
| 6.1 DATE AND TIME..... | 48 |
| 6.2 ACCESS LOGS SETTING | 50 |
| 6.3 FACE PARAMETERS | 51 |
| 6.4 PALM PARAMETERS | 53 |
| 6.5 FINGERPRINT PARAMETERS★ | 53 |
| 6.6 FACTORY RESET..... | 54 |
| 6.7 SECURITY SETTINGS | 55 |
| 6.8 USB UPGRADE..... | 56 |

| | | |
|-------------------------|--|-----------|
| 7 | PERSONALIZE SETTINGS | 57 |
| 7.1 | INTERFACE SETTINGS | 57 |
| 7.2 | VOICE SETTINGS | 58 |
| 7.3 | BELL SCHEDULES..... | 59 |
| 7.4 | PUNCH STATE OPTIONS | 60 |
| 7.5 | SHORTCUT KEY MAPPINGS | 61 |
| 8 | DATA MANAGEMENT | 63 |
| 8.1 | DELETE DATA | 63 |
| 9 | ACCESS CONTROL | 65 |
| 9.1 | ACCESS CONTROL OPTIONS | 66 |
| 9.2 | TIME SCHEDULE | 68 |
| 9.3 | HOLIDAY SETTINGS..... | 70 |
| 9.4 | ACCESS GROUPS | 71 |
| 9.5 | COMBINED VERIFICATION SETTINGS..... | 72 |
| 9.6 | DURESS OPTIONS SETTINGS..... | 73 |
| 10 | USB MANAGER..... | 74 |
| 10.1 | DOWNLOAD | 74 |
| 10.2 | UPLOAD..... | 75 |
| 11 | ATTENDANCE SEARCH | 76 |
| 12 | AUTOTEST | 82 |
| 13 | SYSTEM INFORMATION..... | 83 |
| 14 | CONNECTION TO ZKBIOSECURITY SOFTWARE..... | 84 |
| 14.1 | SET THE COMMUNICATION ADDRESS..... | 84 |
| 14.2 | ADD A DEVICE TO THE SOFTWARE..... | 85 |
| 14.3 | ADD PERSONNEL ON THE SOFTWARE..... | 86 |
| APPENDIX 1 | 87 | |
| | REQUIREMENTS OF LIVE COLLECTION AND REGISTRATION OF VISIBLE LIGHT FACE IMAGES..... | 87 |
| | REQUIREMENTS FOR VISIBLE LIGHT DIGITAL FACE IMAGE DATA | 88 |
| APPENDIX 2 | 89 | |
| | PRIVACY POLICY..... | 89 |
| | ECO-FRIENDLY OPERATION..... | 91 |

Data Security Statement


ZKTeco, as a smart product supplier, may also need to know and collect some of your personal information in order 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 below instructions intend to ensure that the user can use the product correctly to avoid danger or property loss. The following precautions are to keep users safe and prevent any damage. Please read carefully before installation.

 Noncompliance with instructions could lead to product damage or physical injury (may even cause death).

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 Mains AC or DC power source and refer service personnel under the following conditions:
 - When cord or connection control is affected.
 - When the liquid spilled, or an item dropped into the system.
 - If exposed to water or due to inclement weather (rain, snow, and more).
 - If the system is not operating normally, under operating instructions.

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

And do not connect multiple devices to one power adapter as adapter overload can cause over-heat or fire hazard.

7. **Replacement parts** - When replacement parts are needed, service technicians must only use replacement parts provided by the supplier. Unauthorized substitutes can result in a burn, 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 device.
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 from destroying the system.

Recommended installing the devices in areas with limited access.

Electrical Safety

- Before connecting an external cable to the device, complete grounding properly, and set up surge protection; otherwise, static electricity will damage the mainboard.
- Make sure that the power has been disconnected before you wire, install, or dismantle the device.
- Ensure that the signal connected to the device is a weak-current (switch) signal; otherwise, components of the device will get damaged.
- Ensure that the standard voltage applicable in your country or region is applied. If you are not sure about the endorsed standard voltage, please consult your local electric power company. Power mismatch may cause a short circuit or device damage.
- In the case of power supply damage, return the device to the professional technical personnel or your dealer for handling.
- To avoid interference, keep the device far from high electromagnetic radiation devices, such as generators (including electric generators), radios, televisions, (especially CRT) monitors, or speakers.

Operation Safety

- If smoke, odour, or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service centre.
- Transportation and other unpredictable causes may damage the device hardware. Check whether the device has any intense damage before installation.
- If the device has major defects that you cannot solve, contact your dealer as soon as possible.
- Dust, moisture, and abrupt temperature changes can affect the device's service life. You are advised not to keep the device under such conditions.

- Do not keep the device in a place that vibrates. Handle the device with care. Do not place heavy objects on top of the device.
- Do not apply rosin, alcohol, benzene, pesticides, and other volatile substances that may damage the device enclosure. Clean the device accessories with a piece of soft cloth or a small amount of cleaning agent.
- If you have any technical questions regarding usage, contact certified or experienced technical personnel.

**Note:**

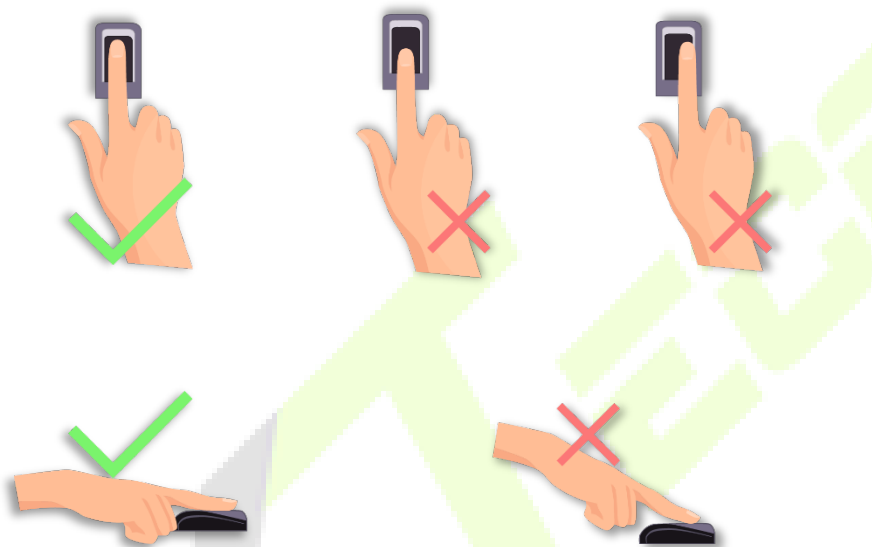
- Make sure whether the positive polarity and negative polarity of the DC 12V power supply is connected correctly. A reverse connection may damage the device. It is not advisable to connect the AC 24V power supply to the DC 12V input port.
- Make sure to connect the wires following the positive polarity and negative polarity shown on the device's nameplate.
- The warranty service does not cover accidental damage, damage caused by mis-operation, and damage due to independent installation or repair of the product by the user.

1 Instructions to use

1.1 Finger Positioning★

Recommended fingers: Index, middle, or ring finger. Avoid using the thumb or little finger, as they are difficult to press accurately on the fingerprint reader.

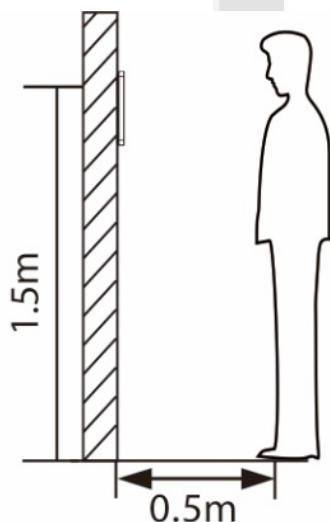
Press your finger on the fingerprint reader. Ensure that the center of your finger is aligned with the fingerprint reader.



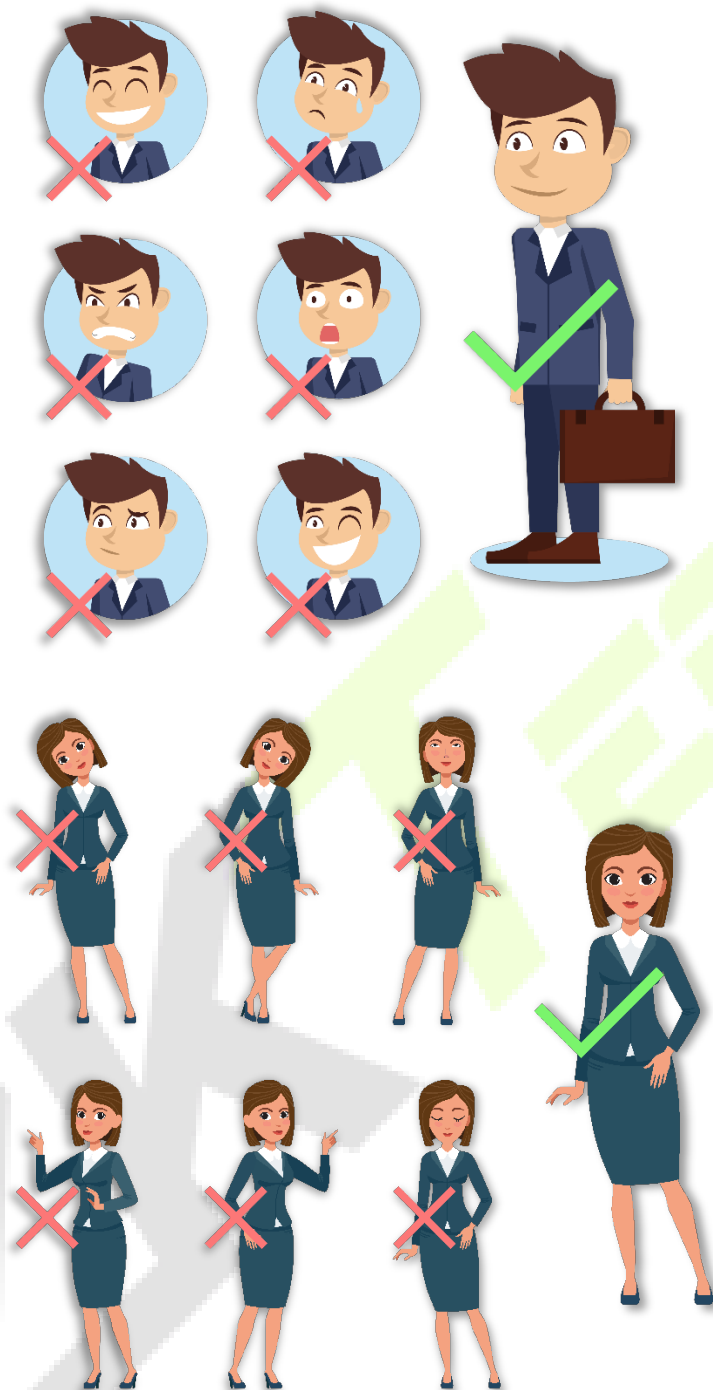
Note: Please use the correct method when pressing your fingers on the fingerprint reader for registration and identification. Our company will assume no liability for recognition issues that may result from incorrect usage of the product. We reserve the right of final interpretation and modification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

1.2 Standing Position, Posture and Facial Expression

Recommended Distance



The distance between the device and a user whose height is within 1.4m-1.8m is recommended to be 0.5m. Users may slightly move forwards and backwards to improve the quality of facial images captured.

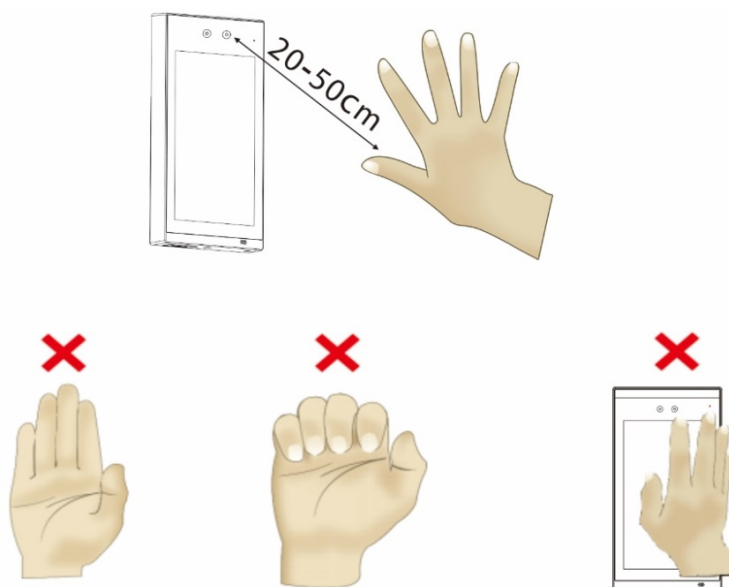
Facial Expression and Standing Posture

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

1.3 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.



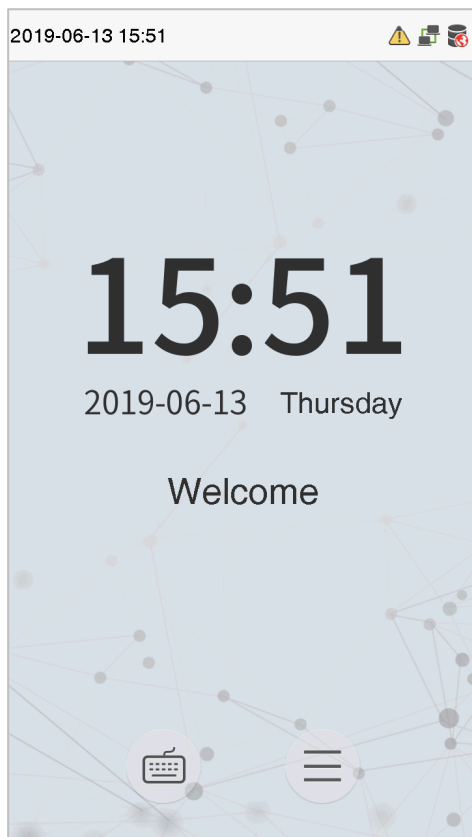
1.4 Face Registration

Keep the face in the center of the screen during registration. Please face the camera and stay still during face registration. The page looks like the following image:





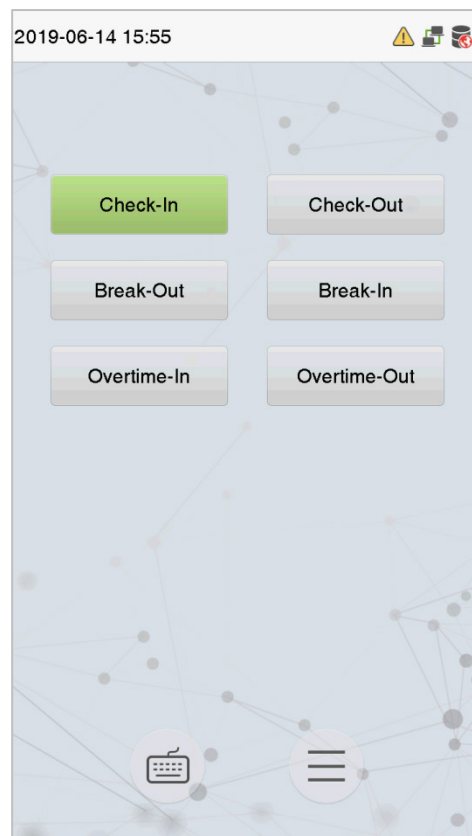
1.5 Standby Interface

After connecting the power supply, the standby interface will be displayed as shown below:



Note:

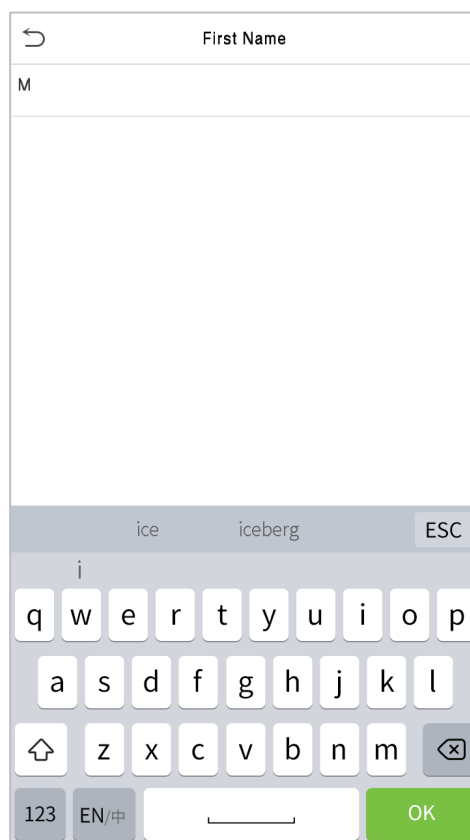
1. Click  to open the User verification interface.
2. When there is no super administrator set in the device, click  to enter the menu. After setting the super administrator, it requires the super administrator's verification before entering the menu operation. For the security of the device, it is recommended to register a super administrator for the first time you use the device.
3. ★The punch states can be switched directly by using the screen shortcut keys. Click anywhere on the screen without icons, and six shortcut keys appear, as shown in the figure below:



Press the corresponding shortcut key to select the current attendance state, which is shown in green. Please refer [7.5 Shortcut Key Mappings](#) for specific operations.

1.6 Virtual Keyboard

The virtual keyboard will be displayed as shown below:



Note: The device supports the input of English, numbers, and symbols. Click **En** to switch to the English keyboard. Press **123** to switch to the numeric and symbolic keyboard and click **ABC** to return to the alphabetic keyboard. Click the input box, the virtual keyboard appears. Click **ESC** to exit the input box.

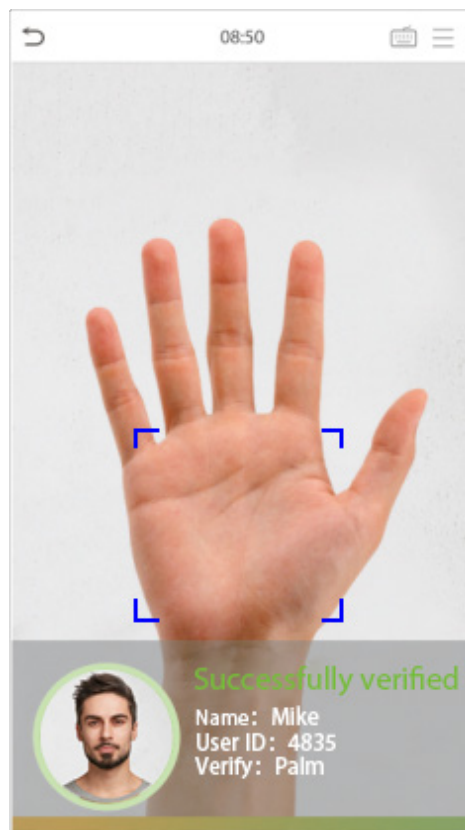
1.7 Verification Modes

1.7.1 Palm Verification

1: N Palm Verification Mode

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

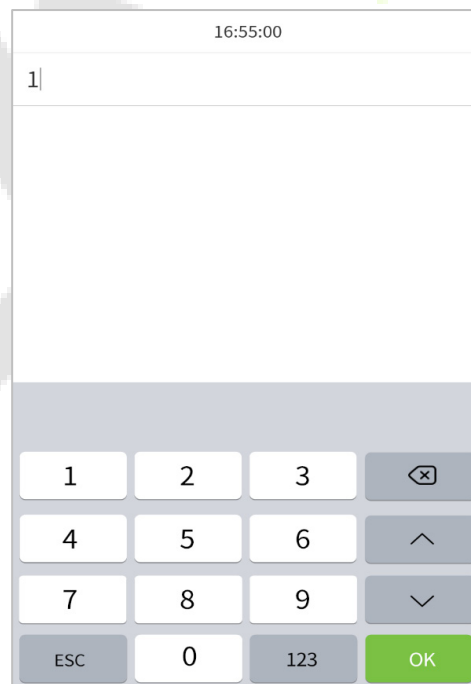
The device will automatically distinguish between the palm and the face verification mode. Place the palm in the palm collector area, and the device will automatically detect the palm verification mode.




1: 1 Palm Verification Mode

Click the  button on the main screen to open 1:1 palm verification mode.

Enter the user ID and press **OK**.



If the user has registered the fingerprint, face, card number and password in addition to his/her palm, and the verification method is set to palm/ fingerprint/ face/ badge/ password verification, the following screen will appear. Select the palm icon  to open the palm verification mode.

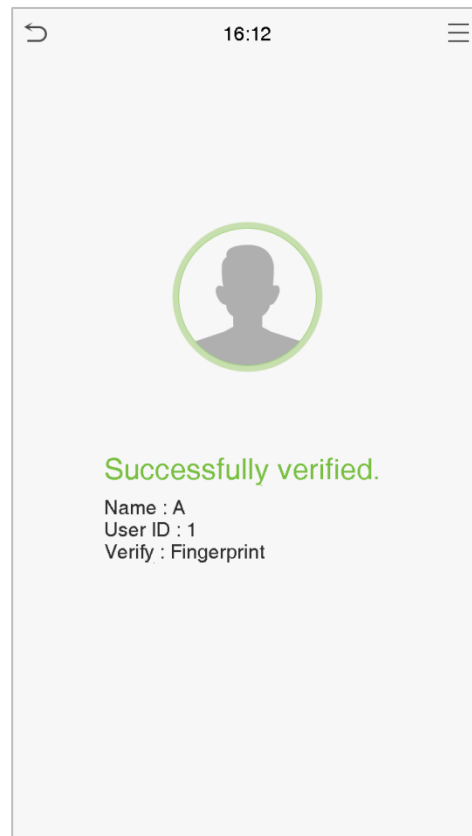
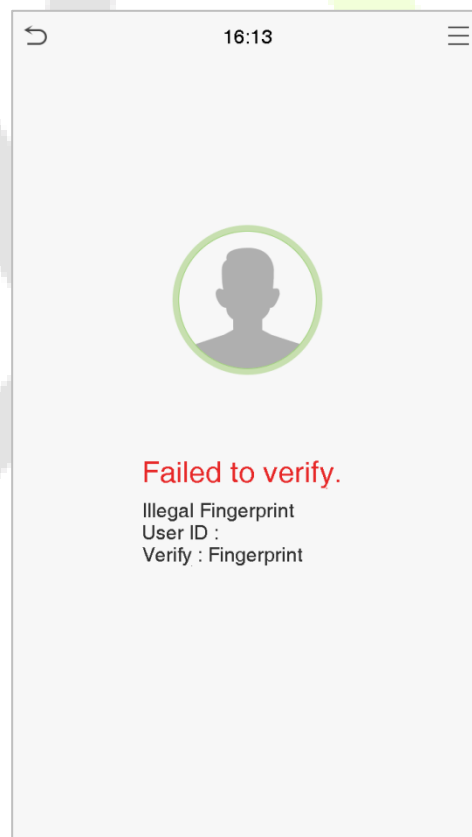


1.7.2 Fingerprint Verification★

1: N Fingerprint Verification Mode

The 1:N Fingerprint Verification mode compares the fingerprint that is being pressed on the fingerprint reader with all of the fingerprint data that is stored in the device.


The device will enter the fingerprint authentication mode when a user presses his/her finger onto the fingerprint scanner. Please follow the instructions to place your finger on the sensor. For details, please refer [1.1 Finger Positioning](#).

Successful Verification:**Failed Verification:**

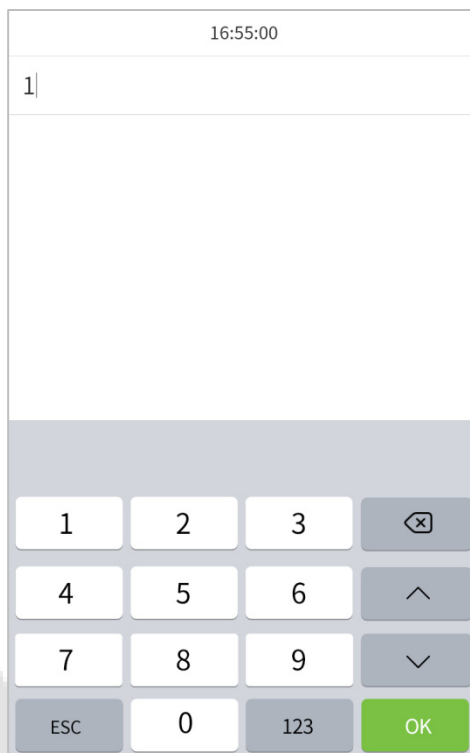
1: 1 Fingerprint Verification Mode


The 1:1 Fingerprint verification mode compares the fingerprint that is being pressed on the fingerprint reader with the fingerprints that are linked to User ID input via the virtual keyboard.

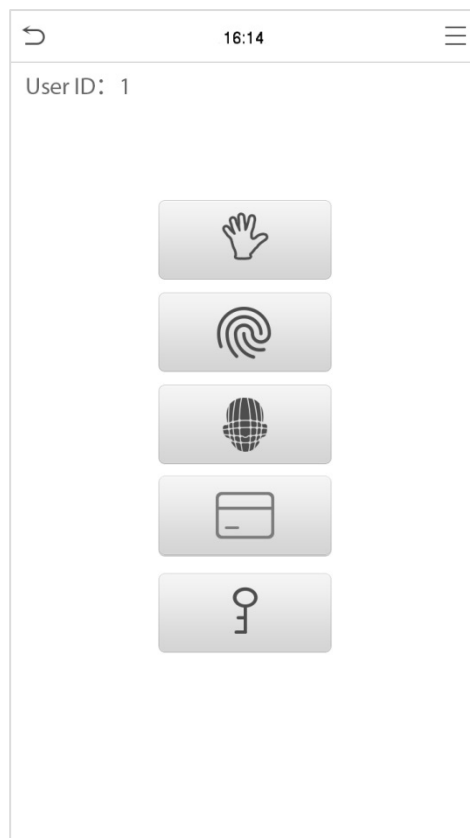
Users may try verifying their identities with 1:1 verification mode when they cannot gain access with 1: N authentication method.

Click the  button on the main screen to open the 1:1 fingerprint verification mode.

1. Enter the User ID and press **OK**.

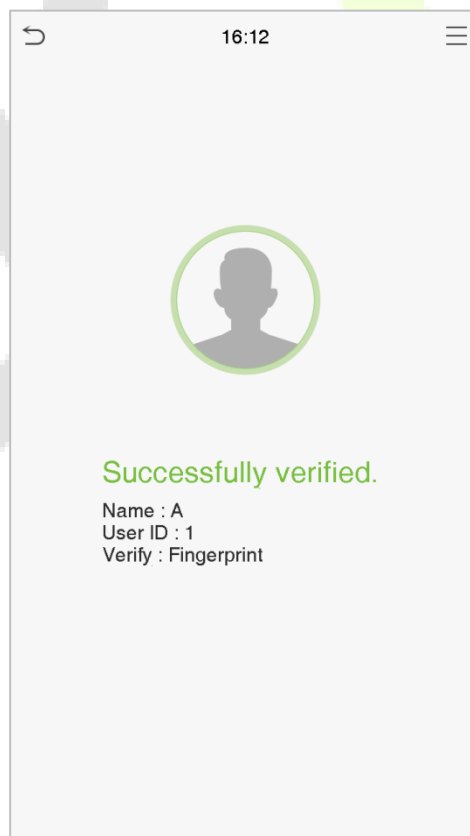


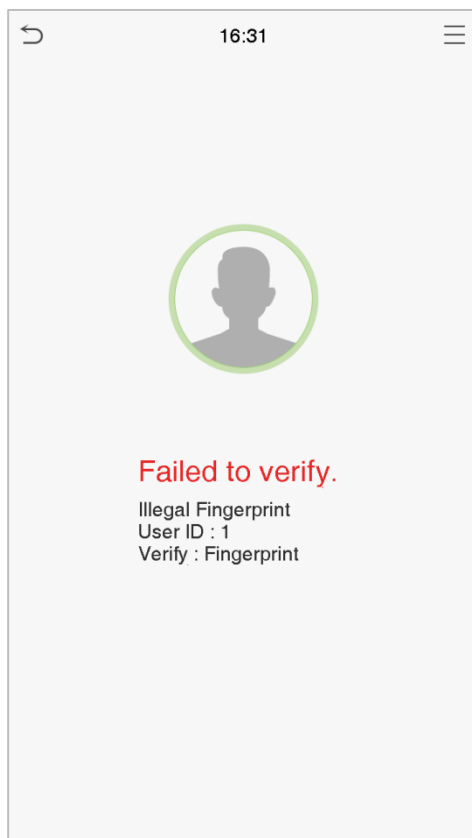
If the user has registered the palm, face, card number and password in addition to his/her fingerprint, and the verification method is set to palm/ fingerprint/ face/ badge/ password verification, the following screen will appear. Select the fingerprint icon  to enter fingerprint verification mode.



2. Press the fingerprint to verify.

Successful Verification:

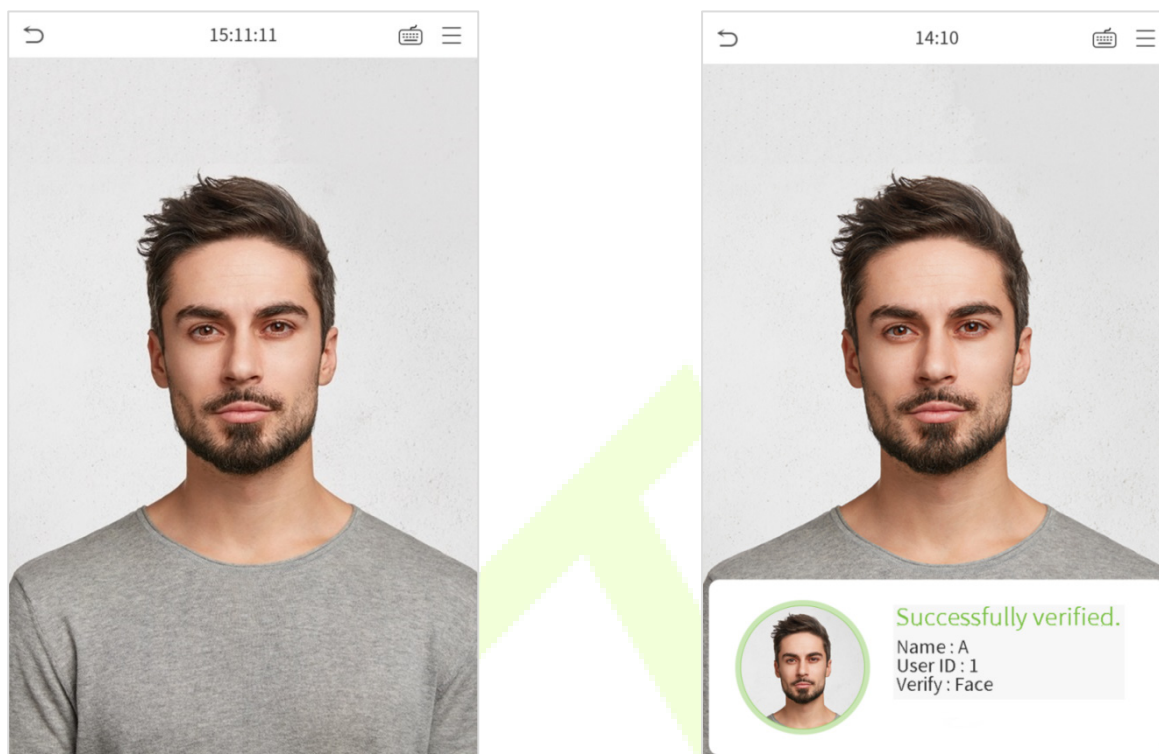


Failed Verification:

1.7.3 Facial Verification


1:N Facial Verification

The 1:N Facial Verification mode compares the acquired facial images with all face data registered in the device. The following is the pop-up prompt box of the comparison result.

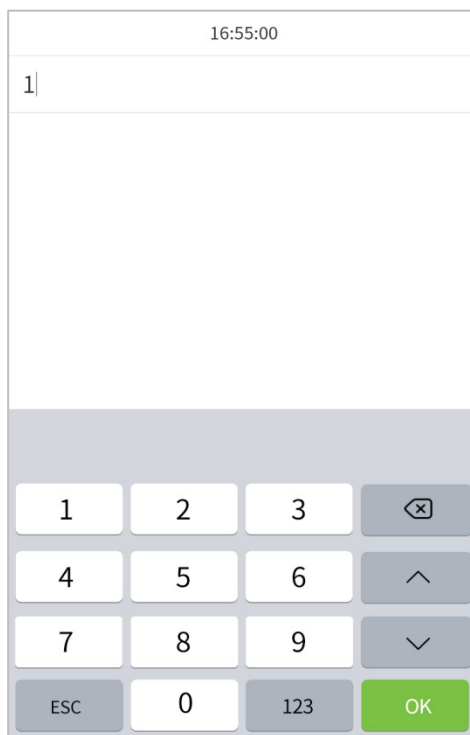



1:1 Facial Verification

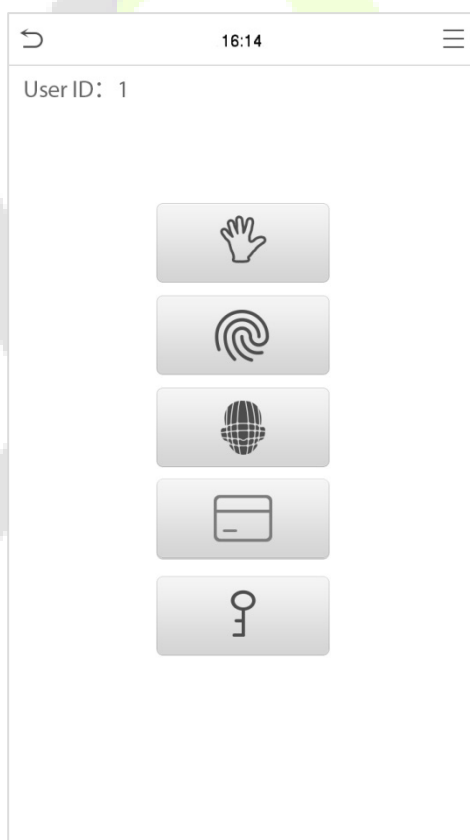
The 1:1 Facial Verification mode compares the face captured by the camera with the facial template related to the entered user ID.

Press  on the main interface to open the 1:1 facial verification mode.

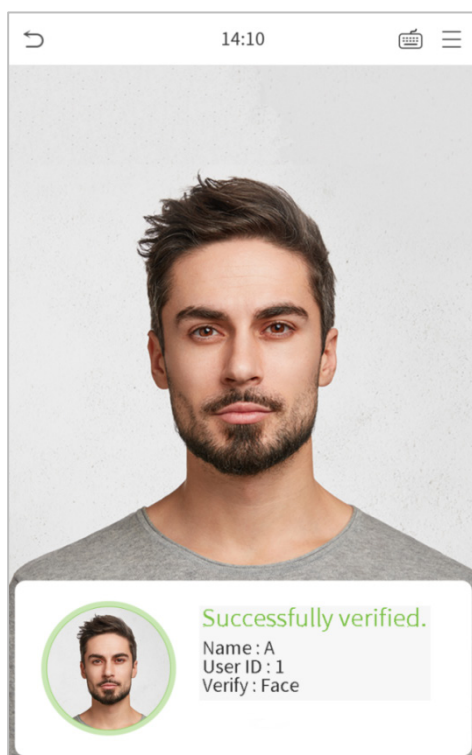
Enter the user ID and click **OK**.



If an employee registers palm, fingerprint, card number and password in addition to the face, the following screen will appear. Select the  icon to enter the face verification mode.



After successful verification, the prompt "**Successfully verified**" will appear.

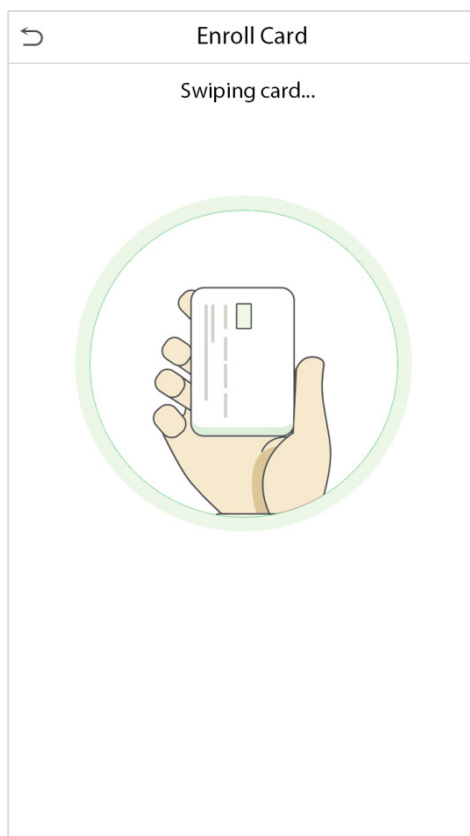


If the verification is failed, it will prompt **"Please adjust your position!"**

1.7.4 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 is the card verification screen.

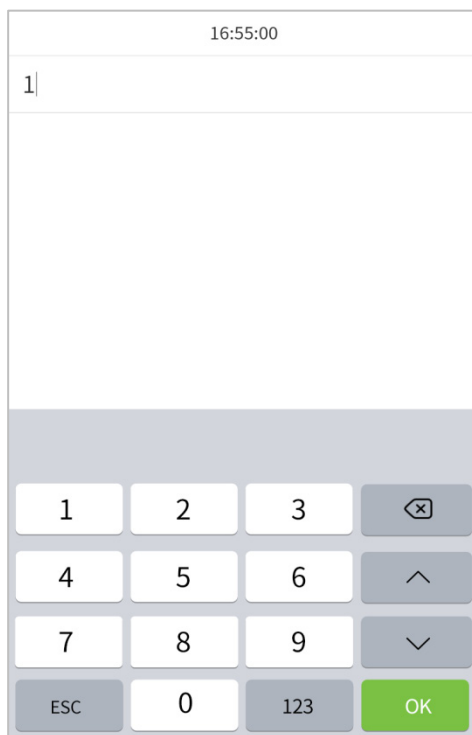



1:1 Card Verification

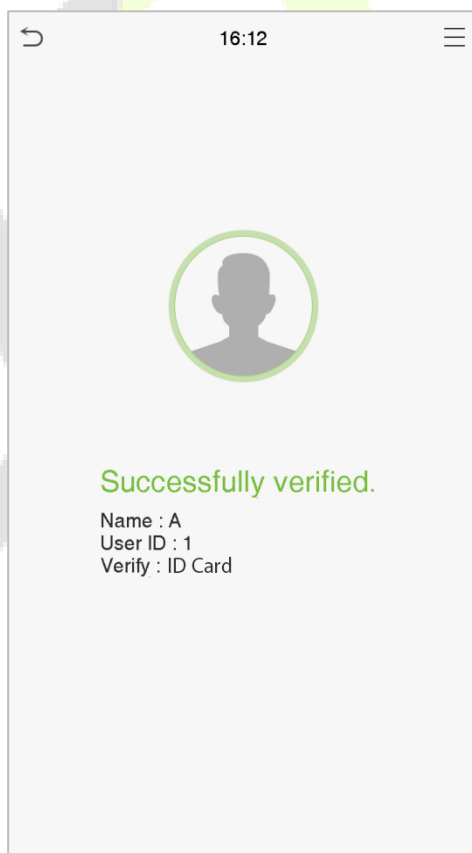
The 1:1 Card Verification mode compares the card number in the card induction area with the number associated with the employee's User ID registered in the device.

Press  on the main interface to open the 1:1 card verification mode.

Enter the user ID and click **OK**.




If an employee registers palm, fingerprint, face, and password in addition to the card, the following screen will appear. Select the  icon to open the card verification mode.

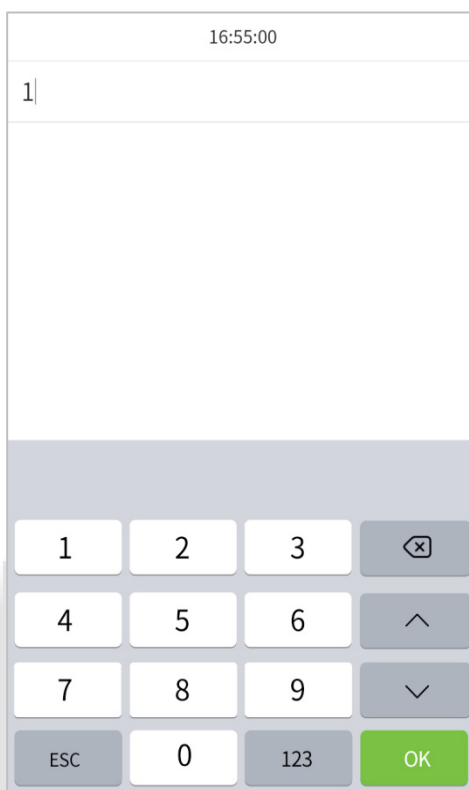



1.7.5 Password Verification

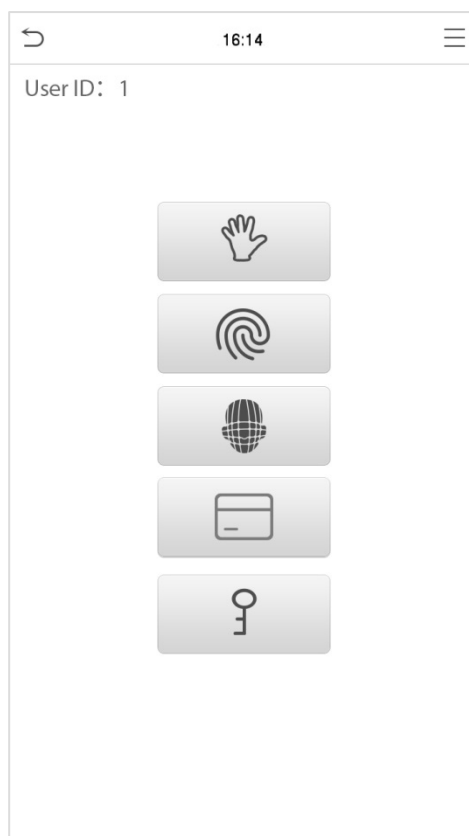
The Password Verification mode compares the entered password with the registered User ID and password.

Click the  button on the main screen to open the 1:1 password verification mode.

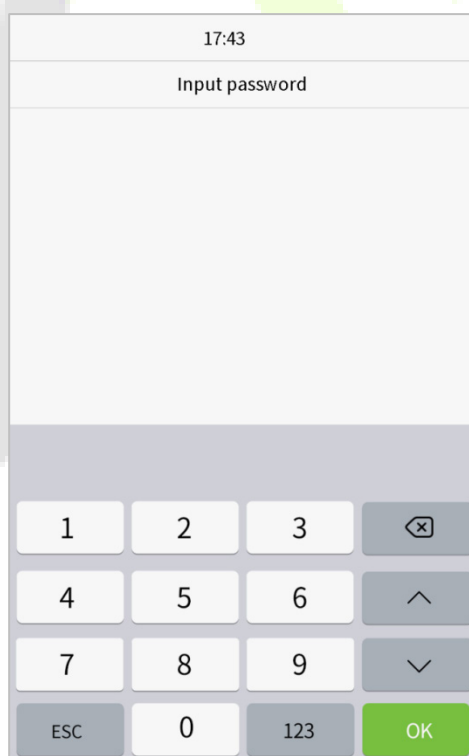
1. Enter the User ID and press **OK**.

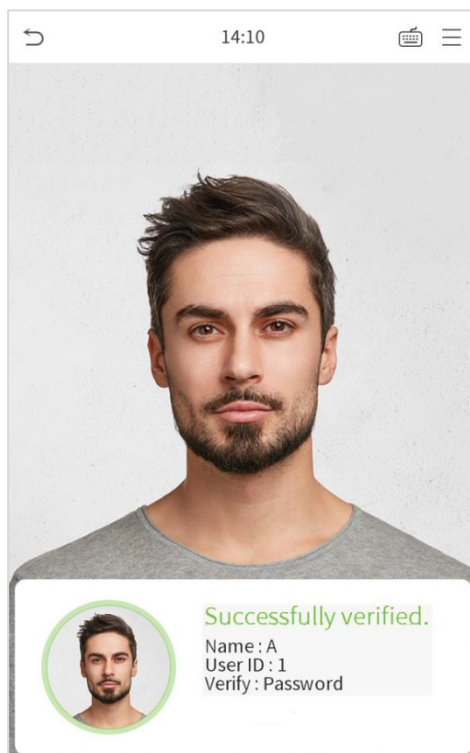
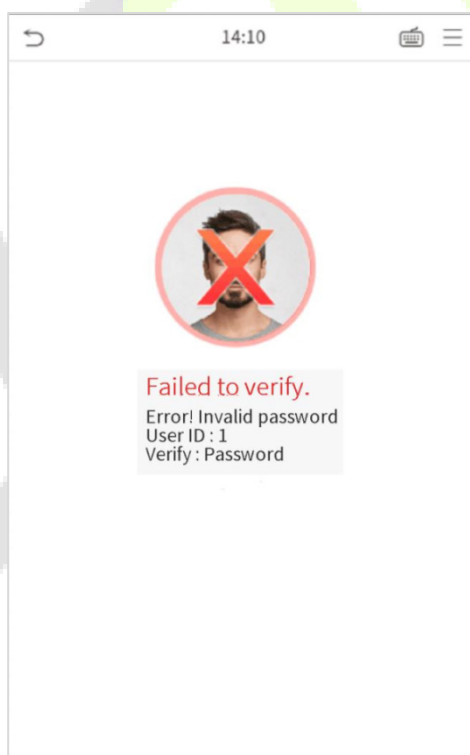


If an employee registers palm, fingerprint, face and card number in addition to the password, the following screen will appear. Select the  icon to open the password verification mode.



2. Enter the password and press **OK**.



Successful Verification:**Failed Verification:**

1.7.6 Combined Verification

To meet the needs of some access control occasions with high security and in consideration of the diversity of access control, the device provides a wide range of verification modes, which can be combined as required for individual users and user groups. The device supports 21 combinations of verification modes, as shown in the following figure.


| Verification Mode |
|--|
| <input checked="" type="radio"/> Apply Group Mode |
| <input type="radio"/> Palm/Fingerprint/Face/Badge/Password |
| <input type="radio"/> Fingerprint only |
| <input type="radio"/> User ID only |
| <input type="radio"/> Password |
| <input type="radio"/> Badge only |
| <input type="radio"/> Fingerprint/Password |
| <input type="radio"/> Fingerprint/Badge |
| <input type="radio"/> User ID+Fingerprint |
| <input type="radio"/> Fingerprint+Password |
| <input type="radio"/> Fingerprint+Badge |
| <input type="radio"/> Fingerprint+Password+Badge |

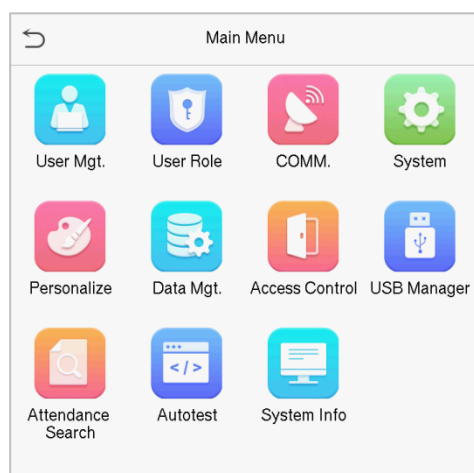
| Verification Mode |
|---|
| <input type="radio"/> Fingerprint+Badge |
| <input type="radio"/> Fingerprint+Password+Badge |
| <input type="radio"/> Password/Badge |
| <input type="radio"/> Fingerprint+(Badge/User ID) |
| <input type="radio"/> Face only |
| <input type="radio"/> Face+Fingerprint |
| <input type="radio"/> Face+Password |
| <input type="radio"/> Face+Badge |
| <input type="radio"/> Face+Fingerprint+Badge |
| <input type="radio"/> Face+Fingerprint+Password |
| <input type="radio"/> Palm |
| <input type="radio"/> Palm+Badge |

Note:

1. "/" means "or", and "+" means "and".
2. You must register the required verification information before using the combination verification mode, otherwise, the verification may fail. For example, if a user uses Face Registration but the verification mode is Face + Password, the user verification will be failed.

2 Main Menu

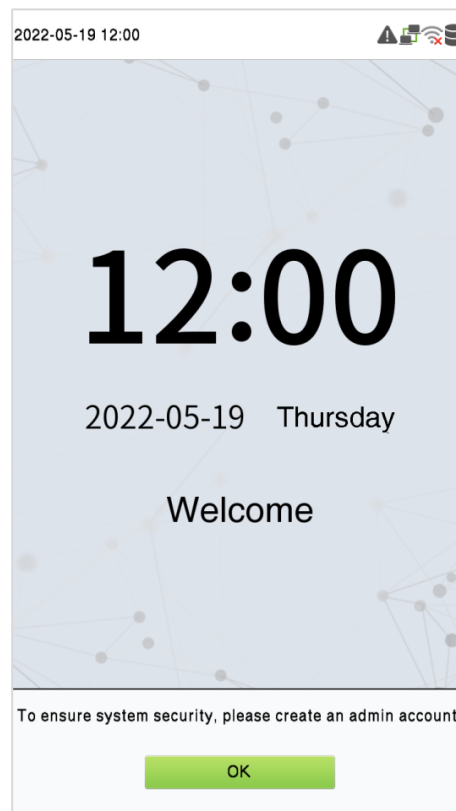
Press  on the Home Screen to open the main menu, as shown below:



| Feature | Description |
|--------------------------|---|
| User Mgt. | To add, edit, view, and delete basic information about a user. |
| User Role | To set the permission scope of the custom role and enroller, that is, the rights to operate the system. |
| COMM. | To set the relevant parameters of Network, PC connection, Cloud server, and Wiegand. |
| System | To set the parameters related to the system, including Date & Time, Access records, Palm, Face, Fingerprint parameters, reset to factory, USB upgrade and security. |
| Personalize | This includes user Interface, voice, bell, punch state options, and shortcut key mappings settings. |
| Data Mgt. | To delete all the relevant data in the device. |
| Access Control | To set the parameters of the lock and the relevant access control device. |
| USB Manager | To upload or download the specific data from a USB drive. |
| Attendance Search | Query the specified access record, check attendance photos and blacklist photos. |
| Autotest | To automatically test whether each module functions properly, including the LCD, voice, fingerprint sensor, camera, 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. Click **User Mgt.** to add an administrator or edit user permissions as a super administrator. 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.

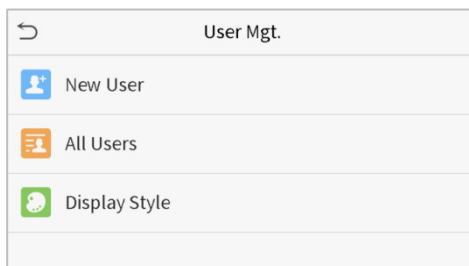


3 User Management

The User Management function enables to add and manage users in the device.

3.1 Adding Users

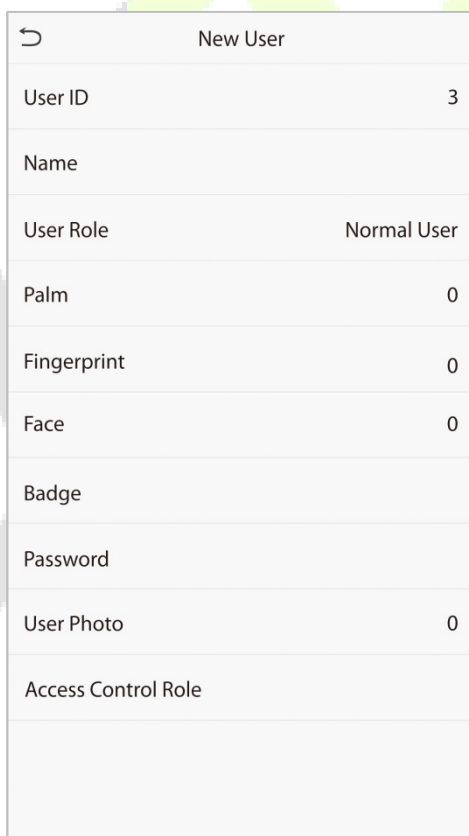
Click **User Mgt.** on the main menu.



Click **New User.**

Register a User ID and Name

Enter the User ID and Name.

A screenshot of a "New User" registration form. It has a back arrow icon in the top left corner. The form consists of several input fields with labels and values: "User ID" with the value "3", "Name" (empty), "User Role" with the value "Normal User", "Palm" with the value "0", "Fingerprint" with the value "0", "Face" with the value "0", "Badge" (empty), "Password" (empty), "User Photo" with the value "0", and "Access Control Role" (empty).

| | |
|---------------------|-------------|
| New User | |
| User ID | 3 |
| Name | |
| User Role | Normal User |
| Palm | 0 |
| Fingerprint | 0 |
| Face | 0 |
| Badge | |
| Password | |
| User Photo | 0 |
| Access Control Role | |

Note:

1. A Username may contain up to 17 characters.
2. The User ID may contain 1 to 9 digits by default.

3. During the initial registration, you can modify your ID, which cannot be modified after registration.
4. If a message "**Duplicated ID**" pops up, you must choose another ID.

Setting the User Role

There are two types of user accounts: the **Normal User** and the **Super Admin**. If there is already a registered administrator, the normal users have no rights to manage the system and may only access the authentication verifications. The Administrator owns all the management privileges. If a custom role is set, you can also select **User Defined Role** permissions for the user.

Click **User Role** to select Normal User or Super Admin.

A screenshot of a mobile application screen titled "User Role". It features a back arrow icon in the top left corner. Below the title, there are three radio button options: "Normal User" (which is selected with a green dot), "User Defined Role 1", and "Super Admin".

| User Role | |
|----------------------------------|---------------------|
| <input checked="" type="radio"/> | Normal User |
| <input type="radio"/> | User Defined Role 1 |
| <input type="radio"/> | Super Admin |

Note: If the selected user role is the Super Admin, the user must validate the identity authentication to access the main menu. The authentication is based on the authentication method(s) that the super administrator has registered. Please refer [1.7 Verification Method](#).

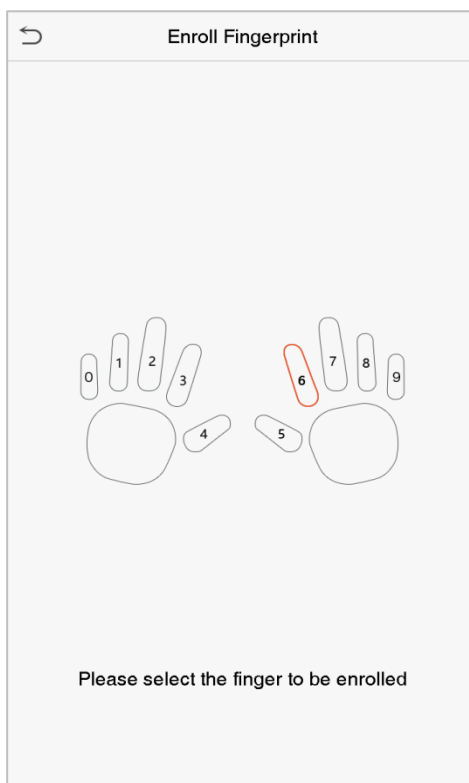
Register Palm

Click **Palm** to enter the palm registration page. Select the palm to be enrolled.

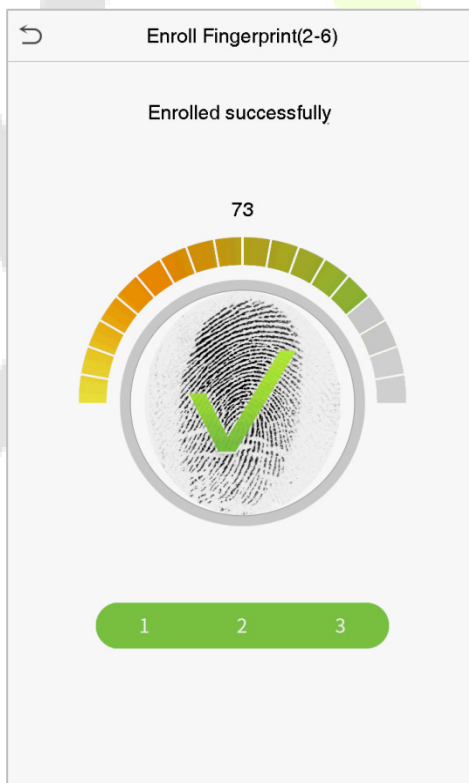


Register Fingerprint★

Click **Fingerprint** to enter the fingerprint registration page. Select the finger to be enrolled.



Press the same finger consecutively until the success message appears.



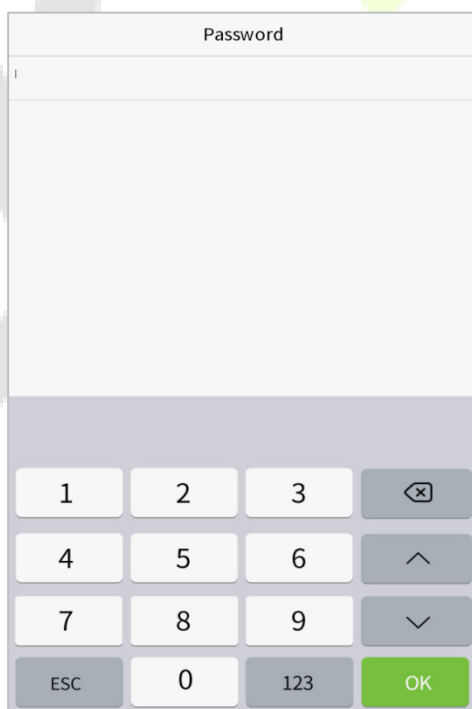
Register Face

Click **Face** to open the face registration page. Please face the camera and stay still during face registration. The registration interface is as follows:



Register Password

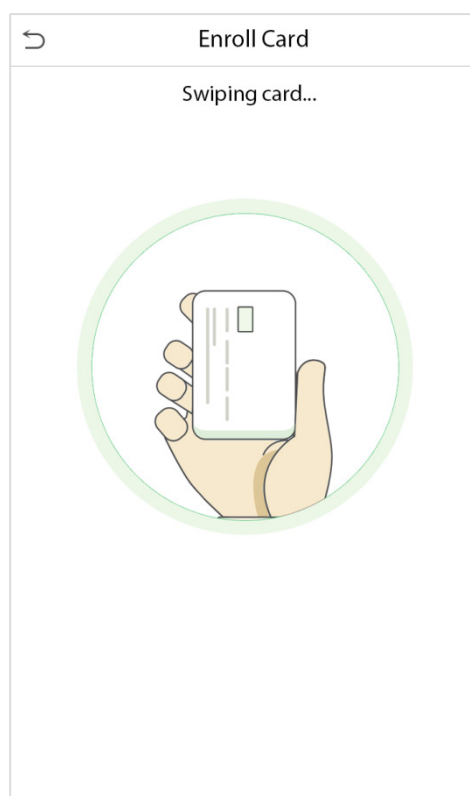
Click **Password** to open the password registration page. Enter a password and re-enter it. Click **OK**. If the two entered passwords are different, the prompt "**Password does not match**" will appear.



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

Register ID Card★

Press your **Badge** close underneath the fingerprint collector. The badge number registration will be successful.



Register User Photo

When a user's verification is successful, the registered photo will be displayed.

Click **User Photo**, click the camera icon to take a photo. The system will return to the New User interface after taking a photo.

Note: While registering a face, the system will automatically capture a picture as the user photo. If you do not want to register a user photo, the system will automatically set the picture captured as the default photo.

Access Control Role

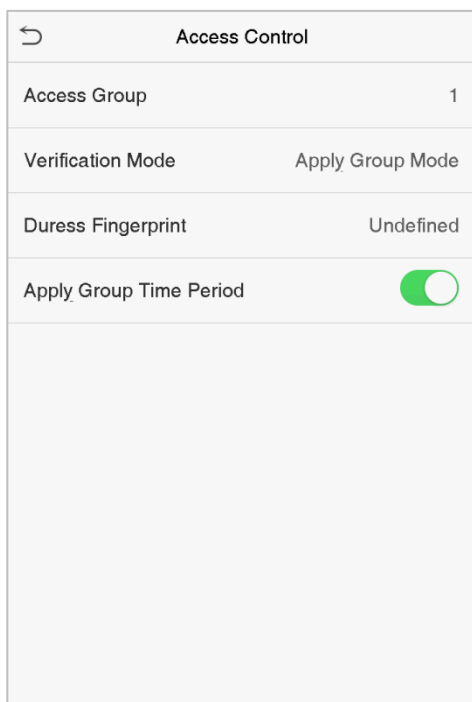
The user access control role sets the door unlocking rights of each person, including the group that the user belongs to, the verification mode, duress fingerprint and whether to apply the group time period.

Click **Access Control Role > Access Group**, assign the registered users to different groups for better management. The new users belong to Group 1 by default and can be reassigned to other groups. The device supports up to 99 access control groups.

Select verification mode for the user, click **Access Control Role > Verification Mode**.

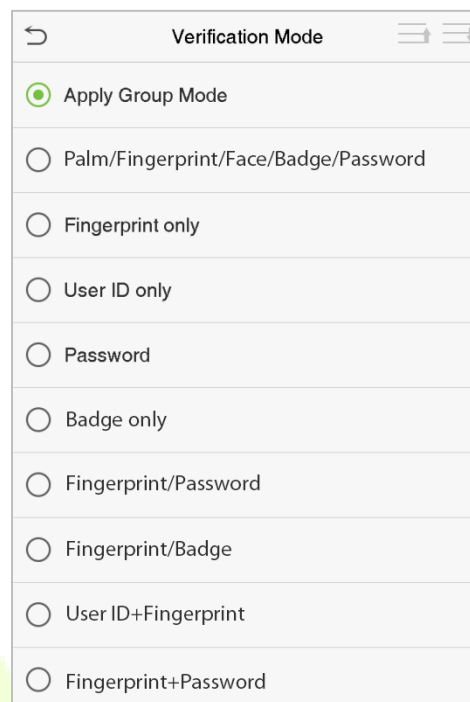
Duress Fingerprint: The user may specify one or more fingerprints that have been registered as a duress fingerprint(s). When press the finger corresponding to the duress fingerprint on the sensor and the verification is successful, the system will immediately generate a duress alarm.

Similarly, select whether to apply the group time period.



Access Control

| | |
|-------------------------|-------------------------------------|
| Access Group | 1 |
| Verification Mode | Apply Group Mode |
| Duress Fingerprint | Undefined |
| Apply Group Time Period | <input checked="" type="checkbox"/> |

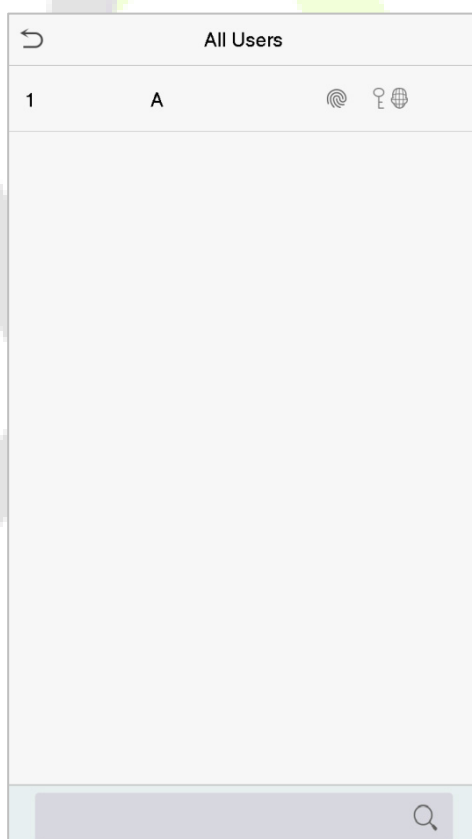


Verification Mode




- ☒ Apply Group Mode
- ☐ Palm/Fingerprint/Face/Badge/Password
- ☐ Fingerprint only
- ☐ User ID only
- ☐ Password
- ☐ Badge only
- ☐ Fingerprint/Password
- ☐ Fingerprint/Badge
- ☐ User ID+Fingerprint
- ☐ Fingerprint+Password

3.2 Search for Users

Click the search bar on the user list and enter the retrieval keyword (The keyword may be an ID, surname or full name.). The system will search for the users related to the information.



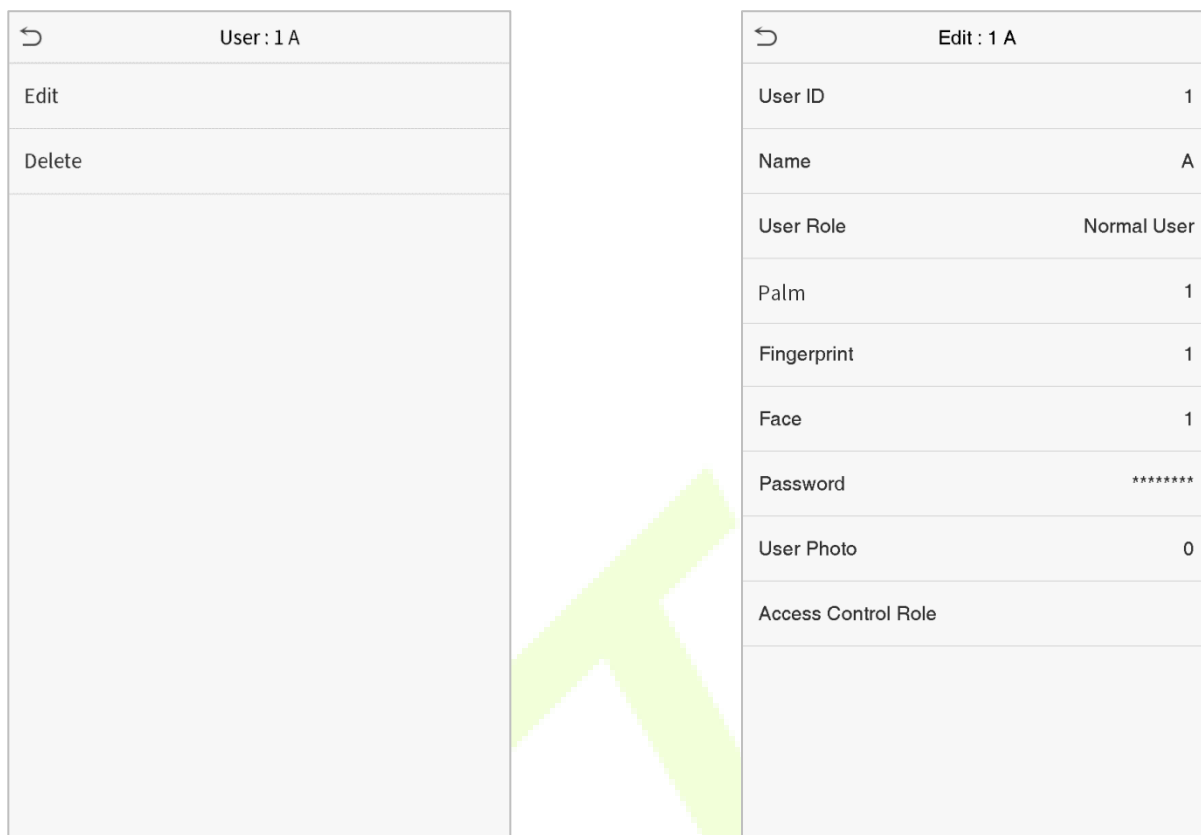
All Users

| | | |
|---|---|---|
| 1 | A |    |
|---|---|---|

Search bar at the bottom with a magnifying glass icon.

3.3 Edit Users

Choose a user from the list and click **Edit** to open the edit user interface:



| User : 1 A | |
|------------|--|
| Edit | |
| Delete | |
| | |

| Edit : 1 A | |
|---------------------|-------------|
| User ID | 1 |
| Name | A |
| User Role | Normal User |
| Palm | 1 |
| Fingerprint | 1 |
| Face | 1 |
| Password | ***** |
| User Photo | 0 |
| Access Control Role | |
| | |

Note: The operation of editing a user is the same as that of adding a user, except that the user ID cannot be modified when editing a user. Refer [3.1 Adding Users](#) for further operations.

3.4 Deleting Users

Select a user from the list and click **Delete** to enter the delete user interface. Select the user information to be deleted and click **OK**.

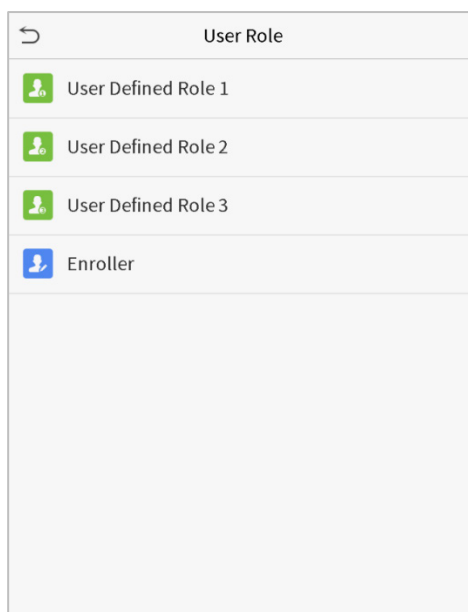
Note: If you select **Delete User**, all information of the user will be deleted.

4 User Role

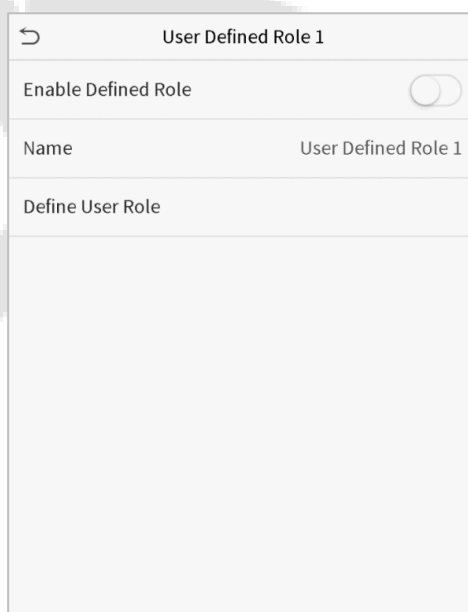
If you need to assign some specific permissions to certain users, you may edit the “User Defined Role” in the **User Role** menu.

You may set the permission scope of the custom role (up to 3 roles) and an enroller, that is, the permission scope of the operation menu.

Click **User Role** on the main menu interface.



1. Click any option to set a defined role. Click the row of **Enable Defined Role** to enable this defined role. Click **Name** and enter the name of the role.



2. Click **Define User Role** to assign privileges to the role. Once the privilege assignment is completed, click **Return**.

| User Defined Role 1 | |
|--|---|
| <input checked="" type="checkbox"/> User Mgt. | <input checked="" type="checkbox"/> New User |
| <input checked="" type="checkbox"/> Comm. | <input checked="" type="checkbox"/> All Users |
| <input checked="" type="checkbox"/> System | <input checked="" type="checkbox"/> Display Style |
| <input type="checkbox"/> Personalize | |
| <input type="checkbox"/> Data Mgt. | |
| <input checked="" type="checkbox"/> Access Control | |
| <input type="checkbox"/> USB Manager | |
| <input type="checkbox"/> Attendance Search | |
| <input type="checkbox"/> Autotest | |
| <input type="checkbox"/> System Info | |
| | |

Note: During the privilege assignment, the main menu is on the left and its sub-menus are on the right. You only need to select the features in sub-menus. If the device has a role enabled, you may assign the roles you set to users by clicking **User Mgt. > New User > User Role**.

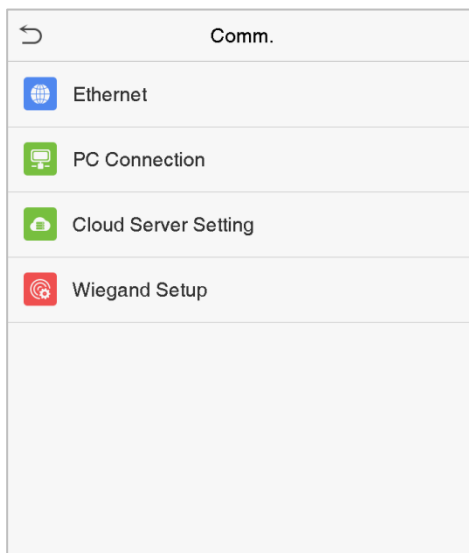
| User Role |
|--|
| <input checked="" type="radio"/> Normal User |
| <input type="radio"/> User Defined Role 1 |
| <input type="radio"/> Super Admin |

If no super administrator is registered, the device will prompt **"Please enroll super admin first!"** after clicking the enable bar.

5 Communication Settings

The Communication Settings set the parameters of the Network, PC connection, Cloud server, and Wiegand.

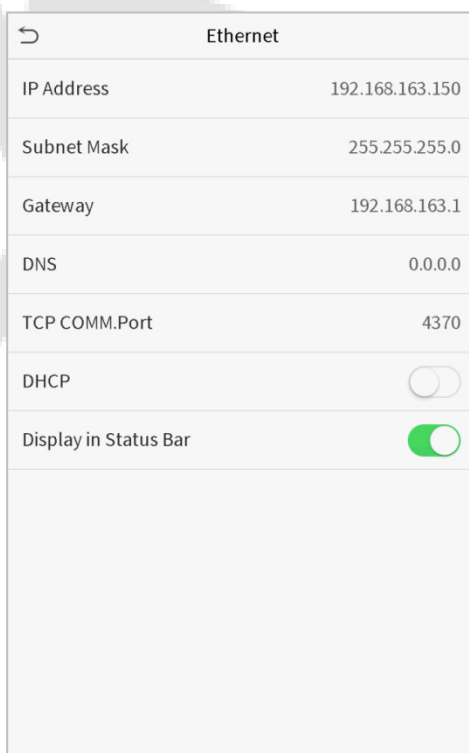
Tap **COMM.** on the main menu.



5.1 Network Settings

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

Click **Ethernet** on the Comm. Settings interface.



| Feature | Description |
|------------------------------|--|
| IP Address | The factory default value is 192.168.1.201. Please adjust them according to the actual network settings. |
| Subnet Mask | The factory default value is 255.255.255.0. Please adjust them according to the actual network settings. |
| Gateway | The factory default address is 0.0.0.0. Please adjust them according to the actual network settings. |
| DNS | The factory default address is 0.0.0.0. Please adjust them according to the actual network settings. |
| TCP COMM. Port | The factory default value is 4370. Please adjust them according to the actual network settings. |
| DHCP | Dynamic Host Configuration Protocol, which is to dynamically allocate the IP addresses for clients via server. |
| Display in Status Bar | To set whether to display the network icon on the status bar. |

5.2 PC Connection

To improve the security of data, set a Comm Key for communication between the device and the PC.

If a Comm Key is set, this connection password must be entered before the device can be connected to the PC software.

Click **PC Connection** on the Comm. Settings interface.

| PC Connection | |
|---------------|---|
| Comm Key | 0 |
| Device ID | 1 |

| Feature | Description |
|------------------|--|
| Comm Key | Comm Key: The default password is 0, which can be changed. The Comm Key may contain 1-6 digits. |
| Device ID | The identity number of the device, which ranges between 1 and 254. If the communication method is RS232/RS485, you need to enter this device ID in the software communication interface. |

5.3 Cloud Server Setting

This represents settings used for connecting the ADMS server.

Click **Cloud Server Setting** on the Comm. Settings interface.

| Cloud Server Setting | |
|----------------------|--------------------------|
| Server Mode | ADMS |
| Enable Domain Name | <input type="checkbox"/> |
| Server Address | 192.168.163.61 |
| Server Port | 8088 |
| Enable Proxy Server | <input type="checkbox"/> |
| HTTPS | <input type="checkbox"/> |

| Feature | | Description |
|----------------------------|-----------------------|---|
| Enable Domain Name | Server Address | When this function is enabled, the domain name mode "http://..." will be used, such as http://www.XYZ.com, while "XYZ" denotes the domain name when this mode is turned ON. |
| Disable Domain Name | Server Address | IP address of the ADMS server. |
| | Server Port | Port used by the ADMS server. |
| Enable Proxy Server | | When you choose to enable the proxy, you need to set the IP address and port number of the proxy server. |
| HTTPS | | <p>To increase the security of browser access, users can enable the HTTPS protocol to create a secure and encrypted network transmission and assure the security of sent data through identity authentication and encrypted communication.</p> <p>This function is enabled by default. This function can be enabled or disabled through the menu interface, and when changing the HTTPS status, the device will pop up a security prompt, and restart after confirmation.</p> |

5.4 Wiegand Setup

This feature sets the Wiegand input and output parameters.

Click **Wiegand Setup** on the Comm. Settings interface.

| Wiegand Setup | |
|----------------|--|
| Wiegand Input | |
| Wiegand Output | |
| | |

5.4.1 Wiegand Input

| Wiegand Options | |
|--------------------|--------------|
| Wiegand Format | |
| Wiegand Bits | 26 |
| Pulse Width(us) | 100 |
| Pulse Interval(us) | 1000 |
| ID Type | Badge Number |
| | |

| Feature | Description |
|---------------------------|---|
| Wiegand Format | Values range from 26 bits, 34 bits, 36 bits, 37 bits, and 50 bits. |
| Wiegand Bits | Number of bits of Wiegand data. |
| Pulse Width(us) | The value of the pulse width sent by the Wiegand data is 100 microseconds by default, which can be adjusted within the range of 20 to 100 microseconds. |
| Pulse Interval(us) | The default value is 1000 microseconds, which can be adjusted within the range of 200 to 20000 microseconds. |
| ID Type | Selects between the User ID and badge number. |

Definitions of various common Wiegand formats:

| Wiegand Format | Definition |
|----------------|---|
| Wiegand26 | ECCCCCCCCCCCCCCCCCCCCCCO Consists of 26 bits of binary code. The 1 st bit is the even parity bit of the 2 nd to 13 th bits, while the 26 th bit is the odd parity bit of the 14 th to 25 th bits. The 2 nd to 25 th bits are the card numbers. |
| Wiegand26a | ESSSSSSSCCCCCCCCCCCCCCO Consists of 26 bits of binary code. The 1 st bit is the even parity bit of the 2 nd to 13 th bits, while the 26 th bit is the odd parity bit of the 14 th to 25 th bits. The 2 nd to 9 th bits are the site codes, while the 10 th to 25 th bits are the card numbers. |
| Wiegand34 | ECCCCCCCCCCCCCCCCCCCCCCCCCCO Consists of 34 bits of binary code. The 1 st bit is the even parity bit of the 2 nd to 17 th bits, while the 34 th bit is the odd parity bit of the 18 th to 33 rd bits. The 2 nd to 25 th bits are the card numbers. |
| Wiegand34a | ESSSSSSSCCCCCCCCCCCCCCCCCCO Consists of 34 bits of binary code. The 1 st bit is the even parity bit of the 2 nd to 17 th bits, while the 34 th bit is the odd parity bit of the 18 th to 33 rd bits. The 2 nd to 9 th bits are the site codes, while the 10 th to 25 th bits are the card numbers. |
| Wiegand36 | OFFFFFFFFFFFFFFFCCCCCCCCCCCCCMME Consists of 36 bits of binary code. The 1 st bit is the odd parity bit of the 2 nd to 18 th bits, while the 36 th bit is the even parity bit of the 19 th to 35 th bits. The 2 nd to 17 th bits are the device codes. The 18 th to 33 rd bits are the card numbers, and the 34 th to 35 th bits are the manufacturer codes. |
| Wiegand36a | FFFFFFFFFFFFFFFCCCCCCCCCCCCCCO Consists of 36 bits of binary code. The 1 st bit is the even parity bit of the 2 nd to 18 th bits, while the 36 th bit is the odd parity bit of the 19 th to 35 th bits. The 2 nd to 19 th bits are the device codes, and the 20 th to 35 th bits are the card numbers. |
| Wiegand37 | OMMMMMSSSSSSSSSSSCCCCCCCCCCCCCCE Consists of 37 bits of binary code. The 1 st bit is the odd parity bit of the 2 nd to 18 th bits, while the 37 th bit is the even parity bit of the 19 th to 36 th bits. The 2 nd to 4 th bits are the manufacturer codes. The 5 th to 16 th bits are the site codes, and the 21 st to 36 th bits are the card numbers. |
| Wiegand37a | EMMMFFFFFFFFFSSSSSSCCCCCCCCCCCCCCO Consists of 37 bits of binary code. The 1 st bit is the even parity bit of the 2 nd to 18 th bits, while the 37 th bit is the odd parity bit of the 19 th to 36 th bits. The 2 nd to 4 th bits are the manufacturer codes. The 5 th to 14 th bits are the device codes, and 15 th to 20 th bits are the site codes, and the 21 st to 36 th bits are the card numbers. |
| Wiegand50 | ESSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCC Consists of 50 bits of binary code. The 1 st bit is the even parity bit of the 2 nd to 25 th bits, while the 50 th bit is the odd parity bit of the 26 th to 49 th bits. The 2 nd to 17 th bits are the site codes, and the 18 th to 49 th bits are the card numbers. |

"C "denotes the card number; "E" denotes the even parity bit; "O" denotes the odd parity bit;
 "F" denotes the facility code; "M" denotes the manufacturer code; "P" denotes the parity bit; and "S"
 denotes the site code.

5.4.2 Wiegand Output

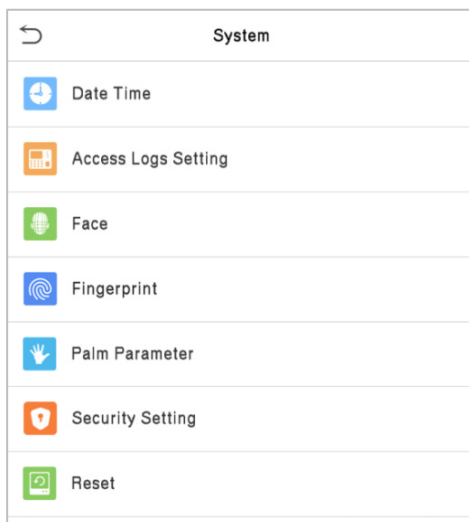
| Wiegand Options | |
|---------------------|--------------|
| Wiegand Format | |
| wiegand output bits | 26 |
| Failed ID | 0 |
| Site Code | 0 |
| Pulse Width(us) | 100 |
| Pulse interval(us) | 1000 |
| ID Type | Badge Number |

| Feature | Description |
|----------------------------|--|
| Wiegand Format | Values range from 26 bits, 34 bits, 36 bits, 37 bits, and 50 bits. |
| Wiegand output bits | After choosing the Wiegand format, you can select one of the corresponding output digits in the Wiegand format |
| Failed ID | If the verification is failed, the system will send the failed ID to the device and replace the card number or Personnel ID with the new ones. |
| Site Code | It is similar to the device ID. The difference is that a site code can be set manually and is repeatable in a different device. The valid value ranges from 0 to 256 by default. |
| Pulse Width(us) | The time width represents the changes in the quantity of electric charge with high-frequency capacitance regularly within a specified time. |
| Pulse Interval(us) | The time interval between the pulses. |
| ID Type | Selects between the User ID and Badge number. |

6 System Settings

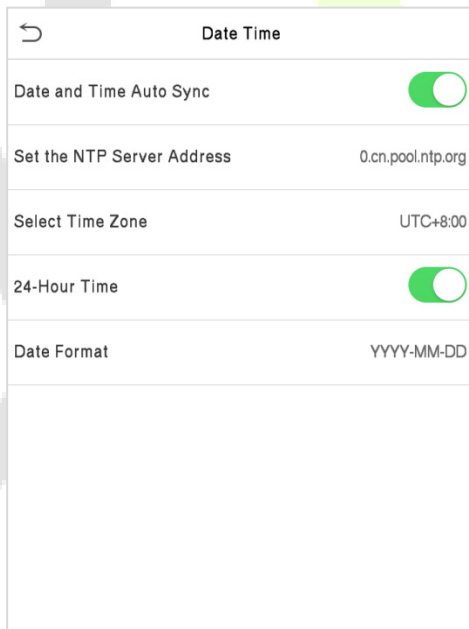
The System settings set the related system parameters to optimize the performance of the device.

Click **System** on the main menu interface.



6.1 Date and Time

Click **Date Time** on the System interface.



1. The product supports the NTP synchronization time mechanism by default. Tap **Date and Time Auto Sync** to enable, and set the corresponding NTP server address link to take effect.
2. If users need to set date and time manually, disable **Date and Time Auto Sync** first, and then tap **Manual Time Setting** to set date and time and tap Confirm to save.

| Date Time | |
|-------------------------|-------------------------------------|
| Date and Time Auto Sync | <input type="checkbox"/> |
| Manual Date and Time | |
| Select Time Zone | UTC+8:00 |
| 24-Hour Time | <input checked="" type="checkbox"/> |
| Date Format | YYYY-MM-DD |

- Click 24-Hour Time to enable or disable this format and select the date format.
- Click Daylight Saving Time to enable or disable the function. If enabled, select a daylight-saving mode and set the switch time.

| Daylight Saving Setup | |
|-----------------------|--------|
| Start Month | 1 |
| Start Week | 1 |
| Start Day | Sunday |
| Start Time | 00:00 |
| End Month | 1 |
| End Week | 1 |
| End Day | Sunday |
| End Time | 00:00 |

Week mode

| Daylight Saving Setup | |
|-----------------------|-------|
| Start Date | 00-00 |
| Start Time | 00:00 |
| End Date | 00-00 |
| End Time | 00:00 |

Date mode

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, 2019) to 18:30 on January 1, 2020. After restoring the factory settings, the time of the equipment will remain 18:30 on January 1, 2020.

6.2 Access Logs Setting

Click **Access Logs Setting** on the System interface.

| Attendance | |
|-------------------------------|-------------------------------------|
| Duplicate Punch Period(m) | None |
| Camera Mode | No photo |
| Display User Photo | <input checked="" type="checkbox"/> |
| Alphanumeric User ID | <input type="checkbox"/> |
| Attendance Log Alert | 99 |
| Cyclic Delete ATT Data | Disabled |
| Cyclic Delete ATT Photo | 99 |
| Cyclic Delete Blacklist Photo | 99 |
| Confirm Screen Delay(s) | 3 |
| Face detect interval(s) | 1 |

| Feature | Description |
|--|---|
| Duplicate Punch Period (m) | Within this time range, the attendance record of the same person will not be saved for more than once; the valid time range is 1 to 999999 minutes. |
| Camera Mode | <p>This function is disabled by default. When enabled, a security prompt will pop-up and the sound of shutter in the camera will turn on mandatorily. There are 5 modes:</p> <p>No Photo: No photo will be taken during user verification.</p> <p>Take photo, no save: Photo will be taken but will be not saved during verification.</p> <p>Take photo and save: Photo will be taken and saved during verification.</p> <p>Save on successful verification: Photo will be taken and saved for each successful verification.</p> <p>Save on failed verification: Photo will be taken and saved for each failed verification.</p> |
| Display User Photo | This function is disabled by default. When enabled, there will be a security prompt. |
| Alphanumeric User ID | Decides whether to support letters in a User ID. |
| Attendance Log Alert/ Access Logs Warning | When the remaining memory space reaches a predefined value, the device will automatically display a record memory warning. Users may disable the function or set a valid value between 1 and 9999. |

| | |
|--|--|
| Cyclic Delete ATT Data/Access Records | When the attendance/access records have reached the full capacity, the device will automatically delete a set value of old attendance/access records. Users may disable the function or set a valid value between 1 and 999. |
| Cyclic Delete ATT Photo | When the attendance photos have reached the full capacity, the device will automatically delete a set value of old attendance photos. Users may disable the function or set a valid value between 1 and 99. |
| Cyclic Delete Blacklist Photo | When the blacklisted photos have reached full capacity, the device will automatically delete a set value of old blacklisted photos. Users may disable the function or set a valid value between 1 and 99. |
| Confirm Screen Delay(s) | The time length to display the message of successful verification. The valid range is 1 to 9 seconds. |
| Face Detect Interval (s) | To set the facial template matching time interval as needed. The valid value range is 0 to 9 seconds. |

6.3 Face Parameters

Click **Face** on the System interface.

| | |
|---------------------------------------|-------------------------------------|
| Face | 1↓ |
| 1:N Threshold Value | 74 |
| 1:N Match Threshold for Masked People | 68 |
| 1:1 Threshold Value | 63 |
| Face Enrollment Threshold | 70 |
| Face Pitch Angle | 35 |
| Face Rotation Angle | 25 |
| Image Quality | 40 |
| LED Light Trigger Value | 80 |
| Motion Detection Sensitivity | 4 |
| Live Detection | <input checked="" type="checkbox"/> |
| Live Detection Threshold | 50 |
| Save Photo as Template | <input checked="" type="checkbox"/> |

| FRR | FAR | Recommended matching thresholds | |
|---------------|--------|---------------------------------|-----|
| | | 1:N | 1:1 |
| High | Low | 85 | 80 |
| Medium | Medium | 82 | 75 |
| Low | High | 80 | 70 |

| Feature | Description |
|----------------------------|---|
| 1:N Match Threshold | Under 1:N verification mode, the verification will only be successful when the similarity between the acquired facial image and all registered facial templates is greater than the set value. The valid value ranges from 65 to 120. The higher the thresholds, the lower the misjudgment rate, the higher the rejection rate, and vice versa. The value 75 is recommended. |

| | |
|--------------------------------------|---|
| 1:1 Match Threshold | Under 1:1 verification mode, the verification will only be successful when the similarity between the acquired facial image and the facial templates enrolled in the device is greater than the set value. The valid value ranges from 55 to 120. The higher the thresholds, the lower the misjudgment rate, the higher the rejection rate, and vice versa. The value 63 is recommended. |
| Face Enrollment Threshold | During face 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 has already been registered. |
| Face Pitch Angle | The pitch angle is the tolerance of a face for facial registration and comparison. If a face's pitch angle exceeds this set value, it will be filtered by the algorithm, i.e. ignored by the terminal thus no registration and comparison interface will be triggered. |
| Face Rotation Angle | The rotation angle is the tolerance of a face for facial template registration and comparison. If a face's rotation angle exceeds this set value, it will be filtered by the algorithm, i.e. ignored by the terminal thus no registration and comparison interface will be triggered. |
| Image Quality | It defines the Image quality for facial registration and comparison. The higher the value, the clearer the image. |
| LED Light Triggered Threshold | This value controls the on and off states of the LED light. The larger the value, the more frequently the LED light will be turned on. |
| Motion Detection Sensitivity | A measurement of the amount of change in a camera's field of view that qualifies as potential motion detection that wakes up the terminal from standby to the comparison interface. The larger the value, the more sensitive the system would be, i.e. if a larger value is set, the comparison interface can be easily and frequently triggered. |
| Live Detection | Detecting a spoof attempt by determining whether the source of a biometric sample is a live human being or a fake representation using visible light images. |
| Live Detection Threshold | Helping to judge whether the visible image comes from an alive body. The larger the value, the better the visible light anti-spoofing performance. |
| Save Photo as Template | This function is enabled by default, and the menu interface supports enabling or disabling this function, and there is a security prompt when switching. When this function is disabled, it will indicate that there is a risk reminder: "Face re-registration is required after an algorithm upgrade." |
| Notes | 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 technician of our company. |

6.4 Palm Parameters

Click **Palm** on the System interface.

| Palm Parameter | |
|-----------------------------|-----|
| Palm 1:1 Matching Threshold | 576 |
| Palm 1:N Matching Threshold | 576 |
| | |

| Feature | Description |
|------------------------------------|--|
| Palm 1:1 Matching 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 will be successful. |
| Palm 1:N Matching 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 will be successful. |

6.5 Fingerprint Parameters★

Click **Fingerprint** on the System interface.

| Fingerprint | |
|-----------------------|-------------|
| 1:1 Match Threshold | 15 |
| 1:N Match Threshold | 35 |
| FP Sensor Sensitivity | Low |
| 1:1 Retry Times | 3 |
| Fingerprint Image | Always show |
| | |

| FRR | FAR | Recommended matching thresholds | |
|--------|--------|---------------------------------|-----|
| | | 1:N | 1:1 |
| High | Low | 45 | 25 |
| Medium | Medium | 35 | 15 |
| Low | High | 25 | 10 |

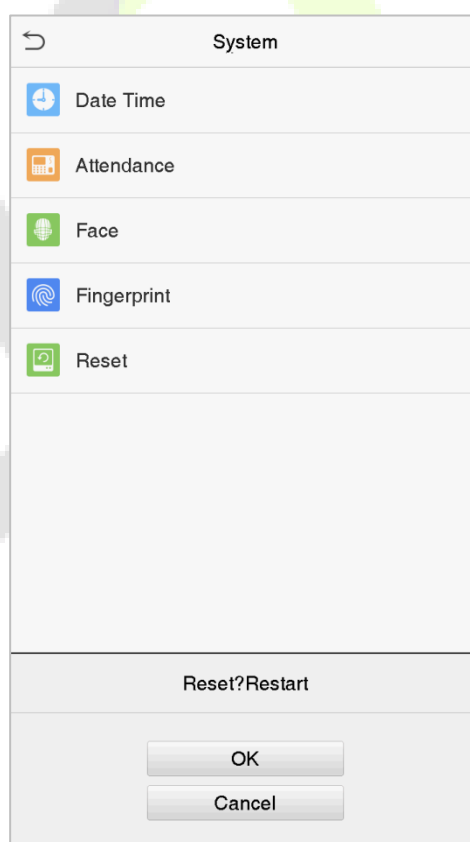
| Feature | Descriptions |
|----------------------------|--|
| 1:1 Match Threshold | Under the 1:1 verification method, the verification will only be successful when the similarity between the acquired fingerprint data and the fingerprint template associated with the entered user ID enrolled in the device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

| | |
|------------------------------|--|
| FP Sensor Sensitivity | Sets the sensibility of fingerprint acquisition. It is recommended to use the default level "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 Times | 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 | <p>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 options are available:</p> <p>Show for enroll: Displays the fingerprint image on the screen only during enrollment.</p> <p>Show for match: Displays the fingerprint image on the screen only during verification.</p> <p>Always show: Displays the fingerprint image on the screen during enrollment and verification.</p> <p>None: The fingerprint image will not be displayed.</p> |

6.6 Factory Reset

This feature restores the device parameters, such as communication settings and system settings, to factory settings (will not clear registered user data).

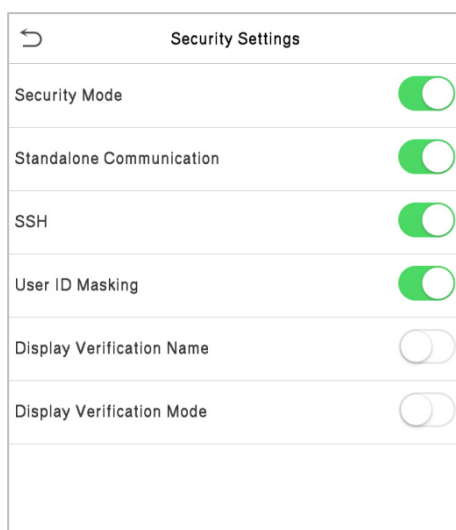
Click **Reset** on the System interface.



Click **OK** to reset.

6.7 Security Settings

Tap **Security Settings** on the **System** interface.



| Function Name | Description |
|----------------------------------|--|
| Security Mode | <p>When enabled, user information verification has a high level of security. This function can be enabled or disabled via the menu interface. When switching on and off, there are security prompts. All data will be deleted and the device will be restarted after confirmation.</p> <p>Note: After turning on the security mode, the product will forcibly enable the function of returning to the standby interface when the menu times out by default (default 60s). It does not support disabling in security mode, but it does support disabling in non-security mode. To configure, go to Personalize > User Interface > Menu Screen Timeout(s).</p> |
| 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. |
| 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. |
| Display Verification Mode | After enabled, the personnel verification result will show the user's verification mode. The verification result will not show the verification mode after you disable it. |

6.8 USB Upgrade

Click **USB Upgrade** on the System interface.

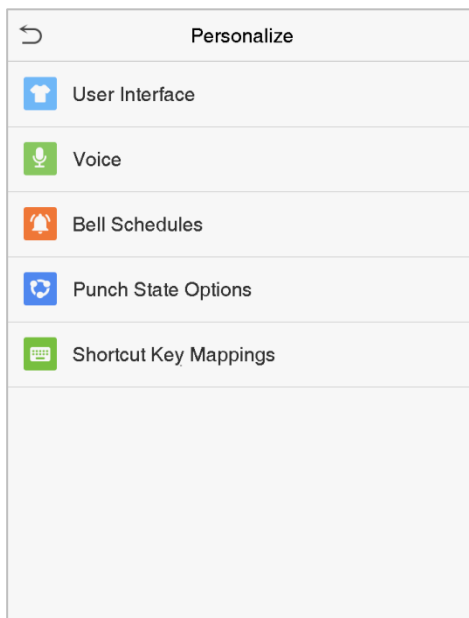
The device's firmware program can be upgraded with the upgrade file in a USB drive. Before conducting this operation, please ensure that the USB drive contains the correct upgrade file and is properly inserted into the device.



7 Personalize Settings

You may customize the interface settings such as voice, bell, punch state options, and shortcut key mappings.

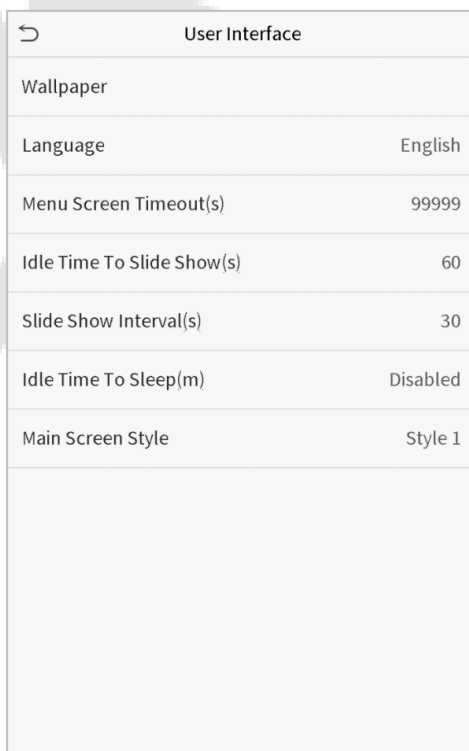
Click **Personalize** on the main menu interface.



7.1 Interface Settings

You can customize the display style of the main interface.

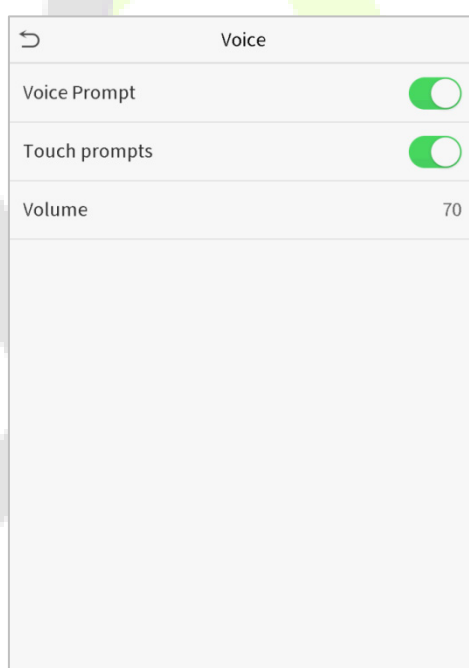
Click **User Interface** on the Personalize interface.



| Feature | Description |
|------------------------------------|---|
| Wallpaper | Selects the main screen wallpaper according to your personal preference. |
| Language | Selects the language of the device. |
| Menu Screen Timeout (s) | When there is no operation, and the time exceeds the pre-set value, the device will automatically go back to the initial interface. You can disable the function or set the value between 60 and 99999 seconds. |
| Idle Time To Slide Show (s) | When there is no operation, and the time exceeds the pre-set value, a slide show will be played. It can be disabled, or you may set the value between 3 and 999 seconds. |
| Slide Show Interval (s) | This refers to the time interval to switch between different slide show images. The function can be disabled, or you may set the time interval between 3 and 999 seconds. |
| Idle Time to Sleep (m) | If you have activated the sleep mode, when there is no operation, the device will enter the standby mode. Press any key or finger to resume normal working mode. You can disable this function or set a value within 1-999 minutes. |
| Main Screen Style | Selects the main screen style according to your personal preference. |

7.2 Voice Settings

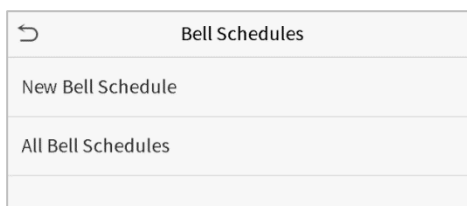
Click **Voice** on the Personalize interface.



| Feature | Description |
|---------------------|---|
| Voice Prompt | Selects whether to enable voice prompts during operating. |
| Touch Prompt | Selects whether to enable keypad sounds. |
| Volume | Adjusts the volume of the device. The valid range is 0-100. |

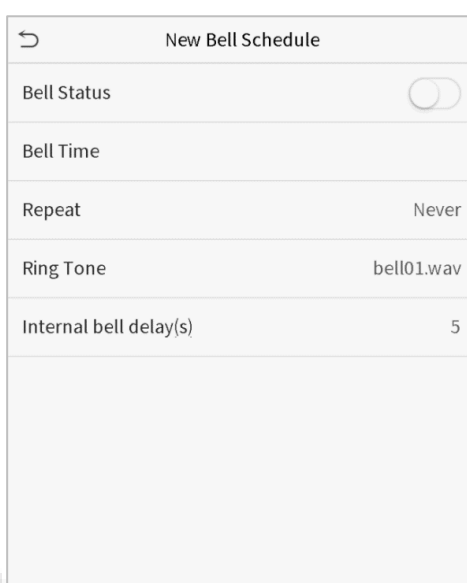
7.3 Bell Schedules

Click **Bell Schedules** on the Personalize interface.



Add a Bell

1. Click **New Bell Schedule** to open the add interface.



| Feature | Description |
|-------------------------------|---|
| Bell Status | Sets whether to enable the bell status. |
| Bell Time | At this time of day, the device automatically rings the bell. |
| Repeat | Sets the repetition cycle of the bell. |
| Ring Tone | Selects a ring tone. |
| Internal bell delay(s) | Sets the duration of the internal bell. The valid value ranges from 1 to 999 seconds. |

2. Click **All Bell Schedules** to view the newly added bell.

Edit a Bell

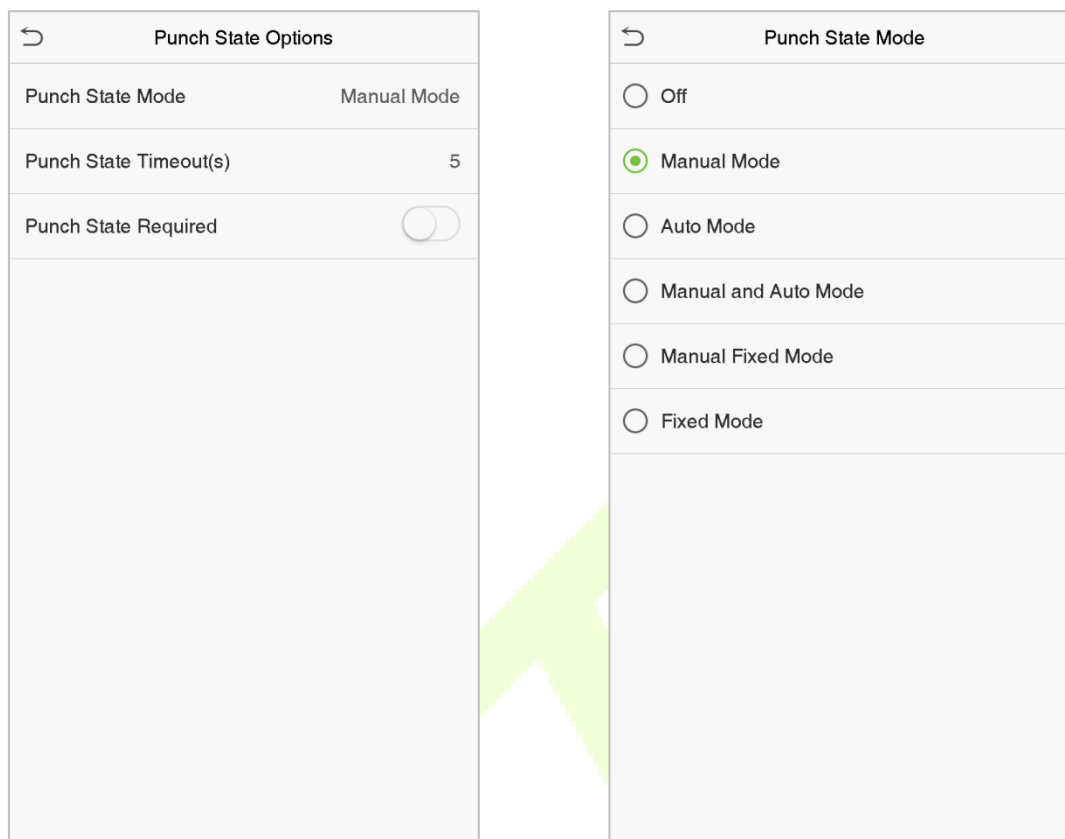
On the All Bell Schedules interface, tap the bell to be edited and click **Edit**. The editing method is the same as the operations of adding a bell.

Delete a Bell

On the All Bell Schedules interface, tap the bell to be deleted and click **Delete**, and select **Yes** to delete the bell.

7.4 Punch State Options

Click **Punch State Options** on the Personalize interface.



| Feature | Description |
|--------------------------------|---|
| Punch State Mode | <p>Selects a punch state mode, which can be:</p> <p>Off: Disables the punch state key function. The punch state key set under the Shortcut Key Mappings menu will not work.</p> <p>Manual Mode: Switches the punch state key manually; the attendance status will be automatically reset after the timeout.</p> <p>Auto Mode: The punch state key will switch to a specified status according to the predefined schedule set under Shortcut Key Mappings.</p> <p>Manual and Auto Mode: The main interface will display the auto-switch punch state key. However, users can still select alternative attendance statuses. After the timeout, the manually switching punch state key will become an auto-switch punch state key.</p> <p>Manual Fixed Mode: After the punch state key is manually switched, the punch state key will remain unchanged until being manually switched again.</p> <p>Fixed Mode: Only the fixed punch state key will be shown. The users cannot change their status by pressing other keys.</p> |
| Punch State Timeout (s) | The time duration for time out, i.e. remaining inactive in the main menu. |
| Punch State Required | Specifies whether an attendance status must be selected during verification. |

7.5 Shortcut Key Mappings

Users may define shortcuts for attendance status or functional keys. On the main interface, when the shortcut keys are pressed, the corresponding attendance status or function interface will be displayed quickly.

Click **Shortcut Key Mappings** on the Personalize interface.

| Shortcut Key Mappings | |
|-----------------------|--------------|
| F1 | Check-In |
| F2 | Check-Out |
| F3 | Break-Out |
| F4 | Break-In |
| F5 | Overtime-In |
| F6 | Overtime-Out |

- Click the shortcut key to enter the shortcut key setting interface, and select the **function** as punch state key or function key (such as new user, all users, etc.), as shown in the figure below:

← F1

Punch State Value 0

Function Punch State Options

Name Check-In

Set Switch Time

← F1

Function New User

- If the key is defined as a function key, the setting is completed; If set to a punch state key, set the punch state value (valid value 0~250), the name and switch time.

How to set the switch time?

The switch time is used in conjunction with the **punch state options**. When the **punch state mode** is set to **auto mode**, the switch time should be set. Select the switching period and set the switch time every day, as shown in the figure below:

The image displays four screenshots of the FaceDepot-7BL device's configuration menu, arranged in a 2x2 grid. A large, faint green watermark is visible across the center of the screenshots.

Top-Left Screenshot: Switch Cycle

This screen shows a list of days of the week with checkboxes. The days Monday through Friday are checked, while Saturday and Sunday are unchecked.

| Day | Checked |
|-----------|---------|
| Monday | ✓ |
| Tuesday | ✓ |
| Wednesday | ✓ |
| Thursday | ✓ |
| Friday | ✓ |
| Saturday | ✗ |
| Sunday | ✗ |

Top-Right Screenshot: Set Switch Time

This screen shows a list of days of the week. The time field is empty.

| Day | Time |
|-----------|------|
| Monday | |
| Tuesday | |
| Wednesday | |
| Thursday | |
| Friday | |

Bottom-Left Screenshot: Monday

This screen shows the time selection interface for Monday. The time is 13:55. The HH (Hour) field is highlighted with a blue border, and the MM (Minute) field is highlighted with a green border.

| Field | Value |
|-------|-------|
| HH | 13 |
| MM | 55 |

Bottom-Right Screenshot: Set Switch Time

This screen shows the time selection interface for Monday. The time is 08:00.

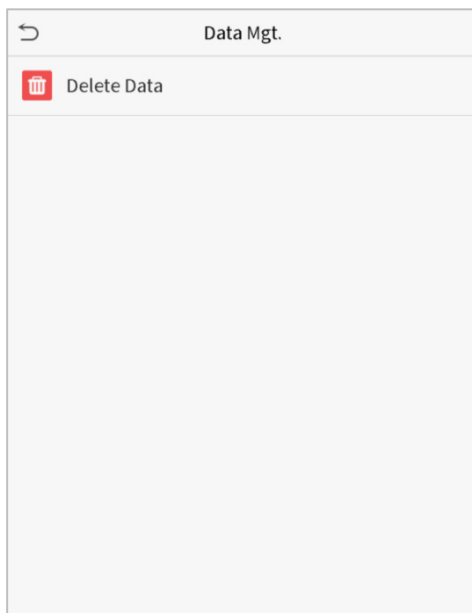
| Day | Time |
|-----------|-------|
| Monday | 08:00 |
| Tuesday | |
| Wednesday | |
| Thursday | |
| Friday | |

Note: When the function is set to undefine, the device will not enable the punch state key.

8 Data Management

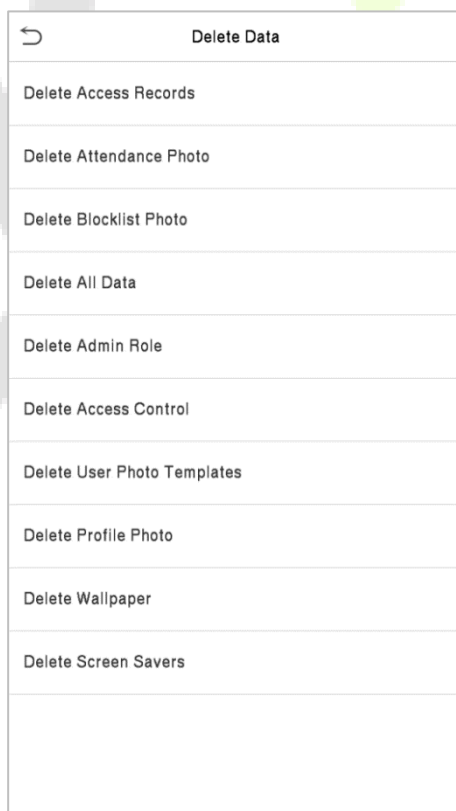
The Data Management function is used to delete the relevant data in the device.

Click **Data Mgt.** on the main menu interface.



8.1 Delete Data

Tap **Delete Data** on the **Data Mgt.** interface to delete the required data.



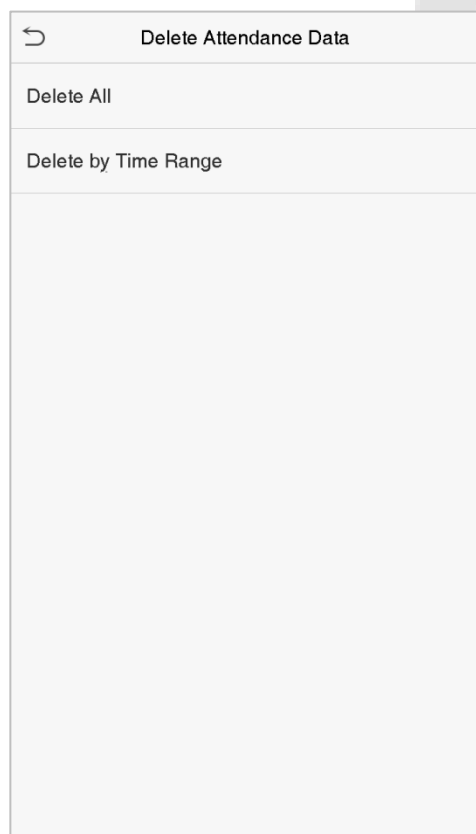
Function Description

| Function Name | Description |
|------------------------------------|--|
| Delete Access Records | To delete attendance data/access records conditionally. |
| Delete Attendance Photo | To delete attendance photos of designated personnel. |
| Delete Blocklist Photo | To delete the photos taken during failed verifications. |
| Delete All Data | To delete information and attendance logs/access records of all registered users. |
| Delete Admin Role | To remove all administrator privileges. |
| Delete Access Control | To delete all access data. |
| Delete User Photo Templates | When deleting template photos, there is a risk reminder: "Face re-registration is required after an algorithm upgrade." |
| Delete Profile Photo | To delete all user photos in the device. |
| Delete Wallpaper | To delete all wallpapers in the device. |
| Delete Screen Savers | To delete the screen savers in the device. |

Note: When deleting the attendance data/access records, attendance photos or blacklisted photos, you may select Delete All or Delete by Time Range. If you select Delete by Time Range, you need to set a specific time range to delete all the data with the period.

Select Delete by Time Range.

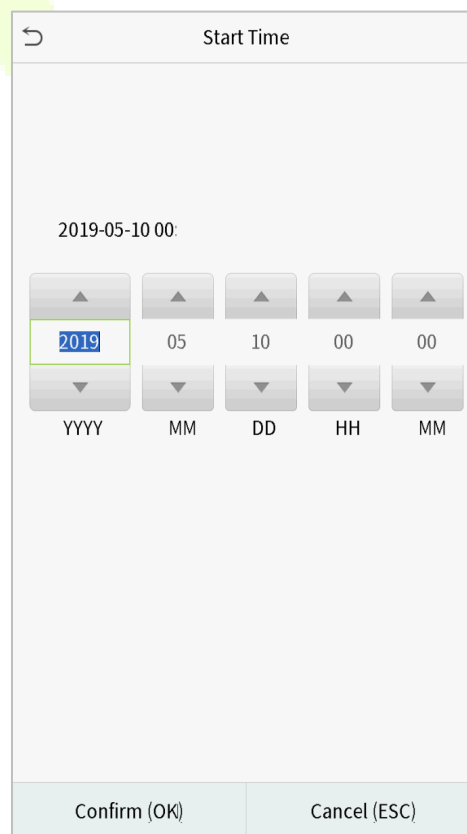
Set the time range and click **OK**.



Delete Attendance Data

Delete All

Delete by Time Range



Start Time

2019-05-10 00:

2019 05 10 00 00

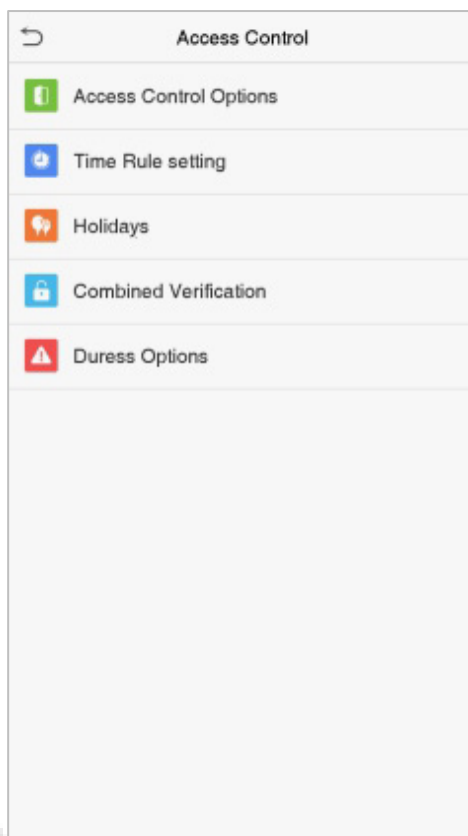
YYYY MM DD HH MM

Confirm (OK) Cancel (ESC)

9 Access Control

The Access Control function is used to schedule the door opening time, locks control and other parameter settings related to access control.

Click **Access Control** on the main menu interface.



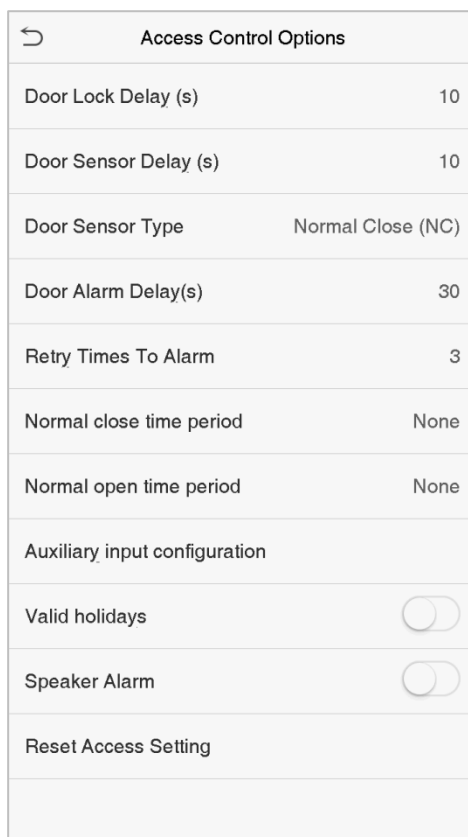
To obtain access, the following criteria's must be satisfied:

1. The current door unlock time should be within any valid time zone of the user time period.
2. The user's group must be in the door unlock combination (when there are other groups in the same access combination, the verification of members of those groups are also required to unlock the door).

In default settings, the new users are allocated into the first group with the default group time zone and access combination as "1" and set to an unlocking state.

9.1 Access Control Options

To set the parameters of the access control, click **Access Control Options** on the Access Control interface.



| Access Control Options | |
|-------------------------------|--------------------------|
| Door Lock Delay (s) | 10 |
| Door Sensor Delay (s) | 10 |
| Door Sensor Type | Normal Close (NC) |
| Door Alarm Delay(s) | 30 |
| Retry Times To Alarm | 3 |
| Normal close time period | None |
| Normal open time period | None |
| Auxiliary input configuration | |
| Valid holidays | <input type="checkbox"/> |
| Speaker Alarm | <input type="checkbox"/> |
| Reset Access Setting | |

| Feature | Description |
|------------------------------|--|
| Gate control mode★ | This feature decides whether to turn on the gate control mode or not. When set to ON, this interface will remove the Door lock relay, Door sensor relay, and Door sensor type function. |
| Door Lock Delay (s) | The length of time that the device controls the electric lock to be unlocked. The valid time range is 1 to 10 seconds; 0 second represents that the function is disabled. |
| Door Sensor Delay (s) | If the door is not closed and locked after opening for a certain duration (Door Sensor Delay), an alarm will be triggered. The valid range of Door Sensor Delay is 1 to 255 seconds. |
| Door Sensor Type | There are three types: None, Normal Open, and Normal Close. None means the door sensor is not in use; Normal Open means the door is always opened when electricity is on; Normal Close means the door is always closed when electricity is on. |
| Door Alarm Delay (s) | When the state of the door sensor is inconsistent with that of the door sensor type, an alarm will be triggered after a specific time period, i.e. the Door Alarm Delay. The valid value ranges from 1 to 999 seconds. 0 indicates an immediate alarm. |
| Retry Times to Alarm | When the number of failed verifications reaches a predefined value, which ranges from 1 to 9 times, an alarm will be triggered. If the value is set as "None", the alarm will never be triggered due to failed verifications. |

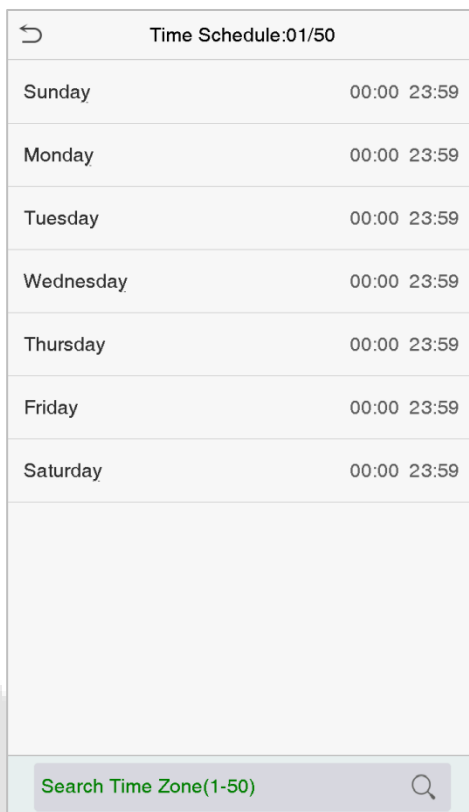
| | |
|--------------------------------------|---|
| Door available time period★ | This function sets the time period for the door so that the door is available only during this time period. |
| Normal Close Time Period | Time period is scheduled for the “Normal Close” mode so that no one can gain access during this period. |
| Normal Open Time Period | Time period is scheduled for the “Normal Open” mode so that the door is always unlocked during this period. |
| Master device★ | When setting up the Master and Slave, the status of the master can be set to out or in. Out: The record verified on the host is the exit record. In: The record verified on the host is the entry record. |
| Auxiliary input configuration | Set the door unlock time period and auxiliary output type of the auxiliary device. Auxiliary output types include None, Trigger door open, Trigger Alarm, Trigger door open and Alarm. |
| Valid holidays | To set if Normal Close Period or Normal Open Period settings are valid during the holiday time period. Choose ON to enable the functions during a holiday. |
| Speaker Alarm | To transmit a sound alarm or disable the alarm from the local. When the door is closed or the verification is successful, the system will cancel the alarm from the local. |
| Reset Access Setting | The restored access control parameters include door lock delay, door sensor delay, door sensor type, normal close time period, normal open time period, auxiliary input configuration and alarm. However, the access control data in Data Mgt. is excluded. |

9.2 Time Schedule

The entire system can define up to 50 time periods. Each time period represents seven time zones, i.e. one week, and each time zone is a valid time period within 24 hours per day. User can only verify within the valid time period. Each time zone format of the time period is HH MM-HH MM, which is accurate to minutes according to the 24-hour clock.

Click **Time Schedule** on the Access Control interface.

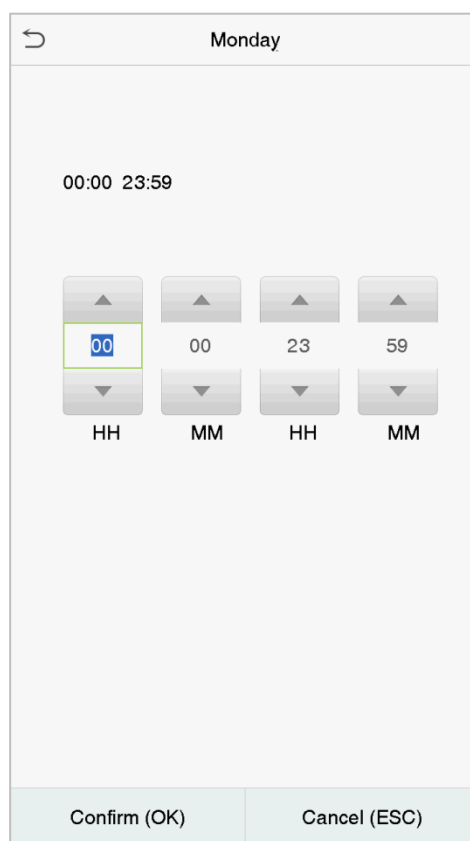
1. Click the grey box to search for a time zone. Enter the number of time zone (maximum: 50 zones).



The screenshot shows a mobile application interface for 'Time Schedule'. At the top, there is a back arrow and the title 'Time Schedule:01/50'. Below this is a table with two columns: the day of the week and the time range. The table lists days from Sunday to Saturday, each with a time range of '00:00 23:59'. Below the table is a large empty grey box. At the bottom, there is a search bar with the placeholder text 'Search Time Zone(1-50)' and a magnifying glass icon.

| Time Schedule:01/50 | |
|--------------------------|-------------|
| Sunday | 00:00 23:59 |
| Monday | 00:00 23:59 |
| Tuesday | 00:00 23:59 |
| Wednesday | 00:00 23:59 |
| Thursday | 00:00 23:59 |
| Friday | 00:00 23:59 |
| Saturday | 00:00 23:59 |
| | |
| Search Time Zone(1-50) 🔍 | |

2. Click the date on which time zone settings is required. Enter the starting and ending time, and then press **OK**.



Monday

00:00 23:59

| | | | |
|----|----|----|----|
| ↑ | ↑ | ↑ | ↑ |
| 00 | 00 | 23 | 59 |
| ↓ | ↓ | ↓ | ↓ |
| HH | MM | HH | MM |

Confirm (OK) Cancel (ESC)

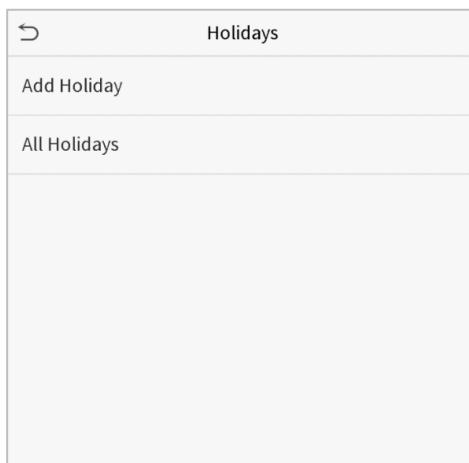
Note:

1. When the ending time is earlier than the starting time, such as 23:57~23:56, it indicates that access is prohibited all day; when the ending time is later than the starting time, such as 00:00~23:59, it indicates that the interval is valid.
2. The effective time period to unlock the door is open all day (00:00~23:59) or when the ending time is later than the starting time, such as 08:00~23:59.
3. The default time zone 1 indicates that the door is open all day long.

9.3 Holiday Settings

Whenever there is a holiday, you may need a special access time; but changing everyone's access time one by one is extremely cumbersome. So, you can set a holiday access time which applies to all the employees, and the user will be able to open the door during the holidays.

Click **Holidays** on the Access Control interface.



Add a New Holiday

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

The screenshot shows the 'Add Holiday' form. It has a title bar with a back arrow and 'Holidays'. The form contains four input fields: 'No.' with the value '1', 'Start Date' with the value 'Undefined', 'End Date' with the value 'Undefined', and 'Time Period' with the value '1'. Below these fields is a large, empty light gray area for additional notes or details.

Edit a Holiday

On the Holiday interface, select a holiday to be modified. Click **Edit** to modify the holiday parameters.

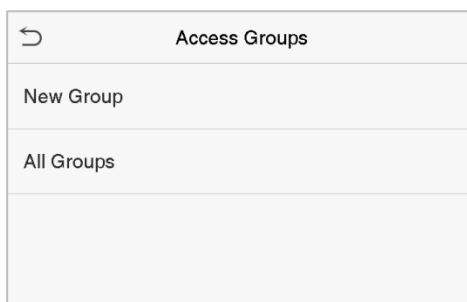
Delete a Holiday

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

9.4 Access Groups

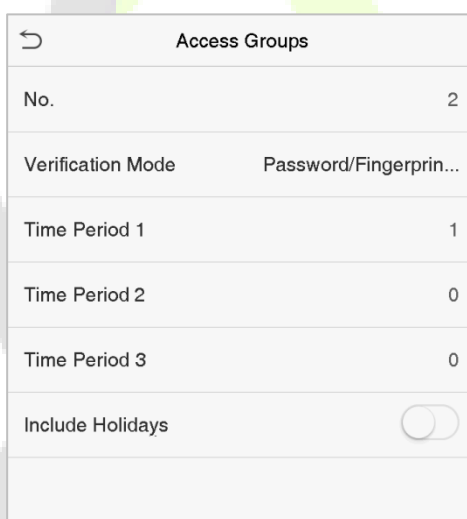
The Access Groups easily manage the users in different access groups. The Access Group settings such as access time zones are applicable to all the members in the group by default. However, users may manually set the time zones as needed. User authentication takes precedence over group authentication when the group authentication modes overlap with the individual authentication methods. Each group can set a maximum of three time zones. By default, newly enrolled users are assigned to Access Group 1; they can also be assigned to other access groups.

Click **Access Groups** on the Access Control interface.



Add a New Group

Click **New Group** on the Access Groups interface and set the access group parameters.



Note:

1. There is a default access group numbered 1, which cannot be deleted but can be modified.
2. A number cannot be modified after being set.
3. When the holiday is set to be valid, personnel in a group may only open the door when the group time zone overlaps with the holiday time period.
4. When the holiday is set to be invalid, the access control time of the personnel in a group is not affected during holidays.

Edit a Group

On the **All Groups** interface, select the access group item to be modified. Click **Edit** and modify the access group parameters.

Delete a Group

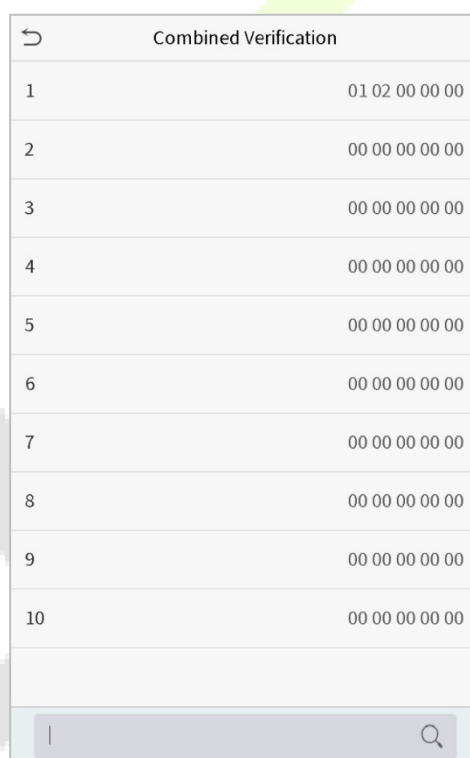
On the **All Groups** interface, select the access group item to be deleted and click **Delete**. Click OK to confirm the deletion. The deleted access group is no longer displayed in All Groups.

9.5 Combined Verification Settings

Access groups are arranged into different door-unlocking combinations to achieve multiple verifications and strengthen security.

In a door-unlocking combination, the range of the combined number N is $0 \leq N \leq 5$, and the number of members N may all belong to one access group or may belong to five different access groups.

Click **Combined Verification** on the Access Control interface.



| Combined Verification | |
|-----------------------|----------------|
| 1 | 01 02 00 00 00 |
| 2 | 00 00 00 00 00 |
| 3 | 00 00 00 00 00 |
| 4 | 00 00 00 00 00 |
| 5 | 00 00 00 00 00 |
| 6 | 00 00 00 00 00 |
| 7 | 00 00 00 00 00 |
| 8 | 00 00 00 00 00 |
| 9 | 00 00 00 00 00 |
| 10 | 00 00 00 00 00 |

Click the door-unlocking combination to be set. Click the up and down arrows to enter the combination number, then press **OK**.

Examples:

The door-unlocking combination 1 is set as (01 03 05 06 08), indicating that the unlocking combination 1 consists of 5 people, and the 5 individuals are from 5 groups, namely, access control group 1 (AC group 1), AC group 3, AC group 5, AC group 6, and AC group 8, respectively.

The door-unlocking combination 2 is set as (02 02 04 04 07), indicating that the unlocking combination 2 consists of 5 people; the first two are from AC group 2, the next two are from AC group 4, and the last person is from AC group 7.

The door-unlocking combination 3 is set as (09 09 09 09 09), indicating that there are 5 people in this combination; all of which are from AC group 9.

The door-unlocking combination 4 is set as (03 05 08 00 00), indicating that the unlocking combination 4 consists of three people. The first person is from AC group 3, the second person is from AC group 5, and the third person is from AC group 8.

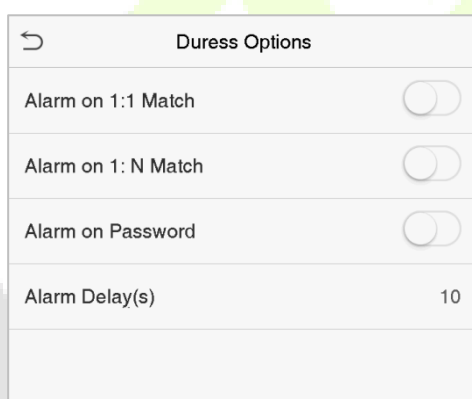
Delete a Door-unlocking Combination

Set all the group number as 0 if you want to delete the door-unlocking combinations.

9.6 Duress Options Settings

If a user activated the duress verification function with a specific authentication method(s), when he/she is under threat during authentication with such a method, the device will unlock the door as usual, but at the same time, a signal will be sent to trigger the alarm.

Click **Duress Options** on the Access Control interface.



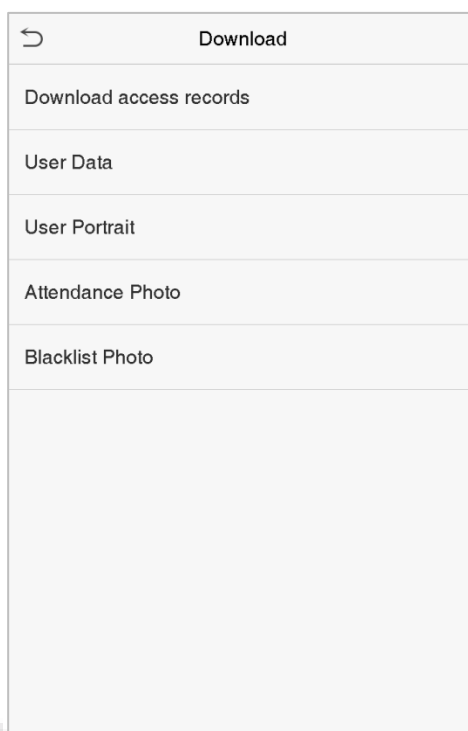
| Duress Options | |
|---------------------|--------------------------|
| Alarm on 1:1 Match | <input type="checkbox"/> |
| Alarm on 1: N Match | <input type="checkbox"/> |
| Alarm on Password | <input type="checkbox"/> |
| Alarm Delay(s) | 10 |

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

10 USB Manager

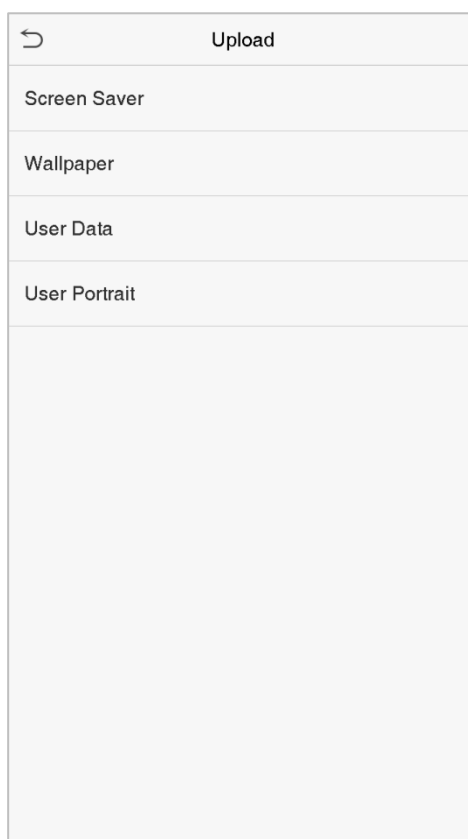
You can download the user information, access data and other data to a USB drive for further processing. Before uploading or downloading data from or to the USB drive, insert the USB drive into the USB slot first. Click the **USB Manager** on the main menu interface.

10.1 Download



| Feature | Description |
|--------------------------------|--|
| Download access records | Downloads the access data within a specified time period or all the data to a USB drive |
| User Data | Downloads all the user information from the device to a USB drive |
| User Portrait | Downloads all the user images from the device to a USB drive |
| Attendance Photo | Downloads the attendance photos stored in the device within a specified time period or all the attendance photos from the device to a USB drive. The default image format is JPG |
| Blacklist Photo | Downloads the blacklisted photos taken after failed verifications within a specified time period or all the pictures taken after failed verifications from the device to a USB drive |

10.2 Upload

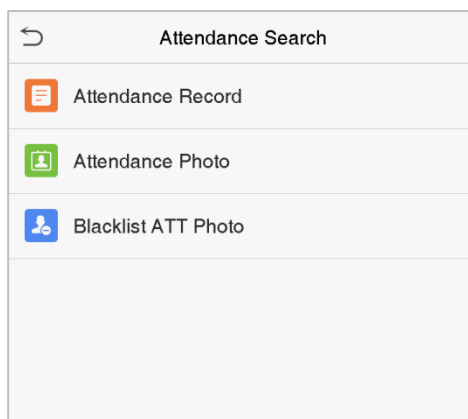


| Feature | Description |
|----------------------|---|
| Screen Saver | Uploads a screen saver from a USB drive to the device. Before uploading, you may select Upload selected picture or Upload all pictures . |
| Wallpaper | Uploads a wallpaper from a USB drive to the device. Before uploading, you may select Upload selected picture or Upload all pictures . The images will be displayed on the screen after manual settings. |
| User Data | Uploads all the user information from a USB drive to the device. |
| User Portrait | Uploads a JPG picture named with a user ID from a USB drive to the device. Before uploading, you may select Upload Current Picture or Upload All Pictures . |

11 Attendance Search

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

Click **Attendance Search** on the main menu interface.



The process of searching attendance and blacklist photos is similar to search the access records. The following is an example of searching for access records.

On the Attendance Search interface, click **Access Records**.

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

 A screenshot of the 'User ID' input screen. At the top, it says 'User ID'. Below that is a text field with the placeholder 'Please Input(query all data without input)'. At the bottom is a numeric keypad with buttons for digits 1-9, 0, and function keys like ESC, 123, and OK.

 A screenshot of the 'Time Range' selection screen. It has a back arrow at the top left. Below the title, there are several radio button options: 'Today' (selected), 'Yesterday', 'This week', 'Last week', 'This month', 'Last month', 'All', and 'User Defined'.

3. Click the record list in green to view its details.

| Personal Record Search | | |
|------------------------|---------|--|
| Date | User ID | Attendance |
| 06-14 | | Number of Records:12 |
| | 1 | 16:40 16:40 16:40 16:40 16:40 16:40 16:40 16:36 16:30 16:12 16:10 16:10 |
| 06-12 | | Number of Records:20 |
| | 1 | 14:43 14:43 14:43 14:43 14:43 14:43 14:43 14:43 14:43 14:43 14:43 14:43 14:15 14:08 14:08 14:07 13:58 13:58 13:58 13:54 |
| 06-11 | | Number of Records:06 |
| | 1 | 19:39 18:36 18:36 18:36 18:36 17:14 |

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

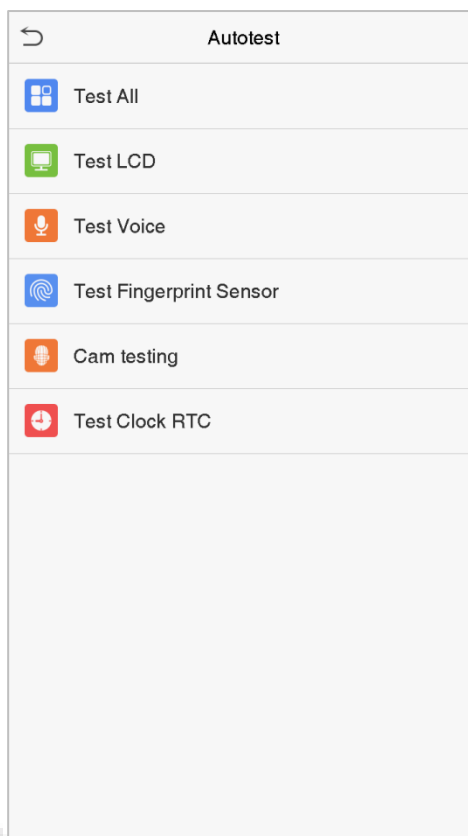
| Personal Record Search | | | | |
|------------------------|------|-------------|------|-------|
| User ID | Name | Attendance | Mode | State |
| 1 | A | 06-11 19:39 | 15 | 1 |
| 1 | A | 06-11 18:36 | 15 | 255 |
| 1 | A | 06-11 18:36 | 15 | 255 |
| 1 | A | 06-11 18:36 | 15 | 1 |
| 1 | A | 06-11 17:14 | 1 | 1 |

Verification Mode : Face Punch State : Check-Out

12 Autotest

The Autotest feature is used to automatically test whether all the modules in the device function properly, including LCD, Voice, Fingerprint sensor★, Camera and real-time clock (RTC).

Click **Autotest** on the main menu interface.

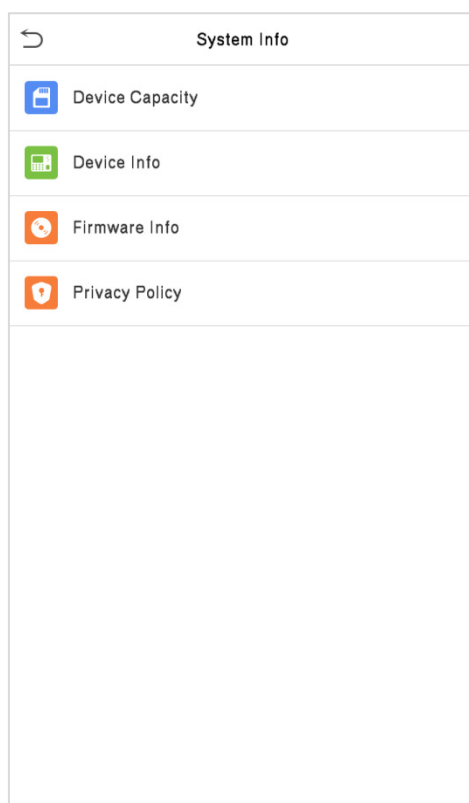


| Feature | Description |
|---------------------------------|--|
| Test All | To automatically test whether the LCD, Audio, Camera, and RTC are normal. |
| Test LCD | To automatically test the display effect of LCD screen by displaying full-color, pure white, and pure black to check whether the screen displays the colors normally. |
| Test Voice | To automatically test whether the audio files stored in the device are complete and the voice quality is good. |
| 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. |
| Camera testing | To test if the camera functions properly by checking the pictures taken to see if they are clear enough. |
| Test Clock RTC | To test whether the clock works normally and accurately with a stopwatch. Touch the screen to start counting and press it again to stop counting. |

13 System Information

In the system information option, you can view the storage status, version information of the device, and so on.

Click **System Info** on the main menu interface.



| Feature | Description |
|------------------------|---|
| Device Capacity | Displays the current device's user storage, palm, password, fingerprint★ and face storage, Administrator details, Access records, attendance and blacklist photos, and user photos. |
| Device Info | Displays the Device's name, Serial number, MAC address, Face algorithm version information, Platform information, and manufacturer details. |
| Firmware Info | Displays the firmware version and other version information of the device. |
| Privacy Policy | <p>The privacy policy control will appear when the gadget turns on for the first time. After clicking "I have read it," the customer can use the product regularly. Click System Info -> Privacy Policy to view the content of the privacy policy. The privacy policy's content does not allow for U disc export.</p> <p>Note: The current privacy policy's text is only available in Simplified Chinese/English. However, translation of other multi-language content is underway, with more iterations.</p> |

14 Connection to ZKBioSecurity Software

14.1 Set the Communication Address

In Device

Click **COMM.** > **Ethernet** in the main menu to set the IP address and Gateway of the device. (**Note:** The IP address should be able to communicate with the ZKBioSecurity Server, preferably in the same network segment with the Server address)

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

Server Address: Set the IP address of the ZKBioSecurity Server.

Server Port: Set the Server port of ZKBioSecurity (The default is 8088).

| Ethernet | |
|-----------------------|-------------------------------------|
| IP Address | 192.168.163.150 |
| Subnet Mask | 255.255.255.0 |
| Gateway | 192.168.163.1 |
| DNS | 0.0.0.0 |
| TCP COMM.Port | 4370 |
| DHCP | <input type="checkbox"/> |
| Display in Status Bar | <input checked="" type="checkbox"/> |

| Cloud Server Setting | |
|----------------------|--------------------------|
| Server mode | ADMS |
| Enable Domain Name | <input type="checkbox"/> |
| Server Address | 0.0.0.0 |
| Server port | 8081 |
| Enable Proxy Server | <input type="checkbox"/> |

In Software

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

Adms Service Settings

Adms Service Port: 8088

⚠ The current port is for device communication service, if there is a network mapping for the service port, please refer to the actual mapped port.

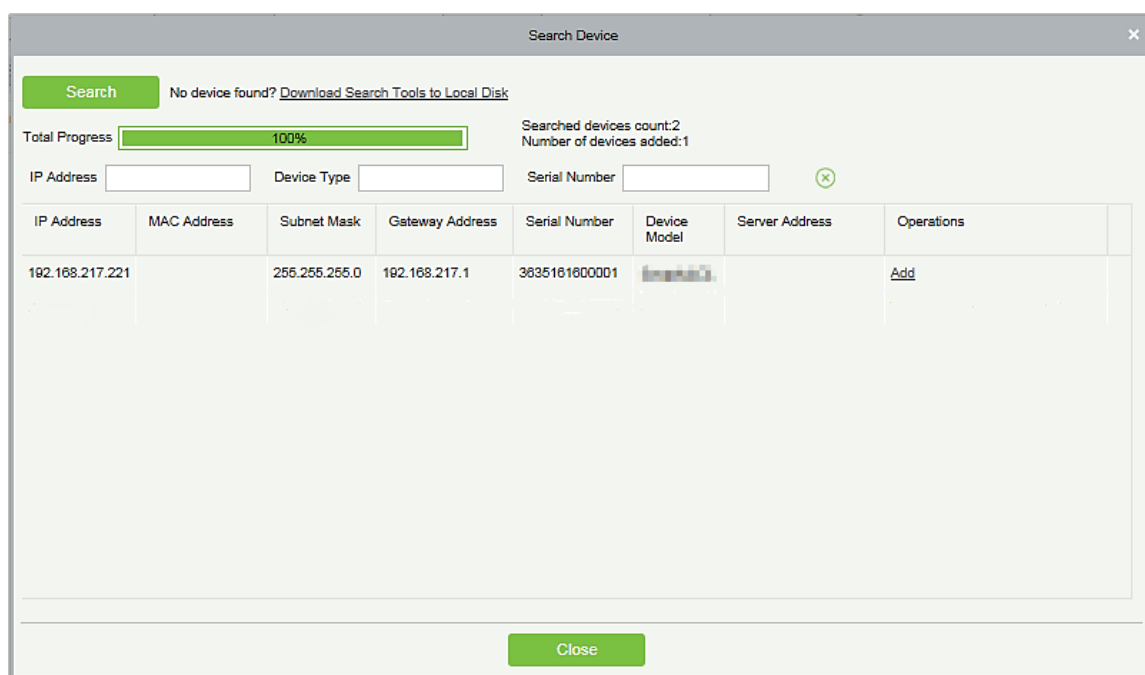
Server Side Network Condition

Whether the Internet connection is normal: Yes

14.2 Add a Device to the Software

You can add a device by the searching process. The procedure is as follows:

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



The screenshot shows a 'Search Device' window with a search bar, a progress bar at 100%, and a table of search results. The table has columns for IP Address, MAC Address, Subnet Mask, Gateway Address, Serial Number, Device Model, Server Address, and Operations. One device is listed with IP 192.168.217.221 and a serial number 3835161800001. The 'Operations' column for this device contains an 'Add' link.

| IP Address | MAC Address | Subnet Mask | Gateway Address | Serial Number | Device Model | Server Address | Operations |
|-----------------|-------------|---------------|-----------------|---------------|--------------|----------------|---------------------|
| 192.168.217.221 | | 255.255.255.0 | 192.168.217.1 | 3835161800001 | | | Add |

4. Click **Add** to add the required device.

14.3 Add Personnel on the Software

1. Click **Personnel** > **Person** > **New** to add new personnel.

The screenshot shows a 'New' personnel form with the following fields and options:

- Personnel ID***: 2
- Department***: General
- First Name**: (empty)
- Last Name**: (empty)
- Gender**: (dropdown menu)
- Password**: (empty)
- Certificate Type**: ID
- Certificate Number**: (empty)
- Social Security Number**: (empty)
- Mobile Phone**: (empty)
- Reservation Code**: 123456
- Birthdate**: (empty)
- Position**: (dropdown menu)
- Card Number**: (empty)
- Biological Template Quantity**: 0
- Hire Date**: (empty)

Below the form, there are tabs for **Access Control**, **Time Attendance**, **Elevator Control**, **Plate Register**, and **Personnel Detail**. The **Personnel Detail** tab is active, showing:

- Levels Settings**: ☒ Master
- Superuser**: No
- Device Operation Role**: Ordinary User
- Delay Passage**: ☐
- Disabled**: ☐
- Set Valid Time**: ☐

At the bottom of the form are three buttons: **Save and New**, **OK**, and **Cancel**.

2. After setting all the parameters, click **OK**.

Note: For other specific operations, please refer *ZKBioSecurity User Manual*.

Appendix 1

Requirements of Live Collection and Registration of Visible Light Face Images

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



Requirements for Visible Light Digital Face Image Data

The digital photo should be straight-edged, coloured, 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 photos captured.

- **Eye Distance**

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

- **Facial Expression**

A neutral face or smile with eyes naturally open are recommended.

- **Gesture and Angel**

The 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 coloured eyeglasses are not allowed. The frame of the eyeglasses should not cover the eyes and should not reflect light. For persons with thick eyeglasses frames, it is recommended to capture two images, one with eyeglasses and the other one without them.

- **Face**

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

- **Image Format**

Should be in BMP, JPG or JPEG.

- **Data Requirement**

Should comply with the following requirements:

- 1) White background with dark-coloured apparel.
- 2) 24bit true color mode.
- 3) JPG format compressed image 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 face or smile is preferred, showing teeth is not preferred.
- 9) The captured person should be easily visible, natural in color, no harsh shadow or light spot or reflection in the face 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 and its affiliates, hereinafter referred as "we", "our", or "us", the 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/cn/index/Index/privacy_protection.html to learn more about how we collect, use, and securely store your personal information. To keep pace with the rapid development of technology, adjustment of business operations, and to cope with customer needs, we will constantly deliberate and optimize our privacy protection measures and policies. Welcome to visit our official website at any time to learn our latest privacy policy.

Eco-friendly Operation



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

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

Hazardous or Toxic substances and their quantities

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

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

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

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

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

Phone : +86 769 - 82109991

Fax : +86 755 - 89602394

www.zkteco.com

