User Manual

M2-LR/M2F PRO-LR

Date: January 2025

Doc Version: 1.0

English

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

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

Trademark

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

Disclaimer

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

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

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

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

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

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

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

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

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

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

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

ZKTeco Headquarters

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

Phone +86 769 - 82109991

Fax +86 755 - 89602394

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

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

About the Company

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

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

About the Manual

This manual introduces the operations of **M2-LR/M2F PRO-LR**.

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

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

Document Conventions

Conventions used in this manual are listed below:

GUI Conventions

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

Symbols

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

TABLE OF CONTENTS

Data Security Statement

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

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

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

Safety Measures

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

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

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

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

perform safety checks to ensure proper operation of the unit.

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

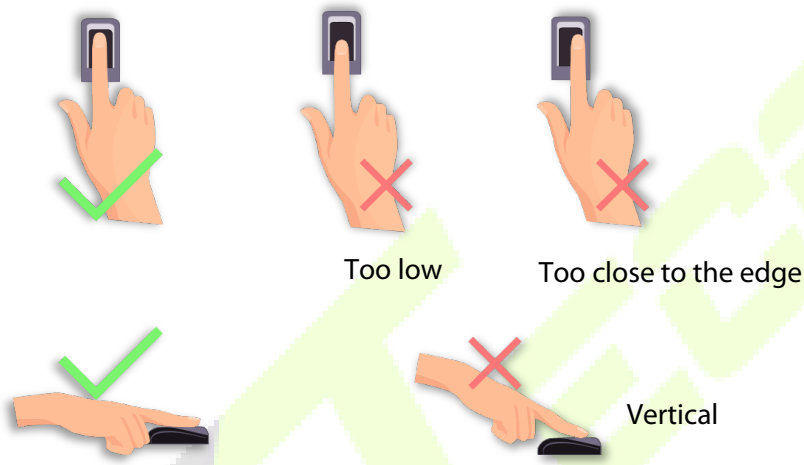
The devices should be installed in areas with limited access.

1 Instruction for Use

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

1.1 Finger Positioning

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

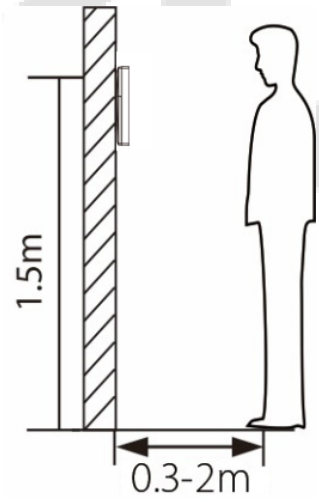


Note: *Please use the correct method when pressing your fingers onto the fingerprint reader for registration and identification. Our company will assume no liability for recognition issues that may result from incorrect usage of the product. We reserve the right of final interpretation and modification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

1.2 Standing Position, Posture and Facial Expression★

(NOTE: Only for M2F PRO-LR.)

- **The recommended distance**



The distance between the device and a user whose height is in a range of 1.55 m to 1.85 m is recommended to be 0.3 m to 2m. Users may slightly move forward or backward to improve the quality of facial images captured.

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

Standing Posture

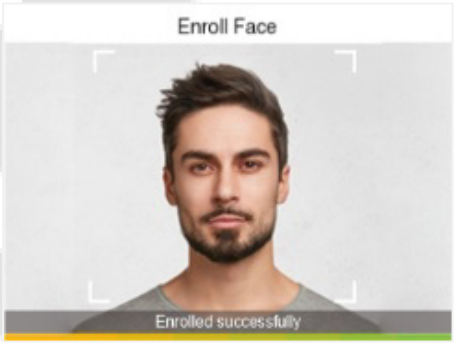
Facial Expression

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

1.3 Face Template Registration★

(NOTE: Only for M2F PRO-LR.)

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



Correct face Registration and Authentication Method

➢ **Recommendation for Registering a Face Template**

- When registering a face template, maintain a distance of 40 cm to 80 cm space between the device and the face template.
- Be careful not to change your facial expression. (Smiling face template, drawn face template, wink, etc.)
- If you do not follow the instructions on the screen, the face template registration may take longer or may fail.

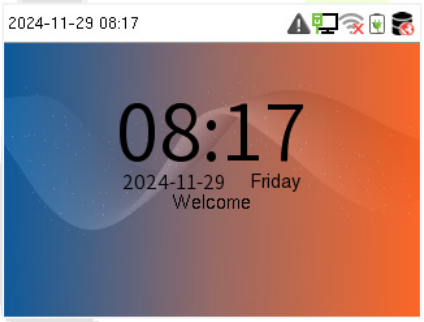
- Be careful not to cover the eyes or eyebrows.
- Do not wear hats, masks, sunglasses, or eyeglasses.
- Ensure only one person is visible in the camera's frame during face template registration.
- It is recommended for a user wearing glasses to register both face templates with and without glasses.

➢ **Recommendation for Authenticating a Face Template**

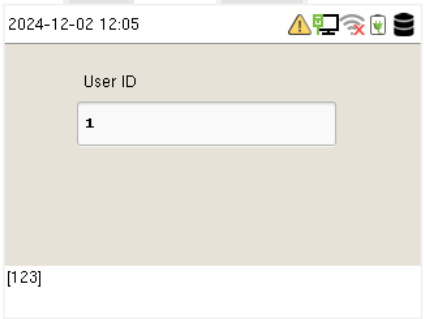
- Ensure that the face template appears inside the guideline displayed on the screen of the device.
- If the glasses have been changed, authentication may fail. If the face template without glasses has been registered, authenticate the face template without glasses further. If the face template with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

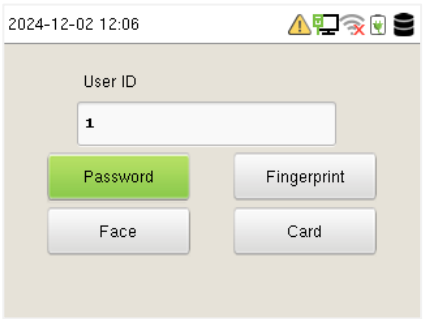
1.4 Standby Interface

The device uses a 2.8-inch color screen, which all operations are performed through the keypad. After connecting the power supply, the following standby interface is displayed:

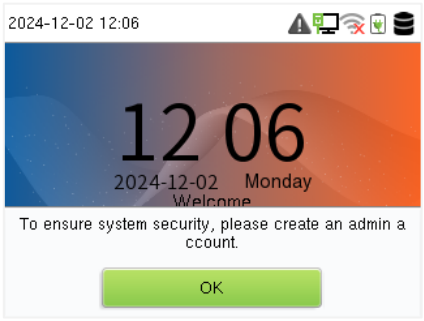


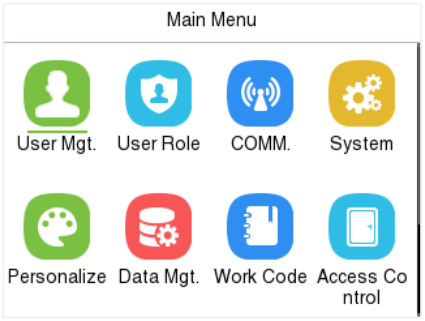
- Enter any number to access the User ID input interface.



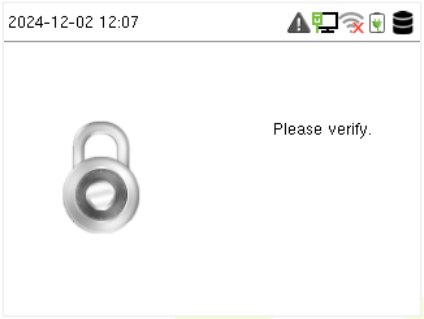


- When there is no Super Administrator set in the device, press **M/OK** to go to the menu.



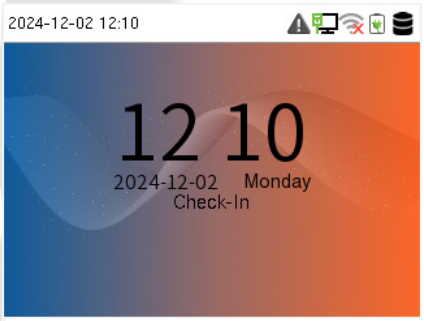


- After adding a Super Administrator on the device, it requires the Super Administrator's verification before opening the menu functions.



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

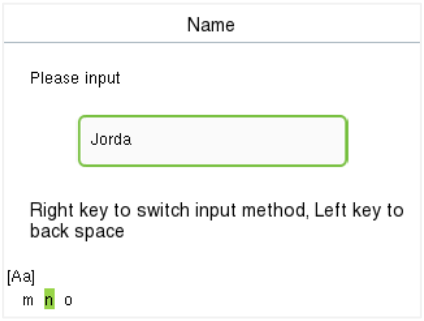
- On the standby interface, the punch state options can also be shown and used directly. The shortcut key mappings will be displayed on the screen if you press the relevant shortcut key on the keypad, as shown in the picture below. For the specific operation method, please see "Shortcut Key Mappings."



1.5 T9 Mode

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

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



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

1.6 Verification Mode

1.6.1 Fingerprint Verification

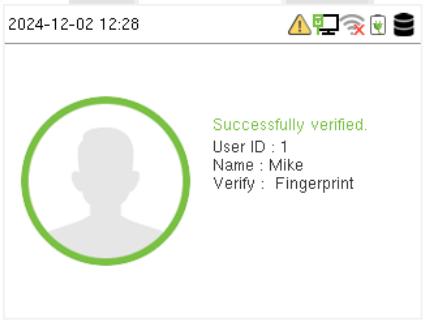
➢ **1: N Fingerprint Verification Mode**

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

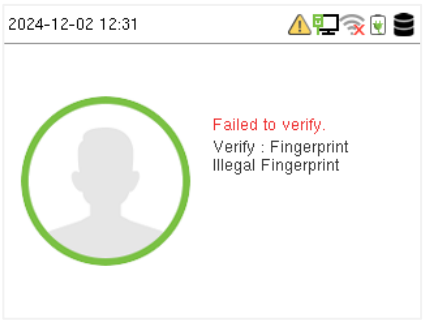
Fingerprint authentication mode is activated when a user places their finger onto the fingerprint scanner.

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

Verification is successful:



Verification is failed:



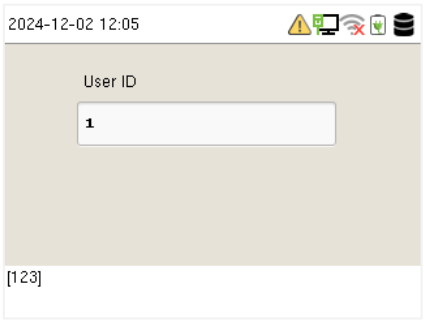
➢ **1: 1 Fingerprint Verification Mode**

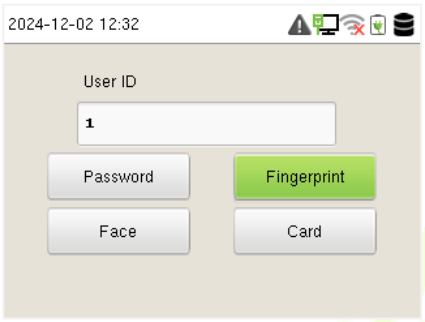
The device compares the current fingerprint with the fingerprints linked to the entered User ID through the keyboard.

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

Enter the user ID and press **M/OK** to enter the 1:1 fingerprint verification mode.

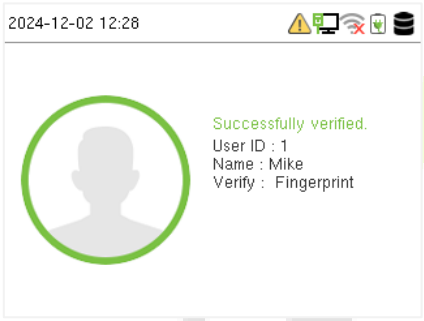
If the user has registered card, face, and password in addition to the fingerprint, and the verification method is set to Password/Fingerprint/Card/Face★, the following screen will appear. Select **Fingerprint** to enter the fingerprint verification mode.



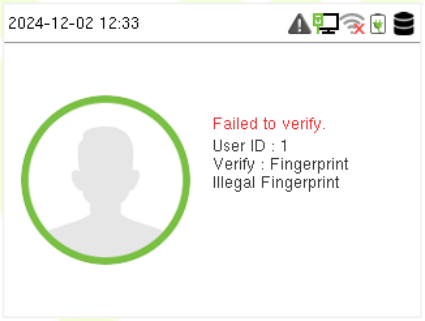


Press the fingerprint to verify.

Verification is successful:



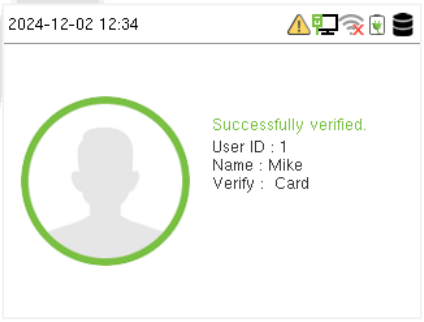
Verification is failed:



1.6.2 Card Verification

➢ **1:N card verification**

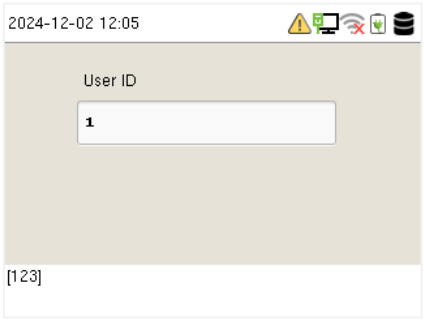
The 1:N card verification mode compares the card number in the card induction area with all the card number data registered in the device; The following screen displays on the card verification:

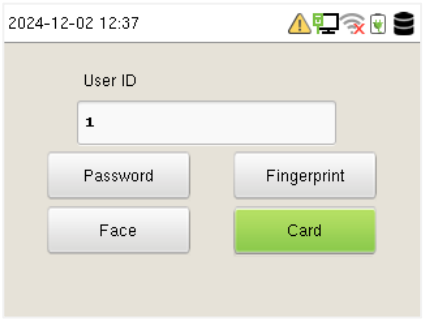


➢ **1:1 Card Verification**

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

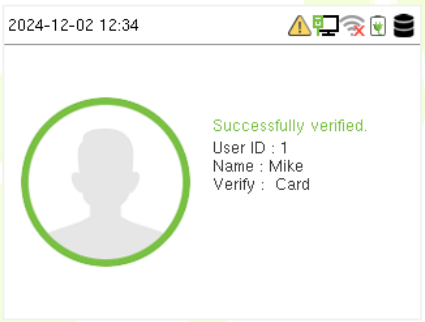
Enter the user ID and press **M/OK** to enter the 1:1 card verification mode.





If the user has registered fingerprint, face, and password in addition to the card, and the verification method is set to Password/Fingerprint/Card/Face★, the following screen will appear. Select **Card** to enter the card verification mode.

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

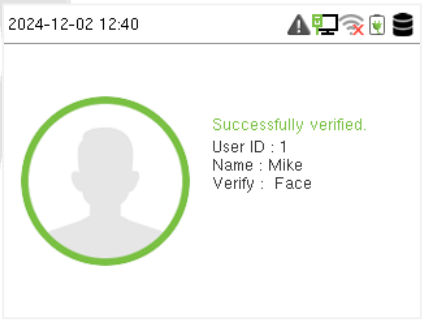


1.6.3 Facial Verification★

(NOTE: Only for M2F PRO-LR.)

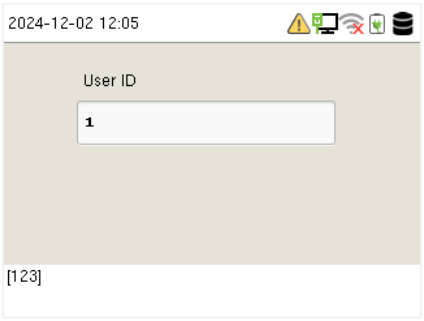
- **1:N Facial Verification**

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

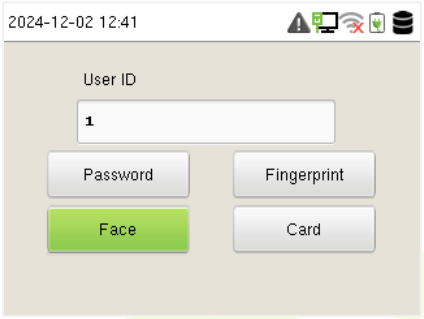


- **1:1 Facial Verification**

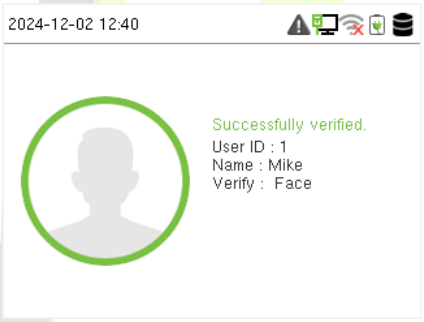
In this verification mode, the device compares the face captured by the camera with the facial template related to the entered user ID. Enter the user ID and press **M/OK** to enter the 1:1 facial verification mode.



If the user has registered fingerprint, card and password in addition to the face, and the verification method is set to Password/Fingerprint/Card/Face, the following screen will appear. Select **Face** to enter the face verification mode.



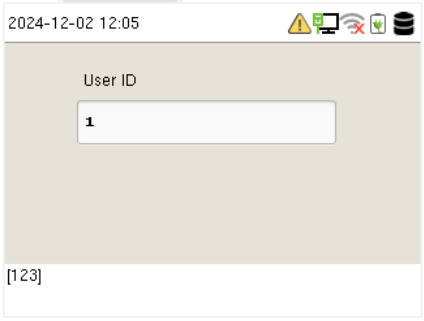
After successful verification, the prompt box displays "**Successfully verified**", as shown below:

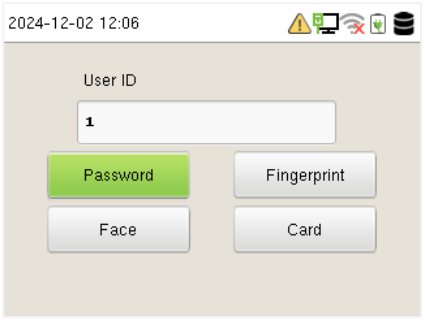


1.6.4 Password Verification

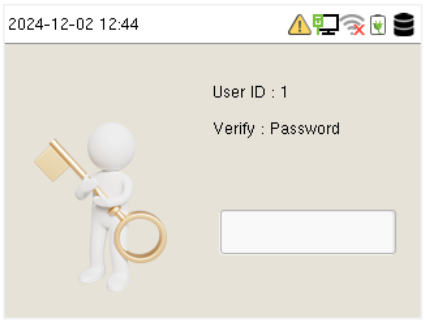
The device compares the entered password with the registered password and User ID.

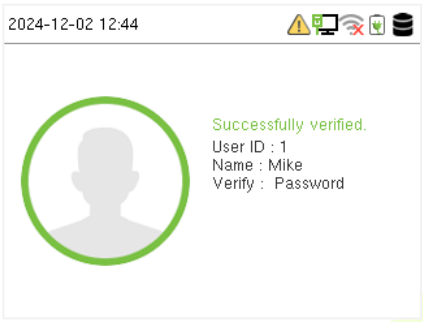
Enter the user ID and press **M/OK** to enter the 1:1 password verification mode. Then, input the user ID and press **M/OK**.





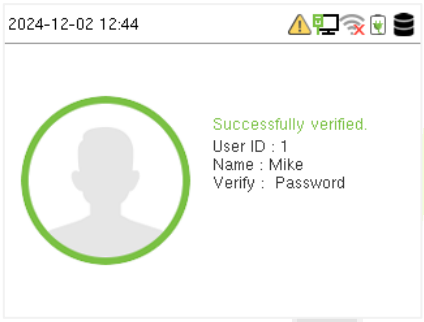
If the user has registered fingerprint, card and face in addition to the password, and the verification method is set to Password/Fingerprint/Card/Face★, the following screen will appear. Select **Password** to enter the password verification mode.



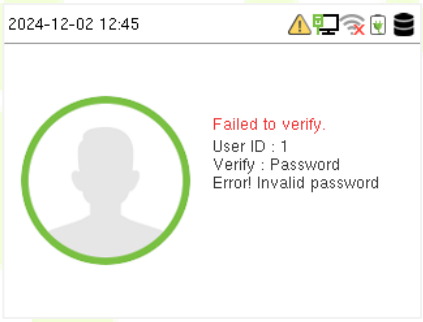


The following screen displays, after inputting a correct password and a wrong password respectively.

Verification is successful:



Verification is failed:

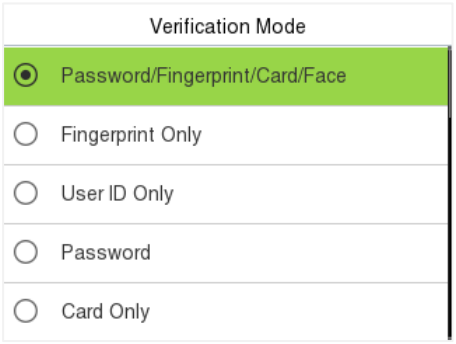


1.6.5 Combined Verification

To increase security, this device offers the option of using multiple forms of verification methods. A total of 21 different verification combinations can be used, as shown below:

Combined Verification Symbol Definition:

Symbol	Definition	Explanation
/	or	This method compares the entered verification of a person with the related verification template previously stored to that Personnel ID in the Device.
+	and	This method compares the entered verification of a person with all the verification template previously stored to that Personnel ID in the Device.

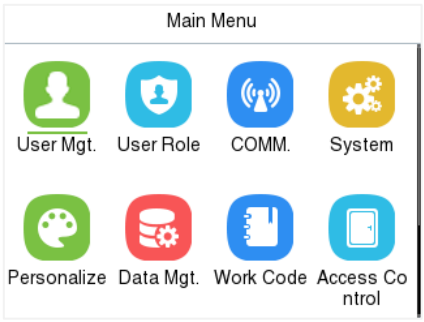


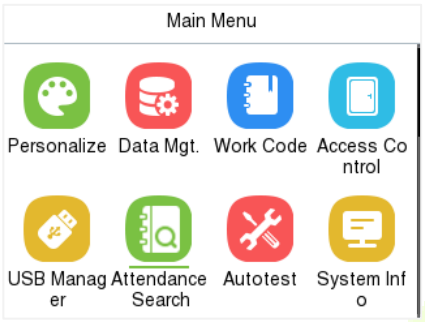
➢ **Procedure to set for Combined Verification Mode:**

- Combined verification requires personnel to register all the different verification method. Otherwise, employees will not be able to successfully verify the combined verification process.
- For instance, when an employee has registered only the data, but the Device verification mode is set as "Face + Password", the employee will not be able to complete the verification process successfully.
- This is because the Device compares the scanned face template of the person with registered verification template (both the Face template and the Password) previously stored to that Personnel ID in the Device.
- But as the employee has registered only the Face template but not the Password, the verification will not get completed and the Device displays "Verification Failed".

2 Main Menu

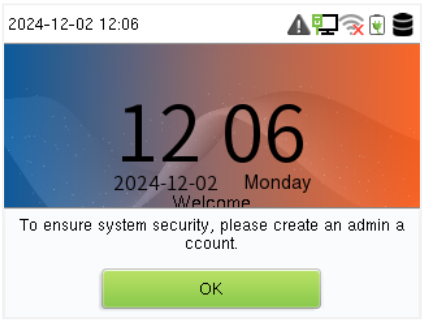
Press **M/OK** to enter the **Main Menu**, the following screen will be displayed:





Menu	Descriptions
User Mgt.	To add, edit, view, and delete basic information of a User.
User Role	To set the permission scope of the custom role for the users, that is, the rights to operate the system.
COMM.	To set the relevant parameters of network, pc connection, wireless network★, cloud server and network diagnosis.
System	To set the parameters related to the system, including date time, attendance, face template★ & fingerprint parameters, security setting, update firmware online, USB upgrade, and reset to factory.
Personalize	This includes user interface, voice, bell schedules, punch state options and shortcut key mappings settings.
Data Mgt.	To delete all relevant data in the device.
Work Code	Set different type of work.
Access Control	To set the parameters of the lock and the relevant access control device.
USB Manager	To upload or download the specific data by a USB drive.
Attendance Search	To query the specified event logs, check attendance photos★ and blocklist attendance photos★.
Autotest	To automatically test whether each module functions properly, including the LCD screen, audio, keyboard, camera★, fingerprint sensor and real-time clock.
System Info	To view data capacity, device and firmware information and privacy policy of the device.

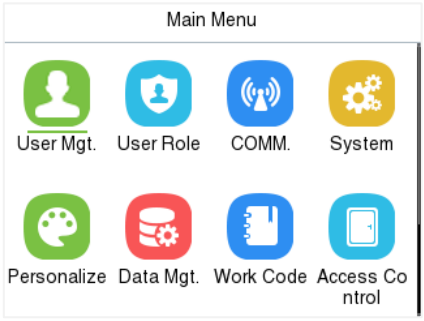
Note: *When users use the product for the first time, they should operate it after setting administrator privileges. Press* ***User Mgt.*** *to add an administrator or edit user permissions as a super administrator. If the product does not have an administrator setting, the system will show an administrator setting command prompt every time you enter the device menu.*

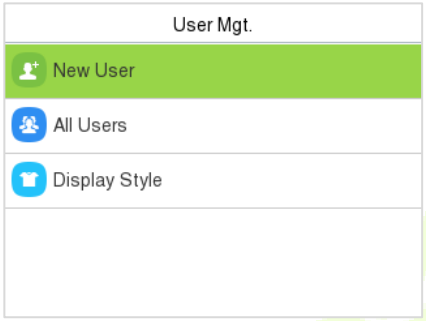


3 User Management

3.1 User Registration

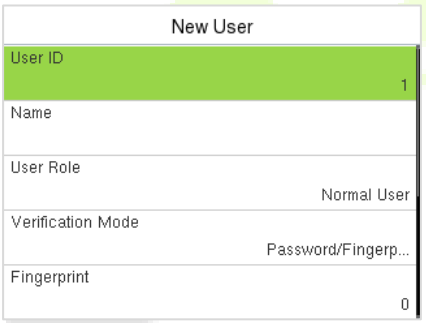
When the device is on the initial interface, press **M/OK** and enter **User Mgt.** > **New User**.





3.1.1 User ID and Name

Enter the **User ID** and **Name**.



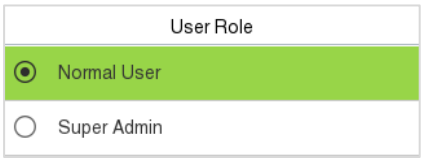
Notes:

- *A username can contain a maximum of 34 characters.*
- *The user ID may contain 1 to 14 digits by default,* supporting both numbers and alphabetic characters.
- *During the initial registration, you can modify your ID, which cannot be modified after registration.*
- *If a message "**Duplicated!**" pops up, you must choose another ID as the enter User ID already exists.*

3.1.2 User Role

On the New User interface, select **User Role** to set the user's role as either **Normal User** or **Super Admin**.

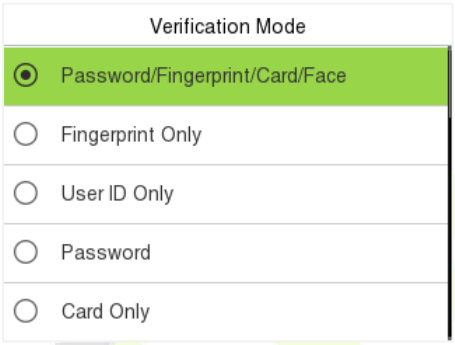
- **Super Admin:** The Super Administrator owns all management privileges in the Device.
- **Normal User:** If the Super Admin is already registered in the Device, then the Normal Users will not have the privileges to manage the system and can only access authentication verifications.
- **User Defined Roles:** The Normal User can also be set with **User Defined Role** which are the custom roles that can be set to the Normal User.



Note: *If the selected user role is the Super Admin, the user must pass 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 to Verification Mode.*

3.1.3 Verification Mode

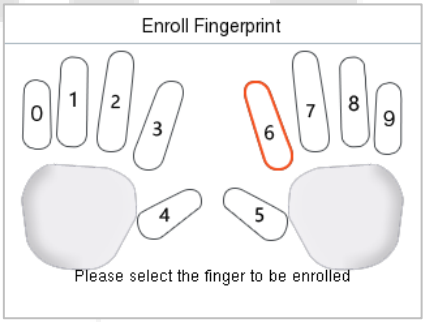
Select the mode of verification for the user, a total of 21 different verification combinations can be used. Please refer to 1.6.5 combined verification for details.

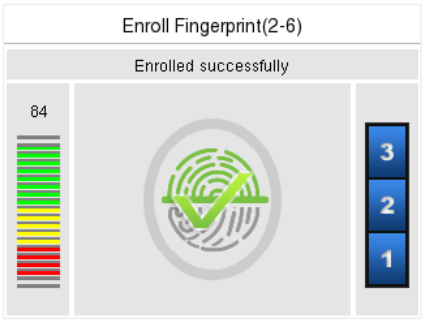


3.1.4 Register Fingerprint

Select **Fingerprint** in the **New User** interface to enter the fingerprint registration page.

- Select the finger to be enrolled.
- Press the same finger on the fingerprint reader three times.
- Green indicates that the fingerprint was enrolled successfully.



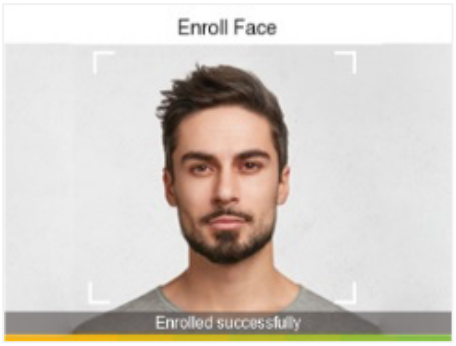


3.1.5 Register Face Template★

Select **Face** in the **New User** interface to enter the face registration page.

- Please face towards the camera and position your face template inside the white guiding box and stay still during face template registration.

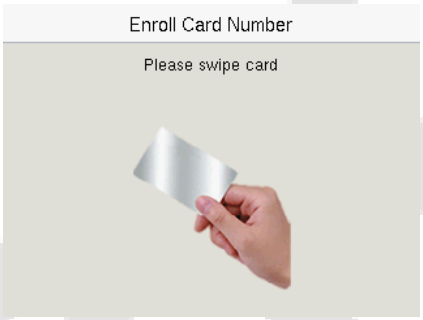
- A progress bar shows up while registering the face template and a **"Enrolled successfully"** is displayed as the progress bar completes.
- If the face template is registered already then, the **"Duplicated Face"** message shows up. The registration interface is as follows:

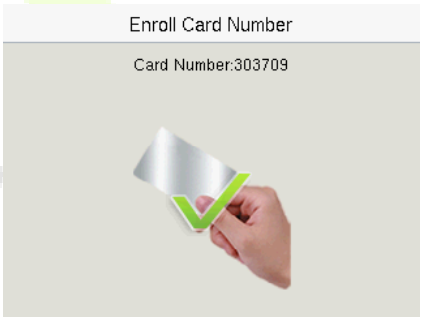


3.1.6 Card

Select **Card** in the **New User** interface to enter the card registration page.

- On the Card interface, swiping card underneath the card reading area. The card registration will be successful.
- If the card is registered already then, the "**Duplicate Card**" message shows up. The registration interface is as follows:

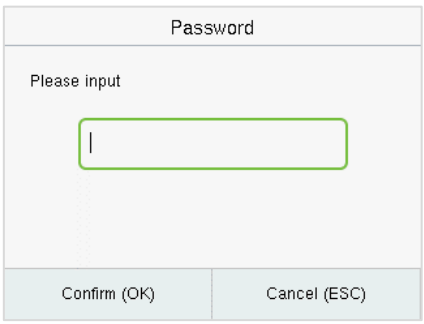


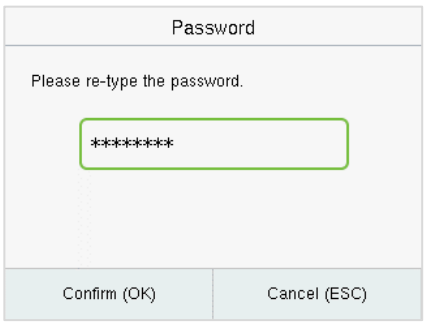


3.1.7 Password

Select **Password** in the **New User** interface to enter the password registration page.

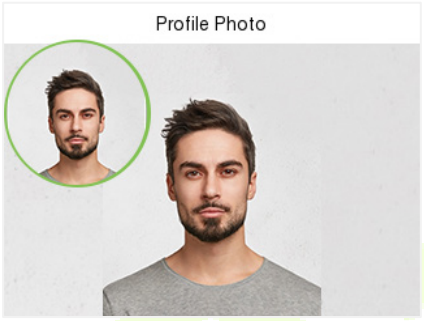
- On the Password interface, enter the required password and re-enter to confirm it and press **M/OK**.
- If the re-entered password is different from the initially entered password, then the device prompts the message as "**Password not match!**", where the user needs to re-confirm the password again.
- The password may contain 6 to 8 digits by default.





3.1.8 Profile Photo★

Select **Profile Photo** in the **New User** interface to go to the Profile Photo registration page.



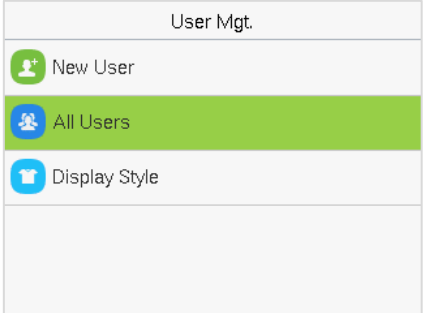
- When a user registered with a photo passes the authentication, the registered photo will be displayed (enter **[System]** > **[Attendance]** to enable **Display User Photo**).
- Press **Profile Photo**, the device's camera will open, then press **M/OK** to take a photo. The captured photo is displayed on the top left corner of the screen. The camera remains active to allow for additional photos if needed.

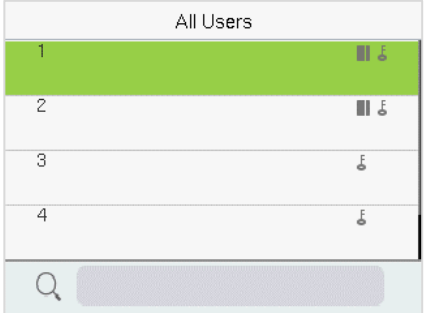
Note: *While registering a face template, the system automatically captures a photo as the user profile photo. If you do not register a profile photo, the system automatically sets the photo captured while registration as the default photo.*

3.2 Search for Users

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

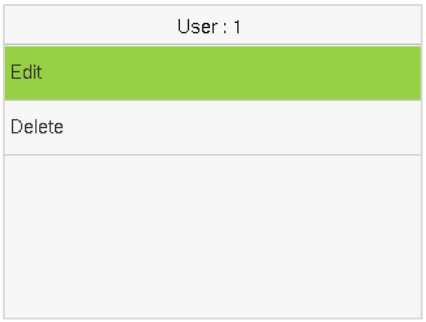
- On the **All Users** interface, select the search bar on the user's list to enter the required retrieval keyword (where the keyword may be the user ID, surname or full name) and the system will search for the related user information.

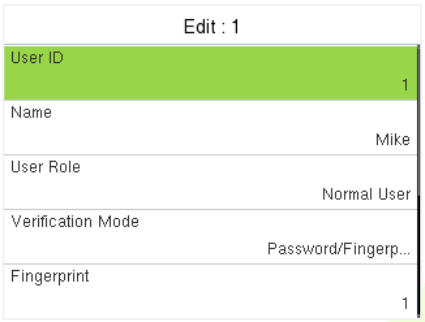




3.3 Edit User

On the **All Users** interface, select the required user from the list and press **M/OK** and select **Edit** to edit the user information.





Note: *The process 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's detail. The process in detail refers to "User Management".*

3.4 Delete User

On the **All Users** interface, select on the required user from the list and press **M/OK** and select **Delete** to delete the user or specific user information from the device. On the **Delete** interface, select on the required operation, and then press **M/OK** to confirm the deletion.

- **Delete operations:**

Delete User: All information of the user will be deleted (deletes the selected User as a whole) from the Device.

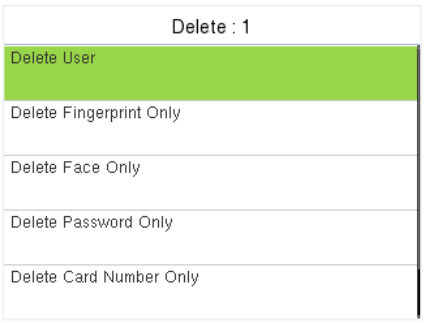
Delete Fingerprint Only: Deletes the fingerprint information of the selected user.

Delete Face Only★: Deletes the face template information of the selected user.

Delete Password Only: Deletes the password information of the selected user.

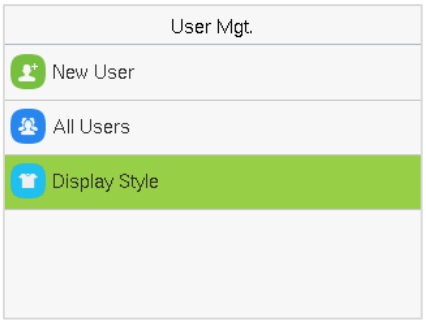
Delete Card Number Only: Deletes the card information of the selected user.

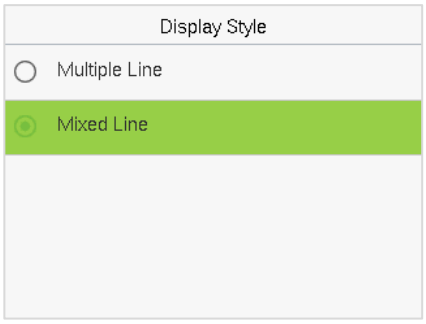
Delete Profile Photo Only★: Deletes the profile photo of the selected user.



3.5 Display Style

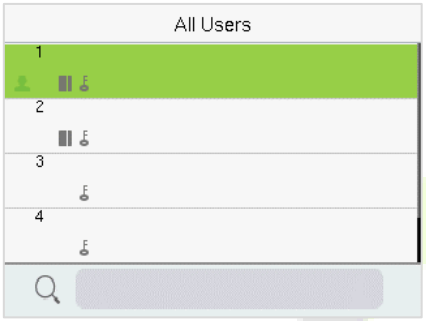
When the device is on the initial interface, press **M/OK** and enter **User Mgt.** > **Display Style**.



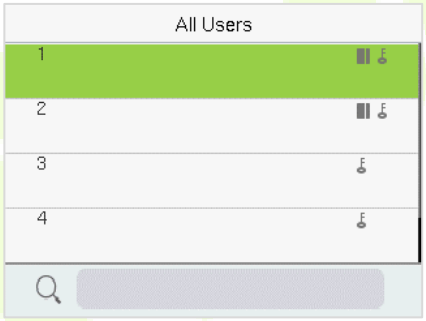


Different display styles are shown as below:

Multiple Line:



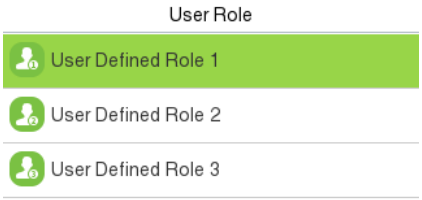
Mixed Line:



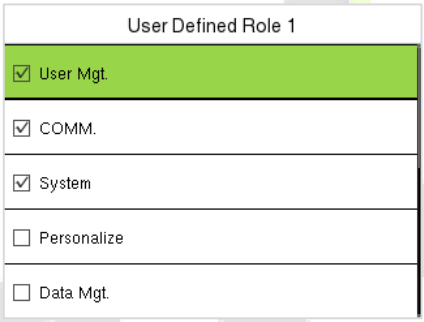
4 User Role

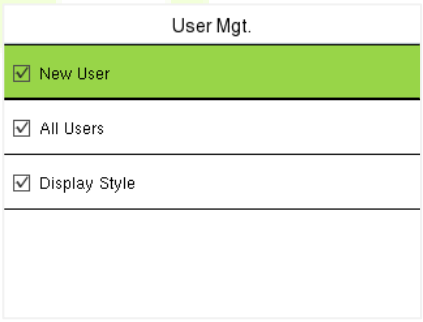
User Role facilitates to assign some specific permissions to specific users, based on the requirement.

- When the device is on the initial interface, press **M/OK** and enter **User Role** > **User Defined Role** to set the user defined permissions.
- The permission scope of the custom role can be set up into 3 roles, that is, the custom operating scope of the menu functions of the user.



- Then, by selecting on Define User Role, select the required privileges for the new role, and then press the **M/OK** key.
- First select the required **Main Menu** function name, then press **M/OK** and select its required sub-menus from the list.



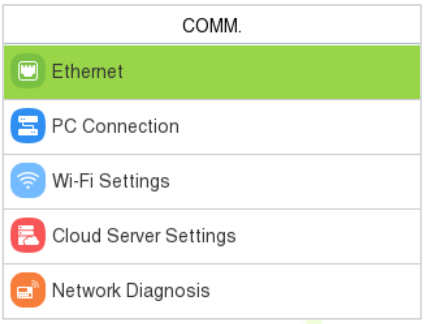


Note: *If the User Role is enabled for the Device, press* ***User Mgt. > New User > User Role*** *to assign the created roles to the required users. But if there is no super administrator registered in the Device, then the device will prompt "Please enroll super admin first!" when enabling the User Role function.*

5 Communication Settings

Communication Settings are used to set the parameters of the Network, PC Connection, Wi-Fi★, Cloud Server, and Network Diagnosis.

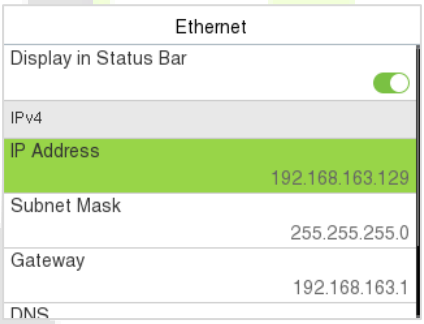
When the device is on the initial interface, press **M/OK** and select **COMM.**



5.1 Network Settings

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

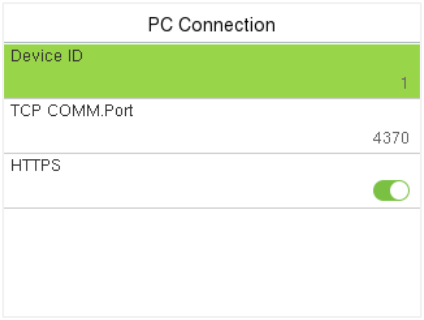
Select **Ethernet** on the **COMM.** Settings interface to configure the settings.



Function Name	Descriptions
Display in Status Bar	Toggle to set whether to display the network icon on the status bar.
IP Address	The default IP address is 192.168.1.201. It can be modified according to the network availability.
Subnet Mask	The default Subnet Mask is 255.255.255.0. It can be modified according to the network availability.
Gateway	The default Gateway address is 0.0.0.0. It can be modified according to the network availability.
DNS	The default DNS address is 0.0.0.0. It can be modified according to the network availability.
DHCP	Dynamic Host Configuration Protocol is to dynamically allocate IP addresses for clients via server.

5.2 PC Connection

Select **PC Connection** on the **COMM.** Settings interface to configure the communication settings.



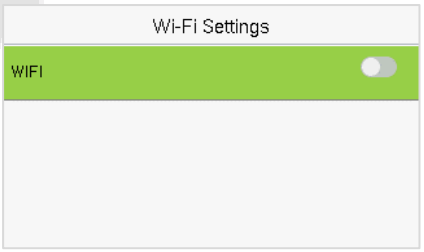
Function Name	Descriptions
Device ID	The identity number of the device, which ranges between 1 and 254.
TCP COMM. Port	The default TCP COMM Port value is 4370. It can be modified according to the network availability.
HTTPS	To increase the security of software access, users can enable the HTTPS protocol to create a secure and encrypted network transmission and assure the security of sent data through identity authentication and encrypted communication. 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.

5.3 Wireless Network★

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

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

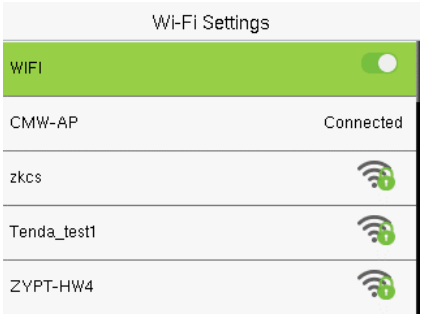
Select **Wi-Fi Settings** on the **COMM.** Settings interface to configure the Wi-Fi settings.



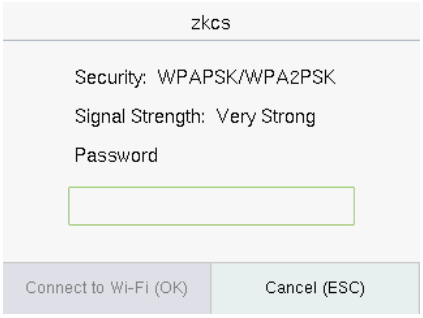
➢ **Search the WIFI Network**

- WIFI is enabled in the Device by default. Toggle on button to enable or disable WIFI.
- Once the Wi-Fi is turned on, the device will search for the available WIFI within the network range.

- Choose the appropriate Wi-Fi name from the available list, and input the correct password in the password interface, and then press **M/OK**.



WIFI Enabled: Press on the required network from the searched network list.



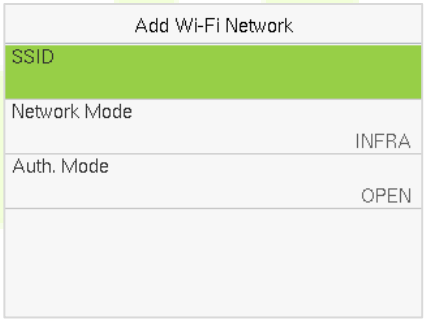
Press on the password field to enter the password, and then press on **M/OK.**

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

➢ Add WIFI Network Manually

The Wi-Fi can also be added manually if the required Wi-Fi does not show on the list.

Press on **Add WIFI Network** to add the WIFI manually.

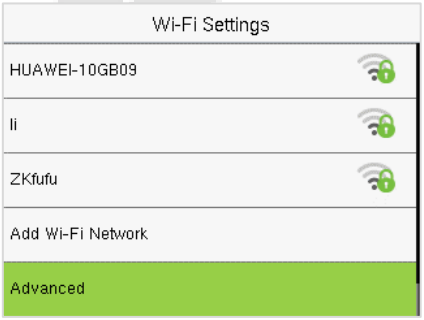


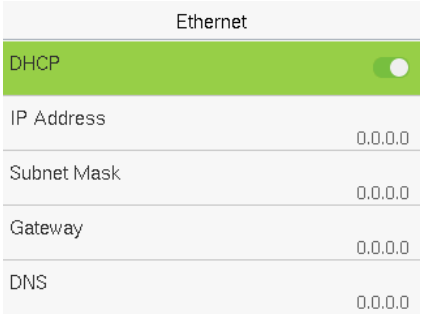
On this interface template, enter the WIFI network parameters. (The added network must exist.)

***Note**: After successfully adding the WIFI manually, follow the same process to search for the added WIFI name.*

➢ Advanced Setting

On the **Wireless Network** interface, press on **Advanced** to set the relevant parameters as required.

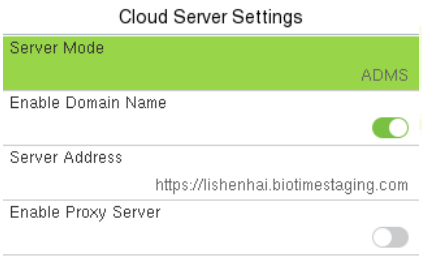




Function Name	Description
DHCP	Dynamic Host Configuration Protocol (DHCP) dynamically allocates IP addresses to network clients. If the DHCP is enabled, then the IP cannot be set manually.
IP Address	IP address for the WIFI network, the default is 0.0.0.0. It can be modified according to the network availability.
Subnet Mask	The default Subnet Mask of the WIFI network is 255.255.255.0. It can be modified according to the network availability.
Gateway	The default Gateway address is 0.0.0.0. Can be modified according to the network availability.
DNS	The default DNS address is 0.0.0.0. It can be modified according to the network availability.

5.4 Cloud Server Setting

Press **Cloud Server Setting** on the **Comm.** Settings interface to connect with the ADMS server.



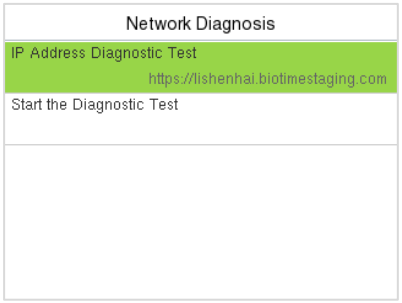
Function Name		Description
Enable Domain Name	**Server Address**	Once this function is enabled, the domain name mode “https://...” will be used, such as https://www.XYZ.com, while “XYZ” denotes the domain name (when this mode is turned ON).
Disable Domain Name	**Server Address**	IP address of the ADMS 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.

Note: When pairing the device with the BioTime Cloud software, you need to enable Domain Name and enter the correct server address.

5.5 Network Diagnosis

It helps to set the network diagnosis parameters.

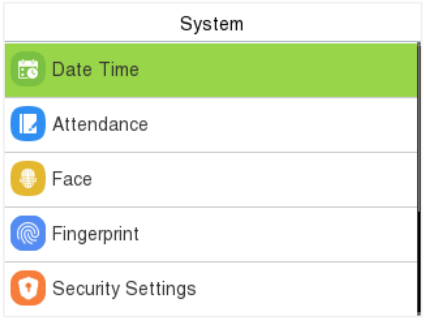
Select **Network Diagnosis** on the **COMM.** Settings interface. Enter the IP address that needs to be diagnosed and press **Start the Diagnostic Test** to check whether the network can connect to the device.

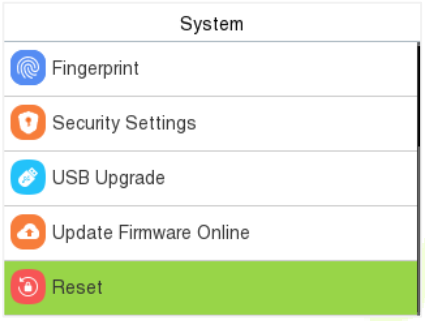


6 System Settings

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

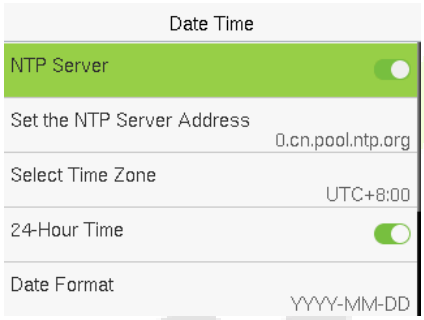
When the device is on the initial interface, press **M/OK** and select **System.**

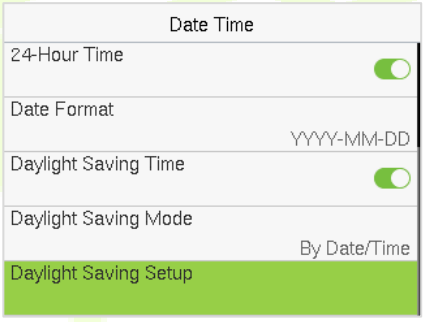




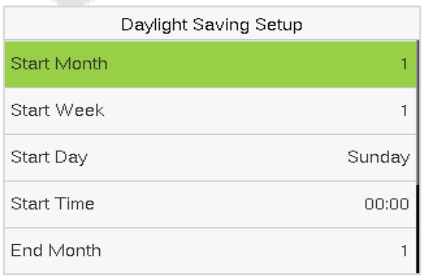
6.1 Date and Time

Select **Date Time** on the **System** interface to set the date and time.

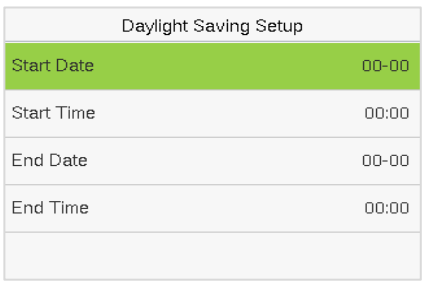




- Press **NTP Server** to enable automatic time synchronization based on the service address you enter.
- Press **Manual Date and Time** to manually set the date and time and then press **M/OK** and save.
- Press **Select Time Zone** to manually select the time zone where the device is located.
- Enable or disable this format by select 24-Hour Time. If enabled, then press **Date Format** to set the date.
- Press **Daylight Saving Time** to enable or disable the function. If enabled, press **Daylight Saving Mode** to select a daylight-saving mode and then press **Daylight Saving Setup** to set the switch time.



Week Mode



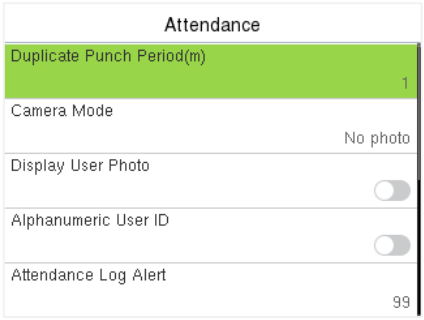
Date Mode

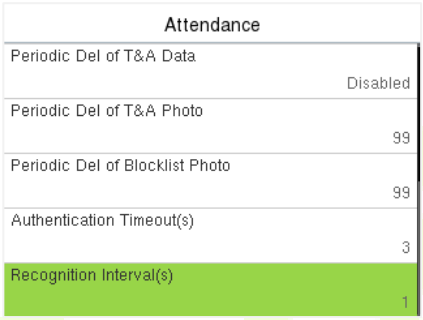
- When restoring the factory settings, the time (24-hour) and date format (YYYY-MM-DD) can be restored, but the device date and time cannot be restored.

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 Attendance

Select **Attendance** on the System interface.



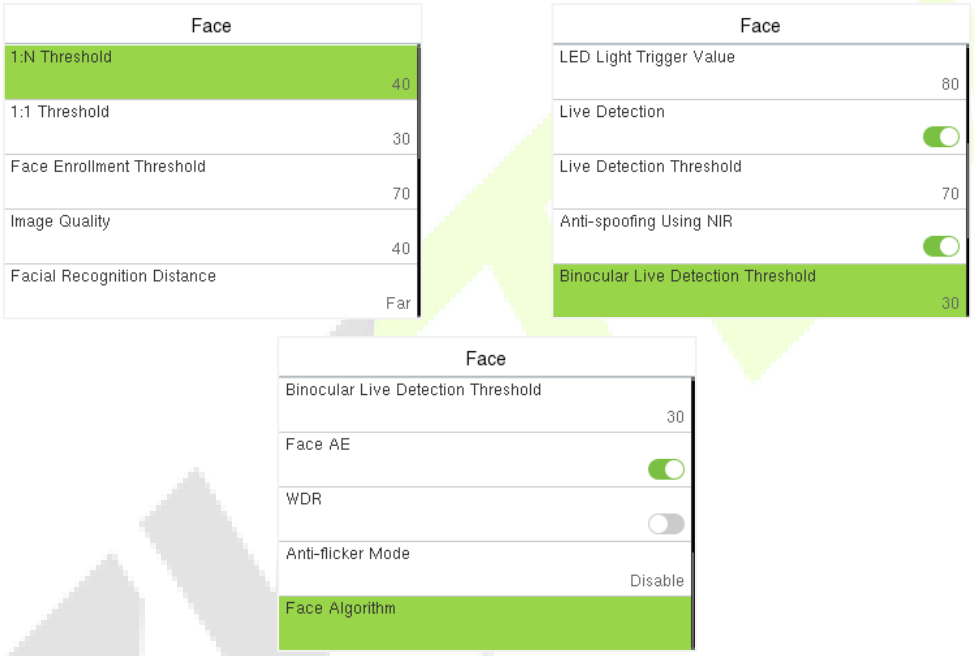


Function Name	Description
Duplicate Punch Period(m)	Within a set time period (unit: minutes), the duplicated attendance record will not be reserved (value ranges from 1 to 999999 minutes).
Camera Mode★	This function is disabled by default. When enabled, a security prompt will pop-up and the sound of shutter in the camera will turn on mandatorily. There are 5 modes: **No photo**: No photo is taken during user verification. **Take photo, no save**: Photo is taken but not saved during verification. **Take photo and save**: All the photos taken during verification is saved. **Save on successful verification**: Photo is taken and saved for each successful verification. **Save on failed verification**: Photo is taken and saved only for each failed verification.
Display User Photo	This function is disabled by default. When enabled, a security prompt will pop-up.
Alphanumeric User ID	Enable/Disable the alphanumeric as User ID.
Attendance Log Alert	When the record space of the attendance reaches the maximum threshold value, the device automatically displays the memory space warning. Users may disable the function or set a valid value between 1 and 9999.
Periodic Del of T&A Data	When attendance records reach its maximum storage capacity, the device automatically deletes a set of old attendance records. Users may disable the function or set a valid value between 1 and 999.
Periodic Del of T&A Photo★	When attendance photos reach its maximum storage capacity, the device automatically deletes a set of old attendance photos. Users may disable the function or set a valid value between 1 and 99.

Periodic Del of Blocklist Photo★	When blocklisted photos reach its maximum storage capacity, the device automatically deletes a set of old block listed photos. Users may disable the function or set a valid value between 1 and 99.
Authentication Timeout(s)	The amount of time taken to display a successful verification message. Valid value: 1~9 seconds.
Recognition Interval(s) ★	After the interval identifying is clicked (selected), for example, if the comparison interval is set to 5 seconds, then the face recognition will verify the face every 5 seconds. Valid value: 0 to 9 seconds. 0 means continuous identifying, 1 to 9 means identifying at intervals.

6.3 Face Template Parameters★

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



Function Name	Description
1:N 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 0 to 100. The higher the thresholds, the lower the misjudgement rate, the higher the rejection rate, and vice versa. It is recommended to set the default value of 40.
1:1 Threshold	Under 1:1 verification mode, the verification will only be successful when the similarity between the acquired facial image and the user's facial templates enrolled in the device is greater than the set value. The valid value ranges from 0 to 100. The higher the thresholds, the lower the misjudgement rate, the higher the rejection rate, and vice versa. It is recommended to set the default value of 30.

Face Enrollment Threshold	During face template enrollment, 1:N comparison is used to determine whether the user has already registered before. When the similarity between the acquired facial image and all registered facial templates is greater than this threshold, it indicates that the face template has already been registered.
Image Quality	Image quality for facial registration and comparison. The higher the value, the clearer the image requires.
Facial Recognition Distance	The farther the individual is, the smaller the face, and the smaller number of pixels of the face obtained by the algorithm. Therefore, adjusting this parameter can adjust the farthest comparison distance of faces.
LED Light Trigger Value	This value controls the turning on and off of the LED light. The larger the value, the LED light will turn on or off more frequently.
Live Detection	It detects the spoof attempt using visible light images to determine if the provided biometric source sample is of a real person (a live human being) or a false representation.
Live Detection Threshold	It facilitates judging whether the captured visible image is a real person (a live human being). The larger the value, the better the anti-spoofing performance using visible light.
Anti-spoofing Using NIR	Using near-infrared spectra imaging to identify and prevent fake photos and videos attack.
Binocular Live Detection Threshold	It is convenient to judge whether the near-infrared spectral imaging is fake photo and video. The larger the value, the better the anti-spoofing performance of near-infrared spectral imaging.
Face AE	When the face is in front of the camera in Face AE mode, the brightness of the face area increases, while the other areas become darker.
WDR	Wide Dynamic Range (WDR) balances light and extends image visibility for surveillance videos under high contrast lighting scenes and improves object identification under bright and dark environments.
Anti-flicker Mode	Used when WDR is turned off. This helps reduce flicker when the device's screen flashes at the same frequency as the light.
Face Algorithm	Facial algorithm related information and pause facial template update.

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

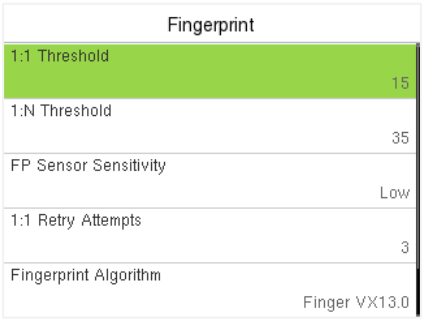
➢ **Process to modify the Face Recognition Accuracy**

- On the **System** interface, press on **Face** and then toggle to enable **Anti-Spoofing using NIR** to set the anti-spoofing.
- Then, on the **Main Menu**, press **Autotest > Test Face** and perform the face test.
- Press three times for the scores on the right upper corner of the screen, and the red rectangular box appears to start adjusting the mode.

- Keep one arm distance between the device and the face. It is recommended not to move the face in a wide range.

6.4 Fingerprint Parameters

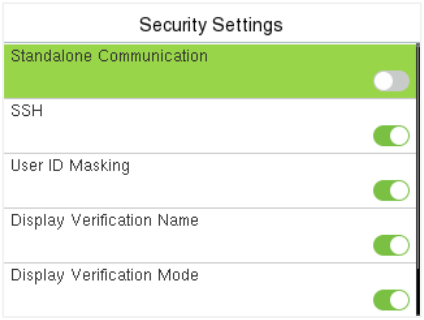
Select **Fingerprint** on the **System** interface to go to the Fingerprint parameter settings.



Function Name	Descriptions
1:1 Threshold	Under 1:1 verification method, the verification will only be successful when the similarity between the acquired fingerprint data and the fingerprint template associated with the entered user ID enrolled in the device is greater than the set value.
1:N Threshold	Under 1:N verification method, the verification will only be successful when the similarity between the acquired fingerprint data and the fingerprint templates enrolled in the device is greater than the set value.
FP Sensor Sensitivity	To set 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 Attempts	In 1:1 Verification, users might forget the registered fingerprint, or press the finger improperly. To reduce the process of re-entering user ID, retry is allowed.
Fingerprint Algorithm	Fingerprint algorithm version. Default support ZKFinger VX13.0, can change to ZKFinger VX10.0.
Fingerprint Image	This function is disabled by default. After disabling it, the fingerprint image will not be displayed when registering and verifying fingerprints. The menu interface allows to enable or disable this function, and there are security prompts when switching. Four choices are available: **Show for Enroll**: to display the fingerprint image on the screen only during enrollment. **Show for Match**: to display the fingerprint image on the screen only during verification. **Always Show**: to display the fingerprint image on screen during enrollment and verification. **None**: not to display the fingerprint image.

6.5 Security Settings

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



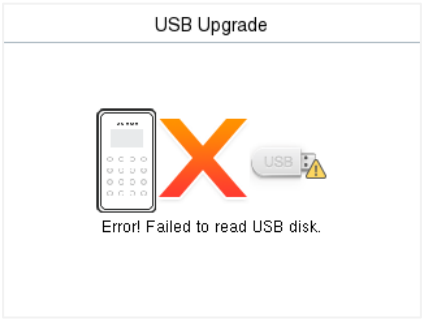
Function Name	Description
Standalone Communication	By default, this function is disabled. This function can be enabled or disabled via the menu interface. When it is switched on, a security prompt appears, and the device will restart after you confirm.
SSH	The device does not support the Telnet feature, 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.
Save Photo as Template	After disabling this function, face template re-registration is required after an algorithm upgrade.

6.6 USB Upgrade

Select **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.

If no USB disk is inserted in, the system gives the following prompt after you press **USB Upgrade** on the System interface.



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

6.7 Update Firmware Online

Press **Update Firmware Online** on the System interface.

Press **Enable Firmware Update Online** function, the device will prompt that the update may bring some data security risks, which requires manual confirmation by the user.

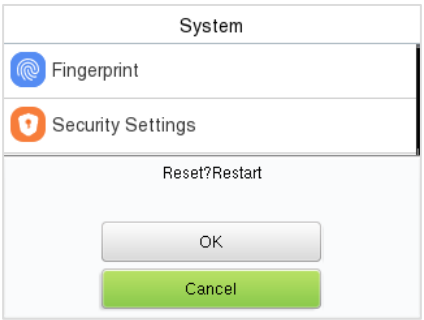
Press **Check for Updates** it may have the following 3 scenarios:

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

6.8 Factory Reset

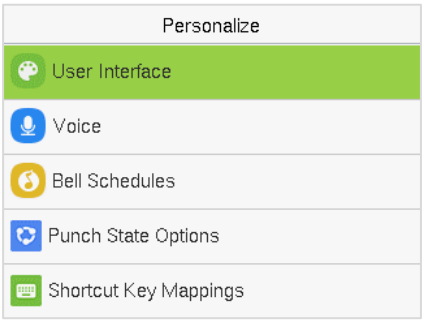
The Factory Reset function restores the device settings such as communication settings and system settings, to the default factory settings (This function does not clear registered user data).

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



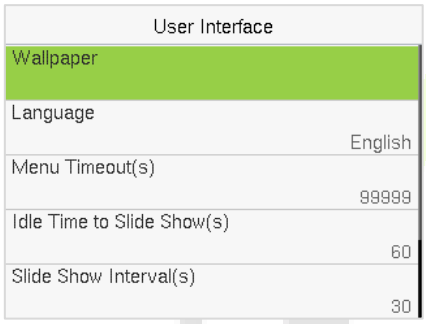
7 Personalize Settings

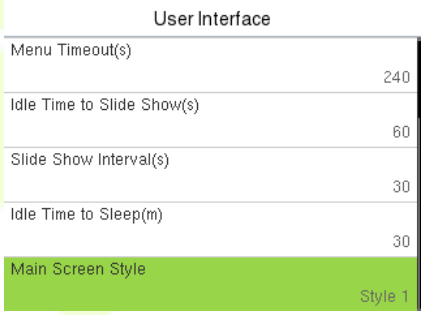
When the device is on the initial interface, press **M/OK** and select **Personalize** to customize the interface settings, voice, bell, punch state options, and shortcut key mappings.



7.1 User Interface Settings

Select **User Interface** on the **Personalize** interface to customize the display style of the main interface.

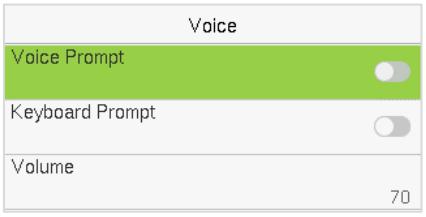




Function Name	Description
Wallpaper	The main screen wallpaper can be selected according to the user preference.
Language	Select the language of the device.
Menu Timeout (s)	When there is no operation, and the time exceeds the set value, the device will automatically go back to the initial interface. The function either can be disabled or set the required value between 60 and 99999 seconds.
Idle Time to Slide Show (s)	When there is no operation, and the time exceeds the set value, a slide show will be played. The function can be disabled, or you may set the value between 3 and 999 seconds.
Slide Show Interval (s)	It is the time interval in switching between different slide show photos. The function can be disabled, or you may set the interval between 3 and 999 seconds.
Idle Time to Sleep (m)	If the sleep mode is activated, and when there is no operation in the device, then the device will enter standby mode. This function can be disabled or set a value within 1-999 minutes.
Main Screen Style	The main screen style can be selected according to the user preference.

7.2 Voice Settings

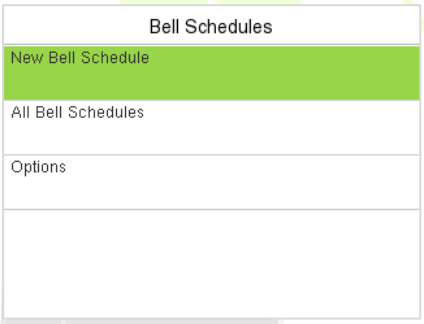
Select **Voice** on the **Personalize** interface to configure the voice settings.



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

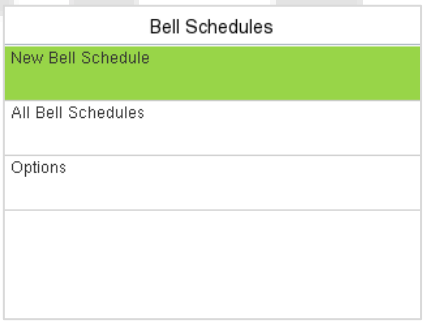
7.3 Bell Schedules

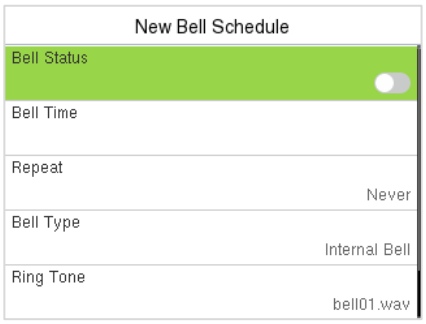
Select **Bell Schedules** on the **Personalize** interface to configure the Bell settings.



➢ **New Bell Schedule**

Select **New Bell Schedule** on the **Bell Schedule** interface to add a new bell schedule.





Function Name	Description
Bell Status	Toggle to enable or disable the bell status.
Bell Time	Once the required time is set, the device will automatically trigger to ring the bell during that time.
Repeat	Set the required number of counts to repeat the scheduled bell.

Bell Type	Select the bell type: Internal Bell, External Bell or Internal and External Bell.
Ring Tone	Select a ring tone.
Internal Bell Delay(s)	Set the replay time of the internal bell. Valid values range from 1 to 999 seconds.

➢ **All Bell Schedules:**

Once the bell is scheduled, on the **Bell Schedules** interface, press **All Bell Schedules** to view the newly scheduled bell.

➢ **Edit the Scheduled Bell:**

On the **All Bell Schedules** interface, select on the required bell schedule, and select **Edit** to edit the selected bell schedule. The editing method is the same as the operations of adding a new bell schedule.

➢ **Delete a Bell:**

On the **All Bell Schedules** interface, select the required bell schedule, and select **Delete**, and then press **M/OK** to delete the selected bell.

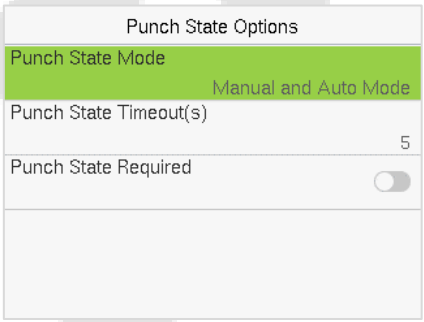
➢ **Options:**

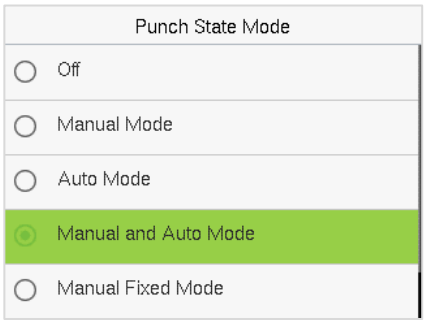
Select **Options** on the **Bell Schedule** interface to set the external bell output terminal NC1/NO1, which is disabled by default.

Note: The external bell and the lock are mutually exclusive options. When the external bell function is enabled, be careful not to connect the wrong wire.

7.4 Punch States Options

Select **Punch States Options** on the **Personalize** interface to configure the punch state settings.





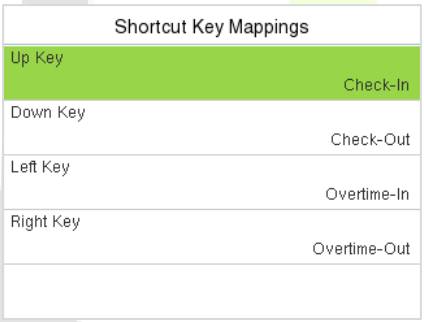
Function Name	Description
Punch State Mode	**Off:** Disable the punch state function. Therefore, the punch state key set under **Shortcut Key Mappings** menu will become invalid. **Manual Mode:** Switch the punch state key manually, and the punch state key will disappear after **Punch State Timeout**. **Auto Mode:** The punch state key will automatically switch to a specific punch status according to the predefined time schedule which can be set in the Shortcut Key Mappings.

	Manual and Auto Mode: The main interface will display the auto-switch punch state key. However, the users will still be able to select alternative that is the manual attendance status. After timeout, the manual switching punch state key will become auto-switch punch state key. **Manual Fixed Mode:** After the punch state key is set manually to a particular punch status, the function will remain unchanged until being manually switched again. **Fixed Mode:** Only the manually fixed punch state key will be shown. Users cannot change the status by pressing any other keys.
Punch State Timeout(s)	It is the time for which the punch state displays. The value ranges from 5 to 999 seconds.
Punch State Required	Select whether an attendance state needs to be selected after verification. **ON:** Attendance state needs to be selected after verification. **OFF:** Attendance state need not requires to be selected after verification.

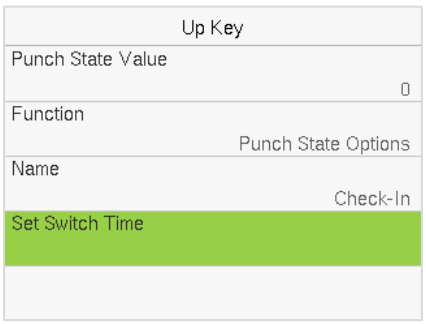
7.5 Shortcut Key Mappings

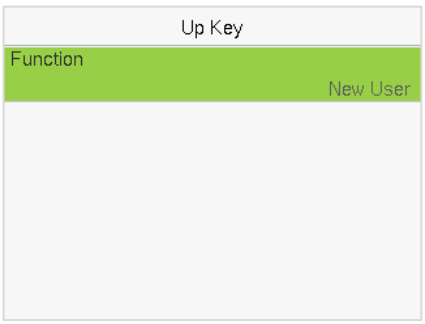
Users may define shortcut keys for attendance status and for functional keys which will be defined on the main interface. So, on the main interface, when the shortcut keys are pressed, the corresponding attendance status or the function interface will be displayed directly.

Select **Shortcut Key Mappings** on the **Personalize** interface to set the required shortcut keys.



- On the **Shortcut Key Mappings** interface, select the required shortcut key to configure the shortcut key settings.
- On the **Shortcut Key** interface, press **Function** to set the functional process of the shortcut key either as punch state key or function key.
- If the Shortcut key is defined as a function key (such as New user, All users, etc.), the configuration is completed as shown in the image below.

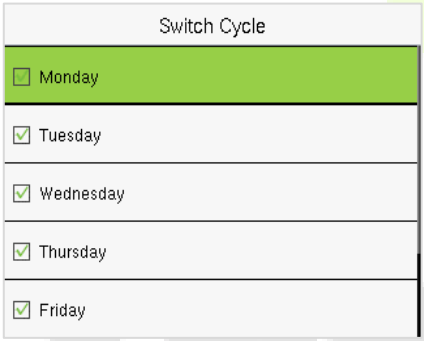


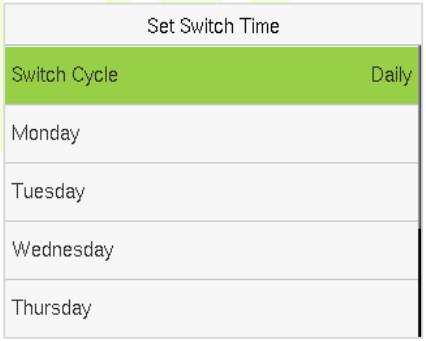


- If the Shortcut key is set as a punch state key (such as check in, check out, etc.), then it is required to set the punch state value (valid value 0~250), name.

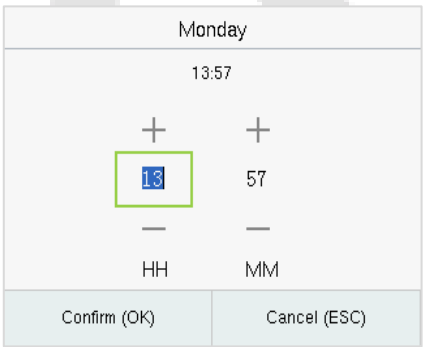
➢ **Set the Switch Time**

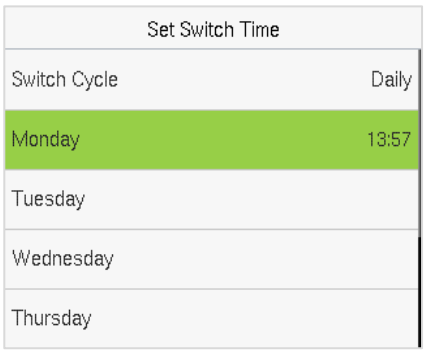
- The switch time is set in accordance with the punch state options.
- When the **Punch State Mode** is set to **Auto Mode**, the switch time should be set.
- On the **Shortcut Key** interface, press **Set Switch Time** to set the switch time.
- On the **Switch Cycle** interface, select the switch cycle (Monday, Tuesday, etc.) as shown in the image below.





- Once the Switch cycle is selected, set the switch time for each day, and press **M/OK** to confirm, as shown in the image below.

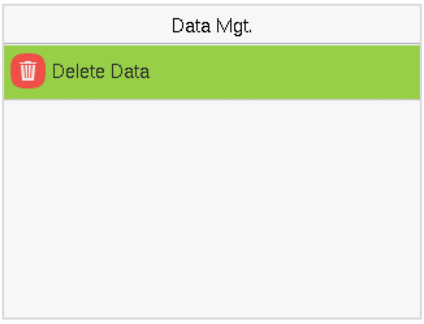




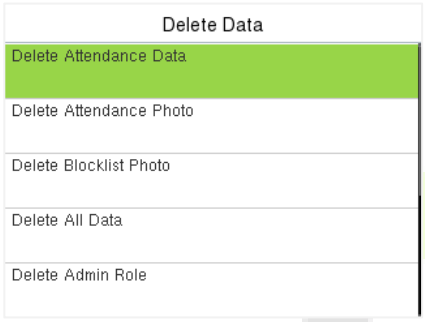
Note: *When the function is set to Undefined, the device will not enable the punch state key.*

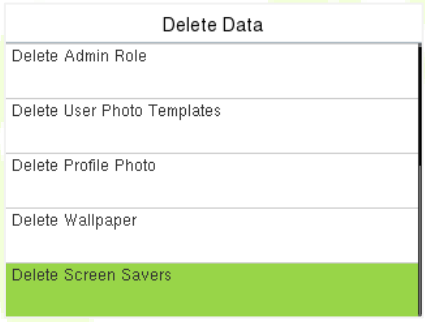
8 Data Management

When the device is on the initial interface, press **M/OK** and select **Data Mgt.** to manage the relevant data in the device.



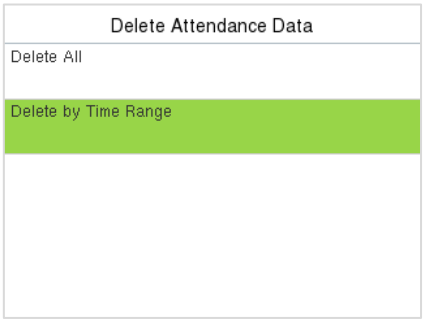
Select **Delete Data** on the **Data Mgt.** interface to delete the required data.





Function Name	Description
Delete Attendance Data	To delete attendance data 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 of all registered users.
Delete Admin Role	To remove all administrator privileges.
Delete User Photo Templates★	To delete user photo templates in the device. 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.

The user may select **Delete All** or **Delete by Time Range** when deleting the attendance data, attendance photos★ or block listed photo★s. Selecting **Delete by Time Range**, you need to set a specific time range to delete all data within a specific period.



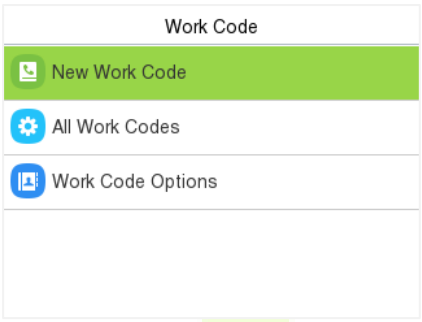
Select **Delete by Time Range**.

Set the time range and press **M/OK**.

9 Work Code

Employees' salaries are subject to their attendance records. An employee can be engaged in more than one type of work which may vary with time. As the pay varies according to the work types, the FFR terminal provides a parameter to indicate the corresponding work type for every attendance record to facilitate rapid understanding of different attendance situations during the handling of attendance data.

Select **Work Code** on the main menu interface.



9.1 Add a Work Code

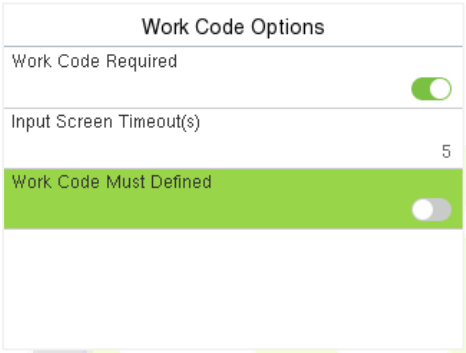
Menu	Description
ID	It is the digital code of the work code. Users may set a valid value between 1 and 99999999.
Name	It is the naming of the work code.

9.2 All Work Codes

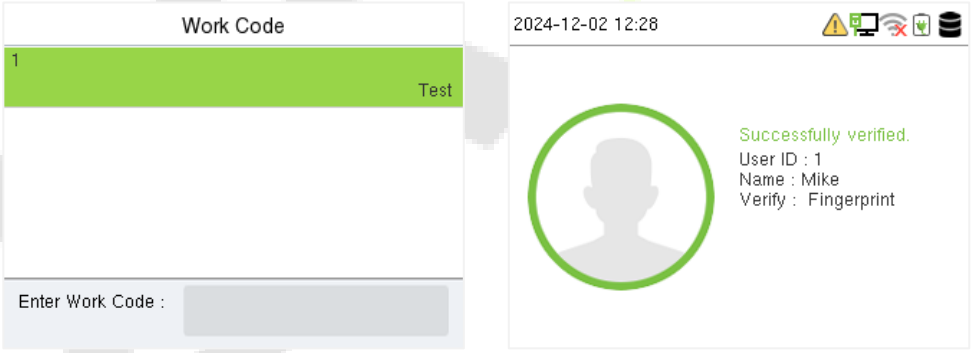
You can view, edit and delete work codes in All Work Codes. The process of editing a work code is the same as adding a work code, except that the ID is not allowed to be modified.

9.3 Work Code Options

To set whether entering the work code is a must and whether the entered work code must exist during authentication.



In **1: N** or **1:1** verification, the system will automatically pop up the following window. Select the corresponding Word Code manually to verify successfully.

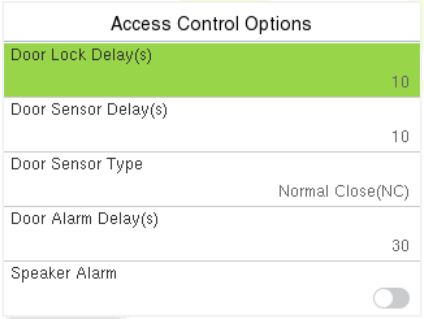


10 Access Control

When the device is on the initial interface, press **M/OK** and select **Access Control** to set the locks control and to configure other parameters settings related to access control.

10.1 Access Control Options

Select **Access Control Options** on the **Access Control** interface to set the parameters of the control lock of the terminal and related equipment.



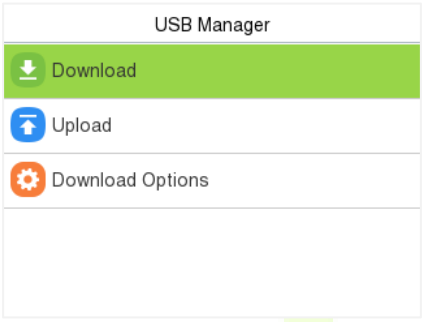
Function Name	Description
Door Lock Delay (s)	The length of time that the device controls the electric lock to be in unlock state. Valid value: 1~10 seconds; 0 seconds represents disabling the function.
Door Sensor Delay (s)	If the door is not locked and is left open for a certain duration (Door Sensor Delay), an alarm will be triggered. The valid value of Door Sensor Delay ranges from 1 to 255 seconds.
Door Sensor Type	There are three Sensor types: **None**, **Normal Open(NO)**, and **Normal Closed(NC)**. **None:** It means the door sensor is not in use. **Normally Open(NO):** It means the door is always left open when electric power is on. **Normally Closed(NC):** It means the door is always left closed when electric power is on.
Door Alarm Delay(s)	When the state of the door sensor is inconsistent with that of the door sensor type, alarm will be triggered after a time period; this time period is the Door Alarm Delay (the value ranges from 0 to 999 seconds).
Speaker Alarm	It transmits a sound alarm or disassembly alarm from the local. When the door is closed or the verification is successful, the system cancels the alarm from the local.

11 USB Manager

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

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

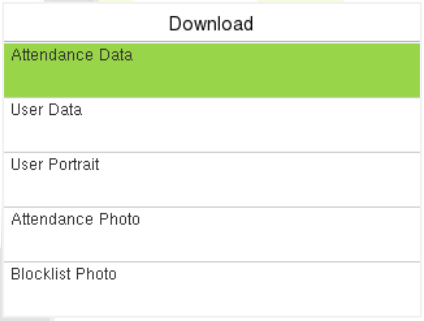
Select **USB Manager** on the main menu interface.



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

11.1 USB Download

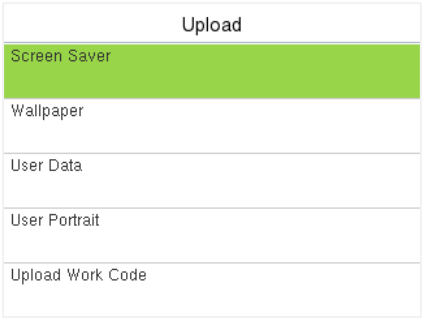
On the **USB Manager** interface, press **Download**.



Function Name	Description
Attendance Data	To download all attendance data in specified time period into USB disk.
User Data	To download all user information from the device into USB disk.
User Portrait	To download all user portraits from the device into USB disk.
Attendance Photo★	To download all attendance photos from the device into USB disk.
Blocklist Photo★	To download all blocklisted photos (photos taken after failed verifications) from the device into USB disk.
Work Code	To download all work code from the device into USB disk.

11.2 USB Upload

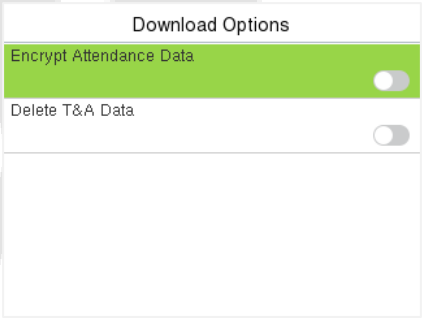
On the **USB Manager** interface, press **Download**.



Function Name	Description
Screen Saver	To upload all screen savers from USB disk into the device. You can choose Upload selected photo or upload all photos. The images will be displayed on the device's main interface after upload.
Wallpaper	To upload all wallpapers from USB disk into the device. You can choose Upload selected photo or upload all photos. The images will be displayed on the screen after upload.
User Data	To upload all the user information from USB disk into the device.
User Portrait	To upload all user portraits from USB disk into the device.
Upload Work Code	To upload all work code from USB disk into the device.

11.3 Download Options

On the **USB Manager** interface, press **Download Options**.

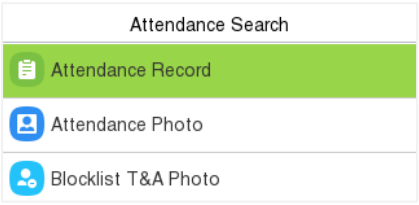


Function Name	Description
Encrypt Attendance Date	The attendance data is encrypted during the uploading and downloading.
Delete T&A Data	After successful downloading, the attendance data on the device is deleted.

12 Attendance Search

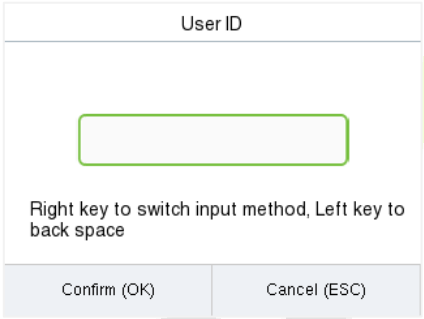
Once the identity of a user is verified, the Event Logs will be saved in the device. This function enables users to check their attendance records.

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

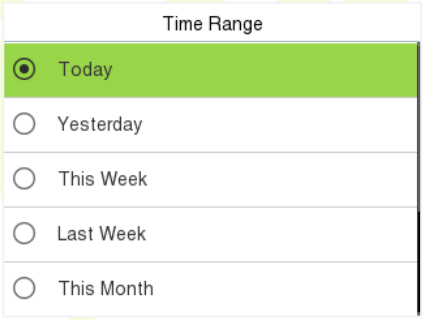


The process of searching for attendance and blocklist photos★ is similar to that of searching for event logs. The following is an example of searching for attendance record.

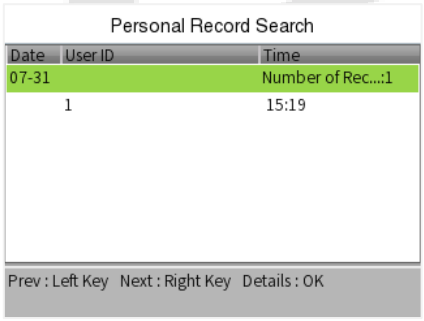
On the **Attendance Search** interface, press **Attendance Record** to search for the required record.



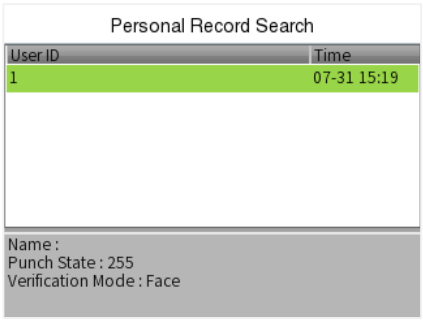
1. Enter the user ID to be searched and press **M/OK**. If you want to search for records of all users, press **M/OK** without entering any user ID.



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



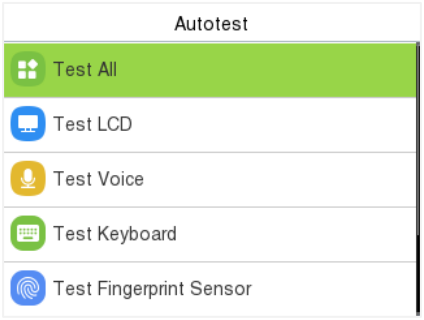
3. Once the record search completes. Press the record highlighted in green to view its details.



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

13 Autotest

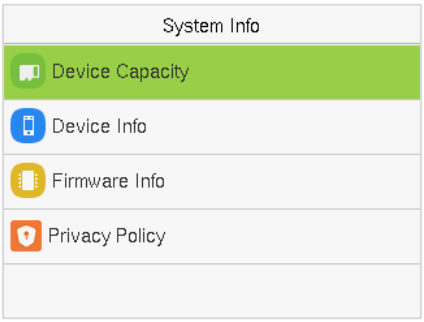
When the device is on the initial interface, press **M/OK** and select **Autotest**, it enables the system to automatically test whether the functions of various modules are working normally, including the LCD, Voice, Keyboard, Fingerprint, Camera★ and Real-Time Clock (RTC).



Function Name	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 colors normally.
Test Voice	To automatically test whether the audio files stored in the device are complete and the voice quality is good.
Test Keyboard	The terminal tests whether every key on the keyboard works normally. Press any key on the **Test Keyboard** interface to check whether the pressed key matches the key displayed on the screen. The keys are displayed as dark grey before and turn green after pressed. Press **ESC** to exit the test.
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.
Cam Test★	To test if the camera functions properly by checking the photos taken to see if they are clear enough. (Same as "Test Face".)
Test Clock RTC	To test the RTC. The device tests whether the clock works normally and accurately with a stopwatch. Press **M/OK** to start counting and press it again to stop counting.

14 System Information

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

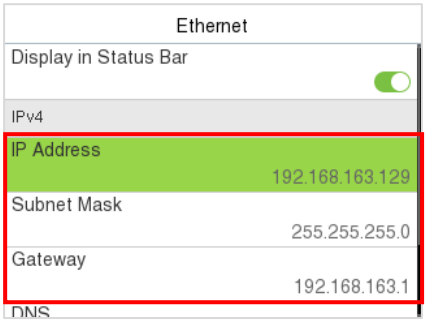


Function Name	Description
Device Capacity	Displays the current device's user storage, password, face template★, fingerprint and card storage, T&A records, attendance and blocklist photos★, and profile photos.
Device Info	Displays the device's name, serial number, MAC address, fingerprint algorithm, face template algorithm★, platform information, MCU Version, BAT MCU and manufacturer.
Firmware Info	Displays the firmware version and other version information of the device.
Privacy Policy	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. ***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.*

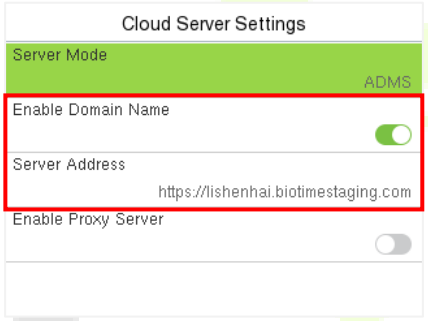
15 Connect to BioTime Cloud Software

15.1 Add Device on the Software

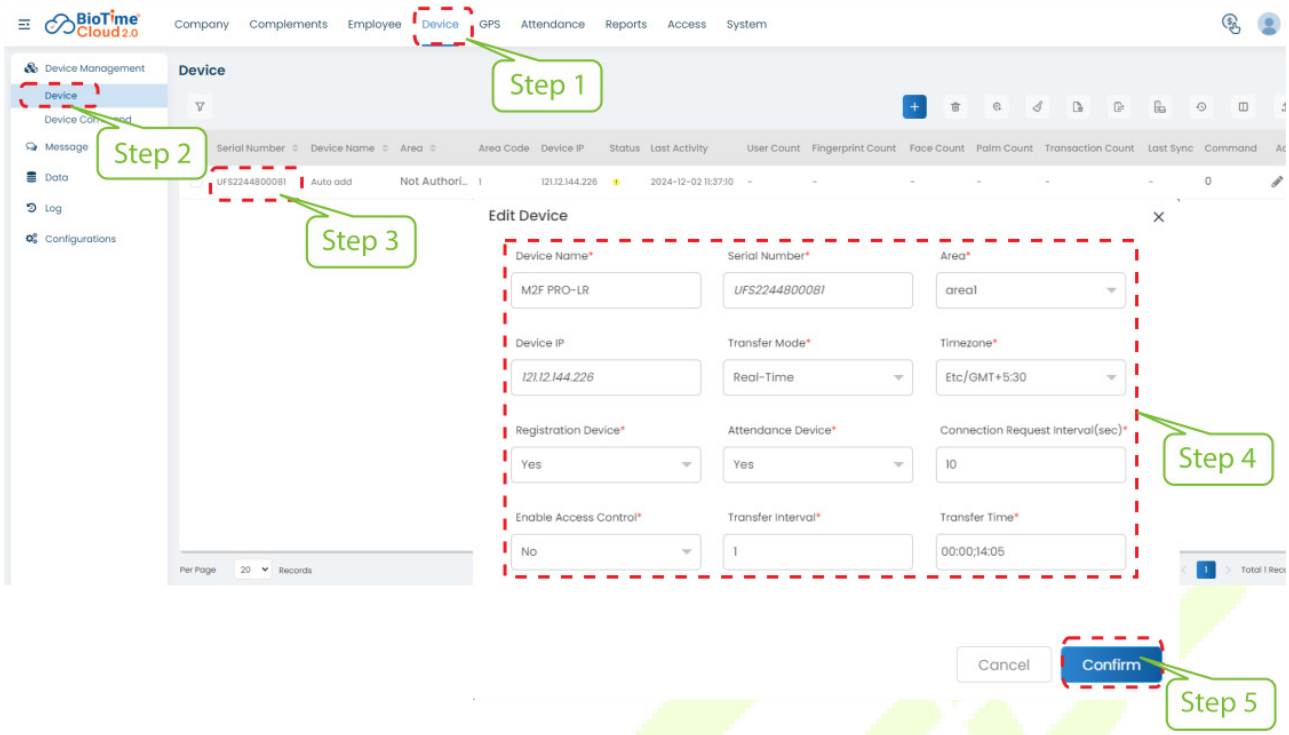
1. Press **COMM.** > **Ethernet** in the main menu to set the IP address and gateway of the device.



2. In the main menu, press **COMM.** > **Cloud Server Settings** to enable Domain Name and enter the correct domain name.

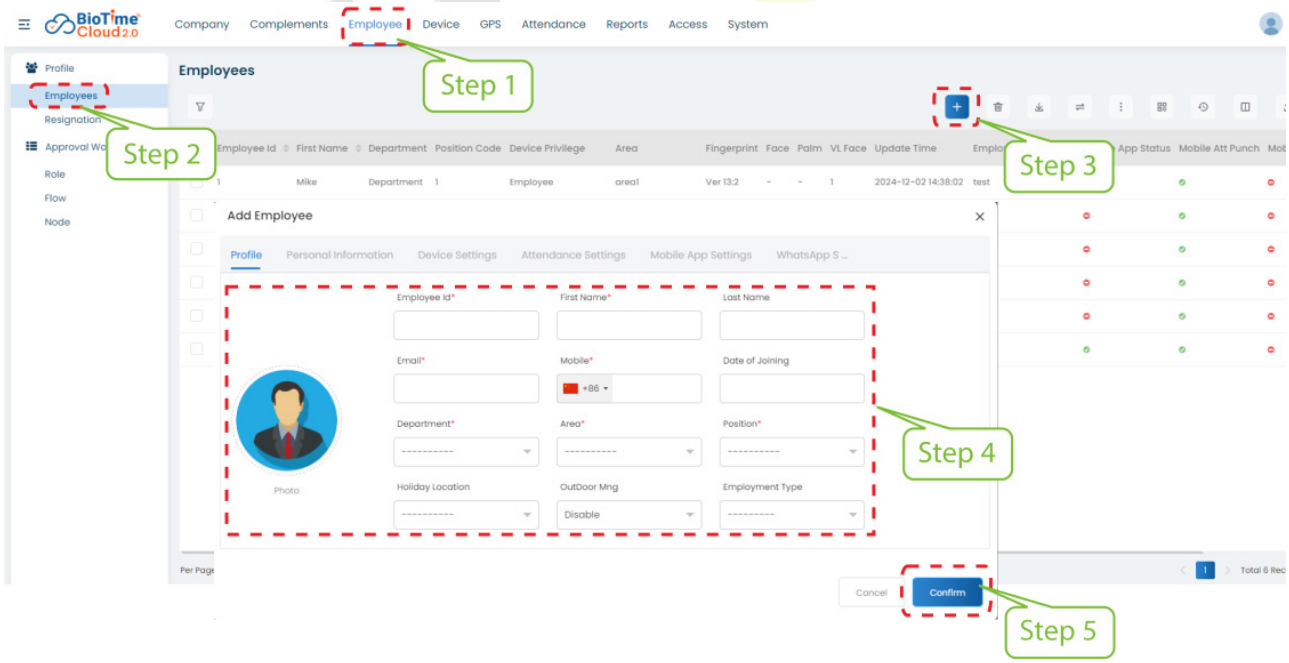


3. After setting on the device, the device will be automatically added to the software. Open BioTime Cloud software, click **Device** > **Device Management** > **Device**, select the device in the list, change the Device Name and Area, then it can communicate with the software.



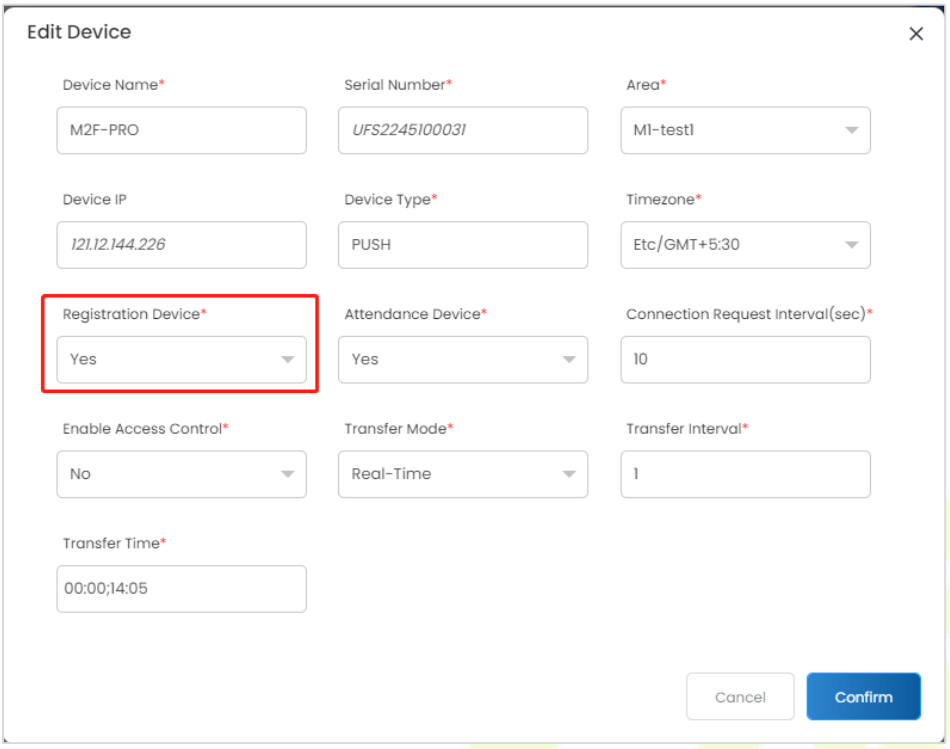
15.2 Add Personnel on the Software and Online Fingerprint Registration

1. Click **Employee** > **Profile** > **Employees** > + icon.

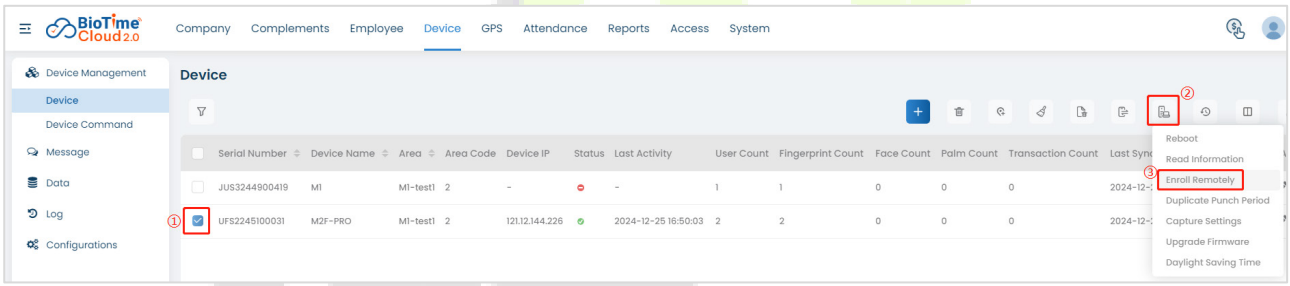


2. Fill in all the required fields and click **Confirm** to register a new user.

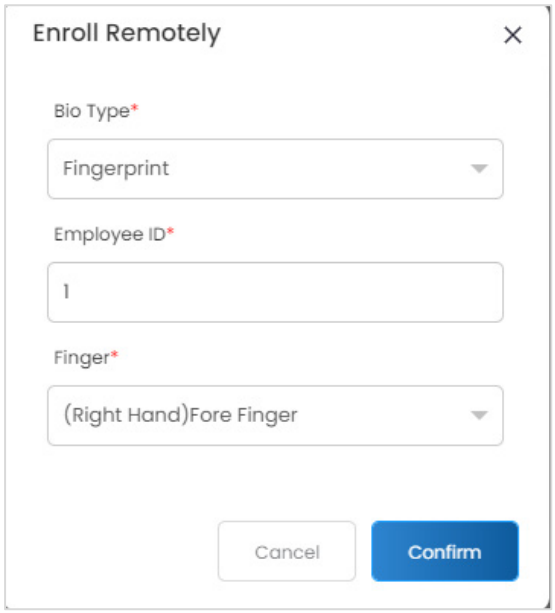
3. Click **Device** > **Device Management** > **Device**, select the device in the list, click icon to enter the Edit Device interface, set the Registration Device as **Yes** and click **Confirm**.



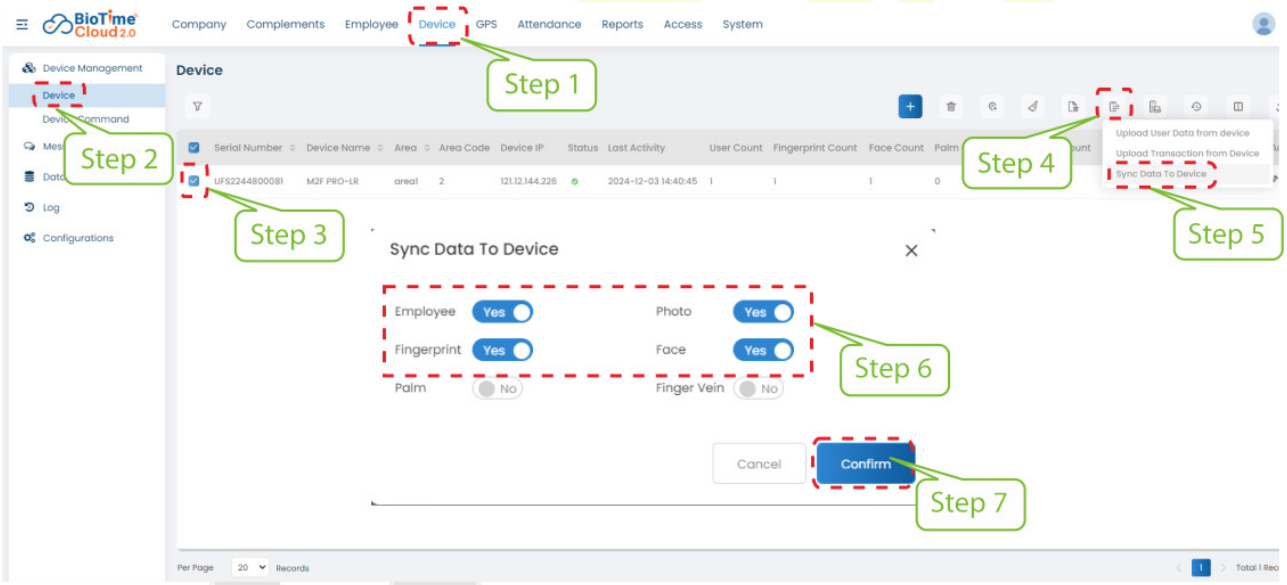
4. Select the device in the list, click icon > **Enroll Remotely.**



5. Enter the Employee ID and select the finger you want to register and press your finger on the fingerprint sensor of the device three times. If the fingerprint is successfully registered, the device will display "Enrolled successfully".



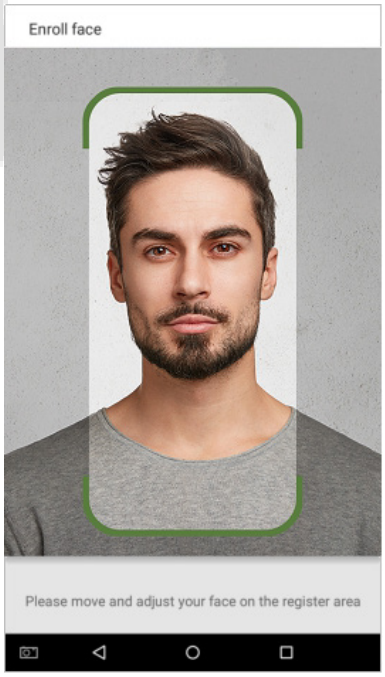
6. Select the device in the list, click icon > **Sync Data to Device** to synchronize all the data into the device including the new users.



Appendix 1

Requirements of Live Collection and Registration of Visible Light Face Templates★

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



Requirements for Visible Light Digital Face Template Data★

The digital photo should be straight-edged, colored, half-portrayed with only one person, and the person should be uncharted and in casuals. Persons who wear eyeglasses should remain to put on eyeglasses for getting photo captured.

- **Eye distance**

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

- **Facial expression**

Neutral face template or smile with eyes naturally open are recommended.

- **Gesture and angle**

Horizontal rotating angle should not exceed ±10°, elevation should not exceed ±10°, and depression angle should not exceed ±10°.

- **Accessories**

Masks or colored eyeglasses are not allowed. The frame of the eyeglasses should not cover eyes and should not reflect light. For persons with thick eyeglasses frame, it is recommended to capture two templates, one with eyeglasses and the other one without the eyeglasses.

- **Face template**

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

- **Template format**

Should be in BMP, JPG or JPEG.

- **Data requirement**

Should comply with the following requirements:

1) White background with dark-colored apparel.
2) 24bit true color mode.
3) JPG format compressed template with not more than 20kb size.
4) Resolution should be between 358 x 441 to 1080 x 1920.
5) The vertical scale of head and body should be in a ratio of 2:1.
6) The photo should include the captured person's shoulders at the same horizontal level.
7) The captured person's eyes should be open and with clearly seen iris.
8) A neutral facial expression or a slight smile is preferred, but showing teeth is not recommended.
9) The captured person should be clearly visible, natural in color, no harsh shadow or light spot or reflection in face template or background. The contrast and lightness level should be appropriate.

Appendix 2

Privacy Policy

Notice:

To help you better use the products and services of ZKTeco (hereinafter referred as "we", "our", or "us") a smart service provider, we consistently collect your personal information. Since we understand the importance of your personal information, we took your privacy sincerely and we have formulated this privacy policy to protect your personal information. We have listed the privacy policies below to precisely understand the data and privacy protection measures related to our smart products and services.

Before using our products and services, please read carefully and understand all the rules and provisions of this Privacy Policy. If you do not agree to the relevant agreement or any of its terms, you must stop using our products and services.

I. Collected Information

To ensure the normal product operation and help the service improvement, we will collect the information voluntarily provided by you or provided as authorized by you during registration and use or generated as a result of your use of services.

1. **User Registration Information:** At your first registration, the feature template (**Fingerprint template/Face template template/Palm template**) will be saved on the device according to the device type you have selected to verify the unique similarity between you and the User ID you have registered. You can optionally enter your Name and Code. The above information is necessary for you to use our products. If you do not provide such information, you cannot use some features of the product regularly.

2. **Product information:** According to the product model and your granted permission when you install and use our services, the related information of the product on which our services are used will be collected when the product is connected to the software, including the Product Model, Firmware Version Number, Product Serial Number, and Product Capacity Information. **When you connect your product to the software, please carefully read the privacy policy for the specific software.**

II. Product Security and Management

1. When you use our products for the first time, you shall set the Administrator privilege before performing specific operations. Otherwise, you will be frequently reminded to set the Administrator privilege when you enter the main menu interface. **If you still do not set the Administrator privilege after receiving the system prompt, you should be aware of the possible security risk (for example, the data may be manually modified).**
2. All the functions of displaying the biometric information are disabled in our products by

default. You can choose Menu > System Settings to set whether to display the biometric information. If you enable these functions, we assume that you are aware of the personal privacy security risks specified in the privacy policy.

3. Only your user ID is displayed by default. You can set whether to display other user verification information (such as Name, Department, Photo, etc.) under the Administrator privilege. **If you choose to display such information, we assume that you are aware of the potential security risks (for example, your photo will be displayed on the device interface).**
4. The camera function is disabled in our products by default. If you want to enable this function to take pictures of yourself for attendance recording or take pictures of strangers for access control, the product will enable the prompt tone of the camera. **Once you enable this function, we assume that you are aware of the potential security risks.**
5. All the data collected by our products is encrypted using the AES 256 algorithm. All the data uploaded by the Administrator to our products are automatically encrypted using the AES 256 algorithm and stored securely. If the Administrator downloads data from our products, we assume that you need to process the data and you have known the potential security risk. In such a case, you shall take the responsibility for storing the data. You shall know that some data cannot be downloaded for sake of data security.
6. All the personal information in our products can be queried, modified, or deleted. If you no longer use our products, please clear your personal data.

III. How we handle personal information of minors

Our products, website and services are mainly designed for adults. Without consent of parents or guardians, minors shall not create their own account. If you are a minor, it is recommended that you ask your parents or guardian to read this Policy carefully, and only use our services or information provided by us with consent of your parents or guardian.

We will only use or disclose personal information of minors collected with their parents' or guardians' consent if and to the extent that such use or disclosure is permitted by law or we have obtained their parents' or guardians' explicit consent, and such use or disclosure is for the purpose of protecting minors.

Upon noticing that we have collected personal information of minors without the prior consent from verifiable parents, we will delete such information as soon as possible.

IV. Others

You can visit https://www.zkteco.com/cn/index/Index/privacy_protection.html to learn more about how we collect, use, and securely store your personal information. To keep pace with the rapid development of technology, adjustment of business operations, and to cope with customer needs, we will constantly deliberate and optimize our privacy protection measures and policies. Welcome to visit our official website at any time to learn our latest privacy policy.

Eco-friendly Operation

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

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

Hazardous or Toxic substances and their quantities

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

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

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

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

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

ZKTeco Industrial Park, No. 32, Industrial Road,

Tangxia Town, Dongguan, China.

Phone : +86 769 - 82109991

Fax : +86 755 - 89602394

www.zkteco.com