

User Manual

M1

Date: February 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.

Copyright © 2025 ZKTECO CO., LTD. All rights reserved.

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

Trademark

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

Disclaimer

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

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

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

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

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

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

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

This manual and the information contained therein may include technical, other inaccuracies or typographical errors. ZKTeco periodically changes the information herein which will be incorporated into new additions/amendments to the manual. ZKTeco reserves the right to add, delete, amend or modify the information contained in the manual from time to time in the form of circulars, letters, notes, etc. for better operation and safety of the machine/unit/equipment. The said additions or amendments are meant for improvement/better operations of the machine/unit/equipment and such

amendments shall not give any right to claim any compensation or damages under any circumstances.

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

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

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

ZKTeco Headquarters

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

Phone +86 769 - 82109991

Fax +86 755 - 89602394

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

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

About the Company

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

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

About the Manual

This manual introduces the operations of **M1**.

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 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	8
SAFETY MEASURES	8
1 INSTRUCTION FOR USE	10
1.1 STANDBY INTERFACE	10
1.2 VERIFICATION MODES	11
1.2.1 FINGERPRINT VERIFICATION	12
1.2.2 CARD NUMBER VERIFICATION	15
1.2.3 PASSWORD VERIFICATION	17
1.3 TEXT INPUT OPERATION	19
1.4 WI-FI CONNECTION	20
2 MAIN MENU	24
3 USER MANAGEMENT	25
3.1 SEARCH FOR USERS	25
4 COMMUNICATION SETTINGS	26
4.1 WIRELESS NETWORK	26
4.2 CLOUD SERVER SETTING	29
5 SYSTEM SETTINGS	30
5.1 DATE AND TIME	30
5.2 ATTENDANCE SETTINGS	32
5.3 FINGERPRINT PARAMETERS	33

5.4 VOICE SETTINGS	34
5.5 AUTO SWITCH SETTINGS	35
5.6 SECURITY SETTING	36
5.7 USB SETTINGS	37
5.8 UPDATE FIRMWARE ONLINE	38
5.9 FACTORY RESET	40
6 DATA MANAGEMENT	41
7 RECORD	42
8 AUTOTEST	44
9 SYSTEM INFORMATION	46
10 CONNECT TO BIOTIME CLOUD SOFTWARE	47
10.1 LOGIN TO THE WEB	47
10.2 ADD DEVICE ON THE SOFTWARE	48
10.3 ADD EMPLOYEE ON THE SOFTWARE	49
10.3.1 ADD EMPLOYEE TO THE SOFTWARE	49
10.3.2 SYNCHRONIZE EMPLOYEES TO DEVICE	50
10.4 REGISTER VERIFICATION MODE FROM DEVICE	51
10.5 MOBILE APP SETTINGS	53
PRIVACY POLICY	54
ECO-FRIENDLY OPERATION	56

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.
11. 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 Standby Interface

1. When the device is connected to the power supply and the device is used for the first time, it enters the standby screen as shown below:








Notes:

- 1) *This device needs to be used in combination with **BioTime Cloud software**. After adding devices to the software, you can unify the management of the device.*
- 2) *For details on how to add the device, see [10.2 Add Device on the Software](#).*
2. After successfully binding the device, the standby screen will be displayed as shown below.



Status Icons

Status Icon	Name	Description
	USB	The device is plugged into a USB flash drive.
	ADMS Server	The connection between device and ADMS server is successful.
		The connection between device and ADMS server is failed.
	Wi-Fi Signal	The Wi-Fi connection is normal.
		The Wi-Fi connection fails.

1.2Verification Modes

In the device, there are three verification modes, namely:

- Fingerprint verification
- Card Number verification
- Password verification

These verification modes can be used for check-in and check-out punches.

1.2.1 Fingerprint Verification

● **Finger Enrolment**

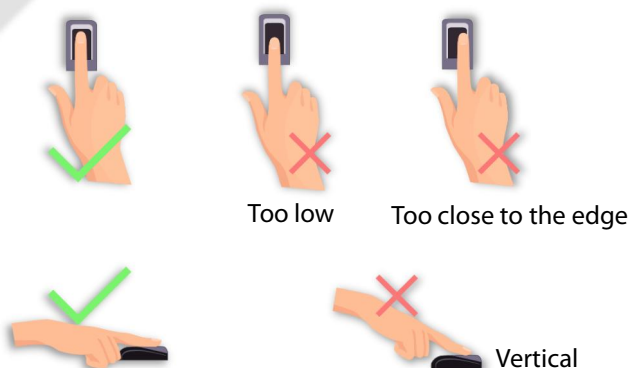
Finger Enrolment procedure involves capturing a user's fingerprint and saving it as a template to the corresponding User ID. To enhance the fingerprint authentication rate, make sure that you enrol the finger correctly.

● **Finger Selection for Enrolment**

- ✧ It is recommended to use the index finger or middle finger to enrol your fingerprint.
- ✧ If the fingerprints on your selected hand are worn or damaged, try to use the other hand.
- ✧ If the fingers are small, try enrolling with the thumb finger.

● **Enrolment Operation**

- ✧ Place the finger flat and centered on the sensor surface.
- ✧ The score for each enrolment will be displayed. Make sure that the score is high enough for proper enrolment and authentication.
- ✧ Place the finger consecutively until the success message appears. An illustration is given below:



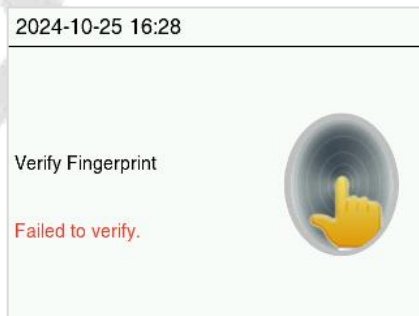
● 1: N Fingerprint Verification Mode

The device compares the current fingerprint collected by the fingerprint sensor with all the fingerprints on the device. Press your finger properly on the fingerprint sensor. If the fingerprint matches with the saved template, the verification is successful.

If the verification is successful, the success message will be displayed as shown below:



If the verification failed, the message will be displayed as shown below:



If the device instructs "**Failed to verify**" then press your finger again. You can attempt verification 2 more times. If the verification fails after these attempts, then the device will return to the standby interface.

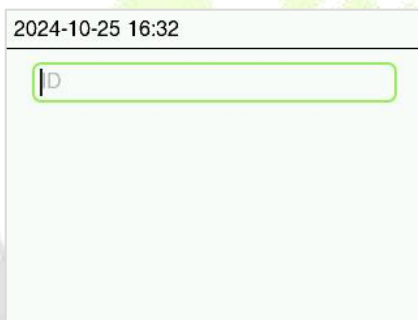
● 1:1 Fingerprint Verification Mode


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.

Press the number keys on the device keypad to enter 1:1 fingerprint verification mode.

1. Input the user ID and press **M/OK**.

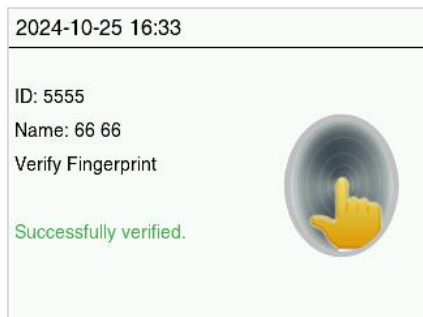


2. If the user has registered card and password in addition to his/her fingerprints and the verification method is set to Fingerprint/Card template verification, the following screen will appear. Select the fingerprint icon to  enter fingerprint verification mode.

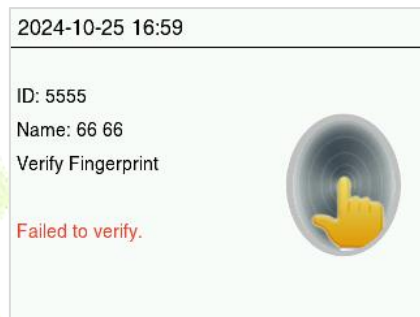


3. Press the fingerprint to verify.

Verification is successful:



Verification is failed:



1.2.2 Card Number verification

● 1: N Card Verification Mode

The device compares the card number in the card induction area with all the card number data registered in the device. The following is the card verification screen.



If the verification failed, the message will be displayed as shown below:

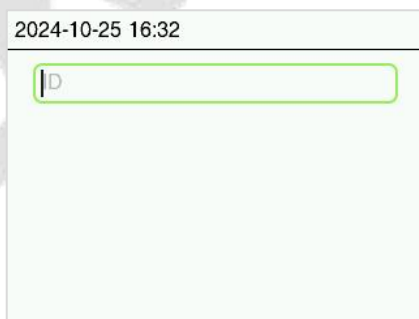



● **1:1 Card Verification Mode**

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

Press the number keys on the device keypad to enter 1:1 card verification mode.

1. Input the user ID and press **M/OK**.

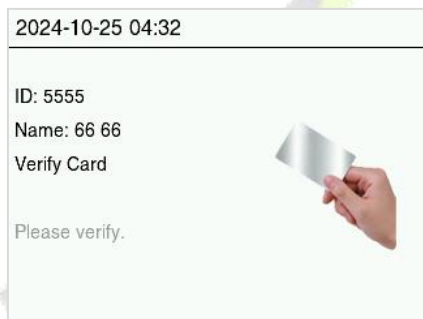


2. If the user has registered fingerprint and password in addition to his/her card, and the verification method is set to Password/Fingerprint/Card verification, the following screen will appear. Select the  icon to enter the card verification mode.



3. Place the card in the collection area for verification.

Verification is successful:




Verification is failed:

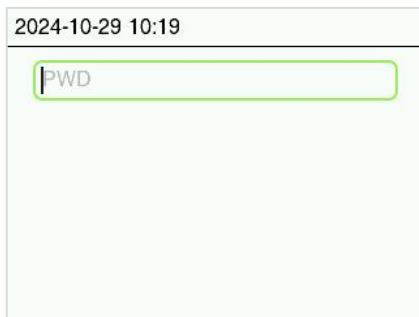


1.2.3 Password verification

The device compares the entered password with the registered password by the given User ID.

Press the number keys on the device keypad to enter 1:1 password verification mode. Then, input the user ID and press **M/OK**.

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

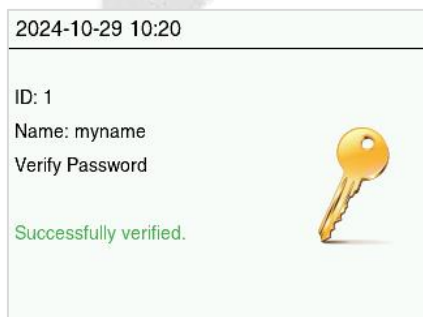


Input the password and press **M/OK**.

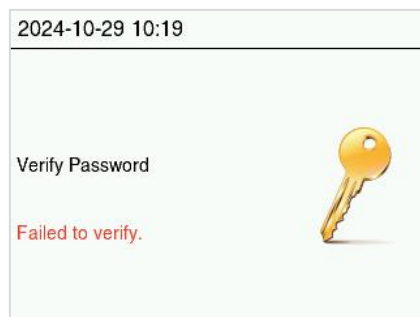


The following screen displays, after inputting a correct password and a wrong password respectively.

Verification is successful:



Verification is failed:

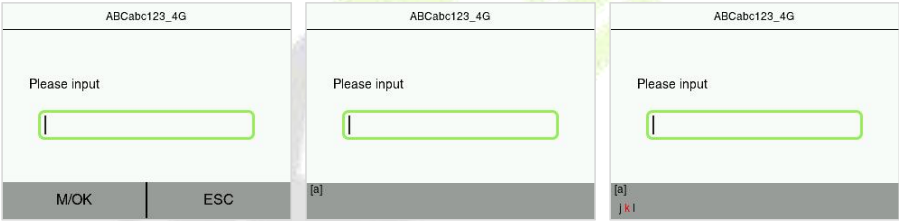


1.3 Text Input Operation

The device can recognize English letters, symbols, and numbers. Press > to display the input method and press > again to switch the input method. Press the ^ / v key to scroll up and down. Press < to delete the entry. Press **ESC** to exit the input method.

Description of entry of English letters and symbols.

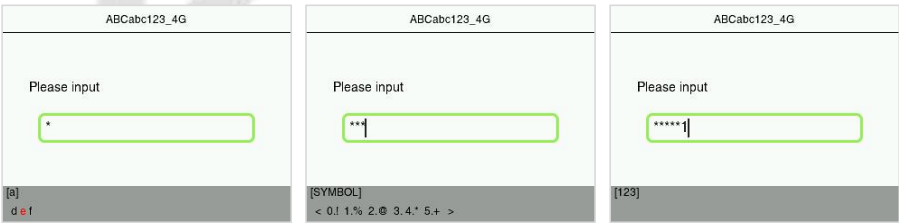
For example, enter the password: key@M1



Press > to display the input method.

Press > again to switch the input method. Select **Aa**, **a**, or **A** for using uppercase and lowercase letters based on requirements.

Press **5_{JKL}** twice to select **k**.



Press **3_{DEF}** twice to select **e**. Finish the text input in the same way.

Press > to switch to the symbol input method and press **2_{ABC}**. Select **@**.

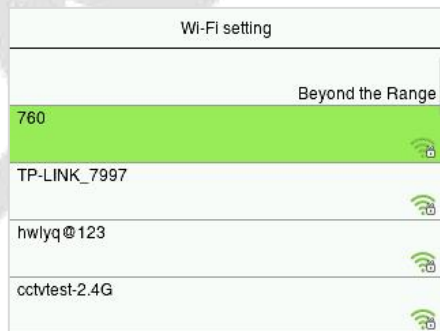
Press > to switch to the numeric input method, then press **1**. When finished, press **ESC** to exit. Then press **M/OK** to save and exit.

1.4 Wi-Fi Connection

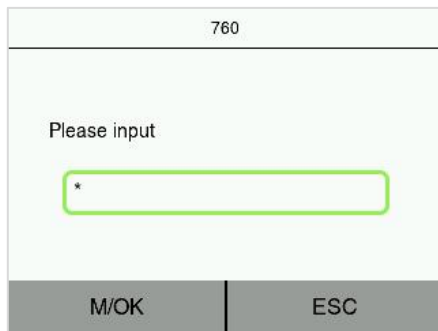
Situation 1: After powering up the device, it enters the Wi-Fi setting shortcut interface, refer to the following steps to connect to Wi-Fi.




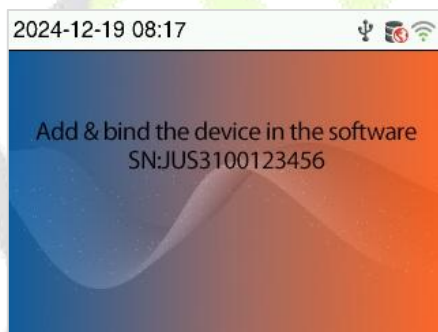
1. Pressing **M/OK** in this shortcut interface will directly enter the Wi-Fi setting interface. The device will search for available Wi-Fi networks within range.



2. Select the available Wi-Fi from the list, you will enter the password interface, enter the password and press **M/OK** to connect.



3. After the Wi-Fi connection is successful, the Wi-Fi  logo will be displayed on the status bar.

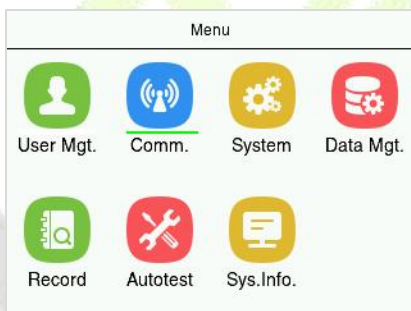


Note: If you are using the device for the first time or if the device is not bound, the Wi-Fi shortcut interface will take you directly to the SN interface after you set up Wi-Fi. In this screen you can view the serial number of the device.

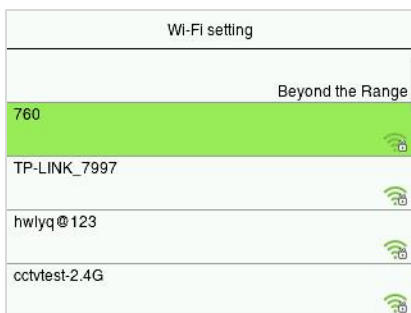
Situation 2: If you have entered the **QR code screen** or have bound the device and entered the **Welcome screen**, refer to the following steps to connect to the Wi-Fi.



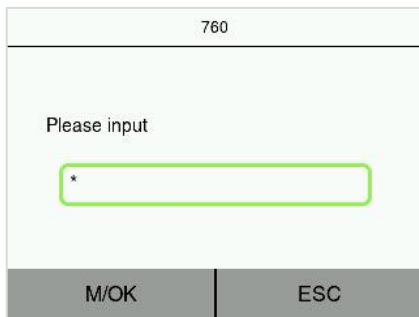
1. Press **M/OK** to access the **Main Menu** if you have bound the device and are in the standby screen.



2. Then click **Comm.** > **Wi-Fi setting** to enter the Wi-Fi setting interface. And the device will search for available Wi-Fi within the network range.



3. Select the available Wi-Fi from the list, you will enter the password interface, enter the password and press **M/OK** to connect.



760

Please input

*

M/OK | ESC

4. After the Wi-Fi connection is successful, the Wi-Fi  logo will be displayed on the status bar.



2 Main Menu

After binding the device, press the **M/OK** key on the keyboard to enter the Main Menu, the following screen will be displayed:



Function Description:

Menu	Descriptions
User Mgt.	View basic information about the user.
Comm.	To set the relevant parameters of wireless network and cloud server.
System	To set the parameters related to the system, including date time, attendance setting, fingerprint parameters, voice setting, auto switch setting, security setting, USB upgrade, update firmware online and reset to factory.
Data Mgt.	To delete all relevant data in the device.
Record	To query the specified event logs, attendance record..
Autotest	To automatically test whether each module functions properly, including the LCD screen, audio, keyboard, fingerprint sensor and real-time clock.
System Info	To view data capacity, device and firmware information and privacy policy of the device.

3 User Management

3.1 Search for Users

When the device is on the initial interface, press **M/OK** button > **[User Mgt.]** > **[All User]** to enter All User interface. Input "User ID" in the search box provided to view the corresponding user.

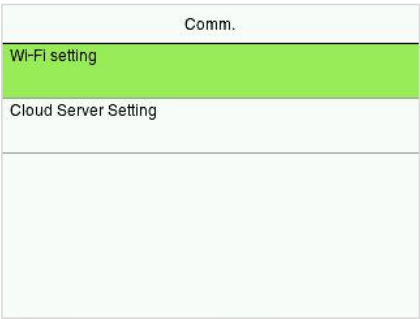
The following screenshots illustrate the steps to search for a user:

- User Mgt. Screen:** Shows the 'User Mgt.' title and a list with 'All Users' selected.
- All Users Screen:** Displays a list of users. The first user is '1230539 null 456'.
- All Users Screen (Search):** Shows the same list with a search bar containing '1' and '(1/1)' results.
- Edit Screen:** Shows the details for user '1230539 null 456'. Fields include ID (1230539), Name (null 456), Purview (User), FP (0), and Card.

Note: Only basic information of all users can be viewed here, for editing, you need to operate on BioTime Cloud Web. Adding users can be found in [10.3 Add Employee on the Software](#).

4 Communication Settings

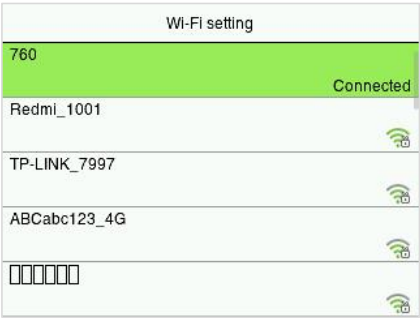
Select **Comm.** on the **Main Menu** to set the relevant parameters of Wireless Network and Cloud Server.



4.1 Wireless Network

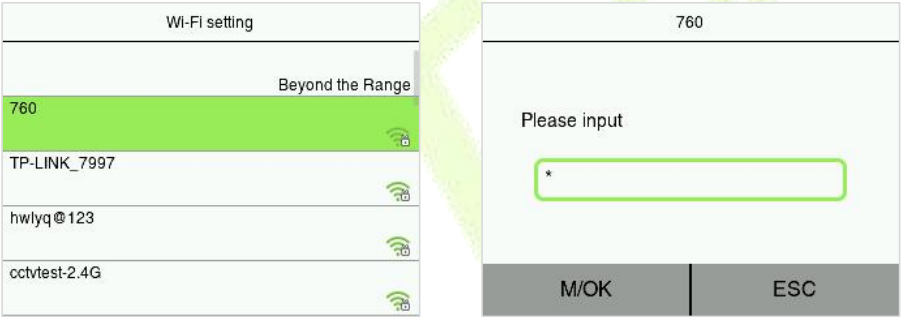
This device provides a built-in Wi-Fi module. The Wi-Fi module enables data transmission via Wi-Fi (Wireless Fidelity) and establishes a wireless network environment.

When the device is on the initial interface, press **M/OK** button > [**Comm.**] > [**Wi-Fi setting**] to configure the Wi-Fi setting.



● **Search the Wi-Fi Network**

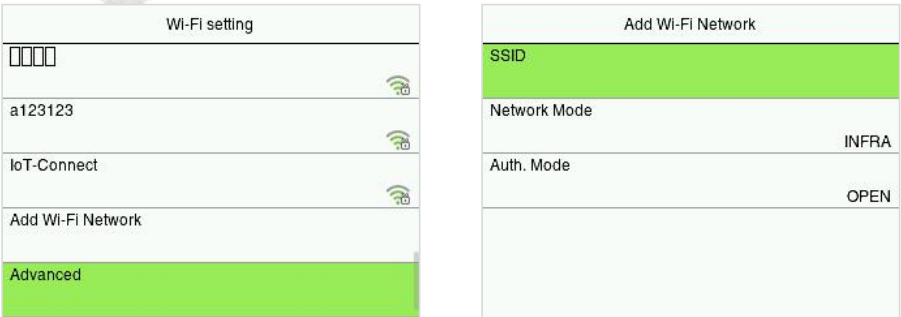
- ✧ Wi-Fi is enabled in the Device by default.
- ✧ Once enter the **Wi-Fi setting** interface, the device will search for the available Wi-Fi within the network range.
- ✧ Choose the appropriate Wi-Fi name from the available list, and input the correct password in the password interface, and then press **M/OK** to connect.



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

● **Add Wi-Fi Network Manually**

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



- 1. Manually add Wi-Fi by selecting '**Add Wi-Fi Network**' using the arrow keys.
- 2. On this interface template, enter the Wi-Fi network parameters. (The added network must exist.)

Note: After successfully adding the Wi-Fi manually, follow the same process to search for the added Wi-Fi name.

● **Advanced Setting**

Wi-Fi setting

□□□□

a123123

IoT-Connect

Add Wi-Fi Network

Advanced

Ethernet

DHCP

IP Address

Subnetmask

GateWay

DNS

192.168.138.88

255.255.255.0

192.168.138.22

192.168.138.22

Function Description:

Menu		Descriptions
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 Wi-Fi 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 Wi-Fi 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.

4.2 Cloud Server Setting

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



Function Description:

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

5 System Settings

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

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

System
Date/Time
Attendance
Fingerprint
Voice
Auto Switch

System
Auto Switch
Security Setting
USB
Update
Reset Opts.

5.1 Date and Time

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



Date/Time
Set Date
2024-10-25
Set Time
16:43:29
24-Hour Time
<input checked="" type="checkbox"/>
Date Format
YYYY-MM-DD
DST
<input checked="" type="checkbox"/>

Date/Time
Set Time
16:43:29
24-Hour Time
<input checked="" type="checkbox"/>
Date Format
YYYY-MM-DD
DST
<input checked="" type="checkbox"/>
Daylight Saving Setup

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

Set Date		
2024-10-25		
^ 2024 v	^ 10 v	^ 25 v
YYYY	MM	DD
M/OK		ESC

Set Time		
16:46:48		
^ 16 v	^ 46 v	^ 48 v
HH	MM	SS
M/OK		ESC

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

DST	
Start Date	01-00
Start Time	00:00
End Date	01-00
End Time	00:00

Start Date	
01-09	
^ 01 v	^ 9 v
MM	DD
M/OK	
ESC	

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

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

5.2 Attendance Settings

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

Attendance	
Duplicate Punch Period(m)	None
Alphanumeric User ID	<input checked="" type="checkbox"/>
Log Alert	Disable
Authentication Timeout(s)	3
Menu Screen Timeout(s)	60

Function Description:

Menu	Descriptions
Duplicate Punch Period(m)	Within a set time period (unit: minutes), the duplicated attendance record will not be reserved (value ranges from 0 to 999999 minutes).
Alphanumeric User ID	Decides whether to support letters in a User ID.
Log Alert	When the record space of the attendance reaches the maximum threshold value, the device automatically displays the memory space warning. Users may disable the function or set a valid value between 1 and 9999.
Authentication Timeout(s)	The time length of the message of successful verification displays. Valid value: 1~9 seconds.

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

5.3 Fingerprint Parameters

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

Fingerprint	
1:1 Threshold Value	30
1:N Threshold Value	35
Sensitivity	Low
1:1 Retry Attempts	3
Fingerprint Image	None

Function Description:

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

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

5.4 Voice Settings

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

Voice	
Voice Prompts	<input checked="" type="checkbox"/>
Key Voice	<input type="checkbox"/>
Volume	70

Function Description:

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

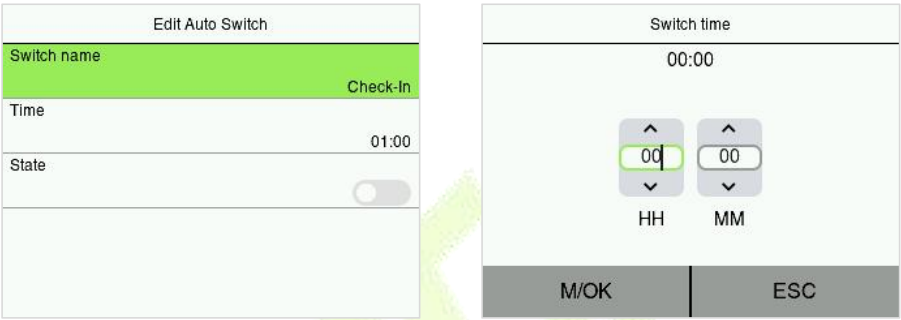
5.5 Auto Switch Settings

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

Auto Switch			
ID	Time	Name	State
1	01:00	Check-In	✘
2	02:00	Check-Out	✘
3	03:00	Break-Out	✘
4	04:00	Break-In	✘
5	05:00	OT-In	✘
			(1/5)

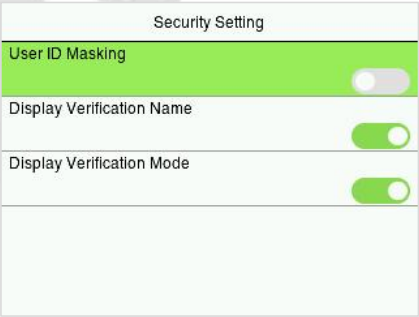
Auto Switch			
ID	Time	Name	State
6	06:00	OT-Out	✘
7	00:00		✘
8	00:00		✘
9	00:00		✘
10	00:00		✘
			(2/5)

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



5.6 Security Setting

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



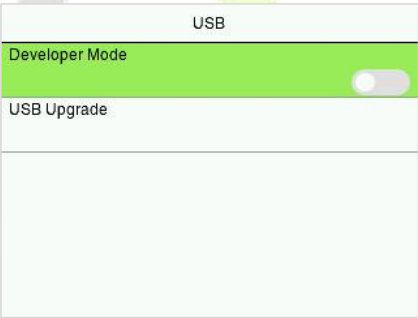
Function Description:

Menu	Descriptions
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.

5.7 USB Settings

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



Function Description:

Menu	Descriptions
Developer Mode	When turned on, the device enters developer mode, at which time the USB upgrade function is disabled.
USB Upgrade	Upgrade firmware via USB drive. <i>Note:</i> This menu item will not be displayed when Developer Mode is turned on.

● USB Upgrade

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

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

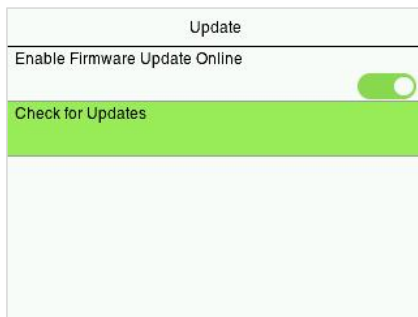


Note: If upgrade file is needed, please contact our technical support. Firmware upgrade is not recommended under normal circumstances.

5.8 Update Firmware Online

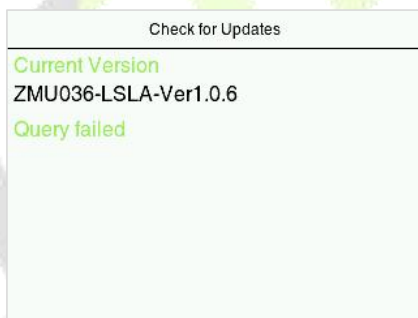
When the device is on the initial interface, press **M/OK** button > [**System**] > [**Update**] to enter the setting interface.

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

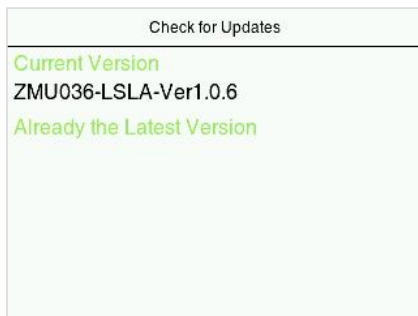


Select [**Check for Updates**] it may have the following 3 scenarios:

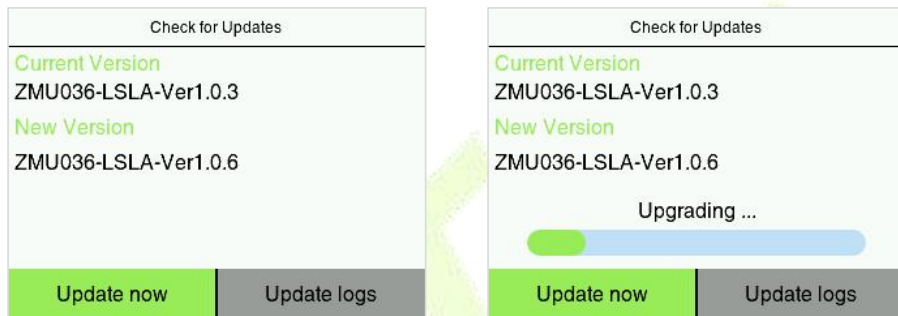
- ✧ If the query fails, the interface will prompt "**Query failed**".



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



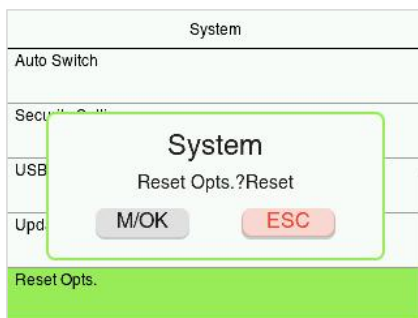
- ✧ If the firmware version of the device is not the latest, the version number and change log of the latest version will be displayed. Users can choose whether to update to the latest firmware version.



5.9 Factory Reset

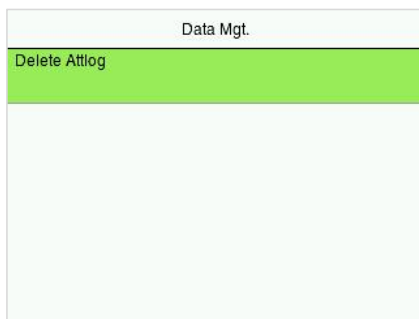
The Factory Reset function restores the device settings such as communication settings and system settings, to the default factory settings (This function does not clear registered user data).

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



6 Data Management

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



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



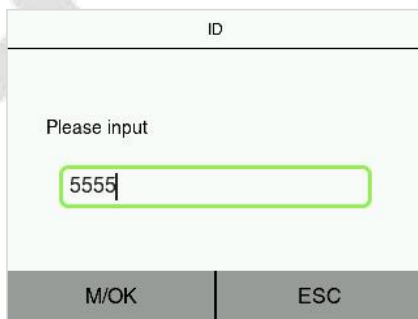
7 Record

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

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



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



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

Start Time

2024-10-25 00:00

2024

10

25

00

00

YYYYMMDDHHMM

M/OKESC

End Time

2024-10-25 23:59

2024

10

25

23

59

YYYYMMDDHHMM

M/OKESC

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

Record	
Date	Sum
2024-10-25	5
ID: 5555 Name: 66 66 (1/1)	

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

Record		
Time	VerType	State
10-25 16:56	Card	None
10-25 16:55	Card	None
10-25 16:33	FP	None
10-25 16:33	Card	None
10-25 16:32	FP	None
ID: 5555 Name: 66 66 (1/1)		

8 Autotest

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

Autotest
Test All
Test LCD
Test Voice
Test Keyboard
Test Fingerprint Sensor

Autotest
Test LCD
Test Voice
Test Keyboard
Test Fingerprint Sensor
Test Clock RTC

Function Description:

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

Test Fingerprint Sensor	To test the fingerprint sensor by pressing a finger on the scanner to check if the acquired fingerprint image is clear. When you are pressing a finger on the scanner, the fingerprint image will display on the screen.
Test Clock RTC	To test the RTC. The device tests whether the clock works normally and accurately with a stopwatch. Tap the screen to start counting and press it again to stop counting.

9 System Information

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

Sys.Info.
Device Capacity
Device Info
Firmware Info
Privacy Policy

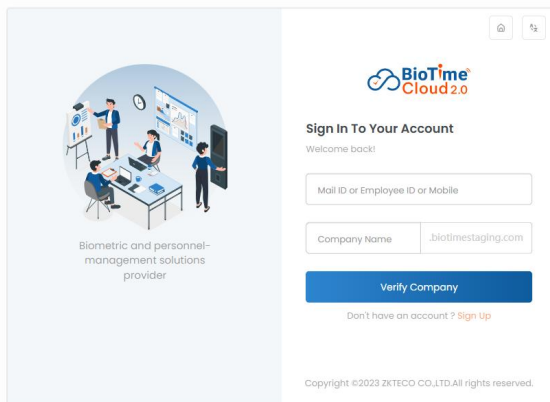
Function Description:

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

10 Connect to BioTime Cloud Software

10.1 Login to the Web

1. Please open the recommended browser and enter the address to access the BioTime Cloud Web.
2. In the Sign In page, enter Email ID and Company Name. Then click **[Verify Company]**.



Biometric and personnel-management solutions provider

Sign In To Your Account
Welcome back!

Mail ID or Employee ID or Mobile

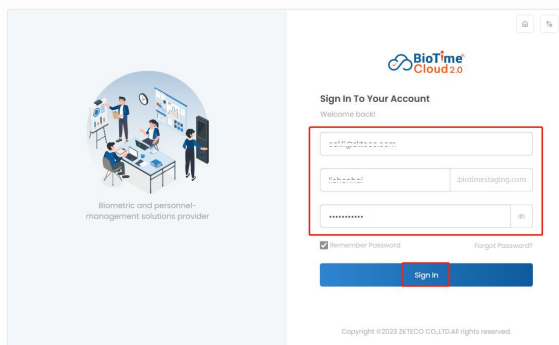
Company Name .biotimestaging.com

Verify Company

Don't have an account ? [Sign Up](#)

Copyright ©2023 ZKTECO CO.,LTD.All rights reserved.

3. Enter the password and click on **[Sign In]**.



Biometric and personnel-management solutions provider

Sign In To Your Account
Welcome back!

12345678901234567890


Company Name .biotimestaging.com

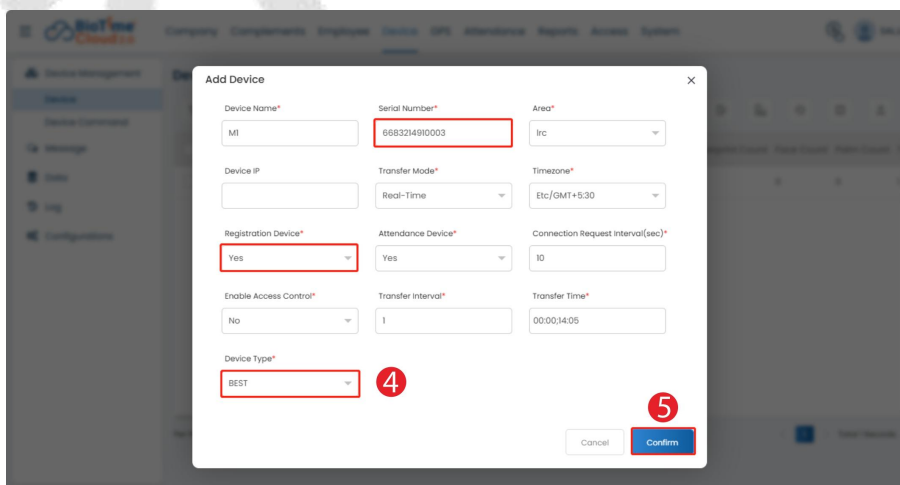
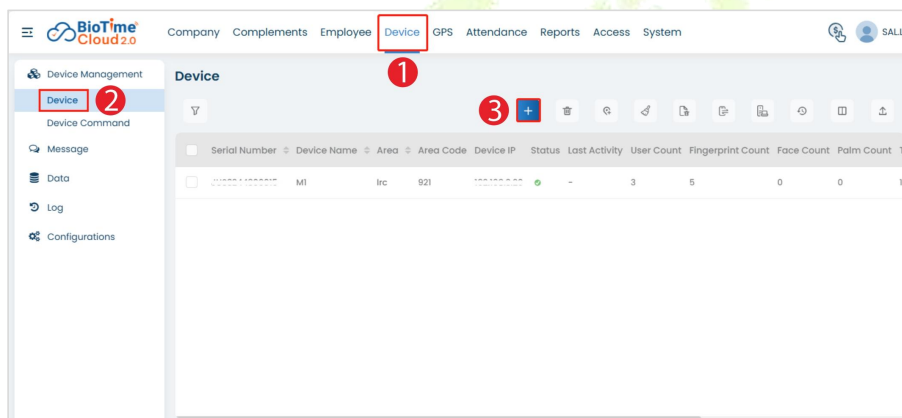
☒ Remember Password [Forgot Password?](#)

Sign In

Copyright ©2023 ZKTECO CO.,LTD.All rights reserved.

10.2 Add Device on the Software

1. Click **[Device]** to enter the device management interface.
2. Then click the  icon and enter the relevant parameters in the pop-up add window to add the device.
3. When you are finished entering, click **[Confirm]** to save and exit.




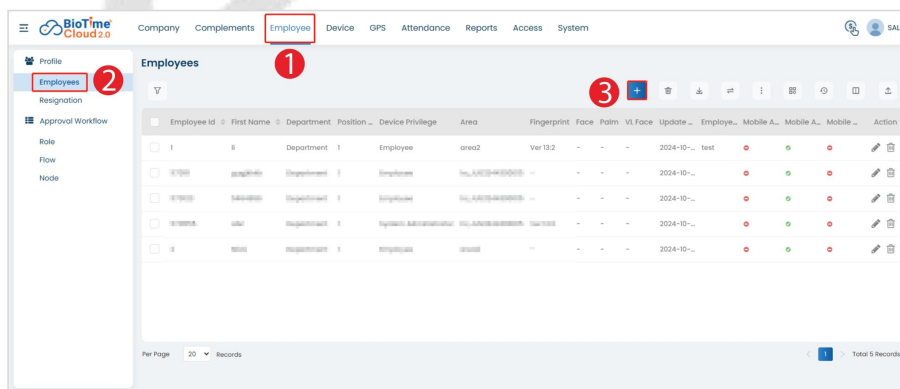
Function Description:

- **Serial Number:** Check the serial number label on the back cover of the device. Or click the **M/OK** button to enter the Main Menu, then click **[System Info.] > [Device Info.] > [Serial No.]** to view the serial number.
- **Area:** Once an area is selected, all personnel in the area will be automatically synchronized to the device.
- **Registration Device:** Select YES to support remote registration.
- **Device Type:** Set the device type to BEST.

10.3 Add Employee on the Software

10.3.1 Add Employee to the Software

1. Click **[Employee]** > **[Employees]** to enter the Employee Settings interface.
2. Then click the  icon and enter the relevant parameters in the pop-up add window to add the person.
3. When you are finished entering, click **[Confirm]** to save and exit.



Add Employee

Employee ID* First Name* Last Name

1 Mick Lee

Email* Mobile* Date of Joining

mick.lee@biotime.com 15912341234

Department* Area* Position*


Department area2/lrc Position

Holiday Location Outdoor Mng Employment Type





Disable

Cancel Confirm

10.3.2 Synchronize Employees to Device

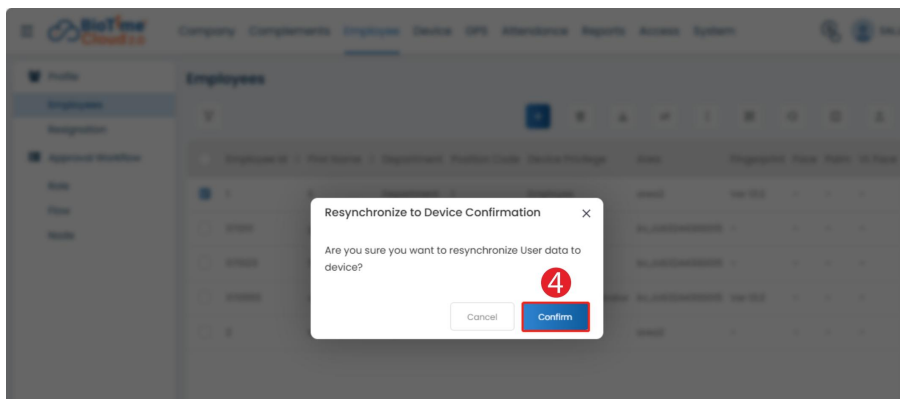
Select the device where you want to synchronize people in the device list, click the  icon and select **[Resynchronize to device]** from the pop-up menu. Then click **[Confirm]** in the pop-up window to confirm.

Employees

Employee ID	First Name	Department	Position Code	Device Privilege	Area	Resync
1	ii	Department	1	Employee	area2	
2	iii	Department	1	Employee	area2	
3	iiii	Department	1	Employee	area2	
4	v	Department	1	Employee	area2	


Per Page: 20 Records

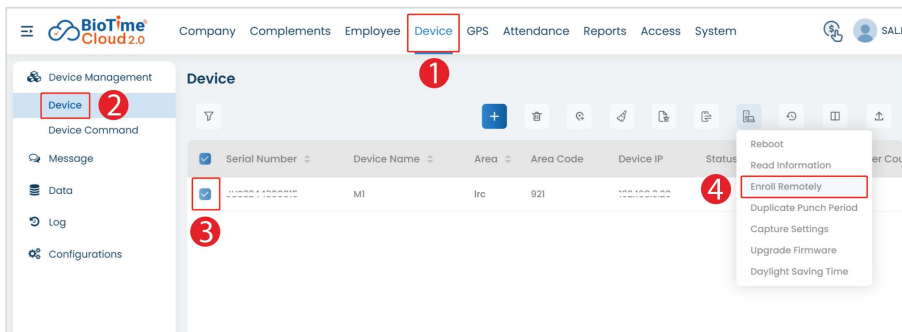
Total 5 Records



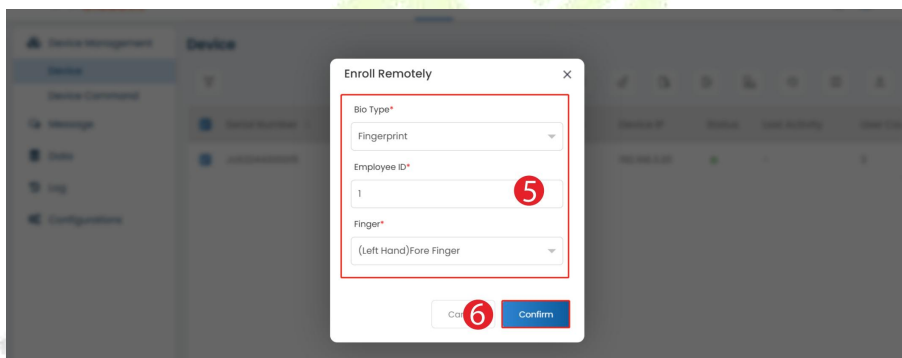
10.4 Register Verification Mode from Device

After successfully synchronizing the person to the device, you can enroll the person with biometric information. The device supports **card** and **fingerprint** verification. Only fingerprint enrolment is illustrated here as an example.

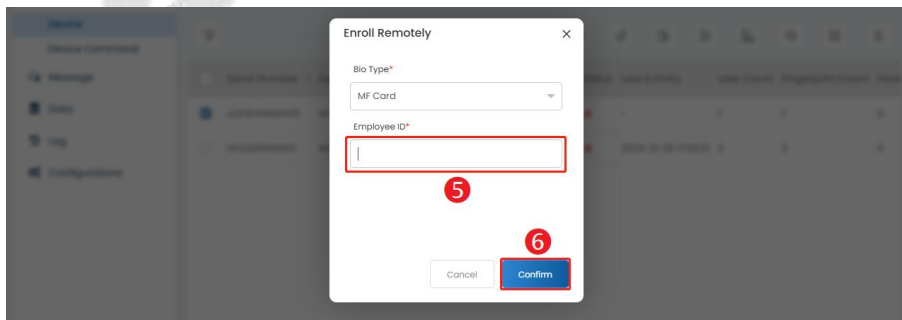
1. Click **[Device]** > **[Device]** to enter the device list interface.
2. Select the device and click the  icon. Select **[Enroll Remotely]** in the drop-down menu that pops up.
3. Then in the pop-up window, set the Bio Type to **Fingerprint**, enter the Employee ID number and select the finger to be enrolled (When registering a card, set the Bio Type to **MF Card** and enter the employee ID number). As shown in the figure below.
4. At the same time the device enters the fingerprint entry screen. According to the prompts, place your finger on the fingerprint collector and press **3** times. When the interface prompts **"Enrolled Success"** it means the fingerprint entry is successful.
5. And you can repeat the above operation to register other fingers.




Fingerprint Registration:

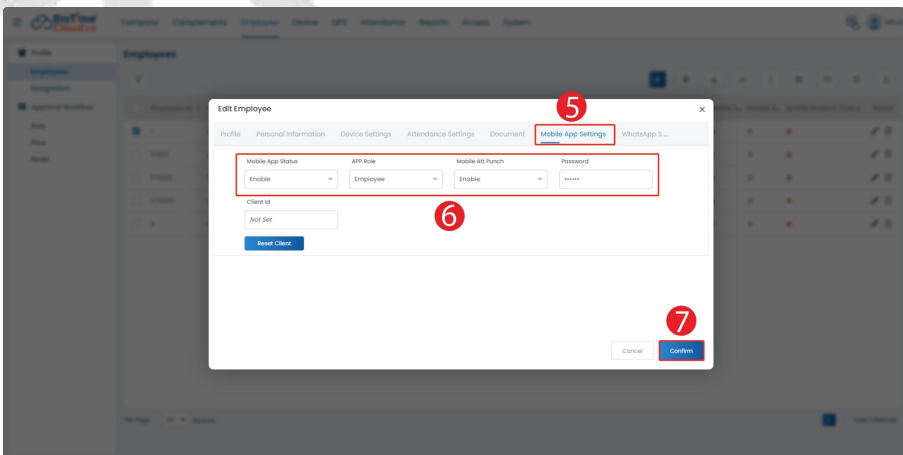
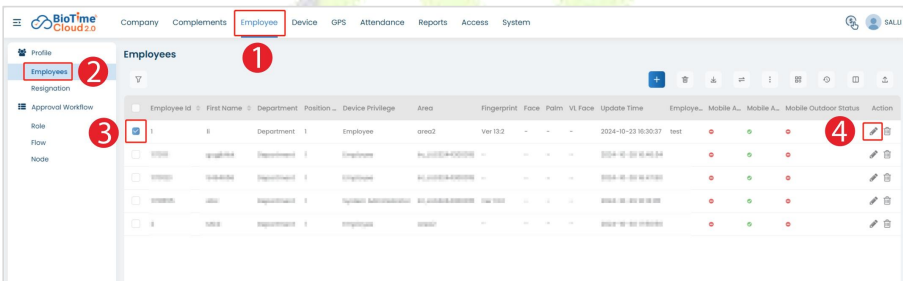


Card Registration:



10.5 Mobile App Settings

1. Click **[Employee]** > **[Employees]** to enter the employee list interface.
2. Select the employee and click the  icon to enter the Edit Employee interface.
3. Then click **[Mobile App Settings]** to set the relevant parameters and enter the password. Click **[Confirm]** to save and exit.
4. Once the setup is complete the employee can use their account and password to log in to the BioTime Cloud App for attendance.



Privacy Policy

Notice:

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

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

I. Collected Information

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

- 1. User Registration Information:** At your first registration, the feature template (**Fingerprint template/Face template/Palm template**) will be saved on the device according to the device type you have selected to verify the unique similarity between you and the User ID you have registered. You can optionally enter your Name and Code. The above information is necessary for you to use our products. If you do not provide such information, you cannot use some features of the product regularly.
- 2. Product information:** According to the product model and your granted permission when you install and use our services, the related information of the product on which our services are used will be collected when the product is connected to the software, including the Product Model, Firmware Version Number, Product Serial Number, and Product Capacity Information. **When you connect your product to the software, please carefully read the privacy policy for the specific software.**

II. Product Security and Management

1. When you use our products for the first time, you shall set the Administrator privilege before performing specific operations. Otherwise, you will be frequently reminded to set the Administrator privilege when you enter the main menu interface. **If you still do not set the Administrator privilege after receiving the system prompt, you should be aware of the possible security risk (for example, the data may be manually modified).**
2. All the functions of displaying the biometric information are disabled in our products by default. You can choose Menu > System Settings to set whether to display the biometric information. If you enable these functions, we assume that you are aware of the personal privacy security risks specified in the privacy policy.

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

III. How We Handle Personal Information of Minors

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

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

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

IV. Others

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

Eco-friendly Operation



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

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

Hazardous or Toxic substances and their quantities

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

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

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

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

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

Phone : +86 769 - 82109991

Fax : +86 755 - 89602394

www.zkteco.com



Copyright © 2025 ZKTECO CO., LTD. All Rights Reserved.