User Manual

MB Plus Series

Applicable model: MB160/360/460 Plus

Date: August 2023

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

Without the prior written consent of ZKTeco, no terminalion 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 the express written permission of ZKTeco.

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

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

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

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

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

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

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

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

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

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

ZKTeco Headquarters

Address ZKTeco Industrial Park, No. 32, Industrial Road,

Tangxia Town, Dongguan, China.

Phone +86 769 - 82109991

Fax +86 755 - 89602394

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

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

About the Company

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

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

About the Manual

This manual introduces the operations of **MB Plus Series**.

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

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

Document Conventions

Conventions used in this manual are listed below:

GUI Conventions

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

Symbols

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

Table of Contents

Safety Measures

The below instructions intend to ensure that the user can use the product correctly to avoid danger or property loss. The following precautions are to keep users safe and prevent any damage. Please read carefully before installation.

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

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

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

   And do not connect multiple devices to one power adapter as adapter overload can cause over-heat or fire hazard.
7. **Replacement parts** - When replacement parts are required, service technicians must only use the replacement parts provided by the supplier. Unauthorized substitutes can lead to the risk of burns, electric shocks, or other potential hazards.
8. **Safety check** - On completion of service or repair work on the unit, ask the service technician to perform safety checks to ensure proper operation of the device.
9. **Power sources** - Operate the system only from the label's power source form. If the sort of power supply to use is unclear, call your dealer.
10. **Lightning** - Can install external lightning conductors to protect against electrical storms. It stops power-ups from destroying the system.

    Recommended installing the devices in areas with limited access.

Electrical Safety

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

Operation Safety

- If smoke, odour, or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service centre.
- Transportation and other unpredictable causes may damage the device's hardware. Check whether the device has any intense damage before installation.
- If the device has major defects that you cannot solve, contact your dealer as soon as possible.
- Dust, moisture, and abrupt temperature changes can affect the device's service life. You are advised not to keep the device under such conditions.
- Do not keep the device in a place that vibrates. Handle the device with care. Do not place heavy objects on top of the device.
- Do not apply rosin, alcohol, benzene, pesticides, and other volatile substances that may damage the device enclosure. Clean the device accessories with a piece of soft cloth or a small amount of cleaning agent.
- If you have any technical questions regarding usage, contact certified or experienced technical personnel.

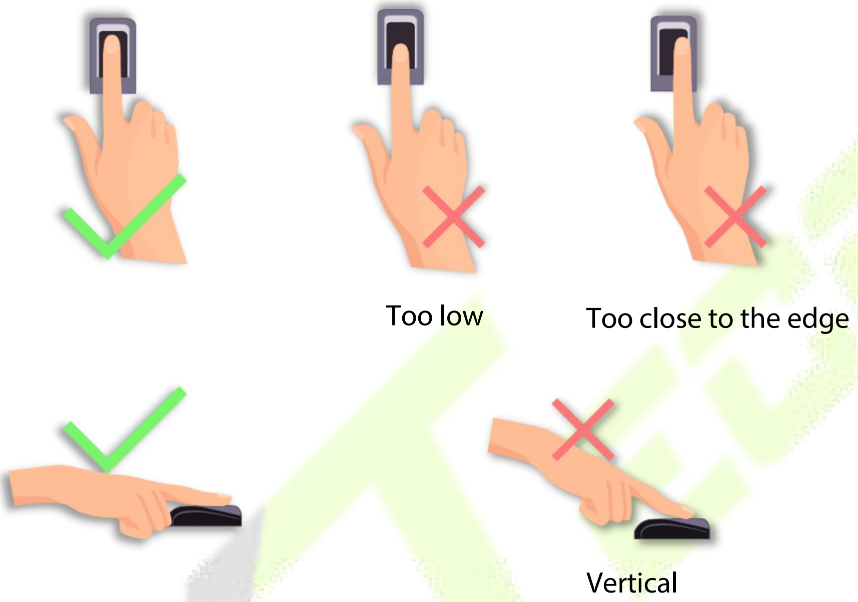
Note

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

1 Instruction for Use

1.1 Finger Positioning

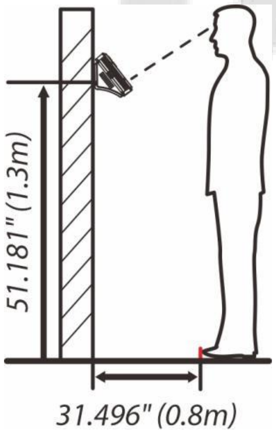
The index, middle, or ring finger are the recommended fingers to use, and avoid using thumb or pinkie finger as they are difficult to position correctly on the fingerprint reader and get suitable output.



Note: The recommended 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, Facial Expression and Standing Posture

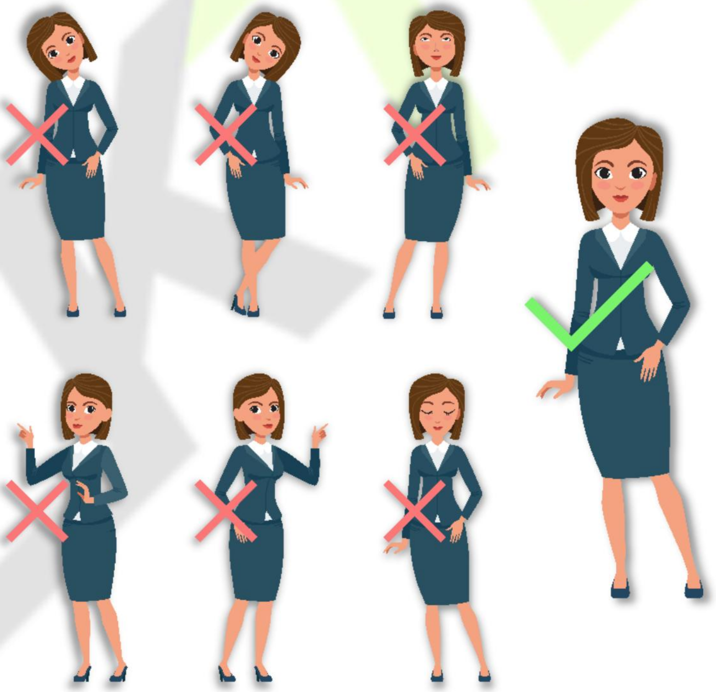
- **The recommended distance:**



For users whose height is between 61.024" to 72.835" (1.55m to 1.85m), the recommended height of the device is 51.181" (1.3m), and the distance from the user to the device is 31.496" (0.8m). Users may slightly move forwards and backward to improve the quality of facial images captured.

- **Facial expression:**

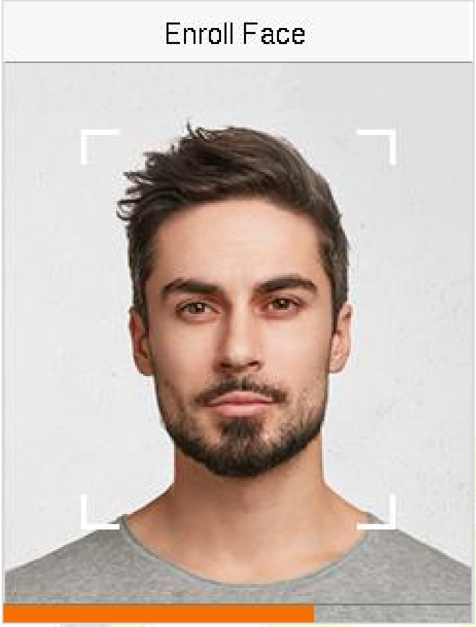
- **Standing posture:**



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

1.3 Face Registration

Please ensure that your face remains in the centre of the screen throughout the registration process. Face the camera directly and maintain a still position during face registration. The screen looks like the image below:



Correct face registration and authentication method:

- **Cautions for registering a face:**
  - When registering a face, maintain a 40cm to 80cm space between your face and the device.
  - Be careful not to change the facial expression (smiling face, drawn face, wink, etc.).
  - If you do not follow the instructions on the screen, the face registration may take longer or may fail.
  - Do not cover your eyes or eyebrows.
  - Do not wear hats, masks, sunglasses, or eyeglasses.
  - Be careful not to display two faces on the screen. It may create confusion and the registration may fail.
  - A user wearing glasses should register their face both with and without glasses.

- **Cautions for authenticating a face:**
  - Ensure that the face appears inside the guideline displayed on the screen of the device.
  - For a person wearing glasses, try authenticating your face with glasses if glasses were used while registering, or else authenticate without glasses if glasses were not used while registration. Otherwise, the recognition may fail or can be difficult. Also, if a different pair of glasses is used than the one used during registration, authentication can also fail. In such a case, the previously worn glasses can be used for authentication.

- Covering any part of the face with a hat, mask, eye patch, or sunglasses may cause authentication to fail. Please avoid covering your face and allow the device to accurately recognize your eyebrows and other facial features.

1.4 Verification Mode

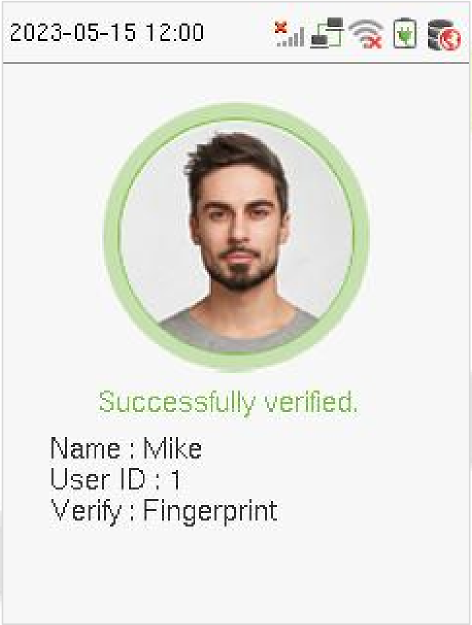
1.4.1 Fingerprint Verification

- **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 *1.1 Finger Positioning.*

The following screen displays on successful and failed verification respectively.

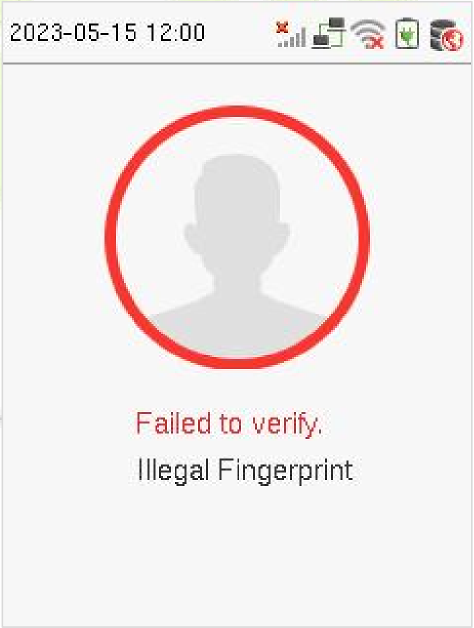


2023-05-15 12:00

Successfully verified.

Name : Mike
User ID : 1
Verify : Fingerprint

On successful verification



2023-05-15 12:00

Failed to verify.

Illegal Fingerprint

On failed verification

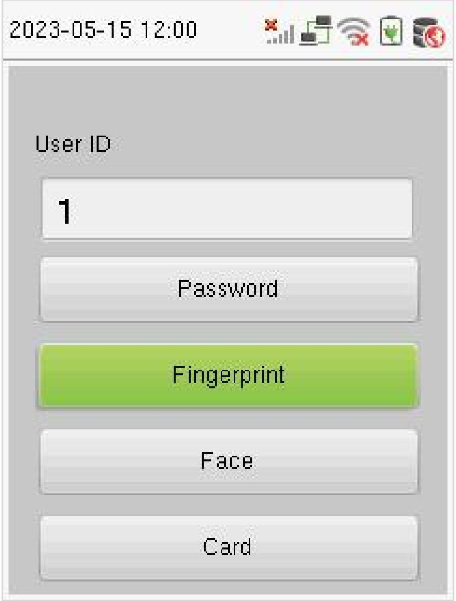
- **1:1 fingerprint verification mode:**

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

To enter the 1:1 fingerprint verification mode, please type the User ID on the main screen.

1. Enter the user ID and press [**M/OK**].

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



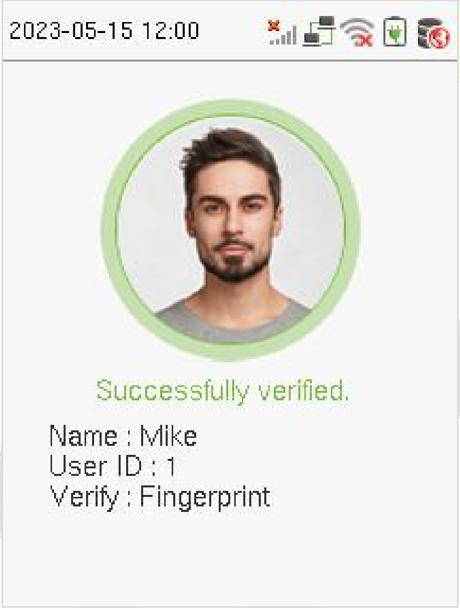
2023-05-15 12:00

User ID

1

2. Press the fingerprint to verify.

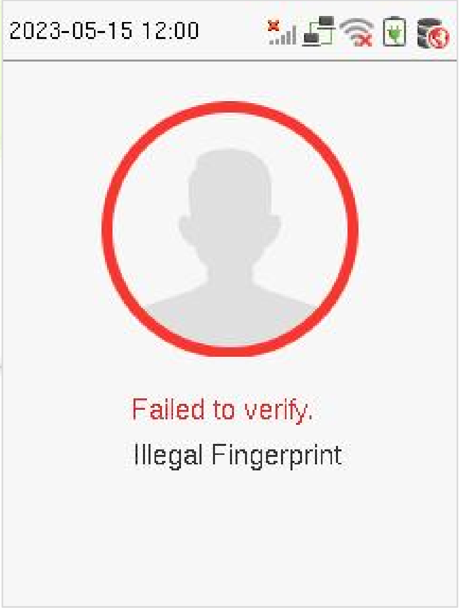
   The following screen displays on successful and failed verification respectively.



2023-05-15 12:00

Successfully verified.

Name : Mike
User ID : 1
Verify : Fingerprint



2023-05-15 12:00

Failed to verify.

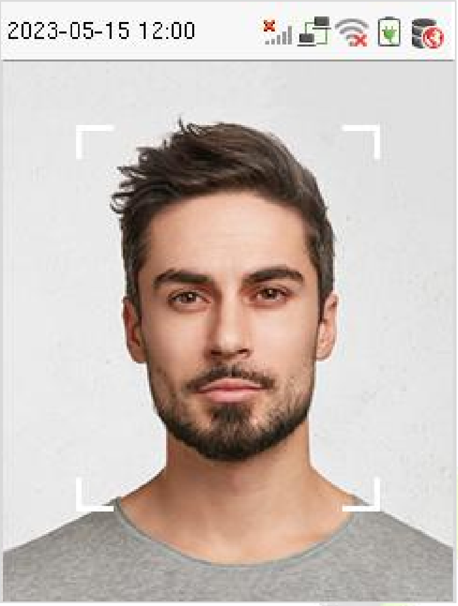
Illegal Fingerprint

On successful verification **On failed verification**

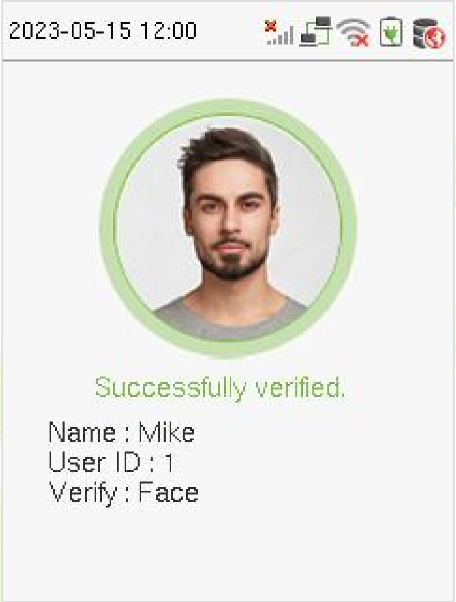
1.4.2 Facial Verification

- **1:N Facial Verification:**

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



2023-05-15 12:00



2023-05-15 12:00

Successfully verified.

Name : Mike

User ID : 1

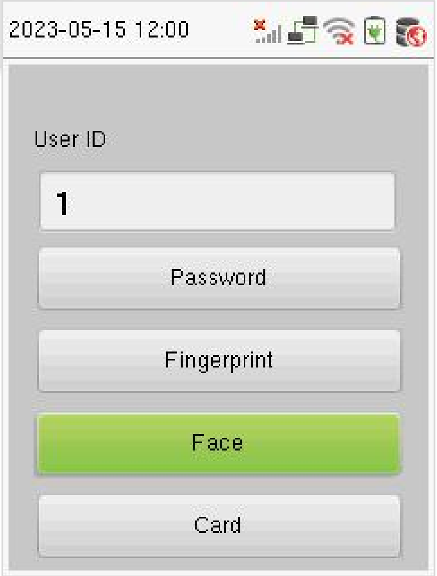
Verify : Face

- **1:1 Facial Verification:**

The device compares the face captured by the camera with the facial template related with the entered user ID.

For 1:1 facial verification, enter the User ID on the main interface and enter the 1:1 facial verification mode. Enter the user ID and press [**M/OK**].

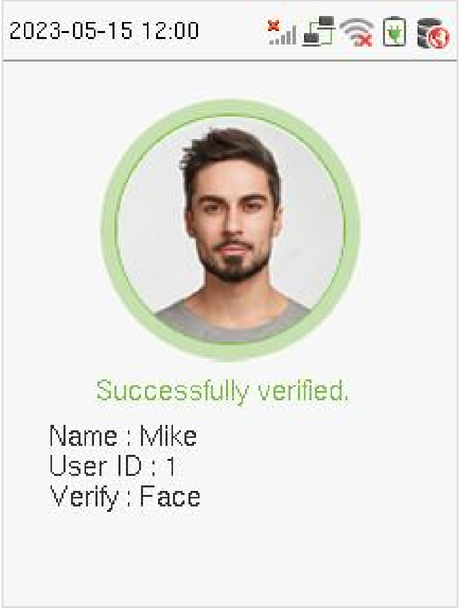
If an employee has registered a password in addition to face, the following screen will appear. Select the face icon to enter face verification mode.



2023-05-15 12:00

User ID: 1

After successful verification, the following display screen appears.



2023-05-15 12:00

Successfully verified.

Name : Mike
User ID : 1
Verify : Face

If the verification fails, it prompts "Please adjust your position!".

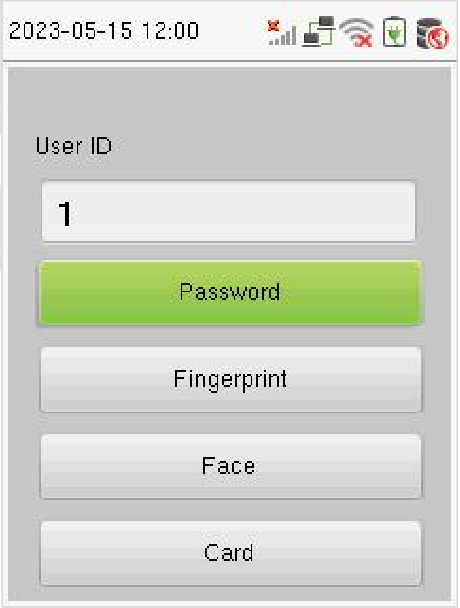
1.4.3 Password Verification

It compares the entered password with the registered User ID and password.

Enter the User ID on the main screen to enter the 1:1 password verification mode.

1. Enter the user ID and press [**M/OK**].

If an employee has registered fingerprint and face in addition to password, the following screen will appear. Select the Password icon to enter password verification mode.

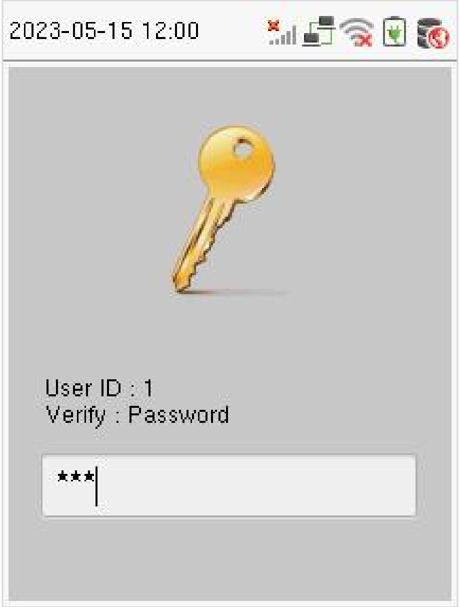


2023-05-15 12:00

User ID

1

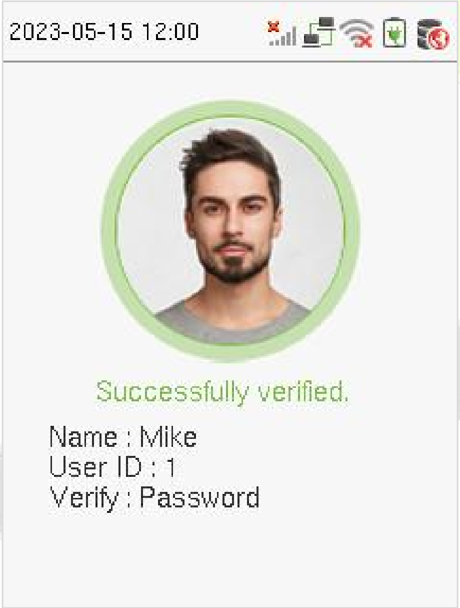
2. Input the password and press [**M/OK**].


2023-05-15 12:00

User ID : 1
Verify : Password

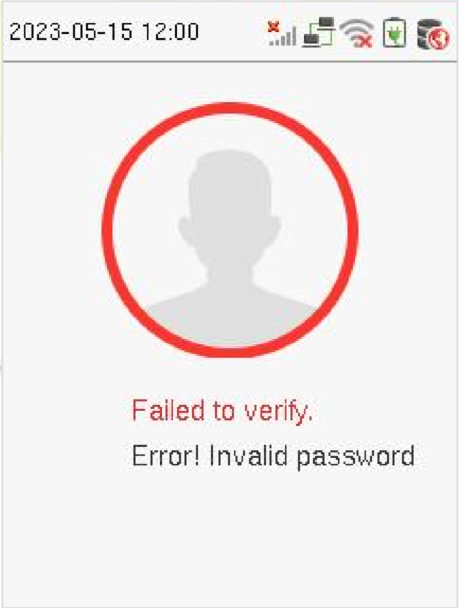
***

The following screen displays on successful and failed verification respectively.


2023-05-15 12:00

Successfully verified.

Name : Mike
User ID : 1
Verify : Password


2023-05-15 12:00

Failed to verify.

Error! Invalid password

On successful verification **On failed verification**

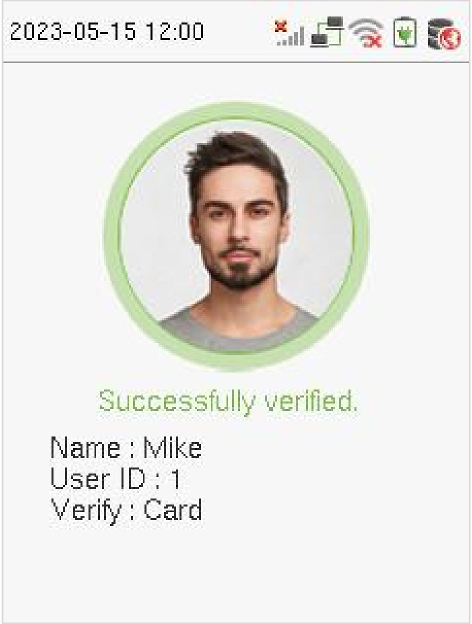
1.4.4 Card Verification

Only the product with the card module offers the card verification function.

- **1:N Card Verification**

It compares the card number in the card induction area with all the card number data that is available in the device. The device enters the Card Verification mode when a user put his/her card on the induction area.

The following screen displays on successful and failed verification respectively.

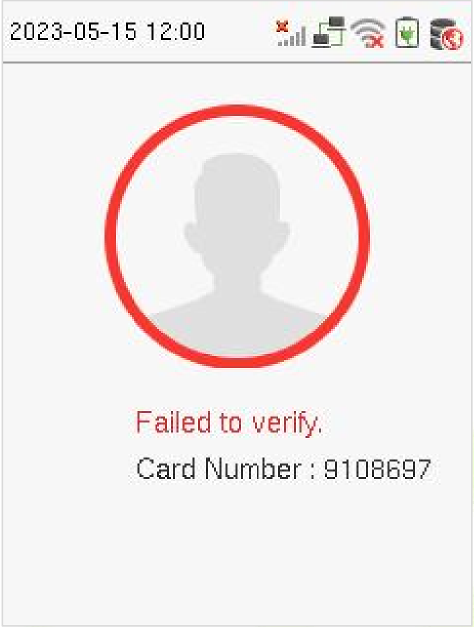


2023-05-15 12:00

Successfully verified.

Name : Mike
User ID : 1
Verify : Card

On successful verification



2023-05-15 12:00

Failed to verify.

Card Number : 9108697

On failed verification

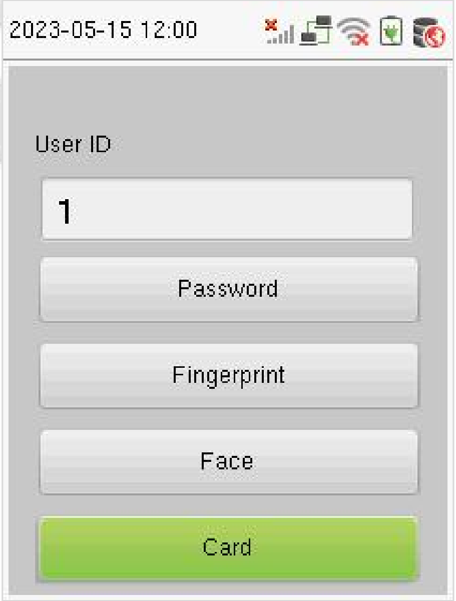
- **1:1 Card Verification**

It compares the card number in the card induction area with the number associated with the employee's User ID registered in the device. Users can try verifying their identity with 1:1 verification mode if they are unable to get access with the 1:N authentication method.

Enter the User ID on the main screen to enter 1:1 card verification mode.

1. Enter the user ID and press [**M/OK**].

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

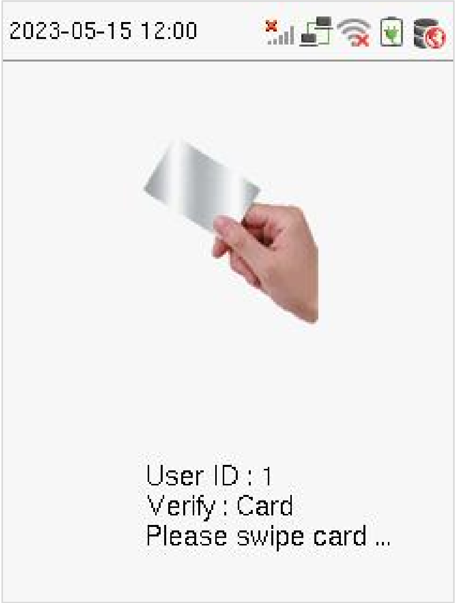


2023-05-15 12:00

User ID

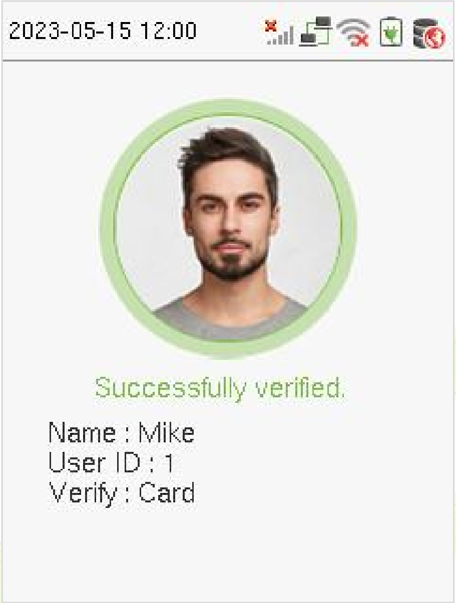
1

2. Place the card in the card induction area to verify. After successful verification, the following display screen appears.



2023-05-15 12:00

User ID : 1
Verify : Card
Please swipe card ...



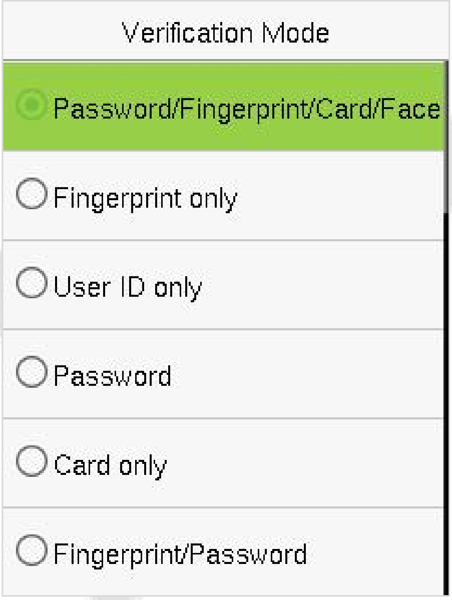
2023-05-15 12:00

Successfully verified.

Name : Mike
User ID : 1
Verify : Card

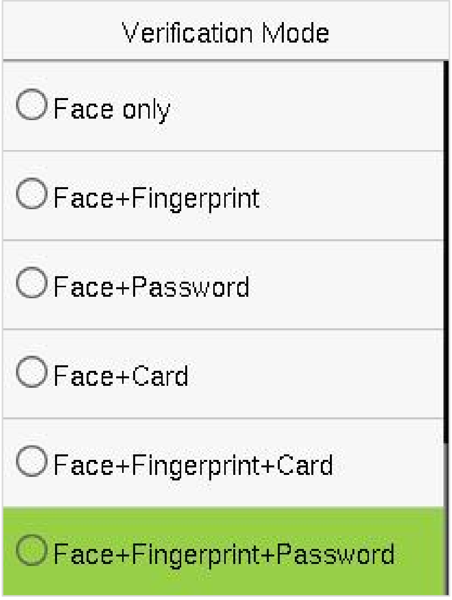
1.4.5 Combined Verification

For enhanced security, this device offers the option of using multiple forms of verification methods, as shown in the picture below.



Verification Mode

- ● Password/Fingerprint/Card/Face
- ○ Fingerprint only
- ○ User ID only
- ○ Password
- ○ Card only
- ○ Fingerprint/Password



Verification Mode

- ○ Face only
- ○ Face+Fingerprint
- ○ Face+Password
- ○ Face+Card
- ○ Face+Fingerprint+Card
- ● Face+Fingerprint+Password

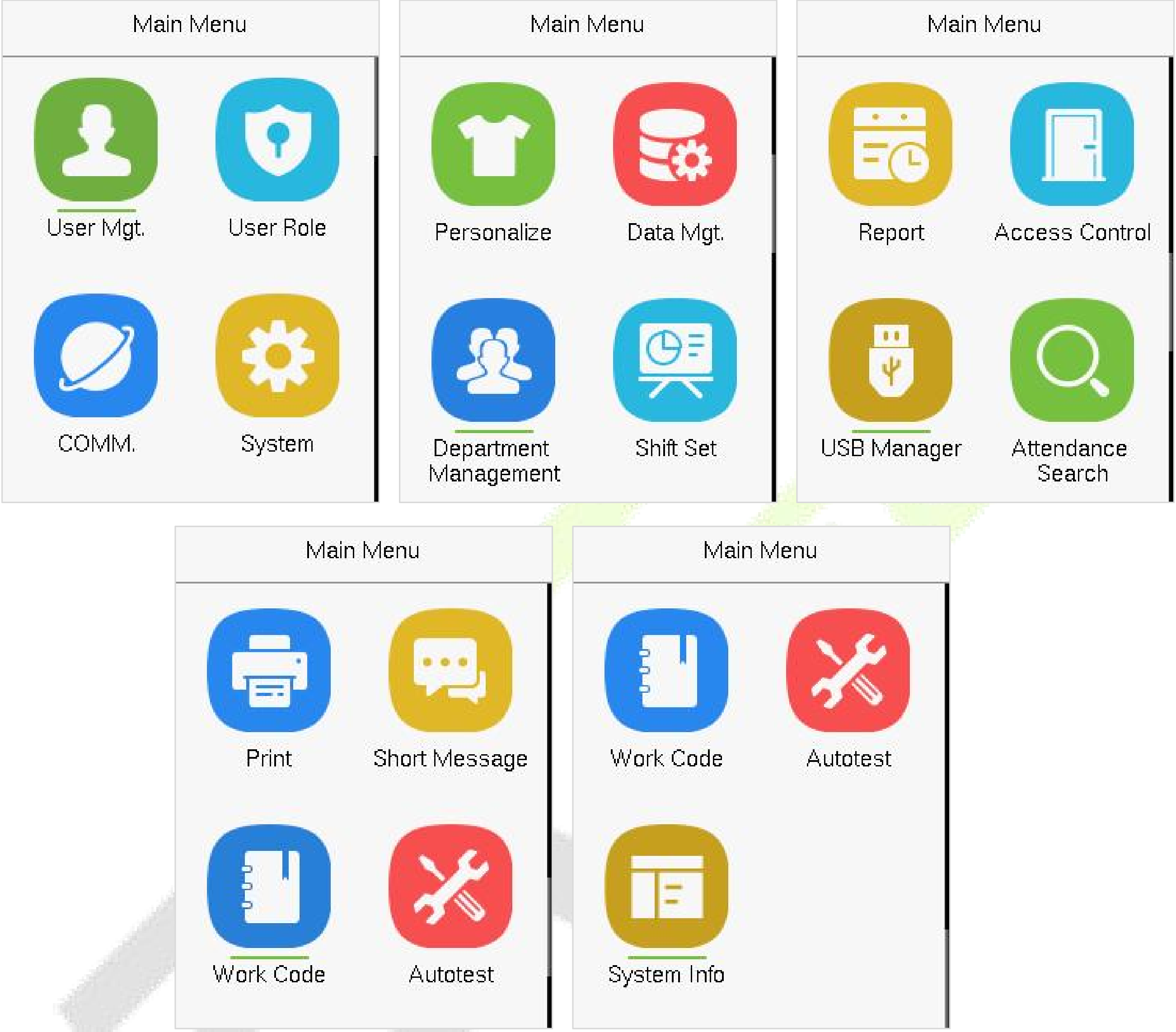
Note:

1) "/" means “or”, and "+" means “and”.

2) You must register the required verification information before using the combination verification mode, otherwise the verification may fail. For example, if a user uses Face Registration but the verification mode is Face + Password, then the user won't be able to pass verification.

2 Main Menu

Click [**M/OK**] on the initial interface to enter the main menu, as shown below:



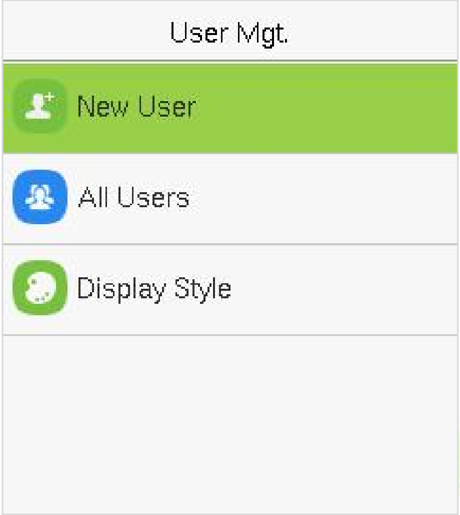
Item	Descriptions
User Mgt.	To add, edit, view, and delete basic information of a user.
User Role	To set the permission scope of the custom role and enroller, that is, the rights to operate the system.
COMM.	To set the relevant parameters of Ethernet, serial comm, PC connection, cellular data network★, wireless network★, cloud server setting★ and network diagnosis.
System	To set parameters related to the system, including date & time, attendance, face, fingerprint, security settings, reset and USB upgrade.

Personalize	To customize settings of interface display, including user interface, voice, bell schedules, punch state options and shortcut key mappings.
Data Mgt.	To delete all relevant data in the device.
Department Management ★	Establish the organizational structure of the department, including functions like adding, editing, or deleting the department, and scheduling the department, etc.
Shift Set ★	Set attendance rules and the number of shifts to be used, and schedule employees. The device supports up to 24 shifts.
Report ★	Use USB flash drive to download the attendance statistics form to check on the computer or download the attendance settings form to set shifts on the computer, assign shifts to employees and then upload the attendance settings form. At this time, the device will give priority to the use of the schedule of the settings form.
Access Control	To set the parameters of the lock and the relevant access control device.
USB Manager	To transfer data such as user data and attendance logs from the USB disk to the supporting software or other devices.
Attendance Search	Query the specified access record, check attendance photos, and blocklist T&A photos.
Print ★	To set printing information and functions (if printer is connected to the device).
Short Message	Used to set a public or private short message. The short message will be displayed to a specified person in the specified time after work attendance check, which facilitates information transfer.
Work Code ★	Used to identify different work types, which facilitates work attendance check.
Auto test	To automatically test whether each module functions properly, including the screen, audio, camera, 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 New Users

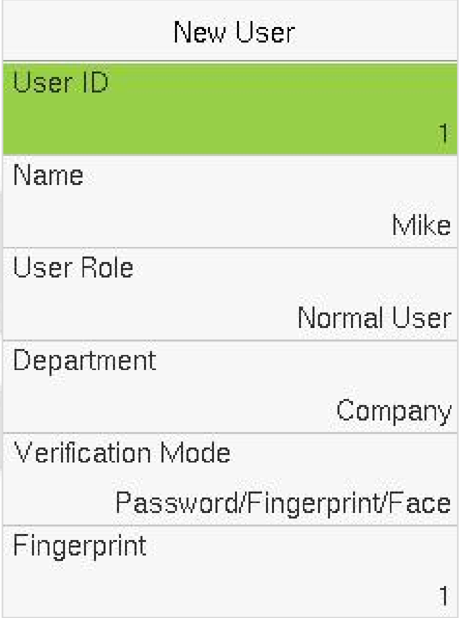
Select **User Mgt.** on the main menu and select **New User**.



User Mgt.

- **Register a User ID and Name:**

Enter the User ID and Name by selecting the respective options.



New User

User ID: 1

Name: Mike

User Role: Normal User

Department: Company

Verification Mode: Password/Fingerprint/Face

Fingerprint: 1

Note:

1) A username can contain a maximum of 17 characters.

2) The user ID may contain 1 to 9 digits by default.

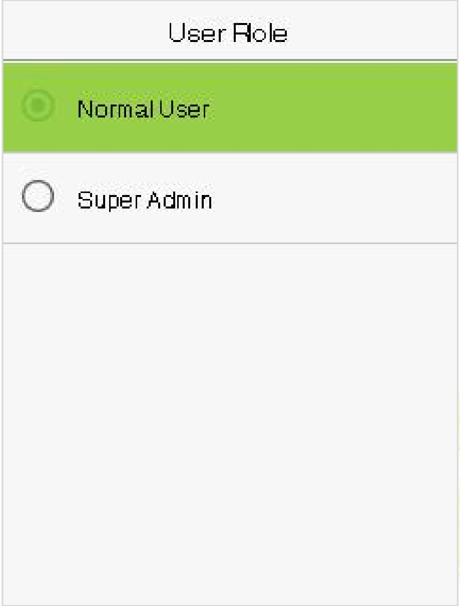
3) You can modify your ID only during the initial registration and can't be modified later.

4) The User ID cannot be duplicated. If there is a voice prompt about duplicate User ID, then you need to choose another User ID that should be unique.

- **Setting the User Role**

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

Select **User Role** to set Normal User or Super Admin.



User Role

● Normal User

○ Super Admin

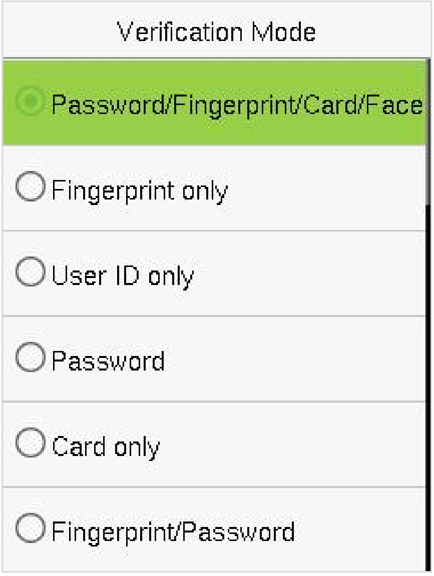
Note: If the selected user role is the Super Admin, the user must pass the identity authentication to access the main menu. The authentication is based on the authentication method(s) that the super administrator has registered.

- **Setting the Verification Mode:**

The verification mode available in the device are:

- Password/ Fingerprint/ Card/ Face
- Fingerprint only
- User ID only
- Password
- Card only
- Fingerprint/ Password
- Fingerprint/ Card
- User ID + Fingerprint
- Fingerprint + Password
- Fingerprint + Card
- Fingerprint + Password + Card
- Password + Card
- Password/ Card
- User ID + Fingerprint + Password
- Fingerprint + (Card/ User ID)
- Face only
- Face + Fingerprint
- Face + Password
- Face + Card
- Face + Fingerprint + Card
- Face + Fingerprint + Password

Select the required **Verification Mode** to set individual verification mode for the user. Select **M/OK** to save and return to the New User interface.



Verification Mode

● Password/Fingerprint/Card/Face

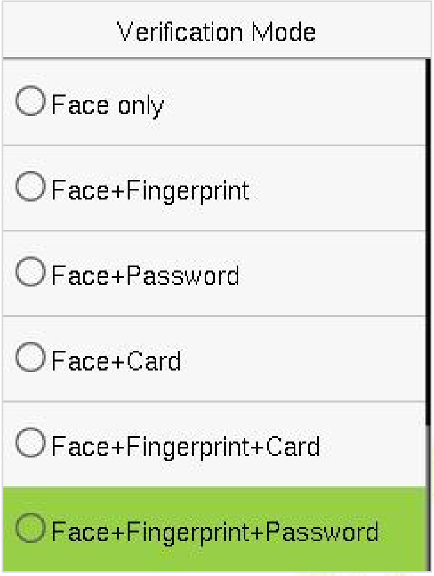
○ Fingerprint only

○ User ID only

○ Password

○ Card only

○ Fingerprint/Password



Verification Mode

○ Face only

○ Face+Fingerprint

○ Face+Password

○ Face+Card

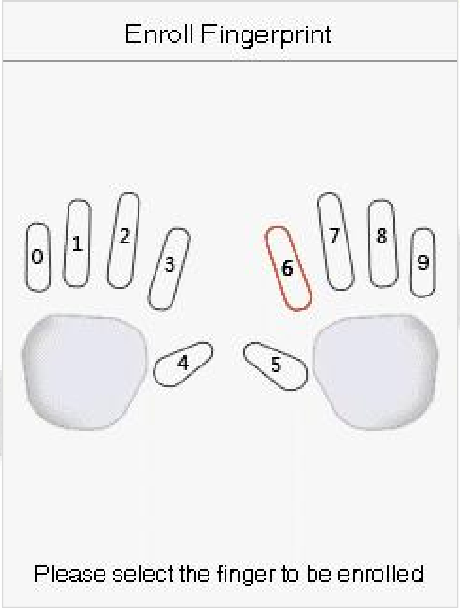
○ Face+Fingerprint+Card

● Face+Fingerprint+Password

- **Register fingerprint:**

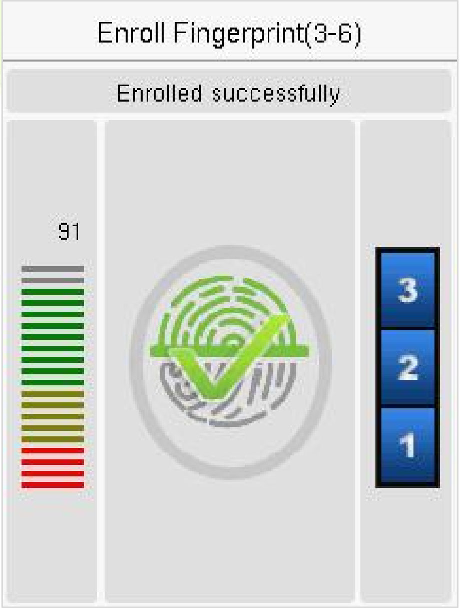
Select **Fingerprint** to enter the enroll fingerprint page. Users can choose one or more fingerprint(s) to enroll.

Press the finger horizontally onto the fingerprint sensor. The registration interface is shown below:



Enroll Fingerprint

Please select the finger to be enrolled

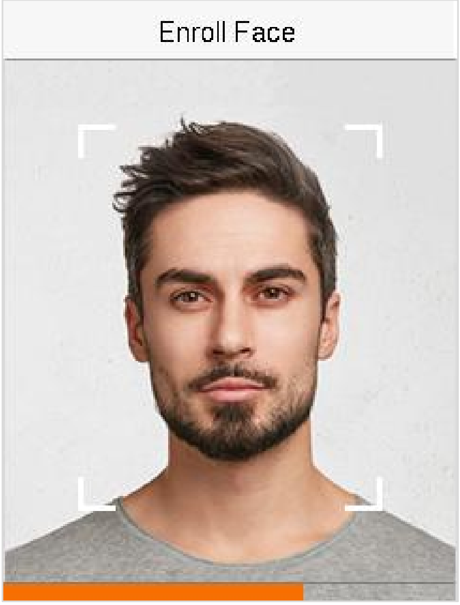


Enroll Fingerprint(3-6)

Enrolled successfully

- **Register Face:**

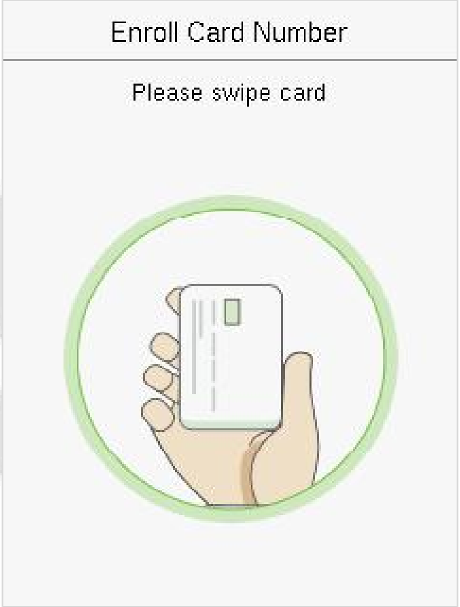
Select **Face** on the Verification mode to enter the face registration page. Users need to face the camera such that their whole face is visible on the device's screen and all the important features of the face are visible. Then stay still for a while during face registration. The registration interface is as follows:



- **Register Card:**

Select **Card** on the Verification mode page to enter the card registration page. On the Card interface, swipe the card underneath the card reading area. The card registration will be successful.

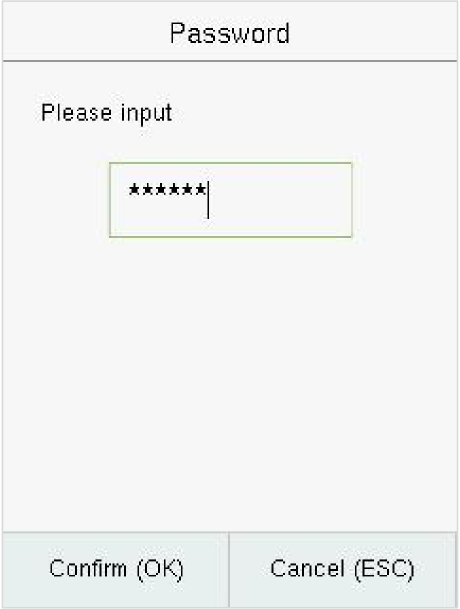
If the card is registered already then, the “Duplicate Card” message shows up. The registration interface is as follows:


Enroll Card Number

Please swipe card

- **Register password:**

Select **Password** on the Verification mode page to enter the password registration page. Enter a password and re-enter it. Select **M/OK**. If the two entered passwords are the same, the system will return to the New User interface.


Password

Please input

******

Confirm (OK) Cancel (ESC)

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

- **Register user photo:**

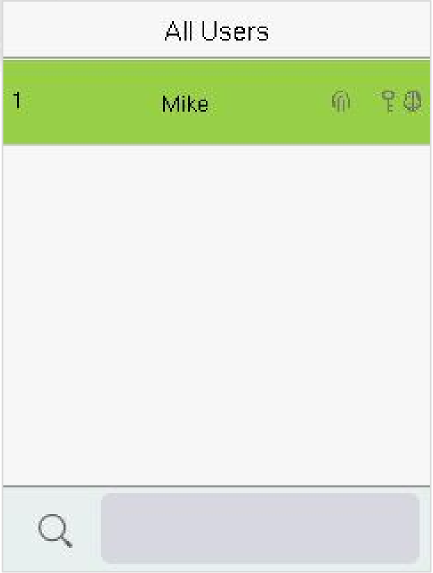
When a user registered with a photo passes the authentication, the registered photo will be displayed.

Select **User Photo**, Select **M/OK** to take a photo. Then Select **ESC** to exit and return to the New User interface.

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

3.2 All Users

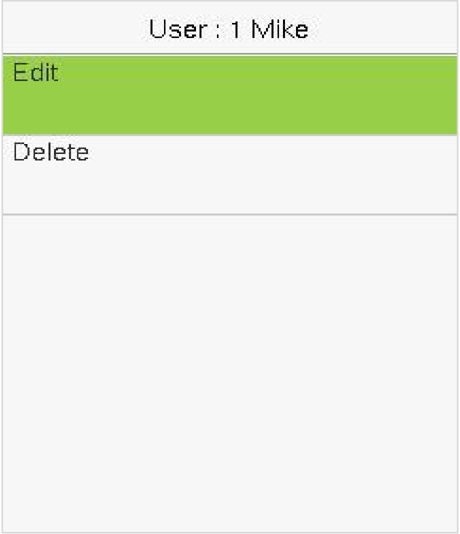
Select the **All Users** option in the **User Mgt.** Then enter the retrieval keyword in the search bar of the user list (keyword may be an ID, surname, or full name). The system will search for the users related to the entered information.


All Users

1 Mike

3.3 Edit Users

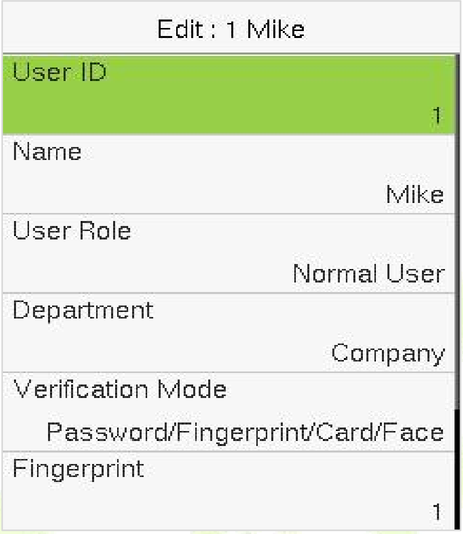
Choose a user from the list and select **Edit** to enter the **Edit** user interface:



User : 1 Mike

Edit

Delete



Edit : 1 Mike

User ID
1

Name
Mike

User Role
Normal User

Department
Company

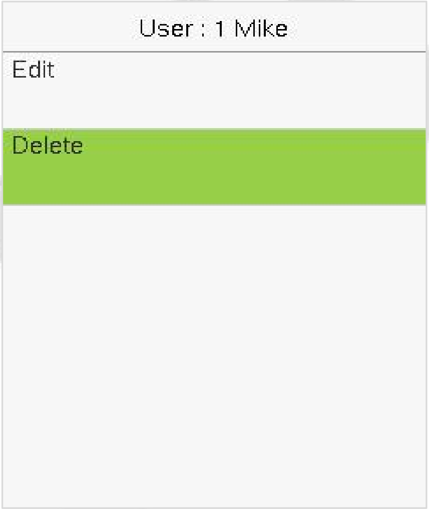
Verification Mode
Password/Fingerprint/Card/Face

Fingerprint
1

Note: The operation of editing a user is the same as that of adding a user, except that the user ID cannot be modified when editing a user’s detail.

3.4 Deleting Users

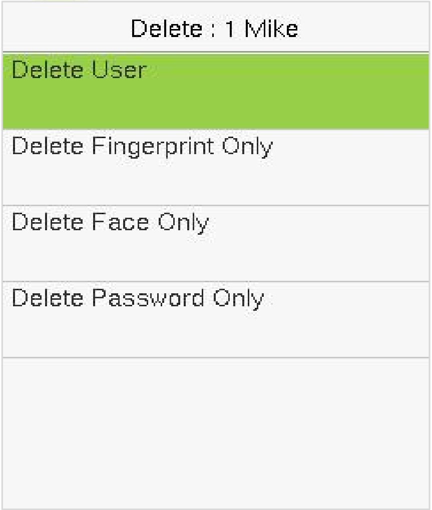
Choose a user from the list and select **Delete** to enter its interface. Select the user information to be deleted and click **M/OK**.



User : 1 Mike

Edit

Delete



Delete : 1 Mike

Delete User

Delete Fingerprint Only

Delete Face Only

Delete Password Only

Note:

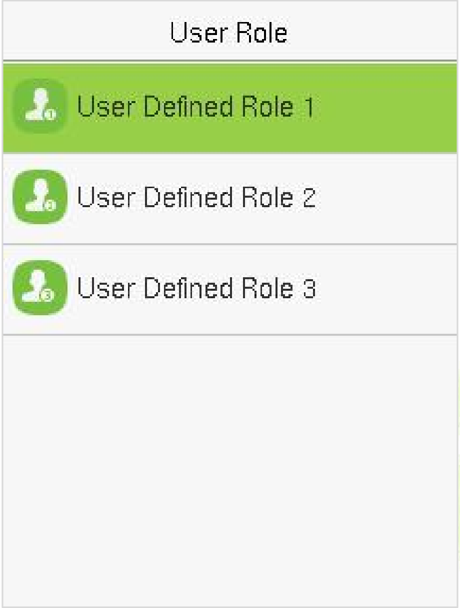
If you select "**Delete User**," all information of the user will be deleted. Only fingerprint data is removed if "**Delete Fingerprint Only**" is selected. Similarly, only face data is removed if "**Delete Face Only**" is selected. Finally, only the password is removed if "**Delete Password Only**" is selected.

4 User Role

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

You may set the permission scope of the custom role (up to 3 roles) and enroller.

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



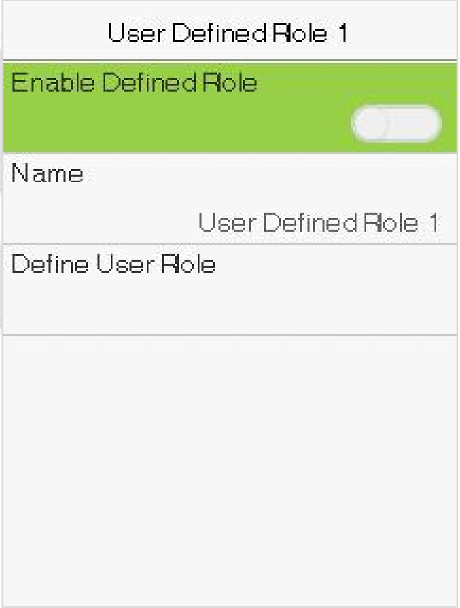
User Role

User Defined Role 1

User Defined Role 2

User Defined Role 3

1. Select an item to set a defined role. Select the **Enable Defined Role** option to enable this defined role. Select **Name** and enter the name of the role.



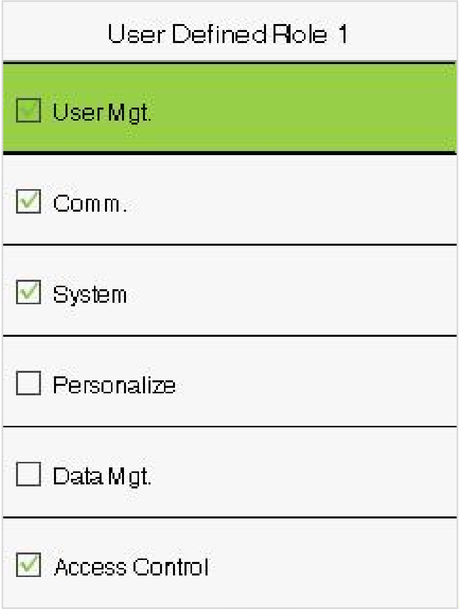
User Defined Role 1

Enable Defined Role

Name: User Defined Role 1

Define User Role

2. Select **Define User Role** to assign the privileges to the role. Click **ESC** to save and return after the privilege assignment is complete.



User Defined Role 1

☑ User Mgt.

☑ Comm.

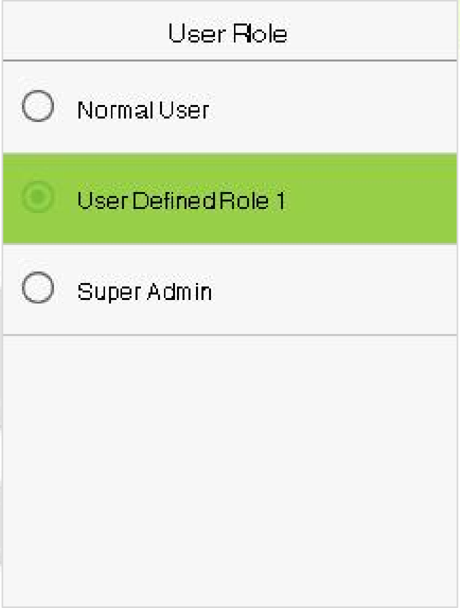
☑ System

□ Personalize

□ Data Mgt.

☑ Access Control

Note: You need to select the features in sub-menus. If the device has a role enabled, you may assign the roles you set to users by selecting **User Mgt. > New User > User Role.**



User Role

○ Normal User

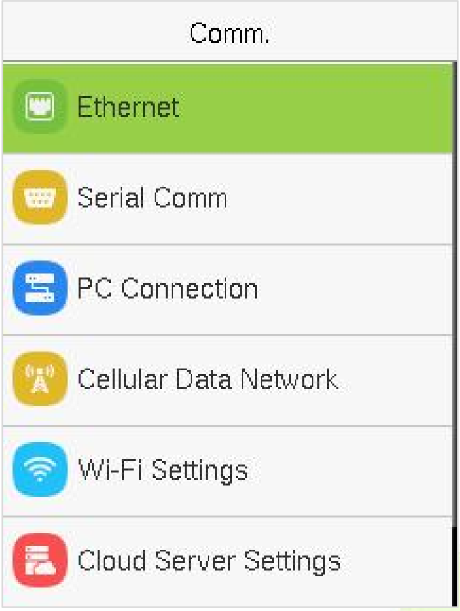
● User Defined Role 1

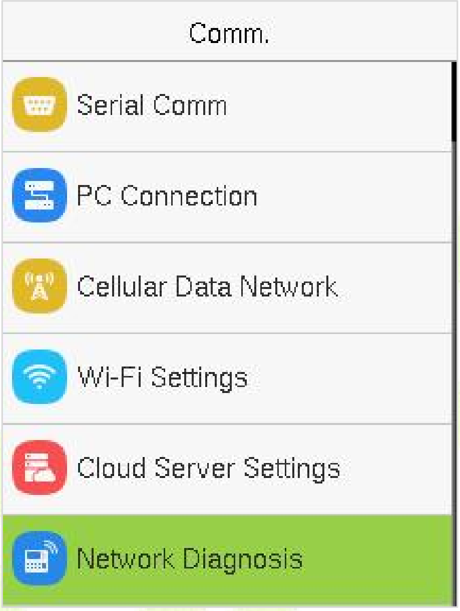
○ Super Admin

If no super administrator is registered, the device will prompt "**Please register super administrator user first!**" after selecting the enable bar.

5 Communication Settings

Select **COMM.** on the main menu to get into communication settings and set parameters of the Ethernet, Serial Comm, PC Connection, Cellular Data Network, Wi-Fi Settings, Cloud Server Settings and Network Diagnosis.

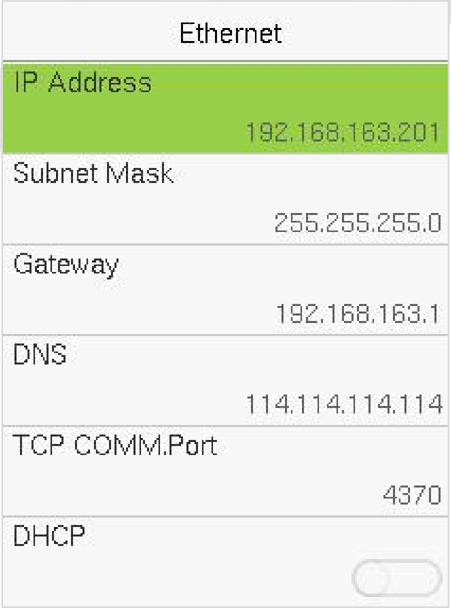




5.1 Ethernet

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.



Ethernet

IP Address 192.168.163.201

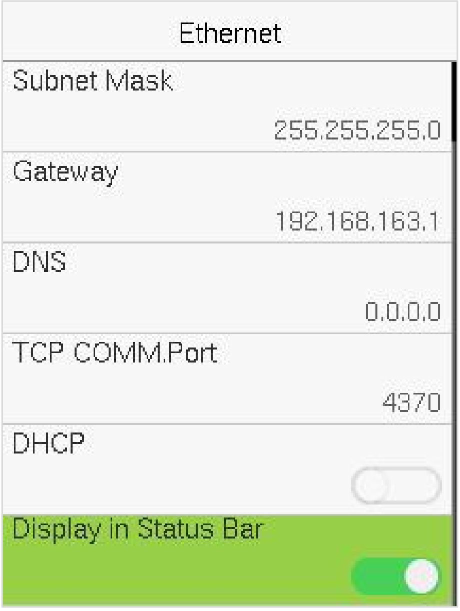
Subnet Mask 255.255.255.0

Gateway 192.168.163.1

DNS 114.114.114.114

TCP COMM.Port 4370

DHCP ○



Ethernet

Subnet Mask 255.255.255.0

Gateway 192.168.163.1

DNS 0.0.0.0

TCP COMM.Port 4370

DHCP ○

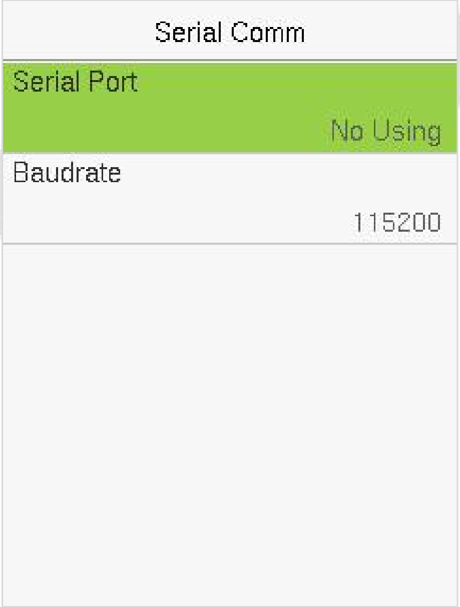
Display in Status Bar ●

Item	Descriptions
IP Address	The factory default value is 192.168.1.201. Please set them according to the actual network situation.
Subnet Mask	The factory default value is 255.255.255.0. Please set them according to the actual network situation.
Gateway	The default Gateway address is 0.0.0.0. It can be modified according to the network availability.
DNS	The factory default address is 0.0.0.0. Please set them according to the actual network situation.
TCP COMM. Port	The factory default value is 4370. Please set them according to the actual network situation.
DHCP	Dynamic Host Configuration Protocol helps in dynamically allocating IP addresses for clients via server.
Display in Status Bar	To set whether to display the network icon on the status bar.

5.2 Serial Comm

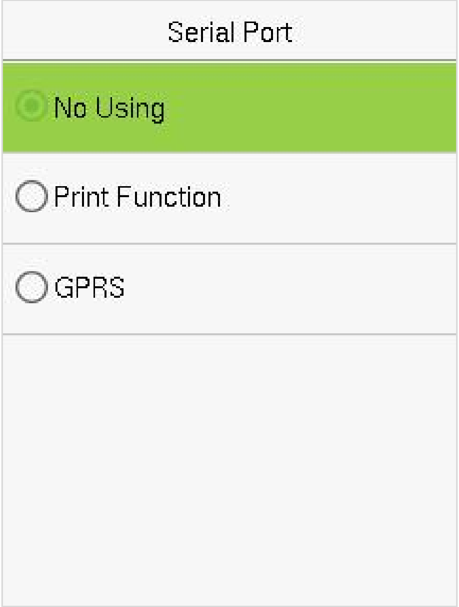
Serial Comm function establishes communication with the device through a serial port (Printer/ GPRS).

Select **Serial Comm** on the **Comm.** Settings interface.



Serial Port: No Using

Baudrate: 115200



● No Using

○ Print Function

○ GPRS

Item	Descriptions
Serial Port	**No Using:** No communication with the device through the serial port. **Print Function:** The device can be connected to the printer when serial port enables the print function.

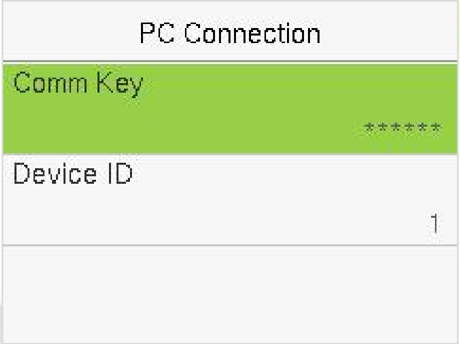
	GPRS: Communication with the device via GPRS serial port. (**Note:** Insert a GPRS capable SIM card into the GPRS module before using the GPRS function.)
Baud Rate	There are 4 baud rate options at which the data communicates with PC. They are: 115200 (default), 57600, 38400, and 19200. The higher is the baud rate, the faster is the communication speed, but also the less reliable. Hence, a higher baud rate can be used when the communication distance is short; when the communication distance is long, choosing a lower baud rate is more reliable.

5.3 PC Connection

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

The connection password needs to be entered before the device can be connected to the PC software if a Comm Key is set.

Select **PC Connection** on the **Comm.** Settings interface to set **Comm Key**.



PC Connection

Comm Key
******

Device ID
1

Item	Descriptions
Comm Key	The default password is 0, which can be changed later. The Comm Key may contain1to 6 digits.
Device ID	It is the identification number of the device, which ranges between 1 and 254. If the communication method is RS232/RS485, you need to input this device ID in the software communication interface.

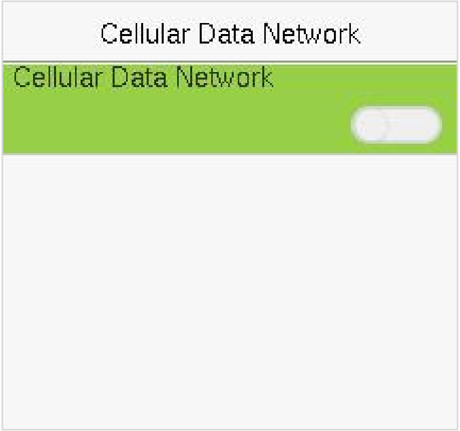
5.4 Cellular Data Network ★

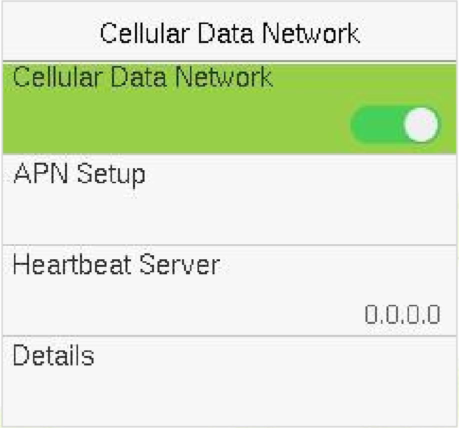
When the equipment is in the Dial-Up Network, make sure the device is in the coverage of GPRS or WCDMA signal, and it is must know of the used modem type, APN name and access number and so on.

Before enabling, please insert the All-in-one card into the 4G module first.

Then select **Cellular Data Network** on the **Comm.** Settings interface to enter the setting interface.

Toggle the button to enable the Cellular Data Network. Under normal circumstances, the device will automatically connect to the mobile network after being enabled. If you cannot connect, you can manually set the relevant parameters to connect. When the mobile network is connected successfully, the initial interface will display the mobile network 4G logo.





Item	Descriptions
Cellular Data Network	Whether to enable access to the mobile network.
APN Setup	Used to set APN information, such as the access number, username, and password
Heartbeat Server	To collect attendance records from the device by using the data collection software provided by ZKTeco. After you set the server IP address for the device correctly, the device will send attendance records to the heartbeat server automatically.
Details	Includes information about the connected mobile network, such as the network mode, telecom operator, IP address, and received and sent data.

5.5 Wi-Fi Settings ★

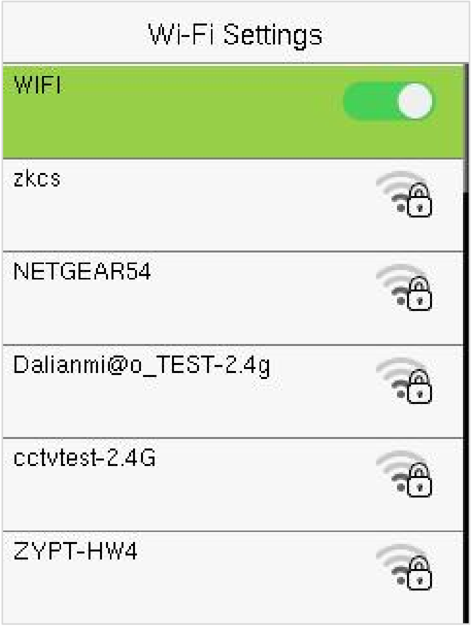
The device provides a Wi-Fi module, which can be built-in within the device module or can be externally connected.

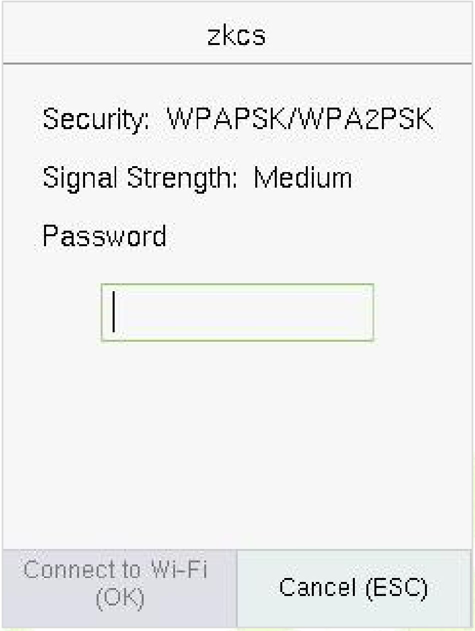
The Wi-Fi module enables data transmission via Wi-Fi (Wireless Fidelity) and establishes a wireless network environment. Wi-Fi is enabled by default in the device. If you don't need to use the Wi-Fi network, you can toggle the Wi-Fi to disable the button.

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

- **Searching the Wi-Fi Network:**

1) WIFI is enabled in the device by default. Toggle the button to enable or disable Wi-Fi.
2) Once the Wi-Fi is turned on, the device searches for the available Wi-Fi within the network range.
3) Choose the required Wi-Fi name from the available list and input the correct password in the password interface, and then select **Connect to Wi-Fi (OK)** and press **[M/OK]** to confirm.





Security: WPAPSK/WPA2PSK

Signal Strength: Medium

Password

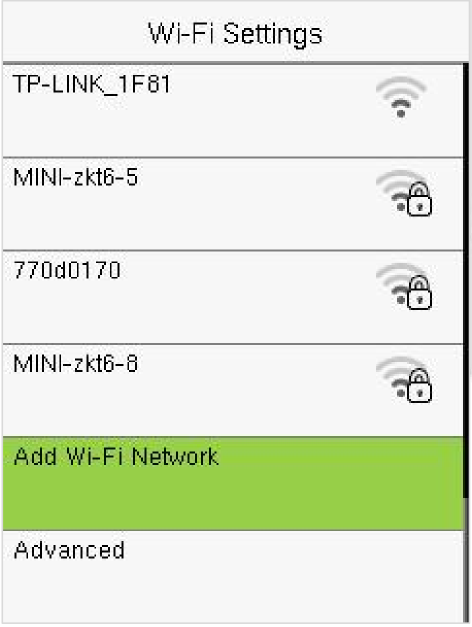
WIFI Enabled: Choose the required network from the searched network list.

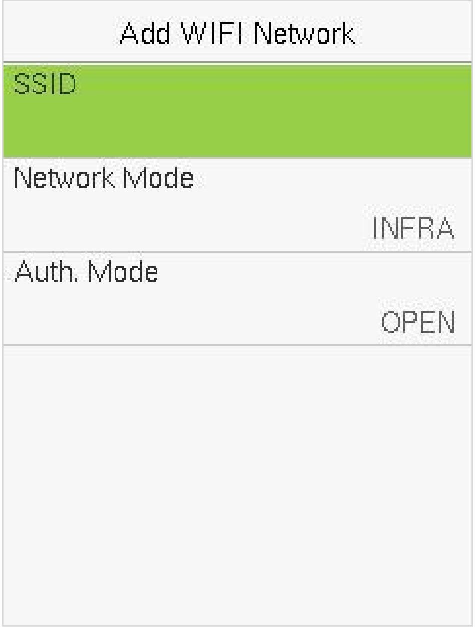
Click the password field to enter the password, and then select **Connect to Wi-Fi (OK)** and press **[M/OK]** to save.

4) 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.





Network Mode INFRA

Auth. Mode OPEN

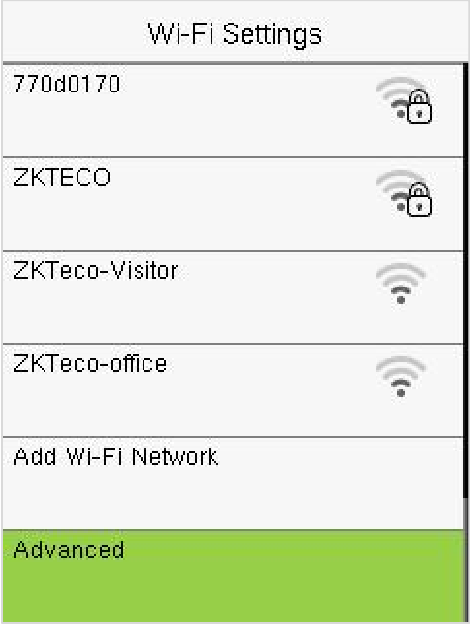
Select **Add Wi-Fi Network** to add the Wi-Fi manually and press **[M/OK]**.

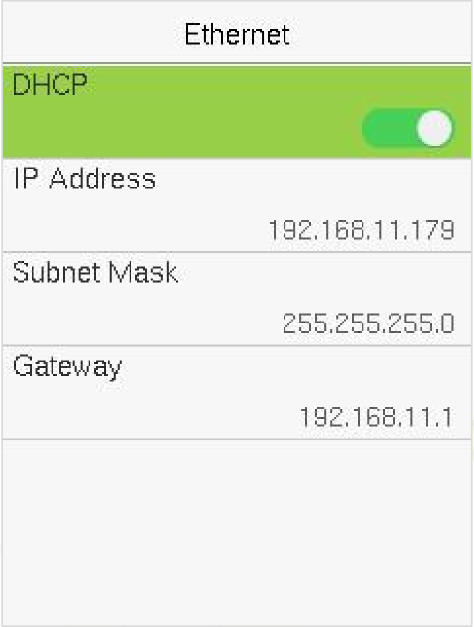
On this interface, enter the Wi-Fi network parameters (the added network must exist.)

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

- **Advanced Setting:**

On the **Wi-Fi Settings** interface, select **Advanced** to set the relevant parameters as required.





Ethernet

DHCP: on

IP Address: 192.168.11.179

Subnet Mask: 255.255.255.0

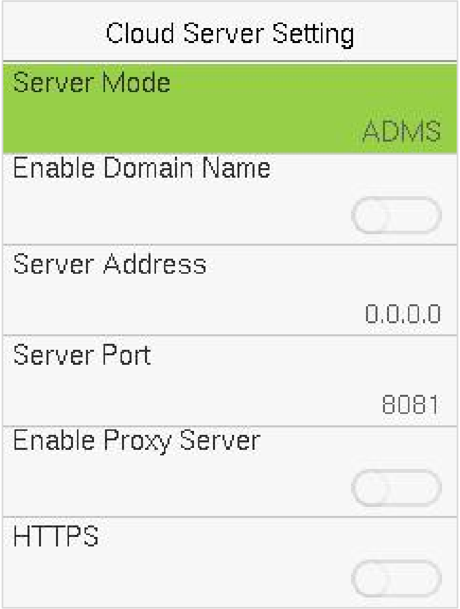
Gateway: 192.168.11.1

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	The 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. It can be modified according to the network availability.

5.6 Cloud Server Settings ★

The Cloud Server setting option helps to set different configurations used for connecting with the ADMS server.

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



Cloud Server Setting

Server Mode: ADMS

Enable Domain Name

Server Address: 0.0.0.0

Server Port: 8081

Enable Proxy Server

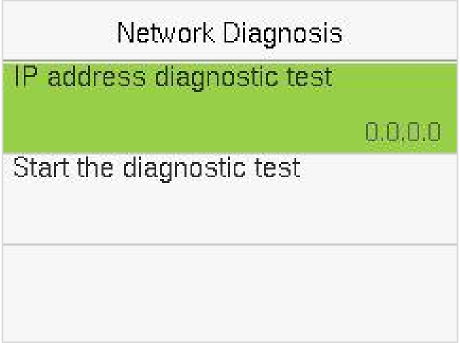
HTTPS

Item		Description
Enable Domain Name	**Server Address**	When enabled, the domain name mode "http://..." is used, such as http://www.XYZ.com, while "XYZ" denotes the domain name.
Disable Domain Name	**Server Address**	The IP address of the ADMS server.
	Server Port	Port used by the ADMS server.
Enable Proxy Server		When a proxy is enabled, you need to set the IP address and port number of the proxy server.
HTTPS		It is an HTTP channel with security as its goal. Based on HTTP, transmission encryption and identity authentication ensure the security of the data transmission process.

5.7 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 click **Start the diagnostic test** to check whether the network can connect to the device.



Network Diagnosis

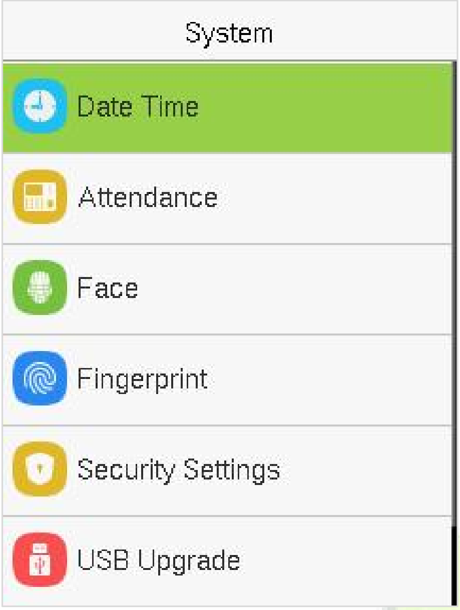
IP address diagnostic test: 0.0.0.0

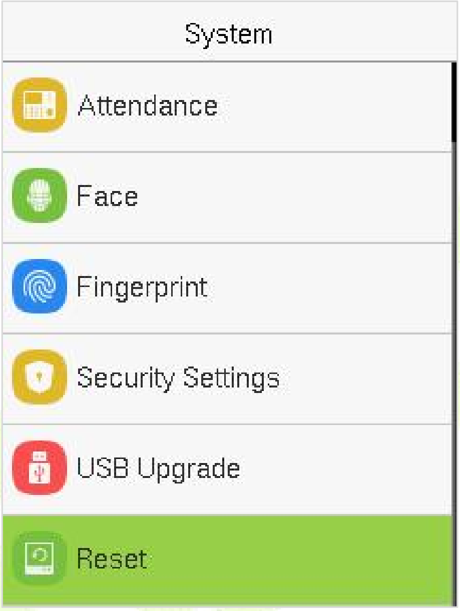
Start the diagnostic test

6 System Settings

It helps to set related system parameters to optimize the performance and usability of the device.

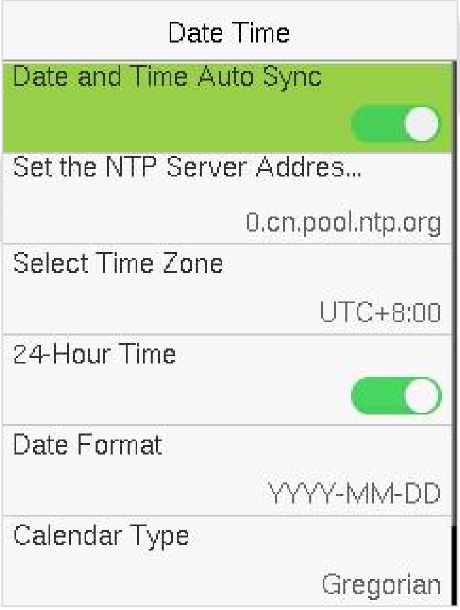
Select **System** on the main menu interface.





6.1 Date and Time

Select **Date Time** on the System Setting interface.



Date Time

Date and Time Auto Sync

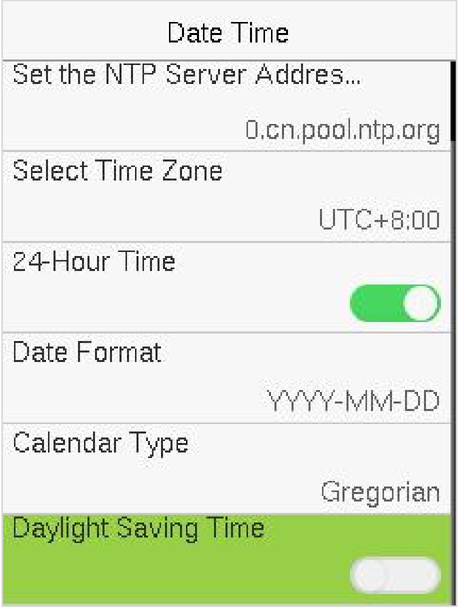
Set the NTP Server Addres... 0.cn.pool.ntp.org

Select Time Zone UTC+8:00

24-Hour Time

Date Format YYYY-MM-DD

Calendar Type Gregorian



Date Time

Set the NTP Server Addres... 0.cn.pool.ntp.org

Select Time Zone UTC+8:00

24-Hour Time

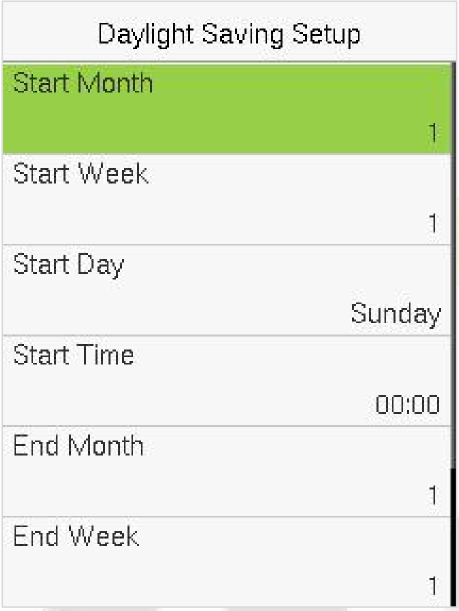
Date Format YYYY-MM-DD

Calendar Type Gregorian

Daylight Saving Time

Item	Descriptions
Date and Time Auto Sync	Automatically determine the time and date of the main interface. You must set the NTP server address, automatically determine the time and date, and select the time zone to take effect.

Set the NTP Server Address	The IP address of the NTP server.
Select Time Zone	To manually select the time zone where the device is located.
24-Hour Time	The device displays 24-Hour time format, when enabled.
Date Format	Select the date format.
Daylight Saving Time	To enable or disable the function. If enabled, tap Daylight Saving Mode to select a daylight-saving mode and then tap Daylight Saving Setup to set the switch time.



Daylight Saving Setup

Start Month
1

Start Week
1

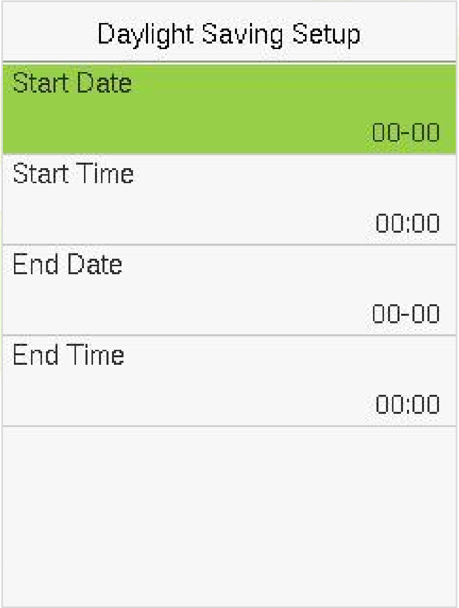
Start Day
Sunday

Start Time
00:00

End Month
1

End Week
1

Week Mode



Daylight Saving Setup

Start Date
00-00

Start Time
00:00

End Date
00-00

End Time
00:00

Date Mode

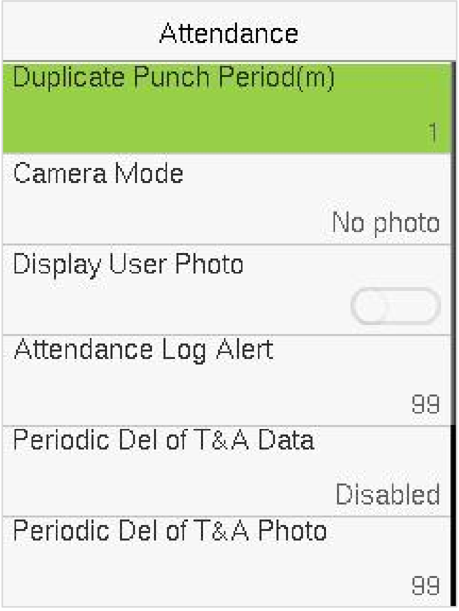
Note:

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

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 device will remain 18:30 on January 1, 2020.

6.2 Attendance

Select **Attendance** on the System interface to alter the attendance rules as required.



Attendance

Duplicate Punch Period(m)
1

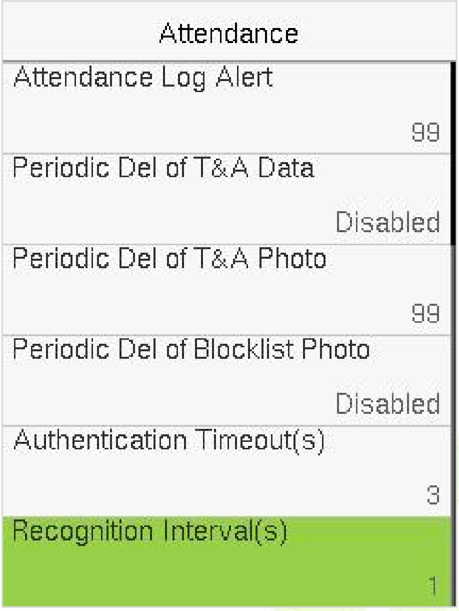
Camera Mode
No photo

Display User Photo
○

Attendance Log Alert
99

Periodic Del of T&A Data
Disabled

Periodic Del of T&A Photo
99



Attendance

Attendance Log Alert
99

Periodic Del of T&A Data
Disabled

Periodic Del of T&A Photo
99

Periodic Del of Blocklist Photo
Disabled

Authentication Timeout(s)
3

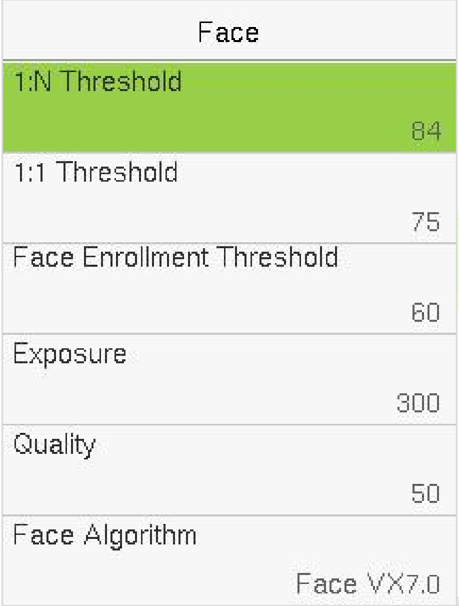
Recognition Interval(s)
1

Item	Description
Duplicate Punch Period (m)	Within a set time (unit: minutes), the duplicated attendance logs will not be reserved (value ranges from 1 to 999999 minutes).
Camera Mode	Choose whether to capture and save the current snapshot image during verification. 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	Choose whether to display the user photo when the user passes the verification.
Attendance Log Alert	When the remaining storage is smaller than the set value, the device will automatically alert users to the remaining storage information. It can be disabled or set to a value ranged from 1 to 9999.
Periodic Del of T&A Data	The number of attendance logs allowed to be deleted at once when the maximum storage is attained. It can be disabled or set to a value ranged from 1 to 999.
Periodic Del of T&A Photo	When attendance photos reach its maximum 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 block listed photos reach its maximum 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 time interval for which the "**Successful Verification**" message displays. Valid value: 1~9 seconds.
Recognition Interval(s)	After the interval identifying is clicked (selected), for example, if the recognition 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

Select **Face** option on the System interface.



Face

1:N Threshold 84

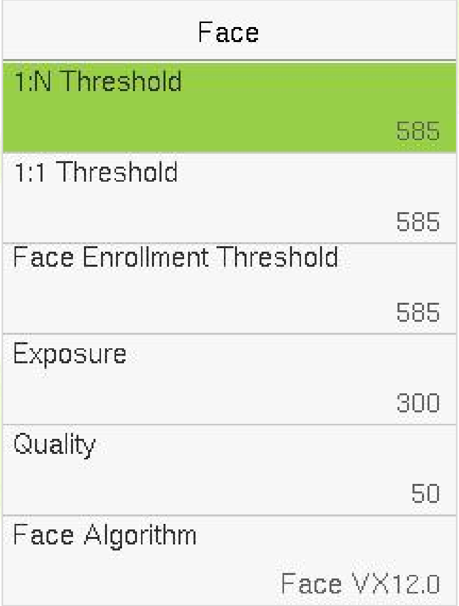
1:1 Threshold 75

Face Enrollment Threshold 60

Exposure 300

Quality 50

Face Algorithm Face VX7.0



Face

1:N Threshold 585

1:1 Threshold 585

Face Enrollment Threshold 585

Exposure 300

Quality 50

Face Algorithm Face VX12.0

Item	Description
1:N Threshold	Under 1:N (One to Many) 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 55 to 1000. The higher the thresholds, the lower the misjudgement rate and higher the rejection rate, and vice versa. The default value for Face VX7.0 is 84, and the default value for Face VX12.0 is 585. It is recommended to use the default value.
1:1 Threshold	Under 1:1 (One to One) verification mode, the verification will only be successful when the similarity between the acquired facial image and the facial templates enrolled in the device is greater than the set value. The valid value ranges from 55 to 1000. The higher the thresholds, the lower the misjudgement rate and higher the rejection rate, and vice versa. The default value for Face VX7.0 is 75, and the default value for Face VX12.0 is 585. It is recommended to use the default value.

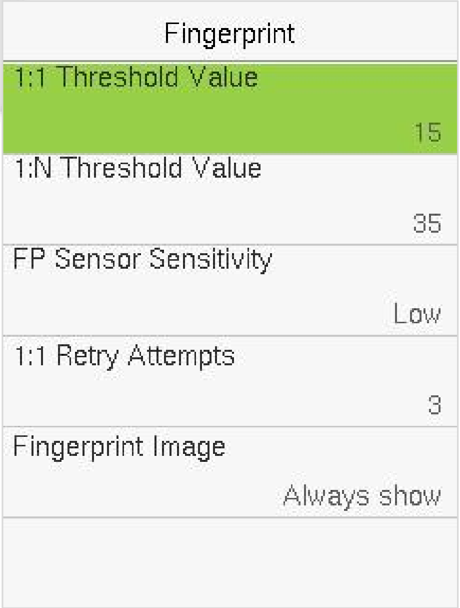
Face Enrollment Threshold	During face enrollment, 1:N (One to Many) comparison is used to determine whether the user has already registered before. When the similarity between the acquired facial image and all registered facial templates is greater than this threshold, it indicates that the face has already been registered. The valid value ranges from 0 to 1000. The default value for Face VX7.0 is 60, and the default value for Face VX12.0 is 585.
Exposure	When the face is in front of the camera, the brightness of the face area increases, and other areas become darker. The valid value ranges from 40 to 1000.
Quality	It sets the image quality for facial registration and comparison. The higher the value, the clearer the image required. The valid value ranges from 50 to 150.
Face Algorithm	Used to switch or view the version of the face algorithm. When selecting an algorithm, make sure to choose carefully. Switchable between Face VX7.0 and Face VX12.0. However, upgrading to the VX12.0 algorithm will reduce the number of face templates from 1,500 to 900 and reset the device's data.

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.

6.4 Fingerprint

Select **Fingerprint** option on the System interface.



Fingerprint

1:1 Threshold Value: 15

1:N Threshold Value: 35

FP Sensor Sensitivity: Low

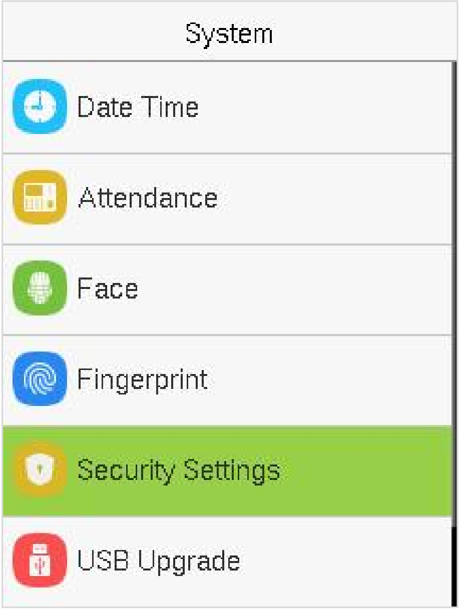
1:1 Retry Attempts: 3

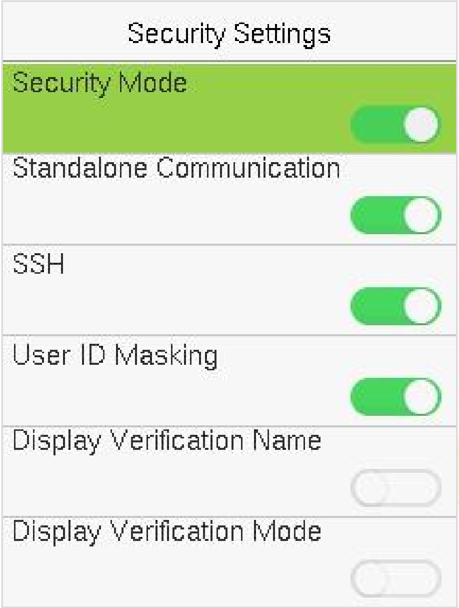
Fingerprint Image: Always show

Item	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 threshold 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 threshold value.
FP Sensor Sensitivity	To set the sensibility of fingerprint acquisition. It is recommended to use the default level "**Medium"** in normal conditions. 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	To choose whether to display the fingerprint image on the screen during fingerprint enrolment or verification. Four choices are available: **Show for enrol**: To display the fingerprint image on the screen only during enrolment. **Show for match**: To display the fingerprint image on the screen only during verification. **Always show**: To display the fingerprint image on the screen during enrolment and verification. **None**: Not to display the fingerprint image.

6.5 Security Settings

Select **Security Settings** option on the System interface.




Security Settings

Security Mode ●

Standalone Communication ●

SSH ●

User ID Masking ●

Display Verification Name ○

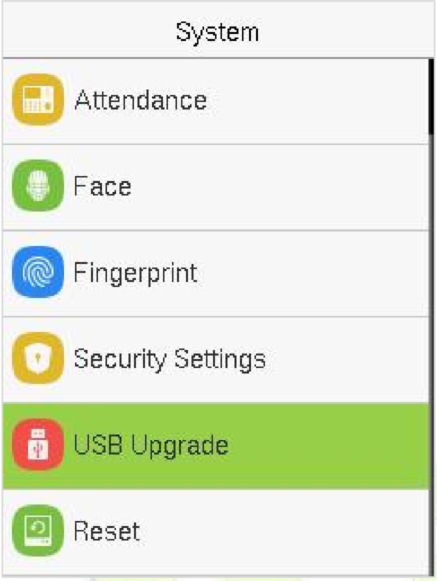
Display Verification Mode ○

Item	Description
Security Mode	When enabled, user information verification has a high level of security. This function can be enabled or disabled via the menu interface. When switching on and off, there are security prompts. All data will be deleted and the device will be restarted after confirmation. **Note:** After turning on the security mode, the product will forcibly enable the function of returning to the standby interface when the menu times out by default (default 60s). It does not support disabling in security mode, but it does support disabling in non-security mode. To configure, go to **Personalize > User Interface > Menu Screen Timeout(s)**.
Standalone Communication	By default, this function is disabled. This function can be enabled or disabled via the menu interface. When it is switched on, a security prompt appears, and the device will restart after you confirm.
SSH	The device does not support the Telnet feature, hence SSH is typically used for remote debugging. By default, SSH is enabled. The menu interface allows you to enable and disable SSH. When enabled, there will be a security prompt, but the device will not need to be restarted after confirmation.
User ID Masking	After enabled, the User ID will be partially displayed after the personnel verification result (only the User ID with more than 2 digits supports the masking display), and it is enabled by default.
Display Verification Name	After enabled, the user's name will be displayed after the personnel verification result. The verification result will not show the name after disabling it.
Display Verification Mode	After enabled, the personnel verification result will show the user's verification mode. The verification result will not show the verification mode after you disable it.

6.6 USB Upgrade

Insert the U disk with upgrade file into the device's USB port, and in the initial interface, press **[M/OK]** > **System** > **USB Upgrade** to complete firmware upgrade operation.

Select **USB Upgrade** option on the System interface.



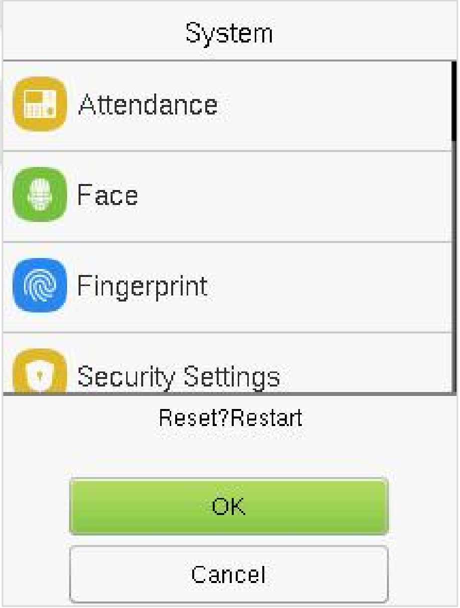
Note: If an upgrade file is needed, please contact our technical support. Deny firmware upgrade under normal circumstances.

6.7 Reset

Restore the device settings to their factory state, such as communication settings, system settings, etc.

(Do not clear registered user data).

Select the **Reset** option on the System interface. Select **OK** to reset.

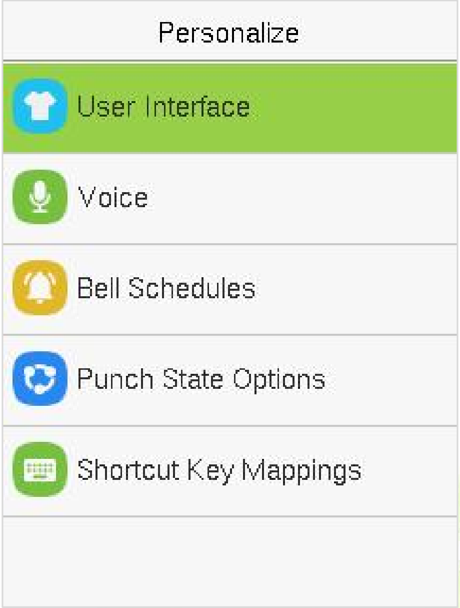


Reset?Restart

7 Personalize

You may customize interface settings under this option.

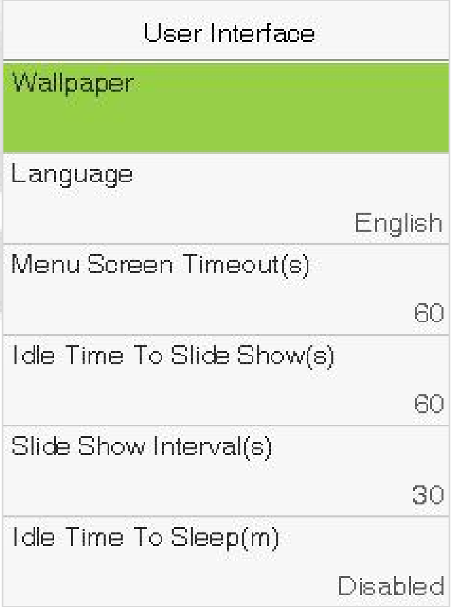
Select **Personalize** option on the main menu interface.



7.1 User Interface

You can customize the display style of the main interface.

Select **User Interface** option on the Personalize interface.


User Interface

Wallpaper

Language: English

Menu Screen Timeout(s): 60

Idle Time To Slide Show(s): 60

Slide Show Interval(s): 30

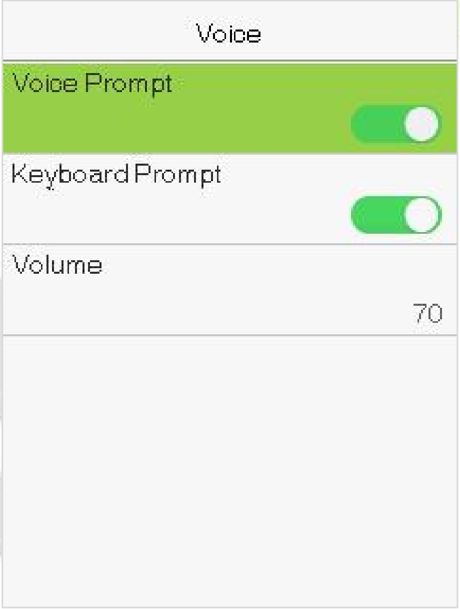
Idle Time To Sleep(m): Disabled

Item	Description
Wallpaper	To select the main screen wallpaper according to your personal preference.
Language	To select the language of the device.

Menu Screen Timeout (s)	When there is no operation on the device, and the time exceeds the set value, then the device will automatically go back to the initial interface. You can disable the function or set the value between 60 and 99999 seconds.
Idle Time To Slide Show (s)	When there is no operation on the device, and the time exceeds the set value, a slide show starts to play. It can be disabled, or you may set the value between 3 and 999 seconds.
Slide Show Interval (s)	It refers to the time interval for switching slide show pictures. The function can be disabled, or you may set the interval between 3 and 999 seconds.
Idle Time to Sleep (m)	If sleep mode is activated when there is no operation, the device enters standby mode. Press any key or finger to resume normal working mode. You can disable this function or set a value within 1-999 minutes.
Main Screen Style	To select the main screen style according to your personal preference.

7.2 Voice

Select **Voice** on the Personalize interface.



Voice

Voice Prompt

Keyboard Prompt

Volume

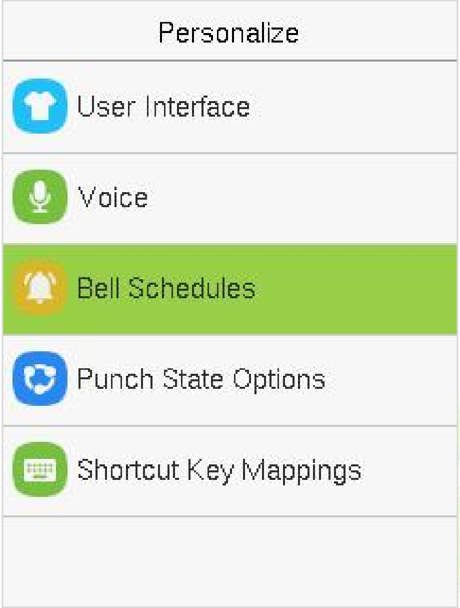
70

Item	Description
Voice Prompt	Select whether to enable voice prompts during operating, press **[M/OK]** to enable it.
Touch Prompt	Select whether to enable keyboard voice while pressing keyboard, press **[M/OK]** to enable it.
Volume	Adjust the volume of device. Press ▶ key to increase the volume, press ◀ key to decrease the volume.

7.3 Bell Schedules

Many companies choose to use the bell to signify on-duty and off-duty time. When reaching the scheduled time for the bell, the device plays the selected ringtone automatically until the ringing duration passes.

Select **Bell Schedules** option on the Personalize interface.



Personalize

User Interface

Voice

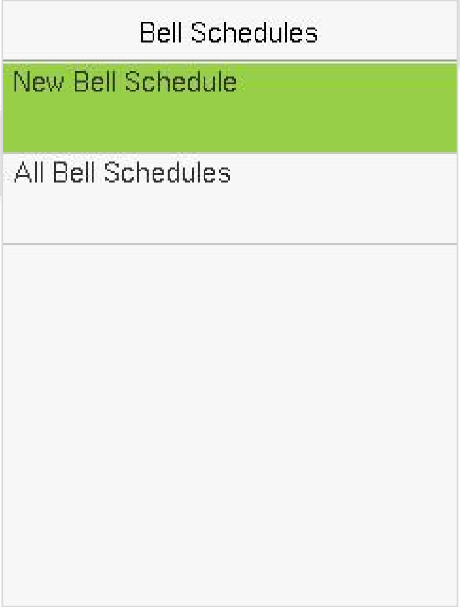
Bell Schedules

Punch State Options

Shortcut Key Mappings

- **Add a Bell**

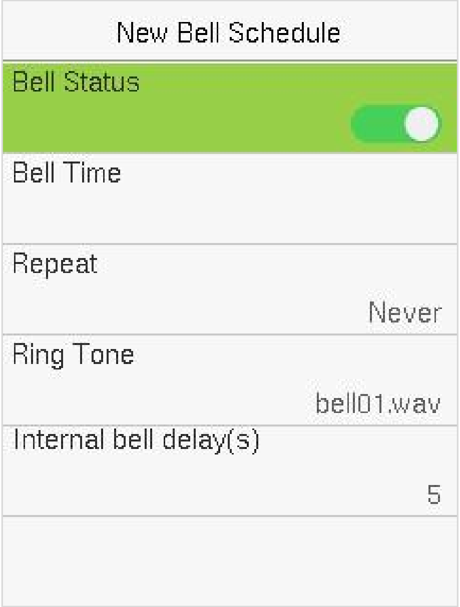
Select **New Bell Schedules** option on the **Bell Schedules** interface. Press **[M/OK]** Bell Status to enable the bell status.



Bell Schedules

New Bell Schedule

All Bell Schedules



New Bell Schedule

Bell Status

Bell Time

Repeat: Never

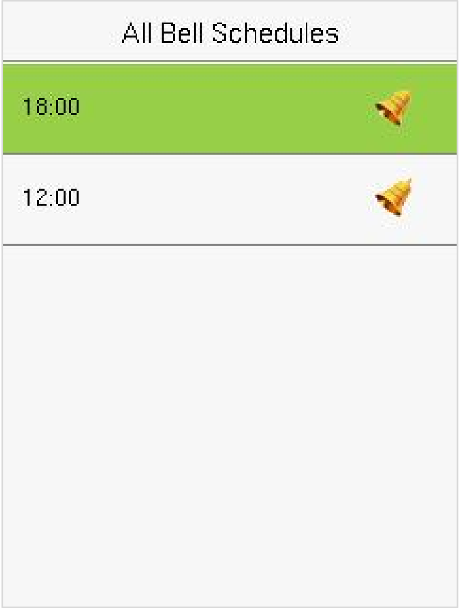
Ring Tone: bell01.wav

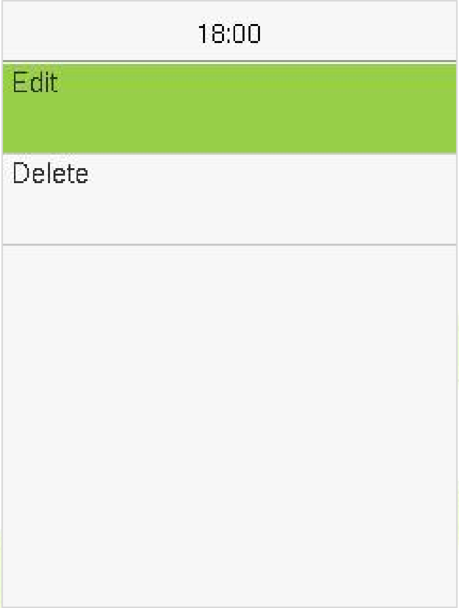
Internal bell delay(s): 5

1. You can manually set the date and time and press [**M/OK**] to save.
2. Set repeat, select a ring tone, and select the internal bell delay.

- **Edit Bell**

On the **All Bell Schedules** interface, select the bell item to be edited.

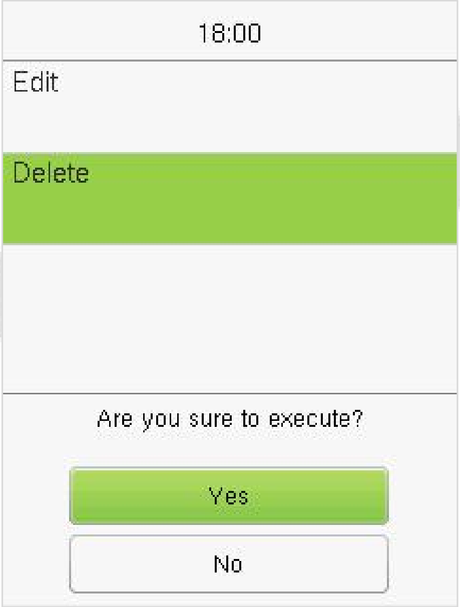




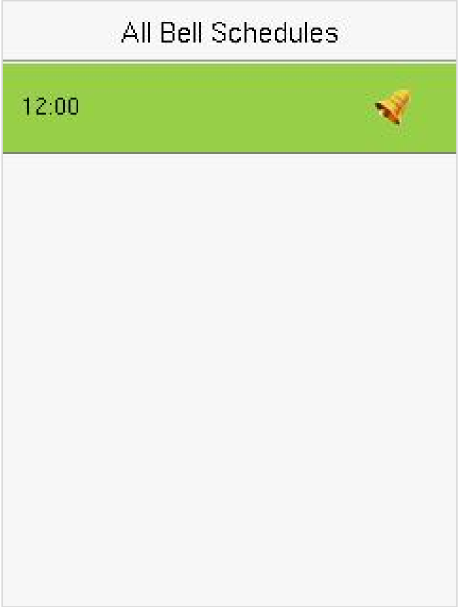
Select **Edit** to edit the bell schedule time. The editing method is the same as that of a new bell.

- **Delete a Bell**

On the **All Bell Schedules** interface, select a bell item to be deleted.



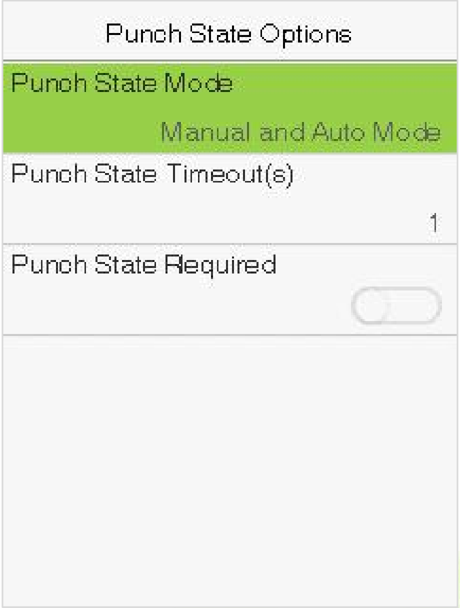
Are you sure to execute?



Select **Delete** and select [**Yes**] to delete the bell schedule.

7.4 Punch States Options

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



Punch State Options

Punch State Mode: Manual and Auto Mode

Punch State Timeout(s): 1

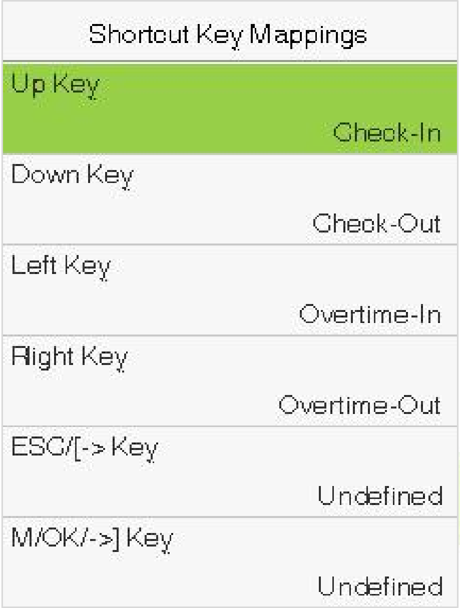
Punch State Required

Item	Description
Punch State Mode	Select a punch state mode under this menu option. The options are: **Off:** Select this to keep the punch state key function disabled. The punch state key set under the **Shortcut Key Mappings** menu becomes invalid. **Manual Mode:** Select to switch the punch state key manually, and the punch state key disappears after **Punch State Timeout**. **Auto Mode:** To make this mode work correctly, the switching time of the punch state key needs to be set in the **Shortcut Key Mappings**. After that, the punch state is automatically fetched by the device according to the switching time in the **Shortcut Key Mapping**. **Manal and Auto Mode:** In this mode, the main interface displays the auto-switching punch state key, meanwhile supports manual switching of the punch state key. After the timeout, the manual switching punch state key becomes an auto-switching punch state key. **Manual Fixed Mode:** In this mode, the punch state key remains unchanged until it is switched manually next time. **Fixed Mode:** It only displays the fixed punch state key, and it cannot be switched.
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 Keys Mappings

Shortcut keys can be defined as punch state keys or menu function key. When the device is on the main interface, pressing the set shortcut key will display the attendance state or enter the menu operation interface.

Select the **Shortcut Key Mappings** option on the Personalize interface.



Shortcut Key Mappings

Up Key
Check-In

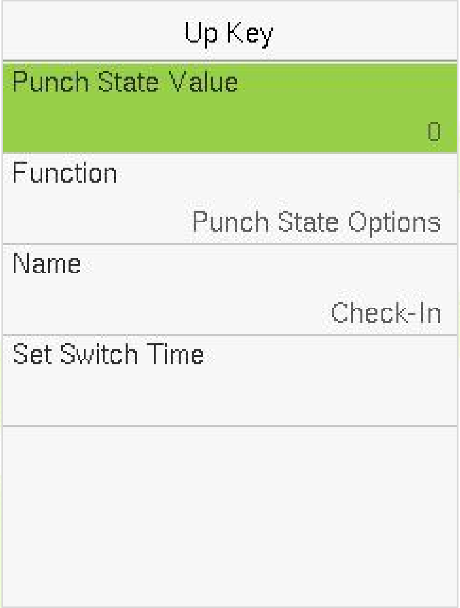
Down Key
Check-Out

Left Key
Overtime-In

Right Key
Overtime-Out

ESC/[-> Key
Undefined

M/OK/->] Key
Undefined



Up Key

Punch State Value
0

Function
Punch State Options

Name
Check-In

Set Switch Time

To set Auto-Switching Time:

Choose any shortcut key and select **Punch State Options** in **Function** to set the auto-switching time.

Auto Switch: A different time interval is set for different Punch State options. When a set time reaches, the device switches its attendance state automatically.

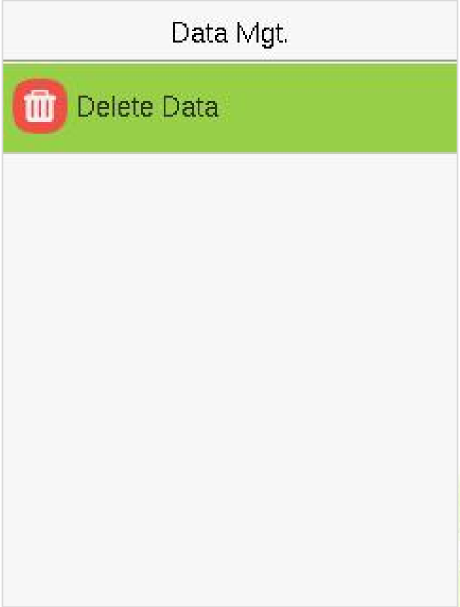
Note:

When the shortcut key is set to **Punch State Key**, but **OFF** mode is selected in the **Punch State Mode** (**Personalize** > **Punch State Options** > **Punch State Mode** > Select **OFF**), then the shortcut key will not be enabled.

8 Data Management

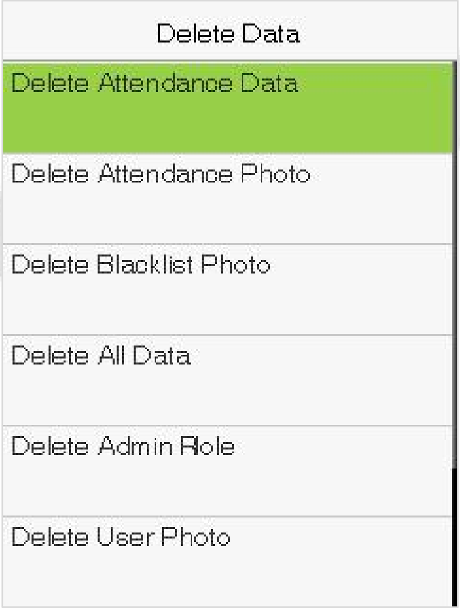
It helps to delete the relevant data in the device.

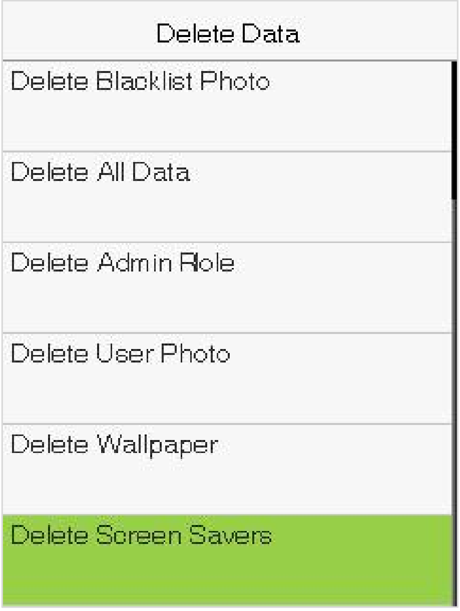
Select **Data Mgt.** option on the main menu interface.



8.1 Delete Data

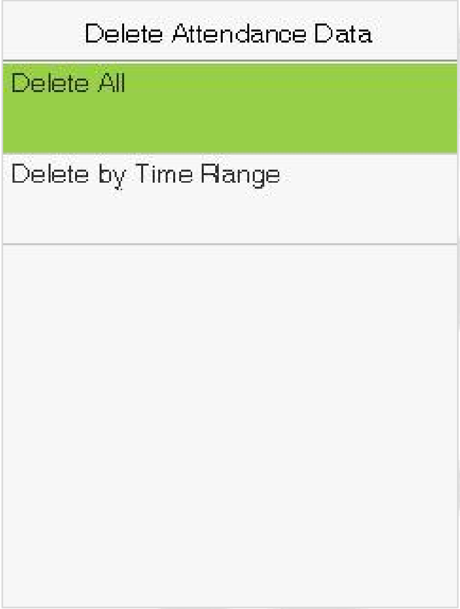
Select **Delete Data** option on the **Data Mgt.** interface.



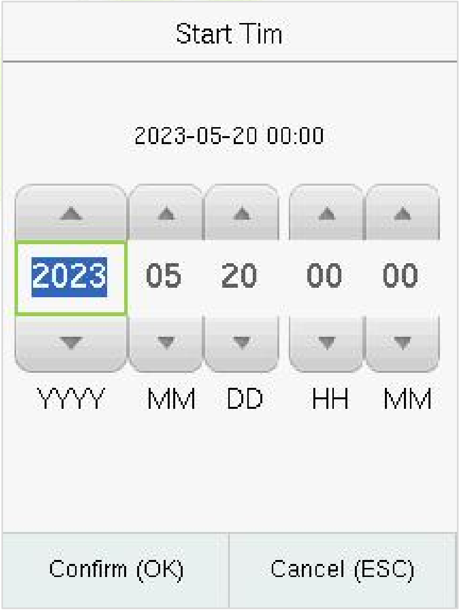


Item	Description
Delete Attendance Data	To delete all attendance data in the device.
Delete Attendance Photo	To delete attendance photos of designated personnel.
Delete Blocklist Photo	To delete the photos taken during failed verifications.
Delete All Data	To delete information and access records of all registered users.
Delete Admin Role	To remove administrator privileges.
Delete Profile Photo	To delete all user photos on the device.
Delete Wallpaper	To delete all wallpapers in the device.
Delete Screen Savers	To delete the screen savers in the device.

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



Select Delete by Time Range

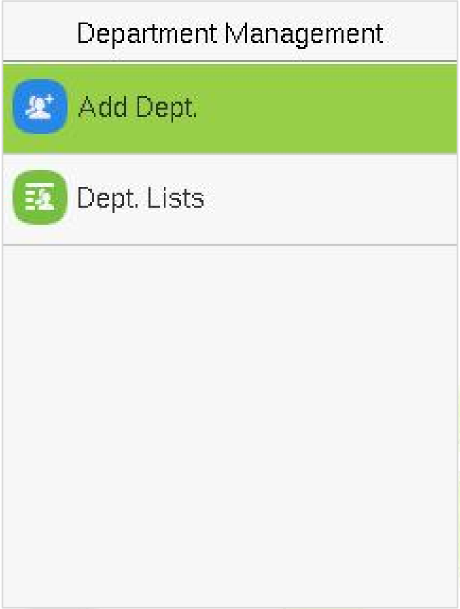


Set the time range and select **Confirm(OK).**

9 Department Management ★

Establishing an organizational structure of the company and arranging departments shift is necessary to view the department information of the device. In this menu option, you can add, edit, or remove a department.

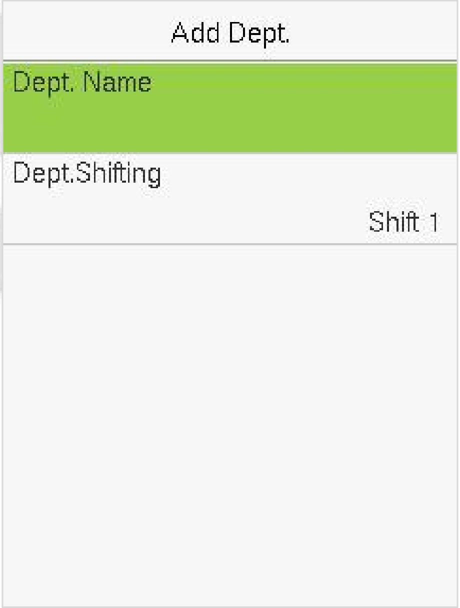
Select **Department** on the main menu interface.



Department Management

9.1 Add Dept.

1. Select **Add Dept.** and press [**M/OK**] to enter.

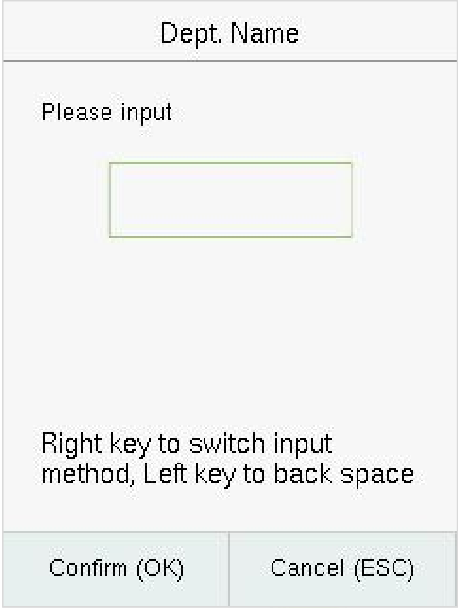


Add Dept.

Dept. Name

Dept.Shifting: Shift 1

2. Select **Dept. Name** and enter the department name using the T9 input method.

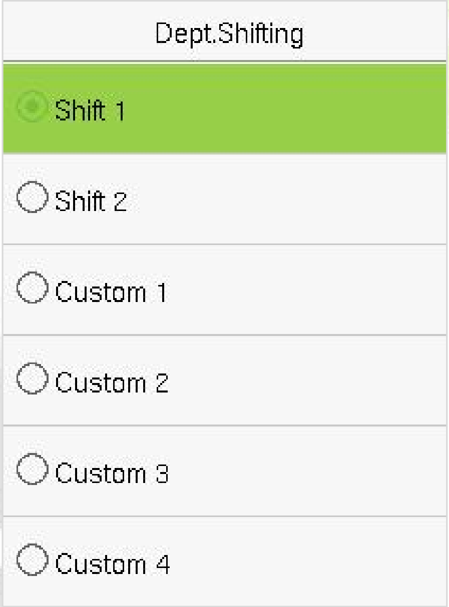


Dept. Name

Please input

Right key to switch input method, Left key to back space

3. Select the **Dept. Shifting** of the department.



Dept.Shifting

● Shift 1

○ Shift 2

○ Custom 1

○ Custom 2

○ Custom 3

○ Custom 4

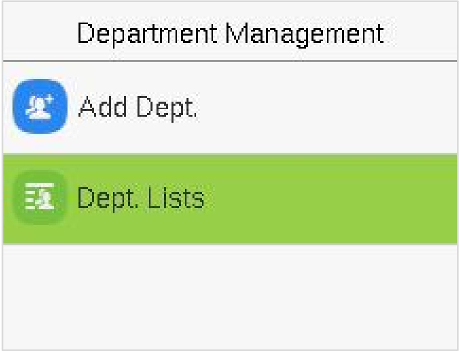
Note:

1. The equipment will automatically assign numbers to departments, starting from 1 and so on.

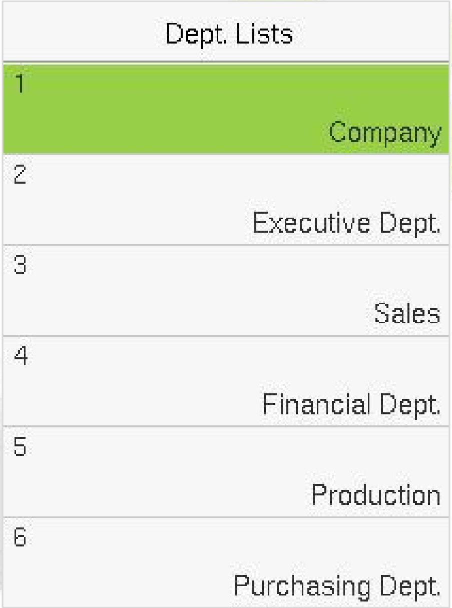
2. **Dept. Shift:** Select the shift attendance used by all users of the department. Shifts can be set in **Shift set** > **Shifts setting**, with a maximum of 24 shifts set by default. Refer to Shift Set section.

9.2 Dept. Lists

There are 8 departments in the device by default. You can edit the department name and department shift, but you cannot delete them. In addition to the 8 default departments, additional departments can be edited and deleted.



1. Select **Dept. Lists** and press [**M/OK**] to enter.



Dept. Lists

1 Company

2 Executive Dept.

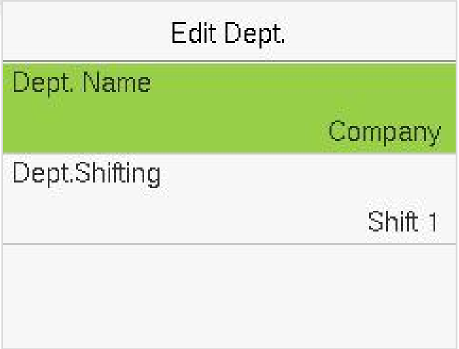
3 Sales

4 Financial Dept.

5 Production

6 Purchasing Dept.

2. Select a department to edit and press [**M/OK**] to enter.



Edit Dept.

Dept. Name: Company

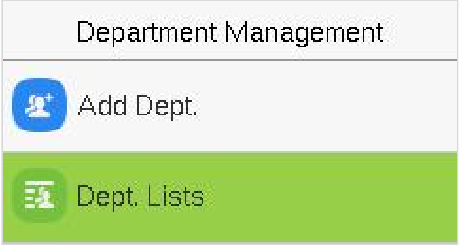
Dept.Shifting: Shift 1

3. Modify **Dept. Name** and **Dept. Shifting** and press [**M/OK**] to save.

   The editing of the department is the same as of **Add Dept**.

9.3 Delete a Department

It helps to remove one or more department as required.

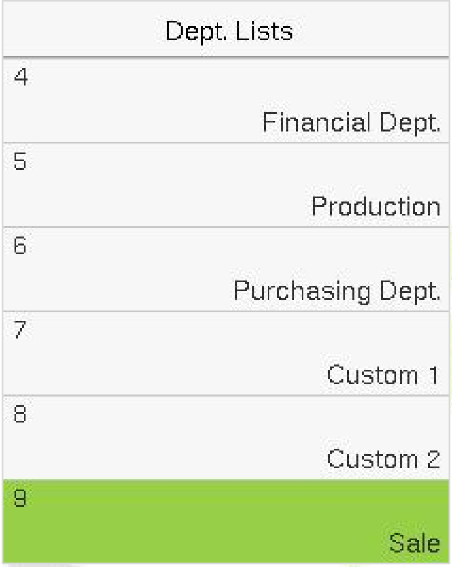


Department Management

Add Dept.

Dept. Lists

1. Select **Dept. Lists** and press [**M/OK**] to enter.



Dept. Lists

4 Financial Dept.

5 Production

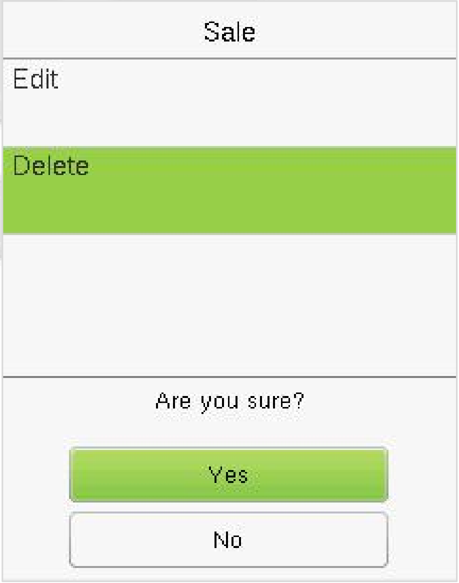
6 Purchasing Dept.

7 Custom 1

8 Custom 2

9 Sale

2. Select a department to delete and press **[M/OK]** to enter.



Sale

Edit

Delete

Are you sure?

Yes

No

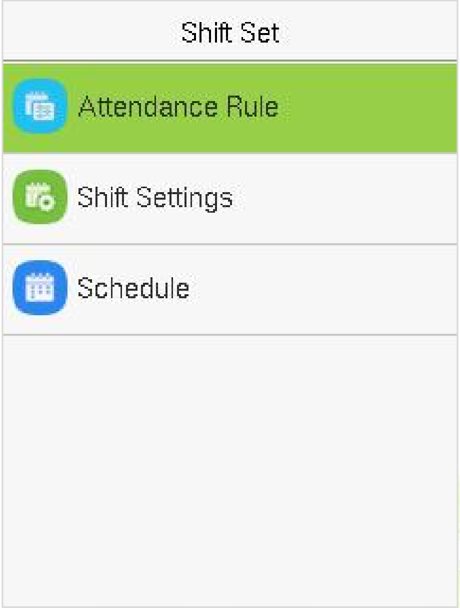
3. Select **Delete** and press **[M/OK]**.

Note: Only departments other than the 8 default departments in the device can be deleted.

10 Shift Set ★

Set attendance rules, number of shifts to be used, and schedule employees.

Select **Shift Set** option on the main menu interface.

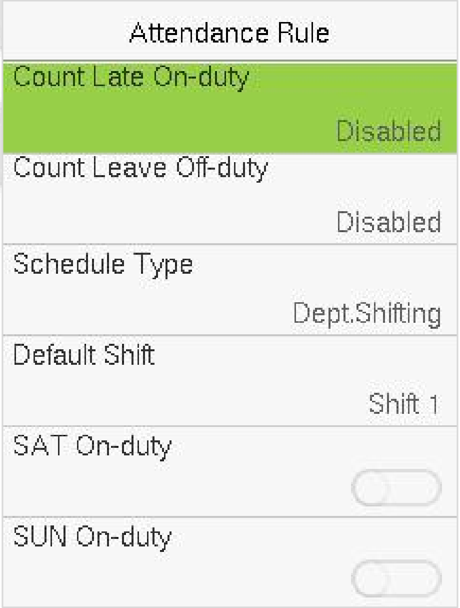


Shift Set

10.1 Attendance Rule

All attendance statistics are conducted according to the attendance rules. Therefore, the staff attendance rules need to be set first, including late, early leave calculation method, and scheduling type. Once the attendance rules are set, it is not recommended to modify them frequently as it may affect the result of attendance calculation and may cause chaos in the scheduling if it is modified in the middle of the month.

Select **Attendance Rule** on the **Shift Set** interface.



Attendance Rule

Count Late On-duty: Disabled

Count Leave Off-duty: Disabled

Schedule Type: Dept.Shifting

Default Shift: Shift 1

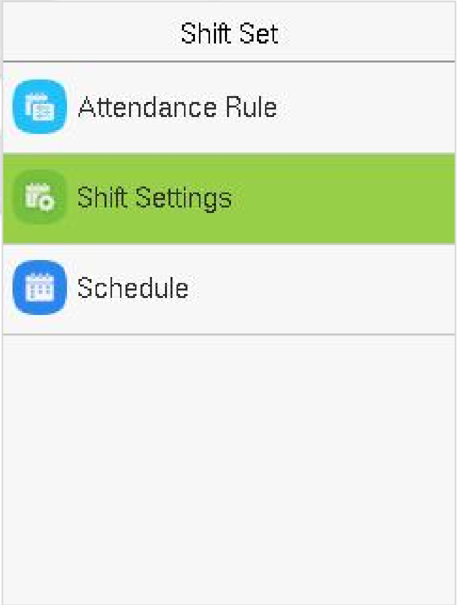
SAT On-duty: ○

SUN On-duty: ○

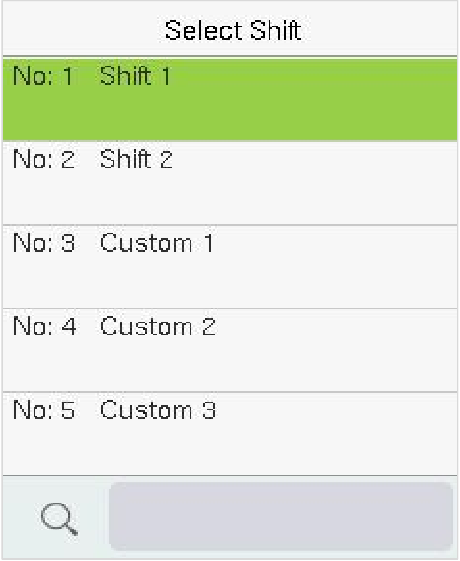
Item	Descriptions
Count Late On-duty	Set a time after which the lateness calculation for an employee should start. If it is disabled, the lateness calculation starts with the start of working hours.
Count Leave Off-duty	Set a time before which the early leave calculation for an employee should start. If disabled, it is calculated with respect to the end of the working hours.
Schedule Type	The device supports both department and individual-based scheduling. If a company uses one timetable, then only one department needs to be set and department-based scheduling is recommended. If the departments have their respective timetables, department-based scheduling is recommended. If employees may take different shifts, individual-based scheduling is recommended.
Default Shift	When individual-based scheduling is used, the default shift applies to all the non-scheduled employees.
SAT On-duty	Enable whether to work normally on Saturdays.
SUN On-duty	Enable whether to work normally on Sundays.

10.2 Shift Settings

Select **Shift Settings** on the Shift set interface.



Select a Shift on the list, and press **[M/OK]**.



Select Shift

No: 1 Shift 1

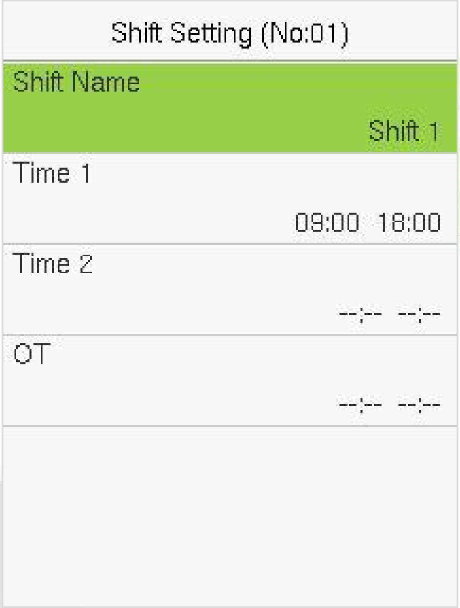
No: 2 Shift 2

No: 3 Custom 1

No: 4 Custom 2

No: 5 Custom 3

Use the T9 input method to enter "Shift Name" and set the required start and end times.



Shift Setting (No:01)

Shift Name: Shift 1

Time 1: 09:00 18:00

Time 2: --:-- --:--

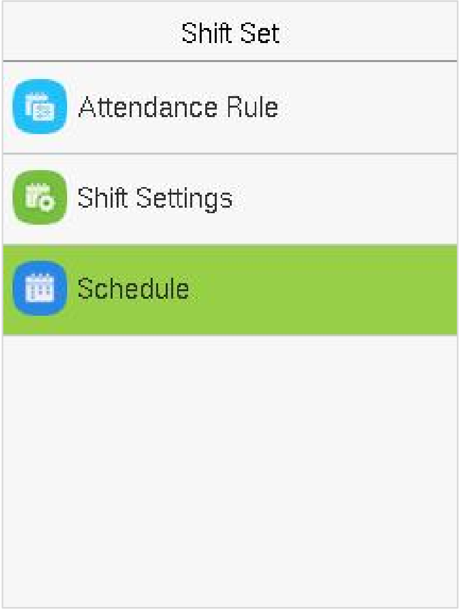
OT: --:-- --:--

Note: The device supports a maximum of 24 shifts including two default shifts (Shift 1 and Shift 2). All the shifts are editable, and a single shift includes three-time ranges at most.

10.3 Schedule

The shifts should be set based on the actual condition of a company. If no shift is set, the system makes attendance calculations based on default shifts set in attendance rules.

Select **Schedule** on the Shift Set interface.

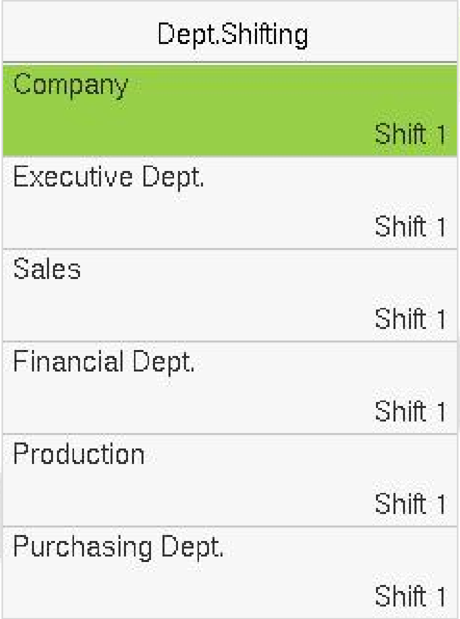


Shift Set

- Attendance Rule
- Shift Settings
- Schedule

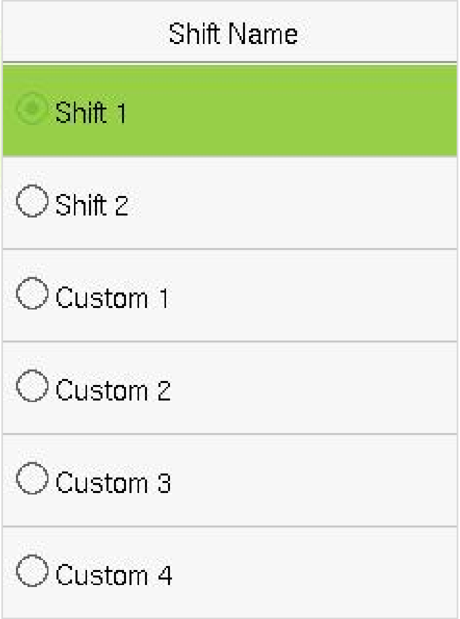
- <u>**Department-based Scheduling:**</u>

Select **Shift Set** > **Attendance Rule** > **Schedule Type** > **Dept. Shifting** to schedule shift for a department.



Dept.Shifting

Company	Shift 1
Executive Dept.	Shift 1
Sales	Shift 1
Financial Dept.	Shift 1
Production	Shift 1
Purchasing Dept.	Shift 1



Shift Name

● Shift 1
○ Shift 2
○ Custom 1
○ Custom 2
○ Custom 3
○ Custom 4

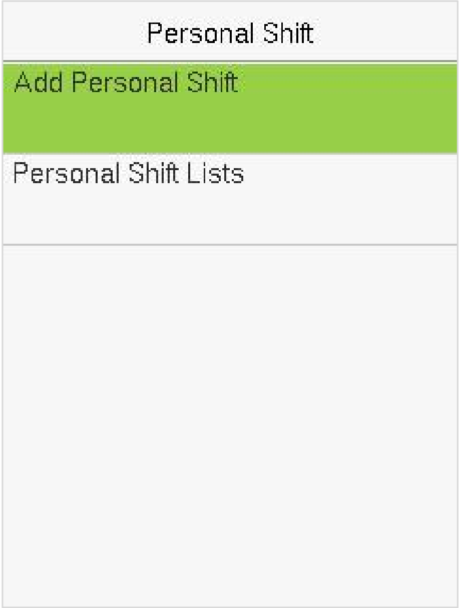
When a shift is selected for a department, it is implemented for all the members of the department.

- <u>**Individual-based Scheduling:**</u>

Select **Shift Set** > **Attendance Rule** > **Schedule Type** > **Personal Shift** to schedule shift for an individual.

1. Add Schedule

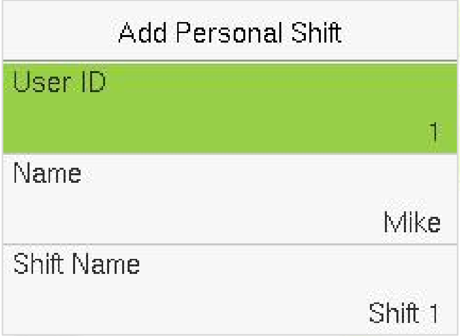
1) Press **[M/OK]** to enter Schedule interface and select **Add Personal Shift**.


Personal Shift

Add Personal Shift

Personal Shift Lists

2) Enter an ID. The device automatically displays the name. Select Shift Name and then press [**M/OK**].


Add Personal Shift

User ID: 1

Name: Mike

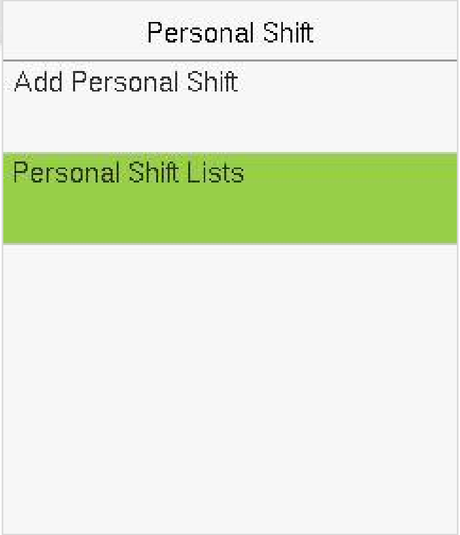
Shift Name: Shift 1

3) Press [**ESC**] to exit and save.

2. Edit Schedule:

Enter the **Personal Shift Lists** for editing when the scheduling of individual employee needs to be adjusted.

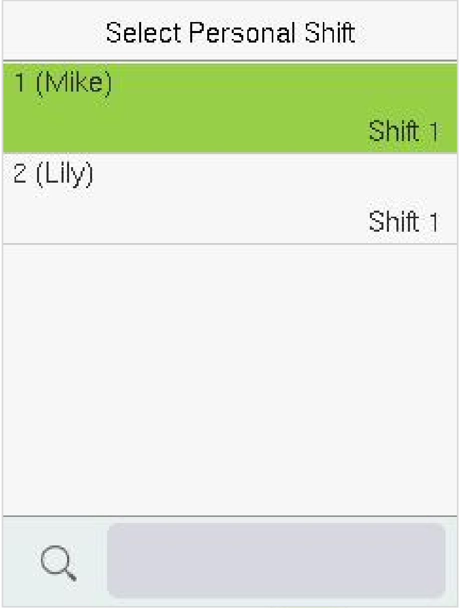
1) Select **Personal Shift Lists** on the Personal Shift interface.


Personal Shift

Add Personal Shift

Personal Shift Lists

2) Select a scheduled user and press **[M/OK**].

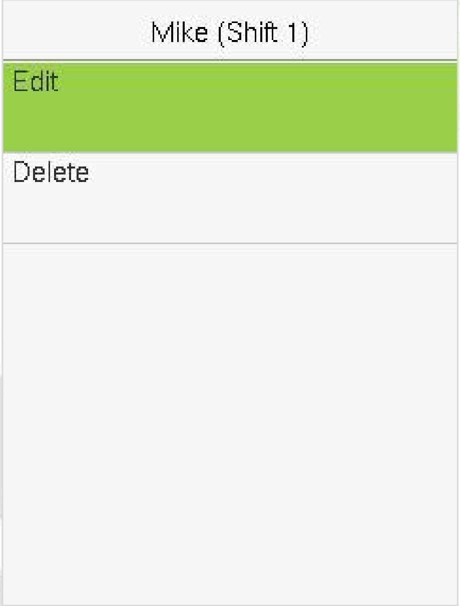


Select Personal Shift

1 (Mike) Shift 1

2 (Lily) Shift 1

3) Select **Edit**, press **[M/OK]** to enter and modify the "Shift Name" of the user.



Mike (Shift 1)

Edit

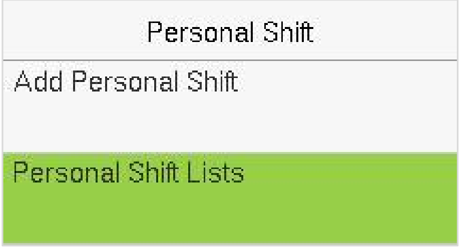
Delete

Note: The User ID cannot be modified. The other operations are the same as those performed to add a shift.

3. Delete a shift:

Go to the **Personal Shift Lists**, to delete an employee's schedule that is no longer required.

1) Select **Personal Shift Lists** on the Personal Shift interface.

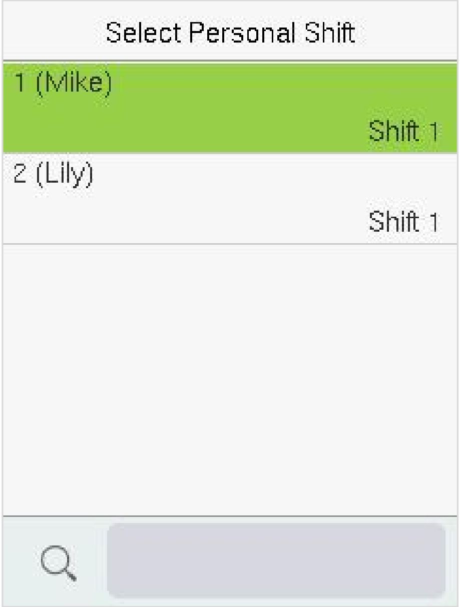


Personal Shift

Add Personal Shift

Personal Shift Lists

2) Select a scheduled user and press **[M/OK**].

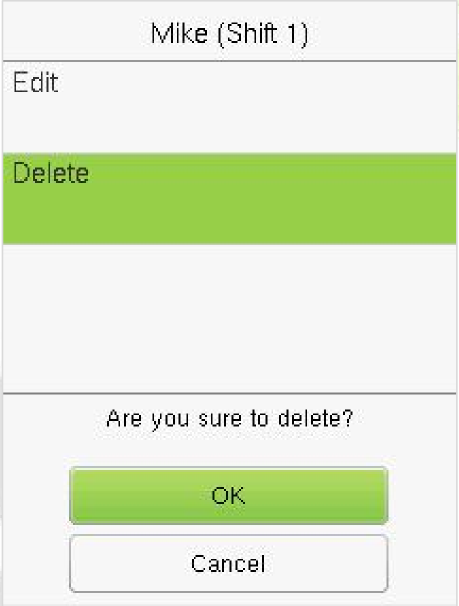


Select Personal Shift

1 (Mike) Shift 1

2 (Lily) Shift 1

3) Select **Delete**, press [**M/OK**], and choose “**OK**” to delete the Shift successfully.



Mike (Shift 1)

Edit

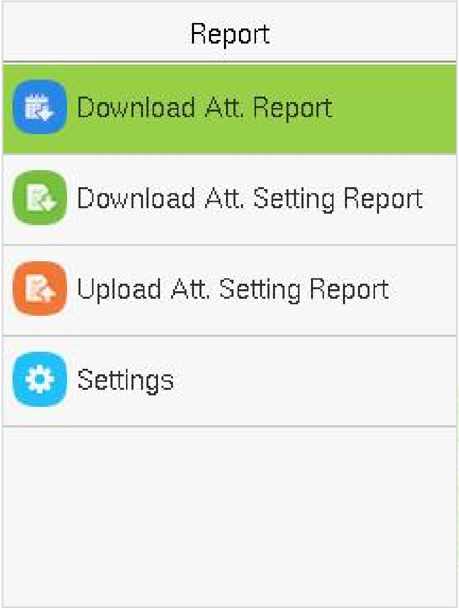
Delete

Are you sure to delete?

11 Report ★

This menu item allows you to download statistical reports of attendance or attendance setting reports to a USB flash drive or SD card. You can also upload attendance setting reports with defined shifts and employees' schedules. The device gives priority to the schedules in an attendance setting report.

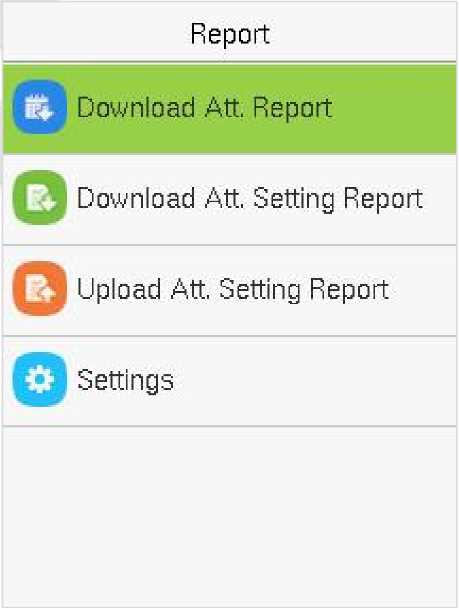
Select **Report** on the main menu interface.



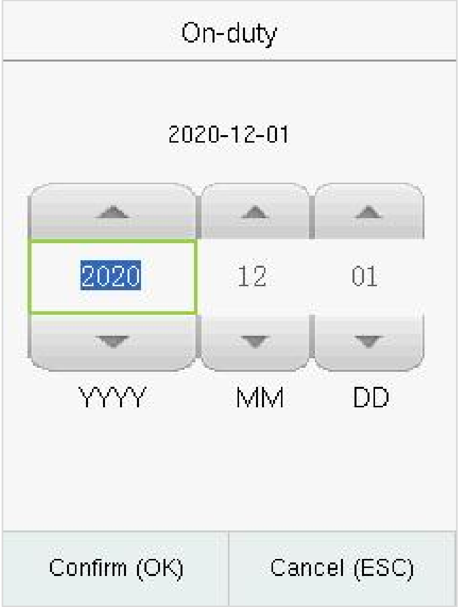
Note: First insert the USB flash drive into the USB slot of the machine, and then enter the main menu to perform the related operations of the **Report**.

11.1 Download Att. Report

Select **Download Att. Report** and press **[M/OK]**.



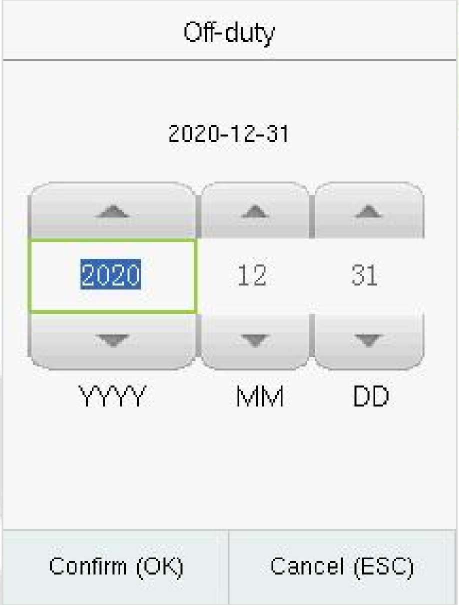
Set the on-duty time and press **[M/OK]**.



On-duty

2020-12-01

Set the off-duty time and press **[Confirm(OK)]**.



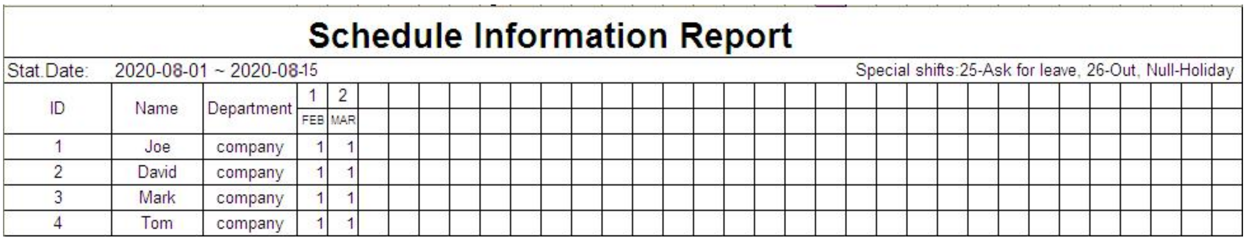
Off-duty

2020-12-31

When Data download succeeds, Press **[Confirm(OK)]** to take out the USB disk or SD card. The SSRTemplateS.xls gets stored in the USB disk or SD card. The Schedule Information, Statistical Report of Attendance, Attendance Record Report, Exception Statistic Report, and Card Report can be viewed on a PC. The following reports show the preceding information:

To make reports more understandable, a report containing two-day attendance records of four employees is provided as an example.

- **Schedule Information Report:** The report allows you to view schedule records of all employees.

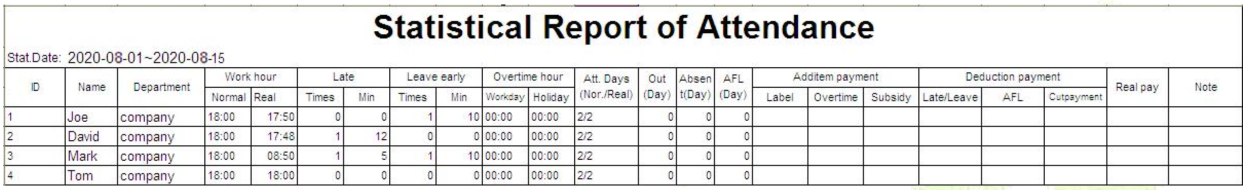


Schedule Information Report

Stat.Date: 2020-08-01 ~ 2020-08-15 Special shifts:25-Ask for leave, 26-Out, Null-Holiday

ID	Name	Department	1	2
			FEB	MAR
1	Joe	company	1	1
2	David	company	1	1
3	Mark	company	1	1
4	Tom	company	1	1

- **Statistical Report of Attendance:** The report allows you to query the attendance of each person in a specified period. Salaries can be calculated directly based on this report.



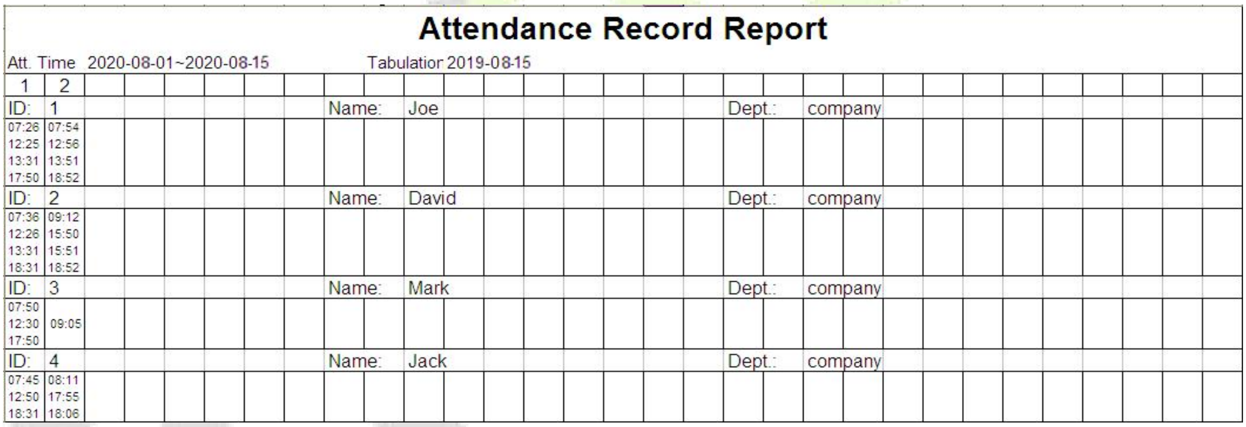
Statistical Report of Attendance

Stat.Date: 2020-08-01~2020-08-15

ID	Name	Department	Work hour		Late		Leave early		Overtime hour		Att. Days	Out	Absen	AFL	Additem payment			Deduction payment			Real pay	Note
			Normal	Real	Times	Min	Times	Min	Workday	Holiday	(Nor./Real)	(Day)	t(Day)	(Day)	Label	Overtime	Subsidy	Late/Leave	AFL	Cutpayment		
1	Joe	company	18:00	17:50	0	0	1	10	00:00	00:00	2/2	0	0	0								
2	David	company	18:00	17:48	1	12	0	0	00:00	00:00	2/2	0	0	0								
3	Mark	company	18:00	08:50	1	5	1	10	00:00	00:00	2/2	0	0	0								
4	Tom	company	18:00	18:00	0	0	0	0	00:00	00:00	2/2	0	0	0								

Note: The unit of Work hour and Overtime hour in the Statistical Report of Attendance is HH: MM. For example, 17:50 indicates that the on-duty time is 17 hours and 50 minutes.

- **Attendance Record Report:** The report lists the daily attendance records of all employees within a specified period.

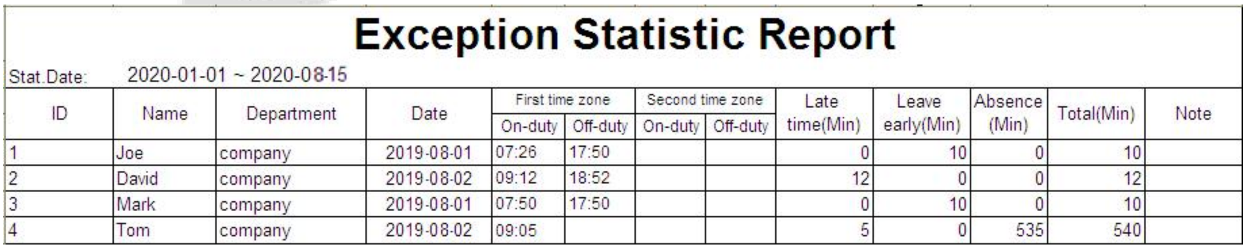


Attendance Record Report

Att. Time 2020-08-01~2020-08-15 Tabulatior 2019-08-15

1	2				
ID:	1	Name:	Joe	Dept.:	company
07:26 12:25 13:31 17:50	07:54 12:56 13:51 18:52				
ID:	2	Name:	David	Dept.:	company
07:36 12:26 13:31 18:31	09:12 15:50 15:51 18:52				
ID:	3	Name:	Mark	Dept.:	company
07:50 12:30 17:50	09:05				
ID:	4	Name:	Jack	Dept.:	company
07:45 12:50 18:31	08:11 17:55 18:06				

- **Exception Statistic Report:** The report displays the attendance exceptions of all employees within a specified period so that the attendance department handles the exceptions and confirm them with the employees involved and their supervisors.

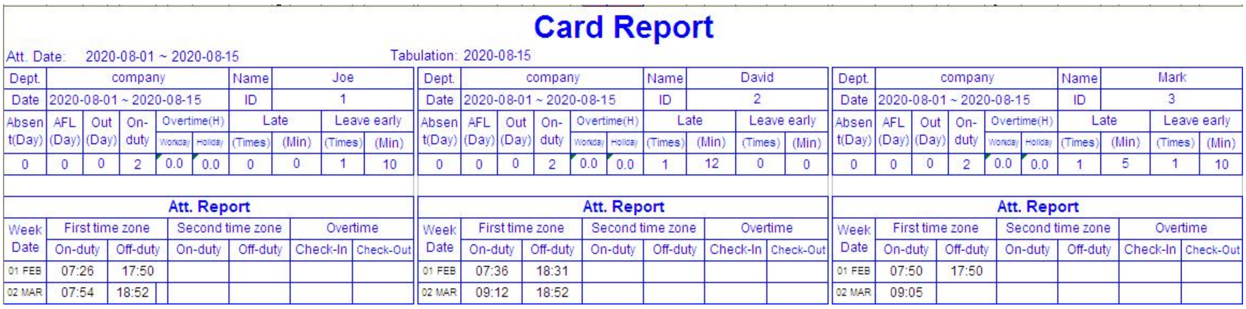


Exception Statistic Report

Stat.Date: 2020-01-01 ~ 2020-08-15

ID	Name	Department	Date	First time zone		Second time zone		Late time(Min)	Leave early(Min)	Absence (Min)	Total(Min)	Note
				On-duty	Off-duty	On-duty	Off-duty					
1	Joe	company	2019-08-01	07:26	17:50			0	10	0	10	
2	David	company	2019-08-02	09:12	18:52			12	0	0	12	
3	Mark	company	2019-08-01	07:50	17:50			0	10	0	10	
4	Tom	company	2019-08-02	09:05				5	0	535	540	

- **Card Report:** The report can substitute for clock-based cards and can be sent to each employee for confirmation.



Card Report

Att. Date: 2020-08-01 ~ 2020-08-15 Tabulation: 2020-08-15

Dept.	company					Name	Joe		
Date	2020-08-01 ~ 2020-08-15					ID	1		
Absent(Day)	AFL (Day)	Out (Day)	On-duty	Overtime(H)		Late		Leave early	
				Workday	Holiday	(Times)	(Min)	(Times)	(Min)
0	0	0	2	0.0	0.0	0	0	1	10

Att. Report

Week Date	First time zone		Second time zone		Overtime	
	On-duty	Off-duty	On-duty	Off-duty	Check-In	Check-Out
01 FEB	07:26	17:50				
02 MAR	07:54	18:52				

Dept.	company					Name	David		
Date	2020-08-01 ~ 2020-08-15					ID	2		
Absent(Day)	AFL (Day)	Out (Day)	On-duty	Overtime(H)		Late		Leave early	
				Workday	Holiday	(Times)	(Min)	(Times)	(Min)
0	0	0	2	0.0	0.0	1	12	0	0

Att. Report

Week Date	First time zone		Second time zone		Overtime	
	On-duty	Off-duty	On-duty	Off-duty	Check-In	Check-Out
01 FEB	07:36	18:31				
02 MAR	09:12	18:52				

Dept.	company					Name	Mark		
Date	2020-08-01 ~ 2020-08-15					ID	3		
Absent(Day)	AFL (Day)	Out (Day)	On-duty	Overtime(H)		Late		Leave early	
				Workday	Holiday	(Times)	(Min)	(Times)	(Min)
0	0	0	2	0.0	0.0	1	5	1	10

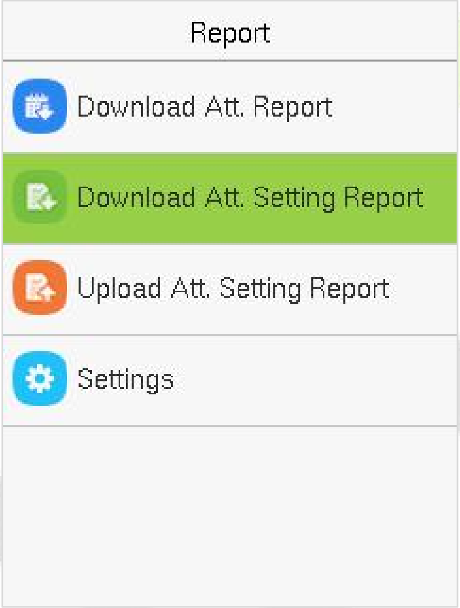
Att. Report

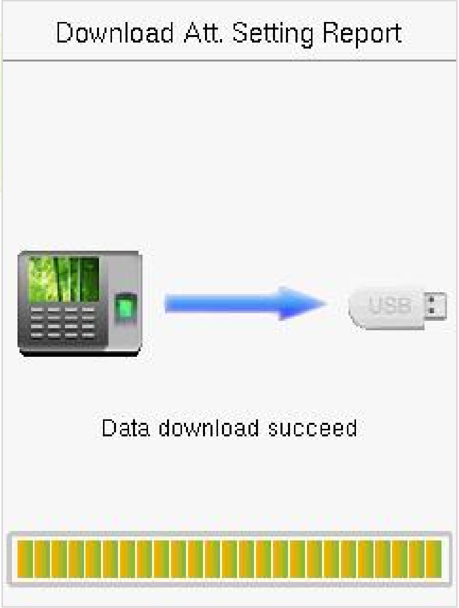
Week Date	First time zone		Second time zone		Overtime	
	On-duty	Off-duty	On-duty	Off-duty	Check-In	Check-Out
01 FEB	07:50	17:50				
02 MAR	09:05					

11.2 Download Att. Setting Report

If shifts are complex or the shifts of a person are not fixed, it is recommended that the attendance setting report be downloaded and shifts and schedules be set for employees in the attendance setting report.

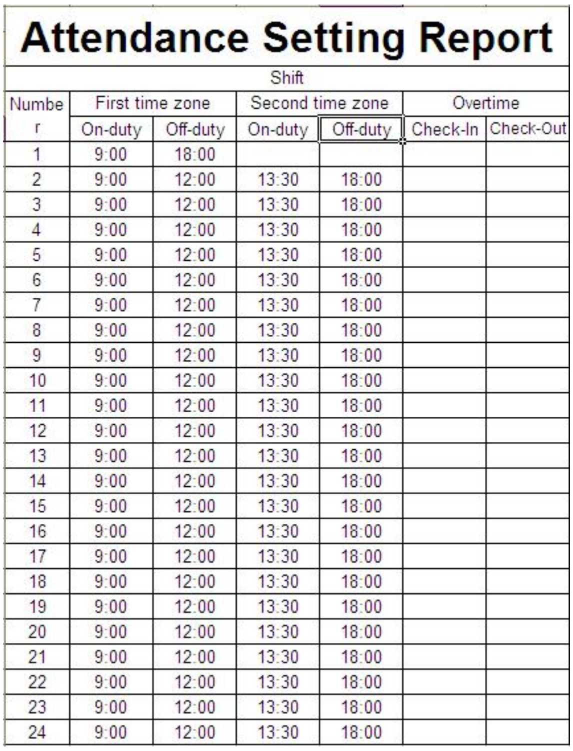
Select **Download Att. Setting Report** and press **[M/OK]**.





Data download succeed

Open the setting "AttSettingE.xls" in the USB disk or SD card on a PC. Set the Shift in the Attendance setting report. The shifts that have been set on the attendance machine shall be displayed. (For more details, see Shift Setting. You can modify the 24 shifts and add more shifts. After modification, the shifts shall prevail on the attendance machine.



Attendance Setting Report

Shift

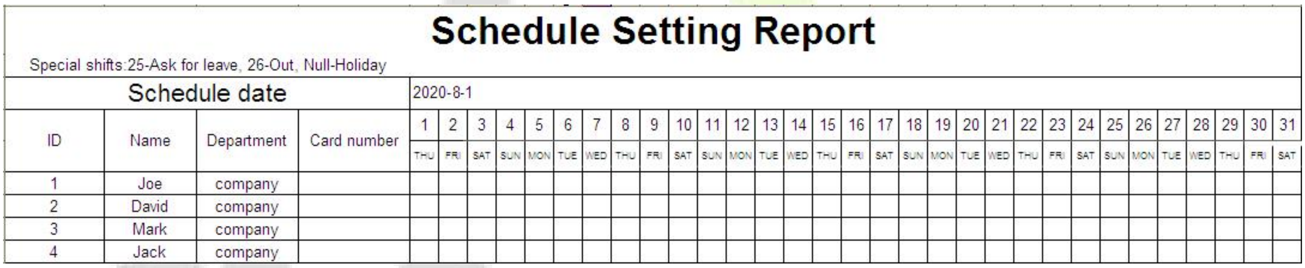
Number	First time zone		Second time zone		Overtime	
	On-duty	Off-duty	On-duty	Off-duty	Check-In	Check-Out
1	9:00	18:00				
2	9:00	12:00	13:30	18:00		
3	9:00	12:00	13:30	18:00		
4	9:00	12:00	13:30	18:00		
5	9:00	12:00	13:30	18:00		
6	9:00	12:00	13:30	18:00		
7	9:00	12:00	13:30	18:00		
8	9:00	12:00	13:30	18:00		
9	9:00	12:00	13:30	18:00		
10	9:00	12:00	13:30	18:00		
11	9:00	12:00	13:30	18:00		
12	9:00	12:00	13:30	18:00		
13	9:00	12:00	13:30	18:00		
14	9:00	12:00	13:30	18:00		
15	9:00	12:00	13:30	18:00		
16	9:00	12:00	13:30	18:00		
17	9:00	12:00	13:30	18:00		
18	9:00	12:00	13:30	18:00		
19	9:00	12:00	13:30	18:00		
20	9:00	12:00	13:30	18:00		
21	9:00	12:00	13:30	18:00		
22	9:00	12:00	13:30	18:00		
23	9:00	12:00	13:30	18:00		
24	9:00	12:00	13:30	18:00		

Enter the On-duty and Off-duty time in the corresponding columns, where the First time zone shall be the On-duty or Off-duty time of Time 1 of Shift Setting, and the Second time zone shall be the On-duty or Off-duty time of Time 2.

For the correct schedule time format, see "What is the correct time format used in the setting reports" in the "Self-Service Attendance Terminal FAQs."

Set a schedule setting report

Enter the **ID**, **Name**, and **Department** respectively on the left of the **Schedule Setting Report**. Set shifts for employees on the right of the **Schedule Setting Report**, where shifts 1–24 are shifts to set the **Attendance Setting Report.** Shift 25 is for leave and Shift 26 is for out.



Schedule Setting Report

Special shifts:25-Ask for leave, 26-Out, Null-Holiday

Schedule date				2020-8-1																														
ID	Name	Department	Card number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
				THU	FRI	SAT	SUN	MON	TUE	WED	THU	FRI	SAT	SUN	MON	TUE	WED	THU	FRI	SAT	SUN	MON	TUE	WED	THU	FRI	SAT	SUN	MON	TUE	WED	THU	FRI	SAT
1	Joe	company																																
2	David	company																																
3	Mark	company																																
4	Jack	company																																

Notes:

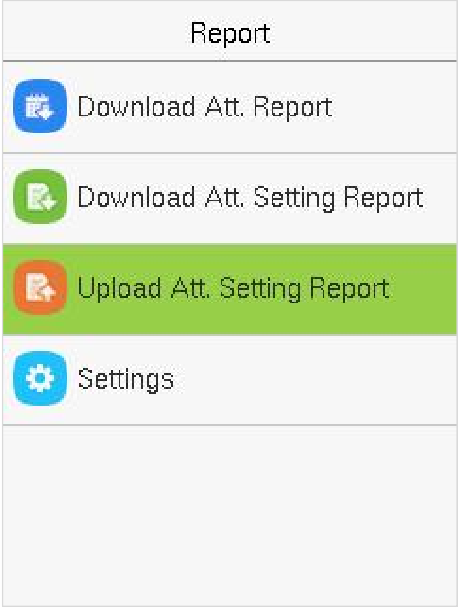
1. The shifts of only 31 days can be arranged in one schedule setting report. For example, if the scheduling date is 2020-1-1, the schedule setting report contains the schedules of 31 days after 2020-1-1, that is, scheduled from 2020-1-1 to 2020-1-31. If the scheduling date is 2020-1-6, the schedule setting report contains the schedules of 31 days after 2020-1-6, that is, scheduled from 2020-1-6 to 2020-2-5.

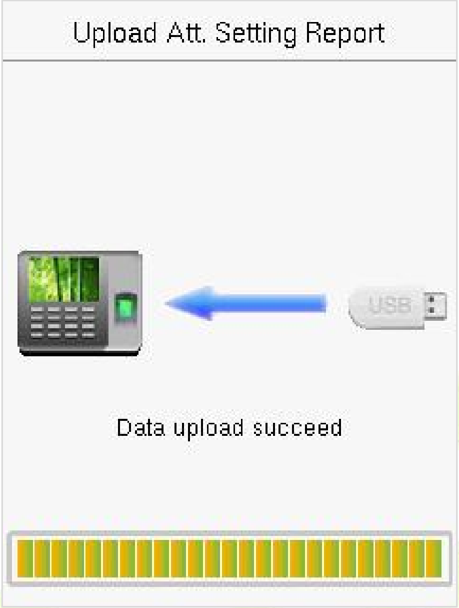
2. If no schedule setting report is set, all employees use Report 1 by default from Monday to Friday.

11.3 Upload Att. Setting Report

After setting the attendance setting table, save the “Setting Report.xls” to the USB flash drive and reinsert the USB flash drive into the USB slot of the device.

Select **Upload Att. Setting Report** on the Report interface and press **[M/OK]**.





Upload Att. Setting Report

Data upload succeed

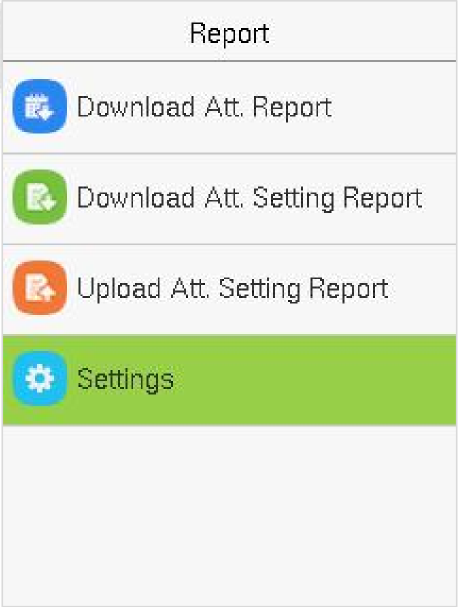
After uploading, remove the USB disk or SD card. At this time, the employee information, shift, and department in the setting report can be viewed respectively by the Management User, Shift Number, and Department available in the device. Or the above information and scheduling information can be seen in the standard download report.

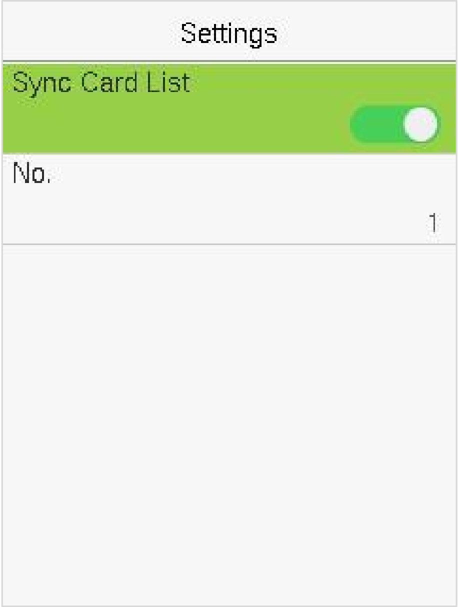
Note: If the schedule time format is incorrect, Re-upload the attendance setting report after modification.

11.4 Settings

Set whether to synchronize the card report and distinguish the device ID when downloading the attendance report.

Select **Settings** on the Report interface and press **[M/OK]**.





Settings

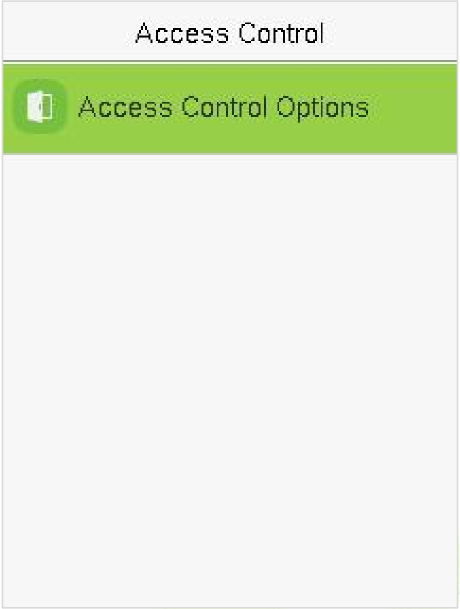
Sync Card List

No.

1

12 Access Control

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

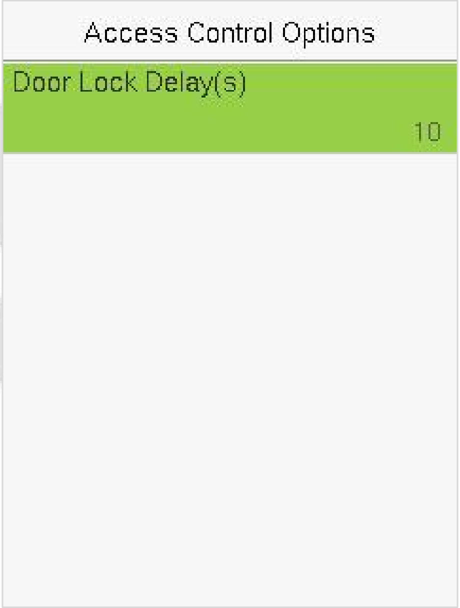

Access Control

Access Control Options

12.1 Access Control Options

To set the parameters of the control lock of the terminal and related equipment.

Select **Access Control Options** on the Access Control interface.


Access Control Options

Door Lock Delay(s)

10

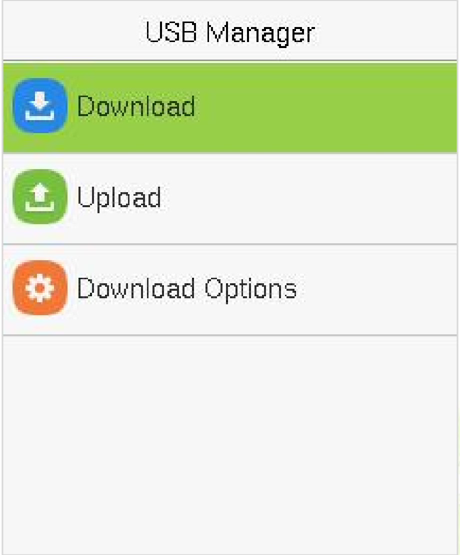
Item	Description
Door Lock Delay (s)	The length of time that the device controls the electric lock to be unlocked. Valid value: 1~10 seconds (0 second represents disabling the function).

13 USB Manager

Use a USB disk upload or download data between the device and the corresponding software using.

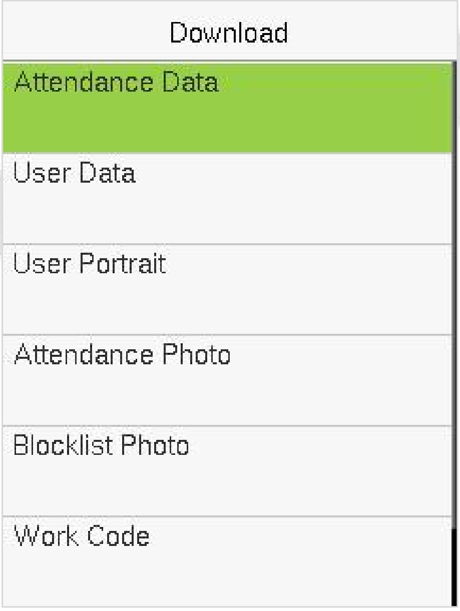
Before uploading/downloading data from/to the USB disk, insert the USB disk into the USB slot first.

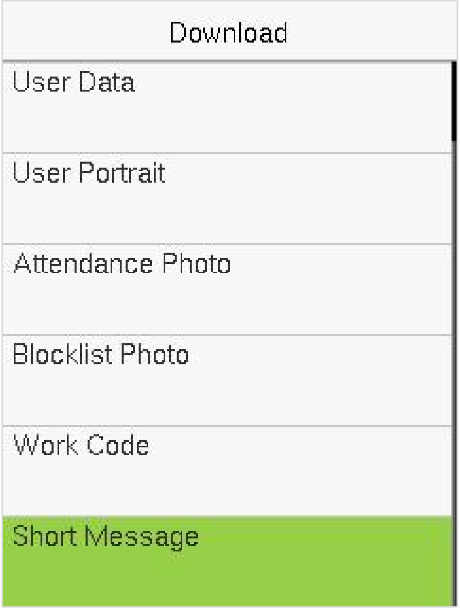
Select **USB Manager** on the main menu interface.



13.1 Download

Select **Download** on the USB Manager interface.



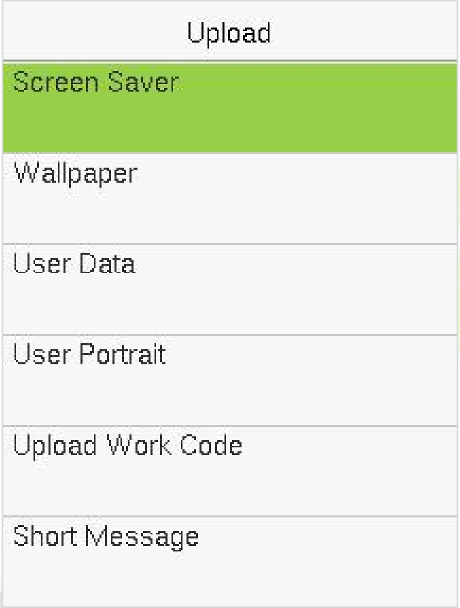


Item	Description
Attendance Data	Import all the attendance data from the device to a USB disk.
User Data	Import all the user information, fingerprints, and facial images from the device to a USB disk.

User Portrait	Import the employees' photos from the terminal to a USB disk.
Attendance Photo	Download attendance photos saved in device to U disk. The format of photo is JPG.
Blocklist Photo	Download block list photos saved in device to U disk. The format is JPG.
Work Code	To save work IDs on the device to a USB drive.
Short Message	Download short message on the device to the USB drive.

13.2 Upload

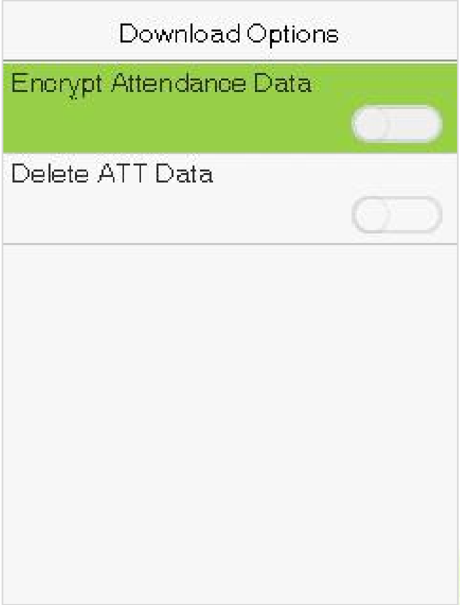
Select **Upload** on the USB Manager interface.



Item	Description
Screen Saver	To upload all screen savers from USB disk into the device. You can choose **[Upload selected picture]** or **[Upload all pictures]**. The images display as screensaver on the device's main interface after upload.
Wallpaper	To upload all wallpapers from USB disk into the device. You can choose **[Upload selected picture]** or **[Upload all pictures]**. The images display as wallpaper after upload.
User Data	Upload the message stored in a USB disk to the terminal.
User Portrait	Upload the JPG documents that are named after the user IDs and stored in a USB disk to the terminal, so that user photos can be displayed after the employees pass the verification.
Upload Work Code	Upload work IDs in a USB drive to the device.
Short Message	Upload short message in a USB drive to the device.

13.3 Download Options

Select **Download Options** on the USB Manager interface.



Download Options

Encrypt Attendance Data

Delete ATT Data

Click **[M/OK]** to enable or disable the **[Encrypt Attendance Data]** and **[Delete ATT Data]** options.

With Encrypt Attendance data-enabled, the data downloads with encryption for better security.

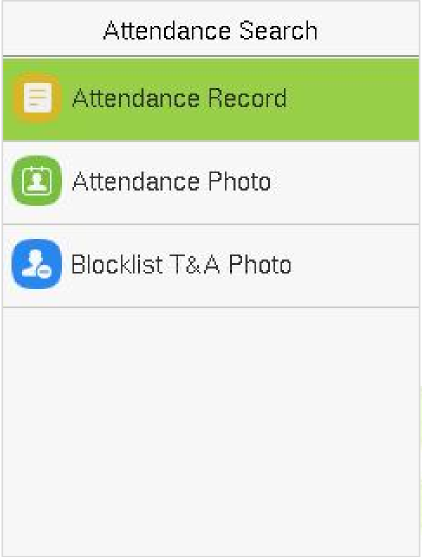
Delete ATT Data deletes all the attendance data.

14 Attendance Search

When the identity of a user is verified, the record is saved on the device. This function enables users to check their access records.

- **Attendance Record:**

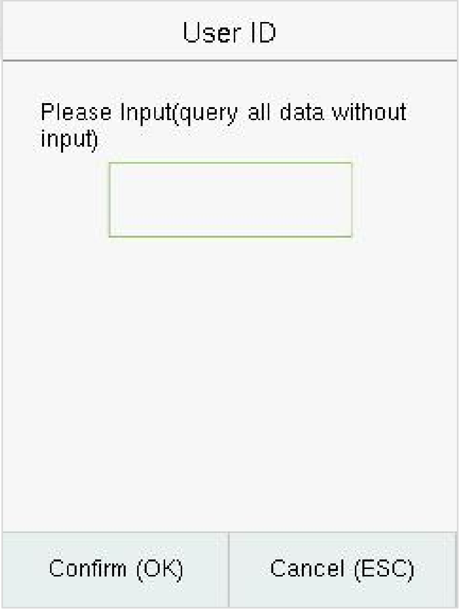
Select **Attendance Search** on the main menu interface.



The process of searching for attendance and blocklist photos is similar to that of searching for access records. The following is an example of searching for access records.

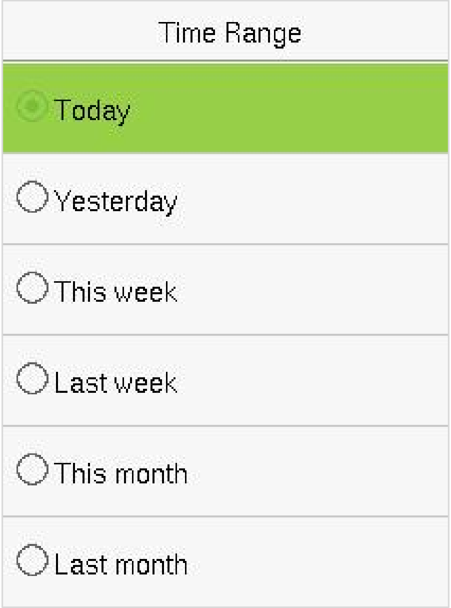
On the Attendance Search interface, Select **Attendance Record**.

1) Enter the user ID to be searched and select **Confirm (OK)**. If you want to search for records of all users, select **Confirm (OK)** without entering any user ID.

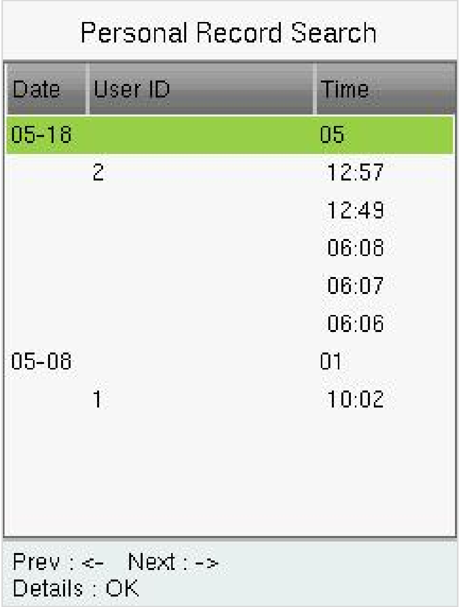


Please Input(query all data without input)

2) Select the time range for the records you want to search.



3) The record search succeeds. Select the record in green to view its details.

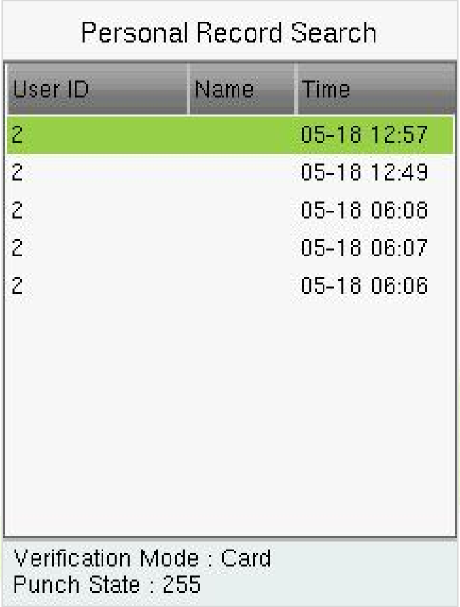


Personal Record Search

Date	User ID	Time
05-18		05
	2	12:57
		12:49
		06:08
		06:07
		06:06
05-08		01
	1	10:02

Prev : <- Next : ->
Details : OK

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



Personal Record Search

User ID	Name	Time
2		05-18 12:57
2		05-18 12:49
2		05-18 06:08
2		05-18 06:07
2		05-18 06:06

Verification Mode : Card
Punch State : 255

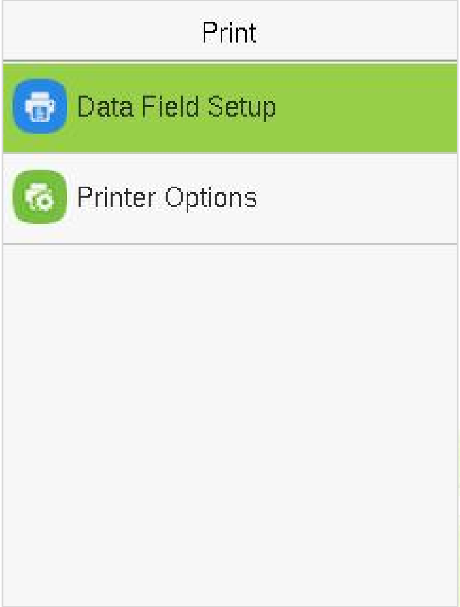
- **Attendance Photo and Blocklist T&A Photo**

The operations are similar to those performed to Attendance Record.

15 Print Settings ★

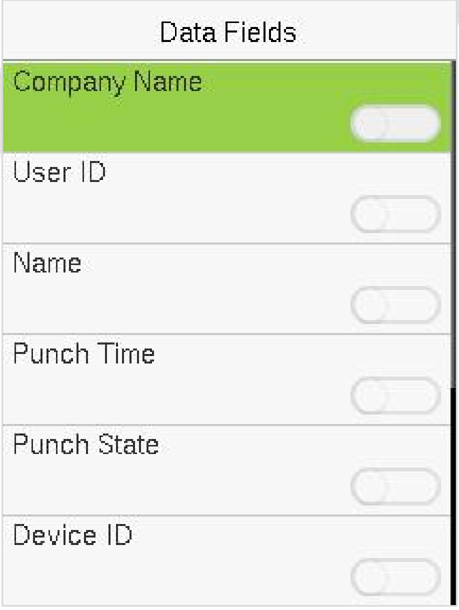
Devices with printing function can print attendance records out when a printer is connected (this function is optional and only be equipped in some products).

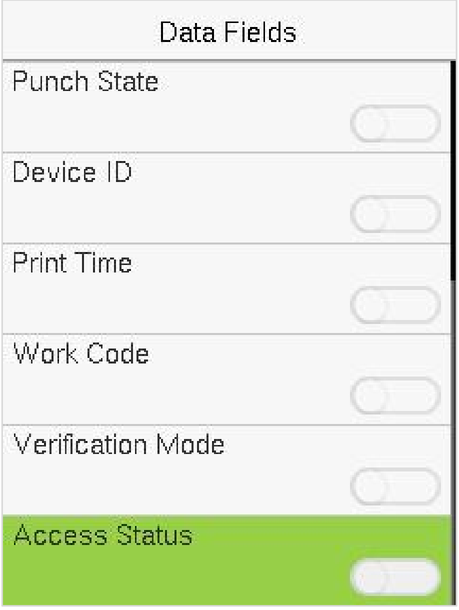
Select **Print** on the main menu interface.



15.1 Print Data Field Settings

Select **Data Field Setup** on the Print interface. Press **[M/OK]** to turn on / off the fields needing to be printed.

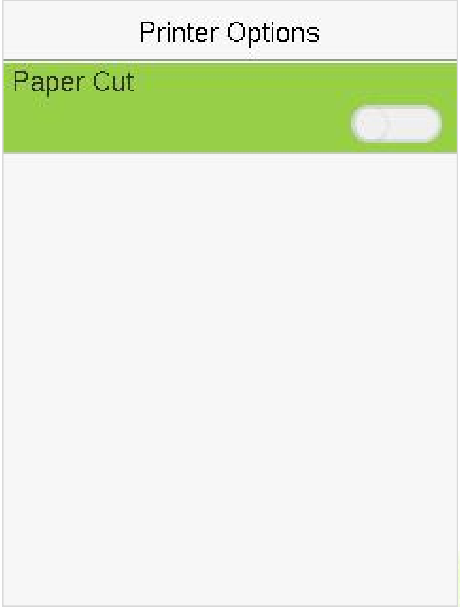




Remarks: In printing, the fields position of the information can be adjusted by the ◀ / ▶ key: press ◀ key to move to the previous item, and press ▶ key to move to the next item.

15.2 Printer Options

Select **Printer Options** on the Print interface. Press **[M/OK]** to turn on / off the **Paper Cut** function.

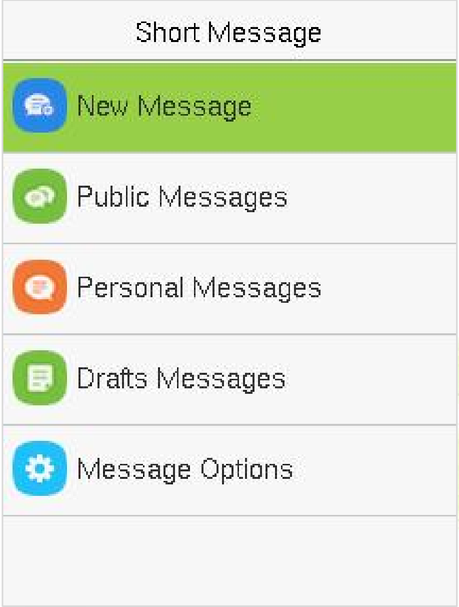


Remarks: To turn on the **Paper Cut** function, it is required to connect the device with a printer with paper cutting function, so that the printer will cut papers according to the selected printing information when printing.

16 Short Message

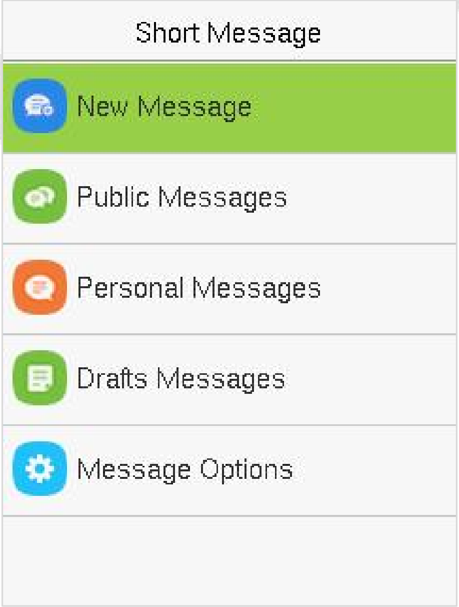
SMS is similar to notice. The operator can edit the notice content in advance and make it into SMS displayed on the screen. SMS includes Public SMS and Personal SMS. If public SMS is set, SMS content will be displayed in information column at the bottom of standby interface in the specified time. If personal SMS is set, the employee who can receive SMS can see SMS after successful attendance.

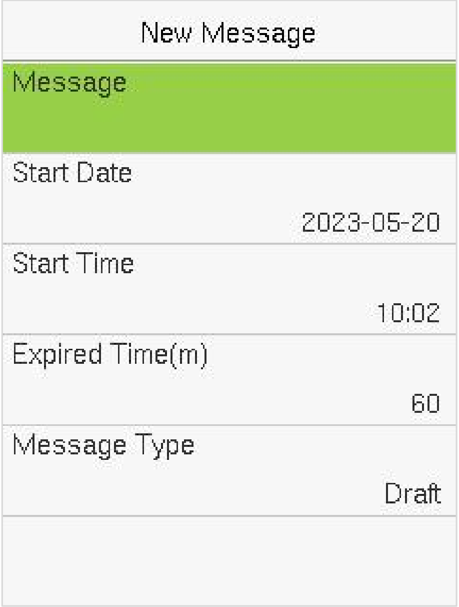
Select **Short Message** option on the main menu interface.



16.1 New Message

1. Select **New Message** on the **Short Message** interface.




New Message

Message

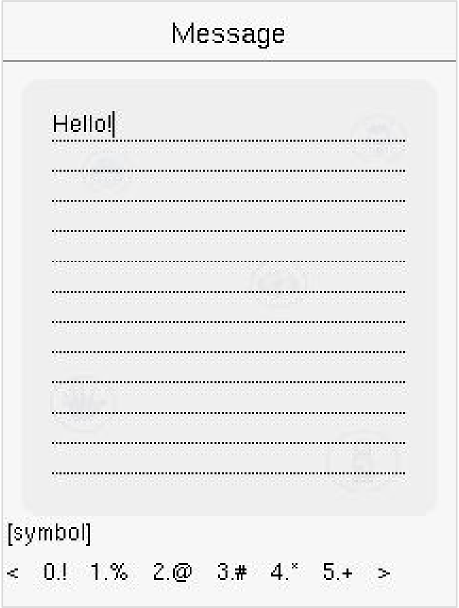
Start Date 2023-05-20

Start Time 10:02

Expired Time(m) 60

Message Type Draft

2. Select **Message** option on the **New Message** interface to edit the notice content and set additional options as needed.

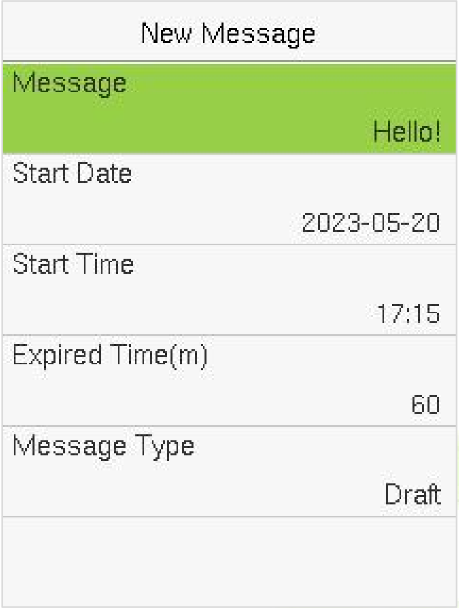


Message

Hello!

[symbol]

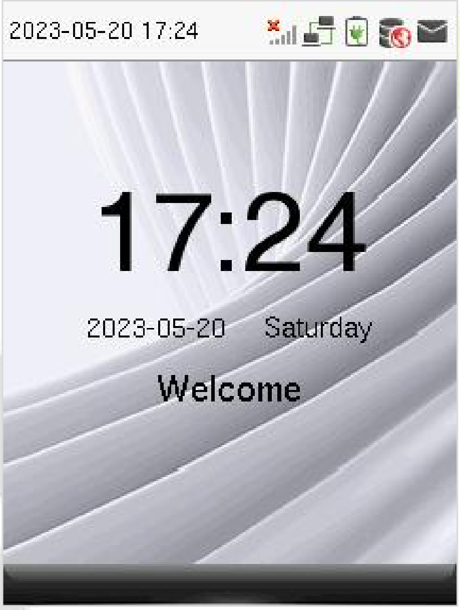
< 0.! 1.% 2.@ 3.# 4.* 5.+ >



New Message

Message	Hello!
Start Date	2023-05-20
Start Time	17:15
Expired Time(m)	60
Message Type	Draft

3. When the message editing is finished, the ✉ icon will be displayed in the upper right corner of the initial screen in the specified time. As shown in the figure below.



2023-05-20 17:24

17:24

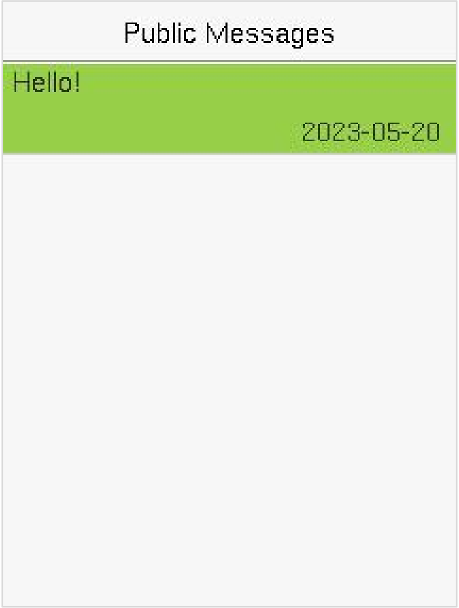
2023-05-20 Saturday

Welcome

16.2 Public Messages

Select **Public** option to set the SMS as a public message and also display it in the public messages list.

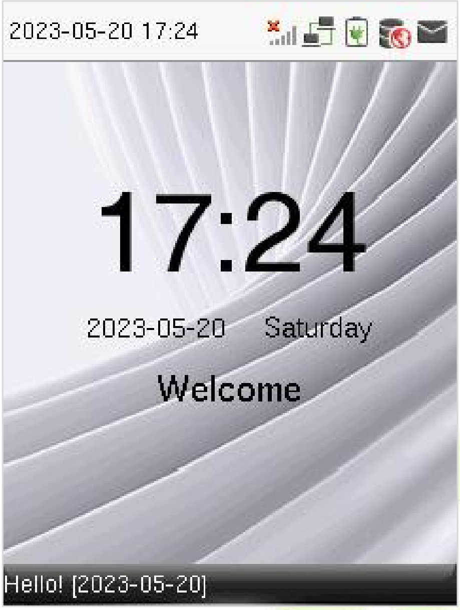
After configuration of a public message, within the specified time period, the main interface displays the short message icon ✉ in the upper right corner and displays the content of public short messages in scrolling mode in the lower part so that all employees can view the information.



Public Messages

Hello!

2023-05-20



2023-05-20 17:24

17:24

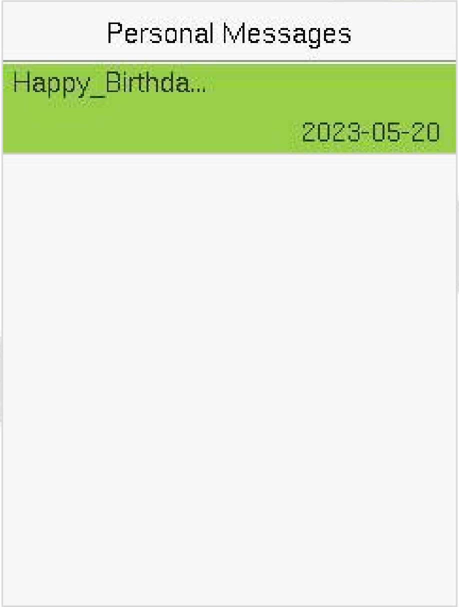
2023-05-20 Saturday

Welcome

Hello! [2023-05-20]

16.3 Personal Messages

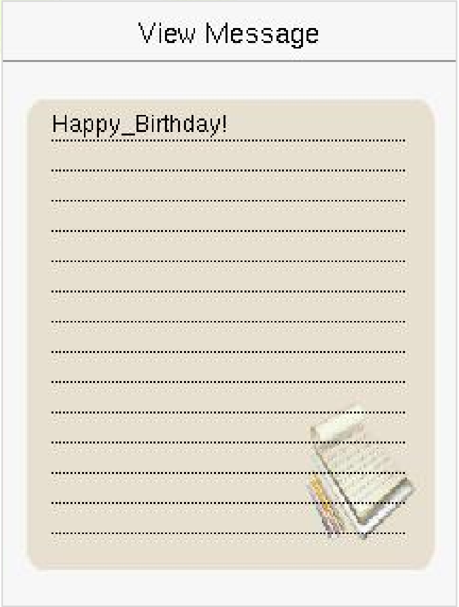
Select **Personal** option to set the SMS as a personal message. After the setting is completed, the SMS will be displayed in the personal messages list. And the content of this personal message will be displayed after this user is authenticated.



Personal Messages

Happy_Birthda...

2023-05-20

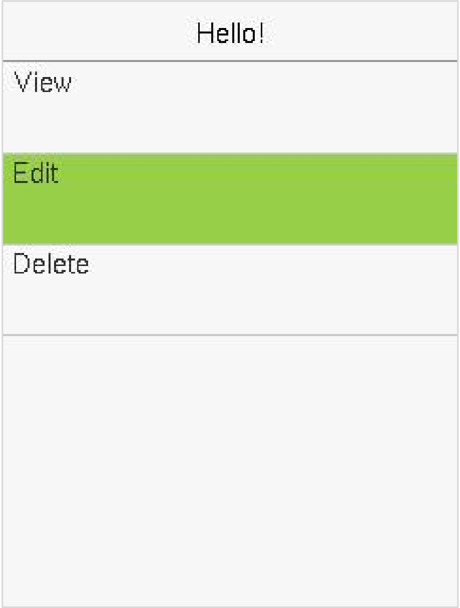


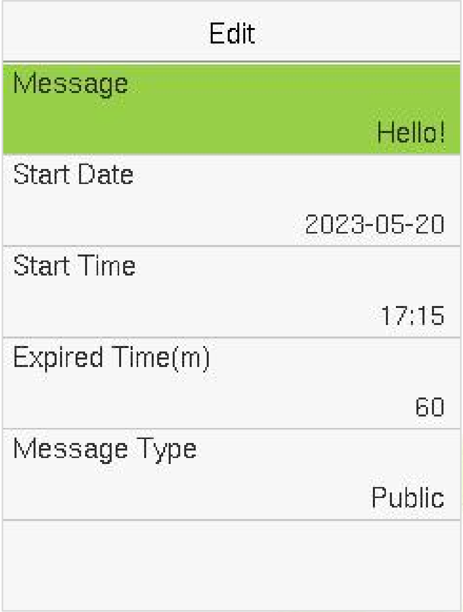
View Message

Happy_Birthday!

16.4 Edit Messages

Choose a message from the list and select **Edit** to enter the **Edit** message interface:




Edit

Message: Hello!

Start Date: 2023-05-20

Start Time: 17:15

Expired Time(m): 60

Message Type: Public

Note: The operation of editing a message is the same as that of adding a message.

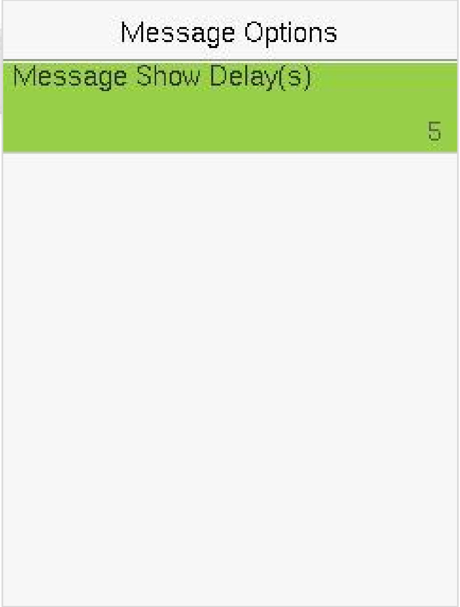
16.5 Delete Messages

Choose a message from the list and select **Delete** to enter its interface. Click **M/OK** to confirm and exit.

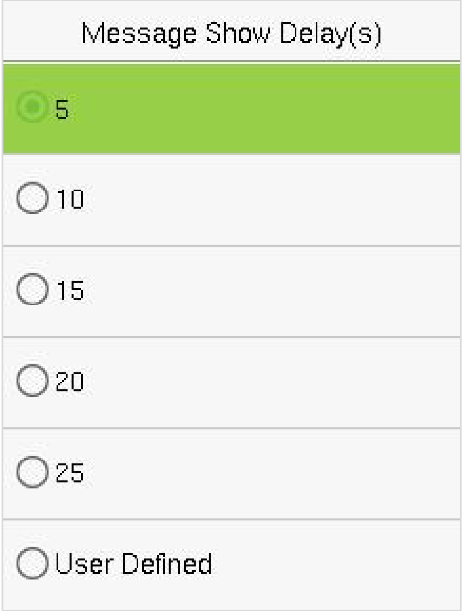
16.6 Message Options

Use to set the personal Message Show Delay time on the initial interface.

Select **Message Options** on the **Short Message** interface.


Message Options

Message Show Delay(s): 5


Message Show Delay(s)

● 5

○ 10

○ 15

○ 20

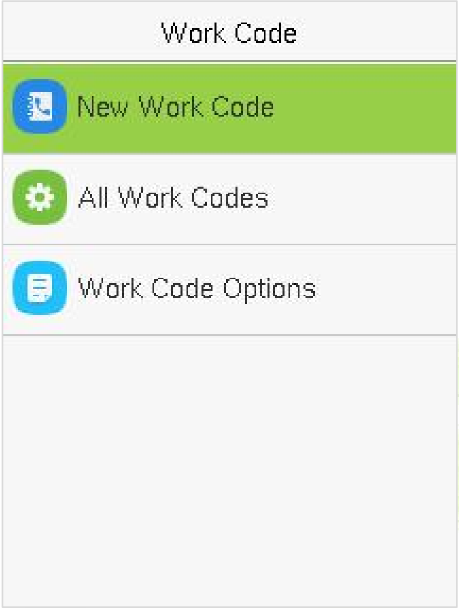
○ 25

○ User Defined

17 Work Code ★

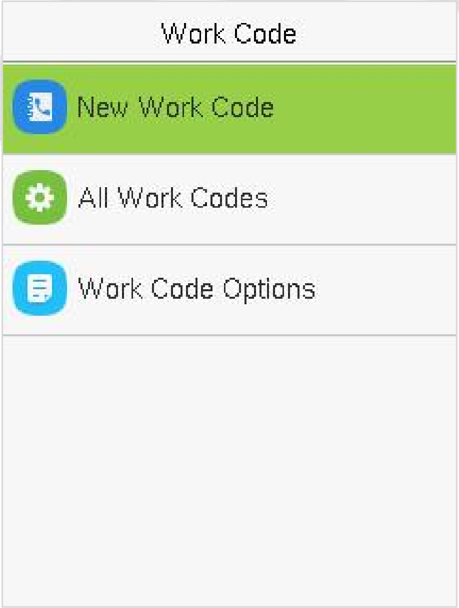
Employees' salaries are subject to their attendance records. Employees may be engaged in different types of work which may vary with time periods. Considering the salaries vary with work types, the FFR terminal provides a parameter to indicate the corresponding work type for every attendance record to facilitate rapid understanding of different attendance situations during the handling of attendance data.

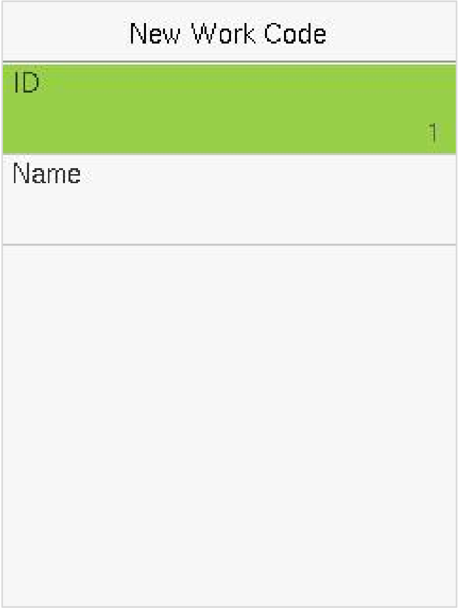
Select **Work Code** option on the main menu interface.



17.1 New Work Code

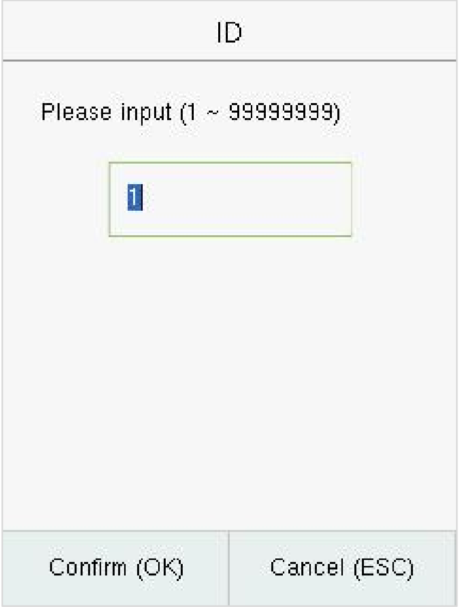
1. Select **New Work Code** on the **Work Code** interface.





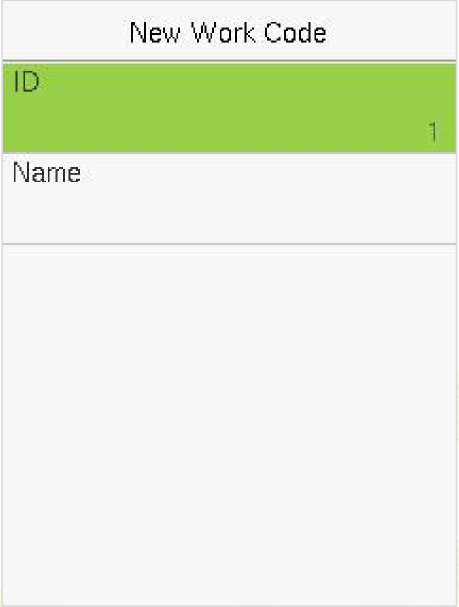
- **ID:** A digital code of the work code.
- **Name:** The meaning of the work code.

2. Enter the user ID using keypad, press **M/OK**.


ID

Please input (1 ~ 99999999)

1

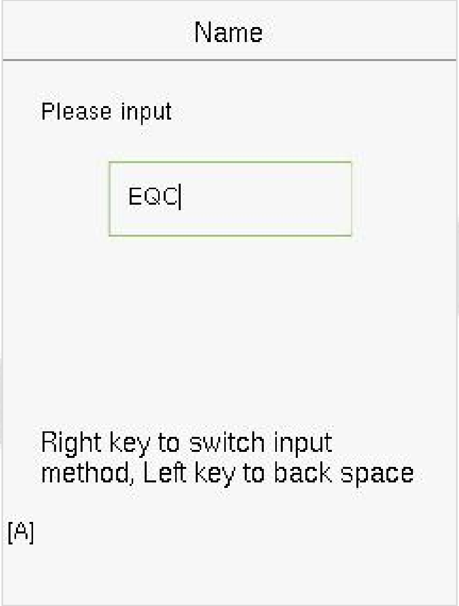

New Work Code

ID: 1

Name

Note: The terminal supports the 1 to 99999999-digit IDs by default. If a prompt message "The ID already exists!" is displayed, enter another ID.

3. Enter the name then press **M/OK**.

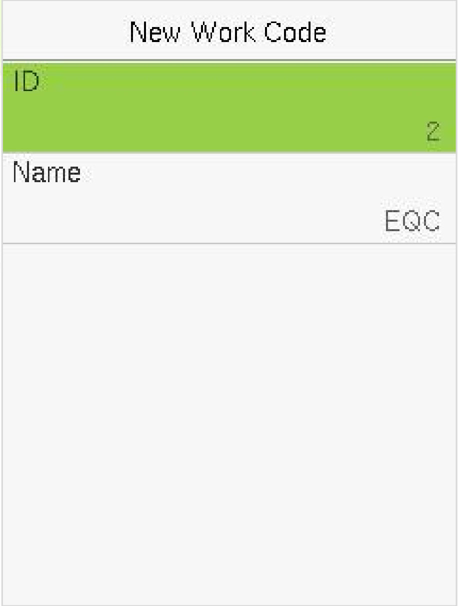

Name

Please input

EQC

Right key to switch input method, Left key to back space

[A]


New Work Code

ID: 2

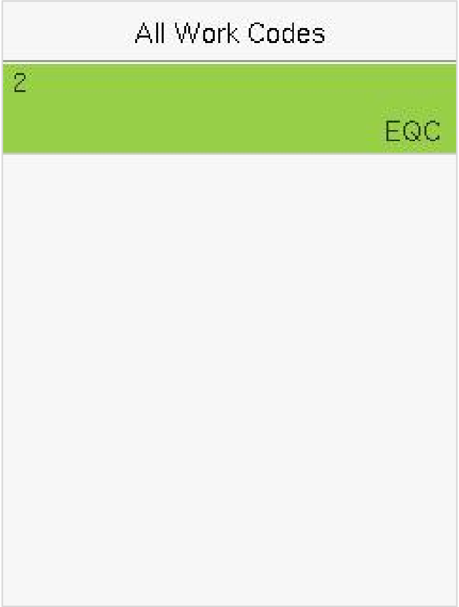
Name: EQC

Note: The terminal supports the 1- to 23-character names by default. For details of enter name, see Appendix1 Text Input Instructions.

17.2 All Work Codes

You can view, edit or delete the work code from the work codes list.

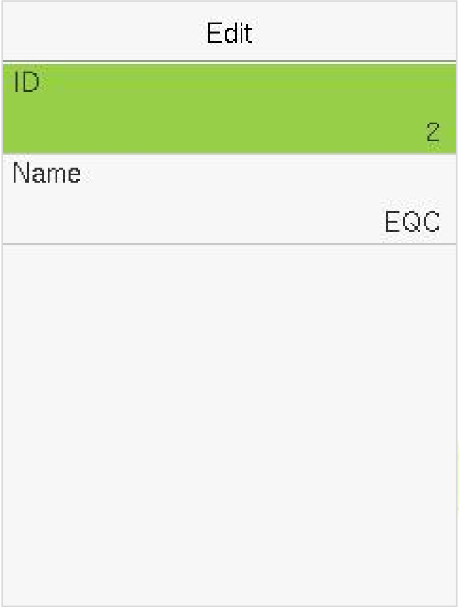
1. Select **All Work Codes** on the **Work Code** interface and to view all work codes and press ▼ to select the one you want to edit or delete.



All Work Codes

2

EQC



Edit

ID

2

Name

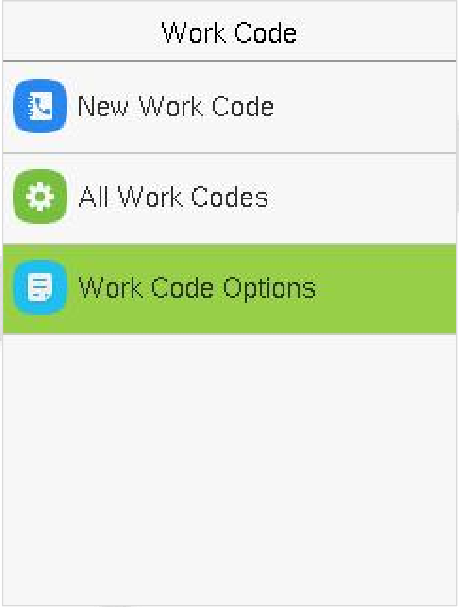
EQC

Note: The operation of editing is the same as that of adding a work code, except that the ID cannot be modified when editing.

17.3 Work Code Options

Used to set verify whether enter the Work Code number must be entered must exist.

Select **Work Code Options** on the **Work Code** interface. Press **M/OK** to open or close.

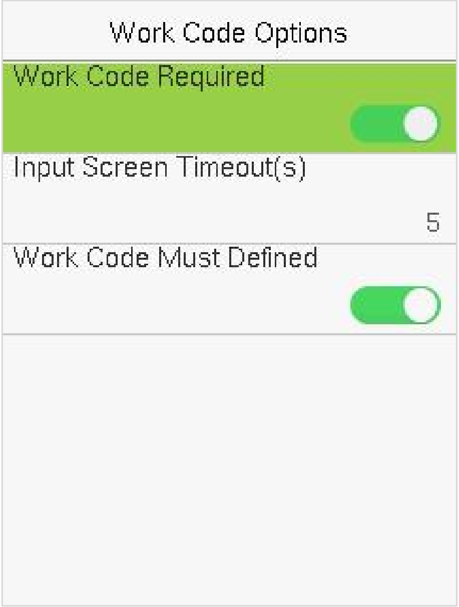


Work Code

New Work Code

All Work Codes

Work Code Options



Work Code Options

Work Code Required

Input Screen Timeout(s)

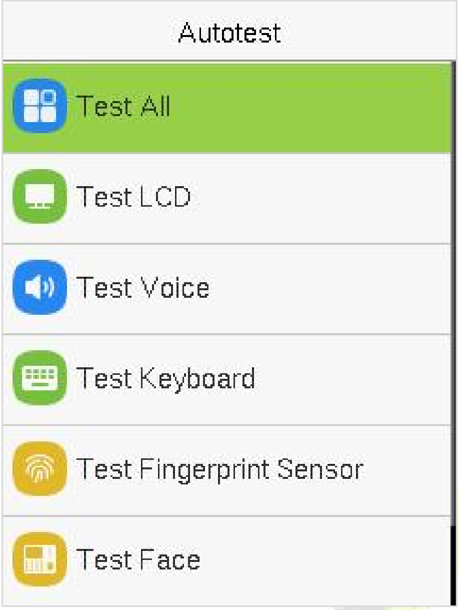
5

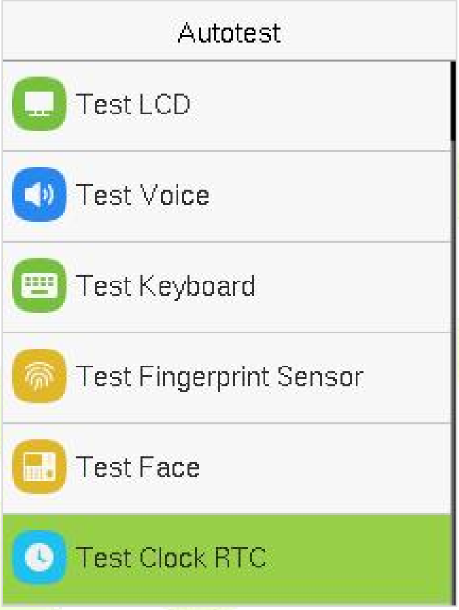
Work Code Must Defined

18 Autotest

The auto test enables the system to automatically test whether the functions of various modules are working normally, including tests for the LCD, voice, sensor, keyboard, and clock.

Select **Autotest** option on the main menu interface.



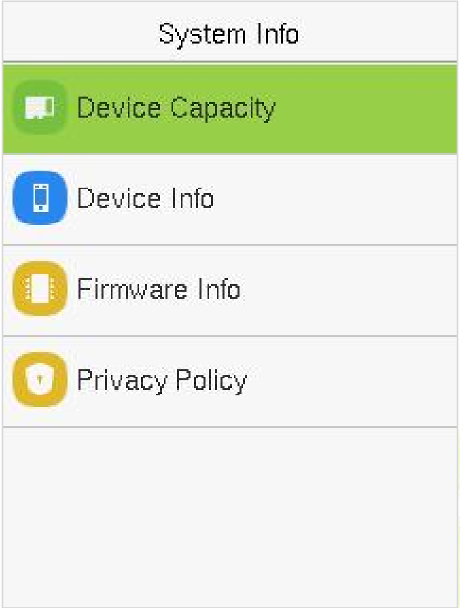


Item	Description
Test All	To automatically test whether the LCD, audio, camera and RTC are working normally.
Test LCD	To automatically test the display of the LCD screen by displaying all the color bands including pure white and pure black to check whether the screen displays the colors accurately.
Test Voice	To automatically test whether the audio files stored in the device are complete and the voice quality is good.
Test Keyboard	The terminal tests whether every key on the keyboard works normally. Press any key on the **[Keyboard Test]** interface to check whether the pressed key matches the key displayed on the screen. The keys are displayed as dark grey before and turn blue after pressed. Press **[ESC]** to exit the test.
Test Fingerprint Sensor	The terminal automatically tests whether the fingerprint collector works properly by checking whether the fingerprint images are clear and acceptable. When the user places his/her finger in the fingered guide, the collected fingerprint image displays on the screen in real-time. Press **[ESC]** to exit the test.
Test Face	To test if the camera functions properly it checks the photos taken and determines if they are clear enough.
Test Clock RTC	To test the RTC. The device checks whether the clock works normally and accurately with a stopwatch. Touch the screen to start counting and press it again to stop counting.

19 System Information

You can use the system information option to view the storage status, version, and firmware information of the device.

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



System Info

Device Capacity

Device Info

Firmware Info

Privacy Policy

Item	Description
Device Capacity	Displays the current device's user storage, password, fingerprint, card and face storage, administrators, access records, attendance and blocklist photos, and profile photos.
Device Info	Displays the device's name, serial number, MAC address, face algorithm version information, fingerprint algorithm version information, platform information, MCU version, manufacturer and and manufacturer date.
Firmware Info	Displays the firmware version and other version information of the device.
Privacy Policy	For personal privacy policy, please refer to Appendix 2 Privacy Policy (This menu is displayed after enabled the **Security Setting** function).

20 Connect to ZKBioTime Software ★

20.1 Set the Communication Address

- **Device side:**

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

   IP address: Set the IP address as of the device.

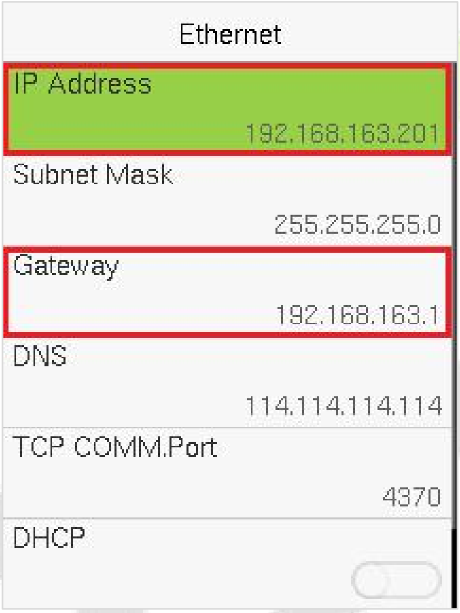
   Gateway: Set the gateway as of the device.

   (**Note:** The IP address should be able to communicate with the ZKBioTime Software Server, preferably in the same network segment with the server address)

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

   Server address: Set the IP address as of ZKBioTime Server.

   Server port: Set the server port as of ZKBioTime Server.



Ethernet

IP Address 192.168.163.201

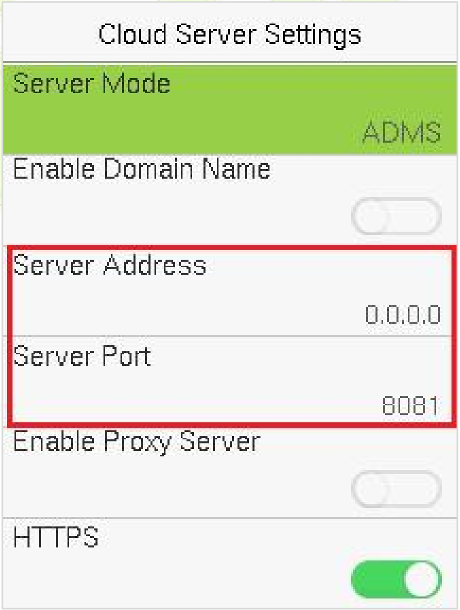
Subnet Mask 255.255.255.0

Gateway 192.168.163.1

DNS 114.114.114.114

TCP COMM.Port 4370

DHCP



Cloud Server Settings

Server Mode ADMS

Enable Domain Name

Server Address 0.0.0.0

Server Port 8081

Enable Proxy Server

HTTPS

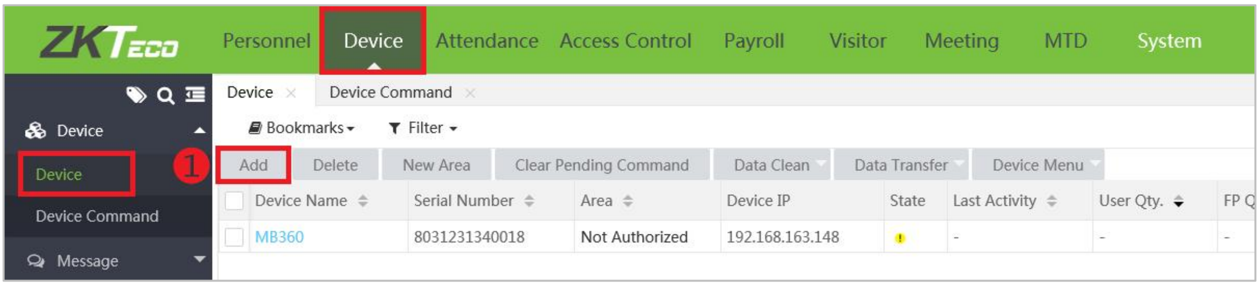
Note:

ADMS is an optional feature. When connecting ZKBioTime software, it is required that the device has ADMS capability and is enabled.

20.2 Add Device on the Software

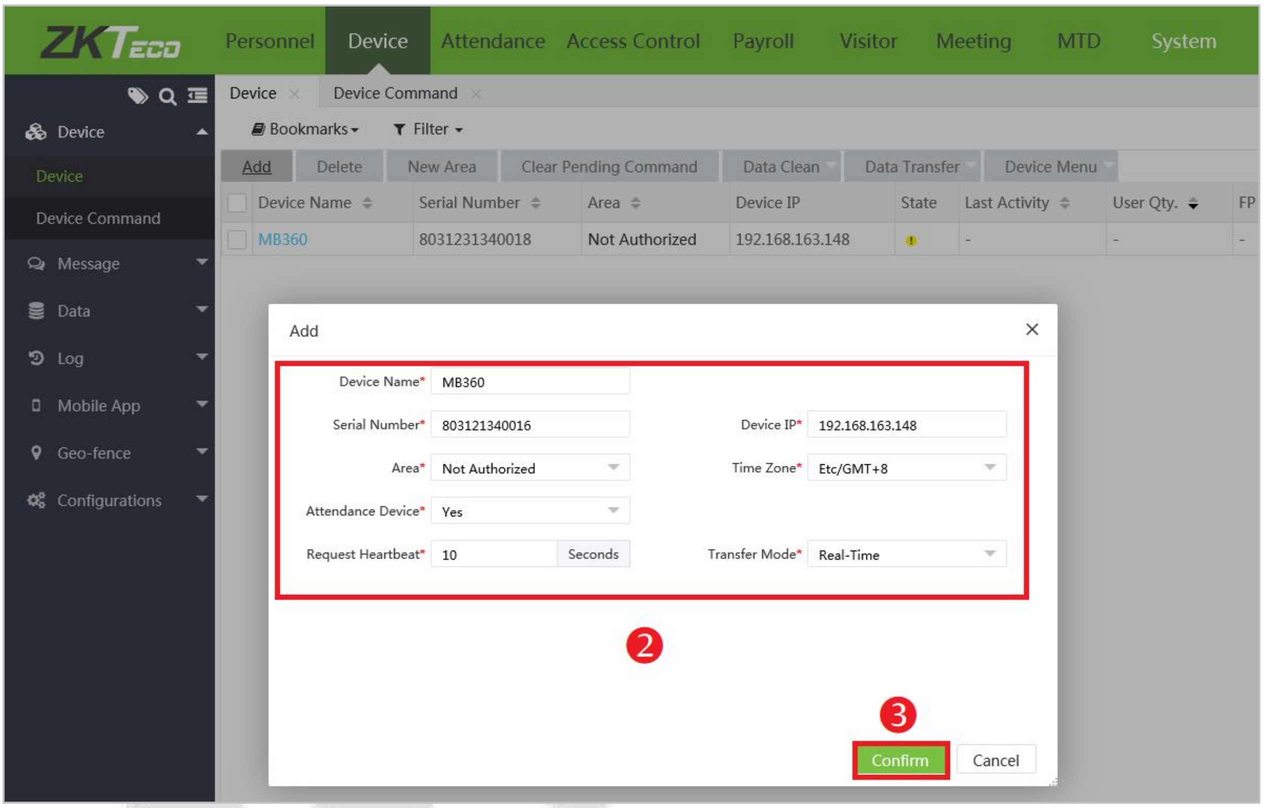
To add the device manually, proceed with the following steps:

1. Click **Device** > **Device** > **Add** to add a device manually.



Device Name	Serial Number	Area	Device IP	State	Last Activity	User Qty.	FP Q
MB360	8031231340018	Not Authorized	192.168.163.148	!	-	-	-

2. In the Add window that pops up, enter the relevant parameters.



Device Name	Serial Number	Area	Device IP	State	Last Activity	User Qty.	FP
MB360	8031231340018	Not Authorized	192.168.163.148	!	-	-	-

Add

Device Name* MB360

Serial Number* 803121340016

Device IP* 192.168.163.148

Area* Not Authorized

Time Zone* Etc/GMT+8

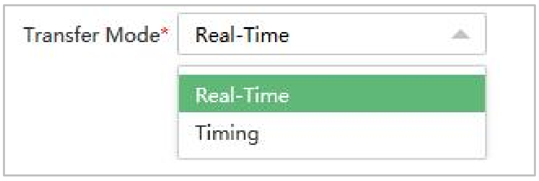
Attendance Device* Yes

Request Heartbeat* 10 Seconds

Transfer Mode* Real-Time

Enter the details as shown below:

- **Device Name:** Enter the device name maximum of 50 characters.
- **Serial Number:** Enter the serial number of the device.
- **Device IP:** Enter the IP address of the device.
- **Area:** In the drop-down list, select the area to which the T&A device belongs.
- **Time Zone:** When a time zone is selected, the time on the T&A device will be automatically synchronized to the standard time in the particular time zone.
- **Attendance Device:** Select whether the device is an attendance device or not.
- **Request Heartbeat:** Set the time for the device to automatically transmit the data to the system.
- **Transfer Mode:** Select the data transfer mode between software and devices. The Transfer mode can be real-time or at a specified time.


Transfer Mode* Real-Time

3. When finished, click **Confirm** to add the device, save and exit.

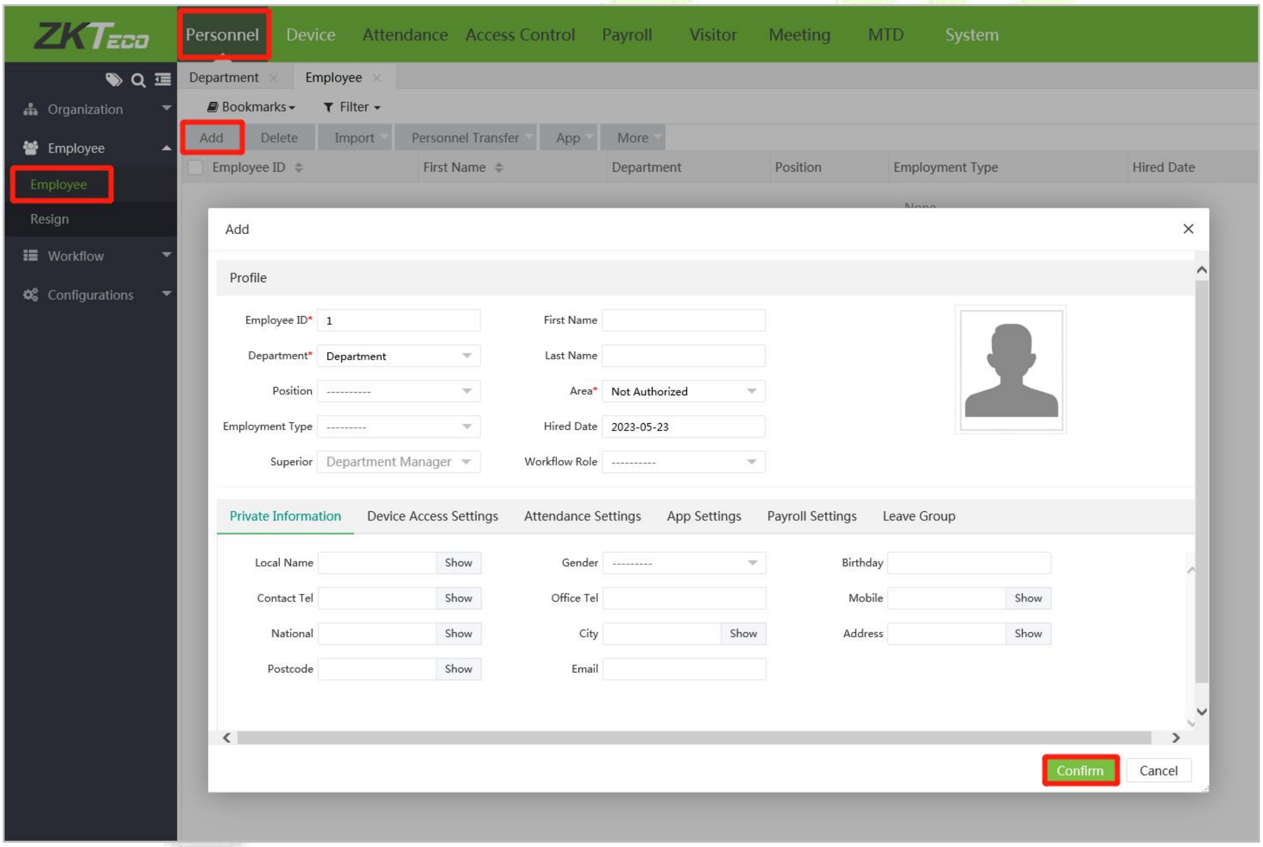
✍**Note:**

When an employee is added to a device, the employee information will be uploaded to the server automatically. It will be synchronized with other devices in the same area.

20.3 Add Personnel on the Software

1. Click **Personnel** > **Employee** > **Employee** > **Add** to register user.

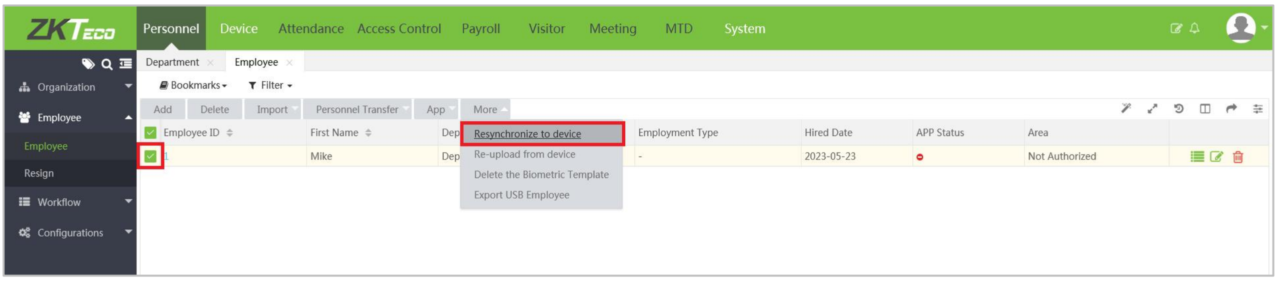
2. Fill in all the required fields and click **Confirm** to register a new user.


Add

Profile

Employee ID* 1
Department* Department
Position ----------
Employment Type ---------
Superior Department Manager
First Name
Last Name
Area* Not Authorized
Hired Date 2023-05-23
Workflow Role ----------

3. Synchronize personnel on the software to devices in the corresponding area. In the personnel module, select **Personnel** > **Employee** > **Employee** and click **More** > **Resynchronize to Device** to access the confirmation interface for synchronizing.



☑	Employee ID	First Name	Dep	Employment Type	Hired Date	APP Status	Area
☑	1	Mike	Dep	-	2023-05-23	●	Not Authorized

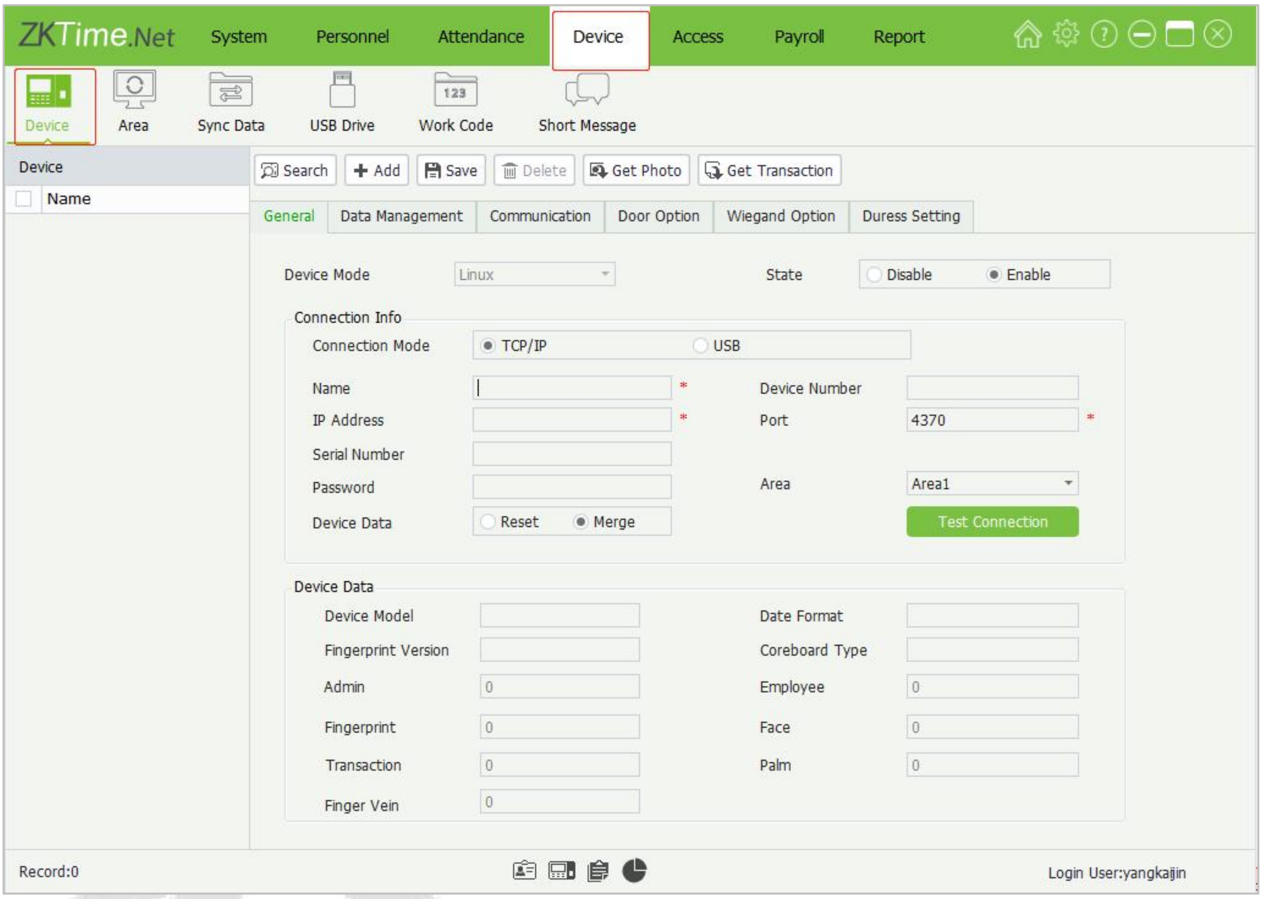
For more details, please refer to the **ZKBioTime Software User Manual**.

21 Connect to ZKTime.Net Software

21.1 Add Device on the Software

To add the device manually, proceed with the following steps:

1. Click **Device** > **Device** to enter to the **Device Management** interface.



Device Mode: Linux

State: ○ Disable ● Enable

Connection Mode: ● TCP/IP ○ USB

Port: 4370 *

Area: Area1

Device Data: ○ Reset ● Merge

Admin: 0

Employee: 0

Fingerprint: 0

Face: 0

Transaction: 0

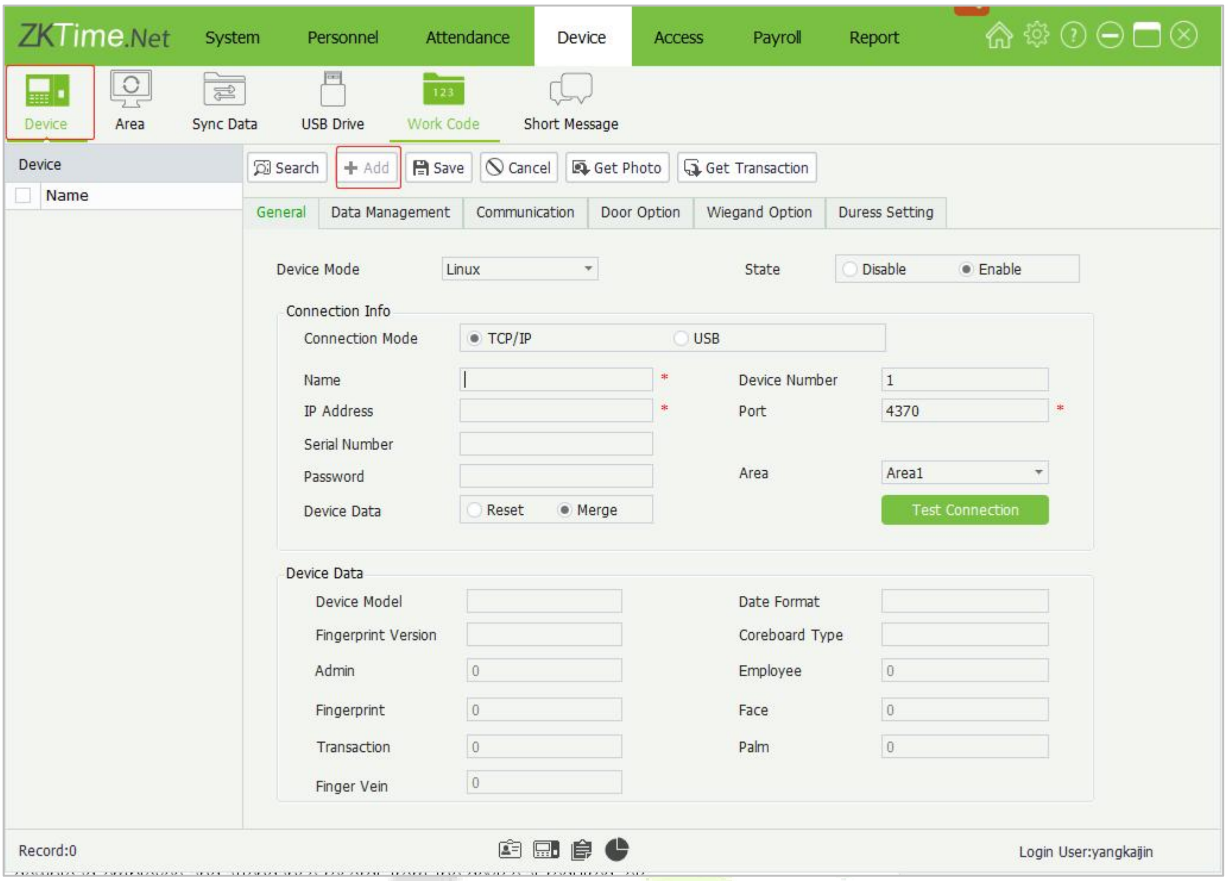
Palm: 0

Finger Vein: 0

Record:0

Login User:yangkaijin

2. Click **Add** to enter the **Add Device** interface. Set the parameters as required.



Device

□ Name

Device Mode	Linux	State	○ Disable ● Enable

Connection Info

Connection Mode	● TCP/IP ○ USB		
Name	*	Device Number	1
IP Address	*	Port	4370 *
Serial Number			
Password		Area	Area1
Device Data	○ Reset ● Merge		

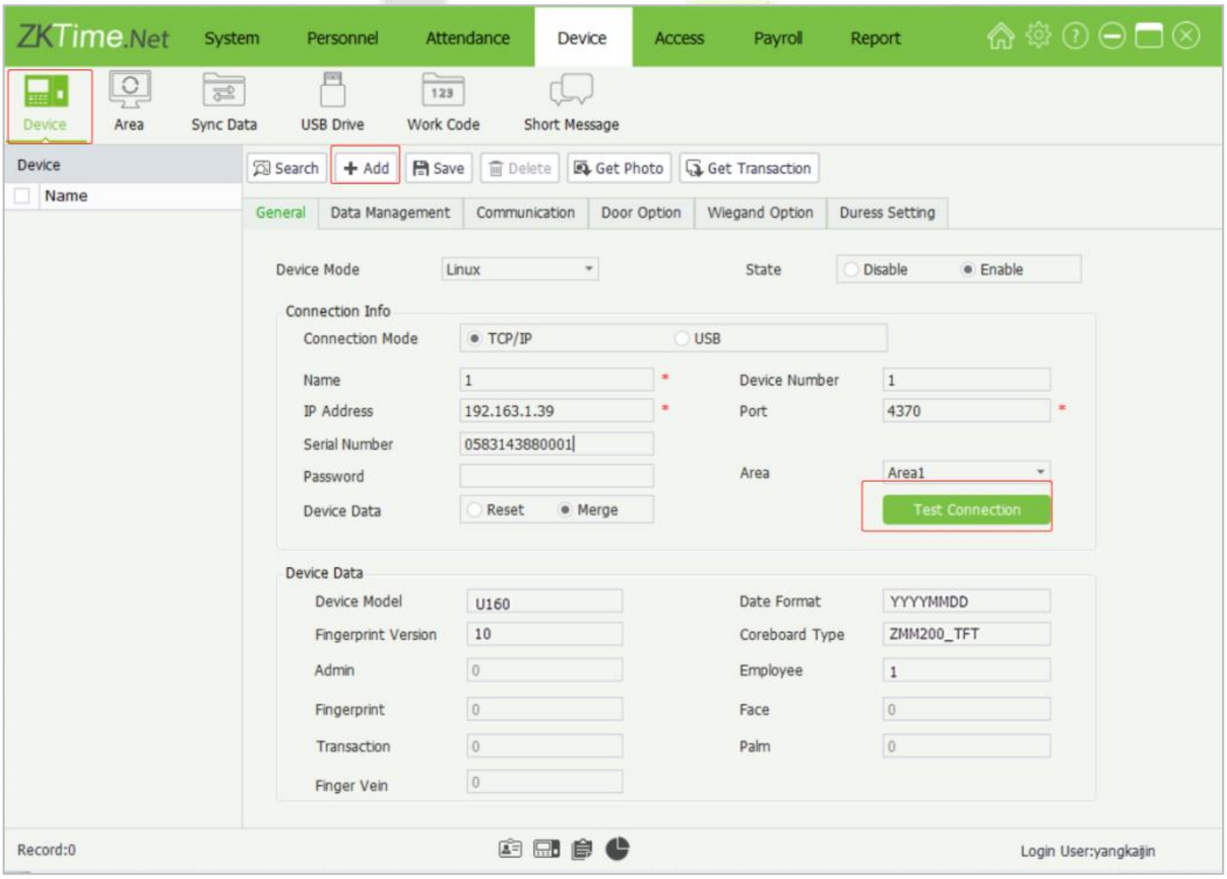
Device Data

Device Model		Date Format	
Fingerprint Version		Coreboard Type	
Admin	0	Employee	0
Fingerprint	0	Face	0
Transaction	0	Palm	0
Finger Vein	0		

Record:0

Login User:yangkaijin

3. After setting, click **Test Connection** to check whether the device is connected to the system.



Device

□ Name

Device Mode	Linux	State	○ Disable ● Enable

Connection Info

Connection Mode	● TCP/IP ○ USB		
Name	1 *	Device Number	1
IP Address	192.163.1.39 *	Port	4370 *
Serial Number	0583143880001		
Password		Area	Area1
Device Data	○ Reset ● Merge		

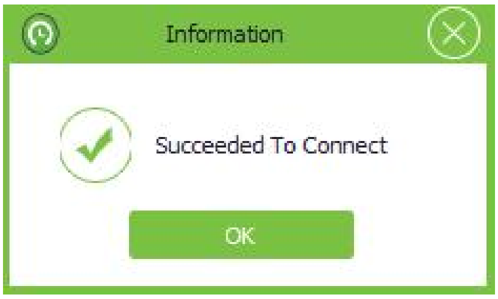
Device Data

Device Model	U160	Date Format	YYYYMMDD
Fingerprint Version	10	Coreboard Type	ZMM200_TFT
Admin	0	Employee	1
Fingerprint	0	Face	0
Transaction	0	Palm	0
Finger Vein	0		

Record:0

Login User:yangkaijin

4. If the connection is successful, the Information box will pop-up.



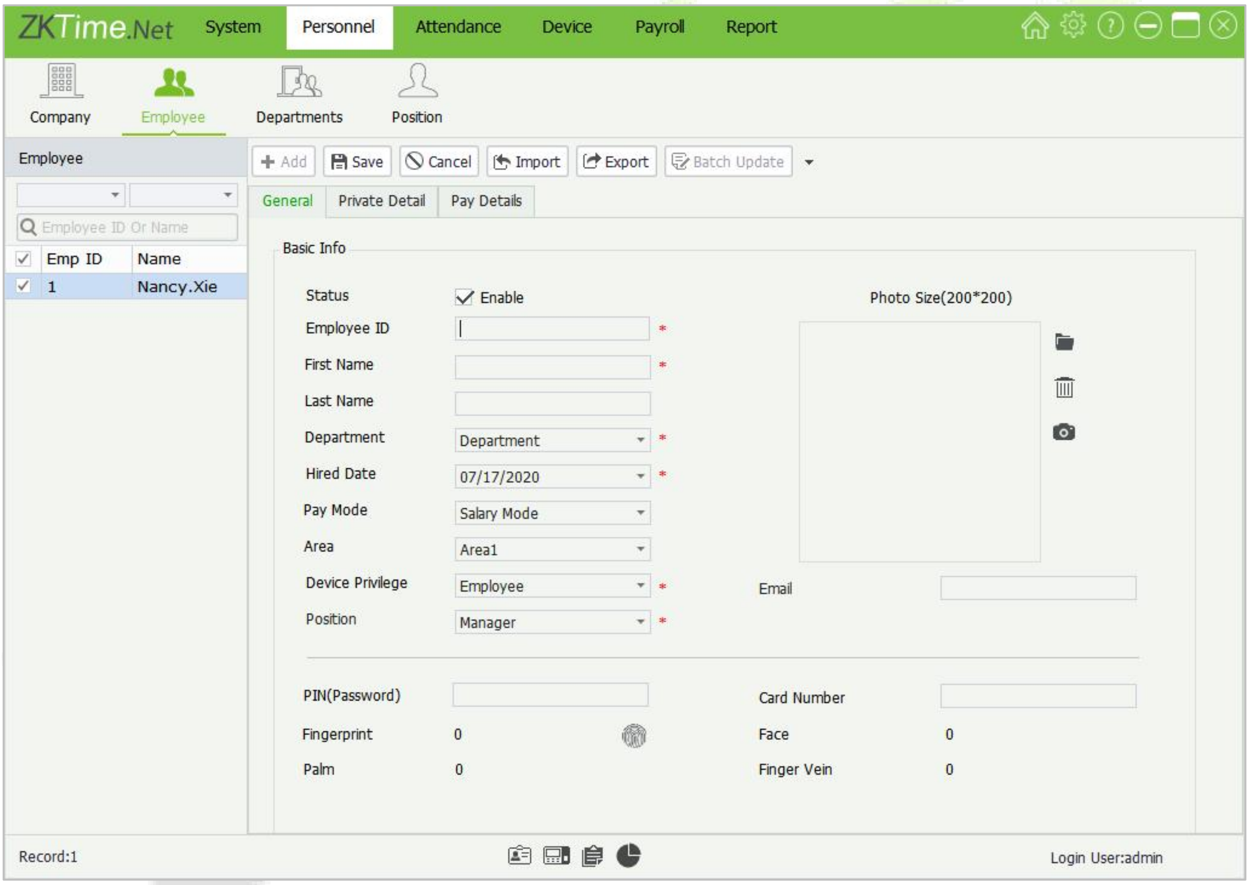
Information

Succeeded To Connect

5. Click **Save** to save device info.

21.2 Add Personnel on the Software

1. Click **Personnel** > **Employee** to enter to the **Employee** interface.



☑	Emp ID	Name
☑	1	Nancy.Xie

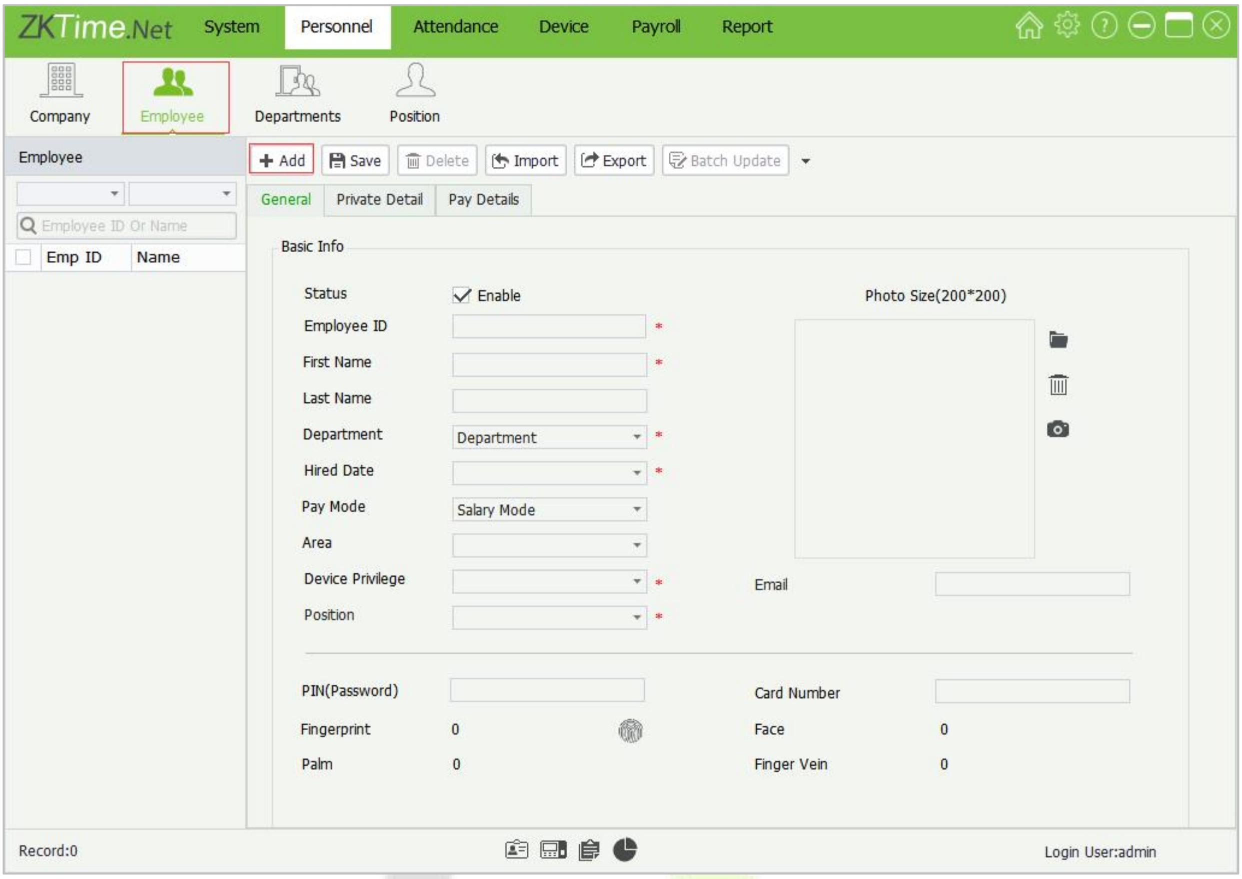
Basic Info

Status	☑ Enable	Photo Size(200*200)	
Employee ID	*		
First Name	*		
Last Name			
Department	Department *		
Hired Date	07/17/2020 *		
Pay Mode	Salary Mode		
Area	Area1		
Device Privilege	Employee *	Email	
Position	Manager *		
PIN(Password)		Card Number	
Fingerprint	0	Face	0
Palm	0	Finger Vein	0

Record:1

Login User:admin

2. Click **Add** to enter the **Add Employee** interface. Add employee info and enroll fingerprint and issue card as required.



Status ☑ Enable

Department: Department

Pay Mode: Salary Mode

Fingerprint 0

Palm 0

Face 0

Finger Vein 0

Record:0

Login User:admin

3. After setting, click **Save** to save employee info.

For more details, please refer to the **ZKTime.Net User Manual**.

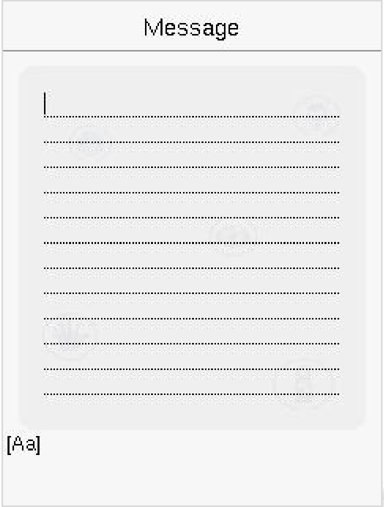
Appendix

Appendix 1 T9 Input

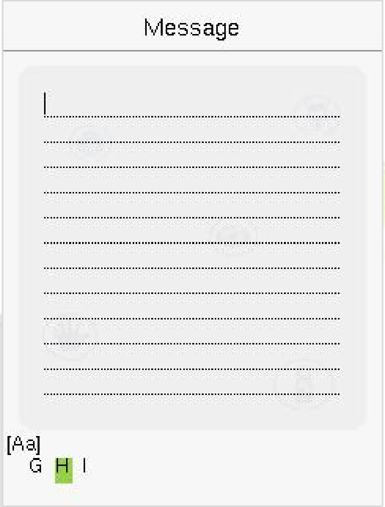
T9 input (intelligent input) is quick and high efficient. The device support T9 English and symbol input. There are 3 or 4 English letters on numeric keys (2~9), for example, A, B, C are on numeric key 2. Press the corresponding key once, and the program will generate effective spelling. By using T9 input, names, user roles, work codes, SMS content and some symbols can be input.

When entering text or characters, press the [**M/OK**] to automatically open the **T9 Input**. Pressing the ► key switches between the input methods [**Aa**], [**a**], [**A**], [**123**] and [**symbol**]. Press the [**ESC**] key to exit.

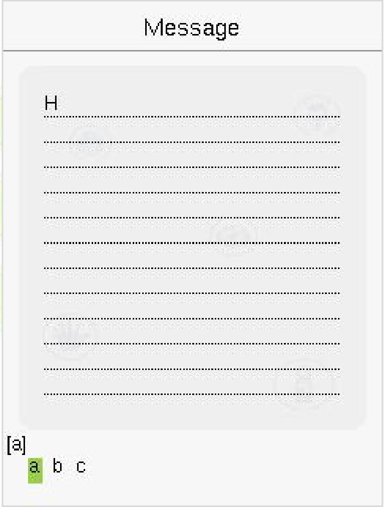
Take inputting a short message as an example:



Press [**M/OK**] to display the input method. Press ► key to switch the input method.

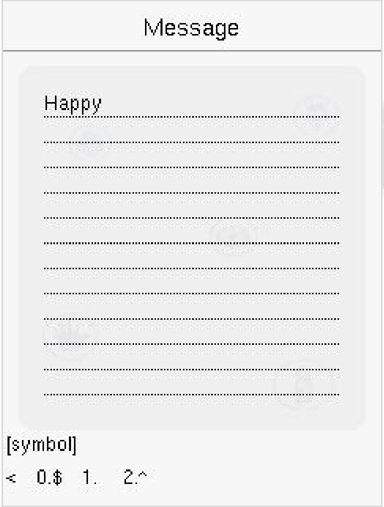


Press the **4**GHI button two times to enter the **H** letter.



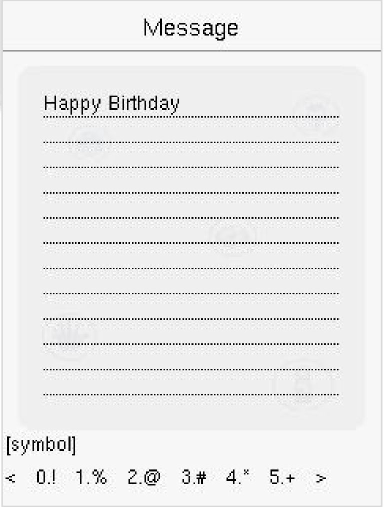
H

Press the **2**ABC button one time to enter the **a** letter.



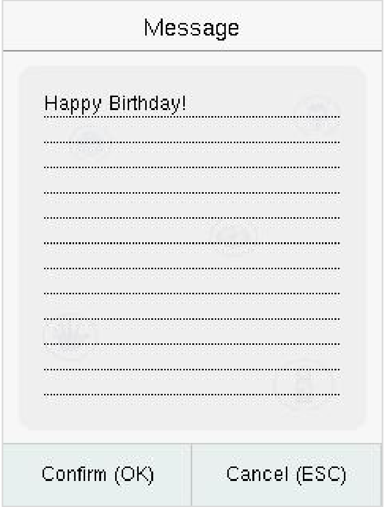
Happy

Press ▲/▼ key to page up or down to select the symbol. Press **1** key to enter the space symbol.



Happy Birthday

Press **0** to enter the exclamation point.



Happy Birthday!

Press [**M/OK**] to save and exit. Press [**ESC**] to exit directly.

Appendix 2 Self-Service Attendance Terminal FAQs

1. Does self-service attendance terminal support scheduling based on every other day?

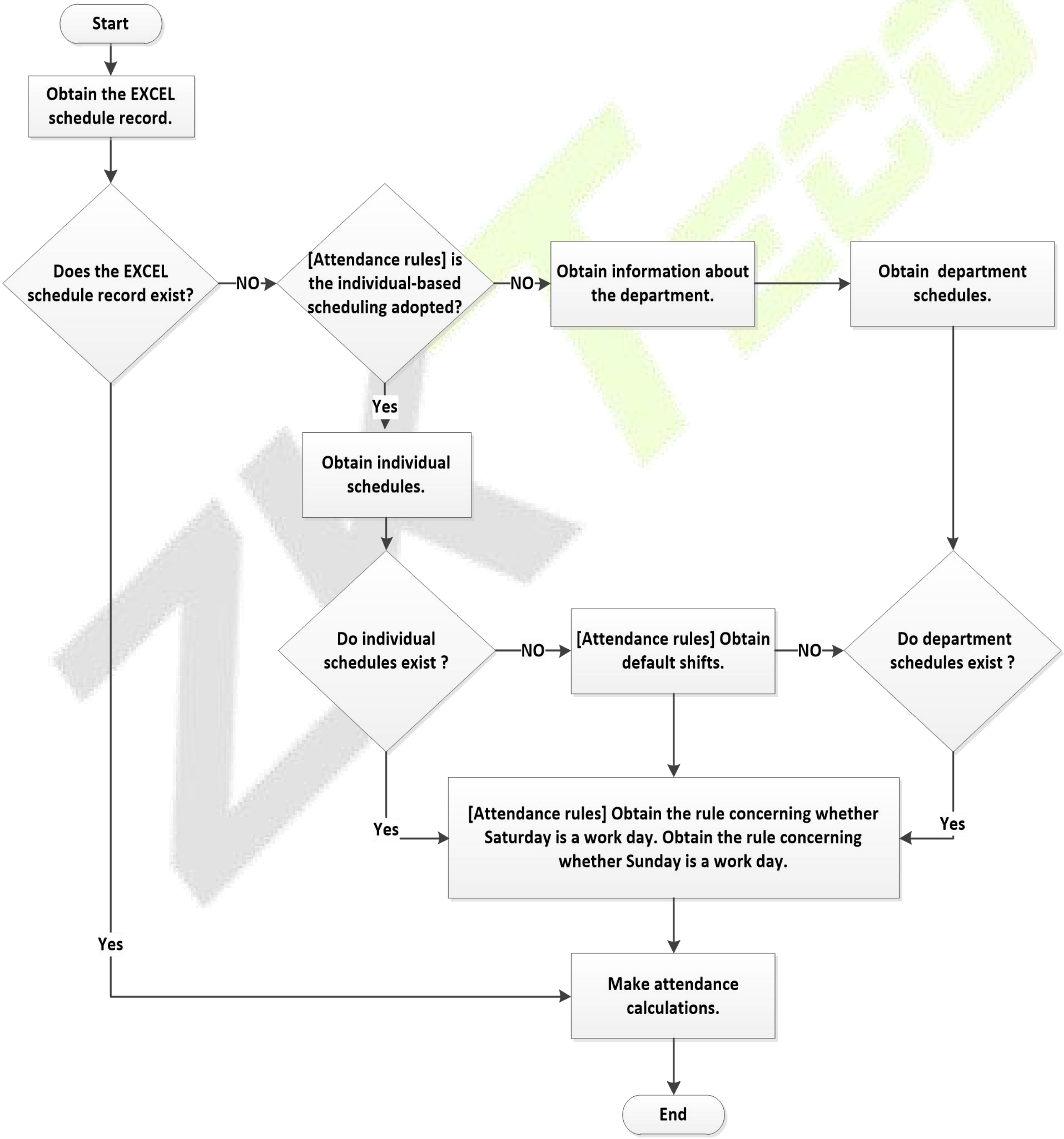
A: No.

2. Can the setting records downloaded from the device be edited on WPS software?

A: Yes. Setting records are supported in Microsoft Office 2003, Microsoft Office 2007, and WPS Office 2012 Personal.

3. What is the attendance calculation flow adopted by the self-service attendance terminal?

A: SSR attendance calculation flow.


Start
Obtain the EXCEL schedule record.
Does the EXCEL schedule record exist?
NO
[Attendance rules] is the individual-based scheduling adopted?
NO
Obtain information about the department.
Obtain department schedules.
Yes
Obtain individual schedules.
Do individual schedules exist ?
NO
[Attendance rules] Obtain default shifts.
NO
Do department schedules exist ?
Yes
[Attendance rules] Obtain the rule concerning whether Saturday is a work day. Obtain the rule concerning whether Sunday is a work day.
Yes
Yes
Make attendance calculations.
End

4. How to calculate special overtime hours?

The following cases are deemed special overtime:

a) When an EXCEL schedule record exists and attendance reports are used for attendance calculation, there are check-in and check-out records though there is no schedule (or rest is arranged) for the current date.

b) When no EXCEL schedule record is available, there are check-in and check-out records though Saturday and Sunday are non-working days.

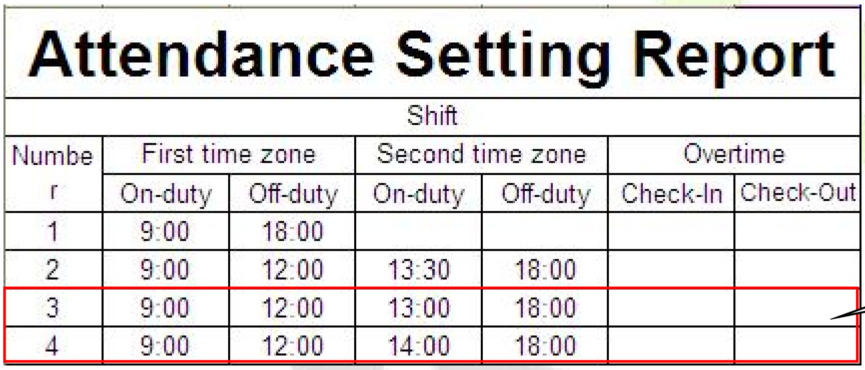
Overtime hours refer to the duration counted from the first check-in time to the last check-out time on the current day.

5. How to arrange schedules using the attendance setting report?

Step 1: Insert a USB flash drive into the USB port or SD card into the SD port of the device and download the Attendance Setting Report.xls to the USB flash drive or SD card.

Step 2: Open the Attendance Setting Report.xls on a computer.

Step 3: Set shifts in the Attendance Setting Report.xls as required.

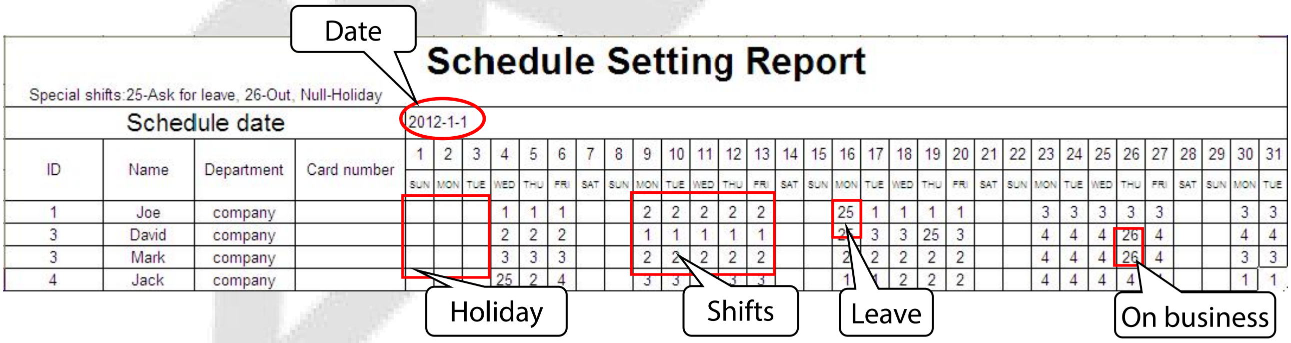


Attendance Setting Report

Shift						
Number	First time zone		Second time zone		Overtime	
	On-duty	Off-duty	On-duty	Off-duty	Check-In	Check-Out
1	9:00	18:00				
2	9:00	12:00	13:30	18:00		
3	9:00	12:00	13:00	18:00		
4	9:00	12:00	14:00	18:00		

Data enclosed by a red rectangle is new shifts (shift 3 and shift 4). To add a shift, enter a time directly, in the range of 00:00 to 24:00.

Step 4: Arrange schedules for employees.



Schedule Setting Report

Special shifts:25-Ask for leave, 26-Out, Null-Holiday

Schedule date 2012-1-1

ID	Name	Department	Card number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
				SUN	MON	TUE	WED	THU	FRI	SAT	SUN	MON	TUE	WED	THU	FRI	SAT	SUN	MON	TUE	WED	THU	FRI	SAT	SUN	MON	TUE	WED	THU	FRI	SAT	SUN	MON	TUE
1	Joe	company					1	1	1			2	2	2	2	2			25	1	1	1	1			3	3	3	3	3			3	3
3	David	company					2	2	2			1	1	1	1	1			25	3	3	25	3			4	4	4	26	4			4	4
3	Mark	company					3	3	3			2	2	2	2	2			2	2	2	2	2			4	4	4	26	4			3	3
4	Jack	company					25	2	4			3	3	[illegible]	3	3			1	1	2	2	2			4	4	4	4	4			1	1

Note: Dates must be set correctly. For example, if the scheduling date is 2012-1-1, the schedule setting report contains the schedules of 31 days after 2012-1-1, that is, the schedule from 2012-1-1 to 2012-1-31. If the scheduling date is 2012-1-6, the schedule setting report contains schedules of 31 days after 2012-1-6, that is, the schedule from 2012-1-6 to 2012-2-5.

Step 5: Insert a USB flash drive into the USB port or SD card into the SD port of the device and upload the *Attendance Setting Report.xls* to the device. Then, the schedules in the *Attendance Setting Report* can be used.

6. What is the correct time format used in the setting reports?

A. The correct time format is shown in the following table.

Shift No.	First Time Range		Second Time Range		Overtime Range	
	On-duty	Off-duty	On-duty	Off-duty	Check-in	Check-out
1	09:00	18:00				
2	09:00	12:00	13:30	18:00		
3	9:5	18:00				

B. Incorrect time formats are as follows:

a) A time value is beyond the time range, such as 24:00.

b) A time value contains Chinese characters, for example, 9:00, which differs from 9:00.

c) A time value is preceded by a space. As shown in the following table, there is a space in front of 09:00 in shift 1.

Shift No.	First Time Range		Second Time Range		Overtime Range	
	On-duty	Off-duty	On-duty	Off-duty	Check-in	Check-out
1	09:00	18:00				
2	09:00	12:00	13:30	18:00		
3	9:5	18:00				

d) A time value contains special characters, for example, _9:00 and 09:-1.

The device performs a validity check and error tolerance for other formats.

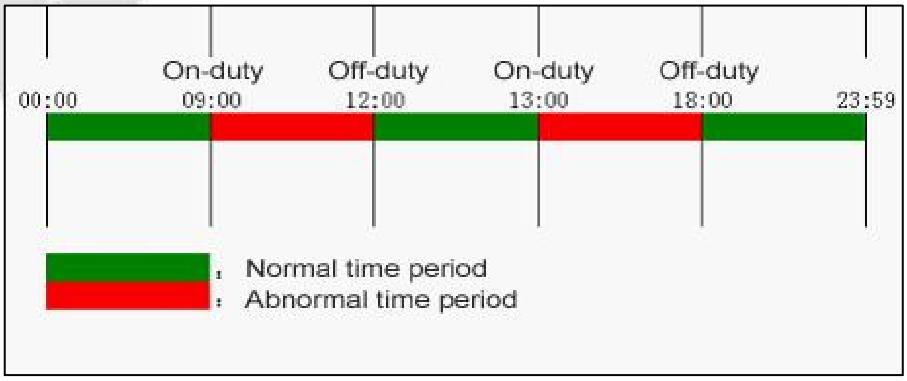
7. How does the self-service attendance terminal collect the correct attendance time based on the preset shift time?

A: The device collects attendance time based on the following principles:

a) Adopt the earliest time for normal attendance and the nearest time for abnormal attendance.

b) Adopt the normal attendance time if the normal attendance time and abnormal attendance time coexist.

c) Adopt a median in the attendance time range.



B: The following uses four examples to describe the preceding principles.

Example 1: Normal attendance

Attendance Time Range	09:00 — 12:00		13:00 — 18:00			
Attendance time of #1 employee	8:30, 8:35, 11:55,12:01, 12:50, 18:02,19:00					
Statistical result based on attendance rules	8:30	12:01	12:50	18:02		

Description: The attendance time 8:30 and 8:35 are earlier than the on-duty time 9:00 and they are within the normal attendance time range. Therefore, 8:30 is adopted for the on-duty time 9:00 based on the principle of adopting the earliest time for normal attendance. 18:02 and 19:00 are later than the off-duty time 18:00, and therefore, 18:02 is adopted based on the same principle.

Example 2: Late arrival

Attendance Time Range	09:00 — 12:00		13:00 — 18:00			
Attendance time of #1 employee	9:01, 9:04, 12:01, 12:50, 18:00					
Statistical result based on attendance rules	9:01	12:01	12:50	18:00		

Description: Employer 1 checks in for work at 9:01 and 9:04 and he/she is late based on the preset on-duty time. Based on the principle of adopting the nearest time for abnormal attendance, the correct check-in time is 9:01 rather than 9:04 because of 9:01 is nearer 9:00.

Example 3: Early leave

Attendance Time Range	09:00 — 12:00		13:00 — 18:00			
Attendance time of #1 employee	8:50, 11:40,11:55, 12:50, 18:01					
Statistical result based on attendance rules	8:50	11:55	12:50	18:01		

Description: The attendance time 12:50 is adopted based on the principle of adopting a median in the attendance time range. For the attendance time range from 9:00 to 12:00, the normal check-out time range for the off-duty time 12:00 is from 12:00 to 12:30 (that is, 12:00 + (13:00 - 12:00)/2). Therefore, the calculated time of attendance is shown in the preceding table.

Example 4: Absence

Case 1:

Attendance Time Range	09:00 — 12:00		13:00 — 18:00			
Attendance time of #1 employee	8:50, 12:50, 18:01					
Statistical result based on attendance rules	8:50	🟥	🟩 12:50	18:01		

Description: The attendance time 12:50 is adopted based on the principle of adopting a median in the attendance time range. For the attendance time range from 9:00 to 12:00, the normal check-out time range for the off-duty time 12:00 is from 12:00 to 12:30 (that is, 12:00 + (13:00 - 12:00)/2). Therefore, the check-out time is blank. The normal check-in time range for the on-duty time from 13:00 is from 12:30 to 13:00. The calculated time of attendance is shown in the preceding table.

Case 2:

Attendance Time Range	09:00 — 12:00		13:00 — 18:00				
Attendance time of #1 employee	8:50, 11:55, 12:20, 18:01						
Statistical result based on attendance rules	8:50	12:20	🟥	18:01			

Description: The time 12:20 is adopted based on the principle of adopting a median in the attendance time range. The normal check-out time range for the off-duty time 12:00 is from 12:00 to 12:30 (that is, 12:00 + (13:00 - 12:00)/2). Therefore, the check-out time of the employee is 12:20. The normal check-in time range for the on-duty time from 13:00 is from 12:30 to 13:00. Therefore, the check-in time of the employee is blank. The calculated time of attendance is shown in the preceding table.

Appendix 3 Privacy Policy

Notice:

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

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

I. Collected Information

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

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

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

II. Product Security and Management

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

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

3. Only your user ID is displayed by default. You can set whether to display other user verification information (such as Name, Department, Photo, etc.) under the Administrator privilege. **If you choose to display such information, we assume that you are aware of the potential security risks (for example, your photo will be displayed on the device interface)**.

4. The camera function is disabled in our products by default. If you want to enable this function to take pictures of yourself for attendance recording or take pictures of strangers for access control, the product will enable the prompt tone of the camera. **Once you enable this function, we assume that you are aware of the potential security risks**.

5. All the data collected by our products is encrypted using the AES 256 algorithm. All the data uploaded by the Administrator to our products are automatically encrypted using the AES 256 algorithm and stored securely. If the Administrator downloads data from our products, we assume that you need to process the data and you have known the potential security risk. In such a case, you shall take the responsibility for storing the data. You shall know that some data cannot be downloaded for sake of data security.

6. All the personal information in our products can be queried, modified, or deleted. If you no longer use our products, please clear your personal data.

III. How we handle personal information of minors

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

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

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

IV. Others

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

Appendix 4 Eco-friendly Operation

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

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

Hazardous or Toxic substances and their quantities

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

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

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

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

Attachment 1

"Hereby, ZKTECO CO.,LTD declares that this Product is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU.

This device complies with Part 15 of the FCC Rules.

Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and

(2) This device must accept any interference received,

including interference that may cause undesired operation.

Warning: Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

"This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment.

This equipment should be installed and operated with a minimum distance of 20 cm between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter."

ZKTeco Industrial Park, No. 32, Industrial Road,

Tangxia Town, Dongguan, China.

Phone : +86 769 - 82109991

Fax : +86 755 - 89602394

www.zkteco.com